k Out of n Region Incrementing Scheme in Visual Cryptography

Ching-Nung Yang, *Senior Member, IEEE,* Hsiang-Wen Shih, Chih-Cheng Wu, and Lein Harn

***Abstract*—Recently, Wang introduced a novel (2, *n*) region incrementing visual cryptographic scheme (RIVCS), which can gradually reconstruct secrets in a single image with multiple security levels. In RIVCS, the secret image is subdivided into multiple regions in such a way that any *t* shadow images, where 2 ≤ *t* ≤ *n*, can be used to reveal the (*t* − 1)th region. However, Wang's scheme suffers from the incorrect-color problem, which the colors of reconstructed images may be reversed (i.e., the black and white are reversed). If the color of text is also the secret information, the incorrect-color problem will compromise the secret. Additionally, Wang's scheme is only suitable for the 2-out-of-*n* case, i.e., (*k*, *n*)-RIVCS where *k* = 2. In this paper, we propose a general (*k*, *n*)-RIVCS, where *k* and *n* are any integers, that is able to reveal correct colors of all regions. This paper has made three main contributions: 1) our scheme is a general (*k*, *n*)-RIVCS, where *k* and *n* can be any integers; 2) the incorrect-color problem is solved; and 3) our (*k*, *n*)-RIVCS is theoretically proven to satisfy the security and contrast conditions.**

***Index Terms*—Image secret sharing, secret sharing, visual cryptography, visual secret sharing.**

I. Introduction

The SECRET image sharing scheme (SISS) is an important and active research area. SISS divides a secret image into shadow images (referred to be shadows). If shadows are combined in a specific way, the secret information can be revealed. SISS is usually referred to be a threshold (k, n)-SISS, where $k \leq n$, that encrypts a secret image into n shadows in such way that for any k or more than k shadows can reconstruct the secret image; but for less than k shadows cannot recover the secret image.

There are two major types of SISS: one is the visual cryptographic scheme (VCS) [1]–[19], and the other is the polynomial-based SISS (PSISS) [20]–[29]. In VCS, each shadow can be made on a transparency. By stacking any k transparencies on an overhead projector, we can visually decode the secret through a human visual system without the assistance of any hardware or computation. However, the reconstructed image of VCS suffers from poor visual quality, which is caused by its intrinsic property in using the OR-operation for decoding. On the contrary, the reconstructed image of PSISS is distortion-less in using Lagrange interpolation.

The first VCS encrypts a halftone (black-and-white) secret image into noise-like shadows [1]. Since the visual quality of a reconstructed image in VCS is degraded by a large pixel expansion, research papers have been published to enhance the visual quality or reduce the pixel expansion. Some of them can even have no pixel expansion (m = 1) which are known as the probabilistic VCS (PVCS) [2]–[4]. The authors in [5] extended the PVCS to share both grey-scale images and color images. A multi-secret VCS (MVCS) explores the possibility of sharing multiple secret images [6]–[11]. MVCS can reveal different secret images by stacking shadows at different positions. VCSs with specific features, such as cheating prevention, solving misalignment problem, achieving the ideal contrast, sharing color image, were proposed [12]–[19]. Although VCS cannot recover the original image without distortion-less, the simplicity of VCS provides new applications in sharing secret images, e.g., visual authentication, steganography, and image encryption. For example, VCS-based authentication can let a user perform verification personally. This type of authentication involving human factor actually enhances the system security like seeing-is-believing and CAPTCHA. The first visual authentication using VCS was proposed by Naor and Pinkas [30]. RcCune *et al.* also adopted VCS to enhance the security in logging to a wireless AP [31]. Some security criteria of VSS-based authentication are formally discussed in [32]. To enhance the recognition of PIN code in visual authentication, the segment-based VCS was introduced [33]. More applications of VCS can be found in Chapter 12 "Applications of Visual Cryptography" in the book [34]. Other VCS applications in combining watermark, fingerprint, Google street view, and bar code were introduced in [35]–[38].

Recently, Wang introduced a novel (2, n) region incrementing visual cryptographic scheme (RIVCS) [39]. In a RIVCS, the secret image is subdivided into multiple regions in such a way that any t shadows, where $2 \leq t \leq n$, can be used to reveal the $(t-1)$th region. The incrementing region property provides an attractive feature in secret image sharing applications since this feature enables more shadows to reveal more secrets. However, in Wang's (2, n)-RIVCS, the colors of reconstructed

Manuscript received August 26, 2011; revised October 27, 2011; accepted November 3, 2011. Date of publication December 21, 2011; date of current version May 1, 2012. This work was supported in part by the Testbed@TWISC, National Science Council, under Grant NSC 100-2219-E-006-001. This paper was recommended by Associate Editor M. Barni.

C.-N. Yang, H.-W. Shih, and C.-C. Wu are with the Department of Computer Science and Information Engineering, National Dong Hwa University, Hualien 974-01, Taiwan (e-mail: cnyang@mail.ndhu.edu.tw; m9821069@ems.ndhu.edu.tw; d9721004@ems.ndhu.edu.tw).

L. Harn is with the Department of Computer Science and Electrical Engineering, University of Missouri-Kansas City, Kansas City, MO 64112 USA.

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TCSVT.2011.2180952

image with different security levels are reversed (i.e., the black color and white color are reversed). The objective of this paper is to design a general (k, n)-RIVCS to reveal correct colors in all regions. The main contributions of this paper are: 1) our scheme is a general (k, n)-RIVCS where k and n are any integers and $k < n$; 2) the scheme reveals correct colors of the secret image; and 3) our (k, n)-RIVCS is theoretically proven to satisfy the security and contrast conditions.

The rest of this paper is organized as follows. In Section II, two VCSs are reviewed. In Section III, we propose three constructions of (k, n)-RIVCS. Our RIVCS not only can overcome the problem of the reverse colors, but also can enhance the contrast and reduces the shadow size for most cases in comparing with Wang's RIVCS. Experimental results and comparison are included in Section IV. The conclusion is in Section V.

II. Previous Works

Our new RIVCS scheme is based on the conventional VCS. Here, we describe the (k, n)-VCS and briefly review Wang's (2, n)-RIVCS.

A. (k, n)-VCS

In a black-and-white (k, n)-VCS, the secret image consists of a collection of black-and-white pixels and each pixel is subdivided into a collection of m black-and-white subpixels in each of the n shadows. The collection of sub pixels can be represented by an $n \times m$ Boolean matrix $S = [s_{ij}]$, where the element s_{ij} represents the jth subpixel in the ith shadow. A white subpixel s_{ij} is represented by a 0, and a black subpixel is represented by a 1. Stacking t shadows together, the grey-level of each secret pixel (m subpixels) of the stacked result is proportional to the Hamming weight (the number of 1s in the vector V) $H(V)$ of the OR-ed ("OR" operation) m-tuple $V = OR(i_1, \ldots, i_t)$ where $i_1, \ldots, i_t$ are t rows of S associated with the shadows we stack. Verheul and Van Tilborg [17] extended the definition of Naor and Shamir's scheme [1]. The formal definition of binary VCS is given below.

Definition 1: A (k, n)-VCS consists of two collections of $n \times m$ Boolean matrices B_0 and B_1. To share a white (respectively black) pixel, the dealer randomly chooses one of the matrices in B_0 (respectively B_1). The chosen matrix defines the color of the m subpixels in each one of the n shadows. The collection C_0 (respectively C_1) can be obtained by permuting the columns of the corresponding matrix B_0 (respectively B_1) in all possible ways. B_0 and B_1 are called basis matrices, and every collection has $m!$ matrices. The (k, n)-VCS is considered valid if the following three conditions are satisfied.

1) For any S in C_0, the OR vector V_0 of any k rows of the n rows satisfies $H(V_0) \leq l$.
2) For any S in C_1, the OR vector V_1 of any k rows of the n rows satisfies $H(V_1) \geq h$, where $0 \leq l < h \leq m$.
3) For any subset $\{i_1, \ldots, i_t\} \subset \{1, \ldots, n\}$ with $t < k$, the two collections of $t \times m$ matrices obtained by restricting each $t \times m$ matrix in C_0 and C_1 to rows $i_1, \ldots, i_t$ are indistinguishable in the sense that they contain the same matrices with the same frequencies.

The first two conditions are called contrast and the third condition is called security. The security condition of VCS is similar to the well-known Shamir's secret sharing [40], and the VCS is perfectly secure. The contrast $\alpha = \frac{H(V_1)-H(V_0)}{m} = \frac{h-l}{m}$ is defined as the difference in weight between a white pixel and a black pixel in the reconstructed image [1]. From Definition 1, the black-and-white (k, n)-VCS can be realized by two Boolean matrices B_0 and B_1. Let $\mathrm{OR}\,(B_i|t)$ denote the "OR"-ed t rows in $B_i, i = 0, 1$, and $H(.)$ be the Hamming weight function. Three conditions in Definition 1 can be rewritten as follows.

(V-1) $H\,(\mathrm{OR}\,(B_1|t)) \geq h$ and $H\,(\mathrm{OR}\,(B_0|t)) \leq l$ for $t = k$, where $0 \leq l < h \leq m$.

(V-2) $H\,(\mathrm{OR}\,(B_1|t)) = H\,(\mathrm{OR}\,(B_0|t))$ for $t \leq (k-1)$.

Example 1: Construct a (2, 2)-VCS of $h = 1$, $l = 0$ and $m = 2$ by $B_0 = \begin{bmatrix} 10 \\ 10 \end{bmatrix}$ and $B_1 = \begin{bmatrix} 10 \\ 01 \end{bmatrix}$.

It is observed that $H\,(\mathrm{OR}\,(B_1|2)) = 2$, $H\,(\mathrm{OR}\,(B_0|2)) = 1$, and $H\,(\mathrm{OR}\,(B_1|1)){=}H\,(\mathrm{OR}\,(B_0|1)) = 1$ satisfy the contrast condition (V-1) and the security condition (V-2). We use $xByW$ to represent $(\overbrace{1\cdots1}^{x},\overbrace{0\cdots0}^{y})$ and its permutations. In a reconstructed image, the black color is 2B0W and the white color is 1B1W. Thus, we can visually decode the secret image. Because every 2-subpixel block in shadows is 1B1W, shadows are noise-like. The contrast for this (2, 2)-VCS is $\alpha = \frac{h-l}{m} = 1/2$. □

B. Wang's (2, n)-RIVCS

Similar to MVCS, Wang's (2, n)-RIVCS can reveal multiple images. However, there are two differences between RIVCS and MVCS.

1) MVCS has multiple secret images, while RIVCS divides a secret image into multiple regions, where each region is an image. Thus, a complete secret image in RIVCS is composed by multiple images.
2) In MVCS, the reconstruction of different secret images is performed by stacking two shadows at different positions. However, RIVCS reveals different images gradually by stacking 2, 3, ..., and n shadows, respectively.

