Theoretical Computer Science 565 (2015) 30–49

Contents lists available at ScienceDirect

Theoretical Computer Science

www.elsevier.com/locate/tcs

# Visual cryptograms of random grids for threshold access structures ☆

Shyong Jian Shyu [1]

*Department of Computer Science and Information Engineering, Ming Chuan University, Guei Shan, Taoyuan 33348, Taiwan*

A R T I C L E I N F O

*Article history:*
Received 22 April 2014
Received in revised form 12 October 2014
Accepted 28 October 2014
Available online 4 November 2014
Communicated by G. Ausiello

*Keywords:*
Visual cryptography
Threshold visual secret sharing
Random grids
Pixel expansion

A B S T R A C T

Based on a new model of visual cryptograms of random grids (VCRG), we design novel algorithms to generate a set of threshold $(k, n)$-VCRG for sharing a secret image $P$ among $n$ participants in such a way that any group of $k$ out of the $n$ encrypted transparencies reveals $P$ to our eyes when superimposed, while any group of less than $k$ transparencies obtains nothing about $P$. Just like conventional visual cryptographic schemes (VCSs), our designs require none of computing devices but merely human visual ability in the decryption process. Yet, our VCRG approach is much simpler and does not need any extra pixel expansion which is inevitable (actually $1/2^{k-1}$ for $n = k$ and even larger for $n > k$) in VCSs. The correctness of our algorithms is formally proved and experimentally demonstrated. The light contrast in our best algorithm is cautiously analyzed and shown to be as effective as that in a quality threshold VCS when $k$ shares are superimposed. With theoretic and practical interests, our VCRG model exposes new possibilities to the researches of visual secret sharing.

© 2014 Elsevier B.V. All rights reserved.

## 1. Introduction

To protect information from malicious interception or depredation, many elegant algorithms have been developed in traditional cryptography. Modern technologies such as data hiding, watermark, steganography, etc., may be other choices for safeguarding information. These approaches require electronic computing devices to provide the computations in both of the encryption and decryption processes. In general, the higher the level of secrecy is demanded, the more the computations are needed. The common vulnerability of these approaches would be the damage of the ciphertext (or key) itself by malicious intruders or improper storage management such as the humidity or exceptional weather disasters (say flood, earthquake, etc.). Once the ciphertext (or key) has been physically ruined, the secret cannot be recovered.

*Secret sharing* is another choice for protecting information. In a $k$ *out of* $n$ (or $(k, n)$) secret sharing scheme, a secret is encoded into $n$ parts distributed to $n$ participants such that any group of $k$ participants can decode the secret using their parts, while that of less than $k$ ones cannot. The secret is thus *shared* among the $n$ participants and tolerant to a loss of $n - k$ parts. This relieves the vulnerability of the aforementioned approaches to a certain degree. Still, the electronic computations are inevitable in both encoding and decoding.

☆ This research was supported in part by the Ministry of Science and Technology, Taiwan, under Grants MOST 102-2221-E-130-005 and 103-2221-E-130-002-MY3.

*E-mail addresses:* sjshyu@mail.mcu.edu.tw, sjshyu@gmail.com.

[1] Tel.: +886 3 3507001x3322; fax: +886 3 3593874.

http://dx.doi.org/10.1016/j.tcs.2014.10.048
0304-3975/© 2014 Elsevier B.V. All rights reserved.

In some circumstances where the cost of computations may not be affordable, the decoding time should be instantly done in a constant time, or the recognition of the secret shape/pattern is sensitive or meaningful only to the human perception, to name a few, these computation-based algorithms become no longer appropriate.

*Visual cryptography* proposed by Naor and Shamir at Eurocrypt'94 [1] is a visual version of secret sharing. A secret image can be shared among several participants and the decoding process is done by human visual ability so that no computation is required. Specifically, a $k$ out of $n$ *threshold visual cryptographic scheme* ($(k,n)$-VCS) is able to encrypt a binary secret image $P$ into $n$ ($\geq 2$) shares printed as transparencies such that only when $k$ ($\leq n$) transparencies are superimposed altogether can $P$ be revealed to our eyes, while any group of less than $k$ transparencies receives nothing about $P$. Their $(k,n)$-VCS integrates the ability of human visual perception into the decryption process to absolve the computation requirement in a perfectly secure way.

With such an attractive feature that no computation is required but only human visual perception in decoding, visual cryptography has drawn much attention since then. Essentially, a $(k,n)$-VCS, based upon the definition in [1], expands each pixel $p$ in $P$ into $n$ shares of $m$ sub-pixels each (represented as an $n \times m$ *basis matrix* $B^p$ for $p \in \{0,1\}$) to diffuse and disguise $p$ which would only be visually perceivable with *a loss of contrast* by stacking $k$ (or more) transparencies. Therefore, (1) the *pixel expansion* ($m$) of the basis matrices, i.e. the number of the sub-pixels to encode each pixel, (2) the *relative contrast* between the reconstructed white and black pixels are the most critical measurements to evaluate the effectiveness of a $(k,n)$-VCS. It is expected that the pixel expansion of a VCS could be as smaller as possible (to avoid a large size of the encoded shares), while the contrast as higher as possible (to ease our visual recognition of the reconstructed result).

The general construction of a $(k,n)$-VCS was first introduced by Naor and Shamir [1]. Based upon their elegant $(k,k)$-VCS (in which the pixel expansion $2^{k-1}$ has been proved to be optimal [1]), they incorporated the skills of *k-wise independent hash functions* or *small-bias probability spaces* to prove the existence of a $(k,n)$ scheme with pixel expansion $m_{\text{VCS}}^{(k,n)} = n^k \times 2^{k-1}$ or $\log n \times 2^{O(k \log k)}$, respectively. Ateniese et al. [2] presented a construction for $(k,n)$-VCSs by using *perfect hashing*. Their scheme takes $m_{\text{VCS}}^{(k,n)} = l \times 2^{k-1}$ where $l$ is about $O((\log n)^{\log(C(k,2)+1)})$ or $O(ke^k)\log n$ depending on the perfect hashing function adopted. Droste [3] deliberately devised a constructive algorithm with a smaller pixel expansion than the previous results. Kotoh and Imai [4] formulated the relations between the basis matrices and the requirements of a $(k,n)$-VCS as a linear system and built the basis matrices by solving the linear system. Their approach results in the same pixel expansion as Droste's scheme. By adopting sophisticated skills of linear programming, the optimum pixel expansion of a $(2,n)$-VCS was shown by Eisen and Stinson [5] and that of a general $(k,n)$-VCS was explored by Shyu and Chen [6].

On the basis of $(k,n)$-VCSs, more interesting subjects such as the constructions, bounds or contrasts [1,7–9,12], *general access structures* (GAS) [2,7], *extended capabilities* [10], *region incrementing* [11], or realizations for color images [12–15], and so on have been developed in the circuit of visual secret sharing. The role of an effective $(k,n)$-VCS is undoubtedly substantial.

The concept of *random grids* was initially introduced in [16] for encrypting a secret image. It may be the first successful incorporation of human visual intelligence and cryptography. Shyu gave a formal definition to the *visual cryptograms of random grids* (VCRG) to make VCRG applicable in visual secret sharing and devised algorithms for $(2,2)$-VCRG [17], $(k,k)$-VCRG [18], VCRG for sharing multiple secrets [19] and VCRG for GAS [20]. Similar works by other research groups could also be found in [21–23]. The most essential advantage of applying VCRG lies in that neither extra pixel expansion nor basis matrices are needed.

Our goals in this paper include (1) to develop more effective algorithms for producing $(k,n)$-VCRG without any extra pixel expansion nor any basis matrix, and (2) to compare the performances of the proposed $(k,n)$-VCRGs. As compared to those $(k,n)$-VCSs which take pixel expansions no less than $2^{k-1}$ and are based upon sophisticated mathematical knowledge, our algorithms are much simpler, not needing any basis matrices and $m_{\text{VCRG}} = 1$ (so that the encoded shares are of the same size as the original secret).

The rest of the paper is organized as follows. Section 2 introduces the definition of a conventional $(k,n)$-VCS, illustrates the basic concepts of VCS and VCRG, and clarifies the advantages/disadvantages between them. Section 3 establishes the foundation of VCRG and presents the designs and analyses of the proposed $(k,n)$-VCRG algorithms. The experimental results and analytic discussions are given in Section 4. Concluding remarks are drawn in Section 5.

## 2. VCS vs. VCRG

### 2.1. Definition of $(k,n)$-VCS

Let $H(V)$ denote the Hamming weight of a binary vector $V$. The definition of a $(k,n)$-VCS proposed by Naor and Shamir [1] with parameters $k$, $n$, $m$, $d$ and $\alpha$ is as follows where $2 \leq k \leq n$, $1 \leq d \leq m$ and $0 < \alpha < 1$.

**Definition 1.** A solution to the $k$ out of $n$ visual secret sharing scheme consists of two collections of $n \times m$ Boolean matrices $C_0$ and $C_1$. To share a white pixel, the dealer randomly chooses one of the matrices in $C_0$, and to share a black pixel, the dealer randomly chooses one of the matrices in $C_1$. The chosen matrix defines the color of the $m$ sub-pixels in each one of the $n$ transparencies. The solution is considered valid if the following three conditions are met:

1. For any $S$ in $C_0$, the "or" $V$ of any $k$ of the $n$ rows satisfies $H(V) \leq d - \alpha \cdot m$.
2. For any $S$ in $C_1$, the "or" $V$ of any $k$ of the $n$ rows satisfies $H(V) \geq d$.

**Table 1**
Encoding $p$ in $(2,2)$-VCS.

| $p$ | Probability | $s_1$ | $s_2$ | $s = s_1 \otimes s_2$ | $H(s)$ | $\alpha(s)$ |
|---|---|---|---|---|---|---|
| □ | 0.5 | □■ | □■ | □■ | 1 | 1/2 |
| | 0.5 | ■□ | ■□ | ■□ | | |
| ■ | 0.5 | □■ | ■□ | ■■ | 0 | |
| | 0.5 | ■□ | □■ | ■■ | | |

3. For any subset $\{i_1, i_2, \ldots, i_q\}$ of $\{1, 2, \ldots, n\}$ with $q < k$, the two collections of $q \times m$ matrices $D_t$ for $t \in \{0,1\}$ obtained by restricting each $n \times m$ matrix in $C_t$ to rows $i_1, i_2, \ldots, i_q$ are indistinguishable in the sense that they contain the same matrices with the same frequencies.

For any $\{i_1, i_2, \ldots, i_k\} \subseteq \{1, 2, \ldots, n\}$, let $V_0$ ($V_1$) be the "or" vector of rows $i_1, i_2, \ldots, i_k$ in $S_0 \in C_0$ ($S_1 \in C_1$). The first two are the *contrast conditions* that ensure the existence of a difference $\alpha \cdot m$ ($>0$) between $H(V_0)$ and $H(V_1)$ so that our eyes are able to identify the color (white or black) of each pixel when $k$ shares are stacked. Consequently, the *contrast*, the relative difference in weight between the reconstructed black and white pixels, is measured by $\alpha = (H(V_1) - H(V_0))/m$ [1]. The third is the *security condition* which insists that $D_0$ and $D_1$ are indistinguishable, which results in the same number of white/black sub-pixels in either white or black pixels, so that our eyes cannot tell white from black pixels when any group of less than $k$ shares are stacked. It is the security condition that guarantees the information-theoretic security in a $(k,n)$-VCS.

Two $n \times m$ Boolean matrices $B^0$ and $B^1$, called *basis matrices*, which generate any matrix in $C_0$ and $C_1$ by simply taking a column permutation where $m! = |C_0| = |C_1|$, have been adopted in [2–10,13–15] to reduce the storage requirement and simplify the discussions. Based on the basis matrices, Shyu and Chen [6] give an equivalent definition for $(k,n)$-VCS as follows:

**Definition 2.** A set of two $n \times m$ Boolean basis matrices $B_0$ and $B_1$, in which the result of a column permutation of $B_p$ defines the color of the $m$ sub-pixels in each one of the $n$ transparencies when sharing each pixel $p \in \{0,1\}$, constitutes a $(k,n)$-VCS ($k \le n$) if the following two conditions are met:

(a) $H(B_U^0) < H(B_U^1)$ for $U = \{i_1, i_2, \ldots, i_k\} \subseteq \{1, 2, \ldots, n\}$ with $|U| = k$;

(b) $H(B_V^0) = H(B_V^1)$ for $V = \{i_1, i_2, \ldots, i_q\} \subseteq \{1, 2, \ldots, n\}$ with $|V| = q < k$;

where $B_U^p$ ($B_V^p$) denotes the "or" result of rows $i_1, i_2, \ldots, i_k$ ($i_1, i_2, \ldots, i_q$) in $B^p$.

(a) and (b) are the contrast and security conditions, respectively. Definition 2 restates Definition 1 in terms of basis matrices and Hamming weights. This inspires our definition of $(k,n)$-VCRG, which will be introduced in Section 3.2, to a certain degree. Let us introduce the basic concepts of VCS and VCRG informally to see the differences between them in the next subsection.

### 2.2. Basic concepts of VCS and VCRG

We first illustrate the encoding process of each secret pixel $p \in P$ in Naor and Shamir's $(2,2)$-VCS in Table 1 where $s_1$ and $s_2$ are the encoded pixels for participant 1 and 2, respectively, and $\otimes$ is the generalized OR operation representing the superimposition of two pixels (or transparencies).

It is seen from Table 1 that $p$, no matter □ (0) or ■ (1), is encoded into $s_1$ and $s_2$ as blocks of two pixels: □■ or ■□. The probability 0.5 means that the patterns in rows 1 and 2 for $p = 0$ (or rows 3 and 4 for $p = 1$) are randomly chosen for each $p \in P$. No clue about $p$ can be retrieved from observing $s_1$ and $s_2$ separately. Note that the probability for guessing $p$ correctly by participant 1 (2) owning $s_1$ ($s_2$) is 1/2, which is the same as that by any one else with a blind guess. That is, owing $s_1$ ($s_2$) individually has no benefit for participant 1 (2) to guess $p$ correctly (that is, participant 1 (2) has no clue to $p$). The security is guaranteed. Further, $p = 0$ is reconstructed by a block of □■ or ■□, while $p = 1$ by a block of ■■. Our visual ability is able to recognize the difference between them so that we can identify $p = 0$ or 1 from $s_1 \otimes s_2$ (even with a loss of contrast). In this $(2,2)$-VCS, $m_{\text{VCS}}^{(2,2)} = 2$ since each pixel is expanded into a block of two pixels, and the contrast is $\alpha(s) = (H(s(1)) - H(s(0)))/m = (2-1)/2 = 1/2$ where $s = s_1 \otimes s_2$ and $s(0)(s(1))$ denotes such an $s$ whose corresponding $p$ is 0 (1).

The encoding concept of $p$ in Table 1 can be represented by two $2 \times 2$ basis matrices:

$$B^0 = \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix} \quad \text{and} \quad B^1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix},$$

in which $H(B_U^0) < H(B_U^1)$ and $H(B_V^0) = H(B_V^1)$ are satisfied for $U = \{1,2\}$ and $V = \{1\}$ or $\{2\}$. By Definition 2, $(B^0, B^1)$ constitutes a $(2,2)$-VCS.

**Table 2**
Encoding $p$ in $(2,2)$-VCRG.

| $p$ | Probability | $r_1$ | $r_2$ | $r = r_1 \otimes r_2$ | $\mathcal{P}r(r=0)$ | $\ell(r)$ |
|---|---|---|---|---|---|---|
| □ | 0.5 | □ | □ | □ | 1/2 | 1/2 |
|  | 0.5 | ■ | ■ | ■ |  |  |
| ■ | 0.5 | □ | ■ | ■ | 0 |  |
|  | 0.5 | ■ | □ | ■ |  |  |

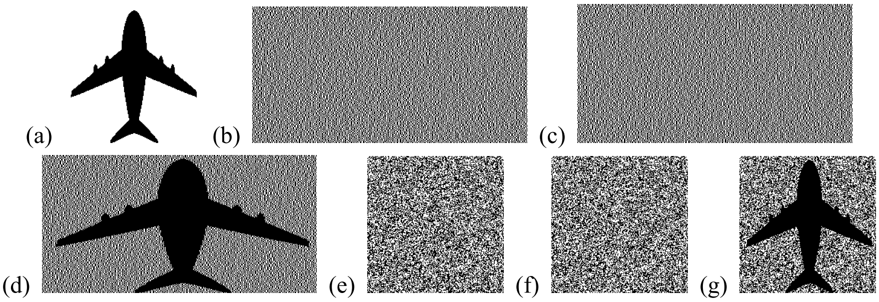

**Fig. 1.** Implementation results of $(2,2)$-VCS and $(2,2)$-VCRG: (a) $P$, (b) $S_1$, (c) $S_2$, (d) $S_1 \otimes S_2$, (e) $R_1$, (f) $R_2$, (g) $R_1 \otimes R_2$.

Table 2 describes the encoding process of a secret pixel $p$ in $(2,2)$-VCRG [17,18] where each $p$ is encoded into two random pixels $r_1$ and $r_2$ without any extra pixel expansion.

