4-Colored Visual Cryptography Schemes with High Contrast

Miyuki Uno[1]*, Yukiko Ishibashi, and Mikio Kano[2] **

[1] University Education Center
Ibaraki University, Mito, Ibaraki, 310-8512 Japan
uno.miyuki@gmail.com
[2] Department of Computer and Information Sciences
Ibaraki University, Hitachi, Ibaraki, 316-8511 Japan
kano@mx.ibaraki.ac.jp

Abstract. In k-out-of-n visual cryptography scheme ((k, n)-VCS), the secret image is encoded into n shares and each share is printed on a transparency. Then the secret image can be obtained only by stacking k of the n shares, but we cannot get any information about the secret image from fewer than k shares. A colored VCS, in which the secret image is comprised of colored pixels, has been studied by some people, but known constructions lose a lot of contrast in reconstructed images. In this paper, we introduce a new colored VCS, which uses only four colors, black, white, red and green, and propose its construction with high contrast by using the property that a stacking of a red subpixel and a green subpixel results a black subpixel. We provide a construction of such a 4-colored $(2, n)$-VCS with contrast $1/(2n-1)$ for $n \geq 2$, and prove that these contrasts are sharp. Moreover, we show that the pixel expansion of our construction are also sharp.

Keywords: visual cryptography scheme, colored VCS, 4-colored VCS, high contrast VCS

1 Introduction

A visual cryptography scheme (VCS) was introduced by Naor and Shamir [8] in 1994. Since then, it have been studied in many papers including [1], [2], [5], [6], [7], [9].

A VCS is a special kind of secret sharing scheme in which the secret is an image comprised of black and white pixels and encoded into n shares, where each share is usually printed on a transparency. In k-out-of-n VCS ((k, n)-VCS), the secret image can be obtained only by stacking k of the n shares, but we cannot get any information about the secret image from fewer than k shares.

* Research is supported by Grant-in-Aid for Scientific Research of Japan.
** Research is supported by Grant-in-Aid for Scientific Research of Japan.

A colored VCS, in which the secret image is comprised of colored pixels, has been studied by some people, but known constructions lose a lot of contrast in reconstructed images. For example, the colored $(2, n)$-VCS given in [7] has contrast $2/kn(n-1)$, where k is the number of colors. In this paper, we introduce a new colored VCS that uses only four colors, black, white, red and green, and has the property that a stacking of a red subpixel and a green subpixel results a black subpixel. This colored VCS is called a *4-colored* VCS. Then we provide constructions of a 4-colored $(2, n)$-VCS with contrast $1/(2n-1)$, and show that these contrasts are sharp. An example of such a construction is given in the appendix.

We explain the above 4-colored VCS more precisely. The secret image is comprised of pixels, and each pixel is colored with four colors, black, white, red or green. Each pixel is split into m subpixels in a share, and the number m is called the *pixel expansion*. Each subpixel of every share is also colored with four colors, black, white, red or green, where white means transparency. The color of each subpixel of a reconstructed image is determined by the following rule.

For convenience, we denote the four colors, black, white, red and green by 1, 0, R and G, respectively. Then for any $X, Y \in \{0, 1, R, G\}$, it follows that

$$X + Y = Y + X, \qquad X + X = X,$$
$$0 + X = X, \qquad 1 + X = 1 \qquad \text{and} \qquad R + G = 1,$$

where $X + Y$ denotes the color of a subpixel of stacking two subpixels with color X and Y, respectively. When we stack more than two shares, the color of each subpixel of a reconstructed image is determined by applying the above rule one by one, and its color is independent of the order of stacking shares. It is known that "red+green=black", and actually it is useful among high school students in Japan. A student marks some important parts of the text book by a special red marker (or a green marker), and put a green transparency sheet (or a red one) on the text book, then he can read the text not colored by a marker but cannot read the colored parts, and tries to check whether he memorizes the important parts or not, and if he removes the colored transparency sheet, he can read all the text.

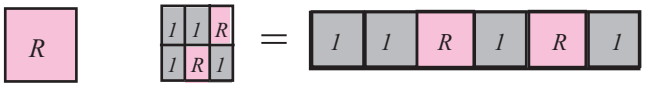
When we consider a construction of a 4-colored VCS, we require the following properties.

(a) Every black pixel of the secret image is recovered into a pure black region, whose all subpixels are black in a reconstructed image.

(b) Every pixel colored with white, red or green of the secret image is recovered into a region whose subpixels are colored with black or the pixel's color (see Figure 1).

