Visual Card Games for Two Parties

Miyuki Uno[1] 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 http://gorogoro.cis.ibaraki.ac.jp/

Abstract

We propose a visual card game for two disjoint parties $\mathcal{X}$ and $\mathcal{Y}$ of boys and girls, respectively. In this game every boy and girl receives a *card*, and when a boy and a girl stack their card together, a hidden secret image is recovered. This game is called *a visual card game of* $K(|\mathcal{X}|, |\mathcal{Y}|)$*-type*, where $K(n, m)$ denotes the complete bipartite graph. We propose constructions of the visual card game of $K(2, n)$-type with contrast $1/4$, and that of $K(r, s)$-type with contrast $6/(11r)$ for $3 \leq r$ are provided. Next we prove that the contrasts of these constructions are sharp if $2 \leq r \leq 6$. Moreover, another construction of visual card game of $K(r, s)$-type with pixel expansion $2r$ and contrast $1/(2r)$ is proposed for all $1 \leq r < s$, and it is shown that this pixel expansion is sharp.

Keywords: visual card game, card game for two groups, visual cryptography scheme

1 Introduction

In this paper, we propose a new card game for two parties $\mathcal{X}$ and $\mathcal{Y}$ of boys and girls, respectively. In this game, every boy and girl receives a card printed on a transparency, and when a boy and a girl stack their card together, a secret image is recovered, namely, they can recognize a hidden secret image by their eyes. This game is called a *visual card game for boys and girls* or

a *visual card game of* $K(|\mathcal{X}|, |\mathcal{Y}|)$*-type*, where $K(n, m)$ denotes a complete bipartite graph.

We explain the visual card game for boys and girls more precisely. Let r and s be positive integers. Let $\mathcal{X} = \{X_1, X_2, \cdots, X_r\}$ and $\mathcal{Y} = \{Y_1, Y_2, \cdots, Y_s\}$ denote the sets of boys and girls, respectively, and $Image(i, j)$ $(1 \leq i \leq r,\ 1 \leq j \leq s)$ be rs secret images, which are comprised of black and white pixels. Each participant X_i and Y_j has a card X_i and Y_j, respectively, where we use the same notation for a participant and his/her card. Each card is printed on a transparency, and is comprised of black pixels and transparent pixels.

We encode the given rs secret images $Image(i, j)$'s into the $r + s$ cards X_i's and Y_j's so that a stack of two cards X_a and Y_b recovers the secret image $Image(a, b)$ for all $1 \leq a \leq r$ and $1 \leq b \leq s$. The above method of obtaining cards from the secret images is called a *construction* of the visual card game. For convenience, we denote the binary operation of stacking two cards X_i and Y_j by $X_i + Y_j$, and so the property that a stack of two cards X_a and Y_b recovers the secret image $Image(a, b)$ is written

$$X_a + Y_b = Image(a, b).$$

Every secret image $Image(i, j)$ is composed of black and white *pixels*. Each pixel of secret images is split into m subpixels in every card, and each subpixel is colored with black or transparent, where transparent subpixel is called a *white* subpixe as commonly used. Moreover, a stack of a black subpixel and a white subpixel recovers a black subpixel, and a stack of two subpixels with the same color recovers its color. This visual card game is briefly called the *card game of* $K(r, s)$*-type*. An example of the card game of $K(2, 3)$-type is shown in Appendix B.

The card game of $K(r, s)$-type is the game satisfying the following conditions.

(a) $X_i + Y_j = Y_j + X_i = Image(i, j)$ for all $1 \leq i \leq r$ and $1 \leq j \leq s$.

(b) Each pixel of the secret images is split into m subpixels in every card, and m is constant for every pixel and is called the *pixel expansion* of the card game. The set of m subpixels of any card corresponding to one pixel of the secret images is called a *share*.

(c) Each share S of any card consists of b_S black subpixels and w_S white subpixels, where $m = b_S + w_S$ and both b_S and w_S are constant and independent of the colors of the pixels of the images corresponding to S though b_S and w_S might change for a share S.

(d) A black pixel of a secret $Image(i,j)$ is recovered into a completely black region in a reconstructed image $X_i + Y_j$, where a region means the set of subpixels of $X_i + Y_j$ corresponding to a pixel of $Image(i,j)$.

The condition (c) says that the numbers b_S and w_S of black subpixels and white subpixels of a share S in a card are constant whenever the colors of corresponding pixels of the secret images are changed. So (c) implies that it is impossible to get any information about a secret images $Image(i,j)$ from one card X_i or Y_j. Namely, a boy X_i cannot get any information about s secret images $Image(i,j)$, $1 \leq j \leq s$, from his card X_i, and a girl Y_j cannot get any information about r secret images $Image(i,j)$, $1 \leq i \leq r$, from her card Y_j. It is well-known that the condition (d) is important for a person to recognize a reconstructed image clearly, and a construction possessing the property (d) is called a *perfect black reconstruction.*

Consider a construction of the card game of $K(r,s)$-type. For two cards X_i and Y_j and a white pixel P in the secret image $Image(i,j)$, let $\#White_P(X_i + Y_j)$ denote the number of white subpixels in the m subpixels of a reconstructed image $X_i + Y_j$ corresponding to P. Under the condition (d), the *contrast* of a construction of the card game is define by

$$\min_P \frac{\#White_P(X_i + Y_j)}{m},$$

where the minimum is taken over all white pixels P of $Image(i,j)$ ($1 \leq i \leq r$, $1 \leq j \leq s$). It is well-known that if the contrast becomes higher or the pixel expansion becomes smaller, then the reconstructed image becomes clearer. Thus contrast and pixel expansion are very important factors for constructions of the card games. Notice that for a construction of the game with contrast τ, if there exists no construction of the game with contrast greater than τ, then the contrast τ of the construction is said to be *sharp.* The sharpness of pixel expansion is similarly defined to be the smallest expansion number.

The condition (a) can be represented by the complete bipartite graph $K(r,s)$ with bipartition $\mathcal{X} \cup \mathcal{Y}$, that is, every vertex of $K(r,s)$ corresponds to a card and every edge corresponds to a secret image, and a stack of two cards corresponding to two vertices recovers the secret image corresponding to the edge joining them. For any graph G, the card game of G-type can be defined as above. However, we do not deal with the card game of G-type for a general graph G here.

This paper is organized as follows: In Sect. 2, we propose a construction of the card games of $K(1,s)$-type with contrast $1/2$ and pixel expansion 2, and one of $K(2,s)$-type with contrast $1/4$ and pixel expansion 4, and show

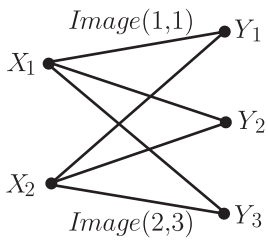

Figure 1: The visual card game of $K(2,3)$-type.

that these contrasts and pixel expansions are sharp. In Sect. 3, we give a construction of the card game of $K(r,s)$-type with pixel expansion $2r$, and the sharpness of this pixel expansion is proved. In Sect. 4, for integers r and s such that $3 \leq r \leq 6$ and $r \leq s$, we present a construction of the card game of $K(r,s)$-type with contrast $6/(11r)$ and pixel expansion 11, 22, 110 and 220, respectively. The sharpness of this contrast is shown in Sect. 5. For integers r and s with $7 \leq r \leq s$, a construction of the card game of $K(r,s)$-type with contrast $6/(11r)$ and pixel expansion $2r(r-1)(r-2)/3$ is given in Appendix A. An example of the card game of $K(2,3)$-type with contrast $1/4$ is given in Appendix B.

