Constructions and Properties of General (k, n) Block-Based Progressive Visual Cryptography

Ching-Nung Yang, Chih-Cheng Wu, Yi-Chin Lin, and Cheonshik Kim

Recently, Hou and others introduced a (2, n) block-based progressive visual cryptographic scheme (BPVCS) in which image blocks can be gradually recovered step by step. In Hou and others' (2, n)-BPVCS, a secret image is subdivided into n non-overlapping image blocks. When t ($2 \le t \le n$) participants stack their shadow images, all the image blocks associated with these t participants will be recovered. However, Hou and others' scheme is only a simple 2-out-of-n case. In this paper, we discuss a general (k, n)-BPVCS for any k and n. Our main contribution is to give two constructions (Construction 1 and Construction 2) of this general (k, n)-BPVCS. Also, we theoretically prove that both constructions satisfy a threshold property and progressive recovery of the proposed (k, n)-BPVCS. For k = 2, Construction 1 is reduced to Hou and others' (2, n)-BPVCS.

Keywords: Secret sharing, visual secret sharing, visual cryptography, progressive recovery.

I. Introduction

A (k, n) visual cryptographic scheme (VCS), where $k \le n$, encodes a secret image into n shadow images (referred to as shadows) distributed to n participants. The secret can be visually reconstructed when k or more shadows are stacked. No information will be revealed with any (k – 1) or fewer shadows. The reconstruction can be done by the human visual system directly without any cryptographic knowledge or the need for a computer. Applications of VCS can be found in [1]. The first VCS was proposed by [2], which used whiteness to distinguish black color from white color. In the VCS of [2], a secret pixel is subdivided into m (the pixel expansion) subpixels in each of n shadows. Most studies tried to reduce the pixel expansion. Some of them, [3]–[6], even have no pixel expansion (m = 1) — known as probabilistic VCS (PVCS). Hence, a conventional VCS with fixed m (m > 1) is referred to as a deterministic VCS (DVCS). Recently, Hou and others [7] proposed a (2, n) block-based progressive VCS (BPVCS) with a progressive recovery scheme, whereby image blocks can be gradually recovered step by step. In Hou and others' (2, n)-BPVCS, a secret image, P, is subdivided into n non-overlapping image blocks; namely, P_i ($1 \le i \le n$). The progressive recovery operates under the assumption that if any t ($2 \le t \le n$) shadows are stacked and participant i ($1 \le i \le n$) is involved, then the image block P_i can be restored. All the image blocks can be recovered when all n participants are involved in the reconstruction. In other words, each participant has their own decryption key for one particular image block. However, Hou and others' (2, n)-BPVCS is only a simple 2-out-of-n case. In this paper, we discuss a general (k, n)-BPVCS where a qualified set of participants consists of any k (≥ 2) participants. Two constructions — "Construction 1" and

Manuscript received Mar. 16, 2014; revised Oct. 12, 2014; accepted July 14, 2015.

The research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) by the Ministry of Education, Science & Technology (20120192).

Ching-Nung Yang (cnyang@mail.ndhu.edu.tw), Chih-Cheng Wu (d9721004@ems.ndhu.edu.tw), and Yi-Chin Lin (u9721020@ems.ndhu.edu.tw) are with the Department of Computer Science and Information Engineering, National Dong Hwa University, Hualien, Taiwan.

Cheonshik Kim (corresponding author, mipsan@paran.com) is with the Department of Digital Media Engineering, Anyang University, Rep. of Korea.

"Construction 2" — using ${}_nC_{k-1}$ and ${}_nC_k$ image blocks, respectively, are proposed. For $k = 2$, Construction 1 is reduced to Hou and others' $(2, n)$-BPVCS.

The rest of this paper is organized as follows. In Section II, we describe the notions of DVCS, PVCS, extended VCS (EVCS) with meaningful shadow, and probabilistic EVCS (PEVCS), which are the basic elements in our new (k, n)-BPVCS. Also, Hou and others' $(2, n)$-BPVCS is introduced. Two constructions of the general (k, n)-BPVCS are proposed in Section III. Furthermore, we theoretically prove that they hold progressive recovery and security. Our experiments are explained along with some discussions in Section IV. Finally, conclusions are given in Section V.

II. Related Works

1. DVCS and PVCS

In DVCS, a black-and-white secret pixel is subdivided into m black-and-white subpixels in each of n shadows. We use "$m - h$"B"h"W (that is, $(m - h)$ black subpixels and h white subpixels) and "$m - l$"B"l"W, where $0 \le l < h \le m$, to represent white and black secret pixels, respectively. The collection of the corresponding m subpixels in n shadows can be represented by an $n \times m$ Boolean matrix $\mathbf{S} = [S_{ij}]$, where the element S_{ij} represents the jth subpixel in the ith shadow. If S_{ij} is a black subpixel, then this is represented by "1"; similarly, if it is a white subpixel, then it is represented by "0." Stacking t shadows together, the grey-level of each secret pixel (m subpixels) in the stacked image is proportional to Hamming weight $H(\mathbf{v})$. The vector $\mathbf{v}$ is OR-ed m-tuple $\mathbf{v} = \mathrm{OR}(i_1, i_2, \ldots, i_t)$, where $i_1, i_2, \ldots, i_t$ are t rows of $\mathbf{S}$ associated with the shadows we stack. The formal definition for a binary DVCS is given as follows [8].

Definition 1. A (k, n)-DVCS consists of two $n \times m$ Boolean matrices, $\mathbf{B}_1$ and $\mathbf{B}_0$. To share a black (respectively white) secret pixel, the dealer arbitrarily chooses one row of a matrix in the set that includes all matrices obtained by permuting the columns in $\mathbf{B}_1$ (respectively $\mathbf{B}_0$) to a relative shadow. The chosen matrix defines the color of this m subpixel block in each one of n shadows. The (k, n)-DVCS is valid if the following three conditions are met:

1) In $\mathbf{B}_1$, the OR-ed vector $\mathbf{v}_1$ of any k out of n rows satisfies $H(\mathbf{v}_1) \ge (m - l)$.
2) In $\mathbf{B}_0$, the OR-ed vector $\mathbf{v}_0$ of any k out of n rows satisfies $H(\mathbf{v}_0) \le (m - h)$.
3) For any subset $\{i_1, i_2, \ldots, i_t\} \subset \{1, 2, \ldots, n\}$ with $t < k$, the two collections of $t \times m$ matrices obtained by restricting each $t \times m$ matrix to rows $i_1, i_2, \ldots, i_t$ are indistinguishable in the sense that they contain the same matrices with the same frequencies.

The first two conditions are called contrast conditions, and the third condition is the security condition. Let $\mathrm{OR}(\mathbf{B}_1|t)$ and $\mathrm{OR}(\mathbf{B}_0|t)$ denote the "OR"-ed of any t rows in $\mathbf{B}_1$ and $\mathbf{B}_0$, respectively. The authors in [9]–[10] rewrite the conditions in Definition 1 as the contrast condition (D-1) and the security condition (D-2) as follows; in addition, they theoretically prove the equivalence of the condition of (3) in Definition 1 and condition (D-2): (D-1) $H(\mathrm{OR}(\mathbf{B}_1|t)) \ge (m - l)$ and $H(\mathrm{OR}(\mathbf{B}_0|t)) \le (m - h)$ for $t = k$. (D-2) $H(\mathrm{OR}(\mathbf{B}_1|t)) = H(\mathrm{OR}(\mathbf{B}_0|t))$ for $t \le (k - 1)$.

In [2], the *contrast* of a DVCS is defined as the difference in weight between a black pixel and a white pixel in the reconstructed image; that is,

$$\alpha = \frac{H(V_1) - H(V_0)}{m} = \frac{(m-l) - (m-h)}{m} = \frac{h-l}{m}.$$

To address the pixel expansion problem, a PVCS adopts the frequency of white pixels in an area to distinguish between the black area and white area in a reconstructed image. In a white area of a reconstructed image, this frequency is higher than that in the black area. In [4], Yang proposed a PVCS with $m = 1$ (that is, no pixel expansion). A (k, n)-PVCS can be constructed by a black set and a white set (C_1 and C_0) consisting of $n \times 1$ column matrices, respectively. When sharing a black (respectively white) pixel, the dealer first randomly chooses one $n \times 1$ column matrix in C_1 (respectively C_0), and then randomly selects one row in this column matrix to a relative shadow. The chosen set defines the color level of the pixel in shadows. The author in [4] showed that we can use all the columns of the basis matrices $\mathbf{B}_0$ and $\mathbf{B}_1$ in a DVCS as the $n \times 1$ column matrices of sets C_0 and C_1 in a PVCS. Let $\mathrm{OR}(C_1 | t)$ and $\mathrm{OR}(C_0 | t)$ denote OR-ed t rows in all column matrices in C_1 and C_0, respectively, and $P(\cdot)$ be the appearance probability of the "0" (whiteness) in a set. The contrast condition and the security condition of (k, n)-PVCS are shown as follows: (P-1) $P(\mathrm{OR}(C_1|t)) \le p_1$ and $P(\mathrm{OR}(C_0|t)) \ge p_0$ for $t = k$, where $p_1 < p_0$. (P-2) $P(\mathrm{OR}(C_1|t)) = P(\mathrm{OR}(C_0|t))$ for $t \le (k - 1)$.

Conditions (P-1) and (P-2) are similar to (D-1) and (D-2), but they are in a probabilistic manner. In (P-1), the different probability of "whiteness" is used to distinguish between black color and white color. Condition (P-2) ensures a (k, n)-PVCS scheme that is of the unconditional security type. A secret image can be successfully recognized through the different probabilities of "whiteness" in the reconstructed image. Since the frequency of white subpixels in the white and black areas is p_0 and p_1, respectively, the average contrast of a PVCS is defined to be $\bar{\alpha} = p_0 - p_1$ [4]. Since all matrices in C_0 and C_1 are $n \times 1$ matrices, it can be said that a PVCS has no pixel expansion. However, shadows of a DVCS are m times those of

a PVCS. We give one example to illustrate the shadows and stacked results of both a DVCS and a PVCS.

