Available online at www.sciencedirect.com
ScienceDirect
Information and Computation 205 (2007) 716–732
Information and Computation
www.elsevier.com/locate/ic

Extended visual cryptography schemes

Andreas Klein *, Markus Wessler

Universität Kassel, Fachbereich fur Mathematik und Informatik, Heinrich Plett Str. 49 (AVZ), D-34132 Kassel, Germany

Received 12 September 2003; revised 9 June 2004
Available online 3 January 2007

Abstract

Visual cryptography schemes have been introduced in 1994 by Naor and Shamir. Their idea was to encode a secret image into n shadow images and to give exactly one such shadow image to each member of a group P of n persons. Whereas most work in recent years has been done concerning the problem of qualified and forbidden subsets of P or the question of contrast optimizing, in this paper we study extended visual cryptography schemes, i.e., shared secret systems where any subset of P shares its own secret.

1. Introduction

A visual cryptography scheme is given by the following set up. Let P be a group of n persons where each participant is given exactly one image (in fact it does not have to be a real image) xeroxed onto a transparency. Stacking all the transparencies together, a secret image is recovered. So in this sense the participants share a secret. This set up can be generalized to the case where some subsets $X \subseteq P$ (which are usually called *qualified subsets of P*) can recover the secret by stacking their transparencies together, whereas other, *forbidden* subsets cannot. Such structures, called *access structures*, have been examined very well. In [5] Naor and Shamir analysed so-called (k, n)-threshold visual cryptography schemes, i.e., schemes where a subset is qualified if and only if it consists of at least k participants. In [1] and [2] their idea was extended to general access structures.

* Corresponding author. Fax: +49(0)561 804 4646.
E-mail addressess: klein@mathematik.uni-kassel.de (A. Klein), wessler@mathematik.uni-kassel.de (M. Wessler).

0890-5401/$ - see front matter © 2007 Published by Elsevier Inc.
doi:10.1016/j.ic.2006.12.005

Most work concerning this subject focuses on two aspects, either the pixel expansion, i.e., the number of subpixels which is needed on the different levels to represent a white or a black pixel, or the contrast, i.e., the difference of subpixels representing a white or a black pixel.

As a further generalization, the existence of a secret image can be concealed by displaying a different image on each transparency. Naor and Shamir [5] solved this problem for the $(2,2)$-threshold scheme. In [3] this problem was considered for a general access structure. In [4] Droste made a further generalization: stacking the transparencies of each participant together, a secret image is recovered, and there is in fact only this single way to recover it. But moreover, the participants of any arbitrary subset X of P share a secret, too. Hence we have $2^n - 1$ more or less secret images.

We start by briefly recalling the work done by Droste and prove that the scheme proposed in [4] has minimal pixel expansion. Then we prove a trade-off theorem between the contrast of the different images.

Finally we give new constructions for generalized visual cryptography schemes with less than $2^n - 1$ subsets in order to achieve a smaller pixel expansion and a better contrast.

2. Preliminaries

A visual cryptography scheme is based on the fact that each pixel of an image is divided into a certain number m of subpixels. This number m is called the *pixel expansion* of the image. If the number of black subpixels needed to represent a white pixel in an image is l, and the number of black subpixels needed to represent a black pixel is h, then we call the number $\alpha = \frac{h-l}{m}$ the *contrast* of the image.

An extended visual cryptography scheme consists of n transparencies $\tau_1, \ldots, \tau_n$ and $2^n - 1$ different images (one for each non-empty subset $T \subseteq \{1, \ldots, n\}$). We denote by I_T the image which is recovered by stacking together exactly the transparencies τ_i for $i \in T$. We generalize this as follows. For any non-empty subset $\mathfrak{S}$ of the powerset $\mathcal{P}(\{1, \ldots, n\})\backslash\{\emptyset\}$ an $\mathfrak{S}$-extended visual cryptography scheme consists of n transparencies $\tau_1, \ldots, \tau_n$ with the following property: let $T \in \mathfrak{S}$. If we stack together the transparencies τ_i for $i \in T$, then we recover the image I_T for which each white pixel is represented by l_T black subpixels and each black pixel is represented by h_T black subpixels. Furthermore, for T' not contained in T, the distribution of subpixels on the transparencies τ_i with $i \in T$ is independent of the image $I_{T'}$, i.e., the information of the transparencies τ_i with $i \in T$ does not suffice to recover the image $I_{T'}$.

More formally, we define an $\mathfrak{S}$-extended visual cryptography scheme as follows. (See also [5] for "usual" visual cryptography schemes and [4] for $\mathfrak{S}$-extended visual cryptography schemes.)

Definition 2.1. Let $\mathfrak{S} \subseteq \mathcal{P}(\{1, \ldots, n\})\backslash\{\emptyset\}$.

An $\mathfrak{S}$-extended visual cryptography scheme is described by multisets $C^{\mathfrak{T}}$ of $n \times m$ Boolean matrices for $\mathfrak{T} \subseteq \mathfrak{S}$. (For given $\mathfrak{T}$ each Boolean matrix in $C^{\mathfrak{T}}$ describes the colors of the subpixels on each transparency, where the corresponding pixel in image I_T is black if and only if $T \in \mathfrak{T}$. For encoding, each matrix in $C^{\mathfrak{T}}$ is chosen with the same probability.)

The multisets $C^{\mathfrak{T}}$ must satisfy the following conditions:

(1) Let $B \in C^{\mathfrak{T}}$. For $\{i_1, \ldots, i_q\} \in \mathfrak{S}$ the Hamming weight of the OR of the rows $i_1, \ldots, i_q$ of B is $h_{\{i_1,\ldots,i_q\}}$ if $\{i_1, \ldots, i_q\} \in \mathfrak{T}$ and $l_{\{i_1,\ldots,i_q\}}$ otherwise, i.e.,

$$w_{Ham}((b_{i_1,1}, \ldots, b_{i_1,m}) \text{ OR } \ldots \text{ OR } (b_{i_q,1}, \ldots, b_{i_q,m})) = \begin{cases} h_{\{i_1,\ldots,i_q\}} \text{ if } \{i_1, \ldots, i_q\} \in \mathfrak{T} \\ l_{\{i_1,\ldots,i_q\}} \text{ if } \{i_1, \ldots, i_q\} \notin \mathfrak{T} \end{cases}.$$

(This means stacking the transparencies $\tau_{i_1}, \ldots, \tau_{i_q}$ together we recover the image $I_{\{i_1,\ldots,i_q\}}$.)