If a construction of a colored VCS has the property (a), then it is called a *perfect black construction*, and if a construction possesses the two properties (a) and (b), then it is called a *perfect colored construction.* In [1], a similar colored VCS using four colors or six colors is considered, but the condition (b) is not required. So a pixel of a secrete image with color C is recovered into regions whose

some number of subpixels are colored with C but the remaining subpixels are colored with any other colors, that is, the remaining subpixels are not necessary to be black. This is different from our method. In this paper, we deal with only perfect colored constructions since they have some advantage in recognition by eyes. So a construction of a 4-colored VCS means its perfect colored construction.



(1) (2) (3)

Fig. 1. (1) A red pixel of the secret image; (2) the corresponding region of a reconstructed image, which consists of 2 red subpixels and 4 black subpixels; and (3) a representation of (2) used in this paper, where 1 means black.

We now explain the contrast of a perfect colored construction of 4-colored VCS. Consider a construction of a 4-colored VCS with pixel expansion m. We say that the construction has a *contrast* δ if for every pixel P of the 4-colored secret image, at least δm subpixels of the region in a reconstructed image corresponding to P are colored with the color of P, and there exists at least one pixel for which exactly δm subpixels of the region are colored with the color of P. It is well-known that if the contrast becomes higher or the pixel expansion becomes smaller, then VCS becomes clearer and better.

This paper is organized as follows: In Sect. 2, two constructions of a 4-colored $(2, 2)$-VCS with contrast $1/3$ are given, and the sharpness of these contrast is shown. In Sect. 3, for every integer $n \geq 3$, a construction of a 4-colored $(2, n)$-VCS with contrast $1/(2n-1)$ and pixel expansion $2n-1$ is provided, and their sharpness is proved.

2 Preliminaries and a 4-colored (2,2)-VCS

We first introduce some notation and definitions. We consider a 4-colored (k, n)-VCS and its perfect colored construction. We denote n shares by $Share(1), \ldots,$ $Share(n)$. Each pixel of the secret image is colored with four colors, black, white, red or green, and is split into m subpixels in each share. The integer m is called the pixel expansion of the VCS, and m always denotes the pixel expansion. For convenience, we consider any fixed pixel P of the secret image. The color of P is denoted by $color(P)$ and the set of subpixels of $Share(i)$ corresponding to the pixel P is written $S(i)$. Then the pixel P corresponds to the $m \times n$ subpixels $S(1) \cup S(2) \cup \cdots \cup S(n)$. These mn subpixels can be expressed by a $m \times n$ $(0, 1, R, G)$-matrix $B = [b_{ij}]$, where $b_{ij} = X$ if the j-th subpixel of $S(i)$ is colored with X, where $X \in \{0, 1, R, G\}$. Namely, the i-th row vector of B corresponds

to $S(i)$, and $S(i)$ is also used to denote the i-th row vector of B. The matrix B is called the *basis matrix* of a construction of VCS.

Now consider a 4-colored $(2, 2)$-VCS. Define $S(1)$ and $S(2)$ as follows.

$$\begin{array}{lll} S(1) = [\ 0\ R\ 1\ ] & & \\ S(2) = [\ 0\ 1\ G\ ] & \text{if} & color(P) = 0, \\ S(2) = [\ 1\ 0\ G\ ] & \text{if} & color(P) = R, \\ S(2) = [\ G\ 1\ 0\ ] & \text{if} & color(P) = G, \\ S(2) = [\ 1\ G\ 0\ ] & \text{if} & color(P) = 1. \end{array}$$

Then the above $S(i)$'s give a perfect colored construction of a 4-colored $(2, 2)$-VCS with $m = 3$ since if P is white, then $S(1) + S(2) = [011]$, if P is red, then $S(1) + S(2) = [1R1]$, if P is green, then $S(1) + S(2) = [G11]$, and if P is black, then $S(1) + S(2) = [111]$. Obviously, the contrast of this construction is $1/3$ and the pixel expansion is 3.