We conclude this section with an explanation of the card game from the point of view of visual cryptography scheme. A visual cryptography scheme, which was introduced in [4], can provide a construction of the card game of $K(r,s)$-type as a special case [3]. However, if we apply this method of construction to the card game, the reconstructed images lose a contrasts a lot though they satisfies much stronger security conditions. For example, such a construction of the card game of $K(3,s)$-type has contrast $1/(6s)$. On the other hand, our construction has a constant contrast $2/11$ and it is optimal. Visual cryptography scheme with many images are dealt in [6] and [7], and other results related to this paper can be found in [1], [2], [5] and etc.

2 Card game of $K(2,s)$-type

In this section we first provide constructions of the card games of $K(1,s)$-type and $K(2,s)$-type. Next we show that these contrasts and pixel expansions are sharp.

Let P be a fixed position of any pixel of secret images, and $img_P(i,j)$ denote the color of the pixel at P in $Image(i,j)$. So $\{img_P(i,j) : 1 \leq i \leq r,\ 1 \leq j \leq s\}$ is the set of pixel colors at P of the secret images. Let $S_P(X_i)$

and $S_P(Y_j)$ denote the two shares of X_i and Y_j, respectively, corresponding to P. Hence $S_P(X_i)$ and $S_P(Y_j)$ recover $img_P(i,j)$. When the fixed position P is known, we use the above notations without index P like $S(X_i)$ or $img(i,j)$. We denote the color of a subpixel by 0 or 1 according to its color is white (transparent) or black. Namely,

$$0 = while = tranparent \qquad \text{and} \quad 1 = black.$$

We begin with a construction of the card game of $K(1,s)$-type, which is given in the following lemma. Note that $K(1,s)$ is often called a *star*.

Lemma 1. *Let $s \geq 1$ be an integer. Then there exists a construction of the card game of $K(1,s)$-type with contrast $1/2$ and pixel expansion 2.*

Proof. Let X be the card corresponding to the center of $K(1,s)$, and $Y_1, \cdots, Y_s$ be the cards corresponding to the end-vertices of $K(1,s)$. We arbitrarily choose a position P of a pixel of the images, and fix it and consider the colors of the pixels at P and those of shares corresponding to P.

Determine the pixel expansion $m = 2$ and define a row vector $S(X) = [0\ 1]$, which implies that the share $S(X)$ consists of one white subpixel and one black subpixel. Next determine $S(Y_j)$ $(1 \leq j \leq s)$ as follows:

$$\begin{aligned} S(Y_j) &= [1\ 0] \qquad \text{if } \ img(1,j) = 1, \text{ and} \\ S(Y_j) &= [0\ 1] \qquad \text{if } \ img(1,j) = 0. \end{aligned} \tag{1}$$

By the above construction, a black pixel of a secret image is recovered into a completely black region since

$$S(X) + S(Y_j) = [1\ 1],$$

where $[1\ 1]$ implies that the two subpixels of $S(X) + S(Y_j)$ are black. On the other hand, a white pixel of a secret image is recovered into a region consisting of one white subpixel and one black subpixel since

$$S(X) + S(Y_j) = [0\ 1].$$

Hence the contrast of this construction is $1/2$, and the pixel expansion is 2.

Notice that when we construct the game of $K(1,s)$-type, for each position P, we randomly permute the two entries of each $S(X)$ and $S(Y_j)$ simultaneously, and use the resulting vectors as $S(X)$ and $S(Y_j)$.

We now show that the contrast and pixel expansion given above are sharp. Assume that there exists a construction of the card game of $K(1,1)$-type with contrast greater than $1/2$. Let m denote the pixel expansion, and

let $\{1, 2, \ldots, m\}$ be the set of positions of subpixels of a pixel. For $Z \in \{X, Y_1\}$, let $B(Z)$ and $W(Z)$ denote the subsets of $\{1, 2, \ldots, m\}$ such that the subpixels at $B(Z)$ of Z are black and and those at $W(Z)$ of Z are white. In particular, $B(Z) \cup W(Z) = \{1, 2, \ldots, m\}$.

Consider the case where $img(1, 1) = 0$. Then $|W(X)| > m/2$ and $|W(Y_1)| > m/2$ since $X + Y_1$ recovers a region containing more than $m/2$ white subpixels. If $img(1, 1) = 1$, then $W(Y_1)$ is included in $B(X)$ since $X + Y_1$ recovers a completely black region, and thus

$$|W(Y_1)| \leq |B(X)| = m - |W(X)| < m/2.$$

This contradicts the above inequality $|W(Y_1)| > m/2$. Therefore, the contrast of the card game of $K(1, 1)$-type is at most $1/2$, which implies that the contrast of the card game of $K(1, s)$-type is also at most $1/2$. It is trivial that a pixel expansion is at least two. $\square$

Theorem 2. *Let $s \geq 2$ be an integer. Then there exists a construction of the card game of $K(2, s)$-type with contrast $1/4$ and pixel expansion 4.*

Proof. Consider the card game of $K(2, s)$-type, where $s \geq 2$. Let $\mathcal{X} = \{X_1, X_2\}$ and $\mathcal{Y} = \{Y_1, Y_2, \cdots, Y_s\}$. First we decompose $K(2, s)$ into two edge disjoint stars $K(1, s)$ whose vertex sets are $\{X_1\} \cup \{Y_1, Y_2, \cdots, Y_s\}$ and $\{X_2\} \cup \{Y_1, Y_2, \cdots, Y_s\}$, respectively. We apply Lemma 1 to each $K(1, s)$, and obtain two $(s + 1) \times 2$ matrices $M(X_1)$ and $M(X_2)$. By inserting a new row vector $[1\ 1]$ into the second row of $M(X_1)$ and into the first row of $M(X_2)$, respectively, we obtain two $(s + 2) \times 2$ matrices, and combine them into a $(s + 2) \times 4$ matrix. This matrix determines the desired construction of the card game of $K(2, s)$-type. An example of the construction given above is shown in the following example. $\square$

Example 1. Consider the card game of $K(2, 3)$-type with $\mathcal{X} = \{X_1, X_2\}$ and $\mathcal{Y} = \{Y_1, Y_2, Y_3\}$. Assume that $(img(1, 1), img(1, 2), img(1, 3)) = (1, 1, 0)$ and $(img(2, 1), img(2, 2), img(2, 3)) = (0, 1, 0)$. Then the two 4×2 matrices corresponding to $K(1, 3)$ are

$$M(X_1) = \begin{bmatrix} S(X_1) \\ S(Y_1) \\ S(Y_2) \\ S(Y_3) \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \\ 1 & 0 \\ 0 & 1 \end{bmatrix} \quad \text{and} \quad M(X_2) = \begin{bmatrix} S(X_2) \\ S(Y_1) \\ S(Y_2) \\ S(Y_3) \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 0 & 1 \\ 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

Then we insert a row vector $[1\ 1]$ into the second row of $M(X_1)$ and into the first row of $M(X_2)$, and combine the resulting two matrices into a 5×4

matrix. Then we obtain the next matrix for the given pixel colors.

$$\begin{bmatrix} S(X_1) \\ S(X_2) \\ S(Y_1) \\ S(Y_2) \\ S(Y_3) \end{bmatrix} = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix}.$$

For example, $S(X_1) + S(Y_1) = [1\ 1\ 1\ 1]$ and $S(X_2) + S(Y_1) = [1\ 1\ 0\ 1]$ and so they recover $image(1,1) = 1$ and $image(2,1) = 0$ with contrast $1/4$ and pixel expansion 4.