(2) For $\{i_1, \ldots, i_q\} \subseteq \{1, \ldots, n\}$ and $\mathfrak{T}, \mathfrak{T}' \subseteq \mathfrak{S}$ with $\mathfrak{T} \cap \mathcal{P}(\{i_1, \ldots, i_q\}) = \mathfrak{T}' \cap \mathcal{P}(\{i_1, \ldots, i_q\})$ we obtain the same multisets if we restrict the matrices in $C^{\mathfrak{T}}$ and $C^{\mathfrak{T}'}$, respectively, to the rows $i_1, \ldots, i_q$.
(This condition guarantees the security of the different images.)

If $\mathfrak{S} = \mathcal{P}(\{1, \ldots, n\})\backslash\{\emptyset\}$ we simply call this an extended visual cryptography scheme.

In this paper, we are primarily interested in the minimal pixel expansion $M(\mathfrak{S})$ of an $\mathfrak{S}$-extended visual cryptography scheme, but we also consider the optimal contrast values.

In [4] Droste gives the following construction for $\mathfrak{S}$-extended visual cryptography schemes using (k, k)-threshold schemes.

Construction 2.2. For each $T \in \mathfrak{S}$ we take $2^{|T|-1}$ subpixels and use them to construct a $(|T|, |T|)$-threshold visual cryptography scheme. If $i \notin T$ the corresponding subpixels on τ_i will be black. The $\mathfrak{S}$-extended visual cryptography scheme is achieved by putting all these schemes together. Since we shall not need the details of this construction in the sequel, we omit a formal definition and refer to [4].

The scheme obtained by this construction has pixel expansion

$$m = \sum_{T \in \mathfrak{S}} 2^{|T|-1}$$

and the contrast of all encoded images is $\frac{1}{m}$. Especially this proves

$$M(\mathfrak{S}) \leqslant \sum_{T \in \mathfrak{S}} 2^{|T|-1}.$$

We shall prove in the following sections that this construction is optimal if $\mathfrak{S} = \mathcal{P}(\{1, \ldots, n\})\backslash\{\emptyset\}$ but it is not optimal for general $\mathfrak{S}$.

3. Pixel expansion and contrast for the extended scheme

It is sufficient to consider the case of one single pixel. For a given non-empty subset $T \subseteq \{1, \ldots, n\}$ let x_T be the number of subpixels which are black exactly on the transparencies i for $i \in T$ and let us denote by x the vector of all the x_T. For $\emptyset \neq S \subseteq \{1, \ldots, n\}$ let r_S be the number of black subpixels needed for the image I_S. Formally we set $r_\emptyset = 0$. We write r for the vector of all the r_S with $\emptyset \neq S \subseteq \{1, \ldots, n\}$.

This leads to the linear equation system given by

$$Mx = r \tag{1}$$

where $M = (m_{S,T})_{\emptyset \neq S,T \subseteq \{1,\ldots,n\}}$ is defined by $m_{S,T} = 1$ if $S \cap T \neq \emptyset$ and $m_{S,T} = 0$ otherwise.

We note that by (1) an $\mathfrak{S}$-extended visual cryptography scheme is completely described. For example

Example 3.1. Let $\mathfrak{S} = \mathcal{P}(\{1,2,3\})\backslash\{\emptyset\}$. For a construction of an $\mathfrak{S}$-extended visual cryptography scheme we choose the following values for h_T and l_T:

$$\begin{array}{ll} h_{\{1,2,3\}} = 13 & l_{\{1,2,3\}} = 12 \\ h_{\{1,2\}} = h_{\{1,3\}} = h_{\{2,3\}} = 12 & l_{\{1,2\}} = l_{\{1,3\}} = l_{\{2,3\}} = 11 \\ h_{\{1\}} = h_{\{2\}} = h_{\{3\}} = 9 & l_{\{1\}} = l_{\{2\}} = l_{\{3\}} = 8. \end{array}$$

Now suppose we want to encode a black pixel on the images $I_{\{1\}}, I_{\{1,2\}}, I_{\{2,3\}}$ and $I_{\{1,2,3\}}$ and a white pixel on all other images. Eq. (1) leads to

$$\begin{pmatrix} 1&0&1&0&1&0&1 \\ 0&1&1&0&0&1&1 \\ 1&1&1&0&1&1&1 \\ 0&0&0&1&1&1&1 \\ 1&0&1&1&1&1&1 \\ 0&1&1&1&1&1&1 \\ 1&1&1&1&1&1&1 \end{pmatrix} \begin{pmatrix} x_{\{1\}} \\ x_{\{2\}} \\ x_{\{1,2\}} \\ x_{\{3\}} \\ x_{\{1,3\}} \\ x_{\{2,3\}} \\ x_{\{1,2,3\}} \end{pmatrix} = \begin{pmatrix} 9 \\ 8 \\ 12 \\ 8 \\ 11 \\ 12 \\ 13 \end{pmatrix}.$$

(The unusual ordering of the variables will become clear in the induction of Lemma 3.2.)

We solve this equation and find that $x_{\{1\}} = x_{\{3\}} = x_{\{2,3\}} = 1, x_{\{2\}} = x_{\{1,2\}} = 2$ and $x_{\{1,3\}} = x_{\{1,2,3\}} = 3$. We distribute these black subpixels at random to satisfy the security condition (2) in Definition 2.1.

Solving the corresponding equations we can obtain the distribution of black subpixels for every possible combination of black and white pixels on the images, i.e., we have a complete description of an $\mathfrak{S}$-extended visual cryptography scheme with the given contrast values.

Of course not every solution of Eq. (1) results in a visual cryptography scheme. We have the additional condition that the variables x_T have to be non-negative integers. Thus we can view the construction of an $\mathfrak{S}$-extended visual cryptography scheme as an integral linear programming problem. In the next lemma, we will prove that for integral values h_T and l_T the solution variables x_T will be automatically integral. Lemma 3.3 helps us to simplify the linear programming problem.

Lemma 3.2. *Eq. (1) has a unique integral solution.*

Proof . We prove this by induction on the number n of transparencies.

Sort the variables x_T by the following order: first we enumerate all subsets that do not contain n. The next subset is the set $\{n\}$. Then the other subsets containing n follow.

Writing $M_1 = (1)$, we obtain the following recursion formula which follows directly from the definition:

$$M_{n+1} = \begin{pmatrix} M_n & \mathbf{0}_{1,n} & M_n \\ \mathbf{0}_{1,n} & 1 & \mathbf{1}_{1,n} \\ M_n & \mathbf{1}_{n,1} & \mathbf{1}_{n,n} \end{pmatrix}.$$

Here the index denotes the number of transparencies. $\mathbf{0}_{i,j}$ or $\mathbf{1}_{i,j}$, respectively, denotes an $(2^i - 1) \times (2^j - 1)$ matrix with all entries 0 or 1, respectively.