One may requires that for each color $X \in \{0, 1, R, G\}$, every $S(i)$ contains the same number of subpixels colored with X. Such a construction with contrast $1/3$ and pixel expansion 6 are given below. Define $S(1)$ and $S(2)$ as follows.

$$\begin{array}{lll} S(1) = [\ 0\ 0\ R\ G\ 1\ 1\ ] & & \\ S(2) = [\ 0\ 0\ 1\ 1\ R\ G\ ] & \text{if} & color(P) = 0, \\ S(2) = [\ R\ 1\ 0\ 1\ 0\ G\ ] & \text{if} & color(P) = R, \\ S(2) = [\ 1\ G\ 1\ 0\ 0\ R\ ] & \text{if} & color(P) = G, \\ S(2) = [\ 1\ 1\ G\ R\ 0\ 0\ ] & \text{if} & color(P) = 1. \end{array}$$

Then the above $S(i)$'s give a perfect colored construction of a 4-colored $(2, 2)$-VCS with $m = 6$. For example, if P is white, then $S(1) + S(2) = [001111]$, and if P is red, then $S(1) + S(2) = [R1R111]$.

When the above constructions are adapted to encode the secret image into shares, for each pixel P, the m entries of both $S(1)$ and $S(2)$ are randomly permuted, and the resulting two row vectors are used. By this method, the construction is secure since $S(i)$ contains a constant number of subpixels colored with X for every color X. Moreover, when one uses the first construction and wants to keep color balance of red and green in each share, he/she should first randomly permute $\{S(1), S(2)\}$ for each pixel, and use the first $S(i)$ for $Share(1)$ and the second $S(j)$ for $Share(2)$, then each share contains almost the same numbers of red and green subpixels.

It is easy to see that there exists no construction of 4-colored (2,2)-VCS with pixel expansion 2 because of 4 colors. Hence the pixel expansion 3 is sharp. We now prove the sharpness of the contrast in the following theorem. The first statement is already shown above.

Theorem 1. *There are two perfect colored constructions of 4-colored $(2, n)$-VCS with contrast 1/3 and pixel expansion 3 and 6, respectively. Moreover, there exists no perfect colored constructions of 4-colored $(2, n)$-VCS with contrast greater than 1/3.*

Proof. Assume that there exists a perfect colored construction of 4-colored $(2,2)$-VCS with contrast greater than $1/3$. Suppose that each pixel is split into m subpixels.

Let $0_i, 1_i, R_i, G_i \subset \{1, 2, \ldots, m\}$ denote the sets of places of white subpixels, black subpixels, red subpixels and of green subpixels of $S(i)$, respectively, where $i \in \{1, 2\}$. Namely, for every color $X \in \{0, 1, R, G\}$, let

$$X_i = \{k \mid \text{the } k\text{-th subpixel (entry) of } S(i) \text{ is } X\} \subset \{1, 2, \ldots, m\}.$$

Let $|X_i|$ denote the number of elements contained in X_i, which is equal to the number of subpixels of $S(i)$ colored with X. Then

$$m = |0_i| + |1_i| + |R_i| + |G_i| \qquad \text{for every } i \in \{1, 2\}. \tag{1}$$

Let

$$\lambda = \min\{|0_1 \cap 0_2| \text{ when } color(P) = 0; \quad |0_1 \cap X_2| + |X_1 \cap 0_2| + |X_1 \cap X_2| \text{ when } color(P) = X, \text{ and } X \text{ runs over } \{R, G\}\ \}. \ (see\ Fig.2)$$

Since the contrast is greater than $1/3$, we have

$$\frac{\lambda}{m} > \frac{1}{3} \qquad \text{and} \qquad m < 3\lambda. \tag{2}$$

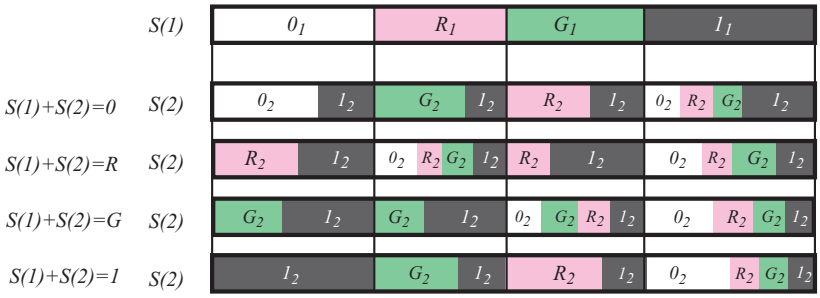


Fig. 2. Two Shares $S(1)$ and $S(2)$ in a construction.