In Wang's (2, n)-RIVCS, when stacking $(j+1)$ shadows, one can decode the jth security level region, where $j = 1, 2, \ldots, (n-1)$. For example, in a (2, 4)-RIVCS, the secret image is divided into three secret level regions, as shown in Fig. 1(a). When stacking two, three, and four shadows, we can decode the first, second, and third security level regions, respectively [see Fig. 1(b)–(d)]. Let LK_j^0 (respectively, LK_j^1), $1 \leq j \leq (n-1)$, be the matrix encoding a white (respectively, black) pixel for the jth security level region, and $|LK_j^0|$ and $|LK_j^1|$ are the number of columns. These matrices LK_j^0 and LK_j^1, $1 \leq j \leq (n-1)$, should satisfy the following four conditions.

(R-1) $|LK_j^0| = |LK_j^1|$ for $1 \leq j \leq (n-1)$.

(R-2) $H\left(\mathrm{OR}\left(LK_j^1|t\right)\right){\neq}H\left(\mathrm{OR}\left(LK_j^0|t\right)\right)$ for $t = j+1$.

(R-3) $H\left(\mathrm{OR}\left(LK_j^1|t\right)\right){=}H\left(\mathrm{OR}\left(LK_j^0|t\right)\right)$ for $t{\leq}j$.

(R-4) $LK_1^0 = LK_2^0 = \cdots = LK_{n-1}^0$.

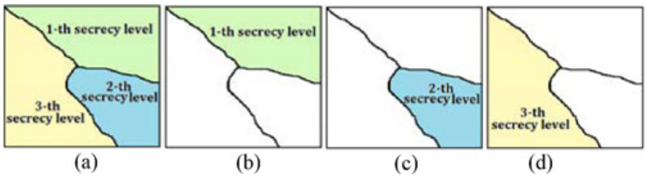


Fig. 1. Partition of three security level regions for the (2, 4)-RIVCS. (a) Three secrecy-level decomposition. (b) Revealed region when stacking two shadows. (c) Revealed region when stacking three shadows. (d) Revealed region when stacking four shadows.

In condition (R-1), the matrices have the same number of columns in order to arrange subpixels of all regions in a shadow. Through (R-2) and (R-3), when stacking $(j + 1)$ shadows, one can decode the jth security level region by the different whiteness for the black and white colors. Meantime, the areas where no secret is revealed are noise-like due to condition (R-4).

Example 2: Construct Wang's (2, 3)-RIVCS by $LK_1^0 = LK_2^0 = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}$, $LK_1^1 = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix}$, and $LK_2^1 = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \end{bmatrix}$.

Obviously, all matrices have four columns, $LK_1^0 = LK_2^0$ and satisfy (R-1) and (R-4), respectively. Every row in all matrices has 2B2W subpixels, and thus all three shadows are noise-like. When stacking any two shadows, we have 3B1W in LK_1^0 and 2B2W in LK_1^1 for the first security level region, 3B1W in LK_2^0 and LK_2^1 for the second security level region. Thus, only the first secret is recovered and its contrast is 1/4. When stacking all three shadows, we have 4B0W and 3B1W in both LK_2^1 and LK_2^0. The contrast is 1/4 for the second secret.

III. Proposed RIVCS

In [39], basis matrices of a (2, n)-RIVCS with $n = 3, 4, 5$ were directly given. However, the author did not explain how to design the basis matrices. Also, in Example 2, the colors of the first security level region are reversed. The combination of 3B1W in the white matrix LK_1^0 is darker than 2B2W in the black matrix LK_1^1. In this paper, we construct a general (k, n)-RIVCS, which the images can be revealed with correct colors for all regions. Our (k, n)-RIVCS is very similar to the scalable (k, n)-PSISS [27]–[29], which has the threshold property and the scalable decoding capability (the scalability). The scalability means that the amount of secret information used in reconstruction is proportional to the number of shadows. The feature of scalability (revealing secrets gradually) is similar to the feature in the well-known ramp secret sharing scheme [41]–[43]. In a (k, L, n)-threshold ramp secret sharing scheme, one can decrypt the secret with any k or more than k shadows; but no information of the secret can be revealed with any $k - L$ or less than $k - L$ shadows. With any set of $k - l$ shadows, $l = 1, 2, \ldots, L - 1$, can learn something about the secret. In the case of $L = 1$, the (k, L, n)-threshold ramp secret sharing scheme is reduced to the original (k, n)-threshold secret sharing scheme. In fact, our (k, n)-RIVCS has the same threshold property and the scalability as the scalable (k, n)-PSISS and the (n, $n - k + 1$, n)-threshold ramp secret sharing scheme.

A. (k, n)-RIVCS with Correct Color for All Regions

Condition (R-2) implies that Wang's (2, n)-RIVC uses the different whiteness of the black and white colors to reveal the secret. If the secret image is a bi-level image, the secret information is not compromised even though the black and white colors are reversed. However, if the color of text is the secret information, the incorrect-color problem will compromise the secret. For this case, (R-2) does not assure the correctness of reconstructing correct colors. In our proposed (k, n)-RIVCS, conditions are modified as follows.

(R-1′) $|LK_j^0|=|LK_j^1|$ for $1 \le j \le (n - k + 1)$.

(R-2′) $H\left(\mathrm{OR}\left(LK_j^1|t\right)\right)>H\left(\mathrm{OR}\left(LK_j^0|t\right)\right)$ for $t = j+k-1$.

(R-3′) $H\left(\mathrm{OR}\left(LK_j^1|t\right)\right)=H\left(\mathrm{OR}\left(LK_j^0|t\right)\right)$ for $t \le j+k-2$.

(R-4′) $LK_1^0 = LK_2^0 = \cdots = LK_{n-k+1}^0$.

Condition (R-2′) is stricter than condition (R-2). The blackness in black color is always darker than that in white color. However, in (R-2), the blackness in different colors is just different.

The proposed (k, n)-RIVCS is based on the $(n-k+1)$ (t, n)-VCSs, $k \le t \le n$. Let $B_1^{(t,n)}$ and $B_0^{(t,n)}$ be the black and white basis matrices of a (t, n)-VCS. Suppose that the background color of a secret image is white. The design concept is described as follows. We unite all white matrices of these (t, n)-VCSs, $k \le t \le n$, to construct LK_j^0. When designing the matrix LK_j^1 for the jth security level region, we use $B_1^{(j+k-1,n)}$ instead of $B_0^{(j+k-1,n)}$ in LK_j^0. Therefore, when stacking t shadows, the secrets in $(t-k+1)$ regions can be revealed. The formal construction is shown in Construction 1. Let the matrix operations "∪" and "−" be the union and minus operations of column vectors. Then, the basis matrices of (k, n)-RIVCS LK_j^0 and LK_j^1, where $1 \le j \le (n-k+1)$, are constructed as follows.

Construction 1: The white matrices LK_j^0, $1 \le j \le (n-k+1)$, are $LK_j^0 = \left[B_0^{(k,n)} \bigcup B_0^{(k+1,n)} \bigcup \cdots \bigcup B_0^{(n,n)}\right]$. The corresponding black matrix for the LK_j^0 is $LK_j^1 = \left[\ B_1^{(j+k-1,n)}\ \middle|\ LK_j^0 - B_0^{(j+k-1,n)}\ \right]$.

Theorem 1: The proposed (k, n)-RIVCS using matrices in Construction 1 satisfies conditions (R-1′), (R-2′), (R-3′), and (R-4′).

Proof: Since $|B_1^{(k,n)}| = |B_0^{(k,n)}|$, we have $|LK_j^1| = \left|\left[\ B_1^{(k,n)}\ \middle|\ LK_j^0 - B_0^{(k,n)}\ \right]\right| = |B_1^{(k,n)}| + |LK_j^0| - |B_0^{(k,n)}| = |LK_j^0|$. Thus, condition (R-1′) is satisfied. Obviously, all white matrices are $\left[B_0^{(k,n)} \bigcup B_0^{(k+1,n)} \bigcup \cdots \bigcup B_0^{(n,n)}\right]$, and thus (R-4′) is satisfied.

From the definition of LK_j^0 and LK_j^0, stacking t shadows in LK_j^0 and LK_j^1 is exactly the same as stacking t shadows in $B_0^{(j+k-1,n)}$ and $B_1^{(j+k-1,n)}$. Since $B_0^{(j+k-1,n)}$ and $B_1^{(j+k-1,n)}$ are the basis matrices of $(j + k - 1, n)$-VCS for $1 \le j \le (n - k + 1)$, considering to stack $t = j + k - 1$ and $t \le j + k - 2$ shadows in $B_0^{(j+k-1,n)}$ and $B_1^{(j+k-1,n)}$, we have

$$\begin{cases} H\left(\mathrm{OR}\left(B_1^{(j+k-1,n)}|t\right)\right) > H\left(\mathrm{OR}\left(B_0^{(j+k-1,n)}|t\right)\right) & \text{for } t = j + k - 1 \\ H\left(\mathrm{OR}\left(B_1^{(j+k-1,n)}|t\right)\right) = H\left(\mathrm{OR}\left(B_0^{(j+k-1,n)}|t\right)\right) & \text{for } t \le j + k - 2. \end{cases} \tag{1}$$

From (1), we can derive the following equation:

$$\begin{cases} H\left(\mathrm{OR}\left(LK_j^1|t\right)\right) > H\left(\mathrm{OR}\left(LK_j^0|t\right)\right) & \text{for } t = j+k-1 \\ H\left(\mathrm{OR}\left(LK_j^1|t\right)\right) = H\left(\mathrm{OR}\left(LK_j^0|t\right)\right) & \text{for } t \leq j+k-2. \end{cases} \tag{2}$$

From (2), the proposed (k, n)-RIVCS satisfies conditions (R-2′) and (R-3′). ■

Example 3: Construct the proposed (2, 3)-RIVCS, (2, 4)-RIVCS, and (2, 5)-RIVCS.