Basically, $r_1$ is randomly chosen from 0 (□, transparent) or 1 (■, opaque) and $r_2 = r_1$ ($\bar{r}_1$, the complement of $r_1$), if $p = 0$ (1). The probability for $r_1 = 0$ is $\mathcal{P}r(r_1 = 0) = 1/2$, the same as $\mathcal{P}r(r_2 = 0)$. In spite of owning $r_1$ ($r_2$), participant 1 (2) still acquires no information about $p = 0$ or 1 so that he can only guess $p$ blindly like any outsider having no share. The security is thus guaranteed (as secure as in $(2,2)$-VCS). Let $r = r_1 \otimes r_2$ and $r(0)$ ($r(1)$) denote such an $r$ whose corresponding $p$ is 0 (1). We see from Table 2 that $r(1)$ recovers $p = 1$ flawlessly with $\mathcal{P}r(r(1) = 0) = 0$, while $r(0)$ recovers $p = 0$ with $\mathcal{P}r(r(0) = 0) = 1/2$. Hence, the black and white pixels can be recognized due to the difference between $r(0)$ and $r(1)$. The probabilities for $r_i(p) = 0$ and $r(p) = 0$ will be defined later as the *light transmissions* of $r_i$ and $r$ for $p \in \{0,1\}$ and $i \in \{1,2\}$ and we shall deliberately judge the security and contrast in VCRG in terms of light transmissions in Section 3. Note that the basis matrices and Hamming weights in VCS do not exist here.

Fig. 1 shows the implementation results of these two schemes. Secret image $P$ is encoded into $S_1$ and $S_2$ ($R_1$ and $R_2$) by $(2,2)$-VCS ($(2,2)$-VCRG), in which each pixel $p \in P$ is encoded according to Table 1 (2). It is easily seen that $S_1$, $S_2$, $R_1$ and $R_2$ are merely random pictures (from which no clue about $P$ can be obtained), whereas $S_1 \otimes S_2$ and $R_1 \otimes R_2$ reveal $P$ to our eyes.

The contrast between the reconstructed white and black pixels in $S_1 \otimes S_2$ is 1/2, and the difference between the light transmissions of those in $R_1 \otimes R_2$ is also 1/2. The size of $S_1$ and $S_2$ is twice of that of $P$ since $m_{\text{VCS}}^{(2,2)} = 2$, while the size of $R_1$ and $R_2$ is the same as that of $P$ because of $m_{\text{VCRG}} = 1$. To maintain the aspect ratio of $P$ in $S_1 \otimes S_2$, we may use

$$B^0 = \begin{bmatrix} 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 \end{bmatrix} \quad \text{and} \quad B^1 = \begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix}$$

to encode $P$ into $S'_1$ and $S'_2$ whose width and height become twice of those of $P$. The pixel expansion then increases up to $m_{\text{VCS}}^{(2,2)} = 4$.

### 2.3. Advantages and disadvantages between VCS and VCRG

VCRG takes no extra pixel expansion, but it sacrifices the reconstruction ability of white pixels. Let us observe $s = s_1 \otimes s_2$ in Table 1 and $r = r_1 \otimes r_2$ in Table 2. From $s(0)$ (□■ or ■□) and $s(1)$ (■■) in VCS, we can exactly recognize the corresponding $p$ as 0 and 1, respectively. However, from $r(0)$ (□ or ■) and $r(1)$ (■) in VCRG, we cannot do so accurately since all $r(1)$'s are ■'s, but about half $r(0)$'s are □ and the other half become ■'s, too. We say that VCS maintains the reconstruction ability of both $p = 0$ and 1 in $s(0)$ and $s(1)$, respectively, at the expense of pixel expansion; whereas, VCRG prevents any pixel from expanding with a compromise of losing about 50% of the reconstruction of $p = 0$ from $r(0)$. Or simply, VCRG saves space but sacrifices precision. Therefore, small false black regions are likely to appear in regions that should be white in VCRG. This may result in: (1) small white regions would be mis-reconstructed as black; or (2) small black regions are hardly recognized when surrounded by false black ones.

Fig. 2 deliberately elucidates the reconstruction abilities of $(2,2)$-VCS and $(2,2)$-VCRG for dealing with small white/black regions. Fig. 2(a) is the secret image $P$ consisting of 8 kinds ($10 \times 10$, $8 \times 8$, $6 \times 6$, $5 \times 5$, $4 \times 4$, $3 \times 3$, $2 \times 2$, $1 \times 1$ pixels) of 8 white regions with a black background; (b) shows $S_1 \otimes S_2$ by $(2,2)$-VCS, which reconstructs all white and black pixels in $P$ flawlessly with $m_{\text{VCS}} = 2$; while (c) gives $R_1 \otimes R_2$ by $(2,2)$-VCRG with $m_{\text{VCRG}} = 1$, in which about 50% $1 \times 1$ white

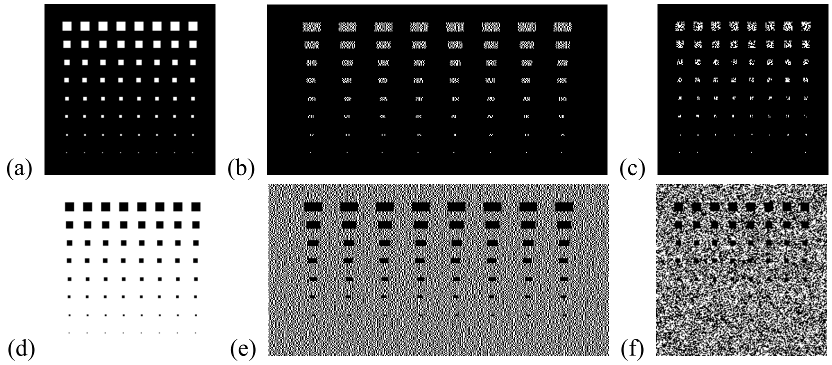

**Fig. 2.** Reconstruction abilities of VCS and VCRG: (a) $P$, (b) $S_1 \otimes S_2$, (c) $R_1 \otimes R_2$; (d) $P'$, (e) $S'_1 \otimes S'_2$, (f) $R'_1 \otimes R'_2$.

regions are mis-reconstructed as black (see the bottom row of Fig. 2(c)). On the other hand, Fig. 2(d) is $P'$ consisting of 8 kinds (as (a)) of 8 black regions with a white background; (e) depicts $S'_1 \otimes S'_2$ by $(2,2)$-VCS, which reconstructs almost all white and black regions in $P'$ flawlessly except those of $1 \times 1$ ones; while (f) illustrates $R'_1 \otimes R'_2$ by $(2,2)$-VCRG, in which those regions no greater than $3 \times 3$ cannot be identified precisely since too many small false black regions are around.

We should point out that the $1 \times 2$ blocks of ■■'s (corresponding to one black pixel in $P'$) in $S'_1 \otimes S'_2$ cannot be recognized, either (see Fig. 2(e)). It is because they are surrounded by either □■ or ■□ (corresponding to white pixels in $P'$) with an equal probability so that blocks of ■■, ■□, □■ or □□ would be seen with an equal chance in the neighborhood. Hence, VCS cannot reconstruct every black pixel on condition that it is surrounded by white pixels.

Nevertheless, VCRG works well as long as the white/black regions are not too small (say, no less than $3 \times 3$ pixels in this $(2,2)$ case) in $P$. Regarding the study on the lower bound of the size of a recognizable white/black region in the reconstructed result for VCRG, please refer to [19,24]. This paper thus excludes the sharing of those secret images whose critical information is characterized by very small white/black regions. As compared to $(k,n)$-VCS, whose pixel expansion is larger than $m_{\mathrm{VCS}}^{(k,k)} = 2^{k-1}$ (see Table 7 in Appendix A), our $(k,n)$-VCRG with $m_{\mathrm{VCRG}}^{(k,n)} = 1$ is more appealing and attractive. The indispensable pixel expansion degrades the attraction of VCSs in some practical applications where a large share size is not preferred or not allowed. For instance, 7 colleagues open a joint bank-account which can be accessed when each group of 5 agrees. When sending them a new/updated group identification number (GIN), the bank sends each of them one share from a set of $(5,7)$-VCRG. Each group of 5 (who agree to access) could see the GIN instantly by superimposing their random grids. On condition that a $(5,7)$-VCS is applied, the size of the shares becomes at least 48 times than that of VCRG since the optimal pixel expansion of $(5,7)$-VCS is 48 $(= 6 \times 8,\ 8 \times 6$, or else) [3,6]. If the aspect ratio would be maintained, the size of the VCS shares grows 49 $(= 7 \times 7)$ times larger. Even though VCRG sacrifices precision for recovering very small white/black regions, the reconstructed GIN containing alphabets and/or numbers would not be misrecognized under VCRG with a moderate size. Using VCS with a size 48 (or 49) times larger would be rather impractical and inconvenient.

## 3. $(k, n)$ visual cryptograms of random grids

To be self-contained, we summarize the basic concepts of random grids [17,18] in Section 3.1 and then define $(k,n)$-VCRG in Section 3.2. Four algorithms: $(2,n)$-, $(k,k)$-, $(k,n)$- and enhanced $(k,n)$-VCRGs and their correctness proofs are presented in Sections 3.3–3.6, respectively.

### 3.1. Preliminaries

Consider a binary transparency $Y$ in which each pixel $y$ is either transparent (0) or opaque (1). Suppose that the value of each pixel $y$ is determined by a biased coin-flip procedure with parameter $\lambda$ such that the probability of $y = 0$ is $\lambda$. We refer to $y$ as a *random pixel* with $\mathcal{P}r(y = 0) = \lambda$. Due to the fact that $y = 0$ lets through light, while $y = 1$ stops it, we define the *light transmission* of $y$, denoted by $t(y)$, to be $\mathcal{P}r(y = 0)$. Formally,

**Definition 3.** $y$ is a random pixel with a light transmission of $t(y) = \lambda$ if and only if $\mathcal{P}r(y = 0) = \lambda$ where $\lambda$ is a constant and $0 < \lambda < 1$.

Once $t(y) = \lambda$ for each pixel $y \in Y$, we call $Y$ a random grid, defined as follows.

**Definition 4.** $Y$ is a *random grid* with a light transmission of $\mathcal{T}(Y) = \lambda$ if and only if $t(y) = \lambda$ for each pixel $y \in Y$.

Figs. 3(a), (b) and (c) illustrate three random grids $Y_1$, $Y_2$ and $Y_3$, respectively, with $\mathcal{T}(Y_i) = t(y_i) = 0.3, 0.5$ and 0.7 for each pixel $y_i \in Y_i$ where $1 \le i \le 3$. It is easily seen that one random grid looks as a seemingly random picture.

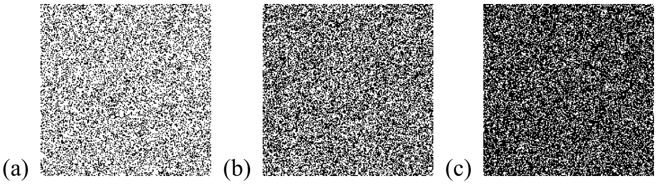

**Fig. 3.** Examples of random grids: (a) $Y_1$, (2) $Y_2$, (3) $Y_3$.

The following explores some primitive properties of random grids (or random pixels).

**Lemma 1.** *If $X$ is a random grid with $\mathcal{T}(X) = \lambda$, $X \otimes X$ is a random grid with $\mathcal{T}(X \otimes X) = \mathcal{T}(X) = \lambda$.*

**Proof.** Since $x \otimes x = x$ for each random pixel $x \in X$, thus $\mathcal{T}(X \otimes X) = t(x \otimes x) = t(x) = \mathcal{T}(X) = \lambda$. □

**Lemma 2.** *If $X$ and $Y$ are two independent random grids with $\mathcal{T}(X) = \lambda_1$ and $\mathcal{T}(Y) = \lambda_2$, $X \otimes Y$ is also a random grid with $\mathcal{T}(X \otimes Y) = \lambda_1\lambda_2$.*

**Proof.** Let $x \in X$ and $y \in Y$ be the *corresponding pixels* whose coordinates are the same in $X$ and $Y$, respectively. We have $t(x) = \mathcal{P}r(x = 0) = \lambda_1$ and $t(y) = \mathcal{P}r(y = 0) = \lambda_2$. Because $x$ and $y$ are independent, $x \otimes y = 0$ if and only if $x = 0$ and $y = 0$. Thus $t(x \otimes y) = \mathcal{P}r(x \otimes y = 0) = \mathcal{P}r(x = 0 \text{ and } y = 0) = \mathcal{P}r(x = 0) \times \mathcal{P}r(y = 0) = \lambda_1\lambda_2$. □

Let $\bar{X}$ be the complement of $X$, that is, each corresponding pixel of $x \in X$ in $\bar{X}$ is $\bar{x}$ and **1** be a transparency consisting of all opaque (1) pixels.

**Lemma 3.** *If $X$ is a random grid with $\mathcal{T}(X) = \lambda$ and $Y = \bar{X}$, $\mathcal{T}(Y) = 1 - \lambda$ and $\mathcal{T}(X \otimes Y) = \mathcal{T}(\mathbf{1}) = 0$.*

**Proof.** Since $y = \bar{x}$ and $t(x) = \lambda$ for each pair of corresponding pixels $x \in X$ and $y \in Y$, we have $t(y) = 1 - \lambda$ and $\mathcal{T}(Y) = 1 - \lambda$. In addition, $x \otimes y = x \otimes \bar{x} = 1$. Therefore, $X \otimes Y$ contains only opaque pixels so that $\mathcal{T}(X \otimes Y) = \mathcal{T}(\mathbf{1}) = 0$. □

### 3.2. Definition of $(k, n)$-VCRG

Let us examine the (2, 2)-VCRG in Section 2.2 where secret image $P$ is encoded into shares $R_1$ and $R_2$. Let $P(0)(P(1))$ denote the area of white/transparent (black/opaque) pixels in $P$ and $A[P(p)]$ be the area in $A$ corresponding to $P(p)$ where $p \in \{0, 1\}$. From Table 2 and Definitions 3 and 4, we know that $r_1 \in R_1$ and $r_2 \in R_2$ are random pixels with $t(r_1) = 1/2 = t(r_2)$ so that $R_1$ and $R_2$ are indeed random grids. The security for $R_i$ is guaranteed by $\mathcal{T}(R_i[P(0)]) = 1/2 = \mathcal{T}(R_i[P(1)])$, which means the areas of white and black pixels in $P$ cannot be recognized from $R_i[P(0)]$ and $R_i[P(1)]$ for $i \in \{1, 2\}$. In addition, the contrast of $R$ $(= R_1 \otimes R_2)$ results from $\mathcal{T}(R[P(0)]) > \mathcal{T}(R[P(1)])$ since $\mathcal{T}(R[P(0)]) = \mathcal{T}(R_1[P(0)] \otimes R_2[P(0)]) = \mathcal{T}(R_1[P(0)]) = 1/2 > 0 = \mathcal{T}(R[P(1)]) = \mathcal{T}(R_1[P(1)] \otimes R_2[P(1)]) = \mathcal{T}(R_1[P(1)] \otimes \overline{R_1[P(1)]}) = \mathcal{T}(\mathbf{1})$ by Lemma 3. We realize that the light transmissions corresponding to $P(0)$ and $P(1)$ on $R_1$, $R_2$ or $R$ $(= R_1 \otimes R_2)$ establish effective measurements for judging the security in each of $R_1$ and $R_2$ and contrast in $R$.

Now, consider $P$ shared among $n$ participants. We define a feasible set of $(k, n)$-VCRG of $P$ in terms of light transmissions formally as follows.

**Definition 5.** Given a secret image $P$, $n$ participants sharing $P$ and a threshold integer $k$ $(\leq n)$, $\mathcal{R} = \{R_1, R_2, \ldots, R_n\}$ is a set of *k out of n visual cryptograms of random grids* (referred to as $(k, n)$-VCRG) of $P$ if the following conditions are met:

(1) $\mathcal{T}(R_i) = 1/2$ for $1 \leq i \leq n$;
(2) $\mathcal{T}(S^{\mathcal{D}}[P(0)]) = \mathcal{T}(S^{\mathcal{D}}[P(1)])$ where $S^{\mathcal{D}} = R_{j_1} \otimes R_{j_2} \otimes \ldots \otimes R_{j_d}$ and $\mathcal{D} = \{R_{j_1}, R_{j_2}, \ldots, R_{j_d}\}$ which is any set of $d$ distinct random grids in $\mathcal{R}$, i.e. $\mathcal{D} \subset \mathcal{R}$, $1 \leq j_v \leq n$, $1 \leq v \leq d$ and $1 < d < k$; and
(3) $\mathcal{T}(S^{\mathcal{K}}[P(0)]) > \mathcal{T}(S^{\mathcal{K}}[P(1)])$ where $S^{\mathcal{K}} = R_{i_1} \otimes R_{i_2} \otimes \ldots \otimes R_{i_k}$ and $\mathcal{K} = \{R_{i_1}, R_{i_2}, \ldots, R_{i_k}\}$ which is any set of $k$ distinct random grids in $\mathcal{R}$, i.e. $\mathcal{K} \subseteq \mathcal{R}$, $1 \leq i_u \leq n$ and $1 \leq u \leq k$.