By considering the case where $color(P)$ is white, red, green or black, we have the following from Figure 2.

$$|0_1 \cap 0_2| \geq \lambda, \tag{3}$$
$$|0_1 \cap R_2| + |R_1 \cap (0_2 \cup R_2)| \geq \lambda, \tag{4}$$
$$|0_1 \cap G_2| + |G_1 \cap (0_2 \cup G_2)| \geq \lambda, \tag{5}$$
$$|1_1| \geq |0_2|, \tag{6}$$
$$|1_2| \geq |0_1|. \tag{7}$$

By (3) and (6), we have $|0_1| \geq \lambda$ and $|1_1| \geq |0_2| \geq \lambda$, which implies by (2) that

$$|R_1| + |G_1| = m - (|0_1| + |1_1|) < 3\lambda - (\lambda + \lambda) = \lambda. \tag{8}$$

Then by (8), (4) and (5), we obtain

$$\begin{aligned} \lambda &> |R_1| + |G_1| \geq |R_1 \cap (0_2 \cup R_2)| + |G_1 \cap (0_2 \cup G_2)| \\ &\geq \lambda - |0_1 \cap R_2| + \lambda - |0_1 \cap G_2| \end{aligned}$$

Hence $|0_1 \cap R_2| + |0_1 \cap G_2| > \lambda$. By (3), (7) and by this inequality, this implies that

$$m = |0_2| + |1_2| + |R_2| + |G_2| \geq \lambda + \lambda + |0_1 \cap R_2| + |0_1 \cap G_2| > 3\lambda.$$

This contradicts (2). Therefore the contrast 1/3 is sharp. □

3 4-colored $(2, n)$-VCS for $n \geq 3$

In this section, for every integer $n \geq 3$, we provide two constructions of 4-colored $(2, n)$-VCS with contrast $1/(2n-1)$, and show that this contrast is sharp.

We first propose a perfect colored construction of 4-colored $(2, n)$-VCS with contrast $1/(2n-1)$ and pixel expansion $2n-1$. Then every pixel is split into $2n-1$ subpixels, and for every $2 \leq i \leq n$, $S(i)$ consists of one 0, one R, one G and $2n-4$ 1's.

We consider any fixed pixel P of the secret image. First define $S(1)$ as follows, which is fixed in the following construction.

$$S(1) \ = \ [0, \underbrace{1, 1, 1, ..., 1}_{2n-2}].$$

If the pixel P is white, then define $S(i)$ as

$$S(i) = [0, \underbrace{1 \ldots, 1}_{i-2}, R, G, \underbrace{1, \ldots, 1}_{2n-i-2}] \qquad \text{for all } \ 2 \leq i \leq n,$$

where R and G are placed at the i-th entry and the $(i+1)$-th entry of $S(i)$, respectively. If P is red, then define

$$S(i) \ = [R, \underbrace{1, \ldots, 1}_{i-2}, G, \underbrace{1, \ldots, 1}_{n-2}, 0, \underbrace{1, \ldots, 1}_{n-i}] \qquad \text{for all } \ 2 \leq i \leq n,$$

where G and 0 are the i-th entry and the $(n+i-1)$-th entry of $S(i)$, respectively. If P is green, then

$$S(i) \ = [G, \underbrace{1 \ldots, 1}_{i-2}, R, \underbrace{1, \ldots, 1}_{n-2}, 0, \underbrace{1, \ldots, 1}_{n-i}] \qquad \text{for all } \ 2 \leq i \leq n,$$

where R and 0 are the i-th entry and the $(n+i-1)$-th entry of $S(i)$, respectively. If P is black, then define

$$S(n) = [1, G, \underbrace{1, \ldots, 1}_{n-3}, R, \underbrace{1, \ldots, 1}_{n-2}, 0],$$

where R is the n-th entry of $S(n)$, and

$$S(i) = [\underbrace{1, \ldots, 1}_{i-1}, R, G, \underbrace{1, \ldots, 1}_{n-3}, 0, \underbrace{1, \ldots, 1}_{n-i}] \qquad \text{for all } \ 2 \le i \le n-1,$$

where R, G and 0 are the i-th entry, the $(i+1)$-th entry, and the $(n+i-1)$-th entry of $S(i)$, respectively.

For example if $n = 4$, then the basis matrix B, whose i-th row vector is $S(i)$, is determined as follows.