Of course, for any other set of pixel colors, the matrix can be obtained in the same way. Moreover, when we construct the card game of $K(2,s)$-type, for each position P, we randomly permute the four column vectors of the $(2+s) \times 4$ matrix, and use the $2+s$ row vectors of the resulting $(2+s) \times 4$ matrix as $S(X_i)$ and $S(Y_j)$. Then no information about $Image(i,j)$, $1 \leq j \leq s$, is obtained from X_i and a similar situation holds for Y_j. Notice that the same method of random permutation is adapted for every construction the card game of $K(r,s)$-type, and so we omit these remark latter.

The sharpness of contrast is proved in the following Theorem 3, and the sharpness of pixel expansion will be proved in Theorem 4.

Theorem 3. *Let $s \geq 3$ be an integer. Then there exists no construction of the card game of $K(2,s)$-type with contrast greater than $1/4$.*

Proof. Since $K(2,3)$ is a subgraph of $K(2,s)$, it suffices to prove the theorem for $K(2,3)$. Assume that there exists a construction of the card game of $K(2,3)$-type with contrast greater than $1/4$. We consider any fixed position P of a pixel of the secret images, and write $img(i,j)$ for the color of the pixel at P in $Image(i,j)$, and $S(X_i)$ and $S(Y_j)$ for the shares of X_i and Y_j corresponding to P, respectively. Suppose that each pixel is split into m subpixels.

Represent two row vectors $S(X_i)$ and $S(Y_j)$ by $S(X_i) = [a_1\ a_2\ \ldots\ a_m]$ and $S(Y_j) = [b_1\ b_2\ \ldots\ b_m]$, where $a_k, b_k \in \{0,1\}$. We briefly call a_k and b_k *entries* of $S(X_i)$ and $S(Y_j)$ instead of colors of subpixels. Let $W(X_i)$, $B(X_i)$ $\subseteq \{1,2,\cdots,m\}$ denote the sets of positions of 0-entries and of 1-entries of $S(X_i)$, respectively. Namely,

$$W(X_i) = \{k\ :\ \text{the } k\text{-th entry of } S(X_i) \text{ is } 0\},$$
$$B(X_i) = \{k\ :\ \text{the } k\text{-th entry of } S(X_i) \text{ is } 1\}.$$

Similarly, $W(Y_i)$ and $B(Y_i)$ are defined as subsets of $\{1, 2, \cdots, m\}$. Let $\mathcal{X} = \{X_1, X_2\}$ and $\mathcal{Y} = \{Y_1, Y_2, Y_3\}$, and define λ as follows.

$$\lambda = \min_{(i,j)}\{|W(X_i) \cap W(Y_j)| \ : \ img(i,j) \text{ is white.}\},$$

where the minimum is taken over all (i, j) $(1 \leq i \leq 2,\ 1 \leq j \leq 3)$ such that the pixels $img(i, j)$ is white. In particular,

$$\frac{\lambda}{m} = \text{contrast}.$$

Hence if $img(i, j)$ is white, then $S(X_i)$ and $S(Y_j)$ have at least λ 0-entries in common place, that is , $|W(X_i) \cap W(Y_j)| \geq \lambda$.

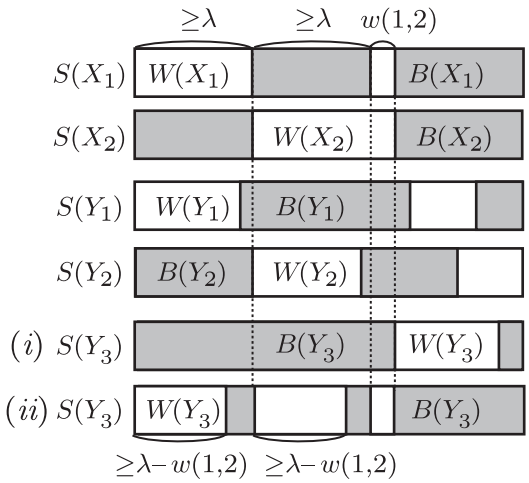

Figure 2: $S(X_i)$ and $S(Y_j)$ of $(img(1,1), img(1,2), img(2,1),\ img(2,2)) = (0, 1, 1, 0)$.

Since the contrast is greater than $1/4$, we have $\lambda/m > 1/4$, and thus

$$4\lambda > m. \tag{2}$$

By a perfect balck reconstrcution (see the condition (d)), if $W(X_i) \cap W(Y_j) \neq \emptyset$, then $X_i + Y_j$ must recover a white pixel, and so $|W(X_i) \cap W(Y_j)| \geq \lambda$. This fact is often used.

Consider the following pixel colors

$$\begin{bmatrix} img(1,1) & img(1,2) \\ img(2,1) & img(2,2) \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix},$$

and fix these pixel colors throughout the proof (see Fig. 2). Then by the condition (d), it follows that

$$W(X_1) \cap W(X_2) \cap W(Y_i) = \emptyset \quad (i = 1, 2),$$

and this implies that

$$\begin{aligned} |W(X_1) \setminus W(X_2)| \geq \ & |W(X_1) \cap W(Y_1)| \geq \lambda, \\ |W(X_2) \setminus W(X_1)| \geq \ & |W(X_2) \cap W(Y_2)| \geq \lambda. \end{aligned} \tag{3}$$

Let

$$w(1, 2) = |W(X_1) \cap W(X_2)|.$$

If $(img(1, 3), img(2, 3)) = (1, 1)$, then $B(Y_3)$ should cover $W(X_1) \cup W(X_2)$ (Fig. 2 (i)). By (3) and the definition of $w(1, 2)$, it holds that

$$|B(Y_3)| \ \geq \ 2\lambda + w(1, 2). \tag{4}$$

If $(img(1, 3), img(2, 3)) = (0, 0)$ (Fig. 2 (ii)), then $|W(X_1) \cap W(Y_3)| \geq \lambda$ and $|W(X_2) \cap W(Y_3)| \geq \lambda$, and so

$$\begin{aligned} |W(Y_3)| \ & \geq \ (\lambda - w(1, 2)) + (\lambda - w(1, 2)) + w(1, 2) \\ & = \ 2\lambda - w(1, 2). \end{aligned} \tag{5}$$

By (4) and (5),

$$m = |B(Y_3)| + |W(Y_3)| \geq 4\lambda.$$

This contradicts (2). Therefore the theorem is proved. □

3 Sharpness of pixel expansion

In the previous section, we provide a construction of the card game of $K(2, s)$-type with pixel expansion 4. We can apply the same procedure to provide a construction of the card game of $K(r, s)$-type with $3 \leq r \leq s$. Namely, we decompose $K(r, s)$ into r edge disjoint $K(1, s)$'s, and use Lemma 1 as in the construction of the card game of $K(2, s)$-type. Notice that we insert $(r - 1)$ row vectors [1 1] into each matrix $M(X_i)$. Then we can obtain a construction of the card game of $K(r, s)$-type with pixel expansion $2r$ and contrast $1/2r$. Thus the first half part of the following theorem holds.