The first two are called the "security" conditions since $\mathcal{T}(R_i) = 1/2$ $(= \mathcal{T}(R_i[P(0)]) = \mathcal{T}(R_i[P(1)]))$ and $\mathcal{T}(S^{\mathcal{D}}[P(0)]) = \mathcal{T}(S^{\mathcal{D}}[P(1)])$ ensure that the areas corresponding to $P(0)$ and $P(1)$ in $R_i$ and $S^{\mathcal{D}}$, respectively, are not perceivable by our eyes. Indeed, $R_i$ and $S^{\mathcal{D}}$ are merely random grids revealing nothing about $P$ for $1 \leq i \leq n$ and $1 < |\mathcal{D}| < k$. The third is the "contrast" condition which guarantees that $P$ is visually perceptible from $S^{\mathcal{K}}$. Note that this definition inherits but differs from that in Naor and Shamir's model (see Definitions 1 and 2). In terms of light transmission (instead of basis matrices and Hamming weights), our VCRG demands $\mathcal{T}(S^{\mathcal{K}}[P(0)]) > \mathcal{T}(S^{\mathcal{K}}[P(1)])$ and $\mathcal{T}(S^{\mathcal{D}}[P(0)]) = \mathcal{T}(S^{\mathcal{D}}[P(1)])$ to guarantee the visual perception to $P$ from $S^{\mathcal{K}}$ and no recognition of $P$ from $S^{\mathcal{D}}$. Note again that we exclude those secret images whose

**Algorithm 1** $(2, n)$-VCRG.

```
Input: an $h \times w$ binary image $P$ and an integer $n$
Output: a set of $n$ random grids $\mathcal{R} = \{R_1, R_2, \ldots, R_n\}$ constituting $(2, n)$-VCRG of $P$
1.    generate $R_1$ as a random grid, $\mathcal{T}(R_1) = 1/2$
2.    for (each pixel $P[i, j]$, $1 \le i \le h$ and $1 \le j \le w$) do
2.1   {     for $(2 \le t \le n - 1)$ do
                if $(P[i, j] = 0)$ then $R_t[i, j] = R_1[i, j]$
                else $R_t[i, j] = random\_pixel()$
      }
3.    output$(R_1, R_2, \ldots, R_n)$
```

critical information is characterized by very small white/black regions. VCRG does not require any basis matrix and there is no extra pixel expansion.

### 3.3. $(2, n)$-VCRG

To be a set of $(2, n)$-VCRG with respect to $P$, $\mathcal{R} = \{R_1, R_2, \ldots, R_n\}$ should satisfy that $R_u$ and $R_v$ are random grids with $\mathcal{T}(R_u) = \mathcal{T}(R_v) = 1/2$ for $1 \le u \ne v \le n$ and $R_u \otimes R_v$ reveals $P$ to our eyes. Inspired from Table 1, Lemmas 1 and 2, we may encode each $p \in P$ into $n$ pixels $r_1 \in R_1, r_2 \in R_2, \ldots, r_n \in R_n$ such that if $p = 0$, they are $n$ 0's or 1's randomly:

$$r_1 = random\_pixel() \quad \text{and} \quad r_t = r_1 \text{ for } 2 \le t \le n;$$

otherwise $(p = 1)$ they are $n$ independent random pixels:

$$r_t = random\_pixel() \quad \text{for } 1 \le t \le n$$

where $random\_pixel()$ returns 0 or 1 randomly. For any pair of corresponding pixels $r_u$ and $r_v$, our idea ensures $t(r_u(0) \otimes r_v(0)) = t(r_1(0)) = 1/2$ by Lemma 1 due to $r_u(0) = r_1(0) = r_v(0)$; and $t(r_u(1) \otimes r_v(1)) = 1/4$ by Lemma 2 since $r_u(1)$ and $r_v(1)$ are independent random pixels where $1 \le u \ne v \le n$. Algorithm 1 gives the pseudo-codes.

Theorem 1 is an immediate consequence of Algorithm 1, Lemmas 1 and 2.

**Theorem 1.** *$\mathcal{R} = \{R_1, R_2, \ldots, R_n\}$ produced by Algorithm 1 with respect to $P$ constitutes a set of $(2, n)$-VCRG of $P$ with $(\mathcal{T}(S^H[P(0)]), \mathcal{T}(S^H[P(1)])) = (1/2, 1/2^h)$ where $H = \{R_{i_1}, R_{i_2}, \ldots, R_{i_h}\} \subseteq \mathcal{R}$ and $h = |H|$ for $1 \le h \le n$.*

### 3.4. $(k, k)$-VCRG

In [18], several visual secret sharing schemes for producing a set of $(k, k)$-VCRG have been developed. We introduce the algorithm that achieves the best contrast in [18] because their ideas form the foundation of our designs for effective $(k, n)$-VCRGs.

Let $f$ be a binary function transcribing the basic idea in Table 2:

$$f(x, s) = \begin{cases} s & \text{if } x = 0; \\ \bar{s} & \text{otherwise,} \end{cases} \tag{1}$$

for $x, s \in \{0, 1\}$ where $\bar{s}$ is the complement of $s$. We say $f(x, s)$ *preserves* the value of $s$ if $x = 0$, while *reverses* it otherwise $(x = 1)$. The behavior of $f(x, s)$ is equivalent to that of a $T$ flip-flop in sequential circuits or an Exclusive-OR operation $(\oplus)$, that is, $f(x, s) = x \oplus s$.

To construct a set of $(k, k)$-VCRG, namely $\mathcal{Q} = \{Q_1, Q_2, \ldots, Q_k\}$, of $P$, we first generate $k - 1$ random grids $Q_1, Q_2, \ldots, Q_{k-1}$ independently with $\mathcal{T}(Q_t) = 1/2$ for $1 \le t \le k - 1$. Thus, for every pixel $p \in P$, its $k - 1$ corresponding pixels $q_1, q_2, \ldots, q_{k-1}$ are totally random where $q_t \in Q_t$ for $1 \le t \le k - 1$. Based upon $q_1, q_2, \ldots, q_{k-1}$, we compute $a_t$ for $1 \le t \le k - 1$ by

$$a_t = \begin{cases} q_1 & \text{if } t = 1; \\ f(q_t, a_{t-1}) & \text{otherwise.} \end{cases} \tag{2}$$

Then, we determine $q_k$ according to $p$ and $a_{k-1}$ by

$$q_k = f(p, a_{k-1}). \tag{3}$$

After all $q_k$'s corresponding to all $p$'s $\in P$ are computed, we obtain $Q_k$. Then, $\mathcal{Q} = \{Q_1, Q_2, \ldots, Q_k\}$ is reported as a set of $(k, k)$-VCRG of $P$. The whole idea is presented in Algorithm 2.

We outline some useful inferences in [18] in the following.

**Lemma 4.** *Given a set of $w$ independent random grids $\mathcal{W} = \{R_1, R_2, \ldots, R_w\}$ with $\mathcal{T}(R_t) = 1/2$ for $1 \le t \le w$, $S^{\mathcal{W}}$ is a random grid with $\mathcal{T}(S^{\mathcal{W}}) = 1/2^w$ where $S^{\mathcal{W}} = R_1 \otimes R_2 \otimes \ldots \otimes R_w$.*

**Algorithm 2** $(k, k)$-VCRG.

```
Input: an $h \times w$ binary image $P$ and an integer $k$
Output: a set of $k$ random grids $\mathcal{Q} = \{Q_1, Q_2, \ldots, Q_k\}$ constituting $(k, k)$-VCRG of $P$
VCRG($k$, $P$)
    for $(1 \le t \le k-1)$ do generate $Q_t$ as a random grid, $\mathcal{T}(Q_t) = 1/2$
    for (each pixel $P[i, j]$, $1 \le i \le h$ and $1 \le j \le w$) do
    {       $a_1 = Q_1[i, j]$
            for $(2 \le t \le k-1)$ do $a_t = f(Q_t[i, j], a_{t-1})$
            $Q_k[i, j] = f(P[i, j], a_{k-1})$
    }
    output($Q_1, Q_2, \ldots, Q_k$)
```

**Algorithm 2-1** $(k, k)$-RG.

```
Input: an $h \times w$ binary image $P$ and an integer $k$
Output: a set of $k$ random grids $\mathcal{C} = \{C_1, C_2, \ldots, C_k\}$ constituting $(k, k)$-VCRG of $P$
RG($k$, $P$)
    $(C_1, D_1) = $ VCRG(2, $P$)
    for $(2 \le t \le k-1)$ do
    {       $(C_i, D_i) = $ VCRG(2, $D_{i-1}$)
    }
    $C_k = D_{k-1}$
    output($C_1, C_2, \ldots, C_k$)
```

Lemma 4 is easily proved by applying Lemma 2.

Let $\mathcal{Q} = \{Q_1, Q_2, \ldots, Q_k\}$ denote the set of $k$ random grids obtained by Algorithm 2 with respect to $P$, i.e. $\mathcal{Q} =$ VCRG($k$, $P$).

**Lemma 5.** *$S^{\mathcal{V}}$ is a random grid with $\mathcal{T}(S^{\mathcal{V}}) = 1/2^v$ $(= \mathcal{T}(S^{\mathcal{V}}[P(0)]) = S^{\mathcal{V}}[P(1)]))$ where $\mathcal{V} = \{Q_{j_1}, Q_{j_2}, \ldots, Q_{j_v}\} \subset \mathcal{Q}$, $1 \le v < k$ and $S^{\mathcal{V}} = Q_{j_1} \otimes Q_{j_2} \otimes \ldots \otimes Q_{j_v}$.*

**Lemma 6.** *$(\mathcal{T}(S^{\mathcal{Q}}[P(0)]), \mathcal{T}(S^{\mathcal{Q}}[P(1)])) = (1/2^{k-1}, 0)$ where $S^{\mathcal{Q}} = Q_1 \otimes Q_2 \otimes \ldots \otimes Q_k$.*

Following Definition 5 and Lemmas 4–6, we obtain Theorem 2.

**Theorem 2.** *$\mathcal{Q} = \{Q_1, Q_2, \ldots, Q_k\}$ produced by Algorithm 2 with respect to $P$ constitutes a set of $(k, k)$-VCRG of $P$ with $(\mathcal{T}(S^{\mathcal{Q}}[P(0)]), \mathcal{T}(S^{\mathcal{Q}}[P(1)])) = (1/2^{k-1}, 0)$.*

Please refer to [18] for the detailed proofs to Lemmas 5, 6 and Theorem 2. Note that Chen and Tsao presented another algorithm independently for the $(k, k)$ structure [21], named as $(k, k)$-RG (since "RG-based scheme" was referred in their subsequent researches [22,23]), in which the $(2, 2)$-VCRG is applied $n-1$ times (see Algorithm 2-1).

The proofs to the correctness of Algorithm 2-1 for producing $\mathcal{C} = \{C_1, C_2, \ldots, C_k\}$ as a set of $(k, k)$-VCRG can be found in [21]. In addition, $(\mathcal{T}(S^{\mathcal{C}}[P(0)]), \mathcal{T}(S^{\mathcal{C}}[P(1)])) = (1/2^{k-1}, 0) = (\mathcal{T}(S^{\mathcal{Q}}[P(0)]), \mathcal{T}(S^{\mathcal{Q}}[P(1)]))$. That is, the resultant light transmissions in Algorithms 2-1 [21] and 2 [18] are exactly the same. In the following designs and proofs, whenever a set of $(k, k)$-VCRG is demanded as a basis, we adopt Algorithm 2.

### 3.5. $(k, n)$-VCRG

An intuitive development for constructing $\mathcal{R} = \{R_1, R_2, \ldots, R_n\}$ as a set of $(k, n)$-VCRG of $P$ is as follows. We first adopt Algorithm 2 to prepare a set of $(k, k)$-VCRG $\mathcal{Q} = \{Q_1, Q_2, \ldots, Q_k\}$ with respect to $P$. For each secret pixel $p \in P$, we organize $\mathcal{Q} = \{q_1, q_2, \ldots, q_k\}$ and $\mathcal{G} = \{g_1, g_2, \ldots, g_{n-k}\}$ where $q_t \in Q_t$ is the corresponding pixel of $p$ for $1 \le t \le k$ and $g_v$ is merely a random pixel with $t(g_v) = 1/2$ for $1 \le v \le n-k$. Then, we encode $p$'s $n$ corresponding pixels $r_1, r_2, \ldots, r_n$ (in $R_1, R_2, \ldots, R_n$, respectively) to be the $n$ elements of a random permutation of $\mathcal{Q} \cup \mathcal{G}$, denoted by $(r_1, r_2, \ldots, r_n) = \mathit{permutation}(\mathcal{Q} \cup \mathcal{G})$, for each $p \in P$. After all sets of $r_1, r_2, \ldots, r_n$ corresponding to all $p$'s in $P$ are thus determined, we claim $\mathcal{R} = \{R_1, R_2, \ldots, R_n\}$ is a set of $(k, n)$-VCRG of $P$. Algorithm 3 states the pseudo-codes of our idea.

We investigate the features of the random grids in $\mathcal{R} = \{R_1, R_2, \ldots, R_n\}$ generated by Algorithm 3.

**Lemma 7.** *$\mathcal{T}(R_i) = 1/2$ where $R_i \in \mathcal{R}$ for $1 \le i \le n$.*

**Proof.** Consider $p \in P$ and its $n$ corresponding pixels $r_1 \in R_1, r_2 \in R_2, \ldots, r_n \in R_n$. We obtain

$$\{r_1, r_2, \ldots, r_n\} = \{q_1, q_2, \ldots, q_k\} \cup \{g_1, g_2, \ldots, g_{n-k}\} \quad \text{(referred to as } \mathcal{R} = \mathcal{Q} \cup \mathcal{G}) \tag{4}$$

**Algorithm 3** $(k, n)$-VCRG.

```
Input: an $h \times w$ image $P$, integers $k$ and $n$
Output: $\mathscr{R} = \{R_1, R_2, \ldots, R_n\}$ as a set of $(k, n)$-VCRG with respect to $P$
TVCRG$(k, n, P)$
1.      $(Q_1, Q_2, \ldots, Q_k) = \mathrm{VCRG}(k, P)$
2.      for (each $(i, j)$, $1 \le i \le h$ and $1 \le j \le w$) do
2.1     {     $\mathcal{Q} = \{Q_1[i, j], Q_2[i, j], \ldots, Q_k[i, j]\}$
2.2           for $(1 \le v \le n - k)$ do $g[v] = random\_pixel()$
2.3           $\mathcal{G} = \{g[1], g[2], \ldots, g[n - k]\}$
2.4           $(R_1[i, j], R_2[i, j], \ldots, R_n[i, j]) = permutation(\mathcal{Q} \cup \mathcal{G})$
        }
3.      output$(R_1, R_2, \ldots, R_n)$
```

according to Algorithm 3 where $q_t \in Q_t (\in \mathscr{Q} = \{Q_1, Q_2, \ldots, Q_k\} = \mathrm{VCRG}(k, P))$ with $\mathscr{t}(q_t) = 1/2$ and $\mathscr{t}(g_v) = 1/2$ for $1 \le t \le k$ and $1 \le v \le n - k$. Regarding $R_i \in \mathscr{R}$, each pixel $r_i \in R_i$ is either from $\mathcal{Q} = \{q_1, q_2, \ldots, q_k\}$ or from $\mathcal{G} = \{g_1, g_2, \ldots, g_{n-k}\}$, thus $\mathscr{t}(r_i) = 1/2$. Consequently, $R_i$ is a random grid with $\mathscr{T}(R_i) = 1/2$ for $1 \le i \le n$. □

Suppose that a set of $h$ $(\le n)$ shares, say $\mathscr{H} = \{R_{i_1}, R_{i_2}, \ldots, R_{i_h}\}$, is randomly chosen from $\mathscr{R}$. Consider $p \in P$ and its $k$ corresponding pixels $\mathcal{Q} = \{q_1, q_2, \ldots, q_k\}$ where $q_i \in Q_i (\in \mathscr{Q})$ for $1 \le i \le k$. Let $\mathcal{H} = \{r_{i_1}, r_{i_2}, \ldots, r_{i_h}\}$ denote $p$'s $h$ corresponding pixels in $\mathscr{H}$ where $r_{i_t} \in R_{i_t} (\in \mathscr{H})$ for $1 \le t \le h$. There are two possibilities for comparing $\mathcal{Q}$ against $\mathcal{H}$:

Case I: $\mathcal{Q} \subseteq \mathcal{H}$ $(\{q_1, q_2, \ldots, q_k\} \subseteq \{r_{i_1}, r_{i_2}, \ldots, r_{i_h}\})$; or
Case II: $\mathcal{Q} \not\subset \mathcal{H}$ $(\{q_1, q_2, \ldots, q_k\} \not\subset \{r_{i_1}, r_{i_2}, \ldots, r_{i_h}\})$, i.e. there exists at least one $q_i \in \mathcal{Q}$ but $q_i \notin \mathcal{H}$.

That is, $\mathcal{H}$ belongs to either the class of Case I or that of Case II. If $h < k$, $\mathcal{H}$ is only possible in the class of Case II.

Let $\hbar = r_{i_1} \otimes r_{i_2} \otimes \ldots \otimes r_{i_h}$ and $\hbar(0)$ $(\hbar(1))$ denote such an $h$ whose corresponding $p$ is 0 (1). We compute the light transmissions of $\hbar_{\mathrm{I}}(0)$ and $\hbar_{\mathrm{I}}(1)$ in Case I as well as $\hbar_{\mathrm{II}}(0)$ and $\hbar_{\mathrm{II}}(1)$ in Case II, respectively, as follows.

**Lemma 8.** *If* $\mathcal{Q} \subseteq \mathcal{H}$, $(\mathscr{t}(\hbar_{\mathrm{I}}(0)), \mathscr{t}(\hbar_{\mathrm{I}}(1))) = (1/2^{h-1}, 0)$.