By Construction 1, we can derive the basis matrices of (2, 3)-RIVCS with $m = 6$, as follows. The basis matrices of Naor and Shamir's (2, 3)-VCS and Naor and Shamir's (3, 3)-VCS used for constructing LK_1^0, LK_1^1, LK_2^0, and LK_2^1 are $B_1^{(2,3)} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$, $B_0^{(2,3)} = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix}$, $B_1^{(3,3)} = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix}$, $B_0^{(3,3)} = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}$

$$\begin{cases} LK_1^0 = LK_2^0 = \left[B_0^{(2,3)} \bigcup B_0^{(3,3)}\right] = \begin{bmatrix} 100 \\ 100 \\ 100 \end{bmatrix} \bigcup \begin{bmatrix} 0011 \\ 0101 \\ 0110 \end{bmatrix} = \begin{bmatrix} 100011 \\ 100101 \\ 100110 \end{bmatrix} \\ LK_1^1 = \left[\, B_1^{(2,3)} \;\middle|\; LK_1^0 - B_0^{(2,3)} \,\right] = \left[\, B_1^{(2,3)} \;\middle|\; \begin{matrix} 011 \\ 101 \\ 110 \end{matrix} \,\right] = \left[\begin{matrix} 100 \\ 010 \\ 001 \end{matrix} \;\middle|\; \begin{matrix} 011 \\ 101 \\ 110 \end{matrix}\right] \\ LK_2^1 = \left[\, B_1^{(3,3)} \;\middle|\; LK_2^0 - B_0^{(3,3)} \right] = \left[\, B_1^{(3,3)} \;\middle|\; \begin{matrix} 10 \\ 10 \\ 10 \end{matrix} \,\right] = \left[\begin{matrix} 1001 \\ 0101 \\ 0011 \end{matrix} \;\middle|\; \begin{matrix} 10 \\ 10 \\ 10 \end{matrix}\right]. \end{cases} \tag{3}$$

Using the same approach, we can derive the basis matrices of (2, 4)-RIVCS with $m = 14$ and (2, 5)-RIVCS with $m = 22$, as shown in (4) and (5), respectively. The basis matrices of (2, 4)-VCS, (3, 4)-VCS, (4, 4)-VCS used for (2, 4)-RIVCS, and the basis matrices of (2, 5)-VCS, (3, 5)-VCS, (4, 5)-VCS, (5, 5)-VCS used for (2, 5)-RIVCS are given in the Appendix.

$$\begin{cases} LK_1^0 = LK_2^0 = LK_3^0 = \left[B_0^{(2,4)} \bigcup B_0^{(3,4)} \bigcup B_0^{(4,4)}\right] = \begin{bmatrix} 10000111111000 \\ 10001011100110 \\ 10001101010101 \\ 10001110001011 \end{bmatrix} \\ LK_1^1 = \left[\, B_1^{(2,4)} \;\middle|\; LK_1^0 - B_0^{(2,4)} \,\right] = \left[\begin{matrix} 1000 \\ 0100 \\ 0010 \\ 0001 \end{matrix} \;\middle|\; \begin{matrix} 0111111000 \\ 1011100110 \\ 1101010101 \\ 1110001011 \end{matrix}\right] \\ LK_2^1 = \left[\, B_1^{(3,4)} \;\middle|\; LK_2^0 - B_0^{(3,4)} \,\right] = \left[\begin{matrix} 100011 \\ 010011 \\ 001011 \\ 000111 \end{matrix} \;\middle|\; \begin{matrix} 10111000 \\ 10100110 \\ 10010101 \\ 10001011 \end{matrix}\right] \\ LK_3^1 = \left[\, B_1^{(4,4)} \;\middle|\; LK_3^0 - B_0^{(4,4)} \,\right] = \left[\begin{matrix} 10001110 \\ 01001101 \\ 00101011 \\ 00010111 \end{matrix} \;\middle|\; \begin{matrix} 000111 \\ 001011 \\ 001101 \\ 001110 \end{matrix}\right]. \end{cases} \tag{4}$$

In the following example, (3, 4)-RIVCS and (3, 5)-RIVCS are schemes with $k > 2$. This example reveals that our general (k, n)-RIVCS has region incrementing ability to reveal different secrets.

Example 4: Construct the proposed (3, 4)-RIVCS and (3, 5)-RIVCS.

From Construction 1, we can derive the basis matrices of (3, 4)-RIVCS with $m = 13$ as (6) and (7).

Using the same approach, we can derive the basis matrices of (3, 5)-RIVCS with $m = 20$.

Although the proposed (k, n)-RIVCS from Construction 1 reveals correct colors for all regions, it has large pixel expansion. Next, we demonstrate a modified version to reduce the shadow size and enhance the contrast. Our modified (k, n)-RIVCS may reveal reverse color for some security levels like Wang's scheme.

B. Modified (k, n)-RIVCS

If the secret image is a bi-level image and the color of image is not a secret, shadowholders want to reveal the secret text or the shape of image. In this case, the secret information is not compromised even though the black and white colors are reversed. Without the requirement of revealing correct color, our construction can be modified to reduce the pixel expansion and enhances the contrast compared with Wang' scheme. In this case, condition (R-2′) can be modified as follows:

(R-2″) $H\left(\mathrm{OR}\left(LK_j^1|t\right)\right) \neq H\left(\mathrm{OR}\left(LK_j^0|t\right)\right)$ for $t = j+k-1$.

In the modified RIVCS, we unite black or white matrices of these (t, n)-VCSs, $k \leq t \leq n$, to construct LK_j^0 with minimal pixel expansion. In designing the matrix LK_j^1 for the jth security level region, if we use $B_1^{(j+k-1,n)}$ (respectively $B_0^{(j+k-1,n)}$) in LK_j^0, we use $B_0^{(j+k-1,n)}$ (respectively $B_1^{(j+k-1,n)}$) in LK_j^1. Let $B_{i_j}^{(t,n)}$ be the black or white matrix of a (k, n)-VCS, where $k \leq t \leq n$, $1 \leq j \leq (n-k+1)$ and $i_j \in \{0, 1\}$. Let the matrix $\overline{B_{i_j}^{(j+k-1,n)}}$ be $B_{(i_j+1) \bmod 2}^{(j+k-1,n)}$ (i.e., $\overline{B_1^{(j+k-1,n)}} = B_0^{(j+k-1,n)}$ and $\overline{B_0^{(j+k-1,n)}} = B_1^{(j+k-1,n)}$). The modified ($k$, n)-RIVCS, with LK_j^0 and LK_j^1 where $1 \leq j \leq (n-k+1)$, is proposed in Construction 2.

Construction 2: The white matrices are $LK_j^0 = \left[B_{i_1}^{(k,n)} \bigcup B_{i_2}^{(k+1,n)} \bigcup \cdots \bigcup B_{i_{n-k+1}}^{(n,n)}\right]$ by choosing i_j in $B_{i_j}^{(j+k-1,n)}$, $1 \leq j \leq (n-k+1)$, from 0 or 1 to minimize $|LK_j^0|$. The corresponding black matrix for the LK_j^0 is $LK_j^1 = \left[\, \overline{B_{i_j}^{(j+k-1,n)}} \;\middle|\; LK_j^0 - B_{i_j}^{(j+k-1,n)} \,\right]$.

Theorem 2: The modified (k, n)-RIVCS using matrices in Construction 2 satisfies conditions (R-1′), (R-2″), (R-3′), and (R-4′).

Proof: Since $|B_{i_j}^{(j+k-1,n)}| = |\overline{B_{i_j}^{(j+k-1,n)}}|$, we have $|LK_j^1| = \left|\left[\, \overline{B_{i_j}^{(j+k-1,n)}} \;\middle|\; LK_j^0 - B_{i_j}^{(j+k-1,n)} \,\right]\right| = \left|\overline{B_{i_j}^{(j+k-1,n)}}\right| + |LK_j^0| - |B_{i_j}^{(j+k-1,n)}| = |LK_j^0|$. Thus, condition (R-1′) is satisfied. Obviously, all white matrices are $\left[B_{i_1}^{(k,n)} \bigcup B_{i_2}^{(k+1,n)} \bigcup \cdots \bigcup B_{i_{n-k+1}}^{(n,n)}\right]$, and condition (R-4′) is satisfied.

From the definition of LK_j^0 and LK_j^1, if $i_j = 0$, stacking t shadows in LK_j^0 and LK_j^1 is exactly the same as stacking t shadows in $B_{i_j}^{(j+k-1,n)} = B_0^{(j+k-1,n)}$ and $\overline{B_{i_j}^{(j+k-1,n)}} = B_1^{(j+k-1,n)}$. This is the same as the proposed scheme, and we derive

$$\begin{cases} H\left(\mathrm{OR}\left(LK_j^1|t\right)\right) > H\left(\mathrm{OR}\left(LK_j^0|t\right)\right) & \text{for } t = j+k-1 \\ H\left(\mathrm{OR}\left(LK_j^1|t\right)\right) = H\left(\mathrm{OR}\left(LK_j^0|t\right)\right) & \text{for } t \leq j+k-2. \end{cases} \tag{8-1}$$

On the other hand, if $i_j = 1$, stacking t shadows in LK_j^0 and LK_j^1 is exactly the same as stacking t shadows in $B_{i_j}^{(j+k-1,n)} =$

$B_1^{(j+k-1,n)}$ and $\overline{B_{i_j}^{(j+k-1,n)}} = B_0^{(j+k-1,n)}$. Following the similar argument, we have

$$\begin{cases} H\left(\mathrm{OR}\left(LK_j^1|t\right)\right) < H\left(\mathrm{OR}\left(LK_j^0|t\right)\right) & \text{for } t = j+k-1 \\ H\left(\mathrm{OR}\left(LK_j^1|t\right)\right) = H\left(\mathrm{OR}\left(LK_j^0|t\right)\right) & \text{for } t \le j+k-2. \end{cases} \tag{8-2}$$

Equations (8-1) and (8-2) imply the following equation:

$$\begin{cases} H\left(\mathrm{OR}\left(LK_j^1|t\right)\right) \neq H\left(\mathrm{OR}\left(LK_j^0|t\right)\right) & \text{for } t = j+k-1 \\ H\left(\mathrm{OR}\left(LK_j^1|t\right)\right) = H\left(\mathrm{OR}\left(LK_j^0|t\right)\right) & \text{for } t \le j+k-2. \end{cases} \tag{9}$$

From (9), the modified (k, n)-RIVCS satisfies (R-2″) and (R-3′). ■

The modified (2, n)-RIVCS in Construction 2 can be further improved in the following construction to enhance the contrast for the first security level region.