$$B = \begin{bmatrix} S(1) \\ S(2) \\ S(3) \\ S(4) \end{bmatrix} = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & R & G & 1 & 1 & 1 & 1 \\ 0 & 1 & R & G & 1 & 1 & 1 \\ 0 & 1 & 1 & R & G & 1 & 1 \end{bmatrix} \qquad \text{if } P \text{ is white,}$$

$$B = \begin{bmatrix} S(1) \\ S(2) \\ S(3) \\ S(4) \end{bmatrix} = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ R & G & 1 & 1 & 0 & 1 & 1 \\ R & 1 & G & 1 & 1 & 0 & 1 \\ R & 1 & 1 & G & 1 & 1 & 0 \end{bmatrix} \qquad \text{if } P \text{ is red,}$$

$$B = \begin{bmatrix} S(1) \\ S(2) \\ S(3) \\ S(4) \end{bmatrix} = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ G & R & 1 & 1 & 0 & 1 & 1 \\ G & 1 & R & 1 & 1 & 0 & 1 \\ G & 1 & 1 & R & 1 & 1 & 0 \end{bmatrix} \qquad \text{if } P \text{ is green, and}$$

$$B = \begin{bmatrix} S(1) \\ S(2) \\ S(3) \\ S(4) \end{bmatrix} = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & R & G & 1 & 0 & 1 & 1 \\ 1 & 1 & R & G & 1 & 0 & 1 \\ 1 & G & 1 & R & 1 & 1 & 0 \end{bmatrix} \qquad \text{if } P \text{ is black.}$$

Then, for every $n \ge 3$ and for all i, j, $1 \le i < j \le n$, it follows that

$$\begin{aligned} S(i) + S(j) &= [0, 1, 1, \ldots, 1] && \text{if } P \text{ is white,} \\ S(i) + S(j) &= [R, 1, 1, \ldots, 1] && \text{if } P \text{ is red,} \\ S(i) + S(j) &= [G, 1, 1, \ldots, 1] && \text{if } P \text{ is green, and} \\ S(i) + S(j) &= [1, 1, 1, \ldots, 1] && \text{if } P \text{ is black.} \end{aligned}$$

Therefore the above $\{S(i)\}$ gives a perfect colored construction of 4-colored $(2, n)$-VCS.

We now show that the pixel expansion $2n - 1$ is best possible. Namely, we prove the next theorem.

Theorem 2. *Let $n \ge 3$ be an integer. Then there exists no perfect colored construction of a 4-colored $(2, n)$-VCS with pixel expansion less than $2n - 1$.*

Proof. Assume that there exists a perfect colored construction of 4-colored $(2, n)$-VCS with pixel expansion m. We consider any fixed pixel P of the secret image. For every $1 \leq i \leq n$, let $0_i, 1_i, R_i, G_i \subset \{1, 2, \ldots, m\}$ denote the set of places of white subpixels, black subpixels, red subpixels and green subpixels of $S(i)$, respectively. So for every color $X \in \{0, 1, G, R\}$,

$$X_i = \{k \mid \text{the } k\text{-th entry of } S(i) \text{ is } X\} \subset \{1, 2, \ldots, m\}.$$

By considering the case where $color(P)$ is white, it is clear that

$$|0_i| \geq 1 \qquad \text{for all} \quad 1 \leq i \leq n. \tag{9}$$

Without loss of generality, we may assume that $|G_1| \leq |G_i|$ for all $2 \leq i \leq n$. If $|G_1| = 0$, then by considering the case where $color(P)$ is green, $S(1) + S(i)$ recovers green and so $|G_i| \geq 1$. Thus

$$|G_i| \geq 1 \qquad \text{for all} \quad 2 \leq i \leq n. \tag{10}$$

If $color(P)$ is black, then $0_i \cup G_i \subseteq R_1 \cup 1_1$ for every $2 \leq i \leq n$ since $S(i) + S(1)$ recovers black. Moreover, for two distinct integer $i, j \in \{2, \ldots, n\}$, it follows that $(G_i \cup 0_i) \cap (G_j \cup 0_j) = \emptyset$ since $S(i) + S(j)$ recovers black. Hence

$$|0_2| + |0_3| + \cdots + |0_n| + |G_2| + |G_3| + \cdots + |G_n| \leq |R_1| + |1_1|. \tag{11}$$

Therefore by (11), (9) and (10), we obtain

$$m = |0_1| + |G_1| + |R_1| + |1_1| \geq \sum_{i=1}^{n} (|0_i| + |G_i|) \geq 2n - 1.$$

Consequently Theorem 2 is proved. □

Theorem 3. *Let $n \geq 3$ be an integer. Then there exists no perfect colored construction of 4-colored $(2, n)$-VCS with contrast greater than $1/(2n - 1)$.*