**Proof.** Since $\mathcal{Q} \subseteq \mathcal{H}$, we realize from Algorithm 3 that $\mathcal{H}$ is composed by all $k$ pixels in $\mathcal{Q}$ and $h - k$ random pixels, say $g_{j_1}, g_{j_2}, \ldots, g_{j_{h-k}}$, in $\mathcal{G}$ corresponding to $p \in P$, that is,

$$\mathcal{H} = \{r_{i_1}, r_{i_2}, \ldots, r_{i_h}\} = \{q_1, q_2, \ldots, q_k\} \cup \{g_{j_1}, g_{j_2}, \ldots, g_{j_{h-k}}\} = \mathcal{Q} \cup \mathcal{G}' \tag{5}$$

where $\mathcal{G}' \subseteq \mathcal{G}$ (see formula (4)) and $1 \le j_v \le n - k$ for $1 \le v \le h - k$. Without loss of generality, let $r_{i_1} = q_1, r_{i_2} = q_2, \ldots, r_{i_k} = q_k$ and $r_{i_{k+1}} = g_{j_1}, r_{i_{k+2}} = g_{j_2}, \ldots, r_{i_h} = g_{j_{h-k}}$ (which can be easily accomplished by renaming all $r_{i_t}$'s for $1 \le t \le h$). Let $\mathscr{q} = r_{i_1} \otimes r_{i_2} \otimes \ldots \otimes r_{i_k}$, $\mathscr{g} = r_{i_{k+1}} \otimes r_{i_{k+2}} \otimes \ldots \otimes r_{i_h}$. Thus $\hbar = \mathscr{q} \otimes \mathscr{g}$. By Theorem 2, we have $(\mathscr{t}(\mathscr{q}(0)), \mathscr{t}(\mathscr{q}(1))) = (1/2^{k-1}, 0)$ where $\mathscr{q}(p) \in S^{\mathcal{Q}}[P(p)]$ for $p \in \{0, 1\}$; also, $\mathscr{t}(\mathscr{g}(0)) = \mathscr{t}(\mathscr{g}(1)) = 1/2^{h-k}$ for stacking $h - k$ random pixels. Since $\mathscr{q}$ and $\mathscr{g}$ are generated independently in Algorithm 3, $\mathscr{t}(\hbar(0)) = \mathscr{t}(\mathscr{q}(0) \otimes \mathscr{g}(0)) = (1/2^{k-1}) \times (1/2^{h-k}) = 1/2^{h-1}$ and $\mathscr{t}(\hbar(1)) = \mathscr{t}(\mathscr{q}(1) \otimes \mathscr{g}(1)) = 0 \times (1/2^{h-k}) = 0$ by Lemmas 2 and 3. Thus, if $\mathcal{Q} \subseteq \mathcal{H}$, $(\mathscr{t}(\hbar_{\mathrm{I}}(0)), \mathscr{t}(\hbar_{\mathrm{I}}(1))) = (1/2^{h-1}, 0)$. □

**Lemma 9.** *If* $\mathcal{Q} \not\subset \mathcal{H}$, $(\mathscr{t}(\hbar_{\mathrm{II}}(0)), \mathscr{t}(\hbar_{\mathrm{II}}(1))) = (1/2^h, 1/2^h)$.

**Proof.** Regarding $\mathcal{Q} \not\subset \mathcal{H}$, we assume that $\mathcal{H}$ is composed of $l$ pixels selected from $\mathcal{Q}$ and $h - l$ random pixels from $\mathcal{G}$ in Algorithm 3 where $0 \le l \le k - 1$. That is, $\mathcal{H} = \{r_{i_1}, r_{i_2}, \ldots, r_{i_h}\} = \{q_{d_1}, q_{d_2}, \ldots, q_{d_l}\} \cup \{g_{j_1}, g_{j_2}, \ldots, g_{j_{h-l}}\}$ where $1 \le d_u \le k$ and $1 \le j_v \le n - k$ for $1 \le u \le l$ and $1 \le v \le h - l$. Without loss of generality, let $r_{i_1} = q_{d_1}, r_{i_2} = q_{d_2}, \ldots, r_{i_l} = q_{d_l}$ and $r_{i_{l+1}} = g_{j_1}, r_{i_{l+2}} = g_{j_2}, \ldots, r_{i_h} = g_{j_{h-l}}$. Let $\ell = r_{i_1} \otimes r_{i_2} \otimes \ldots \otimes r_{i_l}$, $\mathscr{g} = r_{i_{l+1}} \otimes r_{i_{l+2}} \otimes \ldots \otimes r_{i_h}$. Then $\hbar = \ell \otimes \mathscr{g}$. From Lemma 5 (by setting $v = l$), we have $\mathscr{t}(\ell(0)) = \mathscr{t}(\ell(1)) = 1/2^l$. Besides, $\mathscr{t}(\mathscr{g}(0)) = \mathscr{t}(\mathscr{g}(1)) = 1/2^{h-l}$ when stacking $h - l$ random pixels. Thus, $\mathscr{t}(\hbar(0)) = \mathscr{t}(\ell(0) \otimes \mathscr{g}(0)) = (1/2^l) \times (1/2^{h-l}) = 1/2^h = \mathscr{t}(\ell(1) \otimes \mathscr{g}(1)) = \mathscr{t}(\hbar(1))$. As a result, if $\mathcal{Q} \not\subset \mathcal{H}$, $(\mathscr{t}(\hbar_{\mathrm{II}}(0)), \mathscr{t}(\hbar_{\mathrm{II}}(1))) = (1/2^h, 1/2^h)$. □

The following lemma investigates $\mathscr{Pr}(\mathcal{Q} \subseteq \mathcal{H})$ and $\mathscr{Pr}(\mathcal{Q} \not\subset \mathcal{H})$, which are the probabilities of the occurrences for $\mathcal{Q} \subseteq \mathcal{H}$ and $\mathcal{Q} \not\subset \mathcal{H}$, respectively, with regard to $h$, where $\mathrm{C}(n, k)$ denotes the number of all possible combinations for selecting $k$ from $n$ distinct objects.

**Lemma 10.** $(\mathscr{Pr}(\mathcal{Q} \subseteq \mathcal{H}), \mathscr{Pr}(\mathcal{Q} \not\subset \mathcal{H})) = \begin{cases} (0, 1) & \text{if } h < k; \\ (\eta, 1 - \eta) & \text{otherwise} \end{cases}$ *where* $\eta = \dfrac{\mathrm{C}(n - k, h - k)}{\mathrm{C}(n, h)}$.

**Proof.** According to formula (4), there are totally $\mathrm{C}(n, h)$ possibilities to construct $\mathcal{H}$ from the $n$ elements in $\mathcal{R}$. Thus, the probability for constructing a certain $\mathcal{H}$ is $\mathscr{Pr}(\mathcal{H}) = 1/\mathrm{C}(n, h)$ where $\sum_{\mathcal{H}} \mathscr{Pr}(\mathcal{H}) = 1$. $\mathcal{H}$ either belongs to the class of $\mathcal{Q} \subseteq \mathcal{H}$ or that of $\mathcal{Q} \not\subset \mathcal{H}$. Surely, $\mathscr{Pr}(\mathcal{Q} \not\subset \mathcal{H}) + \mathscr{Pr}(\mathcal{Q} \subseteq \mathcal{H}) = 1$.

If $h < k$, only $\mathcal{Q} \not\subseteq \mathcal{H}$ occurs (no chance for $\mathcal{Q} \subseteq \mathcal{H}$). We obtain $\mathcal{P}r(\mathcal{Q} \not\subseteq \mathcal{H}) = \sum_{\mathcal{Q} \not\subseteq \mathcal{H}} \mathcal{P}r(\mathcal{H}) = \mathrm{C}(n,h) \times (1/\mathrm{C}(n,h)) = 1 = \sum_{\mathcal{H}} \mathcal{P}r(\mathcal{H})$. Thus, $(\mathcal{P}r(\mathcal{Q} \subseteq \mathcal{H}), \mathcal{P}r(\mathcal{Q} \not\subseteq \mathcal{H})) = (0, 1)$.

Otherwise ($h \geq k$), either $\mathcal{Q} \subseteq \mathcal{H}$ or $\mathcal{Q} \not\subseteq \mathcal{H}$ occurs. Consider $\mathcal{Q} \subseteq \mathcal{H}$ first. We have $\mathcal{H} = \{q_1, q_2, \ldots, q_k\} \cup \{g_{j_1}, g_{j_2}, \ldots, g_{j_{h-k}}\} = \mathcal{Q} \cup \mathcal{G}'$ where $\mathcal{G}' \subseteq \mathcal{G}$ (see formula (5)). To construct such $\mathcal{H}$, there are $1 \times \mathrm{C}(n-k, h-k)$ possible ways (by choosing all members in $\mathcal{Q}$ in $\mathrm{C}(k,k)$ $(=1)$ ways, and then selecting $h-k$ elements (to form $\mathcal{G}'$) from $n-k$ ones (in $\mathcal{G}$) randomly in $\mathrm{C}(n-k, h-k)$ ways). Thus $\mathcal{P}r(\mathcal{Q} \subseteq \mathcal{H}) = \sum_{\mathcal{Q} \subseteq \mathcal{H}} \mathcal{P}r(\mathcal{H}) = \mathrm{C}(n-k, h-k)/\mathrm{C}(n,h) = \eta$; meanwhile, $\mathcal{P}r(\mathcal{Q} \not\subseteq \mathcal{H}) = 1 - \eta$. □

The expected light transmissions of $S^{\mathcal{H}}[P(0)]$ and $S^{\mathcal{H}}[P(1)]$ can be estimated as follows:

**Lemma 11.** $$(\mathcal{T}(S^{\mathcal{H}}[P(0)]), \mathcal{T}(S^{\mathcal{H}}[P(1)])) = \begin{cases} \left(\dfrac{1}{2^h}, \dfrac{1}{2^h}\right) & \text{if } h < k; \\ \left(\dfrac{1+\eta}{2^h}, \dfrac{1-\eta}{2^h}\right) & \text{otherwise,} \end{cases} \quad \textit{where } \eta = \frac{\mathrm{C}(n-k, h-k)}{\mathrm{C}(n,h)}.$$

**Proof.** If $h < k$, $(\mathcal{P}r(\mathcal{Q} \subseteq \mathcal{H}), \mathcal{P}r(\mathcal{Q} \not\subseteq \mathcal{H})) = (0, 1)$. From Lemmas 9 and 10, we have $\mathcal{T}(S^{\mathcal{H}}[P(0)]) = \sum_{\mathcal{Q} \subseteq \mathcal{H}} t(h_{\mathrm{I}}(0)) \times \mathcal{P}r(\mathcal{H}) + \sum_{\mathcal{Q} \not\subseteq \mathcal{H}} t(h_{\mathrm{II}}(0)) \times \mathcal{P}r(\mathcal{H}) = t(h_{\mathrm{I}}(0)) \times \mathcal{P}r(\mathcal{Q} \subseteq \mathcal{H}) + t(h_{\mathrm{II}}(0)) \times \mathcal{P}r(\mathcal{Q} \not\subseteq \mathcal{H}) = 0 + (1/2^h) \times 1 = 1/2^h = t(h_{\mathrm{I}}(1)) \times \mathcal{P}r(\mathcal{Q} \subseteq \mathcal{H}) + t(h_{\mathrm{II}}(1)) \times \mathcal{P}r(\mathcal{Q} \not\subseteq \mathcal{H}) = \mathcal{T}(S^{\mathcal{H}}[P(1)])$.

Otherwise (i.e. $h \geq k$), $(\mathcal{P}r(\mathcal{Q} \subseteq \mathcal{H}), \mathcal{P}r(\mathcal{Q} \not\subseteq \mathcal{H})) = (\eta, 1-\eta)$. By Lemmas 8–10, $\mathcal{T}(S^{\mathcal{H}}[P(0)]) = t(h_{\mathrm{I}}(0)) \times \mathcal{P}r(\mathcal{Q} \subseteq \mathcal{H}) + t(h_{\mathrm{II}}(0)) \times \mathcal{P}r(\mathcal{Q} \not\subseteq \mathcal{H}) = (1/2^{h-1}) \times \eta + (1/2^h) \times (1-\eta) = (2\eta + 1 - \eta)/2^h = (1+\eta)/2^h$ and $\mathcal{T}(S^{\mathcal{H}}[P(1)]) = t(h_{\mathrm{I}}(1)) \times \mathcal{P}r(\mathcal{Q} \subseteq \mathcal{H}) + t(h_{\mathrm{II}}(1)) \times \mathcal{P}r(\mathcal{Q} \not\subseteq \mathcal{H}) = 0 \times \eta + (1/2^h) \times (1-\eta) = (1-\eta)/2^h$. □

For a comprehensive understanding of how $\mathcal{T}(S^{\mathcal{H}}[P(0)])$ and $\mathcal{T}(S^{\mathcal{H}}[P(1)])$ by Algorithm 3 are computed, please refer to Appendix B where a small problem instance is considered.

**Theorem 3.** *Given a secret image $P$ and $n$ participants sharing $P$ with a threshold number $k$, the set of $n$ random grids $\mathcal{R} = \{R_1, R_2, \ldots, R_n\}$ produced by Algorithm 3 with respect to $P$ is a set of $(k,n)$-VCRG of $P$.*

**Proof.** We prove that the elements in $\mathcal{R}$ satisfying the three conditions in Definition 5:

(1) From Lemma 6, we know $R_i$ is a random grid with $\mathcal{T}(R_i) = 1/2$ for $1 \leq i \leq n$.
(2) Consider $\mathcal{D} = \{R_{j_1}, R_{j_2}, \ldots, R_{j_d}\} \subset \mathcal{R}$ where $1 \leq j_v \leq n$, $1 \leq v \leq d$ and $1 < d < k$. We obtain $\mathcal{T}(S^{\mathcal{D}}[P(0)]) = 1/2^d = \mathcal{T}(S^{\mathcal{D}}[P(1)])$ by setting $h = d (< k)$ in Lemma 11 where $S^{\mathcal{D}} = R_{j_1} \otimes R_{j_2} \otimes \ldots \otimes R_{j_d}$.
(3) Consider $\mathcal{K} = \{R_{i_1}, R_{i_2}, \ldots, R_{i_k}\} \subset \mathcal{R}$ where $1 \leq i_u \leq n$ and $1 \leq u \leq k$. We obtain $\mathcal{T}(S^{\mathcal{K}}[P(0)]) = (1+\eta)/2^k > (1-\eta)/2^k = \mathcal{T}(S^{\mathcal{K}}[P(1)])$ by setting $h = k$ in Lemma 11 where $S^{\mathcal{K}} = R_{i_1} \otimes R_{i_2} \otimes \ldots \otimes R_{i_k}$.

Therefore $\mathcal{R} = \{R_1, R_2, \ldots, R_n\}$ is a set of $(k,n)$-VCRG of $P$. □

### 3.6. Enhanced $(k,n)$-VCRG

It is easy to see from Algorithm 3 or formula (4) that $\mathcal{R} = \mathcal{Q} \cup \mathcal{G}$ (i.e. $\{r_1, r_2, \ldots, r_n\} = \{q_1, q_2, \ldots, q_k\} \cup \{g_1, g_2, \ldots, g_{n-k}\}$) where $r_i \in \mathcal{R}$, $q_t \in \mathcal{Q}$ and $g_v \in \mathcal{G}$ are corresponding pixels of $p \in P$ for $1 \leq i \leq n$, $1 \leq t \leq k$ and $1 \leq v \leq n-k$. The security and contrast requirements for $\mathcal{R}$ to be a set of $(k,n)$ visual cryptograms of random pixels are actually certified by $\mathcal{Q}$ (instead of $\mathcal{G}$). When a set $\mathcal{K}$ of $k$ pixels is randomly chosen from $\mathcal{R}$ $(= \mathcal{Q} \cup \mathcal{G})$, the chance for $\mathcal{K} = \mathcal{Q}$ does exist; however, it is quite small ($\mathcal{P}r(\mathcal{Q} = \mathcal{K}) = \mathrm{C}(k,k)/\mathrm{C}(n,k) = 1/\mathrm{C}(n,k)$ in Algorithm 3). A comprehensive idea to improve such a probability is to replace $\mathcal{G}$ by some $n-k$ elements in $\mathcal{Q}$, that is, we set $\mathscr{R} = \mathcal{Q}$ (instead of $\mathcal{R} = \mathcal{Q} \cup \mathcal{G}$). This undoubtedly increases the chance of holding $q_1, q_2, \ldots, q_k$ when $k$ pixels are randomly selected from $\mathscr{R}$ (instead of $\mathcal{R}$).

Our realization on this idea is simple. Let $\alpha = \lfloor n/k \rfloor$ and $\beta = n - \alpha \times k$. We represent $\mathcal{Q}$ as a *multiset* $\mathscr{Q}$ which consists of $q_1, q_2, \ldots, q_k$ $\alpha$ times and $q_{\tau_1}, q_{\tau_2}, \ldots, q_{\tau_\beta}$ in addition (see formula (6)) where $q_{\tau_v} \in \mathcal{Q}$ and $1 \leq \tau_u \neq \tau_v \leq k$ for $1 \leq u \neq v \leq \beta$. For each secret pixel $p \in P$, we deliberately encode the $n$ corresponding pixels $r_1, r_2, \ldots, r_n$ in $\mathcal{R}_1, \mathcal{R}_2, \ldots, \mathcal{R}_n$ to be the $n$ elements in $\mathscr{Q}$ after a random permutation, i.e. $(\mathcal{R}_1[i,j], \mathcal{R}_2[i,j], \ldots, \mathcal{R}_n[i,j]) = \mathit{permutation}(\mathscr{Q})$. After all $p$'s in $P$ are thus encoded, $\mathscr{R} = \{\mathcal{R}_1, \mathcal{R}_2, \ldots, \mathcal{R}_n\}$ is a set of $(k,n)$-VCRG of $P$. Algorithm 4 organizes our idea.

We prove the feasibility of $\mathscr{R} = \{\mathcal{R}_1, \mathcal{R}_2, \ldots, \mathcal{R}_n\}$ to be a set of $(k,n)$-VCRG produced by Algorithm 4.