Construction 3: For the modified (2, n)-RIVCS in Construction 2, if $B_{i_1}^{(2,n)}$ in LK_j^0 is $B_1^{(2,n)}$, we can use $LK_1^1 = \left[\begin{array}{c|c} & \overbrace{1\cdots1}^{m_1}\overbrace{0\cdots0}^{m_0} \\ \overline{B_1^{(2,n)}} & \vdots\cdots10\cdots0 \\ & 1\cdots10\cdots0 \end{array}\right]$ instead of $LK_1^1 =$

$$\begin{cases}
LK_1^0 = LK_2^0 = LK_3^0 = LK_4^0 = \left[B_0^{(2,5)} \bigcup B_0^{(3,5)} \bigcup B_0^{(4,5)} \bigcup B_0^{(5,5)}\right] \\
= \begin{bmatrix} 1&1&1&1&0&0&1&1&1&1&0&0&1&1&1&1&0&0&0&0&0&0 \\ 1&1&1&1&0&1&0&1&1&1&0&0&1&0&0&0&1&1&1&0&0&0 \\ 1&1&1&1&0&1&1&0&1&1&0&0&0&1&0&0&1&0&0&1&1&0 \\ 1&1&1&1&0&1&1&1&0&1&0&0&0&0&1&0&0&1&0&1&0&1 \\ 1&1&1&1&0&1&1&1&1&0&0&0&0&0&0&1&0&0&1&0&1&1 \end{bmatrix} \\
LK_1^1 = \left[\begin{array}{c|c} B_1^{(2,5)} & LK_1^0 - B_0^{(2,5)} \end{array}\right] = \left[\begin{array}{ccccc|ccccccccccccccccc} 0&1&1&1&1&0&1&1&1&1&0&0&1&1&1&1&0&0&0&0&0&0 \\ 1&0&1&1&1&1&0&1&1&1&0&0&1&0&0&0&1&1&1&0&0&0 \\ 1&1&0&1&1&1&1&0&1&1&0&0&0&1&0&0&1&0&0&1&1&0 \\ 1&1&1&0&1&1&1&1&0&1&0&0&0&0&1&0&0&1&0&1&0&1 \\ 1&1&1&1&0&1&1&1&1&0&0&0&0&0&0&1&0&0&1&0&1&1 \end{array}\right] \\
LK_2^1 = \left[\begin{array}{c|c} B_1^{(3,5)} & LK_2^0 - B_0^{(3,5)} \end{array}\right] = \left[\begin{array}{cccccccc|cccccccccccccc} 1&0&0&0&0&1&1&1&1&1&1&1&1&1&1&1&0&0&0&0&0&0 \\ 0&1&0&0&0&1&1&1&1&1&1&1&1&0&0&0&1&1&1&0&0&0 \\ 0&0&1&0&0&1&1&1&1&1&1&1&0&1&0&0&1&0&0&1&1&0 \\ 0&0&0&1&0&1&1&1&1&1&1&1&0&0&1&0&0&1&0&1&0&1 \\ 0&0&0&0&1&1&1&1&1&1&1&1&0&0&0&1&0&0&1&0&1&1 \end{array}\right] \\
LK_3^1 = \left[\begin{array}{c|c} B_1^{(4,5)} & LK_3^0 - B_0^{(4,5)} \end{array}\right] = \left[\begin{array}{||c|c|c|c|c|c|c|c|c|c|c|c|c|c|c|ccccccc} 0&1&1&1&1&1&0&0&0&0&1&0&0&0&0&1&1&0&1&1&1&1 \\ 1&0&1&1&1&0&1&0&0&0&0&1&0&0&0&1&1&1&0&1&1&1 \\ 1&1&0&1&1&0&0&1&0&0&0&0&1&0&0&1&1&1&1&0&1&1 \\ 1&1&1&0&1&0&0&0&1&0&0&0&0&1&0&1&1&1&1&1&0&1 \\ 1&1&1&1&0&0&0&0&0&1&0&0&0&0&1&1&1&1&1&1&1&0 \end{array}\right] \\
LK_4^1 = \left[\begin{array}{c|c} B_1^{(5,5)} & LK_4^0 - B_0^{(5,5)} \end{array}\right] = \left[\begin{array}{||c|c|c|c|c|c|c|c|c|c|c|c|c|c|c|ccccccc} 1&0&0&0&0&1&1&1&1&1&1&0&0&0&0&1&1&1&1&1&0&0 \\ 0&1&0&0&0&1&1&1&0&0&0&1&1&1&0&1&1&1&1&1&0&0 \\ 0&0&1&0&0&1&0&0&1&1&0&1&1&0&1&1&1&1&1&1&0&0 \\ 0&0&0&1&0&0&1&0&1&0&1&1&0&1&1&1&1&1&1&1&0&0 \\ 0&0&0&0&1&0&0&1&0&1&1&0&1&1&1&1&1&1&1&1&0&0 \end{array}\right]
\end{cases} \tag{5}$$

$$\begin{cases}
LK_1^0 = LK_2^0 = \left[B_0^{(3,4)} \bigcup B_0^{(4,4)}\right] = \begin{bmatrix} 0&1&1&1&0&0 \\ 1&0&1&1&0&0 \\ 1&1&0&1&0&0 \\ 1&1&1&0&0&0 \end{bmatrix} \bigcup \begin{bmatrix} 01&1&10&00&1 \\ 01&0&01&10&1 \\ 00&1&01&01&1 \\ 00&0&10&11&1 \end{bmatrix} = \begin{bmatrix} 0&11&10&01&11&00&01 \\ 1&01&10&01&00&11&01 \\ 1&10&10&00&10&10&11 \\ 1&11&00&00&01&01&11 \end{bmatrix} \\
LK_1^1 = \left[\begin{array}{c|c} B_1^{(3,4)} & LK_1^0 - B_0^{(3,4)} \end{array}\right] = \left[\begin{array}{c|ccccccc} & 1&1&1&0&0&0&1 \\ & 1&0&0&1&1&0&1 \\ B_1^{(3,4)} & 0&1&0&1&0&1&1 \\ & 0&0&1&0&1&1&1 \end{array}\right] = \left[\begin{array}{cccccc|ccccccc} 1&0&0&0&1&1&1&1&1&0&0&0&1 \\ 0&1&0&0&1&1&1&0&0&1&1&0&1 \\ 0&0&1&0&1&1&0&1&0&1&0&1&1 \\ 0&0&0&1&1&1&0&0&1&0&1&1&1 \end{array}\right] \\
LK_2^1 = \left[\begin{array}{c|c} B_1^{(4,4)} & LK_2^0 - B_0^{(4,4)} \end{array}\right] = \left[\begin{array}{c|ccccc} & 0&1&1&1&0 \\ & 1&0&1&1&0 \\ B_1^{(4,4)} & 1&1&0&1&0 \\ & 1&1&1&0&0 \end{array}\right] = \left[\begin{array}{cccccccc|ccccc} 1&0&0&0&1&1&1&0&0&1&1&1&0 \\ 0&1&0&0&1&1&0&1&1&0&1&1&0 \\ 0&0&1&0&1&0&1&1&1&1&0&1&0 \\ 0&0&0&1&0&1&1&1&1&1&1&0&0 \end{array}\right]
\end{cases} \tag{6}$$

$\left[\ \overline{B_1^{(2,n)}}\ \middle|\ LK_1^0 - B_1^{(2,n)}\ \right]$, where the values of m_1 and m_0 are chosen to let the number of ones in a row be exactly the same as LK_1^0. Other matrices are the same as in Construction 2.

Theorem 3: The modified (2, n)-RIVCS using matrices in Construction 3 satisfies conditions (R-1′), (R-2″), (R-3′), and (R-4′).

Proof: We consider two cases: 1) $j \in [2, n-1]$; and 2) $j = 1$ in proving this theorem.

Case 1 $j \in [2, n-1]$.

Same as the proof of Theorem 2.

Case 2 $j = 1$.

For $j = 1$, the only difference is LK_1^1. Therefore, we only need to prove that conditions (R-1′), (R-2″), and (R-3′) are satisfied for $j = 1$. Since m_1 and m_0 are chosen to let the number of ones in a row be exactly the same as LK_1^0, so $|LK_1^0|$=$|LK_1^1|$and $H\left(\text{OR}\left(LK_1^1|t\right)\right)$=$H\left(\text{OR}\left(LK_1^0|t\right)\right)$ for $t = 1$. Thus, (R-1′) and (R-3′) are satisfied. For $j = 1$ and $k = 2$, (R-2″) is reduced as follows: ■

$$H\left(\text{OR}\left(LK_1^1|t\right)\right) \neq H\left(\text{OR}\left(LK_1^0|t\right)\right) \text{ for } t = 2. \tag{10}$$

From construction, we have $LK_1^0 = \left[B_1^{(2,n)} \bigcup B_{i_2}^{(3,n)} \bigcup \cdots \bigcup B_{i_{n-1}}^{(n,n)}\right]$ and $LK_1^1 = \left[\begin{array}{c|c} B_0^{(2,n)} & \begin{array}{c} \overbrace{1\cdots1}^{m_1}\overbrace{0\cdots0}^{m_0} \\ \vdots\cdots10\cdots0 \\ 1\cdots10\cdots0 \end{array} \end{array}\right]$, where every row in LK_1^0 and LK_1^0 has the same Hamming weight. Also, every row in $B_1^{(2,n)}$ and $B_0^{(2,n)}$ has the same Hamming weight. The above statement implies the following equation:

$$\begin{cases} H\left(\text{OR}\left(LK_1^0|1\right)\right) = H\left(\text{OR}\left(LK_1^1|1\right)\right) \\ H\left(\text{OR}\left(LK_1^1|1\right)\right) = H\left(\text{OR}\left(B_0^{(2,n)}|1\right)\right) + m_1 \\ H\left(\text{OR}\left(LK_1^0|1\right)\right) = H\left(\text{OR}\left(B_1^{(2,n)}|1\right)\right) + \\ H\left(\text{OR}\left(\left[B_{i_2}^{(3,n)} \bigcup \cdots \bigcup B_{i_{n-1}}^{(n,n)}\right] |1\right)\right). \end{cases} \tag{11}$$

From (11), we can derive $H\left(\text{OR}\left(\left[B_{i_2}^{(3,n)} \bigcup \cdots \bigcup B_{i_{n-1}}^{(n,n)}\right] |1\right)\right) = m_1$. It is evident that, when stacking any two binary vectors with m_1 constant weights, the Hamming weight is large than m_1. Therefore, we have $H\left(\text{OR}\left(\left[B_{i_2}^{(3,n)} \bigcup \cdots \bigcup B_{i_{n-1}}^{(n,n)}\right] |2\right)\right) \geq m_1$. Finally, we obtain

$$\begin{aligned} &H\left(\text{OR}\left(LK_1^0|2\right)\right) = H\left(\text{OR}\left(B_1^{(2,n)}|2\right)\right) \\ &+H\left(\text{OR}\left(\left[B_{i_2}^{(3,n)} \bigcup \cdots \bigcup B_{i_{n-1}}^{(n,n)}\right] |1\right)\right) \\ &\geq H\left(\text{OR}\left(B_0^{(2,n)}|2\right)\right) \\ &+H\left(\text{OR}\left(\left[B_{i_2}^{(3,n)} \bigcup \cdots \bigcup B_{i_{n-1}}^{(n,n)}\right] |1\right)\right) \\ &\geq H\left(\text{OR}\left(B_0^{(2,n)}|2\right)\right) + m_1 = H\left(\text{OR}\left(LK_1^1|2\right)\right). \end{aligned} \tag{12}$$

In (12), $H\left(\text{OR}\left(LK_1^0|2\right)\right) \geq H\left(\text{OR}\left(LK_1^1|2\right)\right)$ and this result implies $H\left(\text{OR}\left(LK_1^0|2\right)\right) \neq H\left(\text{OR}\left(LK_1^1|2\right)\right)$. So, (R-2″) is satisfied.