Example 1. Construct a (2, 2)-DVCS and (2, 2)-PVCS by $\mathbf{B}_0 = \begin{bmatrix}1&0\\1&0\end{bmatrix}$ and $\mathbf{B}_1 = \begin{bmatrix}1&0\\0&1\end{bmatrix}$. It is observed that $H(\mathrm{OR}(\mathbf{B}_1|2)) = 2$, $H(\mathrm{OR}(\mathbf{B}_0|2)) = 1$, and $H(\mathrm{OR}(\mathbf{B}_1|1)) = H(\mathrm{OR}(\mathbf{B}_0|1)) = 1$; thus, they satisfy (D-1) and (D-2). Suppose that xByW represents $(\overbrace{1\cdots1}^{x}, \overbrace{0\cdots0}^{y})$ and its permutations. In a reconstructed image, the black color is 2B0W and the white color is 1B1W; the contrast is $\alpha = (h - l)/m = 1/2$. Because all 2-subpixel blocks in two shadows are all 1B1W, they are noise-like. On the other hand, we can use all two columns of $\mathbf{B}_0$ and $\mathbf{B}_1$ as the 2 × 1 column matrices in sets $C_0 = \left\{\begin{bmatrix}1\\1\end{bmatrix}, \begin{bmatrix}0\\0\end{bmatrix}\right\}$ and $C_1 = \left\{\begin{bmatrix}1\\0\end{bmatrix}, \begin{bmatrix}0\\1\end{bmatrix}\right\}$, respectively. Since $\mathrm{OR}(C_0|2) = \{1,0\}$ and $\mathrm{OR}(C_1|2) = \{1,1\}$, we have $P(\mathrm{OR}(C_0|t)) \geq p_0 = 1/2$ and $P(\mathrm{OR}(C_1|t)) \leq p_1 = 0$. This satisfies condition (P-1); and the average contrast $\bar{\alpha} = p_0 - p_1 = 1/2$. In addition, $P(\mathrm{OR}(C_1|1)) = P(\mathrm{OR}(C_0|1)) = 1/2$ satisfies condition (P-2). Shadows of (2, 2)-PVCS are not expanded. However, the visual quality of a recovered image will be degraded.

2. EVCS and PEVCS

Noise-like shadows in DVCS (or PVCS) are unusual and susceptible to censors. In addition, the identification and management of noise-like shadows is difficult. Therefore, an EVCS (with its extended ability — "the meaningful shadow") is accordingly proposed. This extended capability was first introduced by Naor and Shamir [2]. They used 3B1W (2B2W) to represent black (white) pixels in shadows, but used 4B0W (3B1W) in reconstructed images to represent black and white colors. With regards to the formal definition of EVCS, one should refer to [11].

Let S_1 and S_2 be two shadows of a (2, 2)-EVCS, and c_i is the cover pixel on S_i, where $i = 1, 2$. Suppose that $\mathbf{B}_1^{c_1c_2}$ ($\mathbf{B}_0^{c_1c_2}$) is a matrix for a black (white) secret pixel in a (2, 2)-EVCS. Then, the associated cover pixel is black ($c_i = 1$) or white ($c_i = 0$), where c_1 and c_2 denote the colors in S_1 and S_2, respectively. The following example shows Naor and Shamir's (2, 2)-EVCS [2].

Example 2. Construct a (2, 2)-EVCS with $m = 4$. All eight basis matrices, $\mathbf{B}_0^{00}, \mathbf{B}_0^{01}, \mathbf{B}_0^{10}, \mathbf{B}_0^{11}, \mathbf{B}_1^{00}, \mathbf{B}_1^{01}, \mathbf{B}_1^{10}$, and $\mathbf{B}_1^{11}$, are given as follows:

$$\mathbf{B}_0^{00} = \begin{bmatrix}1&0&0&1\\1&0&1&0\end{bmatrix}, \mathbf{B}_0^{01} = \begin{bmatrix}1&0&0&1\\1&0&1&1\end{bmatrix}, \mathbf{B}_0^{10} = \begin{bmatrix}1&0&1&1\\1&0&1&0\end{bmatrix}, \mathbf{B}_0^{11} = \begin{bmatrix}1&0&1&1\\1&0&1&1\end{bmatrix},$$

$$\mathbf{B}_1^{00} = \begin{bmatrix}1&0&0&1\\0&1&1&0\end{bmatrix}, \mathbf{B}_1^{01} = \begin{bmatrix}1&0&0&1\\1&1&1&0\end{bmatrix}, \mathbf{B}_1^{10} = \begin{bmatrix}1&0&1&1\\1&1&0&0\end{bmatrix}, \mathbf{B}_1^{11} = \begin{bmatrix}1&0&1&1\\1&1&1&0\end{bmatrix}. \quad (1)$$

The contrast of the recovered image is given by $\alpha = (h - l)/m$ [= (1 − 0)/4 = 1/4]. Since the Hamming weight of the ith row (i =1, 2), is 2 and 3 for $c_i = 0$ and $c_i = 1$, respectively, the contrast of shadow α_s is also (2–1)/4 = 1/4.

If two shadows in this (2, 2)-EVCS have the same cover image, then the colors of c_1 and c_2 are the same (that is, $c_1 = c_2$). Thus, we only require $\mathbf{B}_0^{00}, \mathbf{B}_1^{00}, \mathbf{B}_0^{11}$, and $\mathbf{B}_1^{11}$ from (1) for the (2, 2)-EVCS containing two shadows having the same cover image.

Generally, EVCS has a larger pixel expansion than VCS. For example, let us assume that we have $m = 2$ for (2, 2)-DVCS, while $m = 4$ for (2, 2)-EVCS. As in the case of a DVCS, we can also apply a probabilistic approach (that is, choosing every column randomly each time) to EVCS to implement a PEVCS.

Example 3. Continuation of Example 2.

We use all four columns of the basis matrices featured in (1) to construct sets of 2 × 1 column matrices — $C_0^{00}, C_0^{01}, C_0^{10}, C_0^{11}, C_1^{00}, C_1^{01}, C_1^{10}$ and C_1^{11}. Therefore, the sets of a (2, 2)-PEVCS with two different cover images on shadows are shown as follows:

$$C_0^{00} = \left\{\begin{bmatrix}1\\1\end{bmatrix}\begin{bmatrix}0\\0\end{bmatrix}\begin{bmatrix}0\\1\end{bmatrix}\begin{bmatrix}1\\0\end{bmatrix}\right\}, C_0^{01} = \left\{\begin{bmatrix}1\\1\end{bmatrix}\begin{bmatrix}0\\0\end{bmatrix}\begin{bmatrix}0\\1\end{bmatrix}\begin{bmatrix}1\\1\end{bmatrix}\right\}, C_0^{10} = \left\{\begin{bmatrix}1\\1\end{bmatrix}\begin{bmatrix}0\\0\end{bmatrix}\begin{bmatrix}1\\1\end{bmatrix}\begin{bmatrix}1\\0\end{bmatrix}\right\}, C_0^{11} = \left\{\begin{bmatrix}1\\1\end{bmatrix}\begin{bmatrix}0\\0\end{bmatrix}\begin{bmatrix}1\\1\end{bmatrix}\begin{bmatrix}1\\1\end{bmatrix}\right\},$$

$$C_1^{00} = \left\{\begin{bmatrix}1\\0\end{bmatrix}\begin{bmatrix}0\\1\end{bmatrix}\begin{bmatrix}0\\1\end{bmatrix}\begin{bmatrix}1\\0\end{bmatrix}\right\}, C_1^{01} = \left\{\begin{bmatrix}1\\1\end{bmatrix}\begin{bmatrix}0\\1\end{bmatrix}\begin{bmatrix}0\\1\end{bmatrix}\begin{bmatrix}1\\0\end{bmatrix}\right\}, C_1^{10} = \left\{\begin{bmatrix}1\\1\end{bmatrix}\begin{bmatrix}0\\1\end{bmatrix}\begin{bmatrix}1\\0\end{bmatrix}\begin{bmatrix}1\\0\end{bmatrix}\right\}, C_1^{11} = \left\{\begin{bmatrix}1\\1\end{bmatrix}\begin{bmatrix}0\\1\end{bmatrix}\begin{bmatrix}1\\1\end{bmatrix}\begin{bmatrix}1\\0\end{bmatrix}\right\}. \quad (2)$$

Since $\mathrm{OR}(C_0^{c_1c_2} | 2) = \{1,0,1,1\}$ and $\mathrm{OR}(C_1^{c_1c_2} | 2) = \{1,1,1,1\}$, we have $P(\mathrm{OR}(C_0^{c_1c_2} | 2)) \geq p_0 = 1/4$ and $P(\mathrm{OR}(C_1^{c_1c_2} | 2)) \leq p_1$ (= 0). So, $\bar{\alpha} = p_0 - p_1 = 1/4$. For a (2, 2)-PEVCS with shadows that have an identical cover image, there are only four sets — $C_0^{00}, C_0^{11}, C_1^{00}$, and C_1^{11}.