Proof. Assume that there exists a perfect colored construction of 4-colored $(2, n)$-VCS with pixel expansion m. Consider any fixed pixel P of the secret image. For every $X \in \{0, 1, R, G\}$ and every $1 \leq i \leq n$, let X_i denote the subset of $\{1, 2, \ldots, m\}$ defined as in the proof of Theorem 2. Let

$$\begin{aligned} \lambda = \min_{i,j,X} \{&\text{the number of subpixels of } S(i) + S(j) \text{ colored with } X \\ &\text{when } color(P) = X, \text{ where } X \text{ runs over } \{0, R, G\}, \text{ and} \\ &i \text{ and } j \text{ run over } \{1, 2, \ldots, n\} \text{ with } i \neq j\}. \end{aligned}$$

Hence if the pixel P is colored with $X \in \{R, G\}$, then

$$|X_i \cap 0_j| + |0_i \cap X_j| + |X_i \cap X_j| \geq \lambda \tag{12}$$

since $S(i) + S(j)$ recovers color X.

By considering the case where P is white, we have $|0_1 \cap 0_i| \geq \lambda$ for all $2 \leq i \leq n$, which implies

$$|0_i| \geq \lambda \qquad \text{for all } \ 1 \leq i \leq n. \tag{13}$$

Consider the case where P is red. Then it follows from (12) that

$$|R_1 \cap 0_i| + |R_i| \geq |R_1 \cap 0_i| + |0_1 \cap R_i| + |R_1 \cap R_i| \geq \lambda. \tag{14}$$

Moreover, since $0_i \cap 0_j = \emptyset$ for all $2 \leq i < j \leq n$, we have

$$\begin{aligned} |R_1| &\geq |R_1 \cap (0_2 \cup 0_3 \cup \cdots \cup 0_n)| \\ &= |R_1 \cap 0_2| + |R_2 \cap 0_3| + \cdots + |R_1 \cap 0_n|. \end{aligned} \tag{15}$$

Finally consider the case where P is black. Then 0_i and R_i are contained in $G_1 \cup 1_1$ for every $2 \leq i \leq n$, and if $i \neq j$, then $(0_i \cup R_i) \cap (0_j \cup R_j) = \emptyset$ since $S(i) + S(j)$ recovers a complete black region. Thus

$$|G_1| + |1_1| \geq |0_2| + |R_2| + \cdots + |0_n| + |R_n|. \tag{16}$$

Therefore

$$\begin{aligned} m &= |0_1| + |R_1| + |G_1| + |1_1| \\ &\geq |0_1| + |R_1| + \sum_{i=2}^{n} (|0_i| + |R_i|) && \text{(by (16))} \\ &\geq \sum_{i=1}^{n} |0_i| + \sum_{i=2}^{n} (|R_1 \cap 0_i| + |R_i|) && \text{(by (15))} \\ &\geq \lambda n + (n-1)\lambda = (2n-1)\lambda. && \text{(by (13) and (14))} \end{aligned}$$

This implies

$$\frac{\lambda}{m} \leq \frac{1}{2n-1}.$$

Consequently Theorem 3 is proved. □

We finally give another perfect colored construction of 4-colored VCS with contrast $1/(2n-1)$, in which every share $S(i)$ contains a constant number of subpixels colored with X for every color $X \in \{0, 1, R, G\}$. So all shares seem to be same, and hence it might be useful in some situation though its pixel expansion is $n(2n-1)$ and large.

We consider any fixed pixel P of the secret image. For simplicity, we define $S(i)$ as follows depending on the color of P. Note that every $S(i)$ contains precisely n 0's, $n-1$ R's, $n-1$ G's and $2(n-1)^2$ 1's.

If the pixel P is white, then define

$$S(1) = [\underbrace{0, \ldots, 0}_{n}, \underbrace{R, \ldots, R}_{n-1}, \underbrace{G, \ldots, G}_{n-1}, \underbrace{1, \ldots, 1}_{2(n-1)^2}],$$

$$S(i) = [\underbrace{0, \ldots, 0}_{n}, \underbrace{1, \ldots, 1}_{(n-1)(i-1)}, \underbrace{R, \ldots, R}_{n-1}, \underbrace{G, \ldots, G}_{n-1}, \underbrace{1, \ldots, 1}_{(n-1)(2n-i-1)}]$$

for all $\ 2 \leq i \leq n$.