Example 5: Construct the modified (2, 3)-RIVCS, (2, 4)-RIVCS and (2, 5)-RIVCS.

$$\begin{cases} LK_1^0 = LK_2^0 = LK_3^0 = \left[B_0^{(3,5)} \bigcup B_0^{(4,5)} \bigcup B_0^{(5,5)}\right] = \begin{bmatrix} 0&1&1&1&1&0&0&0&1&1&1&1&0&0&0&0&0&0&1&1 \\ 1&0&1&1&1&0&0&0&1&0&0&0&1&1&1&0&0&0&1&1 \\ 1&1&0&1&1&0&0&0&0&1&0&0&1&0&0&1&1&0&1&1 \\ 1&1&1&0&1&0&0&0&0&0&1&0&0&1&0&1&0&1&1&1 \\ 1&1&1&1&0&0&0&0&0&0&0&1&0&0&1&0&1&1&1&1 \end{bmatrix} \\ LK_1^1 = \left[\ B_1^{(3,5)}\ \middle|\ LK_1^0 - \ B_0^{(3,5)}\right] = \left[\begin{array}{cccccccc|cccccccccccc} 1&0&0&0&0&1&1&1&1&1&1&1&0&0&0&0&0&0&1&1 \\ 0&1&0&0&0&1&1&1&1&0&0&0&1&1&1&0&0&0&1&1 \\ 0&0&1&0&0&1&1&1&0&1&0&0&1&0&0&1&1&0&1&1 \\ 0&0&0&1&0&1&1&1&0&0&1&0&0&1&0&1&0&1&1&1 \\ 0&0&0&0&1&1&1&1&0&0&0&1&0&0&1&0&1&1&1&1 \end{array}\right] \\ LK_2^1 = \left[\ B_1^{(4,5)}\ \middle|\ LK_2^0 - \ B_0^{(4,5)}\right] = \begin{bmatrix} 0&1&1&1&1&1&0&0&0&0&1&0&0&0&0&0&1&1&1&1 \\ 1&0&1&1&1&0&1&0&0&0&0&1&0&0&0&1&0&1&1&1 \\ 1&1&0&1&1&0&0&1&0&0&0&0&1&0&0&1&1&0&1&1 \\ 1&1&1&0&1&0&0&0&1&0&0&0&0&1&0&1&1&1&0&1 \\ 1&1&1&1&0&0&0&0&0&1&0&0&0&0&1&1&1&1&1&0 \end{bmatrix} \\ LK_3^1 = \left[\ B_1^{(5,5)}\ \middle|\ LK_3^0 - \ B_0^{(5,5)}\right] = \begin{bmatrix} 1&0&0&0&0&1&1&1&1&1&1&0&0&0&0&1&1&1&0&0 \\ 0&1&0&0&0&1&1&1&0&0&0&1&1&1&0&1&1&1&0&0 \\ 0&0&1&0&0&1&0&0&1&1&0&1&1&0&1&1&1&1&0&0 \\ 0&0&0&1&0&0&1&0&1&0&1&1&0&1&1&1&1&1&0&0 \\ 0&0&0&0&1&0&0&1&0&1&1&0&1&1&1&1&1&1&0&0 \end{bmatrix} \end{cases} \tag{7}$$

From Construction 3, we can derive the basis matrices of the modified (2, 3)-RIVCS with $m = 4$, as follows:

$$\begin{cases} LK_1^0 = LK_2^0 = B_1^{(2,3)} \bigcup B_1^{(3,3)} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \bigcup \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix} \\ = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix} \\ LK_1^1 = \left[\begin{array}{c|c} \overline{B_1^{(2,3)}} & \begin{array}{c} 1 \\ 1 \\ 1 \end{array} \end{array} \right] = \left[\begin{array}{c|c} B_0^{(2,3)} & \begin{array}{c} 1 \\ 1 \\ 1 \end{array} \end{array} \right] = \left[\begin{array}{ccc|c} 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \end{array} \right] \\ LK_2^1 = \left[\begin{array}{c|c} \overline{B_1^{(3,3)}} & LK_2^0 - B_1^{(3,3)} \end{array} \right] = \left[\begin{array}{c|c} B_0^{(3,3)} & \emptyset \end{array} \right] = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}. \end{cases} \tag{13}$$

If we use $B_1^{(2,3)} = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}$ and $B_0^{(2,3)} = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 0 \end{bmatrix}$, from Construction 3, we have $LK_1^0{=}LK_2^0{=}B_1^{(2,3)}\Box B_0^{(3,3)}{=} \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}$, and $LK_1^1 = \left[\begin{array}{c|c} \overline{B_1^{(2,3)}} & \begin{array}{c} 1 \\ 1 \\ 1 \end{array} \end{array} \right] = \left[\begin{array}{c|c} B_0^{(2,3)} & \begin{array}{c} 0 \\ 0 \\ 0 \end{array} \end{array} \right] \left[\begin{array}{ccc|c} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{array} \right]$, $LK_2^1 = \left[\begin{array}{c|c} \overline{B_0^{(3,3)}} & LK_2^0 - B_0^{(3,3)} \end{array} \right] = \left[\begin{array}{c|c} B_1^{(3,3)} & \emptyset \end{array} \right] = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix}$. We can obtain the same matrices as Wang's (2, 3)-RIVCS.

Using the same approach, we can derive the basis matrices of the modified (2, 4)-RIVCS with $m = 10$ and (2, 5)-RIVCS with $m = 20$, as shown in (14) and (15), respectively, at the top of the next page. □

Example 6: Construct the modified (3, 4)-RIVCS and (3, 5)-RIVCS.

From Construction 2, we can derive the basis matrices of the modified (3, 4)-RIVCS with $m = 10$ and the modified (3, 5)-RIVCS with $m = 20$ as shown in (16) and (17), respectively

$$\begin{cases} LK_1^0{=}LK_2^0{=}B_1^{(3,4)} \bigcup B_1^{(4,4)}{=} \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \\ LK_1^1{=} \left[\begin{array}{c|c} \overline{B_1^{(3,4)}} & LK_1^0 - B_1^{(3,4)} \end{array} \right] = \left[\begin{array}{cccccc|cccc} 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \end{array} \right] \\ LK_2^1{=} \left[\begin{array}{c|c} \overline{B_1^{(4,4)}} & LK_2^0 - B_1^{(4,4)} \end{array} \right] = \left[\begin{array}{cccccccc|cc} 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 \end{array} \right]. \end{cases} \tag{16}$$

□

IV. Experiments and Comparisons

Six schemes are implemented to examine the performance of the proposed (k, n)-RIVCS and the modified (k, n)-RIVCS. Scheme #1 is Wang's (2, 3)-RIVCS, Scheme #2 is the proposed (2, 3)-RIVCS, Schemes #3 and #4 are our modified (2, 3)-RIVCS and (2, 5)-RIVCS. All these four schemes are (2, n)-RIVCS. Schemes #5 and 6 are the (k, n)-RIVCS with $k{>}2$. Scheme #5 is the modified (3, 4)-RIVCS. Scheme #6 is the proposed (3, 5)-RIVCS, and this scheme is the modified (3, 5)-RIVCS. MATLAB source codes of these schemes can be found in the supplementary manuscript on the website (http://cis.csie.ndhu.edu.tw/∼cnyang/RIVCS.htm).

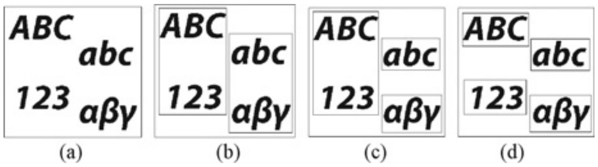


Fig. 2. Secret image and the secrecy-level decomposition. (a) Secret image. (b) Two secrecy-level decomposition $\boxed{\substack{ABC\\123}}$ and $\boxed{\substack{abc\\\alpha\beta\gamma}}$ used for (2, 3)-RIVCS and (3, 4)-RIVCS. (c) Three secrecy-level decomposition $\boxed{\substack{ABC\\123}}$, $\boxed{abc}$ and $\boxed{\alpha\beta\gamma}$ for (3, 5)-RIVCS. (d) Four secrecy-level decomposition $\boxed{ABC}$, $\boxed{abc}$, $\boxed{123}$ and $\boxed{\alpha\beta\gamma}$ used for (2,5)-RIVCS.

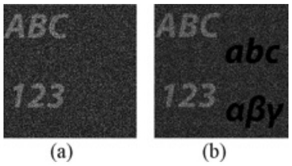


Fig. 3. Wang's (2, 3)-RIVCS. (a) Stacking any two shadows to gain first level secret. (b) Stacking all three shadows to gain second level secret.

Obviously, Wang's RIVCS and our modified RIVCS cannot be extended to grey-level secret images since both schemes have the incorrect color problem. The proposed RIVCS can be extended to grey-level/color secret images. Generally, for processing grey-level or color secret images, a trivial solution is to convert the secret image into the binary image by the halftoning technique [44, 18]. Notice that color images should be halftoned at the primary colors yellow, magenta, and cyan. Then, we process these halftoned images using a black-and-white VCS. However, a better way in designing grey-level/color version needs further study. In all experiments, we only show the black-and-white secret image to demonstrate our improvements in revealing the correct color (the proposed RIVCS) and having less pixel expansion (the modified RIVCS) in comparing with Wang's RIVCS.

As shown in Fig. 2(a), the secret image used for these schemes is a printed-text secret image embracing $\boxed{ABC}$, $\boxed{abc}$, $\boxed{123}$, and $\boxed{\alpha\beta\gamma}$. The two security-level decomposition is shown in Fig. 2(b), the secret image is subdivided into two regions, $\boxed{\substack{ABC\\123}}$ (with first security level) and $\boxed{\substack{abc\\\alpha\beta\gamma}}$ (with second security level). This decomposition is used in Schemes #1, #2, #3, and #5. For Scheme #6 and Scheme #4, we need three and four security-level decompositions, respectively. Fig. 2(c) shows three security regions: $\boxed{\substack{ABC\\123}}$ (with first security level), $\boxed{abc}$ (with second security level), and $\boxed{\alpha\beta\gamma}$ (with third security level), and Fig. 2(d) shows four security regions: $\boxed{ABC}$ (with first security level), $\boxed{abc}$ (with second security level), $\boxed{123}$ (with third security level), and $\boxed{\alpha\beta\gamma}$ (with fourth security level).

The reconstructed images of Scheme #1 are shown in Fig. 3. The revealed secrets by stacking two shadows and all three

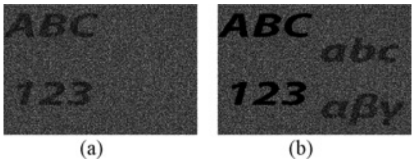


Fig. 4. Proposed (2, 3)-RIVCS. (a) Stacking any two shadows to gain first level secret. (b) Stacking all three shadows to gain second level secret.