3. Hou and Others' (2, n)-BPVCS

In [7], Hou and others propose a (2, n)-BPVCS with non-expanded shadow size. In Hou and others' (2, n)-BPVCS, a secret image P is subdivided into n image blocks $\{P_1, P_2, \ldots, P_n\}$ that satisfy the following two properties: (a) any two image blocks do not have the same overlapping area; that is, $P_i \cap P_j = \phi$ for $i \neq j$ (disjoint property) and (b) their union is the original secret image P; that is, $O = P_1 \cup P_2 \cup \cdots \cup P_n$ (union property). The disjoint property provides the progressive recovery, and the union property ensures that all participants can work together to reconstruct the whole secret image. If participant i, $1 \leq i \leq n$, is involved in reconstruction, then the image block P_i can be recovered. When any t ($2 \leq t \leq n$) shadows are stacked, all the image blocks corresponding to these t participants will be recovered, but other areas are still noise-like. Therefore, each participant has his own decryption key for one particular image block. Considering the example

(2, 3)-BPVCS, the secret image is first subdivided into three image blocks — P_1, P_2, and P_3. When two participants, p_1 and p_2, cooperate together, they can recover image blocks P_1 and P_2, and the other area is noise-like. However, when stacking shadows, $(S_1 + S_3)$ or $(S_2 + S_3)$, the image blocks P_1 and P_3, and P_2 and P_3 are recovered, respectively. All three stacked shadows can recover all image blocks, P_1, P_2, and P_3. There are two types of Hou and others' (2, n)-BPVCS — a (2, n)-BPVCS with noise-like shadows and a (2, n)-BPVCS with meaningful shadows. In fact, Hou and others' (2, n)-BPVCS with noise-like shadows and (2, n)-BPVCS with meaningful shadows are constructed by (2, 2)-PVCS (see Example 1) and (2, 2)-PEVCS with the same cover image (see Example 3), respectively. In Hou and others' (2, n)-BPVCS with noise-like shadows, the dealer applies (2, 2)-PVCS on P_i, $1 \le i \le n$, to get noise-like sub-shadows $S_{i,1}$ and $S_{i,2}$. On the other hand, when constructing Hou and others' (2, n)-BPVCS with meaningful shadows, we should additionally consider the cover image O. The cover image is partitioned into n subcover images to give O_i, $1 \le i \le n$, according to the position of image block P_i. Then, for each P_i and O_i, $1 \le i \le n$, we apply (2, 2)-PEVCS with the same cover image to obtain sub-shadows $S_{i,1}$ and $S_{i,2}$. The method of composition of shadows for these two (2, n)-BPVCSs is the same. The dealer delivers $S_{i,1}$ to participant i and $S_{i,2}$ to the other $(n-1)$ participants. Afterwards, every participant offers up all of their received sub-shadows according to the position of P_i to construct n shadows as follows:

$$S_j = S_{j,1} \cup \left(\bigcup_{i \in \{1,\ldots,n\}, i \neq j} S_{i,2} \right) \quad (1 \le j \le n). \tag{3}$$

Since both a (2, 2)-PVCS and a (2, 2)-PEVCS have a non-expanded shadow size, the shadow size of Hou and others' (2, n)-BPVCS is also not expanded. As an example, Hou and others' (2, 4)-BPVCS is constructed below. By (3), we have four shadows as given below in (4). Figures 1(a) and 1(b) are partitions of a secret image and partitions of a cover image, respectively. Figure 1(c) illustrates four shadows.

$$\begin{cases} S_1 = S_{1,1} \cup S_{2,2} \cup S_{3,2} \cup S_{4,2}, \\ S_2 = S_{1,2} \cup S_{2,1} \cup S_{3,2} \cup S_{4,2}, \\ S_3 = S_{1,2} \cup S_{2,2} \cup S_{3,1} \cup S_{4,2}, \\ S_4 = S_{1,2} \cup S_{2,2} \cup S_{3,2} \cup S_{4,1}. \end{cases} \tag{4}$$

Consider the stacked result of $(S_1 + S_2)$. We have two image blocks, P_1 and P_2, and two noise-like blocks, $S_{3,2}$ and $S_{4,2}$, as shown in (5). By stacking another shadow S_3 on $(S_1 + S_2)$, we obtain three image blocks, P_1, P_2, and P_3, and one noise-like block, $S_{4,2}$, in (6). When stacking all four shadows, we can recover all image blocks (see (7)).

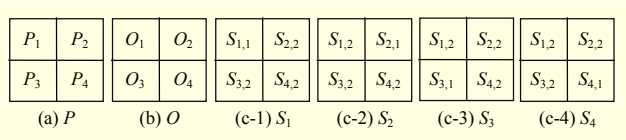

Fig. 1. Composition of shadows for Hou and others' (2, 4)-BPVCS: (a) four image blocks, (b) four subcover images, and (c) four shadows.

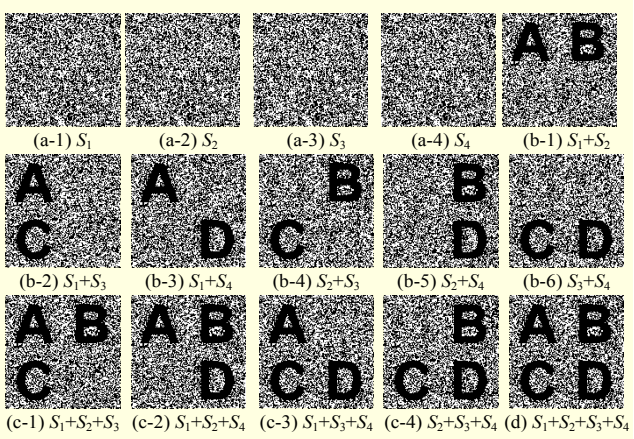

Fig. 2. Progressive recovery of Hou and others' (2, 4)-BPVCS with noise-like shadows: (a) four shadows, (b) stacking any two shadows, (c) stacking any three shadows, and (d) stacking all four shadows.

$$\begin{cases} S_1 + S_2 = (S_{1,1} + S_{1,2}) \cup (S_{2,1} + S_{2,2}) \cup (S_{3,2} + S_{3,2}) \cup (S_{4,2} + S_{4,2}) \\ \quad = \overbrace{P_1 \cup P_2}^{2 \text{ image blocks}} \cup \overbrace{S_{3,2} \cup S_{4,2}}^{2 \text{ noise-like blocks}}. \end{cases} \tag{5}$$

$$\begin{cases} S_1 + S_2 + S_3 = (S_{1,1} + S_{1,2} + S_{1,2}) \cup (S_{2,2} + S_{2,1} + S_{2,2}) \\ \qquad \cup (S_{3,2} + S_{3,2} + S_{3,1}) \cup (S_{4,2} + S_{4,2} + S_{4,2}) \\ \qquad = \overbrace{P_1 \cup P_2 \cup P_3}^{3 \text{ image blocks}} \cup \overbrace{S_{4,2}}^{1 \text{ noise-like block}}. \end{cases} \tag{6}$$

$$\begin{cases} S_1 + S_2 + S_3 + S_4 = (S_{1,1} + S_{1,2} + S_{1,2} + S_{1,2}) \cup (S_{2,2} + S_{2,1} + S_{2,2} + S_{2,2}) \\ \qquad \cup (S_{3,2} + S_{3,2} + S_{3,1} + S_{3,2}) \cup (S_{4,2} + S_{4,2} + S_{4,2} + S_{4,1}) \\ \qquad = \overbrace{P_1 \cup P_2 \cup P_3 \cup P_4}^{4 \text{ image blocks}}. \end{cases} \tag{7}$$

Example 4. Construct Hou and others' (2, 4)-BPVCS with noise-like shadows.

Suppose that a secret image is divided into four image blocks, as in Fig. 1(a). Then, the contents of P_1, P_2, P_3, and P_4 are the printed-texts A, B, C, and D, respectively; that is, P is $\begin{bmatrix} \text{A} & \text{B} \\ \text{C} & \text{D} \end{bmatrix}$. By applying a (2, 2)-PVCS with $C_1 = \left\{ \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix} \right\}$ and $C_0 = \left\{ \begin{bmatrix} 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \end{bmatrix} \right\}$ to P_1, P_2, P_3, and P_4, we obtain sub-shadows

on which Hou and others' (2, 4)-BPVCS can be implemented. Four noise-like shadows and the progressive recovery results of stacking two, three, and four shadows are given in Fig. 2. For example, when stacking S_1 and S_3, we have $S_1 + S_3 = \boxed{\begin{matrix}A\\C\end{matrix}}$ (see Fig. 2(b-2)). By adding another shadow, S_4, we have $S_1 + S_3 + S_4 = \boxed{\begin{matrix}A\\C\ D\end{matrix}}$ (see Fig. 2(c-3)). Obviously, we can implement Hou and others' (2, 4)-BPVCS with the same cover image by using a (2, 2)-PEVCS.

III. Proposed (k, n)-BPVCS

A secret image P is first divided into N image blocks $\{P_1, P_2, \dots, P_N\}$ satisfying both the aforementioned disjoint property and union property. For each P_j, $1 \le j \le N$, we use (k, k)-PVCS to generate k sub-shadows, $S_{i,1}, S_{i,2}, \dots, S_{i,k}$. In this paper, we will show how to construct n shadows from these $(N \times k)$ sub-shadows. Moreover, both constructions use different image blocks (Construction 1: $N = {}_nC_{k-1}$ and Construction 2: $N = {}_nC_k$) and have different progressive recovery ratios. One can choose a construction method according to his application need. Two construction methods are introduced in sequence. Some notations are defined in Table 1.

The design concept of Construction 1 is described as follows. We use a matrix having ${}_nC_{k-1}$ columns with $(k-1)$ 1s in every column. Meantime, we generate k shadows from (k, k)-PVCS. From these k shadows, for every single column, we choose one shadow for all 0s and $(k-1)$ shadows for $(k-1)$ 1s. Therefore, when stacking t shadows, some corresponding image blocks can be revealed. The formal construction is shown in Construction 1.

Table 1. Notations used in proposed (k, n)-BPVCS.