**Lemma 12.** $\mathcal{T}(\mathcal{R}_i) = 1/2$ *for* $1 \leq i \leq n$.

**Proof.** For each pixel $p \in P$, Algorithm 4 produces a set of $n$ shares $\mathscr{R} = \{r_1, r_2, \ldots, r_n\}$ in which $r_i \in \mathscr{R}$ is assigned to be some element in $\mathcal{Q}$, say $q_j$ for $1 \leq i \leq n$ and $1 \leq j \leq k$. Since $t(q_j) = 1/2$ for $1 \leq j \leq k$ by Theorem 2, we obtain $t(r_i) = t(q_j) = 1/2$ for $1 \leq i \leq n$ and $1 \leq j \leq k$. Thus $\mathcal{R}_i$ which consists of all $r_i$'s corresponding to all $p$'s $\in P$ is a random grid with $\mathcal{T}(\mathcal{R}_i) = 1/2$. □

Suppose that a set of $h$ shares, say $\mathscr{H} = \{\mathcal{R}_{i_1}, \mathcal{R}_{i_2}, \ldots, \mathcal{R}_{i_h}\}$, is randomly chosen from $\mathscr{R}$. Consider $p \in P$ and its $k$ corresponding pixels $\mathcal{Q} = \{q_1, q_2, \ldots, q_k\}$ where $q_i \in Q_i (\in Q)$ for $1 \leq i \leq k$. Let its $h$ corresponding pixels in $\mathscr{H}$ be denoted

**Algorithm 4** Enhanced $(k,n)$-VCRG.

```
Input: $h \times w$ image $P$, $k$, $n$
Output: $\mathscr{R}=\{\mathcal{R}_1,\mathcal{R}_2,\dots,\mathcal{R}_n\}$ as a set of $(k,n)$-VCRG of $P$
ETVCRG($r, n, P$)
1.      $(\mathcal{Q}_1,\mathcal{Q}_2,\dots,\mathcal{Q}_k)=$ VCRG($k, P$)
2.      for (each $(i,j)$, $1 \le i \le h$ and $1 \le j \le w$) do
2.1     {   $\mathcal{Q}=\{\mathcal{Q}_1[i,j],\mathcal{Q}_2[i,j],\dots,\mathcal{Q}_n[i,j]\}$
2.2         $\mathscr{Q}=\varnothing$      // $\mathscr{Q}$ is a multiset
2.3         for (each $t$, $1 \le t \le \lfloor n/k \rfloor$) do $\mathscr{Q}=\mathscr{Q}\cup\mathcal{Q}$
2.4         $\mathscr{B}=$ randomly select $\beta(=n-\lfloor n/k\rfloor\times k)$ distinct elements from $\mathcal{Q}$
2.5         $\mathscr{Q}=\mathscr{Q}\cup\mathscr{B}$
2.6         $(\mathcal{R}_1[i,j],\mathcal{R}_2[i,j],\dots,\mathcal{R}_n[i,j])=permutation(\mathscr{Q})$
        }
3.          output($\mathcal{R}_1,\mathcal{R}_2,\dots,\mathcal{R}_n$)
```

as $\mathcal{H}=\{r_{i_1},r_{i_2},\dots,r_{i_h}\}$ where $r_{i_t}\in\mathcal{R}_{i_t}(\in\mathscr{H})$ for $1\le t\le h$. There are two possibilities when comparing $\mathcal{Q}$ against $\mathcal{H}$:

Case I: $\mathcal{Q}\subseteq\mathcal{H}$ ($\{q_1,q_2,\dots,q_k\}\subseteq\{r_{i_1},r_{i_2},\dots,r_{i_h}\}$); or
Case II: $\mathcal{Q}\not\subset\mathcal{H}$ ($\{q_1,q_2,\dots,q_k\}\not\subset\{r_{i_1},r_{i_2},\dots,r_{i_h}\}$), i.e. there exists at least one $q_i\in\mathcal{Q}$ but $q_i\notin\mathcal{H}$.

Let $h=r_{i_1}\otimes r_{i_2}\otimes\dots\otimes r_{i_h}$ and $h(0)$ ($h(1)$) denote such an $h$ whose corresponding $p\in P$ is 0 (1). $t(h_{\mathrm{I}}(0))$ and $t(h_{\mathrm{I}}(1))$ in Case I and $t(h_{\mathrm{II}}(0))$ and $t(h_{\mathrm{II}}(1))$ in Case II are calculated as below.

**Lemma 13.** *If $\mathcal{Q}\subseteq\mathcal{H}$, $(t(h_{\mathrm{I}}(0)),t(h_{\mathrm{I}}(1)))=(1/2^{k-1},0)$.*

**Proof.** Since $\mathcal{Q}\subseteq\mathcal{H}$, we know $h\ge k$. There exists some pair of $r_{i_u}$ and $r_{i_v}$ such that $r_{i_u}=r_{i_v}=q_j$ which causes $r_{i_u}\otimes r_{i_v}=q_j\otimes q_j=q_j$ (by Lemma 1) where $r_{i_u},r_{i_v}\in\mathcal{H}$, $i_u\ne i_v$ and $q_j\in\mathcal{Q}$. We may remove all duplicated elements from $\mathcal{H}$ and the result would be exactly $\mathcal{Q}$. Thus, $h=q$ for either $h=k$ or $h>k$ where $q=q_1\otimes q_2\otimes\dots\otimes q_k$. Therefore, $(t(h_{\mathrm{I}}(0)),t(h_{\mathrm{I}}(1)))=(t(q(0)),t(q(1)))=(1/2^{k-1},0)$ by Theorem 2. □

**Lemma 14.** *If $\mathcal{Q}\not\subset\mathcal{H}$, $(t(h_{\mathrm{II}}(0)),t(h_{\mathrm{II}}(1)))=(1/2^l,1/2^l)$ where $1\le l=|\mathcal{H}'|\le k-1$ and $\mathcal{H}'(\subseteq\mathcal{Q})$ is the result of removing duplicated elements from $\mathcal{H}$.*

**Proof.** Because $\mathcal{Q}\not\subset\mathcal{H}$ and all elements in $\mathcal{H}$ are selected from $\mathcal{Q}$, we obtain $\mathcal{H}'=\{r_{i_1},r_{i_2},\dots,r_{i_l}\}=\{q_{j_1},q_{j_2},\dots,q_{j_l}\}\subset\mathcal{Q}$. Thus, $h=\ell$ where $\ell=q_{j_1}\otimes q_{j_2}\otimes\dots\otimes q_{j_l}$. Therefore, $(t(h_{\mathrm{II}}(0)),t(h_{\mathrm{II}}(1)))=(t(\ell(0)),t(\ell(1)))=(1/2^l,1/2^l)$ by Lemma 5. □

It is noticed that the light transmission $1/2^h$ in Lemma 9 is a constant ($h=|\mathcal{H}|$); while that $1/2^l$ in Lemma 14 may be not ($1\le l(=|\mathcal{Q}'|)<k$).

Before we impart $\mathcal{P}r(\mathcal{Q}\subseteq\mathcal{H})$ and $\mathcal{P}r(\mathcal{Q}\not\subset\mathcal{H})$ in Algorithm 4, we introduce more notations in order to specify the relations among $\mathcal{Q}$, $\mathcal{H}$ and $\mathscr{R}$ from the viewpoint of multisets. When $\mathcal{Q}$ is represented as a multiset $\mathscr{Q}$ corresponding to all of the $n$ elements in $\mathscr{R}$, we obtain

$$\mathscr{R}=\{r_1,r_2,\dots,r_n\}=\Big\{\overbrace{\overbrace{q_1,q_2,\dots,q_k},\overbrace{q_1,q_2,\dots,q_k},\dots,\overbrace{q_1,q_2,\dots,q_k}}^{\alpha},q_{\tau_1},q_{\tau_2},\dots,q_{\tau_\beta}\Big\}=\mathscr{Q} \tag{6}$$

where $\alpha=\lfloor n/k\rfloor$, $\beta=n-\alpha\times k$ and $\{q_{\tau_1},q_{\tau_2},\dots,q_{\tau_\beta}\}=\mathscr{B}$ ($\subseteq\mathcal{Q}$, see Step 2.4) according to Algorithm 4. Let $y_j$ denote the number of $q_j$'s in $\mathscr{Q}$ for $1\le j\le k$. Then,

$$y_j=\begin{cases}\alpha+1 & \text{if } j\in\{\tau_1,\tau_2,\dots,\tau_\beta\}\\ \alpha & \text{otherwise}\end{cases}$$

where $\tau_t\in\{1,2,\dots,k\}$ for $1\le t\le\beta$. Consider $\mathcal{H}=\{r_{i_1},r_{i_2},\dots,r_{i_h}\}$ which is randomly selected from $\mathscr{R}(=\mathscr{Q})$. We denote it as $x_i$ the number of $q_i$'s which are selected from $\mathscr{Q}$ and assigned to be the members of $\mathcal{H}$ where $\sum_{j=1}^{k}x_j=h$ for $0\le x_j\le y_j$. Therefore, a feasible assignment to $(x_1,x_2,\dots,x_k)$ determines a corresponding set of $\mathcal{H}=\{r_{i_1},r_{i_2},\dots,r_{i_h}\}$ where $0\le x_j\le y_j$ for $1\le j\le k$. Let $\mathbb{U}$ be the set of all feasible assignments to $(x_1,x_2,\dots,x_k)$ under these constraints, i.e.

$$\mathbb{U}=\left\{(x_1,x_2,\dots,x_k)\,\middle|\,\sum_{j=1}^{k}x_j=h,\ y_j=\begin{cases}\alpha+1 & \text{if } j\in\{\tau_1,\tau_2,\dots,\tau_\beta\}\\ \alpha & \text{otherwise}\end{cases}\ \text{where } 0\le x_j\le y_j \text{ for } 1\le j\le k\right\}.$$

The further strict constraint of $1\le x_j\le y_j$ (instead of $0\le x_j\le y_j$) guarantees $\mathcal{Q}\subseteq\mathcal{H}$; otherwise (i.e. there exists at least one $x_j=0$ for $1\le j\le k$), $\mathcal{Q}\not\subset\mathcal{H}$ occurs. Let $\mathbb{X}$ represent the set of all assignments that result in $\mathcal{Q}\subseteq\mathcal{H}$, i.e.

$$\mathbb{X}=\left\{(x_1,x_2,\ldots,x_k)\,\middle|\,\sum_{j=1}^{k}x_j=h,\ y_j=\begin{cases}\alpha+1 & \text{if } j\in\{\tau_1,\tau_2,\ldots,\tau_\beta\}\\ \alpha & \text{otherwise}\end{cases}\ \text{where } 1\le x_j\le y_j \text{ for } 1\le j\le k\right\}.$$

It is easy to realize that $\mathbb{U}-\mathbb{X}$ comprises all assignments causing $\mathcal{Q}\not\subseteq\mathcal{H}$.

Based upon the above notations, the following lemma explores $\mathcal{P}r(\mathcal{Q}\subseteq\mathcal{H})$ and $\mathcal{P}r(\mathcal{Q}\not\subseteq\mathcal{H})$.

**Lemma 15.** $(\mathcal{P}r(\mathcal{Q}\subseteq\mathcal{H}),\mathcal{P}r(\mathcal{Q}\not\subseteq\mathcal{H}))=\begin{cases}(0,1) & \text{if } h<k;\\ (\kappa,1-\kappa) & \text{otherwise}\end{cases}$ *where* $\kappa=\sum_{(x_1,x_2,\ldots,x_k)\in\mathbb{X}}\dfrac{\prod_{j=1}^{k}\mathrm{C}(y_j,x_j)}{\mathrm{C}(n,h)}$.

**Proof.** Assume that the assignment $(x_1,x_2,\ldots,x_k)\in\mathbb{U}$ determines $\mathcal{H}(=\{r_{i_1},r_{i_2},\ldots,r_{i_h}\}\subseteq\mathscr{Q})$. For a particular value of $x_j$, there are $\mathrm{C}(y_j,x_j)$ possible ways to select $q_j$ ($x_j$ times) from $\mathscr{Q}$ as members in $\mathcal{H}$ for $1\le j\le k$. Therefore, the number of all possible combinations to construct this $\mathcal{H}$ (with regard to $(x_1,x_2,\ldots,x_k)$) is $\prod_{j=1}^{k}\mathrm{C}(y_j,x_j)$ with a probability of $\mathcal{P}r(\mathcal{H})=\prod_{j=1}^{k}\mathrm{C}(y_j,x_j)/\mathrm{C}(n,h)$ ($>\mathcal{P}r(\mathscr{H})$ in Lemma 10). Surely, $\sum_{(x_1,x_2,\ldots,x_k)\in\mathbb{U}}\mathcal{P}r(\mathcal{H})=1$.

If $h<k$, $\mathcal{Q}\subseteq\mathcal{H}$ is impossible so that $(\mathcal{P}r(\mathcal{Q}=\mathcal{H}),\mathcal{P}r(\mathcal{Q}\neq\mathcal{H}))=(0,1)$. Otherwise ($h\ge k$), consider the case of $\mathcal{Q}\subseteq\mathcal{H}$ first. Each assignment $(x_1,x_2,\ldots,x_k)$ of $\mathcal{H}$ satisfying $\mathcal{Q}\subseteq\mathcal{H}$ should belong to $\mathbb{X}$. Actually, the class of $\mathcal{Q}\subseteq\mathcal{H}$ consists of those $\mathcal{H}$'s with regard to all legal assignments $(x_1,x_2,\ldots,x_k)$'s $\in\mathbb{X}$. That is,

$$\mathcal{P}r(\mathcal{Q}\subseteq\mathcal{H})=\sum_{\mathcal{Q}=\mathcal{H}}\mathcal{P}r(\mathcal{H})=\sum_{(x_1,x_2,\ldots,x_k)\in\mathbb{X}}\mathcal{P}r(\mathcal{H})=\sum_{(x_1,x_2,\ldots,x_k)\in\mathbb{X}}\frac{\prod_{j=1}^{k}\mathrm{C}(y_j,x_j)}{\mathrm{C}(n,h)}=\kappa.$$

On the contrary, the class of $\mathcal{Q}\not\subseteq\mathcal{H}$ comprises those $\mathcal{H}$'s with regard to all assignments $(x_1,x_2,\ldots,x_k)$'s $\in\mathbb{U}-\mathbb{X}$. Thus,

$$\mathcal{P}r(\mathcal{Q}\not\subseteq\mathcal{H})=\sum_{\mathcal{Q}\neq\mathcal{H}}\mathcal{P}r(\mathcal{H})=\sum_{(x_1,x_2,\ldots,x_k)\in\mathbb{U}-\mathbb{X}}\frac{\prod_{j=1}^{k}\mathrm{C}(y_j,x_j)}{\mathrm{C}(n,h)}=1-\sum_{(x_1,x_2,\ldots,x_k)\in X}\frac{\prod_{j=1}^{k}\mathrm{C}(y_j,x_j)}{\mathrm{C}(n,h)}=1-\kappa.\qquad\square$$

We are ready to compute the expected light transmissions of $S^{\mathcal{H}}[P(0)]$ and $S^{\mathcal{H}}[P(1)]$.

**Lemma 16.** $(\mathcal{T}(S^{\mathcal{H}}[P(0)]),\mathcal{T}(S^{\mathcal{H}}[P(1)]))=\begin{cases}(\xi,\xi) & \text{if } h<k;\\ \left(\dfrac{\kappa}{2^{k-1}}+\xi,\xi\right) & \text{otherwise,}\end{cases}$ *where* $\kappa=\sum_{(x_1,x_2,\ldots,x_k)\in\mathbb{X}}\dfrac{\prod_{j=1}^{k}\mathrm{C}(y_j,x_j)}{\mathrm{C}(n,h)}$ *and* $\xi=\sum_{(x_1,x_2,\ldots,x_k)\in\mathbb{U}-\mathbb{X}}\dfrac{1}{2^l}\times\dfrac{\prod_{j=1}^{k}\mathrm{C}(y_j,x_j)}{\mathrm{C}(n,h)}$ *in which $l$ is the number of non-zero members in $(x_1,x_2,\ldots,x_k)$ (i.e. $l=k-zero(x_1,x_2,\ldots,x_k)$ where $zero(x_1,x_2,\ldots,x_k)$ counts the number of 0's in $(x_1,x_2,\ldots,x_k)$).*

**Proof.** Consider $(x_1,x_2,\ldots,x_k)\in\mathbb{U}$ with regard to $\mathcal{H}=\{r_{i_1},r_{i_2},\ldots,r_{i_h}\}$ corresponding to $p\in P$ in which $\mathcal{P}r(\mathcal{H})=\prod_{j=1}^{k}\mathrm{C}(y_j,x_j)/\mathrm{C}(n,h)$ and $\sum_{(x_1,x_2,\ldots,x_k)\in\mathbb{U}}\mathcal{P}r(\mathcal{H})=1$ (see the proof of Lemma 15).