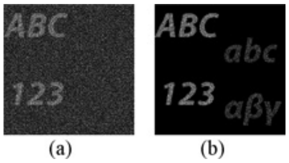


Fig. 5. Modified (2, 3)-RIVCS. (a) Stacking any two shadows to gain first level secret. (b) Stacking all three shadows to gain second level secret.

shadows are $\boxed{\begin{matrix}ABC\\123\end{matrix}}$ [Fig. 3(a)], $\boxed{\begin{matrix}abc\\\alpha\beta\gamma\end{matrix}}$ [Fig. 3(b)], respectively. It is observed that the color of $\boxed{\begin{matrix}ABC\\123\end{matrix}}$ is lighter than the background, while the color of $\boxed{\begin{matrix}abc\\\alpha\beta\gamma\end{matrix}}$ is darker than the background. This is the incorrect color problem in Wang's scheme. Scheme #2 solves this incorrect color problem. However, it has pixel expansion $m = 6$. From the reconstructed images in Scheme #2 [Fig. 4(a), (b)], all printed texts are darker than the background, and show the correct color. Scheme #3 has $m = 4$, which is the same as Scheme #1. Fig. 5 shows the reconstructed images of Scheme #3. Although both (2, 3)-RIVCSs have same pixel expansion $m = 4$, Wang's (2, 3)-RIVCS scheme has $\alpha = 1/4$ for the first security level region when stacking three shadows, while our modified (2, 3)-RIVCS scheme enhances the contrast to $\alpha = 1/2$ by stacking

$$\left\{\begin{array}{l}
LK_1^0{=}LK_2^0{=}LK_3^0 = B_1^{(2,4)} \bigcup B_1^{(3,4)} \bigcup B_1^{(4,4)} = \begin{bmatrix} 1&0&0&0&1&1&1&0&1&1\\ 0&1&0&0&1&1&0&1&1&1\\ 0&0&1&0&1&0&1&1&1&1\\ 0&0&0&1&0&1&1&1&1&1 \end{bmatrix}\\
LK_1^1{=}\left[\begin{array}{c|cccccc} & 1&1&1&1&1&0\\ \overline{B_1^{(2,4)}} & 1&1&1&1&1&0\\ & 1&1&1&1&1&0\\ & 1&1&1&1&1&0 \end{array}\right] = \left[\begin{array}{c|cccccc} & 1&1&1&1&1&0\\ B_0^{(2,4)} & 1&1&1&1&1&0\\ & 1&1&1&1&1&0\\ & 1&1&1&1&1&0 \end{array}\right] = \left[\begin{array}{cccc|cccccc} 1&0&0&0&1&1&1&1&1&0\\ 1&0&0&0&1&1&1&1&1&0\\ 1&0&0&0&1&1&1&1&1&0\\ 1&0&0&0&1&1&1&1&1&0 \end{array}\right]\\
LK_2^1 = \left[\ \overline{B_1^{(3,4)}}\ \middle|\ LK_2^0 - B_1^{(3,4)}\ \right] = \left[\begin{array}{cccccc|cccc} 0&1&1&1&0&0&1&1&1&0\\ 1&0&1&1&0&0&1&1&0&1\\ 1&1&0&1&0&0&1&0&1&1\\ 1&1&1&0&0&0&0&1&1&1 \end{array}\right]\\
LK_3^1 = \left[\ \overline{B_1^{(4,4)}}\ \middle|\ LK_3^0 - B_1^{(4,4)}\ \right] = \left[\begin{array}{cccccccc|cc} 0&1&1&1&0&0&0&1&1&1\\ 0&1&0&0&1&1&0&1&1&1\\ 0&0&1&0&1&0&1&1&1&1\\ 0&0&0&1&0&1&1&1&1&1 \end{array}\right]
\end{array}\right. \tag{14}$$

$$\left\{\begin{array}{l}
LK_1^0 = LK_2^0 = LK_3^0 = LK_4^0 = B_1^{(2,5)} \bigcup B_0^{(3,5)} \bigcup B_0^{(4,5)} \bigcup B_0^{(5,5)} = \begin{bmatrix} 0&1&1&1&1&0&0&0&0&0&0&1&1&1&1&0&0&0&1&1\\ 0&1&0&0&0&1&1&1&0&0&0&1&1&1&0&1&0&0&1&1\\ 0&0&1&0&0&1&0&0&1&1&0&1&1&0&1&1&0&0&1&1\\ 0&0&0&1&0&0&1&0&1&0&1&1&0&1&1&1&0&0&1&1\\ 0&0&0&0&1&0&0&1&0&1&1&0&1&1&1&1&0&0&1&1 \end{bmatrix}\\
LK_1^1 = \left[\begin{array}{c|ccccccccccccccc} & 1&1&1&1&1&1&0&0&0&0&0&0&0&0&0\\ & 1&1&1&1&1&1&0&0&0&0&0&0&0&0&0\\ \overline{B_1^{(2,5)}} & 1&1&1&1&1&1&0&0&0&0&0&0&0&0&0\\ & 1&1&1&1&1&1&0&0&0&0&0&0&0&0&0\\ & 1&1&1&1&1&1&0&0&0&0&0&0&0&0&0 \end{array}\right]\\
= \left[\begin{array}{ccccc|ccccccccccccccc} 1&1&1&1&0&1&1&1&1&1&1&0&0&0&0&0&0&0&0&0\\ 1&1&1&1&0&1&1&1&1&1&1&0&0&0&0&0&0&0&0&0\\ 1&1&1&1&0&1&1&1&1&1&1&0&0&0&0&0&0&0&0&0\\ 1&1&1&1&0&1&1&1&1&1&1&0&0&0&0&0&0&0&0&0\\ 1&1&1&1&0&1&1&1&1&1&1&0&0&0&0&0&0&0&0&0 \end{array}\right]\\
LK_2^1 = \left[\ \overline{B_0^{(3,5)}}\ \middle|\ LK_2^0 - B_0^{(3,5)}\ \right] = \left[\begin{array}{cccccccc|cccccccccccc} 1&0&0&0&0&1&1&1&1&1&1&1&0&0&0&0&0&0&1&1\\ 0&1&0&0&0&1&1&1&1&0&0&0&1&1&1&0&0&0&1&1\\ 0&0&1&0&0&1&1&1&0&1&0&0&1&0&0&1&1&0&1&1\\ 0&0&0&1&0&1&1&1&0&0&1&0&0&1&0&1&0&1&1&1\\ 0&0&0&0&1&1&1&1&0&0&0&1&0&0&1&0&1&1&1&1 \end{array}\right]\\
LK_3^1 = \left[\ \overline{B_0^{(4,5)}}\ \middle|\ LK_3^0 - B_0^{(4,5)}\ \right] = \left[\begin{array}{ccccccccccccccc|ccccc} 0&1&1&1&1&1&0&0&0&0&1&0&0&0&0&1&1&1&1&0\\ 1&0&1&1&1&0&1&0&0&0&0&1&0&0&0&1&1&1&0&1\\ 1&1&0&1&1&0&0&1&0&0&0&0&1&0&0&1&1&0&1&1\\ 1&1&1&0&1&0&0&0&1&0&0&0&0&1&0&1&0&1&1&1\\ 1&1&1&1&0&0&0&0&0&1&0&0&0&0&1&0&1&1&1&1 \end{array}\right]\\
LK_4^1 = \left[\ \overline{B_0^{(5,5)}}\ \middle|\ LK_4^0 - B_0^{(5,5)}\ \right] = \left[\begin{array}{cccccccccccccccc|cccc} 1&0&0&0&0&1&1&1&1&1&1&0&0&0&0&1&0&0&1&1\\ 0&1&0&0&0&1&1&1&0&0&0&1&1&1&0&1&0&0&1&1\\ 0&0&1&0&0&1&0&0&1&1&0&1&1&0&1&1&0&0&1&1\\ 0&0&0&1&0&0&1&0&1&0&1&1&0&1&1&1&0&0&1&1\\ 0&0&0&0&1&0&0&1&0&1&1&0&1&1&1&1&0&0&1&1 \end{array}\right]
\end{array}\right. \tag{15}$$

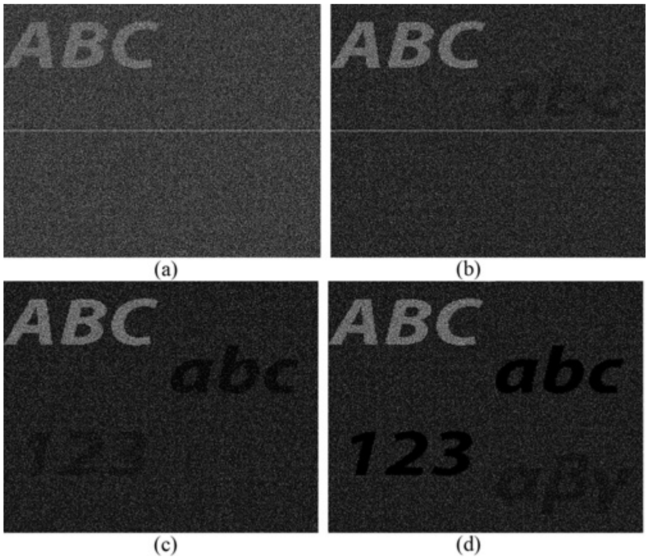


Fig. 6. Modified (2, 5)-RIVCS. (a) Stacking any two shadows to obtain first level secret. (b) Stacking any three shadows to obtain second level secret. (c) Stacking any four shadows to obtain third level secret. (d) Stacking all five shadows to obtain fourth level secret.

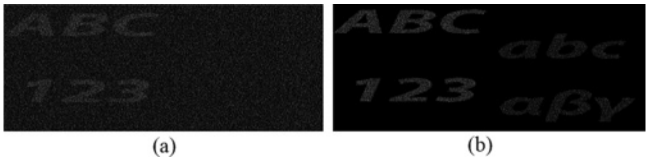


Fig. 7. Modified (3, 4)-RIVCS. (a) Stacking any three shadows to obtain first level secret. (b) Stacking all four shadows to obtain second level secret.