With $M_1^{-1} = (1)$ we obtain the following recursion formula for M_n^{-1}:

$$M_{n+1}^{-1} = \begin{pmatrix} \mathbf{0}_{n,n} & -M_n^{-1}\mathbf{1}_{n,1} & M_n^{-1} \\ -\mathbf{1}_{1,n}M_n^{-1} & 0 & \mathbf{1}_{1,n}M_n^{-1} \\ M_n^{-1} & M_n^{-1}\mathbf{1}_{n,1} & -M_n^{-1} \end{pmatrix}.$$

Thus M is invertible, i.e., Eq. (1) has a unique solution.

We notice that the components of $M_n^{-1}\mathbf{1}_{n,1}$ are only $-1, 0$ and 1 and that $\mathbf{1}_{1,n}M_n^{-1}\mathbf{1}_{n,1} = 1$. Then the formula can be proved by induction.

Thus M_n^{-1} contains only the entries $-1, 0$ and 1 and therefore the solution of Eq. (1) is integral. □

Lemma 3.3. *The solution of (1) is non-negative if and only if for each $S \subsetneq \{1, \ldots, n\}$ the condition*

$$\sum_{S \subseteq T \subseteq \{1,\ldots,n\}} (-1)^{|S|+|T|} r_T \leqslant 0 \tag{2}$$

is satisfied.

Proof . We claim that $x = (x_S)$ with

$$x_S = \sum_{\{1,\ldots,n\} \setminus S \subseteq T \subseteq \{1,\ldots,n\}} (-1)^{|T|+|S|+n+1} r_T \tag{3}$$

solves Eq. (1) and due to Lemma 3.2 this solution is unique.

To prove this we substitute x in Eq. (1). For $\emptyset \neq U \subseteq \{1, \ldots, n\}$ the line of the system of linear equations corresponding to U yields

$$\begin{aligned} \sum_{\emptyset \neq S \subseteq \{1,\ldots,n\}} m_{U,S} x_S &= \sum_{S \subseteq \{1,\ldots,n\}} m_{U,S} \sum_{\{1,\ldots,n\} \setminus S \subseteq T \subseteq \{1,\ldots,n\}} (-1)^{|T|+|S|+n+1} r_T \\ &= \sum_{T \subseteq \{1,\ldots,n\}} \sum_{\{1,\ldots,n\} \setminus T \subseteq S \subseteq \{1,\ldots,n\}} (-1)^{|T|+|S|+n+1} r_T m_{U,S} \\ &= \sum_{\emptyset \neq T \subseteq \{1,\ldots,n\}} (-1)^{|T|} r_T \sum_{\{1,\ldots,n\} \setminus T \subseteq S \subseteq \{1,\ldots,n\}} (-1)^{|S|+n+1} m_{U,S}. \end{aligned} \tag{4}$$

If $T \not\subseteq U$ we choose $t \in T \setminus U$ and obtain

$$\sum_{\{1,\dots,n\}\setminus T \subseteq S \subseteq \{1,\dots,n\}} (-1)^{|S|+n+1} m_{U,S}$$

$$= \sum_{\{1,\dots,n\}\setminus \{T\cup\{t\}\} \subseteq S \subseteq \{1,\dots,n\}\setminus\{t\}} (-1)^{|S|+n+1} m_{U,S} + (-1)^{|S|+1+n+1} m_{U,S\cup\{t\}} = 0$$

since $m_{U,S} = m_{U,S\cup\{t\}}$.
If $T \subsetneq U$ and $T \neq \emptyset$ we find

$$\sum_{\{1,\dots,n\}\setminus T \subseteq S \subseteq \{1,\dots,n\}} (-1)^{|S|+n+1} m_{U,S} = \sum_{\{1,\dots,n\}\setminus T \subseteq S \subseteq \{1,\dots,n\}} (-1)^{|S|+n+1} = 0$$

since $m_{U,S} = 1$.
But for $\emptyset \neq T = U$ we find

$$\sum_{\{1,\dots,n\}\setminus T \subseteq S \subseteq \{1,\dots,n\}} (-1)^{|S|+n+1} m_{U,S} = \sum_{\{1,\dots,n\}\setminus T \subseteq S \subseteq \{1,\dots,n\}} (-1)^{|S|+n+1} - (-1)^{|\{1,\dots,n\}\setminus U|+n+1}$$
$$= (-1)^{|\{1,\dots,n\}\setminus U|+n}$$

since $m_{U,S} = 1$ for $S \not\subseteq \{1,\dots,n\}\setminus U$.
Thus Eq. (4) yields

$$\sum_{\emptyset\neq S\subseteq\{1,\dots,n\}} m_{U,S} x_S = \sum_{\emptyset\neq T\subseteq\{1,\dots,n\}} (-1)^{|T|} r_T \sum_{\{1,\dots,n\}\setminus T \subseteq S \subseteq \{1,\dots,n\}} (-1)^{|S|+n+1} m_{U,S}$$
$$= (-1)^{|U|} r_U (-1)^{|\{1,\dots,n\}\setminus U|+n}$$
$$= (-1)^{2n} r_U = r_U.$$

This proves that x is a solution of Eq. (1) and the lemma follows. □

Now we can solve (2) to derive bounds for the pixel expansion and the contrast.

Theorem 3.4. *An extended visual cryptography scheme with n transparencies needs at least* $\frac{1}{2}(3^n - 1)$ *subpixels. Hence Construction 2.2 is optimal with respect to the pixel expansion, i.e.,*

$$M(\mathcal{P}(\{1,\dots,n\})\setminus\{\emptyset\}) = \frac{1}{2}(3^n - 1).$$

Proof . In left hand side of inequality (2) we have the sum over r_T for $|S| + |T|$ even and over $-r_T$ for $|S| + |T|$ odd. This becomes maximal if all r_T with $|S| + |T|$ even are as large as possible (i.e.,

equal h_T) and all r_t with $|S| + |T|$ odd are as small as possible (i.e., equal l_T). Thus an extended visual cryptography scheme exists if and only if

$$\sum_{\substack{S \subseteq T \subseteq \{1,\ldots,n\} \\ |S| \equiv |T| \bmod 2}} h_T \leqslant \sum_{\substack{S \subseteq T \subseteq \{1,\ldots,n\} \\ |S| \not\equiv |T| \bmod 2}} l_T \tag{5}$$

holds for each $S \subsetneq \{1,\ldots,n\}$.

For each $\emptyset \neq T \subseteq \{1,\ldots,n\}$ let $\delta_T = h_T - l_T$. Our goal is to prove that

$$m \geqslant h_{\{1,\ldots,n\}} \geqslant \sum_{\emptyset \neq T \subseteq \{1,\ldots,n\}} \delta_T 2^{|T|-1}. \tag{6}$$

As the first step in this proof we show that, for given values δ_T (for $\emptyset \neq T \subseteq \{1,\ldots,n\}$), the number $h_{\{1,\ldots,n\}}$ is minimal if for all $S \subsetneq \{1,\ldots,n\}$ inequality (5) is satisfied with equality.