If $h<k$, only the case of $\mathcal{Q}\not\subseteq\mathcal{H}$ happens. It also indicates $(x_1,x_2,\ldots,x_k)\in\mathbb{U}-\mathbb{X}$. By Lemma 14, we have $t(h_{\mathrm{II}}(0))=t(h_{\mathrm{II}}(1))=1/2^l=1/2^{k-zero(x_1,x_2,\ldots,x_k)}$ where $h=r_{i_1}\otimes r_{i_2}\otimes\ldots\otimes r_{i_h}$, $l=|\mathcal{H}'|$ (or equivalently $l=k-zero(x_1,x_2,\ldots,x_k)$) and $\mathcal{H}'\subset\mathcal{Q}$ with $1\le l\le k-1$. (Assume $\mathcal{H}'=\{q_{j_1},q_{j_2},\ldots,q_{j_l}\}\subset\mathcal{Q}$ and $\mathcal{Q}-\mathcal{H}'=\{q_{j_{l+1}},q_{j_{l+2}},\ldots,q_{j_k}\}$. It implies $x_{j_u}\neq 0$ and $x_{j_v}=0$ for $1\le j_u\neq j_v\le k$, $1\le u\le l$ and $1\le v\le k-l$ where $k=|\mathcal{Q}|$. Thus, $l=k-zero(x_1,x_2,\ldots,x_k)$.) When considering all possible assignments $(x_1,x_2,\ldots,x_k)$'s in $\mathbb{U}-\mathbb{X}$, we obtain the expected light transmissions of $S^{\mathcal{H}}[P(0)]$ and $S^{\mathcal{H}}[P(1)]$:

$$\begin{aligned}\mathcal{T}\big(S^{\mathcal{H}}[P(0)]\big)&=\sum_{(x_1,x_2,\ldots,x_k)\in\mathbb{U}-\mathbb{X}}t\big(h_{\mathrm{II}}(0)\big)\mathcal{P}r(\mathcal{H})=\sum_{(x_1,x_2,\ldots,x_k)\in\mathbb{U}-\mathbb{X}}\big(1/2^l\big)^{\prod_{j=1}^{k}\mathrm{C}(y_j,x_j)}/\mathrm{C}(n,h)=\xi\\&=\sum_{(x_1,x_2,\ldots,x_k)\in\mathbb{U}-\mathbb{X}}t\big(h_{\mathrm{II}}(1)\big)\mathcal{P}r(\mathcal{H})=\mathcal{T}\big(S^{\mathcal{H}}[P(1)]\big).\end{aligned}$$

Otherwise ($h\ge k$), both cases of $\mathcal{Q}\subseteq\mathcal{H}$ and $\mathcal{Q}\not\subseteq\mathcal{H}$ may occur. Therefore,

$$\begin{aligned}\mathcal{T}\big(S^{\mathcal{H}}[P(0)]\big)&=\sum_{(x_1,x_2,\ldots,x_k)\in\mathbb{X}}t\big(h_{\mathrm{I}}(0)\big)\mathcal{P}r(\mathcal{H})+\sum_{(x_1,x_2,\ldots,x_k)\in\mathbb{U}-\mathbb{X}}t\big(h_{\mathrm{II}}(0)\big)\mathcal{P}r(\mathcal{H})\\&=\sum_{(x_1,x_2,\ldots,x_k)\in\mathbb{X}}\big(1/2^{k-1}\big)\times\frac{\prod_{j=1}^{k}\mathrm{C}(y_j,x_j)}{\mathrm{C}(n,h)}+\sum_{(x_1,x_2,\ldots,x_k)\in\mathbb{U}-\mathbb{X}}\frac{1}{2^l}\times\frac{\prod_{j=1}^{k}\mathrm{C}(y_j,x_j)}{\mathrm{C}(n,h)}\\&=\big(1/2^{k-1}\big)\sum_{(x_1,x_2,\ldots,x_k)\in\mathbb{X}}\frac{\prod_{j=1}^{k}\mathrm{C}(y_j,x_j)}{\mathrm{C}(n,h)}+\xi=\frac{\kappa}{2^{k-1}}+\xi,\end{aligned}$$

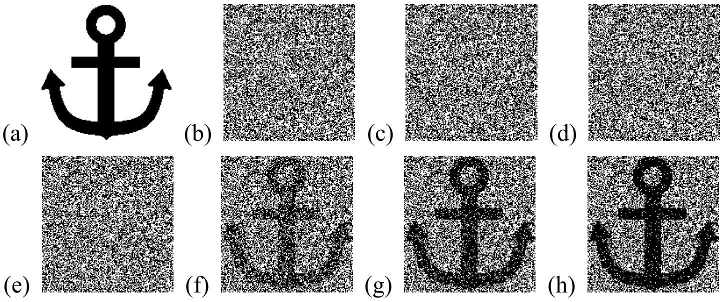

**Fig. 4.** Results of Algorithm 1 for (2, 4)-VCRG: (a) $P$, (b) $R_1$, (c) $R_2$, (d) $R_3$, (e) $R_4$, (f) $R_1 \otimes R_2$, (g) $R_1 \otimes R_2 \otimes R_3$, (h) $R_1 \otimes R_2 \otimes R_3 \otimes R_4$.

$$\mathcal{T}\big(S^{\mathcal{H}}\big[P(1)\big]\big) = \sum_{(x_1,x_2,\ldots,x_k)\in\mathbb{X}} t\big(h_{\mathrm{I}}(1)\big)\mathcal{P}r(\mathcal{H}) + \sum_{(x_1,x_2,\ldots,x_k)\in\mathbb{U}-\mathbb{X}} t\big(h_{\mathrm{II}}(1)\big)\mathcal{P}r(\mathcal{H})$$

$$= \sum_{(x_1,x_2,\ldots,x_k)\in\mathbb{X}} 0 \times \frac{\prod_{j=1}^{k} \mathrm{C}(y_j, x_j)}{\mathrm{C}(n,h)} + \sum_{(x_1,x_2,\ldots,x_k)\in\mathbb{U}-\mathbb{X}} \frac{1}{2^l} \times \frac{\prod_{j=1}^{k} \mathrm{C}(y_j, x_j)}{\mathrm{C}(n,h)} = 0 + \xi = \xi. \qquad \square$$

The computations for $\mathcal{T}(S^{\mathcal{H}}[P(0)])$ and $\mathcal{T}(S^{\mathcal{H}}[P(1)])$ by Algorithm 4 are exemplified in Appendix C. Theorem 4 is a logical consequence from Lemmas 12–16.

**Theorem 4.** *Given a secret image $P$ and $n$ participants sharing $P$ with a threshold number $k$, the set of $n$ random grids $\mathcal{R} = \{\mathcal{R}_1, \mathcal{R}_2, \ldots, \mathcal{R}_n\}$ produced by Algorithm 4 with respect to $P$ is a set of $(k,n)$-VCRG of $P$.*

## 4. Experiments and discussions

### 4.1. Experimental results

Let $R$ denote a set of $(k,n)$-VCRG produced by one of our algorithms and $H \subseteq R$ where $1 \le h(= |H|) \le n$. We verify the feasibility of our $(k,n)$-VCRG algorithms by showing experimental results of $S^H$, the superimposed result of all encoded shares in $H$, from computer simulations. We also compare the analytic light transmissions, i.e. $(\mathcal{T}(S^H[P(0)]), \mathcal{T}(S^H[P(1)]))$ obtained in Section 3, against the computational counterparts in our experiments, referred to as $(\mathcal{L}(S^H[P(0)]), \mathcal{L}(S^H[P(1)]))$ defined as:

$$\mathcal{L}\big(S^H\big[P(0)\big]\big) = \frac{n_0(S^H[P(0)])}{n_0(P)} \quad \text{and} \quad \mathcal{L}\big(S^H\big[P(1)\big]\big) = \frac{n_0(S^H[P(1)])}{n_1(P)} \tag{7}$$

where $n_0(X)$ $(n_1(X))$ denotes the number of transparent (opaque) pixels in $X$.

To evaluate the degree of visual perception to $P$ from $S^H$, we adopt two types of *light contrast* in terms of $\mathcal{T}(S^H[P(0)])$ and $\mathcal{T}(S^H[P(1)])$:

$$l_1\big(S^H\big) = \mathcal{T}\big(S^H\big[P(0)\big]\big) - \mathcal{T}\big(S^H\big[P(1)\big]\big) \quad \text{and} \quad l_2\big(S^H\big) = \frac{\mathcal{T}(S^H[P(0)]) - \mathcal{T}(S^H[P(1)])}{1 + \mathcal{T}(S^H[P(1)])} \tag{8}$$

which were first discussed in [17,18]. Both measurements favor a larger $\mathcal{T}(S^H[P(0)]) - \mathcal{T}(S[P(1)])$, yet the latter in addition prefers a smaller (darker) $\mathcal{T}(S[P(1)])$ due to the reason that a larger (brighter) $\mathcal{T}(S[P(1)])$ weakens our visual recognition between $S[P(0)]$ and $S[P(1)]$ (than a smaller (darker) one) under a same $\mathcal{T}(S^H[P(0)]) - \mathcal{T}(S^H[P(1)])$. It is lucid that for a feasible $(k,n)$-VCRG algorithm $l_i(S^H) = 0$ if $h < k$; $l_i(S^H) > 0$ otherwise where $i \in \{1, 2\}$.

The computer programs were coded in Borland C++ Builder and run in a PC with MS Windows. Two experiments were conducted: Experiment 1 focused on (2, 4)-VCRGs by Algorithms 1, 3 and 4, while Experiment 2 compared (3, 5)-VCRGs by Algorithms 3 and 4.

Experiment 1 (2, 4)-VCRG

Fig. 4 gives the experimental results of Algorithm 1 where (a) shows the 150 × 156 binary secret image $P$, (b)–(e) are the four encoded random grids, namely $R_1$, $R_2$, $R_3$ and $R_4$, and (f)–(h) are the superimposed outcomes of $R_1 \otimes R_2$, $R_1 \otimes R_2 \otimes R_3$, and $R_1 \otimes R_2 \otimes R_3 \otimes R_4$, respectively. Note that the superimposed results of the other groups of two and three out of the four shares look similar as (f) and (g), respectively, in our experiment. Thus, we skip them here. Figs. 5 and 6 illustrate the corresponding experimental results of Algorithms 3 and 4 where $(R_1, R_2, R_3, R_4) = \mathrm{TVCRG}(2, 4, P)$ and $(\mathcal{R}_1, \mathcal{R}_2, \mathcal{R}_3, \mathcal{R}_4) = \mathrm{ETVCRG}(2, 4, P)$.

As seen from Figs. 4–6, each of the four encoded shares by Algorithms 1, 3 and 4 ($R_i$'s, $R_i$'s and $\mathcal{R}_i$'s for $1 \le i \le 4$) is a random grid which leaks nothing about $P$ individually; while the superimposed result of each group of two, three or four

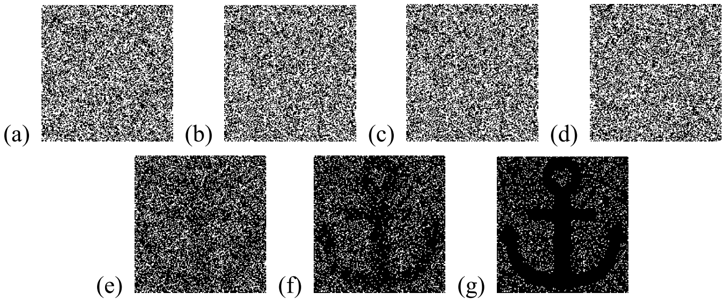

**Fig. 5.** Results of Algorithm 3 for (2, 4)-VCRG of $P$: (a) $R_1$, (b) $R_2$, (c) $R_3$, (d) $R_4$, (e) $R_1 \otimes R_2$, (f) $R_1 \otimes R_2 \otimes R_3$, (g) $R_1 \otimes R_2 \otimes R_3 \otimes R_4$.

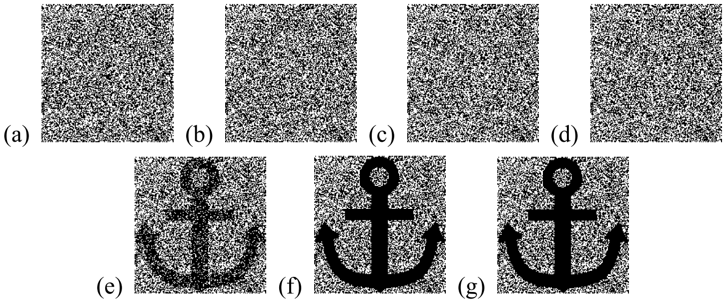

**Fig. 6.** Results of Algorithm 4 for (2, 4)-VCRG of $P$: (a) $\mathcal{R}_1$, (b) $\mathcal{R}_2$, (c) $\mathcal{R}_3$, (d) $\mathcal{R}_4$, (e) $\mathcal{R}_1 \otimes \mathcal{R}_2$, (f) $\mathcal{R}_1 \otimes \mathcal{R}_2 \otimes \mathcal{R}_3$, (g) $\mathcal{R}_1 \otimes \mathcal{R}_2 \otimes \mathcal{R}_3 \otimes \mathcal{R}_4$.

**Table 3**
Comparison on light transmissions and light contrasts of $S^H$ in (2, 4)-VCRGs.

| Light transmission | $h$ | Algorithm 1 | Algorithm 3 | Algorithm 4 |
|---|---|---|---|---|
| $(\mathcal{T}(S^H[P(0)]), \mathcal{T}(S^H[P(1)]))$ | 1 | (0.5, 0.5) | (0.5, 0.5) | (0.5, 0.5) |
| | 2 | (0.5, 0.25) | (0.292, 0.208) | (0.5, 0.167) |
| | 3 | (0.5, 0.125) | (0.186, 0.063) | (0.5, 0) |
| | 4 | (0.5, 0.0625) | (0.125, 0) | (0.5, 0) |
| $(\Delta_0, \Delta_1)^+$ | 1 | (0.001326, 0.000619) | (0.000688, 0.002383) | (0.001277, 0.002223) |
| | 2 | (0.001326, 0.001810) | (0.000514, 0.001147) | (0.001277, 0.000935) |
| | 3 | (0.000688, 0.002618) | (0.004859, 0.000411) | (0.001277, 0) |
| | 4 | (0.000688, 0.001406) | (0.000602, 0) | (0.000688, 0) |
| $(l_1(S^H), l_1 - l_2(S^H))$ | 1 | (0, 0) | (0, 0) | (0, 0) |
| | 2 | (0.25, 0.05) | (0.084, 0.014) | (0.333, 0.048) |
| | 3 | (0.375, 0.042) | (0.123, 0.007) | (0.5, 0) |
| | 4 | (0.4375, 0.026) | (0.125, 0) | (0.5, 0) |

$^+(\Delta_0, \Delta_1) = (|\mathcal{T}(S^H[P(0)]) - \mathcal{L}(S^H[P(0)])|, |\mathcal{T}(S^H[P(1)]) - \mathcal{L}(S^H[P(1)])|)$ where $\mathcal{L}(S^H[P(p)])$ is the average result of all C(4, $h$) cases for $p \in \{0, 1\}$.

random grids reveals $P$ to our eyes. These provide the visualized evidences to the correctness of Algorithms 1, 3 and 4 in delivering sets of (2, 4)-VCRGs of $P$. Moreover, the degree of visual perception of $P$ from $S^H$ grows as $h$ increases when $2 \le h \le 4$ for each of the three algorithms.

The values of $(\mathcal{T}(S^H[P(0)]), \mathcal{T}(S^H[P(1)]))$, $(\mathcal{L}(S^H[P(0)]), \mathcal{L}(S^H[P(1)]))$, their differences and light contrast $l_1(S^H)$ and $l_1(S^H) - l_2(S^H)$ (for easy comparison) are summarized in Table 3 for $1 \le h \le 4$ and $H \subseteq \mathcal{R}$ ($\mathcal{R}$ or $\mathscr{R}$) by Algorithm 1 (3 or 4). Observing the values of $\Delta_0$'s and $\Delta_1$'s (possibly $\in [0, 1]$) in Table 3 which are all less than 0.005, we realize that $\mathcal{T}(S^H[P(0)])$ ($\mathcal{T}(S^H[P(1)])$) is almost the same as $\mathcal{L}(S^H[P(0)])$ ($\mathcal{L}(S^H[P(1)])$). The analytic light transmissions are thus computationally verified. When discussing light transmissions in the following, we simply refer to the analytic ones.

When $h = 1$, all of the three algorithms have the same light contrast as 0; while $h > 1$, they produce light contrasts greater than 0 by both $l_1$ and $l_2$ measurements. These, as expected, coincide with the conditions for being a feasible set of (2, 4)-VCRG. We also point out that the difference $l_1(S^H) - l_2(S^H) (\in [0, 1])$ in Table 3 are not major (all $< 0.05$). It implies that the difference between $l_1(S^H)$ and $l_2(S^H)$ is not so crucial in this experiment.

Fig. 7 intentionally depicts the values of $l_1(S^H)$ with regard to $1 \le h \le 4$ by the three algorithms. It is thus easily seen that Algorithm 4 achieves the highest light contrast among the three, while Algorithm 3 the worst. This is also experimentally supported by Figs. 4–6. We say that Algorithm 4 is better than Algorithms 1 and 3 in dealing with (2, 4)-VCRG. We also clarify from Fig. 7 that $S^H$ tends to be more visually perceptible as $h$ increases (as shown in Figs. 4–6) for the three algorithms (except $l_1(S^H) = 0.5$ for $h = 3$ and 4 by Algorithm 4).