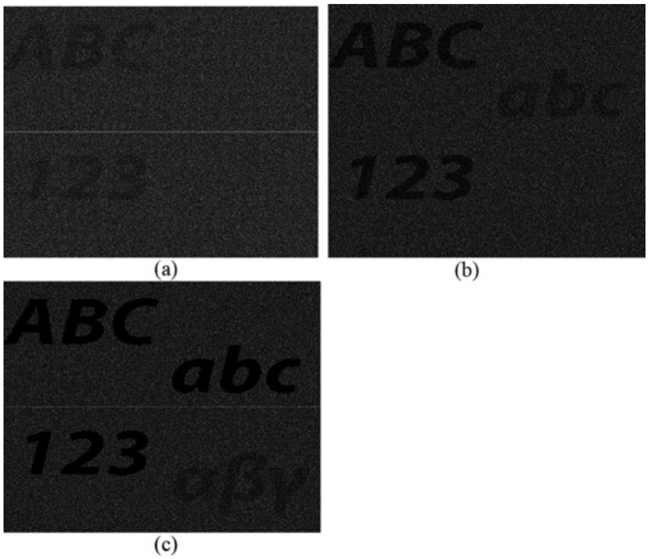


Fig. 8. Proposed (3, 5)-RIVCS [also is the modified (3, 5)-RIVCS]. (a) Stacking three shadows to obtain first level secret. (b) Stacking four shadows to obtain second level secret. (c) Stacking five shadows to obtain third level secret.

three shadows. It is observed that $\boxed{\begin{smallmatrix} ABC \\ 123 \end{smallmatrix}}$ in Fig. 5(b) is clearer than Fig. 3(b). Experimental results of Scheme #4 are shown in Fig. 6. We gradually reveal the secret images with different security levels by stacking 2, 3, 4 and 5 shadows, respectively. Scheme #4 has pixel expansion $m = 20$, which is lesser than $m = 23$ in Wang's (2, 5)-RVICS. Experimental results of Scheme #5 and Scheme #6, where $k \geq 3$, are shown in Figs. 7 and 8. The color of text in the reconstructed image in our modified (3, 4)-RIVCS is reversed. Scheme #6 is the

$$
\begin{cases}
LK_1^0{=}LK_2^0 = LK_3^0 = B_0^{(3,5)} \bigcup B_0^{(4,5)} \bigcup B_0^{(5,5)} = \left[\begin{array}{cccccccccccccccccccc}
0&1&1&1&1&0&0&0&1&1&1&1&0&0&0&0&0&0&1&1\\
1&0&1&1&1&0&0&0&1&0&0&0&1&1&1&0&0&0&1&1\\
1&1&0&1&1&0&0&0&0&1&0&0&1&0&0&1&1&0&1&1\\
1&1&1&0&1&0&0&0&0&0&1&0&0&1&0&1&0&1&1&1\\
1&1&1&1&0&0&0&0&0&0&0&1&0&0&1&0&1&1&1&1
\end{array}\right] \\
LK_1^1 = \left[\ \overline{B_0^{(3,5)}}\ \middle|\ LK_1^0 - B_0^{(3,5)}\ \right] = \left[\begin{array}{cccccccc|cccccccccccc}
1&0&0&0&0&1&1&1&1&1&1&1&0&0&0&0&0&0&1&1\\
0&1&0&0&0&1&1&1&1&0&0&0&1&1&1&0&0&0&1&1\\
0&0&1&0&0&1&1&1&0&1&0&0&1&0&0&1&1&0&1&1\\
0&0&0&1&0&1&1&1&0&0&1&0&0&1&0&1&0&1&1&1\\
0&0&0&0&1&1&1&1&0&0&0&1&0&0&1&0&1&1&1&1
\end{array}\right] \\
LK_2^1 = \left[\ \overline{B_0^{(4,5)}}\ \middle|\ LK_2^0 - B_0^{(4,5)}\ \right] = \left[\begin{array}{cccccccccccccccccccc}
0&1&1&1&1&1&0&0&0&0&1&0&0&0&0&0&1&1&1&1\\
1&0&1&1&1&0&1&0&0&0&0&1&0&0&0&1&0&1&1&1\\
1&1&0&1&1&0&0&1&0&0&0&0&1&0&0&1&1&0&1&1\\
1&1&1&0&1&0&0&0&1&0&0&0&0&1&0&1&1&1&0&1\\
1&1&1&1&0&0&0&0&0&1&0&0&0&0&1&1&1&1&1&0
\end{array}\right] \\
LK_3^1 = \left[\ \overline{B_0^{(5,5)}}\ \middle|\ LK_3^0 - B_0^{(5,5)}\ \right] = \left[\begin{array}{cccccccccccccccc|cccc}
1&0&0&0&0&1&1&1&1&1&1&0&0&0&0&1&1&1&0&0\\
0&1&0&0&0&1&1&1&0&0&0&1&1&1&0&1&1&1&0&0\\
0&0&1&0&0&1&0&0&1&1&0&1&1&0&1&1&1&1&0&0\\
0&0&0&1&0&0&1&0&1&0&1&1&0&1&1&1&1&1&0&0\\
0&0&0&0&1&0&0&1&0&1&1&0&1&1&1&1&1&1&0&0
\end{array}\right]
\end{cases}
\tag{17}
$$

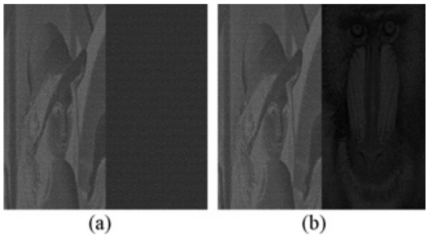


Fig. 9. Wang's (2, 3)-RIVCS. (a) Stacking any two shadows to gain first level secret (*Lena*). (b) All three shadows to gain second level secret (*Baboon*).

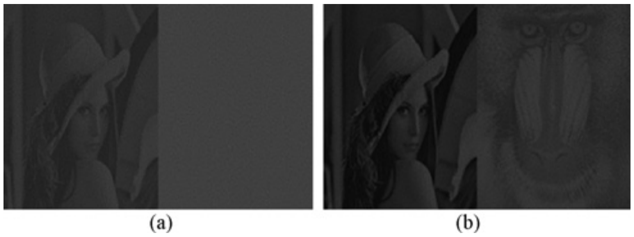


Fig. 10. Proposed (2, 3)-RIVCS. (a) Stacking any two shadows to gain first level secret (*Lena*). (b) All three shadows to gain second level secret (*Baboon*).

TABLE I

COMPARISON OF PIXEL EXPANSION

(k, n)-RIVCS		Proposed Scheme	Modified Scheme	Wang' Scheme
k = 2	n = 3	6	4	4
	n = 4	14	10	10
	n = 5	22	20	23
k = 3	n = 4	13	10	–
	n = 5	20	20	–
k = 4	n = 5	20	20	–

proposed (3, 5)-RIVCS. Since $\{B_{i_1}^{(3,5)} \cup B_{i_2}^{(4,5)} \cup B_{i_3}^{(5,5)}\}$ has minimal pixel expansion m=20 for i_1=i_2=i_1=0, the proposed (3, 5)-RIVCS is also the modified (3, 5)-RIVCS. Fig. 8 shows three reconstructed images with different security levels for our (3, 5)-RIVCS.

The secret image in all above experiments is a printed-text secret. Figs. 9 and 10 show that Wang's (2, 3)-RIVCS and the proposed (2, 3)-RIVCS use two halftoned photos (*Lena* and *Baboon*) as secret images for two regions. In stacking any two and three shadows, we can gain the first level secret (*Lena*) and second level secret (*Baboon*), respectively. It is observed that the color of the *Lena* image is reversed in Wang's (2, 3)-RIVCS (Fig. 9), while the proposed (2, 3)-RIVCS (Fig. 10) reveals these two photo images in correct contrast.

The pixel expansions of the proposed (k, n)-RIVCS, the modified (k, n)-RIVCS, and Wang's (2, n)-RIVCS, where $2 \leq k \leq 4$ and $3 \leq n \leq 5$, are illustrated in Table I. Although the proposed scheme has larger pixel expansion than the modified scheme, it shows correct colors for all regions. In comparing with Wang's scheme, our modified (2, 3)-RIVCS and (2, 4)-RIVCS have the same pixel expansion, and the modified (2, 5)-RIVCS has smaller pixel expansion. Contrasts of our modified (2, n)-RIVCS and Wang's (2, n)-RIVCS are shown in Table II, where the asterisk denotes better contrast. It is observed that our modified scheme has better contrasts for most cases.

TABLE II

COMPARISON OF CONTRAST

(k, n)-RIVCS		Security Level	Contrast of Our Modified Scheme (Wang' Scheme)			
			Stacking 2 Shadows	Stacking 3 Shadows	Stacking 4 Shadows	Stacking 5 Shadows
k = 2	n = 3	First	1/4 (1/4)	1/2* (1/4)	–	–
		Second	–	1/4 (1/4)	–	–
	n = 4	First	1/5 (1/5)	3/10 (3/10)	2/5* (3/10)	–
		Second	–	1/0 (1/10)	1/5* (1/10)	–
		Third	–	–	1/10 (1/10)	–
	n = 5	First	1/5* (4/23)	3/10* (6/23)	7/20* (7/23)	7/20* (7/23)
		Second	–	1/20* (1/23)	1/10 (3/23*)	3/20 (6/23*)
		Third	–	–	1/20* (1/23)	3/20* (3/23)
		Fourth	–	–	–	1/20* (1/23)
k = 3	n = 4	First	–	1/10	1/5	–
		Second	–	–	1/10	–
	n = 5	First	–	1/20	1/10	3/20
		Second	–	–	1/20	3/20
		Third	–	–	–	1/20
k = 4	n = 5	First	–	–	1/20	3/20
		Second	–	–	–	1/20

V. CONCLUSION

Our paper presented a systematic way to construct two types of (k, n)-RIVCSs for any values of k and n, where $k < n$. Also, we theoretically proved that our (k, n)-RIVCSs satisfy security and contrast conditions. The proposed (k, n)-RIVCS reveals correct colors for all regions, and the modified (k, n)-RIVCS has smaller shadow size and enhances the contrast.

APPENDIX

Base matrices used for constructing our (k, n)-RIVCS are shown below.

Naor and Shamir's (2, 4)-VCS

$$B_1^{(2,4)} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \qquad B_0^{(2,4)} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}.$$

Naor and Shamir's (3, 4)-VCS

$$B_1^{(3,4)} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 \end{bmatrix}$$

$$B_0^{(3,4)} = \begin{bmatrix} 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 \end{bmatrix}.$$

Naor and Shamir's (4, 4)-VCS

$$B_1^{(4,4)} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}$$

$$B_0^{(4,4)} = \begin{bmatrix} 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}.$$

Naor and Shamir's reversed (2, 5)-VCS

$$B_1^{(2,5)} = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 \end{bmatrix}$$

$$B_0^{(2,5)} = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 \end{bmatrix}.$$

Naor and Shamir's (3, 5)-VCS

$$B_1^{(3,5)} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

$$B_0^{(3,5)} = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

Droste's (4, 5)-VCS [45]

$$B_1^{(4,5)} = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

$$B_0^{(4,5)} = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \end{bmatrix}.$$

Naor and Shamir's (4, 5)-VCS

$$B_1^{(5,5)} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

$$B_0^{(5,5)} = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}.$$

REFERENCES

[1] M. Naor and A. Shamir, "Visual cryptography," in *Proc. Eurocrypt'94*, LNCS 950. 1995, pp. 1–12.