Theorem 4. *Let r and s be integers such that $2 \leq r \leq s$. Then there exists a construction of the card game of $K(r, s)$-type with pixel expansion $2r$ and contrast $1/2r$. Moreover, if $r + 1 \leq s$, then there exists no construction of the card game of $K(r, s)$-type with pixel expansion less than $2r$.*

Proof. Since $K(r,s)$ contains $K(r,r+1)$ as a subgraph, it suffices to show that the pixel expansion of any construction of the card game of $K(r,r+1)$-type is at least $2r$. Consider any construction of the card game of $K(r,r+1)$-type, and let m be its pixel expansion.

We consider any fixed position P of a pixel of the secret images, and use the same notations $img(i,j)$, $B(X_i)$, $W(X_i)$, $B(Y_j)$ and $W(Y_j)$ as in the proof of Theorem 3. Consider the $r(r+1)$ pixel colors determined by the following $r \times r$ matrix

$$[img(i,j)] = \begin{bmatrix} 0 & 1 & \cdots & 1 \\ 1 & 0 & \cdots & 1 \\ \cdot & \cdot & \cdot & \cdot \\ 1 & 1 & \cdots & 0 \end{bmatrix},$$

and fix these pixel colors throughout the proof. Then $\{S(X_i), S(Y_j) \ : \ 1 \leq i \leq r, \ 1 \leq j \leq r\}$ satisfy

$$S(X_i) + S(Y_j) = \begin{cases} \mathsf{w} \ (white) & \text{if } i = j \leq r, \\ \mathsf{1} \ (black) & \text{if } i \neq j \leq r, \end{cases} \tag{6}$$

where w means that the reconstructed region corresponding to $S(X_i)+S(Y_i)$ containing at least λ white subpixels, and $\mathsf{1}$ means that the reconstructed region is completely black.

We illustrate a $(2r+1) \times m$ matrix, which will be considered.

$$\begin{bmatrix} S(X_1) \\ S(X_2) \\ \cdots \\ S(X_r) \\ S(Y_1) \\ \cdots \\ S(Y_r) \\ S(Y_{r+1}) \end{bmatrix} = \begin{bmatrix} 01\cdots1 & u_1 & \cdots & z_1 & 1 & \cdot & 1 \\ 10\cdots1 & u_2 & \cdots & z_2 & 1 & \cdot & 1 \\ \cdots\cdot & \cdot & \cdots & \cdot & 1 & \cdot & 1 \\ 11\cdots0 & u_r & \cdots & z_r & 1 & \cdot & 1 \\ 01\cdots1 & \cdot & \cdots & \cdot & & \cdots & \\ \cdots\cdot & \cdot & \cdots & \cdot & & \cdots & \\ 11\cdots0 & \cdot & \cdots & \cdot & & \cdots & \\ \cdots\cdot & \cdot & \cdots & \cdot & & \cdots & \end{bmatrix}.$$

There exists a column vector whose first entry and the $(r+1)$-th entry are both 0 since $S(X_1)+S(Y_1)$ recovers *white*, a w-region in other words. Then the remaining entries of this column vectors except the entries of $S(Y_{r+1})$ must be 1 by (6). We move such a column vector to the first column vector. By repeating this procedure, the first r column vectors are obtained as above.

Let n be the number of column vectors in the upper $r \times m$ submatrix which contain at least one 0-entry each but not contained in the first r-columns. Namely, for very $r+1 \leq k \leq r+n$, the k-th column vector, which

lies between two column vectors $[u_i]$ and $[z_i]$, contains at least one 0 entry in its upper r entires.

If Y_{r+1} satisfies $S(X_i) + S(Y_{r+1}) = \mathsf{1}$ for all $1 \le i \le r$, then

$$|B(Y_{r+2})| \ge r + n. \tag{7}$$

If $|W(Y_{r+1})| \ge r - n$, then

$$m = |B(Y_{r+1})| + |W(Y_{r+1})| \ge r + n + r - n = 2r.$$

This is the desired inequality about the pixel expansion. Therefore we may assume that $|W(Y_{r+1})| < r - n$, which also implies $n < r$.

For an integer $r + 1 \le k \le r + n$, let us define $\Delta_k \subseteq \{1, 2, \ldots, r\}$ as

$$\Delta_k = \{i \ : \ \text{the } i\text{-th entry of } k\text{-th column vector is } 0\}.$$

Since $n < r$, we can take a subset $\{a, b, \ldots, g\}$ of $\{1, 2, \ldots, r\}$ with at most n elements such that

$$\Delta_k \cap \{a, b, \ldots, g\} \ne \emptyset \qquad \text{for all} \quad r + 1 \le k \le r + n.$$

Consider a card Y_{r+1} that satisfies

$$S(X_i) + S(Y_{r+1}) = \begin{cases} \mathsf{1} & \text{if } i \in \{a, b, \ldots, g\}, \\ \mathsf{w} & \text{otherwise.} \end{cases}$$

Then since every k-th entry of Y_{r+1} for $r + 1 \le k \le r + n$ must be 1, $S(X_j) + S(Y_{r+1}) = \mathsf{w}$ implies that the j-th entry of Y_{r+1} is 0. Hence $|W(Y_{r+1})| \ge r - n$ since $S(X_j) + S(Y_{r+1}) = \mathsf{w}$ for at least $r - n$ X_j's. Thus again we obtain

$$m = |B(Y_{r+1})| + |W(Y_{r+1})| \ge r + n + r - n = 2r.$$

□

4 Card game of $K(r, s)$-type with $3 \le r \le 6$

In this section, we provide a construction of the card game of $K(r, s)$-type with contrast $6/(11r)$ for $3 \le r \le 6$. We first give a construction of $K(3, s)$-type with contrast $2/11$ and pixel expansion 11.

Define $S(X_1)$, $S(X_2)$, $S(X_3)$ as follows.

$$\begin{bmatrix} S(X_1) \\ S(X_2) \\ S(X_3) \end{bmatrix} = \begin{bmatrix} 0\,0\,1\,1\,1\,1\,0\,1\,1\,1\,1 \\ 1\,1\,0\,0\,1\,1\,0\,1\,1\,1\,1 \\ 1\,1\,1\,1\,0\,0\,0\,1\,1\,1\,1 \end{bmatrix}. \tag{8}$$

Then we show that $S(Y_j)$ can be determined for every set $\{img(1,j), img(2,j), img(3,j)\}$ of pixel colors as follows. Thus a construction is guaranteed.

Let n denote the number of white pixels in $\{img(1,j), img(2,j), img(3,j)\}$. If $n = 3$, then determine

$$S(Y_j) = [0\ 1\ 0\ 1\ 0\ 1\ 0\ 1\ 1\ 1\ 1].$$

Then $S(X_i) + S(Y_j)$ is a region with two white subpixels for every $1 \le i \le 3$, and so this case is done. If $n = 2$ and $img(1,j) = img(2,j) = 0$, then determine

$$S(Y_j) = [0\ 0\ 0\ 0\ 1\ 1\ 1\ 1\ 1\ 1\ 1].$$

Then $S(X_1) + S(Y_j)$ and $S(X_2) + S(Y_j)$ are regions with two white subpixels each and $S(X_3) + S(Y_j)$ is a completely black region, as desired. If $n = 1$ and $img(1,j) = 0$ then determine

$$S(Y_j) = [0\ 0\ 1\ 1\ 1\ 1\ 1\ 0\ 0\ 1\ 1].$$

If $n = 0$, then determine

$$S(Y_j) = [1\ 1\ 1\ 1\ 1\ 1\ 1\ 0\ 0\ 0\ 0].$$

By symmetry, the above rule gives a construction of the card game of $K(3,s)$-type with contrast $2/11$ and pixel expansion 11.