Notation	Description
$D(\cdot)$	Function dividing an image into $N = {}_nC_{k-1}$ image blocks in Construction 1 and $N = {}_nC_k$ image blocks in Construction 2 satisfies disjoint property and union property.
P_j	Divide a secret image into N image blocks P_j, $1 \le j \le N$, where $D(P) = \{P_1, P_2, \dots, P_N\}$.
O_j	Divide a cover image into N subcover images O_j, $1 \le j \le N$, where $D(O) = \{O_1, O_2, \dots, O_N\}$.
$\text{PVCS}_{k,k}(\cdot)$	Encoding function of (k, k)-PVCS.
$\text{PEVCS}_{k,k}(\cdot,\cdot)$	Encoding function of (k, k)-PEVCS.
$S_{j,1}, \dots, S_{j,k}$	k sub-shadows of an image block P_j by using $\text{PVCS}_{k,k}(\cdot)$ or $\text{PEVCS}_{k,k}(\cdot,\cdot)$.
$B_{n,k-1}$	$n \times {}_nC_{k-1}$ binary matrix $B_{n,k-1} = [b_{ij}]$ used in Construction 1, where $b_{ij} \in [0, 1]$, $1 \le i \le n$ and $1 \le j \le {}_nC_{k-1}$, and every column vector has Hamming weight $(k-1)$.
$B'_{n,k}$	$n \times {}_nC_k$ binary matrix $B'_{n,k} = [b_{ij}]$ used in Construction 2, where $b_{ij} \in [0, 1]$, $1 \le i \le n$ and $1 \le j \le {}_nC_k$, and every column vector has Hamming weight k.
S_i	n shadows, $1 \le i \le n$, in the proposed (k, n)-BPVCS

Construction 1. Encoding of the proposed (k, n)-BPVCS.
Input: a secret image P.
Output: n shadows S_i, $i \in [1, n]$.
(Step 1-1) Obtain image blocks $P_j, j \in [1, N]$, by $D(P)$, where $N = {}_nC_{k-1}$.
(Step 1-2) Obtain subcover images $O_j, j \in [1, N]$, where $N = {}_nC_{k-1}$.
/* (Step 1-2) is only required for the proposed (k, n)-BPVCS with meaningful shadows */
(Step 2-1) For every image block P_j, create k sub-shadows $(S_{j,1}, \dots, S_{j,k})$ by $\text{PVCS}_{k,k}(P_j)$.
(Step 2-2) For every image block P_j and sub cover image O_j, create k sub-shadows $(S_{j,1}, \dots, S_{j,k})$ by $\text{PEVCS}_{k,k}(P_j, O_j)$.
/* (Step 2-2) is only required for the proposed (k, n)-BPVCS with meaningful shadows */
(Step 3) Set $S_1 = S_2 = \cdots S_n = \phi$.
(Step 4) Choose a matrix $B_{n,k-1} = [b_{ij}]$.
(Step 5) **for** $j = 1$ to N **do**
{Set $x = 2$;
for $i = 1$ to n do{If $b_{ij} = 1$ then $\hat{S}_{i,j} = S_{j,x}$ and $x = x + 1$; else $\hat{S}_{i,j} = S_{j,1}$;}
};
(Step 6) $S_i = \cup_{j=1}^{N} \hat{S}_{i,j}, i \in [1, n]$.
/* each participant puts up received $\hat{S}_{i,j}$ according to the position of P_j to construct S_i */

1. Construction 1: (k, n)-BPVCS Using ${}_nC_{k-1}$ Image Blocks

The encoding procedure of the proposed (k, n)-BPVCS with noise-like and meaningful shadows by ${}_nC_{k-1}$ image is shown below. (Step 1-1) and (Step 2-1) (respectively, (Step 1-2) and (Step 2-2)) are used for noise-like (respectively, meaningful) shadows.

Theorem 1. The scheme from Construction 1 is a (k, n)-BPVCS having both the progressive recovery and threshold property.

Proof. We first prove the security condition (that is, the threshold property), in which t $(t \le k-1)$ shadows cannot recover any image block. Any t $(t \le k-1)$ rows in $B_{n,k-1}$ do not have $(k-1)$ 1s and at least one 0 in a column; so, there are not enough k sub-shadows in a (k, k)-PVCS (or (k, k)-PEVCS) to reconstruct any image block. With regards to progressive recovery, every column vector has $(k-1)$ 1s and $(n-k+1)$ 0s. So, any t $(t \ge k)$ rows in $B_{n,k-1}$ have ${}_tC_{k-1}$ t-tuples with $(k-1)$ 1s and $(t-k+1)$ 0s, and have enough k sub-shadows for

reconstructing ${}_tC_{k-1}$ image blocks. For $k = 2$, the number of image blocks is $N = {}_nC_{k-1} = {}_nC_1 = n$. Shadows obtained from Construction 1 are exactly the same as those in (3), and Construction 1 will be reduced to Hou and others' (2, n)-BPVCS. The following example shows a (3, 4)-BPVCS where $k > 2$ by using Construction 1. ■

Example 5. Generate four shadows of the proposed (3, 4)-BPVCS by Construction 1.

A secret image P is first partitioned into $6 = {}_4C_2$ image blocks, $P_1, P_2, \ldots, P_6$. Each image block is divided into three sub-shadows by (3, 3)-PVCS (or (3, 3)-PEVCS). The matrices $B_{n,k-1} = B_{4,2}$ and $[\hat{S}_{i,j}]$ of a (3, 4)-BPVCS are given as follows:

$$B_{4,2} = \begin{bmatrix} b_{11} & b_{12} & b_{13} & b_{14} & b_{15} & b_{16} \\ b_{21} & b_{22} & b_{23} & b_{24} & b_{25} & b_{26} \\ b_{31} & b_{32} & b_{33} & b_{34} & b_{35} & b_{36} \\ b_{41} & b_{42} & b_{43} & b_{54} & b_{45} & b_{46} \end{bmatrix} = \begin{bmatrix} 1\,1\,1\,0\,0\,0 \\ 1\,0\,0\,1\,1\,0 \\ 0\,1\,0\,1\,0\,1 \\ 0\,0\,1\,0\,1\,1 \end{bmatrix}. \quad (8)$$

$$[\hat{S}_{i,j}] = \begin{bmatrix} \hat{S}_{1,1} & \hat{S}_{1,2} & \hat{S}_{1,3} & \hat{S}_{1,4} & \hat{S}_{1,5} & \hat{S}_{1,6} \\ \hat{S}_{2,1} & \hat{S}_{2,2} & \hat{S}_{2,3} & \hat{S}_{2,4} & \hat{S}_{2,5} & \hat{S}_{2,6} \\ \hat{S}_{3,1} & \hat{S}_{3,2} & \hat{S}_{3,3} & \hat{S}_{3,4} & \hat{S}_{3,5} & \hat{S}_{3,6} \\ \hat{S}_{4,1} & \hat{S}_{4,2} & \hat{S}_{4,3} & \hat{S}_{4,4} & \hat{S}_{4,5} & \hat{S}_{4,6} \end{bmatrix} = \begin{bmatrix} S_{1,2} & S_{2,2} & S_{3,2} & S_{4,1} & S_{5,1} & S_{6,1} \\ S_{1,3} & S_{2,1} & S_{3,1} & S_{4,2} & S_{5,2} & S_{6,1} \\ S_{1,1} & S_{2,3} & S_{3,1} & S_{4,3} & S_{5,1} & S_{6,2} \\ S_{1,1} & S_{2,1} & S_{3,3} & S_{4,1} & S_{5,3} & S_{6,3} \end{bmatrix}. \quad (9)$$

Four shadows, S_1, S_2, S_3, and S_4, are then generated by $S_i = \bigcup_{j=1}^{6} \hat{S}_{i,j}$, $i \in [1, 4]$.

$$\begin{cases} S_1 = \hat{S}_{1,1} \cup \hat{S}_{1,2} \cup \hat{S}_{1,3} \cup \hat{S}_{1,4} \cup \hat{S}_{1,5} \cup \hat{S}_{1,6} = S_{1,2} \cup S_{2,2} \cup S_{3,2} \cup S_{4,1} \cup S_{5,1} \cup S_{6,1}, \\ S_2 = \hat{S}_{2,1} \cup \hat{S}_{2,2} \cup \hat{S}_{2,3} \cup \hat{S}_{2,4} \cup \hat{S}_{2,5} \cup \hat{S}_{2,6} = S_{1,3} \cup S_{2,1} \cup S_{3,1} \cup S_{4,2} \cup S_{5,2} \cup S_{6,1}, \\ S_3 = \hat{S}_{3,1} \cup \hat{S}_{3,2} \cup \hat{S}_{3,3} \cup \hat{S}_{3,4} \cup \hat{S}_{3,5} \cup \hat{S}_{3,6} = S_{1,1} \cup S_{2,3} \cup S_{3,1} \cup S_{4,3} \cup S_{5,1} \cup S_{6,2}, \\ S_4 = \hat{S}_{4,1} \cup \hat{S}_{4,2} \cup \hat{S}_{4,3} \cup \hat{S}_{4,4} \cup \hat{S}_{4,5} \cup \hat{S}_{4,6} = S_{1,1} \cup S_{2,1} \cup S_{3,3} \cup S_{4,1} \cup S_{5,3} \cup S_{6,3}. \end{cases} \quad (10)$$

$$\begin{cases} S_1 + S_2 \\ = (S_{1,2} \cup S_{2,2} \cup S_{3,2} \cup S_{4,1} \cup S_{5,1} \cup S_{6,1}) + (S_{1,3} \cup S_{2,1} \cup S_{3,1} \cup S_{4,2} \cup S_{5,2} \cup S_{6,1}) \\ = \overbrace{(S_{1,2} + S_{1,3}) \cup (S_{2,2} + S_{2,1}) \cup (S_{3,2} + S_{3,1}) \cup (S_{4,1} + S_{4,2}) \cup (S_{5,1} + S_{5,2}) \cup (S_{6,1})}^{6 \text{ noise-like blocks}}. \end{cases} \quad (11)$$

$$\begin{cases} S_1 + S_3 + S_4 = (S_{1,2} \cup S_{2,2} \cup S_{3,2} \cup S_{4,1} \cup S_{5,1} \cup S_{6,1}) \\ + (S_{1,1} \cup S_{2,3} \cup S_{3,1} \cup S_{4,3} \cup S_{5,1} \cup S_{6,2}) + (S_{1,1} \cup S_{2,1} \cup S_{3,3} \cup S_{4,1} \cup S_{5,3} \cup S_{6,3}) \\ = (S_{1,2} + S_{1,1}) \cup (S_{2,2} + S_{2,3} + S_{2,1}) \\ \cup (S_{3,2} + S_{3,1} + S_{3,3}) \cup (S_{4,1} + S_{4,3}) \cup (S_{5,1} + S_{5,3}) \cup (S_{6,1} + S_{6,2} + S_{6,3}) \\ = \overbrace{P_2 \cup P_3 \cup P_6}^{3 \text{ image blocks}} \cup \overbrace{(S_{1,2} + S_{1,1}) \cup (S_{4,1} + S_{4,3}) \cup (S_{5,1} + S_{5,3})}^{3 \text{ noise-like blocks}}. \end{cases} \quad (12)$$

Figures 3(a) and 3(b) are partitions of the secret image and cover image. Figure 3(c) shows the composition of shadows for the proposed (3, 4)-BPVCS by Construction 1.