To this end, suppose

$$\sum_{\substack{S \subseteq T \subseteq \{1,\ldots,n\} \\ |S| \equiv |T| \bmod 2}} h_T < \sum_{\substack{S \subseteq T \subseteq \{1,\ldots,n\} \\ |S| \not\equiv |T| \bmod 2}} l_T$$

for some $S \subsetneq \{1,\ldots,n\}$. But the contrast levels

$$\bar{h}_T = \begin{cases} h_T & \text{for } T \subseteq S \\ h_T - 1 & \text{otherwise} \end{cases}$$

and

$$\bar{l}_T = \begin{cases} l_T & \text{for } T \subseteq S \\ l_T - 1 & \text{otherwise} \end{cases}$$

satisfy (5), since

$$|\{T \mid S \subseteq T \subseteq \{1,\ldots,n\};\ |T| \equiv |S| \bmod 2\}| = |\{T \mid S \subseteq T \subseteq \{1,\ldots,n\};\ |T| \not\equiv |S| \bmod 2\}|.$$

This proves that if inequality (5) is not satisfied with equality we can find smaller values for the parameters l_T and h_T which also satisfy (5). Thus in an optimal scheme (i.e., a scheme with the smallest possible values for l_T and h_T) inequality (5) is satisfied with equality for each $T \subsetneq \{1,\ldots,n\}$.

Next we claim that

$$h_T = \sum_{\emptyset \neq T' \subseteq \{1,\ldots,n\}} \delta_{T'} 2^{|T'|-1} - \sum_{T \subsetneq T' \subseteq \{1,\ldots,n\}} \delta_{T'} 2^{|T'|-1-|T|} \tag{7}$$

for $\emptyset \neq S \subseteq \{1,\ldots,n\}$ satisfy (5) with equality.

To prove this we have to show that

$$\sum_{\substack{S\subseteq T\subseteq\{1,\dots,n\}\\ |S|\equiv|T| \bmod 2}}\left[\sum_{\emptyset\neq T'\subseteq\{1,\dots,n\}}\delta_{T'}2^{|T'|-1}-\sum_{T\subsetneq T'\subseteq\{1,\dots,n\}}\delta_{T'}2^{|T'|-1-|T|}\right]$$
$$=\sum_{\substack{S\subseteq T\subseteq\{1,\dots,n\}\\ |S|\not\equiv|T| \bmod 2}}\left(\left[\sum_{\emptyset\neq T'\subseteq\{1,\dots,n\}}\delta_{T'}2^{|T'|-1}-\sum_{T\subsetneq T'\subseteq\{1,\dots,n\}}\delta_{T'}2^{|T'|-1-|T|}\right]-\delta_T\right)$$

or equivalently

$$\sum_{\emptyset\neq T'\subseteq\{1,\dots,n\}}\delta_{T'}\left[\sum_{\substack{S\subseteq T\subseteq\{1,\dots,n\}\\ |S|\equiv|T| \bmod 2}}2^{|T'|-1}-\sum_{\substack{S\subseteq T\subsetneq T'\\ |S|\equiv|T| \bmod 2}}2^{|T'|-1-|T|}\right]$$
$$=\sum_{\emptyset\neq T'\subseteq\{1,\dots,n\}}\delta_{T'}\left[\sum_{\substack{S\subseteq T\subseteq\{1,\dots,n\}\\ |S|\not\equiv|T| \bmod 2}}2^{|T'|-1}-\sum_{\substack{S\subseteq T\subsetneq T'\\ |S|\not\equiv|T| \bmod 2}}2^{|T'|-1-|T|}\right]+\delta_{T'}\frac{(-1)^{|T'|+|S|}-1}{2}.$$

(Note that the last summand is equal to $-\delta_{T'}$ for $|T'|\not\equiv|S| \bmod 2$ and equal to 0 otherwise.) Comparing coefficients for each $\delta_{T'}$ we obtain

$$2^{n-|S|-1}\cdot 2^{|T'|-1}-\sum_{\substack{S\subseteq T\subsetneq T'\\ |S|\equiv|T| \bmod 2}}2^{|T'|-1-|T|}$$
$$=2^{n-|S|-1}\cdot 2^{|T'|-1}-\left(\sum_{\substack{S\subseteq T\subsetneq T'\\ |S|\not\equiv|T| \bmod 2}}2^{|T'|-1-|T|}\right)+\frac{(-1)^{|T'|+|S|}-1}{2},\tag{8}$$

but this is true since

$$(-1)^{|T'|-|S|}=(1-2)^{|T'|-|S|}$$
$$=\sum_{i=0}^{|T'|-|S|}\binom{|T'|-|S|}{i}(-2)^i$$

$$= \sum_{\substack{i=0 \\ i \text{ even}}}^{|T'|-|S|} \binom{|T'|-|S|}{i} 2^i - \sum_{\substack{i=0 \\ i \text{ odd}}}^{|T'|-|S|} \binom{|T'|-|S|}{i} 2^i$$

$$= \sum_{\substack{S \subseteq T \subseteq T' \\ |T'| \equiv |T| \bmod 2}} 2^{|T'|-|T|} - \sum_{\substack{S \subseteq T \subseteq T' \\ |T'| \not\equiv |T| \bmod 2}} 2^{|T'|-|T|}, \text{ since } \binom{|T'|-|S|}{i} = \sum_{\substack{S \subseteq T \subseteq T' \\ |T|-|S|=i}} 1.$$

Thus

$$\sum_{\substack{S \subseteq T \subseteq T' \\ |T'| \equiv |T| \bmod 2}} 2^{|T'|-|T|} = \left(\sum_{\substack{S \subseteq T \subseteq T' \\ |T'| \not\equiv |T| \bmod 2}} 2^{|T'|-|T|} \right) + (-1)^{|T'|-|S|}$$

and therefore

$$\left(\sum_{\substack{S \subseteq T \subsetneq T' \\ |T'| \equiv |T| \bmod 2}} 2^{|T'|-|T|} \right) + 1 = \left(\sum_{\substack{S \subseteq T \subsetneq T' \\ |T'| \not\equiv |T| \bmod 2}} 2^{|T'|-|T|} \right) + (-1)^{|T'|+|S|}.$$

(Note that $(-1)^{|T'|-|S|} = (-1)^{|T'|+|S|}$.) Division by 2 gives

$$\left(\sum_{\substack{S \subseteq T \subsetneq T' \\ |T'| \equiv |T| \bmod 2}} 2^{|T'|-1-|T|} \right) = \left(\sum_{\substack{S \subseteq T \subsetneq T' \\ |T'| \not\equiv |T| \bmod 2}} 2^{|T'|-1-|T|} \right) + \frac{(-1)^{|T'|+|S|} - 1}{2}$$

as required for Eq. (8).