Next we propose a construction of the card game of $K(6,s)$-type with contrast $1/11$ and pixel expansion $m = 220$, which is different from the former construction. Let $\mathcal{R} = \{1,2,3,4,5,6\}$ and $\lambda = 20$, and let

$$\Omega = \{\Delta \subset \mathcal{R} : |\Delta| = 3\} = \{\Delta_1, \Delta_2, \ldots, \Delta_N\},$$

where $N = {}_6C_3 = 20 = \lambda$. Notice that all Δ_i are distinct. First determine $S(X_1)$, $S(X_2)$, $\cdots$, $S(X_6)$ as follows.

$$\begin{bmatrix} S(X_1) \\ S(X_2) \\ \cdot \\ S(X_6) \end{bmatrix} = [I, Q, J] = \begin{bmatrix} 0\cdot 01\cdot 1\cdots 1\cdot 1 & q_{11} & \cdots & q_{1N} & 1 & \cdots & 1 \\ 1\cdot 10\cdot 0\cdots 1\cdot 1 & q_{21} & \cdots & q_{2N} & 1 & \cdots & 1 \\ \cdot\cdot & \cdot & \cdots & \cdot & 1 & \cdots & 1 \\ 1\cdot 11\cdot 1\cdots 0\cdot 0 & q_{61} & \cdots & q_{6N} & 1 & \cdots & 1 \end{bmatrix},$$

where I is a $6\times 6\lambda$ matrix obtained from a unit matrix of order 6 by replacing 0 and 1 by row vectors $[0\cdots 0]$ and $[1\cdots 1]$ with λ entries, Q is a $6\times N$ matrix defined below, and J is a $6\times 4\lambda$ matrix with all entries 1. In particular $[I, Q, J]$ is a $6\times 11\lambda$ matrix. The i-th row vector $[q_{i1}\ q_{i2}\ \cdots\ q_{i\lambda}]$ of Q is defined as

$$q_{ik} = \begin{cases} 0 & \text{if } i \in \Delta_k, \\ 1 & \text{otherwise.} \end{cases}$$

Then we show that $S(Y_j)$ can be determined for every set $\{img(1,j),\cdots,img(6,j)\}$ of pixel colors as follows. Thus this provides the desired construction.

Let x^n denote a sequence $x\cdots x$ consisting of n x's, and let n denote the number of white pixels in $\{img(1,j),\cdots,img(6,j)\}$. If $n=6$, then determine

$$\begin{aligned} S(Y_j) &= [A_1,B_1,C_1], \quad \text{where} \\ A_1 &= [0^{10}1^{10}0^{10}1^{10}0^{10}1^{10}0^{10}1^{10}0^{10}1^{10}0^{10}1^{10}] \\ B_1 &= [\underbrace{0\cdots0}_{20}] = [0^{20}], \quad C_1 = [\underbrace{1\cdots1}_{80}] = [1^{80}]. \end{aligned}$$

If $n=5$, then we may assume that $img(1,j)=img(2,j)=img(3,j)=img(4,j)=img(5,j)=0$ by symmetry. Hense $S(Y_j)$'s are defined as follows:

$$\begin{aligned} S(Y_j) &= [A_2,Q_2,C_2], \qquad \text{where} \\ A_2 &= [0^{14}1^60^{14}1^60^{14}1^60^{14}1^60^{14}1^61^{20}], \\ C_2 &= [1^{80}],\ Q_2 = [y_1,\cdots,y_{20}], \quad \text{where} \\ y_i &= \begin{cases} 0 & \text{if } \Delta_k \subset \{1,2,3,4,5\}, \\ 1 & \text{otherwise.} \end{cases} \end{aligned}$$

If $n=4$, then $S(Y_j)=[A_3,B_3,C_3]$, where $A_3=[0^{80}1^{40}]$, $B_3=[1^{20}]$, $C_3=[1^{80}]$. If $n=3$, then $S(Y_j)=[A_4,B_4,C_4]$, where $A_4=[0^{60}1^{60}]$, $B_4=[1^{20}]$ and $C_4=[1^{60}0^{20}]$. If $n=2$, then $S(Y_6)=[A_6,B_6,C_6]$, where $A_6=0^{40}$, $B_6=1^{100}$ and $C_6=[1^{40}0^{40}]$. If $n=1$, then $S(Y_5)=[A_5,B_5,C_5]$, where $A_5=0^{20}$, $B_5=1^{120}$ and $C_5=[1^{20}0^{60}]$. If $n=0$, then $S(Y_j)=[A_7,B_7,C_7]$, where $A_7=[1^{120}]$, $B_7=[1^{20}]$, $C_7=[0^{80}]$.

In every case each $S(Y_j)$ contains exactly 80 white subpixels and 120 black subpixels, respectively.

For example, if $n=5$ and $i\in\{1,2,3,4,5\}$, then $S(X_i)+S(Y_j)$ contains $|\{\Delta : i\in\Delta\subset\{1,2,3,4,5\}|=6$ plus 14 0-entries, and hence it recovers a region containing 20 white subpixels. In any case, if $img(i,j)=0$, then $S(X_i)+S(Y_j)$ recovers a region containing $20=\lambda$ white subpixels. Hence the contrast is $\lambda/(11\lambda)=1/11$.

Constructions of the card game of $K(4,s)$-type and $K(5,s)$-type are omitted thought basically a construction of $K(4,s)$-type is similar to that of $K(3,s)$-type, and a construction of $K(5,s)$-type is similar to that of $K(6,s)$-type.

5 Sharpness of contrast

In this section, we shall prove the following theorem. Notice that every case is proved simultaneously, however, the proof technique does not work when $r \geq 7$.

Theorem 5. *Let r and s be integers such that $3 \leq r \leq 6$ and $r+1 \leq s$. Then there exists no construction of the card game of $K(r,s)$-type with contrast greater than $6/(11r)$.*

Proof. Since $K(r,s)$ contains $K(r,r+1)$ as a subgraph, it suffice to show that the theorem holds for $K(r,r+1)$. Assume that there exists a construction of the card game of $K(r,r+1)$-type with contrast greater than $6/(11r)$. Define λ as in the proof of Theorem 3. Then the contrast is λ/m, and if $img(i,j) = 0$, then $|W(X_i) \cap W(Y_j)| \geq \lambda$. We use the same notations $img(i,j)$, $S(X_i)$, $S(Y_j)$, $W(X_i)$, $B(X_i)$, $W(Y_j)$ and $W(Y_j)$ as defined in the proof of Theorem 3.

Consider the following r^2 pixel colors

$$[img(i,j)] = \begin{bmatrix} 0 & 1 & \cdots & 1 \\ 1 & 0 & \cdots & 1 \\ \cdot & \cdot & \cdots & \cdot \\ 1 & 1 & \cdots & 0 \end{bmatrix}, \tag{9}$$

and fix these pixel colors throughout the proof. Then $\{S(X_i),\ S(Y_j)\ :\ 1 \leq i \leq r,\ 1 \leq j \leq r\}$ satisfy

$$S(X_i) + S(Y_j) = \begin{cases} \mathsf{w} & \text{if } i = j, \\ \mathsf{1} & \text{otherwise,} \end{cases}$$

where w and $\mathsf{1}$ mean that the reconstructed images are white and black, respectively.