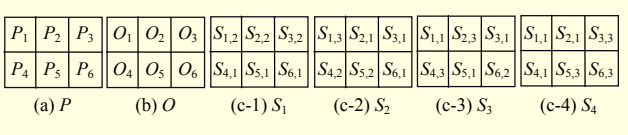

Fig. 3. Composition of shadows for proposed (3, 4)-BPVCS: (a) six image blocks, (b) six sub-cover images, and (c) four shadows.

$$\begin{cases} S_1 + S_2 + S_3 + S_4 = (S_{1,2} \cup S_{2,2} \cup S_{3,2} \cup S_{4,1} \cup S_{5,1} \cup S_{6,1}) \\ + (S_{1,3} \cup S_{2,1} \cup S_{3,1} \cup S_{4,2} \cup S_{5,2} \cup S_{6,1}) + (S_{1,1} \cup S_{2,3} \cup S_{3,1} \cup S_{4,3} \cup S_{5,1} \cup S_{6,2}) \\ + (S_{1,1} \cup S_{2,1} \cup S_{3,3} \cup S_{4,1} \cup S_{5,3} \cup S_{6,3}) \\ = (S_{1,2} + S_{1,3} + S_{1,1} + S_{1,1}) \cup (S_{2,2} + S_{2,1} + S_{2,3} + S_{2,1}) \cup (S_{3,2} + S_{3,1} + S_{3,1} + S_{3,3}) \\ \cup (S_{4,1} + S_{4,2} + S_{4,3} + S_{4,1}) \cup (S_{5,1} + S_{5,2} + S_{5,1} + S_{5,3}) \cup (S_{6,1} + S_{6,1} + S_{6,2} + S_{6,3}) \\ = \overbrace{P_1 \cup P_2 \cup P_3 \cup P_4 \cup P_5 \cup P_6}^{6 \text{ image blocks}}. \end{cases} \quad (13)$$

Let us consider a reconstruction. It can be easily verified that any two shadows do not have enough sub-shadows for reconstructing an image block. For example, when stacking S_1 and S_2, we have six noise-like image blocks (see (11)). As shown in (12), by stacking S_1, S_3, and S_4, we can recover three image blocks, P_2, P_3, and P_6, and three noise-like blocks. All four stacked shadows can recover all image blocks (see (13)).

2. Construction 2: (k, n)-BPVCS Using ${}_nC_k$ Image Blocks

The design concept of Construction 2 is described as follows. We use a matrix having ${}_nC_k$ columns with k 1s in every column. Meantime, we generate k shadows from (k, k)-PVCS. For every single column, we assign these k shadows to k 1s, and generate one random shadow for "0." Therefore, when stacking t shadows, some corresponding image blocks can be revealed. The formal construction is shown in Construction 2.

The encoding procedure of Construction 2 is similar to Construction 1, except using $N = {}_nC_k$ instead of $N = {}_nC_{k-1}$, and $B'_{n,k}$ instead of $B_{n,k-1}$. Also, (Step 5) in Construction 1 is modified as (Step 5′) in Construction 2 (see Fig. 4).

Random sub-shadows $S_{j,0}$ in Construction 2, $1 \le j \le N$, are randomly generated in the (k, n)-BPVCS with noise-like shadows. For the (k, n)-BPVCS with meaningful shadows, meaningful sub-shadows $S_{j,0}$ $1 \le j \le N$, are generated according to P_j and O_j, where the subpixels for black and white pixels are the same as those in (k, k)-PEVCS. For the case $k = 3$ in the proposed (k, n)-BPVCS, we need (3, 3)-PVCS and (3, 3)-PEVCS. Suppose that we use Naor and Shamir's (3, 3)-PVCS [2] and Liu and others' (3, 3)-PEVCS [12] to implement our (3, 4)-BPVCS with noise-like and meaningful shadows, respectively. Since Naor and Shamir's (3, 3)-PVCS uses shadows that contain an equal number of black and white

ETRI Journal, Volume 37, Number 5, October 2015
http://dx.doi.org/10.4218/etrij.15.0114.0327

(Step 5′) for $j = 1$ to N do

{Set $x = 1$;

for $i = 1$ to n do {

if $b_{ij} = 1$ then $\hat{S}_{i,j} = S_{j,x}$ and $x = x + 1$;

else $\hat{S}_{i,j} = S_{j,0}$ };

}

Fig. 4. Modified (Step 5′) in Construction 2.

pixels, $S_{j,0}$ in the (3, n)-BPVCS with noise-like shadows is randomly generated. On the other hand, Liu and others' (3, 3)-PEVCS adopts probabilities 5/9 and 4/9 of blackness to represent black and white secret pixels. Therefore, the black and white pixels of $S_{j,0}$ for (3, n)-BPVCS with meaningful shadows are generated according to the above probabilities; so, we can visually view the cover image on shadow. However, the sub-shadow $S_{j,0}$ is not related to other sub-shadows, $S_{j,1}$, $S_{j,2}$, … , $S_{j,k}$; thus, it does not have any contribution for reconstruction.

Theorem 2. The scheme from Construction 2 is a (k, n)-BPVCS having both the progressive recovery and threshold property.

Proof. We put k sub-shadows of P_j at the element of "1" in the jth column. Since t ($t \le k - 1$) rows in $B'_{n,k}$ do not have k 1s, there are not enough k sub-shadows in a (k, k)-PVCS (or (k, k)-PEVCS) to reconstruct any image block. For the progressive recovery, we only consider the sub-shadows in position "1" because the sub-shadow $S_{j,0}$ in position "0" has no contribution for reconstruction. Every column vector has k 1s and ($n - k$) 0s. So, any t ($t \ge k$) rows in $B'_{n,k}$ have ${}_tC_k$ t-tuples with k 1s, and have enough sub-shadows for reconstructing ${}_tC_k$ image blocks. ■

Example 6. Generate four shadows of the proposed (3, 4)-BPVCS by Construction 2.

A secret image P is first partitioned into $4 = {}_4C_3$ image blocs, P_1, P_2, P_3, and P_4. Each image block is shared into three sub-shadows by (3, 3)-PVCS (or (3, 3)-PEVCS). Also, we generate four random and meaningful sub-shadows, $S_{1,0}$, $S_{2,0}$, $S_{3,0}$, and $S_{4,0}$, for the (3, 4)-BPVCS with noise-like and meaningful shadows, respectively. The matrices $B'_{n,k} = B'_{4,3}$ and $[\hat{S}_{i,j}]$ of a (3, 4)-BPVCS are shown as follows:

$$B'_{4,3} = \begin{bmatrix} b_{11} & b_{12} & b_{13} & b_{14} \\ b_{21} & b_{22} & b_{23} & b_{24} \\ b_{31} & b_{32} & b_{33} & b_{34} \\ b_{41} & b_{42} & b_{43} & b_{54} \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix}, \tag{14}$$

$$[\hat{S}_{i,j}] = \begin{bmatrix} \hat{S}_{1,1} & \hat{S}_{1,2} & \hat{S}_{1,3} & \hat{S}_{1,4} \\ \hat{S}_{2,1} & \hat{S}_{2,2} & \hat{S}_{2,3} & \hat{S}_{2,4} \\ \hat{S}_{3,1} & \hat{S}_{3,2} & \hat{S}_{3,3} & \hat{S}_{3,4} \\ \hat{S}_{4,1} & \hat{S}_{4,2} & \hat{S}_{4,3} & \hat{S}_{4,4} \end{bmatrix} = \begin{bmatrix} S_{1,1} & S_{2,1} & S_{3,1} & S_{4,0} \\ S_{1,2} & S_{2,2} & S_{3,0} & S_{4,1} \\ S_{1,3} & S_{2,0} & S_{3,2} & S_{4,2} \\ S_{1,0} & S_{2,3} & S_{3,3} & S_{4,3} \end{bmatrix}. \tag{15}$$

Four shadows, S_1, S_2, S_3, S_4, are then generated by

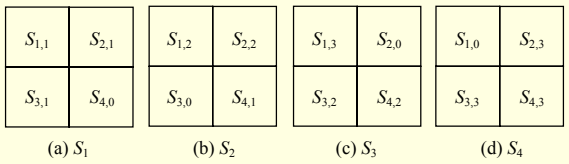

Fig. 5. Composition of shadows for proposed (3, 4)-BPVCS.

$$S_i = \bigcup_{j=1}^{4} \hat{S}_{i,j},\ i \in [1,\ 4].$$

$$\begin{cases} S_1 = \hat{S}_{1,1} \cup \hat{S}_{1,2} \cup \hat{S}_{1,3} \cup \hat{S}_{1,4} = S_{1,1} \cup S_{2,1} \cup S_{3,1} \cup S_{4,0}, \\ S_2 = \hat{S}_{2,1} \cup \hat{S}_{2,2} \cup \hat{S}_{2,3} \cup \hat{S}_{2,4} = S_{1,2} \cup S_{2,2} \cup S_{3,0} \cup S_{4,1}, \\ S_3 = \hat{S}_{3,1} \cup \hat{S}_{3,2} \cup \hat{S}_{3,3} \cup \hat{S}_{3,4} = S_{1,3} \cup S_{2,0} \cup S_{3,2} \cup S_{4,2}, \\ S_4 = \hat{S}_{4,1} \cup \hat{S}_{4,2} \cup \hat{S}_{4,3} \cup \hat{S}_{4,4} = S_{1,0} \cup S_{2,3} \cup S_{3,3} \cup S_{4,3}. \end{cases} \tag{16}$$

By using partitions of both the secret and cover images in Figs. 3(a) and 3(b), the composition of shadows for the proposed (3, 4)-BPVCS by Construction 2 is shown in Fig. 5.