Suppose that $\bar{h}_T$ (for $\emptyset \neq T \subseteq \{1, \ldots, n\}$) satisfy (5) with equality, too.

If inequality (5) is satisfied with equality for all a subsets S, we can solve these equations recursively and get

$$h_S = h_{\{1,\ldots,n\}} + F_S(\delta_T \mid T \subseteq \{1, \ldots, n\}),$$

for some function F_S. Since inequality (5) is satisfied with equality for the contrast values h_T and h'_T this yields

$$\bar{h}_S = h_S + \bar{h}_{\{1,\ldots,n\}} - h_{\{1,\ldots,n\}}.$$

But for $S = \emptyset$ inequality (5) yields $\bar{h}_{\{1,\ldots,n\}} = h_{\{1,\ldots,n\}}$ and therefore $\bar{h}_T = h_T$ for all $\emptyset \neq T \subseteq \{1, \ldots, n\}$. This proves that (7) is the only solution of (5) that satisfies all inequalities with equality.

Thus we find

$$m \geqslant h_{\{1,\ldots,n\}} \geqslant \sum_{\emptyset \neq T' \subseteq \{1,\ldots,n\}} \delta_{T'} 2^{|T'|-1} \geqslant \sum_{\emptyset \neq T' \subseteq \{1,\ldots,n\}} 2^{|T'|-1} = \frac{1}{2}(3^n - 1). \quad \square$$

Remark 3.5. Note that in no equation in the proof of Theorem 3.4 we have a variable l_T and a variable h_S with $|S| = |T|$. Thus we have proven even the following theorem:

Let $\mathfrak{S} = \mathcal{P}(\{1,\ldots,n\})\backslash\{\emptyset\}$. Assume that the images I_S and I_T are equal whenever $|S| = |T|$. Then the minimal pixel expansion needed to achieve that $\mathfrak{S}$-extended visual cryptography scheme is $\frac{1}{2}(3^n - 1)$.

Next we prove a trade-off between the contrast of the different images.

Theorem 3.6. *For $\emptyset \neq T \subseteq \{1,\ldots,n\}$ let $\alpha_T = \frac{h_T - l_T}{m}$ be the contrast of the image I_T. The contrast levels of the images satisfy*

$$\sum_{\emptyset \neq T \subseteq \{1,\ldots,n\}} 2^{|T|-1} \alpha_T \leqslant 1. \tag{9}$$

Further let $\alpha'_T \geqslant 0$ (for $\emptyset \neq T \subseteq \{1,\ldots,n\}$) satisfy (9). Then for every $\varepsilon > 0$ there exists a generalized visual cryptography scheme with contrast levels α_T (for $\emptyset \neq T \subseteq \{1,\ldots,n\}$) where $|\alpha_T - \alpha'_T| < \varepsilon$ for non-empty subsets T of $\{1,\ldots,n\}$.

Proof . Let $\delta_T = h_T - l_T$. By (7) we conclude

$$m \geqslant h_{\{1,\ldots,n\}} \geqslant \sum_{\emptyset \neq T \subseteq \{1,\ldots,n\}} \delta_T 2^{|T|-1}$$

and therefore

$$\sum_{\emptyset \neq T \subseteq \{1,\ldots,n\}} 2^{|T|-1} \alpha_T = \frac{1}{m} \sum_{\emptyset \neq T \subseteq \{1,\ldots,n\}} \delta_T 2^{|T|-1} \leqslant 1.$$

Now assume (9) holds for α'_T. Then we choose $\delta_T \in \mathbb{N}$ and $M \in \mathbb{N}$ with

$$0 \leqslant \alpha'_T - \frac{\delta_T}{M} \leqslant \varepsilon.$$

By (7) we know that there exists an extended visual cryptography scheme with contrast levels $h_T - l_T = \delta_T$ and minimal pixel expansion

$$m = \sum_{\emptyset \neq T \subseteq \{1,\ldots,n\}} 2^{|T|-1} \delta_T.$$

Since $\frac{\delta_T}{M} \leqslant \alpha'_T$ and α'_T satisfy (9) we find $m < M$.

If we add useless subpixels (e.g., subpixels that are always black) to the extended visual cryptography scheme constructed above, we obtain a scheme with contrast $\alpha_T = \frac{\delta_T}{M}$. This proves the theorem. $\square$

4. Pixel expansion and contrast for the $\mathfrak{S}$-extended scheme

In the previous section, we proved that Construction 2.2 is optimal if $\mathfrak{S} = \mathcal{P}(\{1,\dots,n\})\backslash\{\emptyset\}$.

Let now $\mathfrak{S}$ be arbitrary. If we set $\delta_T = 1$ for $T \in \mathfrak{S}$ and $\delta_T = 0$ for $T \notin \mathfrak{S}$ in Eq. (7) we obtain the same contrast values as in Construction 2.2. In this sense Construction 2.2 can be viewed as a $(\mathcal{P}(\{1,\dots,n\})\backslash\{\emptyset\})$-extended visual cryptography scheme with degenerated contrast values.

Now fix a subset $\{i_1,\dots,i_k\}$ of $\{1,\dots,n\}$ and assume $\{i_1,\dots,i_k\} \notin \mathfrak{S}$. The security condition (Condition (2) in Definition 2.1) assures that the gray level of the stack of the transparencies $i_1,\dots,i_k$ depends only on the images $I_{S'}$ with $S' \subset \{i_1,\dots,i_k\}$. Now assume that no subset S' of $\{i_1,\dots,i_k\}$ is in $\mathfrak{S}$. In this case the gray level of the stack of the transparencies $i_1,\dots,i_k$ is entirely independent of the chosen images and hence constant. Thus we have proven.

Theorem 4.1. *Let $\mathfrak{S} \subseteq \mathcal{P}(\{1,\dots,n\})\backslash\{\emptyset\}$ satisfy that $S \notin \mathfrak{S}$ implies $S' \notin \mathfrak{S}$ for each subset S' of S.*

Then an $\mathfrak{S}$-extended visual cryptography scheme must be realized as a $(\mathcal{P}(\{1,\dots,n\})\backslash\{\emptyset\})$-extended visual cryptography scheme with degenerated contrast values.

In particular Theorem 3.6 implies

$$M(\mathfrak{S}) = \sum_{S\in\mathfrak{S}} 2^{|S|-1}.$$

We now give an example in which Construction 2.2 is not optimal.

Example 4.2. Let $\mathfrak{S} = \mathcal{P}(\{1,\dots,n\})\backslash\{\emptyset,\{1,\dots,n\}\}$ and n even then Construction 2.2 is not optimal.