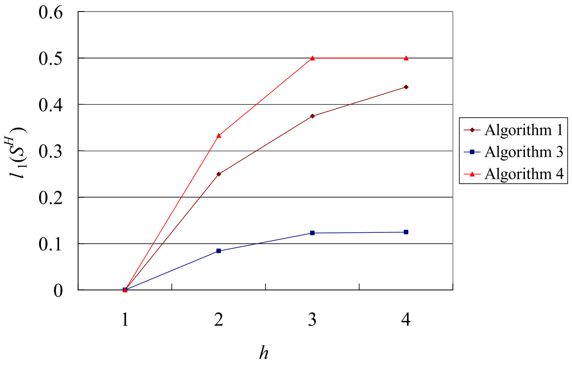

**Fig. 7.** Light contrast $l_1(S^H)$ with regard to $1 \le h \le 4$ in $(2,4)$-VCRGs by Algorithms 1, 3 and 4.

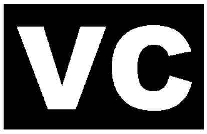

**Fig. 8.** Secret image $P$ for Experiment 2.

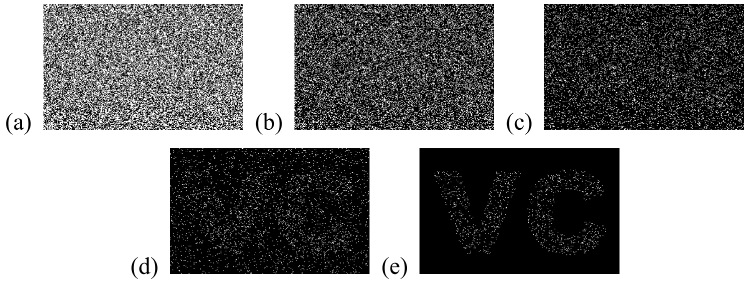

**Fig. 9.** Superimposed results from $(3,5)$-VCRG of $P$ by Algorithm 3: (a) $R_1$, (b) $R_1 \otimes R_2$, (c) $R_1 \otimes R_2 \otimes R_3$, (d) $R_1 \otimes R_2 \otimes R_3 \otimes R_4$, (e) $R_1 \otimes R_2 \otimes R_3 \otimes R_4 \otimes R_5$.

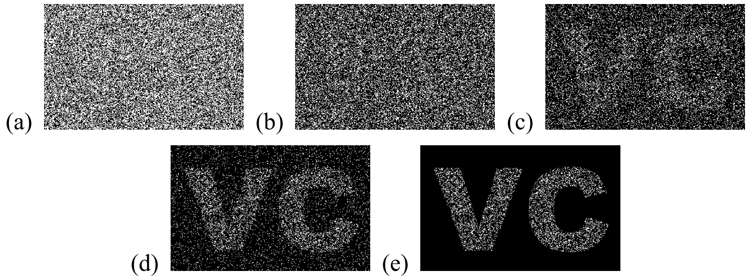

**Fig. 10.** Results from $(3,5)$-VCRG of $P$ by Algorithm 4: (a) $\mathcal{R}_1$, (b) $\mathcal{R}_1 \otimes \mathcal{R}_2$, (c) $\mathcal{R}_1 \otimes \mathcal{R}_2 \otimes \mathcal{R}_3$, (d) $\mathcal{R}_1 \otimes \mathcal{R}_2 \otimes \mathcal{R}_3 \otimes \mathcal{R}_4$, (e) $\mathcal{R}_1 \otimes \mathcal{R}_2 \otimes \mathcal{R}_3 \otimes \mathcal{R}_4 \otimes \mathcal{R}_5$.

Experiment 2 $(3,5)$-VCRG

We adopted Algorithms 3 and 4 to produce sets $\mathcal{R} = \{R_1, R_2, \ldots, R_5\}$ and $\mathscr{R} = \{\mathcal{R}_1, \mathcal{R}_2, \ldots, \mathcal{R}_5\}$, respectively, as $(3,5)$-VCRGs of $P$ $(320 \times 200)$ as shown in Fig. 8. Figs. 9 and 10 only exhibit some of $S^H$'s, i.e. one (out of the C$(5,h)$ cases) for each group of the $h$ shares in $H \subseteq \mathcal{R}$ or $\mathscr{R}$ for $1 \le h \le 5$.

It is not hard to see from Fig. 10(c)–(e) that $S^{\mathscr{H}}$ reveals $P$ for $3 \le h \le 5$; besides, $P$ becomes visually clearer in $S^{\mathscr{H}}$ as $h$ increases where $\mathscr{H} \subseteq \mathscr{R}$ by Algorithm 4. Similarly, $S^{\mathcal{H}}$ in Fig. 9(c)–(e), recovers $P$ with only a small light contrast, which is hard to recognize, where $\mathcal{H} \subseteq \mathcal{R}$ by Algorithm 3. Note that enlarging $S^{\mathcal{H}}$ or counting 0/1 pixels area by area using computers may help revealing $P$, yet it is beyond the scope of this paper.

Table 4 lists the values of $(\mathcal{T}(S^H[P(0)]), \mathcal{T}(S^H[P(1)]))$, $(\mathcal{L}(S^H[P(0)]), \mathcal{L}(S^H[P(1)]))$, their difference and light contrast $l_1(S^H)$ and $l_1(S^H) - l_2(S^H)$ for $1 \le h \le 5$ and $H \in \{\mathcal{H}, \mathscr{H}\}$. Likewise, the small values of $\Delta_0$'s and $\Delta_1$'s in Table 4 (all less than 0.007) support the correctness of the analytic light transmissions. Observing the light contrasts for $h = 1$ and 2 in terms of $l_1(S^H)$ or $l_2(S^H)$ that are 0's, we assure that any group of less than 3 shares cannot tell $P$ from $S^H$ where $H \in \{\mathcal{H}, \mathscr{H}\}$. The fact that each single share $R_i \in \mathcal{H}$ or $\mathcal{R}_i \in \mathscr{H}$ for $1 \le i \le 5$ is truly a random grid can also be manifested here. While

**Table 4**
Comparison on light transmissions and light contrasts of $S^H$ in $(3,5)$-VCRGs.

| Light transmission | $h$ | Algorithm 3 | Algorithm 4 |
|---|---|---|---|
| $(\mathcal{T}(S^H[P(0)]), \mathcal{T}(S^H[P(1)]))$* | 1 | $(0.5, 0.5)$ | $(0.5, 0.5)$ |
| | 2 | $(0.25, 0.25)$ | $(0.3, 0.3)$ |
| | 3 | $(0.1375, 0.1125)$ | $(0.25, 0.15)$ |
| | 4 | $(0.0875, 0.0375)$ | $(0.25, 0.05)$ |
| | 5 | $(0.0625, 0)$ | $(0.25, 0)$ |
| $(\Delta_0, \Delta_1)$+ | 1 | $(0.000025, 0.001031)$ | $(0.002923, 0.004411)$ |
| | 2 | $(0.001056, 0.001169)$ | $(0.004180, 0.006370)$ |
| | 3 | $(0.001831, 0.001472)$ | $(0.005182, 0.013489)$ |
| | 4 | $(0.000212, 0.000048)$ | $(0.001179, 0.015235)$ |
| | 5 | $(0.000546, 0)$ | $(0.003537, 0)$ |
| $(l_1(S^H), l_1(S^H) - l_2(S^H))$ | 1 | $(0, 0)$ | $(0, 0)$ |
| | 2 | $(0, 0)$ | $(0, 0)$ |
| | 3 | $(0.025, 0.002528)$ | $(0.1, 0.013043)$ |
| | 4 | $(0.05, 0.001807)$ | $(0.2, 0.009524)$ |
| | 5 | $(0.0625, 0)$ | $(0.25, 0)$ |

* See Appendices B and C for Algorithms 3 and 4, respectively.

+ $(\Delta_0, \Delta_1) = (|\mathcal{T}(S^H[P(0)]) - \mathcal{L}(S^H[P(0)])|, |\mathcal{T}(S^H[P(1)]) - \mathcal{L}(S^H[P(1)])|)$ where $\mathcal{L}(S^H[P(p)])$ is the average result of all $C(5,h)$ cases.

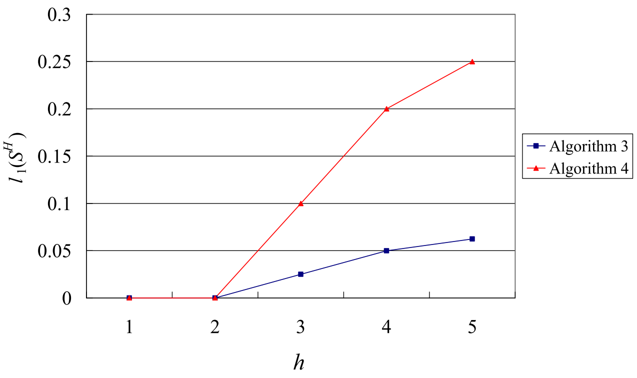

**Fig. 11.** Light contrast $l_1(S^H)$ with regard to $1 \le h \le 5$ in $(3,5)$-VCRGs by Algorithms 3 and 4.

$h \ge 3$, all light contrasts are greater than 0 by both $l_1$ and $l_2$ measurements. $\mathcal{R}$ and $\mathscr{R}$ are indeed sets of $(3,5)$-VCRGs either analytically or experimentally. The difference $l_1(S^H) - l_2(S^H)$ in Table 4 is insignificant (all $< 0.014$) so that the measurements by $l_1$ or $l_2$ induce little difference here.

Fig. 11 illustrates the values of $l_1(S^{\mathcal{H}})$ and $l_1(S^{\mathscr{H}})$ with regard to $h$ where $\mathcal{H} \subseteq \mathcal{R}$ and $\mathscr{H} \subseteq \mathscr{R}$ by Algorithms 3 and 4, respectively. It is easy to see that $l_1(S^{\mathscr{H}})$ is greater than $l_1(S^{\mathcal{H}})$ and their difference grows as $h$ increases for $3 \le h \le 5$; while all corresponding values of $l_1(S^{\mathcal{H}})$'s are no greater than 0.012. This explains why $P$ becomes visually clearer from $S^{\mathscr{H}}$ in Fig. 10 when $h$ increases; yet, it is hard to recognize from $S^{\mathcal{H}}$ in Fig. 9. The superiority of Algorithm 4 over Algorithm 3 in achieving a better light contrast is analytically and experimentally clarified.

### 4.2. Light contrasts in VCS and VCRG

Let $\mathscr{R}$ be the set of $(k,n)$-VCRG by Algorithm 4 and $U$ be the set of $n$ encoded shares by the quality VCS in [3,4]. Consider sets of $k$ shares $\mathcal{K} \subseteq \mathscr{R}$ and $V \subseteq U$ where $|\mathcal{K}| = k = |V|$. We would like to compare the visual perception of $P$ from $S^{\mathcal{K}}$ with that from $S^V$ since the superimposition of $k$ shares is the boundary condition for the participants to see the secret in a $(k,n)$ visual sharing structure.

The degree of the visual perception in $S^{\mathcal{K}}$ is measured by $l_1(S^{\mathcal{K}})$ or $l_2(S^{\mathcal{K}})$, while that in $S^V$ by $c_1(S^V) = (h-l)/m$ [1] or $c_2(S^V) = (h-l)/(m+l)$ [12] where $h(l)$ is the number of white pixels in each reconstructed white (black) block. Note that both $c_1(S^V)$ and $c_2(S^V)$ evaluate the contrast of $S^V$ in terms of $h-l$, while $c_2$ includes the interference of white pixels in a reconstructed black block (which is the darker (a smaller $l$) the better). From the view of light transmission, $c_1$ and $c_2$ actually measure the amount of light passing through a block (via white pixels) so that they are essentially equivalent to $l_1$ and $l_2$, respectively. We list the values of $m$ and $l$ for $|V| = k$ (in which $h$ should be $l+1$) in $(k,n)$-VCSs [3,4] for $2 \le k \le n \le 10$ in Table 7.

We summarize in Table 5 the values of $l_1(S^{\mathcal{K}})$ and $l_2(S^V)$ for $2 \le k \le n \le 10$ and in Table 6 those of $l_1(S^{\mathcal{K}}) - c_1(S^V)$ and $l_2(S^{\mathcal{K}}) - c_2(S^V)$ to ease comparison. A positive, negative or 0 value in Table 6 indicates that the light contrast of $S^{\mathcal{K}}$ is better, worse than or the same as that of $S^V$ accordingly.

**Table 5**
Light contrasts $l_1(S^{\mathcal{K}})$ and $l_2(S^{\mathcal{K}})$ by Algorithm 4 for $2 \le k \le n \le 10$.

| | $n \rightarrow$<br>$k \downarrow$ | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|
| $l_1(S^{\mathcal{K}})$ | 2 | 0.500 | 0.333 | 0.333 | 0.300 | 0.300 | 0.286 | 0.286 | 0.278 | 0.278 |
| | 3 | | 0.250 | 0.125 | 0.100 | 0.100 | 0.086 | 0.080 | 0.080 | 0.075 |
| | 4 | | | 0.125 | 0.050 | 0.033 | 0.029 | 0.029 | 0.024 | 0.021 |
| | 5 | | | | 0.063 | 0.021 | 0.012 | 0.009 | 0.008 | 0.008 |
| | 6 | | | | | 0.031 | 0.009 | 0.004 | 0.003 | 0.002 |
| | 7 | | | | | | 0.016 | 0.004 | 0.002 | 0.001 |
| | 8 | | | | | | | 0.008 | 0.002 | 0.001 |
| | 9 | | | | | | | | 0.004 | 0.001 |
| | 10 | | | | | | | | | 0.002 |
| $l_2(S^{\mathcal{K}})$ | 2 | 0.500 | 0.286 | 0.286 | 0.250 | 0.250 | 0.235 | 0.235 | 0.227 | 0.227 |
| | 3 | | 0.250 | 0.111 | 0.087 | 0.087 | 0.073 | 0.068 | 0.068 | 0.063 |
| | 4 | | | 0.125 | 0.047 | 0.030 | 0.026 | 0.026 | 0.021 | 0.019 |
| | 5 | | | | 0.063 | 0.020 | 0.011 | 0.008 | 0.007 | 0.007 |
| | 6 | | | | | 0.031 | 0.009 | 0.004 | 0.003 | 0.002 |
| | 7 | | | | | | 0.016 | 0.004 | 0.002 | 0.001 |
| | 8 | | | | | | | 0.008 | 0.002 | 0.001 |
| | 9 | | | | | | | | 0.004 | 0.001 |
| | 10 | | | | | | | | | 0.002 |

**Table 6**
Differences of $l_1(S^{\mathcal{K}}) - c_1(S^V)$ and $l_2(S^{\mathcal{K}}) - c_2(S^V)$ for $2 \le k \le n \le 10$.

| | $n \rightarrow$<br>$k \downarrow$ | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|
| $l_1(S^{\mathcal{K}}) - c_1(S^V)$ | 2 | 0.000 | 0.000 | 0.083 | 0.100 | 0.133 | 0.143 | 0.161 | 0.167 | 0.178 |
| | 3 | | 0.000 | −0.042 | −0.025 | 0.000 | 0.002 | 0.009 | 0.018 | 0.019 |
| | 4 | | | 0.000 | −0.017 | −0.008 | 0.000 | 0.008 | 0.008 | 0.009 |
| | 5 | | | | 0.000 | −0.013 | −0.009 | −0.005 | −0.002 | 0.000 |
| | 6 | | | | | 0.000 | −0.005 | −0.003 | −0.002 | −0.001 |
| | 7 | | | | | | 0.000 | −0.003 | −0.002 | −0.001 |
| | 8 | | | | | | | 0.000 | −0.001 | −0.001 |
| | 9 | | | | | | | | 0.000 | −0.001 |
| | 10 | | | | | | | | | 0.000 |
| $l_2(S^{\mathcal{K}}) - c_2(S^V)$ | 2 | 0.000 | 0.036 | 0.119 | 0.125 | 0.150 | 0.152 | 0.164 | 0.165 | 0.172 |
| | 3 | | 0.000 | −0.032 | −0.013 | 0.010 | 0.011 | 0.016 | 0.023 | 0.023 |
| | 4 | | | 0.000 | −0.012 | −0.003 | 0.005 | 0.011 | 0.011 | 0.011 |
| | 5 | | | | 0.000 | −0.011 | −0.007 | −0.004 | −0.001 | 0.001 |
| | 6 | | | | | 0.000 | −0.005 | −0.003 | −0.001 | 0.000 |
| | 7 | | | | | | 0.000 | −0.003 | −0.002 | −0.001 |
| | 8 | | | | | | | 0.000 | −0.001 | −0.001 |
| | 9 | | | | | | | | 0.000 | −0.001 |
| | 10 | | | | | | | | | 0.000 |

From Table 6 we find that the light contrasts of VCRG and VCS are the same when $n = k$, that of VCS is preferable only when $n$ closes to $k$, while that of VCRG is better when $n$ is large. Nevertheless, the differences (either $l_1 - c_1$ or $l_2 - c_2$) are rather slight. We may simply conclude that the light contrast of $S^{\mathcal{K}}$ in our $(k, n)$-VCRG is *comparable* to that of $S^V$ in a quality $(k, n)$-VCS when $k$ shares are superimposed. However, a $(k, n)$-VCRG does not expand any pixel (i.e. $m_{\text{VCS}} = 1$), while the pixel expansion of a $(k, n)$-VCS takes at least $2^{k-1}$ (say, $m_{\text{VCS}}^{(4,10)} = 80$ or $m_{\text{VCS}}^{(9,10)} = 630$; see Table 7).

The design of our $(k, n)$-VCRG algorithm is relatively easier than the construction of a $(k, n)$-VCS. The contributions of our research are now clear. We also note that the light contrast in either VCRG or VCS for a larger $k$ or $n$ is with more theoretic but less practical interests since it would be too small to be easily recognized by human visual ability.