Let $\mathcal{R} = \{1, 2, \ldots, r\}$. For every subset $\Delta \subseteq \mathcal{R}$ with $|\Delta| \geq 2$, define

$$W(\Delta) = \Big(\bigcap_{i \in \Delta} W(X_i)\Big) \cap \Big(\bigcap_{j \notin \Delta} B(X_j)\Big),$$
$$w(\Delta) = |W(\Delta)|.$$

Then $W(\Delta) \subset \{1, \ldots, m\}$, and if $x \in W(\Delta) \neq \emptyset$, then

(i) the x-th entry of every $X_i, i \in \Delta$, is 0,

(ii) the x-th entry of every $X_j, j \notin \Delta$, is 1,

(iii) if the x-th entry of Y_t is 0, then $S(X_i) + S(Y_t) = \mathsf{w}$ for all $i \in \Delta$.

For convenience, Δ *always denote a subset of* $\mathcal{R}$ *containing at least two elements*, and all the following summations are taken over such Δ.

Lemma 6. *There exists an integer* $t \in \mathcal{R}$ *such that*

$$\sum_{\Delta \subset \mathcal{R}} (|\Delta| - 2) w(\Delta) \leq \frac{r}{6} \sum_{t \in \Delta \subset \mathcal{R}} (|\Delta| - 1) w(\Delta) \tag{10}$$

and

$$\left(1 - \frac{r}{6}\right) \sum_{t \in \Delta \subset \mathcal{R}} (|\Delta| - 1) w(\Delta) \leq \sum_{t \in \Delta \subset \mathcal{R}} w(\Delta) - \sum_{\Delta \subset \mathcal{R} - \{t\}} (|\Delta| - 2) w(\Delta). \tag{11}$$

Proof. We first show that the two inequalities (10) and (11) are equivalent. It follows that

$$\sum_{\Delta \subset \mathcal{R}} (|\Delta| - 2) w(\Delta) = \sum_{t \in \Delta \subset \mathcal{R}} (|\Delta| - 2) w(\Delta) + \sum_{\Delta \subset \mathcal{R} - \{t\}} (|\Delta| - 2) w(\Delta).$$

Hence (10) is equivalent to

$$\sum_{t \in \Delta \subset \mathcal{R}} (|\Delta| - 2) w(\Delta) + \sum_{\Delta \subset \mathcal{R} - \{t\}} (|\Delta| - 2) w(\Delta) \leq \frac{r}{6} \sum_{t \in \Delta \subset \mathcal{R}} (|\Delta| - 1) w(\Delta).$$

This inequality is equivalent to (11).

Suppose that (10) does not hold for any $t \in \mathcal{R}$. By summing the inverse inequality of (10) over all $t \in \mathcal{R}$, we obtain

$$r \sum_{\Delta \subset \mathcal{R}} (|\Delta| - 2) w(\Delta) > \frac{r}{6} \sum_{\Delta \subset \mathcal{R}} |\Delta| (|\Delta| - 1) w(\Delta) \tag{12}$$

since

$$\sum_{t \in \mathcal{R}} \sum_{t \in \Delta \subset \mathcal{R}} f(\Delta) = \sum_{\Delta \subset \mathcal{R}} |\Delta| f(\Delta).$$

We now show that the following holds for every Δ.

$$r(|\Delta| - 2) \leq \frac{r}{6} |\Delta| (|\Delta| - 1). \tag{13}$$

This is equivalent to

$$|\Delta|^2 - 7|\Delta| + 12 \geq 0.$$

The above inequality holds since the inequality holds when $|\Delta| = 3$ or 4, and the left side takes the minimum when $\Delta = 7/2$. Hence (13) holds, which contradicts (12). Therefore, (10) holds for at least one $t \in \mathcal{R}$. $\square$

Lemma 7. *(i) If $S(X_i) + S(Y_{r+1}) = \mathsf{w}$ for all $1 \le i \le r$, then*

$$|W(Y_{r+1})| \ge \sum_{i \in \mathcal{R}} \Big(\lambda - \sum_{i \in \Delta \subset \mathcal{R}} w(\Delta) \Big) + \sum_{\Delta \subset \mathcal{R}} w(\Delta). \tag{14}$$

(ii) Let $t \in \mathcal{R}$ be the integer obtained in Lemma 6. If $S(X_i) + S(Y_{r+1}) = \mathsf{w}$ for all $i \ne t$ and $S(X_t) + S(Y_{r+1}) = \mathsf{1}$, then

$$|W(Y_{r+1})| \ge \sum_{i \in \mathcal{R} - \{t\}} \Big(\lambda - \sum_{i \in \Delta \subset \mathcal{R} - \{t\}} w(\Delta) \Big) + \sum_{\Delta \subset \mathcal{R} - \{t\}} w(\Delta). \tag{15}$$

Proof. We prove (i). Assume that $S(X_1), \ldots, S(X_r)$ are given and $S(X_i) + S(Y_{r+1}) = \mathsf{w}$ for all $1 \le i \le r$. Take any $\Delta \subset \mathcal{R}$ with $W(\Delta) \ne \emptyset$. Let $a \in W(\Delta)$. If the a-th entry of Y_{r+1} is 0, then the a-th entry of $S(X_i) + S(Y_{r+1})$ is 0 for every $i \in W(\Delta)$, that is, one 0 entry of Y_{r+1} contributes $w(\Delta)$ times. Thus in order to obtain Y_{r+1} with small number of 0 entries, we should first determine the x-th entry of Y_{r+1} is 0 for all $x \in W(\Delta)$ and Δ with $w(\Delta) \ge 1$. Since $|W(X_i) \cap W(Y_{r+1})| \ge \lambda$ for every i, the number of 0 entries of Y_{r+1} is

$$\begin{aligned} & |W(Y_{r+1})| \\ \ge & \sum_{\Delta \subset \mathcal{R}} w(\Delta) + \sum_{i \in \mathcal{R}} \max \Big\{ \lambda - \sum_{i \in \Delta \subset \mathcal{R}} w(\Delta), 0 \Big\} \\ \ge & \sum_{\Delta \subset \mathcal{R}} w(\Delta) + \sum_{i \in \mathcal{R}} \Big(\lambda - \sum_{i \in \Delta \subset \mathcal{R}} w(\Delta) \Big). \end{aligned}$$

By the same argument, we can obtain (15). □

Lemma 8. *The right side of (14) is greater than or equal to the right side of (15) if and only if*

$$\lambda \ge \sum_{t \in \Delta \subset \mathcal{R}} (|\Delta| - 1) w(\Delta). \tag{16}$$

Proof. The right side of (14) becomes

$$\begin{aligned} & \sum_{i \in \mathcal{R}} \Big(\lambda - \sum_{i \in \Delta \subset \mathcal{R}} w(\Delta) \Big) + \sum_{\Delta \subset \mathcal{R}} w(\Delta) \\ = & \lambda |\mathcal{R}| - \sum_{\Delta \subset \mathcal{R}} (|\Delta| - 1) w(\Delta) \qquad (17) \\ = & \lambda |\mathcal{R}| - \sum_{t \in \Delta \subset \mathcal{R}} (|\Delta| - 1) w(\Delta) - \sum_{\Delta \subset \mathcal{R} - \{t\}} (|\Delta| - 1) w(\Delta). \qquad (18) \end{aligned}$$