Let us consider a reconstruction. When stacking two shadows, S_1 and S_2, we have four noise-like image blocks (see (17)). As shown in (18), when stacking S_1, S_3, and S_4, we will have one image block, P_3, and three noise-like blocks since $S_{1,0}$, $S_{2,0}$, and $S_{4,0}$ are unrelated in the reconstruction; thus, we have nothing when stacking ($S_{1,1} + S_{1,3} + S_{1,0}$), ($S_{2,1} + S_{2,0} + S_{2,3}$), ($S_{3,1} + S_{3,2} + S_{3,3}$), and ($S_{4,0} + S_{4,2} + S_{4,3}$).

$$\begin{cases} S_1 + S_2 = (S_{1,1} \cup S_{2,1} \cup S_{3,1} \cup S_{4,0}) + (S_{1,2} \cup S_{2,2} \cup S_{3,0} \cup S_{4,1}) \\ = \overbrace{(S_{1,1} + S_{1,2}) \cup (S_{2,1} + S_{2,2}) \cup (S_{3,1} + S_{3,0}) \cup (S_{4,0} + S_{4,1})}^{\text{4 noise-like blocks}} \end{cases}, \tag{17}$$

$$\begin{cases} S_1 + S_3 + S_4 = (S_{1,1} \cup S_{2,1} \cup S_{3,1} \cup S_{4,0}) + (S_{1,3} \cup S_{2,0} \cup S_{3,2} \cup S_{4,2}) \\ \qquad + (S_{1,0} \cup S_{2,3} \cup S_{3,3} \cup S_{4,3}) \\ = (S_{1,1} + S_{1,3} + S_{1,0}) \cup (S_{2,1} + S_{2,0} + S_{2,3}) \cup (S_{3,1} + S_{3,2} + S_{3,3}) \\ \cup (S_{4,0} + S_{4,2} + S_{4,3}) \\ = \overbrace{P_3}^{\text{1 image block}} \cup \overbrace{(S_{1,1} + S_{1,3} + S_{1,0}) \cup (S_{2,1} + S_{2,0} + S_{2,3}) \cup (S_{4,0} + S_{4,2} + S_{4,3})}^{\text{3 noise-like blocks}}. \end{cases} \tag{18}$$

Obviously, we can recover all image blocks when stacking all shadows (see (19)).

$$\begin{cases} S_1 + S_2 + S_3 + S_4 = (S_{1,1} \cup S_{2,1} \cup S_{3,1} \cup S_{4,0}) + (S_{1,2} \cup S_{2,2} \cup S_{3,0} \cup S_{4,1}) \\ + (S_{1,3} \cup S_{2,0} \cup S_{3,2} \cup S_{4,2}) + (S_{1,0} \cup S_{2,3} \cup S_{3,3} \cup S_{4,3}) \\ = (S_{1,1} + S_{1,2} + S_{1,3} + S_{1,0}) \cup (S_{2,1} + S_{2,2} + S_{2,0} + S_{2,3}) \\ \cup (S_{3,1} + S_{3,0} + S_{3,2} + S_{3,3}) \cup (S_{4,0} + S_{4,1} + S_{4,2} + S_{4,3}) \\ = \overbrace{P_1 \cup P_2 \cup P_3 \cup P_4}^{\text{4 image blocks}}. \end{cases} \tag{19}$$

3. Image Blocks in (k, n)-BPVCS

With regards to the recovered image blocks, in Hou and others' (2, n)-BPVCS, each participant has his own decryption key for one particular image block; for example, t participants (say $p_1, p_2, \ldots, p_t$) can stack their shadows to recover the image blocks ($P_1, P_2, \ldots, P_t$). So, every participant has his own image block. We have n participants; thus, there are n image blocks. In Construction 1, there are ${}_nC_{k-1}$ image blocks. There are ${}_4C_2 = 6$ image blocks for our (3, 4)-BPVCS. Here, we rename these six image blocks $P_1, P_2, \ldots, P_6$, as $P_{1,2}$, $P_{1,3}$, $P_{1,4}$, $P_{2,3}$, $P_{2,4}$, and $P_{3,4}$, respectively. As shown in (20), for $P_{1,4}$ (see the third column), there are two 1s elements — one in the first row and the other in the fourth row.

$$B_{4,2} = \begin{array}{c} \\ p_1 \rightarrow \\ p_2 \rightarrow \\ p_3 \rightarrow \\ p_4 \rightarrow \end{array} \begin{bmatrix} \overset{\frown}{P_{1,2}} & \overset{\frown}{P_{1,3}} & \overset{\frown}{P_{1,4}} & \overset{\frown}{P_{2,3}} & \overset{\frown}{P_{2,4}} & \overset{\frown}{P_{3,4}} \\ 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}. \quad (20)$$

In Construction 1, we use the same sub-shadow $S_{j,1}$ for "0." Therefore, the shadows S_1 and S_4 for each of the "1" elements are necessary in reconstructing the image block $P_{1,4}$. This implies that the involved three participants need p_1 and p_4 to recover $P_{1,4}$. Therefore, p_1 and p_4 have their own decryption key for the particular image block $P_{1,4}$. In Construction 1, we have ${}_nC_{k-1}$ image blocks $P_{j_1, j_2, \ldots, j_{k-1}}$, where $j_i \in \{1, 2, \ldots, n\}$ and $i = 1, 2, \ldots, k-1$. When t participants (say $p_1, p_2, \ldots, p_t$) are involved in reconstruction, then ${}_tC_{k-1}$ image blocks, $P_{j_1, j_2, \ldots, j_{k-1}}$, where $j_i \in \{1, 2, \ldots, t\}$ and $i = 1, 2, \ldots, k-1$, associated with these t participants can be recovered. For example, in a (3, 4)-BPVCS by Construction 1, S_1, S_3, and S_4 can be stacked to recover $P_{1,3}$, $P_{1,4}$, and $P_{3,4}$. On the other hand, in a (3, 4)-BPVCS by Construction 2, there are ${}_4C_3 = 4$ image blocks. Here, we rename the four image bocks, P_1, P_2, P_3, and P_4, as $P_{1,2,3}$, $P_{1,2,4}$, $P_{1,3,4}$, and $P_{2,3,4}$, respectively.

Let us consider the first column in (21), we use sub-shadows $S_{1,1}$, $S_{1,2}$, and $S_{1,3}$ for the element "1"; thus, the participants p_1, p_2, and p_3 are necessary in reconstructing the image block $P_{1,2,3}$. Thus, we can say they have their own decryption key for the particular image block $P_{1,2,3}$.

From the above description, t participants in both constructions have their own decryption keys for ${}_tC_{k-1}$ (Construction 1) or ${}_tC_k$ (Construction 2) particular image blocks. The proposed (k, n)-BPVCS has a similar progressive recovery to that of Hou and others' (2, n)-BPVCS. In fact, Construction 1 is reduced to Hou and others' (2, n)-BPVCS for $k = 2$.

$$B'_{4,3} = \begin{array}{c} \\ p_1 \rightarrow \\ p_2 \rightarrow \\ p_3 \rightarrow \\ p_4 \rightarrow \end{array} \begin{bmatrix} \overset{\frown}{P_{1,2,3}} & \overset{\frown}{P_{1,2,4}} & \overset{\frown}{P_{1,3,4}} & \overset{\frown}{P_{2,3,4}} \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix}. \quad (21)$$

IV. Experiment and Discussion

1. Experimental Results

There are two types of Hou and others' (2, n)-BPVCS — one containing noise-like shadows and one containing meaningful shadows. Construction 1 and Construction 2 can also be implemented with noise-like and meaningful shadows. The difference is that one uses (k, k)-PVCS and the other uses (k, k)-PEVCS with the same cover image. Here, we conduct two experiments to evaluate the performance of the proposed (k, n)-BPVCS with noise-like shadows by Construction 1 and Construction 2.

Experiment A. Construct the proposed (3, 4)-BPVCS with noise-like shadows by Construction 1.

Here, we use (3, 3)-PVCS with $C_1 = \left\{ \begin{bmatrix}1\\0\\0\end{bmatrix}, \begin{bmatrix}0\\1\\0\end{bmatrix}, \begin{bmatrix}0\\0\\1\end{bmatrix}, \begin{bmatrix}1\\1\\1\end{bmatrix} \right\}$ and $C_0 = \left\{ \begin{bmatrix}0\\0\\0\end{bmatrix}, \begin{bmatrix}0\\1\\1\end{bmatrix}, \begin{bmatrix}1\\0\\1\end{bmatrix}, \begin{bmatrix}1\\1\\0\end{bmatrix} \right\}$. Suppose that the secret image is $P = \boxed{\begin{matrix}\text{A B C}\\ \text{D E F}\end{matrix}}$, and that this is divided into six image blocks $P_1 = \boxed{\text{A}}$, $P_2 = \boxed{\text{B}}$, $P_3 = \boxed{\text{C}}$, $P_4 = \boxed{\text{D}}$, $P_5 = \boxed{\text{E}}$, and $P_6 = \boxed{\text{F}}$.