If P is red, then define

$$\begin{aligned} S(1) &= [0, \underbrace{R, \ldots, R}_{n-1}, \underbrace{G, \ldots, G}_{n-1}, \underbrace{0, \ldots, 0}_{n-1}, \underbrace{1, \ldots, 1}_{2(n-1)^2}] \\ S(i) &= [\underbrace{R, \ldots, R}_{i-1}, 0, \underbrace{R, \ldots, R}_{n-i}, \underbrace{1, \ldots, 1}_{2(n-1)(i-1)}, \underbrace{G, \ldots, G}_{n-1}, \underbrace{0, \ldots, 0}_{n-1}, \underbrace{1, \ldots, 1}_{2(n-1)(n-i)}] \end{aligned}$$

for all $2 \le i \le n$. If P is green, then $S(i)$ is determined as in the case where P is red, and so we omit it. Assume that P is black. Let $\mathbf{T} = [R, G, 1, \ldots, 1]$, which consists of one R, one G and $n-2$ 1's. Then

$$\begin{aligned} S(1) &= [\underbrace{\mathbf{T}, \mathbf{T}, \ldots, \mathbf{T}}_{n-1}, \underbrace{0, 0, \ldots, 0}_{n}, \underbrace{1, 1, \ldots, 1}_{n(n-1)}] \\ &= [R, G, 1, \ldots, 1, R, G, 1, \ldots, 1, \cdots, R, G, 1 \ldots, 1, \underbrace{0, \ldots, 0}_{n}, \underbrace{1, \ldots, 1}_{n(n-1)}], \end{aligned}$$

which consists of $n-1$ $\mathbf{T}$'s, n 0's and $n(n-1)$ 1's. Then by shifting every entry of $[\mathbf{T}, \mathbf{T}, \ldots, \mathbf{T}]$ to one space to the right, and by moving the last entry to the first entry, we obtain $\mathbf{Q}(1)$. By applying the same procedure i times to $[\mathbf{T}, \mathbf{T}, \ldots, \mathbf{T}]$, we obtain $\mathbf{Q}(i)$. Then $S(i)$ is defined by

$$S(i) = [\mathbf{Q}(i), \underbrace{1, \ldots, 1}_{n(i-1)}, \underbrace{0, \ldots, 0}_{n}, \underbrace{1, \ldots, 1}_{n(n-i)}] \qquad \text{for all } \ 2 \le i \le n-1,$$

where $|\mathbf{Q}(i)| = (n-1)n$.

For example if $n = 3$, then $\mathbf{T} = [RG1RG1]$ and $S(i)$'s are determined as follows.

$$B = \begin{bmatrix} 0\,0\,0\,R\,R\,G\,G\,1\ \ 1\ \ 1\ \ 1\,1\,1\,1 \\ 0\,0\,0\,1\ \ 1\ R\,R\,G\,G\,1\ \ 1\,1\,1\,1\,1 \\ 0\,0\,0\,1\ \ 1\ \ 1\ \ 1\ R\,R\,G\,G\,1\,1\,1\,1 \end{bmatrix} \quad \text{if } P \text{ is white,}$$

$$B = \begin{bmatrix} 0\ R\,R\,G\,G\,0\,0\,1\ \ 1\,1\,1\,1\ \ 1\,1\,1 \\ R\ 0\ R\,1\ \ 1\,1\,1\,G\,G\,0\,0\,1\ \ 1\,1\,1 \\ R\,R\ 0\ \ 1\ \ 1\,1\,1\,1\ \ 1\,1\,1\,G\,G\,0\,0 \end{bmatrix} \quad \text{if } P \text{ is red,}$$

$$B = \begin{bmatrix} 0\ G\,G\,R\,R\,0\,0\,1\ \ 1\,1\,1\,1\ \ 1\,1\,1 \\ G\ 0\ G\,1\ \ 1\,1\,1\,R\,R\,0\,0\,1\ \ 1\,1\,1 \\ G\,G\ 0\ \ 1\ \ 1\,1\,1\,1\ \ 1\,1\,1\,R\,R\,0\,0 \end{bmatrix} \quad \text{if } P \text{ is green, and}$$

$$B = \begin{bmatrix} R\,G\ 1\ R\,G\ 1\ 0\,0\,0\,1\,1\,1\,1\,1\,1 \\ 1\ R\,G\ 1\ R\,G\,1\,1\,1\,0\,0\,0\,1\,1\,1 \\ G\ 1\ R\,G\ 1\ R\,1\,1\,1\,1\,1\,1\,0\,0\,0 \end{bmatrix} \quad \text{if } P \text{ is black.}$$