## 5. Concluding remarks

In conventional $(k, n)$-VCSs, the general construction of the basis matrices is based on complicated mathematics with a pixel expansion of at least $2^{k-1}$ (which increases additionally as $n$ grows). Without any extra pixel expansion, we design novel and simple algorithms for producing sets of $(k, n)$-VCRGs in this paper. The correctness of these algorithms is formally proved and the corresponding light transmissions/contrasts are also analyzed. The experimental results demonstrate the feasibility and applicability of our algorithms. In spite of the simplicity, the light contrast of our best $(k, n)$-VCRG algorithm is competitive to that of the conventional $(k, n)$-VCS when $k$ shares are superimposed, which is the most critical situation in a $(k, n)$ structure.

The feature of $m_{\text{VCS}} = 1$ without any extra pixel expansion in our approach is much attractive in practical applications as long as the secret image does not contain very small white or black regions. Even though the reconstruction ability is not as good as VCS, our VCRG ideas still establish a sound and constructive model for the research of visual secret sharing. The proofs for verifying our algorithms and the analysis of the light transmissions/contrasts are also informative from the theoretical point of view.

There are some further research including whether or not the light transmission of $k$ or $n$ superimposed shares could be improved, how to analyze the reconstruction ability of $(k, n)$-VCRG, could we find the bound of contrast (and/or small regions) under which our eyes cannot recognize the reconstructed white and black pixels, and so on. It is also interesting to investigate other subjects of VCS in view of VCRG.

## Appendix A. *m* and *l* in $(k, n)$-VCS

Table 7 gives the pixel expansion ($m$) of a certain $(k, n)$-VCS in [3,4] and the corresponding number of white pixels in a reconstructed black block by $k$ shares ($l$) for $2 \le k \le n \le 10$.

**Table 7**
$m$ and $l$ of a $(k, n)$-VCS in [3,4] for $2 \le k \le n \le 10$.

| | $m$ | | | | | | | | | $l$ | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $k \downarrow$ $n \to$ | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| 2 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| 3 | | 4 | 6 | 8 | 10 | 12 | 14 | 16 | 18 | | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 4 | | | 8 | 15 | 24 | 35 | 48 | 63 | 80 | | | 0 | 2 | 6 | 12 | 20 | 30 | 42 |
| 5 | | | | 16 | 30 | 48 | 70 | 96 | 126 | | | | 0 | 2 | 6 | 12 | 20 | 30 |
| 6 | | | | | 32 | 70 | 128 | 210 | 320 | | | | | 0 | 3 | 12 | 31 | 64 |
| 7 | | | | | | 64 | 140 | 256 | 420 | | | | | | 0 | 3 | 12 | 31 |
| 8 | | | | | | | 128 | 315 | 640 | | | | | | | 0 | 4 | 20 |
| 9 | | | | | | | | 256 | 630 | | | | | | | | 0 | 4 |
| 10 | | | | | | | | | 512 | | | | | | | | | 0 |

## Appendix B. An example of light transmissions achieved by Algorithm 3

Consider $(k, n) = (3, 5)$. By Algorithm 3, we have $\mathcal{Q} = \{q_1, q_2, q_3\}$, $\mathcal{G} = \{g_1, g_2\}$ and $\mathcal{R} = \mathcal{Q} \cup \mathcal{G} = \{q_1, q_2, q_3, g_1, g_2\}$ (see formula (4)) into which each pixel $p \in P$ is encoded. Table 8 summarizes the outcomes in Lemmas 8–11 corresponding to all possible combinations of $\mathcal{H} = \{r_{i_1}, r_{i_2}, \dots, r_{i_h}\} \subseteq \mathcal{R}$ with regard to $1 \le h \le 5$.

**Table 8**
Results of $\mathcal{H} = \{r_{i_1}, r_{i_2}, \dots, r_{i_h}\}$ with regard to $1 \le h \le 5$ by Algorithm 3.

| $h$, $1 \le h \le 5$ | $\mathcal{H} = \{r_{i_1}, r_{i_2}, \dots, r_{i_h}\}$, $r_{i_j} \in \{q_1, q_2, q_3, g_1, g_2\}$ | Whether $\mathcal{Q} \subseteq \mathcal{H}$ | Number of possible combinations | $(t(h_{\mathrm{I}}(0))$, $t(h_{\mathrm{I}}(1))) =$ $(1/2^{h-1}, 0)$ | $(t(h_{\mathrm{II}}(0))$, $t(h_{\mathrm{II}}(1))) =$ $(1/2^h, 1/2^h)$ | $(\mathcal{P}r(\mathcal{Q} \subseteq \mathcal{H})$, $\mathcal{P}r(\mathcal{Q} \not\subseteq \mathcal{H})) =$ $(\eta, 1-\eta)$ | $(\mathcal{T}(S^{\mathcal{H}}[P(0)])$, $\mathcal{T}(S^{\mathcal{H}}[P(1)]))$ |
|---|---|---|---|---|---|---|---|
| 1 | $\{q_1\}$, $\{q_2\}$, $\{q_3\}$, $\{g_1\}$, $\{g_3\}$ | no | 5 | – | (1/2, 1/2) | (0, 1) | (0.5, 0.5) |
| 2 | $\{q_1, q_2\}$, $\{q_1, q_3\}$, $\{q_1, g_1\}$, $\{q_1, g_2\}$, $\{q_2, q_3\}$, $\{q_2, g_1\}$, $\{q_2, g_2\}$, $\{q_3, g_1\}$, $\{q_3, g_2\}$, $\{g_1, g_2\}$ | no | 10 | – | (1/4, 1/4) | (0, 1) | (0.25, 0.25) |
| 3 | $\{q_1, q_2, q_3\}$ | yes | 1 | (1/4, 0) | – | (1/10, 9/10) | $(0.1375, 0.1125)$ $(= (\frac{1}{4} \times \frac{1}{10} + \frac{1}{8} \times \frac{9}{10}, \frac{1}{8} \times \frac{9}{10})$ |
| | $\{q_1, q_2, g_1\}$, $\{q_1, q_2, g_2\}$, $\{q_1, q_3, g_1\}$, $\{q_1, q_3, g_2\}$, $\{q_1, g_1, g_2\}$, $\{q_2, q_3, g_1\}$, $\{q_2, q_3, g_2\}$, $\{q_2, g_1, g_2\}$, $\{q_3, g_1, g_2\}$ | no | 9 | – | (1/8, 1/8) | | |
| 4 | $\{q_1, q_2, q_3, g_1\}$,<br>$\{q_1, q_2, q_3, g_2\}$ | yes | 2 | (1/8, 0) | – | (2/5, 3/5) | $(0.0875, 0.0375)$ $(= (\frac{1}{8} \times \frac{2}{5} + \frac{1}{16} \times \frac{3}{5}, \frac{1}{16} \times \frac{3}{5})$ |
| | $\{q_1, q_2, g_1, g_2\}$,<br>$\{q_1, q_3, g_1, g_2\}$,<br>$\{q_2, q_3, g_1, g_2\}$ | no | 3 | – | (1/16, 1/16) | | |
| 5 | $\{q_1, q_2, q_3, g_1, g_5\}$ | yes | 1 | (1/16, 0) | – | (1, 0) | $(0.0625, 0)$ $(= (\frac{1}{16} \times 1, 0))$ |

## Appendix C. An example of light transmissions achieved by Algorithm 4

Consider again $(k, n) = (3, 5)$. Without loss of generality, we assume that Algorithm 4 generates $\mathscr{R} = \{r_1, r_2, \dots, r_5\} = \{q_1, q_1, q_2, q_2, q_3\}$, which indicates $(y_1, y_2, y_3) = (2, 2, 1)$, for a certain pixel $p \in P$. Note that the following computations are similar for $(y_1, y_2, y_3) = (2, 1, 2)$ or $(1, 2, 2)$. The calculations in Lemma 16 for this case are summarized in Table 9.

**Table 9**
Relationships among $(x_1, x_2, x_3)$, $\mathcal{H} = \{r_{i_1}, r_{i_2}, \ldots, r_{i_h}\}$, number of occurrences, probability and light transmissions with regard to $1 \le h \le 5$ and $1 \le l \le h$ by Algorithm 4.

| $h$,<br>$1 \le h \le 5$ | $l$,<br>$1 \le l \le h$ | $(x_1, x_2, x_3)$,<br>$0 \le x_j \le l$<br>and<br>$\sum_{j=1}^{3} x_j = h$ | $(x_1, x_2, x_3) \in \mathbb{X}$<br>or $\mathbb{U} - \mathbb{X}$ | $\mathcal{H} = \{r_{i_1}, r_{i_2}, \ldots, r_{i_h}\}$,<br>$r_{i_j} \in \{q_1, q_2, q_3\}$ | Number of occurrences<br>$\prod_{j=1}^{k} \mathrm{C}(y_j, x_j)$ | Probability<br>$\frac{\prod_{j=1}^{k} \mathrm{C}(y_j, x_j)}{\mathrm{C}(n,h)}$ | $\kappa/2^{k-1}$ | $\xi$ | $(\mathcal{T}(S^{\mathcal{H}}[P(0)]),$<br>$\mathcal{T}(S^{\mathcal{H}}[P(1)]))$ |
|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | (1, 0, 0),<br>(0, 1, 0),<br>(0, 0, 1) | $\mathbb{U} - \mathbb{X}$ | $\{q_1\}$,<br>$\{q_2\}$,<br>$\{q_3\}$ | $\mathrm{C}(2, 1) = 2$<br>$\mathrm{C}(2, 1) = 2$<br>$\mathrm{C}(1, 1) = 1$ | 2/5<br>2/5<br>1/5 | – | 1/2 | (0.5, 0.5) |
| 2 | 1 | (2, 0, 0),<br>(0, 2, 0) | $\mathbb{U} - \mathbb{X}$ | $\{q_1, q_1\}$,<br>$\{q_2, q_2\}$ | $\mathrm{C}(2, 2) = 1$<br>$\mathrm{C}(2, 2) = 1$ | 1/10<br>1/10 | – | 3/10<br>$(= \frac{1}{2} \times \frac{2}{10} +$<br>$\frac{1}{4} \times \frac{8}{10})$ | (0.3, 0.3) |
| | 2 | (1, 1, 0),<br>(1, 0, 1),<br>(0, 1, 1) | $\mathbb{U} - \mathbb{X}$ | $\{q_1, q_2\}$,<br>$\{q_1, q_3\}$,<br>$\{q_2, q_3\}$ | $\mathrm{C}(2, 1) \times \mathrm{C}(2, 1) = 4$<br>$\mathrm{C}(2, 1) \times \mathrm{C}(1, 1) = 2$<br>$\mathrm{C}(2, 1) \times \mathrm{C}(1, 1) = 2$ | 4/10<br>2/10<br>2/10 | | | |
| 3 | 1 | – | – | $\varnothing$ | – | 0 | – | 3/20<br>$(= \frac{1}{4} \times \frac{6}{10})$ | (0.25, 0.15)<br>$(= (\frac{1}{10} + \frac{3}{20}, \frac{3}{20}))$ |
| | 2 | (2, 1, 0),<br>(1, 2, 0),<br>(2, 0, 1),<br>(0, 2, 1) | $\mathbb{U} - \mathbb{X}$ | $\{q_1, q_1, q_2\}$,<br>$\{q_1, q_2, q_2\}$,<br>$\{q_1, q_1, q_3\}$,<br>$\{q_2, q_2, q_3\}$ | $\mathrm{C}(2, 2) \times \mathrm{C}(2, 1) = 2$<br>$\mathrm{C}(2, 1) \times \mathrm{C}(2, 2) = 2$<br>$\mathrm{C}(2, 2) \times \mathrm{C}(1, 1) = 1$<br>$\mathrm{C}(2, 2) \times \mathrm{C}(1, 1) = 1$ | 2/10<br>2/10<br>1/10<br>1/10 | | | |
| | 3 | (1, 1, 1) | $\mathbb{X}$ | $\{q_1, q_2, q_3\}$ | $\mathrm{C}(2, 1) \times \mathrm{C}(2, 1) \times \mathrm{C}(1, 1) = 4$ | 4/10 | 1/10<br>$(= \frac{1}{4} \times \frac{4}{10})$ | – | |
| 4 | 1 | – | – | $\varnothing$ | 0 | 0 | – | 1/20<br>$(= \frac{1}{4} \times \frac{1}{5})$ | (0.25, 0.05)<br>$(= (\frac{1}{5} + \frac{1}{20}, \frac{1}{20}))$ |
| | 2 | (2, 2, 0) | $\mathbb{U} - \mathbb{X}$ | $\{q_1, q_1, q_2, q_2\}$ | $\mathrm{C}(2, 2) \times \mathrm{C}(2, 2) = 1$ | 1/5 | | | |
| | 3 | (2, 1, 1),<br>(1, 2, 1) | $\mathbb{X}$ | $\{q_1, q_1, q_2, q_3\}$,<br>$\{q_1, q_2, q_2, q_3\}$ | $\mathrm{C}(2, 2) \times \mathrm{C}(2, 1) \times \mathrm{C}(1, 1) = 2$<br>$\mathrm{C}(2, 1) \times \mathrm{C}(2, 2) \times \mathrm{C}(1, 1) = 2$ | 4/5 | 1/5<br>$(= \frac{1}{4} \times \frac{4}{5})$ | – | |
| 5 | 1 | – | – | $\varnothing$ | 0 | 0 | – | 0 | (0.25, 0) |
| | 2 | – | – | $\varnothing$ | 0 | 0 | | | |
| | 3 | (2, 2, 1) | $\mathbb{X}$ | $\{q_1, q_1, q_2, q_2, q_3\}$ | $\mathrm{C}(2, 2) \times \mathrm{C}(2, 2) \times \mathrm{C}(1, 1) = 1$ | 1 | 1/4 | – | |

## References

[1] M. Naor, A. Shamir, Visual cryptography, in: Proceedings of Advances in Cryptology: Eurpocrypt'94, in: Lecture Notes in Computer Science, vol. 950, Springer, 1995, pp. 1–12.

[2] G. Ateniese, C. Blundo, A. De Santis, D.R. Stinson, Visual cryptography for general access structures, Inform. and Comput. 129 (1996) 86–106.

[3] S. Droste, New results on visual cryptography, in: Proceedings of Advances in Cryptology: CRYPTO'96, in: Lecture Notes in Computer Science, vol. 1109, Springer, 1996, pp. 401–415.

[4] T. Kotoh, H. Imai, Some visual secret sharing schemes and their share sizes, in: Proc. of Intl. Conf. on Cryptology and Information Security, 1996, pp. 41–47.

[5] P.A. Eisen, D.R. Stinson, Threshold visual cryptography schemes with specified whiteness levels of reconstructed pixels, Des. Codes Cryptogr. 25 (2002) 15–61.

[6] S.J. Shyu, M.C. Chen, Optimum pixel expansions for threshold visual secret sharing schemes, IEEE Trans. Inform. Forensics Secur. 6 (3) (September 2011) 960–969.

[7] G. Ateniese, C. Blundo, A. De Santis, D.R. Stinson, Constructions and bounds for visual cryptography, in: Proceedings of Automata, Languages and Programming: ICALP 96, in: Lecture Notes in Computer Science, vol. 1099, Springer, 1996, pp. 416–428.

[8] C. Blundo, A. De Santis, D.R. Stinson, On the contrast in visual cryptography schemes, J. Cryptogr. 12 (1999) 261–289.

[9] C. Blundo, A. De Santis, D.R. Stinson, Improved schemes for visual cryptography, Des. Codes Cryptogr. 24 (2001) 255–278.

[10] G. Ateniese, C. Blundo, A. De Santis, D.R. Stinson, Extended capabilities for visual cryptography, Theoret. Comput. Sci. 250 (2001) 143–161.

[11] R.-Z. Wang, Region incrementing visual cryptography, IEEE Signal Process. Lett. 16 (2009) 659–662.

[12] E.R. Verheul, H.C.A. Van Tilborg, Constructions and properties of $k$ out of $n$ visual secret sharing schemes, Des. Codes Cryptogr. 11 (1997) 179–196.

[13] C.-N. Yang, C.-S. Laih, New colored visual secret sharing schemes, Des. Codes Cryptogr. 20 (2000) 325–335.

[14] Y.-C. Hou, Visual cryptography for color images, Pattern Recognit. 36 (2003) 1619–1629.

[15] S.J. Shyu, Efficient visual secret sharing scheme for color images, Pattern Recognit. 39 (2006) 866–880.

[16] O. Kafri, E. Keren, Encryption of pictures and shapes by random grids, Opt. Lett. 12 (1987) 377–379.

[17] S.J. Shyu, Image encryption by random grids, Pattern Recognit. 40 (2007) 1014–1031.

[18] S.J. Shyu, Image encryption by multiple random grids, Pattern Recognit. 42 (2009) 1582–1596.

[19] S.J. Shyu, C. Kun, Visual multiple-secret sharing by circle random grids, SIAM J. Imaging Sci. 3 (4) (2010) 926–953.

[20] S.J. Shyu, Visual cryptograms of random grids for general access structures, IEEE Trans. Circuits Syst. Video Technol. 23 (3) (March 2013) 414–424.

[21] T.-H. Chen, K.-H. Tsao, Visual secret sharing by random grids revisited, Pattern Recognit. 42 (2009) 2203–2217.

[22] T.-H. Chen, K.-H. Tsao, Threshold visual secret sharing by random grids, J. Syst. Softw. 84 (2011) 1197–1208.

[23] T.-H. Chen, K.-H. Tsao, User-friendly random grid-based visual secret sharing, IEEE Trans. Circuits Syst. Video Technol. 21 (11) (2011) 1693–1703.

[24] C.-N. Yang, New visual secret sharing schemes using probabilistic method, Pattern Recognit. Lett. 25 (2004) 481–494.