Proof . Let $\delta_T = 1$ for $\emptyset \neq T \subsetneq \{1,\dots,n\}$ and $\delta_{\{1,\dots,n\}} = 0$. Then h_T and $l_T = h_T - \delta_T$ as in (7) satisfy (5) and these are the solutions given by 2.2.

We show that we can find a better construction in the sense that fewer subpixels are required. Setting $\overline{h}_T = h_T - 1$ and $\overline{l}_T = l_T - 1$ for $\emptyset \neq T \subseteq \{1,\dots,n\}$ and $\overline{h}_\emptyset = \overline{l}_\emptyset = 0$ we observe that inequality (5) still holds for all $S \neq \emptyset$. Thus the solution $x = (x_T)_{\emptyset\neq T\subseteq\{1,\dots,n\}}$ of Eq. (1) satisfies $x_T \geqslant 0$ for $T \neq \{1,\dots,n\}$.

The value of $x_{\{1,\dots,n\}}$ will be non-negative unless $r_T = \overline{h}_T$ for $|T|$ even and $r_T = \overline{l}_T$ for $|T|$ odd. In this special case Eq. (3) gives the solution $x_{\{1,\dots,n\}} = -1$. To obtain a solution with positive $x_{\{1,\dots,n\}}$ we adjust the value of $r_{\{1,\dots,n\}}$ from $\overline{h}_{\{1,\dots,n\}}$ to $\overline{h}_{\{1,\dots,n\}} - 1$. (This is possible, since $\{1,\dots,n\} \notin \mathfrak{S}$ which means that the number of black subpixels in the stack of all transparencies does not matter.) Now (3) reveals the solution

$$\begin{aligned} x_{\{1,\dots,n\}} &= \sum_{T\subseteq\{1,\dots,n\}} (-1)^{|T|+1} r_T \\ &= \sum_{\substack{T\subseteq\{1,\dots,n\}\\ |T| \text{ odd}}} \overline{l}_T - \left(\sum_{\substack{T\subseteq\{1,\dots,n\}\\ |T| \text{ even}}} \overline{h}_T \right) + 1 = -1 + 1 = 0. \end{aligned}$$

For $S \neq \{1,\dots,n\}$ and $|S|$ even we obtain

$$x_S = \sum_{\{1,\ldots,n\}\setminus S\subseteq T\subseteq\{1,\ldots,n\}} (-1)^{|T|+|S|+n+1} r_T$$

$$= \sum_{\substack{\{1,\ldots,n\}\setminus S \subseteq T \subseteq \{1,\ldots,n\} \\ |T| \text{ odd}}} \overline{l}_T - \left(\sum_{\substack{\{1,\ldots,n\}\setminus S \subseteq T \subseteq \{1,\ldots,n\} \\ |T| \text{ even}}} \overline{h}_T \right) + 1 = 0 + 1 = 1.$$

For $|S|$ odd we obtain

$$x_S = \sum_{\{1,\ldots,n\}\setminus S\subseteq T\subseteq\{1,\ldots,n\}} (-1)^{|T|+|S|+n+1} r_T$$

$$= \left(\sum_{\substack{\{1,\ldots,n\}\setminus S \subseteq T \subseteq \{1,\ldots,n\} \\ |T| \text{ even}}} \overline{h}_T \right) - 1 - \sum_{\substack{\{1,\ldots,n\}\setminus S \subseteq T \subseteq \{1,\ldots,n\} \\ |T| \text{ odd}}} \overline{l}_T$$

$$> \sum_{\substack{\{1,\ldots,n\}\setminus S \subseteq T \subseteq \{1,\ldots,n\} \\ |T| \text{ even}}} \overline{l}_T - \left(\sum_{\substack{\{1,\ldots,n\}\setminus S \subseteq T \subseteq \{1,\ldots,n\} \\ |T| \text{ odd}}} \overline{h}_T \right) - 1 = -1.$$

Thus all possible values of r lead to non-negative solutions for x, hence an $\mathfrak{S}$-extended visual cryptography scheme with $m = \overline{h}_{\{1,\ldots,n\}} < h_{\{1,\ldots,n\}}$ exists, i.e., the solution given by 2.2 is not optimal. □

We notice that the proof is also valid if $\delta_T = 0$ for some T (i.e., if some contrast values degenerate). In fact, it is sufficient to assume $h_T \neq 0$ where h_T is defined by (7). A short calculation proves that this is the case if $\mathfrak{S} \not\subseteq \mathcal{P}(S)$ for a proper subset S of $\{1,\ldots,n\}$. Thus we find

Corollary 4.3. *For $\mathfrak{S} \subseteq \mathcal{P}(\{1,\ldots,n\})\setminus\{\emptyset,\{1,\ldots,n\}\}$, $\mathfrak{S} \not\subseteq \mathcal{P}(S)$ for any proper subset S of $\{1,\ldots,n\}$ and n even, Construction 2.2 is not optimal, i.e.,*

$$M(\mathfrak{S}) < \sum_{T\in S} 2^{|T|-1}.$$

We can generalize the idea behind Example 4.2 to get the following theorem:

Theorem 4.4. *Let $\mathfrak{S} = \mathcal{P}(\{1,\ldots,n\})\setminus\{\emptyset,\{1,\ldots,n\}\}$ then*

$$M(\mathfrak{S}) = \begin{cases} \frac{1}{2}(3^n-1) - 2^{n-1} - 1 & \text{for } n \text{ even} \\ \frac{1}{2}(3^n-1) - 2^{n-1} & \text{for } n \text{ odd.} \end{cases}$$

Proof . As in the proof of Theorem 3.4 we use Lemma 3.3 to derive inequalities in l_T and h_T. Especially for $T = \{1, \ldots, i-1, i+1, \ldots n\}$ we find $h_T \leqslant M(\mathfrak{S})$ and as in the proof of Theorem 3.4 we see that for a scheme with minimal pixel expansion these inequalities are satisfied with equality.

Now we consider a set $S \neq \emptyset$. Without loss of generality we assume $n \in S$. Now we set $r_{\{1,\ldots,n-1\}} = M(\mathfrak{S})$ and thus $r_{\{1,\ldots,n\}} = M(\mathfrak{S})$ in Lemma 3.3. We choose the remaining values as in the proof of Theorem 3.4 and find

$$\sum_{\substack{S \subseteq T \subseteq \{1,\ldots,n\} \\ |S| \equiv |T| \bmod 2}} h_T \leqslant \sum_{\substack{S \subseteq T \subseteq \{1,\ldots,n\} \\ |S| \not\equiv |T| \bmod 2}} l_T$$

where we formally set $l_{\{1,\ldots,n\}} = h_{\{1,\ldots n\}} = M(\mathfrak{S})$. Following the arguments in the proof of Theorem 3.4 we see that in a scheme with minimal pixel expansion these inequalities are satisfied with equality and therefore

$$h_S = M(\mathfrak{S}) - \sum_{S \subsetneq T \subsetneq \{1,\ldots n\}} 2^{|T|-1-|S|}$$

(compare Eq. (7)).