Notice that if $n = 4$ and P is black, then $\mathbf{T} = [RG11RG11RG11]$ and

$$B = \begin{bmatrix} R\,G\;1\;1\;R\,G\;1\;1\;R\,G\;1\;1\;0\,0\,0\,0\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1 \\ 1\;R\,G\;1\;1\;R\,G\;1\;1\;R\,G\;1\;1\,1\,1\,1\,0\,0\,0\,0\,1\,1\,1\,1\,1\,1\,1 \\ 1\;1\;R\,G\;1\;1\;R\,G\;1\;1\;R\,G\;1\,1\,1\,1\,1\,1\,1\,1\,0\,0\,0\,0\,1\,1\,1\,1 \\ G\;1\;1\;R\,G\;1\;1\;R\,G\;1\;1\;R\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,0\,0\,0\,0 \end{bmatrix}$$

We can easily see that the above $S(i), 1 \leq i \leq n$, give a perfect colored construction of 4-colored VCS with contrast $1/(2n-1)$ since for every color $X \in \{0, G, R\}$, $S(i) + S(j)$ recovers a region containing precisely n subpixels colored with X and $m = n(2n-1)$.

4 Conclusion

We proposed a new colored VCS, called 4-colored VCS, and gave perfect colored constructions of 4-colored $(2, n)$-VCS. Then we showed that their contrasts are optimal and also some of their pixel expansion are also optimal. Finding a construction of perfect colored construction of 4-colored (k, n)-VCS with $3 \leq k \leq n$ is a future work and an open problem.

References

1. A. Adhikari and S. Sikdar " A new (2,n)-visual threshold scheme for color images", Progress in Cryptology-Indocrypt 2003 (LNCS 2904), (2003) 148–161
2. G. Ateniese, C. Blundo, A. De Santis, and D.R. Stinson, "Visual cryptography for general access structures," Information and Computation, vol.129 (1996) 86-106.
3. C. Blundo, A. De. Bonis and A. De. Santis, "Improved schemes for visual cryptography," Designs, Codes and Cryptography," vol. 24 (2001) 255–278.
4. C. Blundo, A.De Santis, and D.R. Stinson, "On the Contrast in Visual Cryptography Schemes," J. Cryptology, vol. 12 (1999) 261–289.
5. C. Blundo and A. De Santis, "Visual cryptography schemes with perfect reconstruction of black pixels," Computer and Graphics, vol.22, no.4, (1998) pp.449-455.
6. S. Droste, "New results on visual cryptography," Advances in Cryptology-CRYPTO'96, LNCS, vol. 1109 (1996), 401–415.
7. H. Koga and H. Yamamoto, "Proposal of a lattice-based visual secret sharing scheme for color and gray-scale images, IEICE Trans. Fundamentals, Vol. E81-A, (1998) 1262–1269 (2006) 81–102.
8. M. Naor and A. Shamir, "Visual cryptography," Advances in Cryptology, Eurocrypt'94, LNCS, vol. 950 (1994) 1–12.
9. F. Yi, D. Wang, P. Luo, L. Huang, Y. Dai, "Multi secret image color visual cryptography schemes for general access structures," Progr. Natur. Sci. (English Ed.) 16 (2006), no. 4, 431–436.

A Appendix: A construction of a 4-colored (2,3)-VCS

A construction of a 4-colored (2,3)-VCS with contrast 1/5 and pixel expansion 5 is shown below. By our construction, $S(1)+S(2)$, $S(2)+S(3)$ and $S(1)+S(3)$ recover exactly the same reconstructed images.

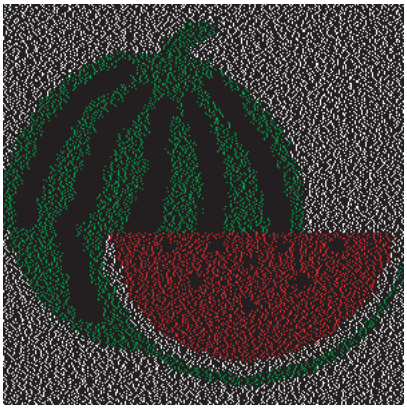


Fig. 3. A reconstructed image $S(1) + S(2)$.

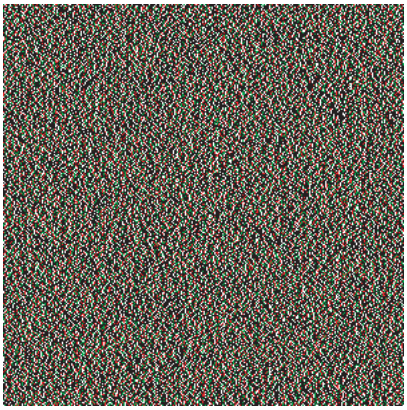


Fig. 4. A share $S(1)$, and other shares $S(2)$ and $S(3)$ are similar to $S(1)$.