Similarly, the right side of (15) becomes

$$\begin{aligned}
&\sum_{i\in\mathcal{R}-\{t\}}\Big(\lambda-\sum_{i\in\Delta\subset\mathcal{R}-\{t\}}w(\Delta)\Big)+\sum_{\Delta\subset\mathcal{R}-\{t\}}w(\Delta)\\
=&\lambda(|\mathcal{R}|-1)-\sum_{\Delta\subset\mathcal{R}-\{t\}}|\Delta|w(\Delta)+\sum_{\Delta\subset\mathcal{R}-\{t\}}w(\Delta)\\
=&\lambda(|\mathcal{R}|-1)-\sum_{\Delta\subset\mathcal{R}-\{t\}}(|\Delta|-1)w(\Delta). \qquad (19)
\end{aligned}$$

It is easy to see that (18) $\geq$ (19) if and only if (16) holds. Therefore the lemma is proved. □

Lemma 9. *It follows that*

$$|B(Y_{r+1})|\geq r\lambda+\sum_{\Delta\subset\mathcal{R}}w(\Delta). \qquad (20)$$

Proof. It follows from (9) that $|W(X_i)\cap W(Y_i)|\geq\lambda$ for all $1\leq i\leq r$, and $(W(X_i)\cap W(Y_i))\cap(W(X_j)\cap W(Y_j))\subseteq W(X_i)\cap W(Y_j)=\emptyset$ for all $1\leq i<j\leq r$. Moreover $W(\Delta)\cap(W(X_i)\cap W(Y_i))=\emptyset$ for every $1\leq i\leq r$ and $\Delta\subset\mathcal{R}$. Consider the case where $S(X_i)+S(Y_{r+1})=1$ for all $1\leq i\leq r$. Then $B(Y_{r+1})$ covers all $W(X_i)$, $1\leq i\leq r$, and hence

$$\begin{aligned}
|B(Y_{r+1})|&\geq\sum_{1\leq i\leq r}|W(X_i)\cap W(Y_i)|+\sum_{\Delta\subset\mathcal{R}}|W(\Delta)|\\
&\geq\lambda r+\sum_{\Delta\subset\mathcal{R}}w(\Delta).
\end{aligned}$$

We are now ready to prove that the contrast $6/(11r)$ is sharp for $3\leq r\leq 6$. We first choose $t\in\mathcal{R}$ so that Lemma 6 holds. Then Lemmas 7 and 8 hold for this t.

Case 1. *The right side of (14) is greater than or equal to the right side of (15).*

By the condition of Case 1, (17), (20) and by $|\mathcal{R}|=r$, we have

$$\begin{aligned}
m&=|B(Y_{r+1})|+|W(Y_{r+1})|\\
&\geq\ r\lambda+\sum_{\Delta\subset\mathcal{R}}w(\Delta)+r\lambda-\sum_{\Delta\subset\mathcal{R}}(|\Delta|-1)w(\Delta)\\
&=2r\lambda-\sum_{\Delta\subset\mathcal{R}}(|\Delta|-2)w(\Delta)\\
&\geq 2r\lambda-\frac{r\lambda}{6}=\frac{11r\lambda}{6}\qquad\text{(by (10) and (16))}.
\end{aligned}$$

This implies that the contrast $\lambda/m \leq 6/(11r)$.

Case 2. *The right side of (14) is less than the right side of (15).*

By (20) and (15), we have

$$\begin{aligned}
m &= |B(Y_{r+1})| + |W(Y_{r+1})| \\
&= r\lambda + \sum_{\Delta \subset \mathcal{R}} w(\Delta) + \sum_{i \in \mathcal{R}-\{t\}} \Big(\lambda - \sum_{i \in \Delta \subset \mathcal{R}-\{t\}} w(\Delta)\Big) + \sum_{\Delta \subset \mathcal{R}-\{t\}} w(\Delta) \\
&= (2r-1)\lambda + \sum_{t \in \Delta \subset \mathcal{R}} w(\Delta) + \sum_{\Delta \subset \mathcal{R}-\{t\}} w(\Delta) \\
&\qquad - \sum_{\Delta \subset \mathcal{R}-\{t\}} |\Delta| w(\Delta) + \sum_{\Delta \subset \mathcal{R}-\{t\}} w(\Delta) \\
&= (2r-1)\lambda + \sum_{t \in \Delta \subset \mathcal{R}} w(\Delta) - \sum_{\Delta \subset \mathcal{R}-\{t\}} (|\Delta| - 2) w(\Delta) \\
&\geq (2r-1)\lambda + \big(1 - \frac{r}{6}\big) \sum_{t \in \Delta \subset \mathcal{R}} (|\Delta| - 1) w(\Delta) \quad \text{(by (11))} \\
&\geq (2r-1)\lambda + \big(1 - \frac{r}{6}\big)\lambda \qquad \text{(by Lemma 8 and } r \leq 6) \\
&= \frac{11r\lambda}{6}.
\end{aligned}$$

This implies that $\lambda/m \leq 6/(11r)$. Consequently the proof of Theorem 5 is complete. $\square$

6 Concluding Remarks

We introduced a new visual card game called a card game of $K(r,s)$-type, and proposed some its constructions. Then we showed that these constructions are optimal in a sense that there exists no construction with greater contrast or with lower pixel expansion. However, for $r \geq 7$, it is not known whether the contrast of the given construction of the card game of $K(r,s)$-type is sharp or not. The card game of $K(r,s)$-type is naturally extended to the card game of G-type for a general graph G. The research about this card game will be future work.

References

[1] G. Ateniese, C. Blundo, A. De Santis, and D.R. Stinson, "Visual Cryptography for General Access Structures," Information and Computation, **129** (1996) 86–106.

[2] C. Blundo and A. De Santis, "Visual cryptography schemes with perfect reconstruction of black pixels," Computer and Graphics, **22**, no.4, (1998) 449–455.

[3] S. Droste, "New results on visual cryptography," Advances in Cryptology-CRYPTO'96, LNCS, **1109** (1996), 401–415.

[4] M. Naor and A. Shamir, "Visual cryptography," Advances in Cryptology, Eurocrypt'94, LNCS, **950** (1994) 1–12.

[5] P.A. Eisen and D.R. Stinson, "Threshold Visual cryptography Schemes With Specified Whiteness Levels of Reconstructed Pixels," Designs Codes and Cryptography **25**, no.1, pp.15–61.

[6] M. Uno and M. Kano, " Visual Cryptography Schemes with Dihedral Group Access Structure for Many Images," ISPEC2007, LNCS, **4464**, (2007) 344–359.

[7] M. Uno and M. Kano, " Visual Secret Sharing Schemes with Cyclic Access Structure for Many Images ," ICISC2008, LNCS, **5461**, (2009) 84–97.

Appendix A

We prove the next theorem.