Now we set $S = \emptyset$. Lemma 3.3 yields

$$\pm r_{\{1,\ldots n\}} + \sum_{\substack{T \subsetneq \{1,\ldots,n\} \\ |T| \text{ even}}} \overline{h}_T \leqslant \sum_{\substack{T \subsetneq \{1,\ldots,n\} \\ |T| \text{ odd}}} \overline{l}_T. \tag{10}$$

where the sign of $r_{\{1,\ldots,n\}}$ depends on the parity of n. From this inequality we get a bound for $M(\mathfrak{S})$, i.e., for the pixel expansion.

If n is even the sign of $r_{\{1,\ldots,n\}}$ is positive and thus we choose $r_{\{1,\ldots,n\}} = l_{\{1,\ldots,n-1\}} = M(\mathfrak{S}) - 1$ to get the lowest possible bound. For n odd the sign of $r_{\{1,\ldots,n\}}$ is negative and thus we choose $r_{\{1,\ldots,n\}} = M(\mathfrak{S})$ to get the lowest possible bound.

As in Theorem 3.4 we can solve inequality (10) and get

$$M(\mathfrak{S}) \geqslant \begin{cases} \frac{1}{2}(3^n - 1) - 2^{n-1} - 1 & n \text{ even} \\ \frac{1}{2}(3^n - 1) - 2^{n-1} & n \text{ odd.} \end{cases}$$

We have already seen that these bounds are sharp (Example 4.2 and the preceding remark). □

To illustrate Theorem 4.4 we give two examples.

Example 4.5. Perhaps the difference between the construction of Theorem 4.4 and Construction 2.2 or a $(\mathcal{P}(\{1,\ldots,n\})\backslash\{\emptyset\})$-extended visual cryptography scheme with degenerated contrast values can be best understood in the simple case $n = 2$, i.e., in the case of an $\{\{1\},\{2\}\}$-extended visual cryptography scheme.

Construction 2.2 requires two subpixels. On the first transparency the second subpixel is always black and the image is represented by the first subpixel. On the second transparency the roles of the subpixels are interchanged. This enforces that the stack of the two transparencies is black.

But we have no restriction on the stack of the two transparencies. Thus the optimal solution is simply to take two "normal" transparencies with no encoding. This is exactly the solution produced by Theorem 4.4 in the case $n = 2$.

We can view this as follows:

Construction 2.2 guarantees that the stack of the transparencies τ_i with $i \in S$ does not reveal any information about the images I_T with $T \neq S$. But if we can stack all transparencies τ_i with $i \in S$ we can also stack the transparencies τ_i with $i \in S'$ for each subset S' of S. Thus the guarantees of Construction 2.2 are too strong. We only need that the stack of the transparencies τ_i with $i \in S$ does not reveal any information about the images I_T with $T \not\subseteq S$. (Note that in the situation in "ordinary" secret sharing we have a corresponding requirement. If S is a qualified subset we require that all supersets of S are qualified, too.)

Although this example is a good illustration it is not so interesting, since no image is reconstructed by a proper stack of transparencies. For this reason we give a more complex example with four transparencies.

Example 4.6. Now we look at the construction of the $(\mathcal{P}(\{1,\ldots,4\})\backslash\{\{1,2,3,4\},\emptyset\})$-extended visual cryptography scheme. By Theorem 4.4 this scheme requires 31 subpixels and hence the contrast is $\frac{1}{31}$. This is too small for a physical realization. Furthermore the 15 possible images imply 2^{15} possible white/black combinations and therefore the formal description of a $(\mathcal{P}(\{1,\ldots,4\})\backslash\{\{1,2,3,4\},\emptyset\})$-extended visual cryptography scheme requires 2^{15} multisets of 4×31 boolean matrices.

Thus we restrict ourselves to a $\{\{1,2,3\},\{1,2,4\},\{1,3,4\},\{2,3,4\}\}$-extended visual cryptography scheme. If we use degenerated contrast values in the construction of Theorem 4.4 we need 15 subpixels whereas Construction 2.2 needs 16 subpixels.

There are five different cases. The first case is that all images show a white pixel. In this case the multiset $C^{\emptyset}$ contains the matrix

$$B_0 = \begin{pmatrix} 1&1&1&0&0&0&1&1&1&1&1&1&0&0&0 \\ 1&0&0&1&1&0&1&1&1&1&0&0&1&1&0 \\ 0&1&0&1&0&1&1&1&0&0&1&1&1&1&0 \\ 0&0&1&0&1&1&0&0&1&1&1&1&1&1&0 \end{pmatrix}$$

and all matrices obtained by permutations of columns of B_0.

Representative for the case that one image shows a black pixel and the other images show white pixels we construct the multiset $C^{\{\{1,2,3\}\}}$. This multiset contains

$$B_1 = \begin{pmatrix} 1&0&0&1&0&0&1&1&1&1&1&1&1&0&0 \\ 0&1&0&0&1&0&1&1&1&1&1&0&0&1&1 \\ 0&0&1&0&0&1&1&1&1&0&0&1&1&1&1 \\ 0&0&0&1&1&1&0&0&0&1&1&1&1&1&1 \end{pmatrix}$$

and all column permutations of that matrix.

Representative for the case that two images show a black pixel and the other images show white pixels we construct the multiset $C^{\{\{1,2,3\},\{1,2,4\}\}}$. This multiset contains

$$B_2 = \begin{pmatrix} 1\,0\,1\,1\,0\,0\,0\,0\,1\,1\,1\,1\,1\,0\,1 \\ 0\,1\,0\,0\,1\,1\,0\,0\,1\,1\,1\,1\,0\,1\,1 \\ 0\,0\,1\,0\,1\,0\,1\,1\,1\,1\,0\,0\,1\,1\,1 \\ 0\,0\,0\,1\,0\,1\,1\,1\,0\,0\,1\,1\,1\,1\,1 \end{pmatrix}$$

and all its column permutations.

Representative for the case that three images show a black pixel and only one image shows a white pixel we construct the multiset $C^{\{\{1,2,3\},\{1,2,4\},\{1,3,4\}\}}$. This multiset contains

$$B_3 = \begin{pmatrix} 1\,1\,1\,1\,0\,0\,0\,0\,0\,0\,1\,1\,1\,1\,1 \\ 0\,1\,0\,0\,1\,1\,1\,1\,0\,0\,1\,1\,0\,1\,1 \\ 0\,0\,1\,0\,1\,1\,0\,0\,1\,1\,1\,0\,1\,1\,1 \\ 0\,0\,0\,1\,0\,0\,1\,1\,1\,1\,0\,1\,1\,1\,1 \end{pmatrix}$$

and all column permutations of that matrix.