Figure 6 reveals four noise-like shadows and the results of stacking two, three, and four shadows. Obviously, we have six noise-like image blocks, and we do not have any secret

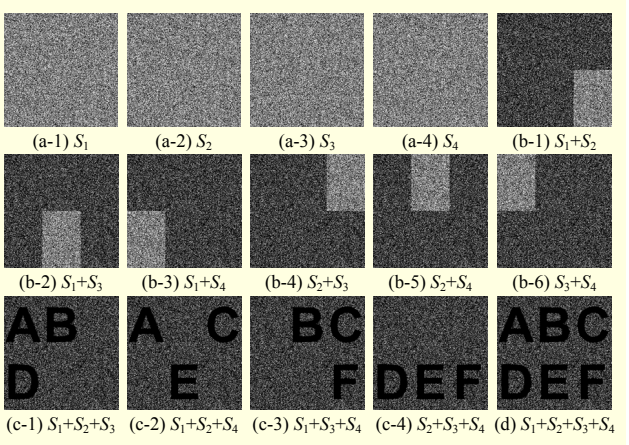

Fig. 6. Progressive recovery of (3, 4)-BPVCS with noise-like shadows by Construction 1: (a) four shadows, (b) stacking any two shadows, (c) stacking any three shadows, and (d) stacking all four shadows.

information for stacking any two shadows. However, in Fig. 6(b), it is observed that there is one noise-like image block lighter than the other five noise-like image blocks when stacking two shadows. When stacking S_1 and S_2, the area of P_6 only has one sub-shadow, $S_{6,1}$ (see (11)); however, the other five areas have two stacked sub-shadows. Therefore, the area of P_6 is lighter than the other areas. When stacking any three shadows, we can recover ${}_3C_2 = 3$ image blocks. For example, when stacking S_1, S_3, and S_4 (see (12)), we will have three image blocks, P_2, P_3, and P_6, and three noise-like blocks. The stacked result of $(S_1 + S_3 + S_4)$ with the contrast $\bar{\alpha} = 1/4$ is illustrated in Fig. 6(c-3). As shown in Fig. 6(d), the complete secret $\boxed{\begin{matrix}A\,B\,C\\D\,E\,F\end{matrix}}$ is recovered for stacking all four shadows, and the contrast is still 1/4.

Experiment B. Construct the proposed (3, 4)-BPVCS with noise-like shadows by Construction 2.

We use the (3, 3)-PVCS in Experiment A. Construction 2 only needs four image blocks. Suppose that the secret image is $P = \mathrm{M}\boxed{\begin{matrix}A\,B\\C\,D\end{matrix}}$, and that this is divided into four image blocks $P_1 = \boxed{A}$, $P_2 = \boxed{B}$, $P_3 = \boxed{C}$, and $P_4 = \boxed{D}$.

Figure 7 reveals four noise-like shadows and the stacked results of stacking two, three, and four shadows. Any two stacked shadows have two stacked sub-shadows in each image-block area; thus, we have nothing. When stacking any three shadows, we can recover ${}_3C_3 = 1$ image block. For example, when stacking S_1, S_3, and S_4 (see (18)), we have one image block, P_3, and three noise-like blocks. The stacked result of $(S_1 + S_3 + S_4)$ is illustrated in Fig. 7(c-3). The contrast for this image block is $\bar{\alpha} = (1-0)/4 = 1/4$. The complete secret $\boxed{\begin{matrix}A\,B\\C\,D\end{matrix}}$ is recovered for four stacked shadows (see Fig. 7(d)), and the contrast is reduced to 1/8 due to stacking an extra random sub-shadow, $S_{j,0}$.

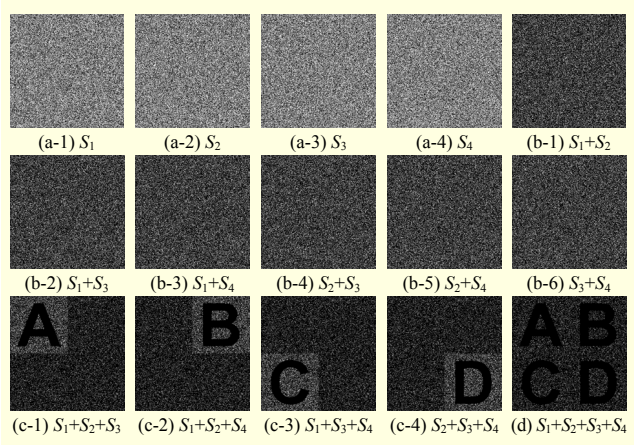

Fig. 7. Progressive recovery of (3, 4)-BPVCS with noise-like shadows by Construction 2: (a) four shadows, (b) stacking any two shadows, (c) stacking any three shadows, and (d) stacking all four shadows.

2. Comparison and Discussion

Hou and others' scheme is a simple 2-out-of-n BPVCS. Both our constructions can be applied to any k and n. Hou and others' scheme uses n image blocks, but Construction 1 and Construction 2 use ${}_nC_{k-1}$ and ${}_nC_k$ image blocks, respectively.

Although the three schemes have different numbers of image blocks, any t ($\geq k$) participants in all these three schemes have their own decryption keys for the particular image blocks. In fact, ${}_nC_{k-1}$ image blocks in Construction 1 is reduced to ${}_nC_{2-1} = n$ in Hou and others' (2, n)-BPVCS. When stacking k shadows, all three schemes have the same contrast to that of (k, k)-PVCS (note: k is 2 in Hou and others' scheme).

When stacking $(k + 1)$ or more shadows, the contrasts of Hou and others' scheme and Construction 1 are invariant. However, the contrast of Construction 2 is compromised due to an extra sub-shadow, $S_{j,0}$. Next, we discuss the following issues of the proposed (k, n)-BPVCS in detail: (a) non-uniform stacked results, (b) reconstruction of image blocks, (c) progressive recovery ratio, and (d) requirement of $S_{j,0}$ in Construction 2.

A. Non-uniform Stacked Results

Form our experimental results, it is observed that Construction 1 has the non-uniform stacked results when stacking t shadows, where $2 \leq t \leq k-1$. Since Construction 1 is based on the matrix $B_{n,k-1}$, where every column has $(k-1)$ 1s, the stacked result has ${}_tC_r \times {}_{n-t}C_{k-1-t+r}$ t-tuples with r 0s. We use the same sub-shadow $S_{j,1}$ at the element "0" in the jth column; thus, the color in the stacked result is lighter if this image block has r 0s, where $r \geq 2$. A (3, 4)-BPVCS by Construction 1 has ${}_2C_0 \times {}_{4-2}C_{3-1-2+0} = 1$ 2-tuples with zero 0s, ${}_2C_1 \times {}_{4-2}C_{3-1-2+1} = 4$ 2-tuples with one 0, and ${}_2C_2 \times {}_{4-2}C_{3-1-2+2} = 1$ with two 0s, respectively. As shown in Fig. 6(b), there are five darker image blocks ($r = 0$ and 1) and one lighter image block ($r = 2$) when stacking $t = 2$ shadows. Construction 2 also has a similar characteristic, because we use the same sub-shadow $S_{j,0}$ at the element "0" in the jth column. Since every column of $B'_{n,k}$ has k 1s, so the stacked result has ${}_tC_r \times {}_{n-t}C_{k-t+r}$ t-tuples with r 0s. Therefore, when stacking two shadows, a (3, 4)-BPVCS by Construction 2 has ${}_2C_0 \times {}_{4-2}C_{3-2+0} = 2$ 2-tuples with zero 0s and ${}_2C_1 \times {}_{4-2}C_{3-2+1} = 2$ 2-tuples with one 0, respectively. So, there are four darker image blocks ($r = 0$ and 1) but no lighter image block (see Fig. 7(b)). Our scheme extends Hou and others' (2, n)-BPVCS to the BPVCS with $k > 2$ by using the same sub-shadow for each "0" element in matrices $B_{n,k-1}$ and $B'_{n,k}$. This

approach causes color darkening in some areas when stacking less than k shadows. Although our (k, n)-BPVCS may have non-uniform stacked results, it does not compromise the security.

B. Reconstruction of Image Blocks

In Construction 1, we have ${}_nC_{k-1}$ image blocks and n participants. Every participant has privilege to recover the particular ${}_{n-1}C_{k-2}$ image blocks when they are involved in reconstruction. On the other hand, Construction 2 has ${}_nC_k$ image blocks, and every participant has privilege to recover the particular ${}_{n-1}C_{k-1}$ image blocks. For Construction 1 with $k = 2$ (that is, Hou and others' (2, n)-BPVCS), the number of image blocks, ${}_nC_{2-1} = n$, happens to equal the number of participants. For this case, each participant p_i can be assigned for recovering ${}_{n-1}C_{2-2} = 1$ image block P_i, and it is easy to understand the statement [14] about Hou and others' (2, n)-BPVCS, "Each participant has his/her own decryption key for one particular image block." Suppose that four image blocks of (2, 4)-BPVCS using Construction 1 (that is, Hou and others' (2, 4)-BPVCS) are P_1, P_2, P_3, and P_4. Two participants, p_i and p_j, can recover two image blocks, P_i and P_j. In this reconstruction, the participant p_i is necessary for recovering the image block P_i. Each participant is required for their image block. For another (2, 4)-BPVCS by Construction 2, suppose that six image blocks are $P_{1,2}$, $P_{1,3}$, $P_{1,4}$, $P_{2,3}$, $P_{2,4}$, and $P_{3,4}$. When participant p_1 cooperates with another participant, p_2, p_3, or p_4, respectively, they can recover $P_{1,2}$, $P_{1,3}$, or $P_{1,4}$. So, every participant has privilege to recover ${}_{4-1}C_{2-1} = 3$ particular image blocks. Thus, each participant in Construction 2 also has his own decryption key for particular image blocks.