[2] R. Ito, H. Kuwakado, and H. Tanaka, "Image size invariant visual cryptography," *IEICE Trans. Fund. Elect. Commun. Comp. Sci.*, vol. E82-A, no. 10, pp. 2172–2177, 1999.

[3] C. N. Yang, "New visual secret sharing schemes using probabilistic method," *Pattern Recognit. Lett.*, vol. 25, no. 4, pp. 481–494, 2004.

[4] S. Cimato, R. De Prisco, and A. De Santis, "Probabilistic visual cryptography schemes," *Comput. J.*, vol. 49, no. 1, pp. 97–107, 2006.

[5] D. Wang, F. Yi, and X. Li, "Probabilistic visual secret sharing schemes for grey-scale images and color images," *Inform. Sci.*, vol. 181, no. 11, pp. 2189–2208, Jun. 2011.

[6] H. C. Wu and C. C. Chang, "Sharing visual multi-secrets using circle shares," *Comput. Standards Interfaces*, vol. 28, no. 1, pp. 123–135, Jul. 2005.

[7] S. J. Shyu, S. Y. Huang, Y. K. Lee, R. Z. Wang, and K. Chen, "Sharing multiple secrets in visual cryptography," *Pattern Recognit.*, vol. 40, no. 12, pp. 3633–3651, Dec. 2007.

[8] J. B. Feng, H. C. Wu, C. S, Tsai, Y. F. Chang, and Y. P. Chu, "Visual secret sharing for multiple secrets," *Pattern Recognit.*, vol. 41, no. 12, pp. 3572–3581, Dec. 2008.

[9] L. G. Fang, Y. M. Li, and B. Yu, "Multi-secret visual cryptography based on reversed images," in *Proc. Int. Conf. Inform. Comput.*, vol. 4. Jun. 2010, pp. 195–198.

[10] K. H. Lee and P. L. Chiu, "A high contrast and capacity efficient visual cryptography scheme for the encryption of multiple secret images," *Opt. Commun.*, vol. 284, no. 12, pp. 2730–2741, Jun. 2011.

[11] C. N. Yang and T. H. Chung, "A general multi-secret visual cryptography scheme," *Opt. Commun.*, vol. 283, no. 24, pp. 4949–4962, Dec. 2010.

[12] D. S. Tsai, T. H. Chen, and G. Horng, "A cheating prevention scheme for binary visual cryptography with homogeneous secret images," *Pattern Recognit.*, vol. 40, no. 8, pp. 2356–2366, Aug. 2007.

[13] C. N. Yang, A. G. Peng, and T. S. Chen, "MTVSS: (M)isalignment (t)olerant (v)isual (s)ecret (s)haring on resolving alignment difficulty," *Signal Process.*, vol. 89, no. 8, pp. 1602–1624, Aug. 2009.

[14] F. Liu, C. K. Wu, and X. J. Lin, "The alignment problem of visual cryptography schemes," *Designs Codes Cryptography*, vol. 50, no. 2, pp. 215–227, 2009.

[15] S. Cimato, A. DeSantis, A. L. Ferrara, and B. Masucci, "Ideal contrast visual cryptography schemes with reversing," *Inform. Process. Lett.*, vol. 93, no. 4, pp. 199–206, Feb. 2005.

[16] C. N. Yanh, C. C. Wang, and T. S. Chen, "Visual cryptography schemes with reversing," *Comput. J.*, vol. 51, no. 6, pp. 710–722, 2008.

[17] E. R. Verheul and H. C. A. Van Tilborg, "Constructions and properties of k out of n visual secret sharing scheme," *Designs Codes Cryptography*, vol. 11, no. 2, pp. 179–196, 1997.

[18] S. J. Shyu, "Efficient visual secret sharing scheme for color images," *Pattern Recognit.*, vol. 39, no. 5, pp. 866–880, May 2006.

[19] C. N. Yang and T. S. Chen, "Colored visual cryptography scheme based on additive color mixing," *Pattern Recognit.*, vol. 41, no. 10, pp. 3114–3129, Oct. 2008.

[20] C. C. Thien and J. C. Lin, "Secret image sharing," *Comput. Graph.*, vol. 26, no. 5, pp. 765–770, 2002.

[21] C. C. Thien and J. C. Lin, "An image-sharing method with user-friendly shadow images," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 13, no. 12, pp. 1161–1169, Dec. 2003.

[22] C. C. Lin and W. H. Tsai, "Secret image sharing with steganography and authentication," *J. Syst. Softw.*, vol. 73, no. 3, pp. 405–414, Nov.–Dec. 2004.

[23] C. N. Yang, T. S. Chen, K. H. Yu, and C. C. Wang, "Improvements of image sharing with steganography and authentication," *J. Syst. Softw.*, vol. 80, no. 7, pp. 1070–1076, Jul. 2007.

[24] C. C. Chang, Y. P. Hsieh, and C. H. Lin, "Sharing secrets in stego images with authentication," *Pattern Recognit.*, vol. 41, no. 10, pp. 3130–3137, Oct. 2008.

[25] C. N. Yang and C. B. Ciou, "A comment on sharing secrets in stego images with authentication," *Pattern Recognit.*, vol. 42, no. 7, pp. 1615–1619, Jul. 2009.

[26] Z. Eslami, S. H. Razzaghi, and J. Zarepour Ahmadabadi, "Secret image sharing with authentication-chaining and dynamic embedding," *J. Syst. Softw.*, vol. 84, no. 5, pp. 803–809, May 2011.

[27] R. Z. Wang and S. J. Shyu, "Scalable secret image sharing: Signal processing," *Image Commun.*, vol. 22, no. 4, pp. 363–373, 2007.

[28] C. N. Yang and S.-M. Huang, "Constructions and properties of k out of n scalable secret image sharing," *Opt. Commun.*, vol. 283, no. 9, pp. 1750–1762, 2010.

[29] C. N. Yang and Y. Y. Chu, "A general (k, n) scalable secret image sharing scheme with the smooth scalability," *J. Syst. Softw.*, vol. 84, no. 10, pp. 1726–1733, Oct. 2011.

[30] M. Naor and B. Pinkas, "Visual authentication and identification," in *Proc. CRYPTO*, LNCS 1294. 1997, pp. 322–336.

[31] J. M. McCune, A. Perrig, and M. K. Reiter, "Seeing-is-believing: Using camera phones for human-verifiable authentication," in *Proc. IEEE Symp. Security Privacy*, Nov. 2005, pp. 110–124.

[32] C. N. Yang and T. S. Chen, "Security analysis on authentication of images using recursive visual cryptography," *Cryptologia*, vol. 32, no. 2, pp. 131–136, Apr. 2008.

[33] B. Borchert, "Segment-based visual cryptography," Wilhelm-Schickard-Instit. Informatik, Univ. Tubingen, Tubingen, Germany, Tech. Rep. WSI-2007-04, 2007.

[34] S. Cimato and C. N. Yang, *Visual Cryptography and Secret Image Sharing*. Boca Raton, FL: CRC Press/Taylor and Francis, 2011.

[35] B. Surekha, G. Swamy, and K. S. Rao, "A multiple watermarking technique for images based on visual cryptography," *Int. J. Comput. Applicat.*, vol. 1, no. 11, pp. 77–81, 2010.

[36] T. Monoth and B. Anto P, "Tamperproof transmission of fingerprints using visual cryptography schemes," *Procedia Comput. Sci.*, vol. 2, pp. 143–148, Dec. 2010.

[37] J. Weir and W. Yan, "Resolution variant visual cryptography for street view of Google maps," in *Proc. ISCAS*, May–Jun. 2010, pp. 1695–1698.

[38] C. N. Yang, T. S. Chen, and M. H. Ching, "Embed additional private information into two-dimensional barcodes by the visual secret sharing scheme," *Integr. Comput.-Aided Eng.*, vol. 13, no. 2, pp. 189–199, 2006.

[39] R. Z. Wang, "Region incrementing visual cryptography," *IEEE Signal Process. Lett.*, vol. 16, no. 8, pp. 659–662, Aug. 2009.

[40] A. Shamir, "How to share a secret," *Commun. Assoc. Comput. Mach.*, vol. 22, no. 11, pp. 612–613, Nov. 1979.

[41] G. R. Blakley and C. Meadows, "Security of ramp schemes," in *Proc. Crypto'84*, LNCS 196. 1985, pp. 242–2695.

[42] K. Kurosawa, K. Okada, K. Sakano, W. Ogata, and T. Tsujii, "Nonperfect secret sharing schemes and matroids," in *Proc. Eurocrypt*, vol. 765. 1993, pp. 126–141.

[43] W. Ogata and K. Kurosawa, "Some basic properties of general nonperfect secret sharing schemes," *J. Universal Comput. Sci.*, vol. 4, no. 8, pp. 690–704, 1998.

[44] C. C. Lin and W. H. Tsai, "Visual cryptography for gray-level images by dithering techniques," *Pattern Recognit. Lett.*, vol. 24, nos. 1–3, pp. 349–358, Jan. 2003.

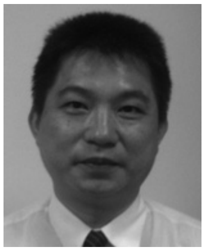
[45] S. Droste, "New results on visual cryptography," in *Proc. CRYPTO*, LNCS 1109. 1996, pp. 401–415.

Ching-Nung Yang (SM'11) received the B.S. and M.S. degrees, both from the Department of Telecommunication Engineering, National Chiao Tung University, Hsinchu, Taiwan, in 1983 and 1985, respectively, and the Ph.D. degree in electrical engineering from National Cheng Kung University, Tainan, Taiwan, in 1997.

From 1987 to 1989, and from 1990 to 1999, he was with the Telecommunication Laboratory and with the Training Institute Kaohsiung Center, Chunghwa Telecom Company, Ltd., Kaohsiung, Taiwan, respectively. He is currently a Full Professor with the Department of Computer Science and Information Engineering, National Dong Hwa University, Hualien, Taiwan. His current research interests include coding theory, information security, and cryptography.

Hsiang-Wen Shih is currently a Graduate Student with the Department of Computer Science and Information Engineering, National Dong Hwa University, Hualien, Taiwan.

His current research interests include visual cryptography and data hiding.



Chih-Cheng Wu is currently a Graduate Student with the Department of Computer Science and Information Engineering, National Dong Hwa University, Hualien, Taiwan.

His current research interests include visual cryptography, secret image sharing, and digital signature.

Lein Harn received the B.S. degree in electrical engineering from National Taiwan University, Taipei, Taiwan, in 1977, the M.S. degree in electrical engineering from the State University of New York, Stony Brook, in 1980, and the Ph.D. degree in electrical engineering from the University of Minnesota, Minneapolis, in 1984.

Currently, he is a Full Professor with the Department of Computer Science and Electrical Engineering, University of Missouri-Kansas City, Kansas City. His current research interests include cryptography, network security, and wireless communication security. He has published a number of papers on digital signature design and applications, wireless, and network security.