Theorem 10. *Let r and s be integers such that $7 \leq r \leq s$. Then there exists a construction of the card game of $K(r,s)$-type with contrast $6/(11r)$ and pixel expansion $11r(r-1)(r-2)/6$.*

Proof. Let Ω be the family of subsets of $\mathcal{R} = \{1, 2, \ldots, r\}$ with size 3, and let $\nu = |\Omega|$. Then

$$\Omega = \{\Delta \subset \mathcal{R} : |\Delta| = 3\} = \{\Delta_1, \Delta_2, \ldots, \Delta_\nu\},$$
$$\nu = |\Omega| = {}_rC_3 = \frac{r(r-1)(r-2)}{6}.$$

Define three row vectors O, I and J as follows. O consists of $(r-1)(r-2)$ 0-entries, I consists of $(r-1)(r-2)$ 1-entries and J consists of $2r(r-1)(r-2)/3$ 1-entries. Thus

$$O = [\underbrace{0\ 0\ \ldots\ 0\ 0}_{(r-1)(r-2)}],\quad I = [\underbrace{1\ 1\ \ldots\ 1\ 1}_{(r-1)(r-2)}] \qquad \text{and} \qquad J = [\underbrace{1\ 1\ \ldots\ 1\ 1}_{\frac{2}{3}r(r-1)(r-2)}].$$

We next define each $S(X_i)$ with m entries as follows.

$$S(X_i) = [\underbrace{I \ldots I}_{(i-1)} O \underbrace{I \ldots I}_{(r-i)} \ \Delta_1(i) \ldots \Delta_\nu(i) \ J],$$

$$\text{where} \quad \Delta_j(i) = \begin{cases} 0 & \text{if } i \in \Delta_j, \\ 1 & \text{otherwise.} \end{cases}$$

Then

$$\begin{aligned} m = |S(X_i)| &= r(r-1)(r-2) + \nu + \frac{2r(r-1)(r-2)}{3} \\ &= \frac{11}{6} r(r-1)(r-2). \end{aligned}$$

The parameter λ is defined as

$$\lambda = (r-1)(r-2) = |O|.$$

Next we show that for any fixed $1 \le t \le s$ and for arbitrarily given pixel colors $\{img(i,t) : 1 \le i \le r\}$, we can determine $S(Y_t)$ so that $S(X_i)+S(Y_t) = img(i,t)$ for every $1 \le i \le r$. Let

$$\Gamma = \{i \ : \ img(i,t) = 0\} \qquad \text{and} \qquad \rho = |\Gamma|.$$

So ρ is the number of white pixels in $\{img(i,t) \ : \ 1 \le i \le r\}$. If $\rho \le \frac{2r}{3}$, then we determine

$$S(Y_t) = [A_1 \ A_2 \ \ldots \ A_r \ \underbrace{1 \ 1 \cdots 1}_{\nu} \ \ J^*],$$

$$\text{where} \quad A_k = \begin{cases} O & \text{if } \ k \in \Gamma, \\ I & \text{otherwise,} \end{cases}$$

and J^* is obtained from J by replacing $|J| - \rho(r-1)(r-2)$ 0-entries by 1-entries.

This is possible since

$$\begin{aligned} & |J| - \rho(r-1)(r-2) \\ \ge\ & \frac{2r}{3}(r-1)(r-2) - \frac{2r}{3}(r-1)(r-2) \\ =\ & 0. \end{aligned}$$

If $k \in \Gamma$, then $S(X_k)$ and $S(Y_t)$ contains one O in common, and so $S(X_k) + S(Y_t) = \mathsf{w}$. If $h \in \{1, \ldots, m\} - \Gamma$, then $S(X_h)$ and $S(Y_t)$ have no 0-entry in common and so $S(X_k) + S(Y_t) = \mathsf{1}$. Hence this case is done.

Next assume $\rho > \frac{2r}{3}$. Let Q be the following row vector with λ entries.

$$Q = [\underbrace{0 \cdots 0}_{\lambda -_{\rho-1} \mathrm{C}_2} \ \underbrace{1 \cdots 1}_{\rho-1 \mathrm{C}_2}].$$

Determine $S(Y_t)$ as follows:

$$S(Y_t) = [B_1 \ B_2 \ \ldots \ B_r \ b_1 \ldots b_\nu \ \ J^{**}], \qquad \text{where}$$

$$B_k = \begin{cases} Q & \text{if } \ k \in \Gamma, \\ I & \text{otherwise,} \end{cases} \qquad b_k = \begin{cases} 0 & \text{if } \ \Delta_i \subseteq \Gamma, \\ 1 & \text{otherwise,} \end{cases}$$

and J^{**} is obtained from J by replacing

${}_\rho\mathrm{C}_3 + (\lambda -_{\rho-1} \mathrm{C}_2)\rho$ 1-entries by 0-entries.

Assume that $k \in \Gamma$. Then $S(X_k)$ and $S(Y_t)$ contains one Q in common, and $\Delta_j(k)$'s of $S(X_k)$ and b_k's of $S(Y_t)$ have ${}_{|\Gamma-\{k\}|}\mathrm{C}_2 =_{\rho-1} \mathrm{C}_2$ 0-entries in common. Thus $S(X_k)$ and $S(Y_t)$ contains

$$\lambda -_{\rho-1} \mathrm{C}_2 +_{\rho-1} \mathrm{C}_2 = \lambda$$

0-entries in common. Thus $S(X_k) + S(Y_t) = \mathsf{w}$. If $h \in \{1, \ldots, m\} - \Gamma$, then $S(X_h)$ and $S(Y_t)$ have no 0-entry in common and so $S(X_k) + S(Y_t) = \mathsf{1}$.

Lastly, we show that J^{**} is well-defined. In order to do so, it suffices to show that

$$\frac{2}{3}r(r-1)(r-2) \geq_\rho \mathrm{C}_3 + \rho\Big(\lambda - \frac{(\rho-1)(\rho-2)}{2}\Big) \geq 0.$$

The second inequality holds since $\lambda = (r-1)(r-2)$ and $\rho \leq r$. The first inequality is equivalent to

$$f(\rho) = \big(\frac{2}{3}r - \rho\big)(r-1)(r-2) + \frac{\rho(\rho-1)(\rho-2)}{3} \geq 0.$$

Since $f(\rho)$ is decreasing between $2r/3 < \rho \leq r$ and $f(r) = 0$, we obtain $f(\rho) \geq 0$ for $2r/3 < \rho \leq r$. Hence the proof is complete. $\square$

Appendix B

We show a construction the card game of $K(2,3)$-type with contrast $1/4$ and pixel expansion 4. Here we show only two cards X_1 and Y_1 since other X_i's and Y_j's look very similar to X_1 and Y_1, respectively.

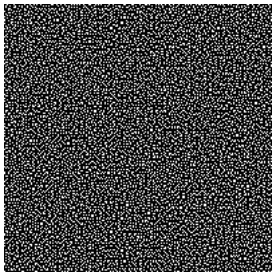

Figure 3: The card X_1

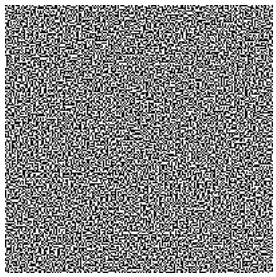

Figure 4: The card Y_1

Figure 5: The reconstructed image $X_1 + Y_1$

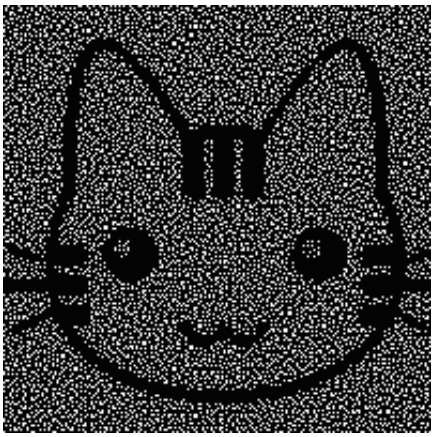

Figure 6: The reconstructed image $X_1 + Y_2$