C. Progressive Recovery Ratio

Here, we define the progressive recovery ratio as the number of recovered image blocks over the number of whole image blocks when stacking t shadows, where $k \le t \le n$. The progressive recovery ratios of Hou and others' (2, n)-BPVCS, Construction 1, and Construction 2 are $R_H = t/n$, $R_1 = {}_tC_{k-1}/{}_nC_{k-1}$, and $R_2 = {}_tC_k/{}_nC_k$, respectively. It can be easily verified that the difference of R_H, R_1, and R_2 between stacking t and $(t-1)$ shadows is $R_H = 1/n$, $R_1 = [(k-1) \times {}_{t-1}C_{k-1}]/[(t+1-k) \times {}_nC_{k-1}]$, and $R_2 = [k \times {}_{t-1}C_k]/[(t-k) \times {}_nC_k]$. Hou and others' scheme $R_H = 1/n$ is fixed, so its progressive recovery ratio is linear and smooth. For the case $k << n$, the variation of ${}_{t-1}C_k$ is greater than ${}_{t-1}C_{k-1}$, so R_1 is more uniform than R_2. Figure 8 reveals the progressive recovery ratios for (2, 30)-BPVCS and (3, 30)-BPVCS.

D. Requirement of $S_{j,0}$ in Construction 2

In Construction 2, we use a random $S_{j,0}$ for each element "0" in $B'_{n,k}$. This sub-shadow is completely unrelated to other sub-shadows. It has no contribution for recovering the secret but only degrades the contrast. However, it has k 1s in every column in $B'_{n,k}$, where we use k sub-shadows from (k, k)-PVCS (or (k, k)-PEVCS). Actually, we do not need a sub-shadow for the "0" elements. Consider (3, 4)-BPVCS by Construction 2. If we do not use a random sub-shadow, $S_{1,0}$, $S_{2,0}$, $S_{3,0}$ and $S_{4,0}$, then (15) will be modified as (22).

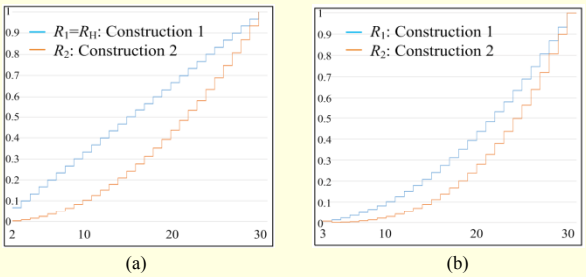

Fig. 8. Progressive recovery ratios, $k \le t \le n$, of proposed (k, n)-BPVCS by Construction 1 and Construction 2: (a) (2, 30)-BPVCS and (b) (3, 30)-BPVCS.

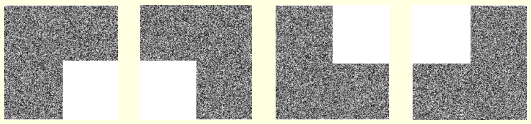

Fig. 9. Four shadows of (3, 4)-BPVCS by Construction 2 with noise-like shadows.

$$\left[\hat{S}_{i,j}\right] = \begin{bmatrix} \hat{S}_{1,1} & \hat{S}_{1,2} & \hat{S}_{1,3} & \hat{S}_{1,4} \\ \hat{S}_{2,1} & \hat{S}_{2,2} & \hat{S}_{2,3} & \hat{S}_{2,4} \\ \hat{S}_{3,1} & \hat{S}_{3,2} & \hat{S}_{3,3} & \hat{S}_{3,4} \\ \hat{S}_{4,1} & \hat{S}_{4,2} & \hat{S}_{4,3} & \hat{S}_{4,4} \end{bmatrix} = \begin{bmatrix} S_{1,1} & S_{2,1} & S_{3,1} & \phi \\ S_{1,2} & S_{2,2} & \phi & S_{4,1} \\ S_{1,3} & \phi & S_{3,2} & S_{4,2} \\ \phi & S_{2,3} & S_{3,3} & S_{4,3} \end{bmatrix}. \tag{22}$$

Four shadows, S_1, S_2, S_3, and S_4, are then generated in (23), and each shadow only has three sub-shadows. For example, $S_1 = S_{1,1} \cup S_{2,1} \cup S_{3,1}$; there is no sub-shadow at the position of image block P_4.

$$\begin{cases} S_1 = \hat{S}_{1,1} \cup \hat{S}_{1,2} \cup \hat{S}_{1,3} \cup \hat{S}_{1,4} = S_{1,1} \cup S_{2,1} \cup S_{3,1}, \\ S_2 = \hat{S}_{2,1} \cup \hat{S}_{2,2} \cup \hat{S}_{2,3} \cup \hat{S}_{2,4} = S_{1,2} \cup S_{2,2} \cup S_{4,1}, \\ S_3 = \hat{S}_{3,1} \cup \hat{S}_{3,2} \cup \hat{S}_{3,3} \cup \hat{S}_{3,4} = S_{1,3} \cup S_{3,2} \cup S_{4,2}, \\ S_4 = \hat{S}_{4,1} \cup \hat{S}_{4,2} \cup \hat{S}_{4,3} \cup \hat{S}_{4,4} = S_{2,3} \cup S_{3,3} \cup S_{4,3}. \end{cases} \tag{23}$$

In Fig. 9, four shadows generated from (23) look so odd without using the sub-shadow $S_{j,0}$. This is why we use $S_{j,0}$ in Construction 2.

V. Conclusion

In this paper we provided two constructions for a general

(k, n)-BPVCS. Also, we theoretically proved that the proposed (k, n)-BPVCS satisfies the threshold property and progressive recovery. For the special case $k = 2$, Construction 1 is reduced to Hou and others' (2, n)-BPVCS. Both constructions using different image blocks have different progressive recovery ratios.

References

[1] S. Cimato and C.-N. Yang, "*Visual Cryptography and Secret Image Sharing*," New York, USA: CRC Press, Aug. 2011, pp. 5–16.

[2] M. Naor and A. Shamir, "Visual Cryptography," *Workshop Theory Appl. Cryptographic Techn.*, Perugia, Italy, May 9–12, 1994, pp. 1–12.

[3] R. Ito, H. Kuwakado, and H. Tanaka, "Image Size Invariant Visual Cryptography," *IEICE Trans. Fundam. Electron., Commun. Comput. Sci.*, vol. E82-A, Oct. 1999, pp. 2172–2177.

[4] C.-N. Yang, "New Visual Secret Sharing Schemes Using Probabilistic Method," *Pattern Recogn. Lett.*, vol. 25, no. 4, Mar. 2004, pp. 481–494.

[5] S. Cimato, R. de Prisco, and A. de Santis, "Probabilistic Visual Cryptography Schemes," *Comput. J.*, vol. 49, no. 1, Jan. 2006, pp. 97–107.

[6] D. Wang, F. Yi, and X. Li, "Probabilistic Visual Secret Sharing Schemes for Grey-Scale Images and Color Images," *Inf. Sci.*, vol. 181, no. 11, June 2011, pp. 2189–2208.

[7] Y.C. Hou et al., "Block-Based Progressive Visual Secret Sharing," *Inf. Sci.*, vol. 233, June 2013, pp. 290–304.

[8] E.R. Verheul and H.C.A. van Tilborg, "Constructions and Properties of k out of n Visual Secret Sharing Schemes," *Des., Codes Cryptography*, vol. 11, no. 2, May 1997, pp. 179–196.

[9] M. Bose and R. Mukerjee, "Optimal (k, n) Visual Cryptographic Schemes for General k," *Des., Codes, Cryptography*, vol. 55, no. 1, Apr. 2010, pp. 19–35.

[10] S.J. Shyu and M.C. Chen, "Optimum Pixel Expansions for Threshold Visual Secret Sharing Schemes," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, May 2011, pp. 960–969.

[11] G. Ateniese et al., "Extended Capabilities for Visual Cryptography," *Theoretical Comput. Sci.*, vol. 250, no. 1–2, Jan. 2001, pp. 143–161.

[12] F. Liu, C.K. Wu, and X.J. Lin, "Some Extensions on Threshold Visual Cryptography Schemes," *Comput. J.*, vol. 53, no. 1, Jan. 2010, pp. 107–119.

Ching Nung Yang received his BS and MS degrees in telecommunication engineering from National Chiao Tung University, Hsinchu, Taiwan. He received his PhD degree in electrical engineering from National Cheng Kung University, Tainan, Taiwan. Since 2009, he has been working as a professor with the Computer Science and Information Engineering Department, National Dong Hwa University, Hualien, Taiwan. He is also an IEEE senior member. He has published a number of journal and conference papers in the areas of information security, multimedia security, and coding theory. He is the guest editor of a special issue on "Visual Cryptography Schemes" for Communication of CCISA, and a coauthor of a series of articles on "Image Secret Sharing" for the Encyclopedia of Multimedia. He is the coeditor of two books, "Visual Cryptography and Secret Image Sharing" published by CRC Press/Taylor & Francis, and "Steganography and Watermarking" published by Nova Science Publishers, Inc. He serves as a technical reviewer for over 30 major scientific journals in the areas of his expertise, and serves on the editorial boards of selected journals. He is the recipient of the 2000, 2006, 2010, 2012, and 2014 Fine Advising Award in the Thesis of Master/PhD of Science awarded by the Institute of Information & Computer Machinery of Dong Wha University. His current research interests include coding theory, information security, and cryptography.

Chih Cheng Wu is a graduate student in computer science and information engineering at National Dong Hwa University, Hualien, Taiwan. His research interests are visual cryptography, secret image sharing, and digital signatures.

Yi-Chin Lin is a graduate student in computer science and information engineering at National Dong Hwa University, Hualien, Taiwan. His current research interests include visual cryptography and secret image sharing.

Cheonshik Kim received his PhD degree in computer engineering from Hankuk Univesity of Foreign Studies, Seoul, Rep. of Korea, in 2003. From March 2013, he worked for Digital System Engineering, Anyang University, Rep. of Korea. His researches were supported by NRF (2012–2015). He was a subject of biographical record in Marquis Who's Who in the World 2013–2015.