Finally we have to construct the multiset $C^{\{\{1,2,3\},\{1,2,4\},\{1,3,4\},\{2,3,4\}\}}$ which represents the case that all images show a black pixel. This multiset contains

$$B_4 = \begin{pmatrix} 1\,1\,1\,1\,1\,1\,0\,0\,0\,0\,0\,0\,1\,1\,1 \\ 1\,1\,0\,0\,0\,0\,1\,1\,1\,1\,0\,0\,1\,1\,1 \\ 0\,0\,1\,1\,0\,0\,1\,1\,0\,0\,1\,1\,1\,1\,1 \\ 0\,0\,0\,0\,1\,1\,0\,0\,1\,1\,1\,1\,1\,1\,1 \end{pmatrix}$$

and all its column permutations.

As one can check these multisets satisfy Definition 2.1. For example, if we choose $\{i_1,\ldots,i_q\} = \{1,2\}$ in the second condition, Definition 2.1 claims that the first two rows of the matrices $B_0,\ldots,B_4$ may only differ in a column permutation and indeed in all matrices these rows are a permutation of

$$\begin{pmatrix} 0\,0\,1\,1\,1\,1\,0\,0\,0\,0\,1\,1\,1\,1\,1 \\ 0\,0\,0\,0\,0\,0\,0\,1\,1\,1\,1\,1\,1\,1\,1 \end{pmatrix}.$$

We now prove two useful recursion formulas for the minimal pixel expansion $M(\mathfrak{S})$.

Lemma 4.7. *Let $\mathfrak{S} \subseteq \mathcal{P}(S)$ and $\mathfrak{T} \subseteq \mathcal{P}(T)$. If $S \cap T = \emptyset$ we have*

$$M(\mathfrak{S} \cup \mathfrak{T}) \leqslant \max\{M(\mathfrak{S}), M(\mathfrak{T})\}.$$

Proof . Let $m = \max\{M(\mathfrak{S}), M(\mathfrak{T})\}$. We can construct an $\mathfrak{S}$- and $\mathfrak{T}$-extended scheme with m subpixels each. (Just add unnecessary white subpixels.) The transparencies of these schemes form together an $(\mathfrak{S} \cup \mathfrak{T})$-extended scheme. □

Lemma 4.8. *Let $\mathfrak{S} \subseteq \mathcal{P}(\{1,\ldots,m\})$ and $\mathfrak{S} \subseteq \mathfrak{T} \subseteq \mathcal{P}(\{1,\ldots,n\})$. If*

$$(\mathfrak{T} \backslash \mathfrak{S}) \cap \mathcal{P}(\{1,\ldots m\}) = \emptyset,$$

then

$$M(\mathfrak{T}) \leqslant M(\mathfrak{S}) + \sum_{T \in \mathfrak{T} \setminus \mathfrak{S}} 2^{|T|-1}.$$

Proof . The idea of the proof is basically the same as behind Construction 2.2.

We use $M(\mathfrak{S})$ subpixels to construct an $\mathfrak{S}$-extended visual cryptography scheme. For each $T \in \mathfrak{T} \setminus \mathfrak{S}$ we use $2^{|T|-1}$ subpixels to construct the $|T|$-out-of-$|T|$ visual cryptography scheme described in [5]. For each participant i with $1 \leqslant i \leqslant m$ we set the subpixels belonging to the $|T|$-out-of-$|T|$ visual cryptography schemes with $i \notin T$ black and for each participant j with $m < j \leqslant n$ we set the subpixels belonging to the $\mathfrak{S}$-extended visual cryptography scheme and all pixels belonging to a $|T|$-out-of-$|T|$ visual cryptography schemes with $j \notin T$ black.

Formally we start with the contrast values h_S, l_S ($S \in \mathcal{P}(\{1, \ldots, m\})$) of the $\mathfrak{S}$-extended visual cryptography scheme and define the contrast values of the $\mathfrak{T}$-extended visual cryptography scheme by

$$\hat{h}_S = \begin{cases} M(\mathfrak{S}) + \sum_{S' \in \mathfrak{T} \setminus \mathfrak{S}} 2^{|S'|-1} - \sum_{\substack{S' \in \mathfrak{T} \setminus \mathfrak{S} \\ S \subsetneq S'}} 2^{|S'|-1-|S|} & \text{for } S \not\subseteq \{1, \ldots, m\} \\ h_S + \sum_{S' \in \mathfrak{T} \setminus \mathfrak{S}} 2^{|S'|-1} - \sum_{\substack{S' \in \mathfrak{T} \setminus \mathfrak{S} \\ S \subsetneq S'}} 2^{|S'|-1-|S|} & \text{for } S \subseteq \{1, \ldots, m\} \end{cases}$$

and check that the restrictions of Lemma 3.3 are satisfied. □

If we apply this Lemma to Example 4.2 we get:

Corollary 4.9. *Let $\mathfrak{S} \subseteq \mathcal{P}(\{1, \ldots, n\}) \setminus \{\emptyset\}$. Let us assume that there exists a non-empty subset $T \in \mathcal{P}(\{1, \ldots, n\}) \setminus \mathfrak{S}$ with $|T|$ even and that $\mathfrak{S} \cap \mathcal{P}(T) \not\subseteq \mathcal{P}(T')$ for each proper subset T' of T. Then Construction 2.2 is not optimal.*

Note that with the trivial bound $M(\emptyset) = 0$ Lemma 4.8 yields

$$M(\mathfrak{S}) \leqslant \sum_{T \in \mathfrak{S}} 2^{|T|-1},$$

i.e., the bound given by Construction 2.2.

5. Conclusions and further remarks

Eq. (3) gives us a simple method to construct an $\mathfrak{S}$-extended visual cryptography scheme with given contrast values l_T and h_T. Furthermore, for fixed n and $\mathfrak{S}$, Eq. (3) leads to a linear programming problem which describes all possible $\mathfrak{S}$-extended visual cryptography schemes. For small values of n this problem can easily be solved.

In this article, we have given a full solution for the special cases $\mathfrak{S} = \mathcal{P}(\{1, \ldots, n\}) \setminus \{\emptyset\}$ and $\mathfrak{S} = \mathcal{P}(\{1, \ldots, n\}) \setminus \{\emptyset, \{1, \ldots, n\}\}$. We close by presenting the following open problems:

(1) We conjecture: Let $\mathfrak{S} \subseteq \mathcal{P}(\{1,\ldots,n\})\backslash\{\emptyset\}$. Then Construction 2.2 is optimal for an $\mathfrak{S}$-extended visual cryptography scheme if and only if for all $\emptyset \neq T \notin \mathfrak{S}$ we have either $|T|$ odd or $\mathfrak{S} \cap \mathcal{P}(T) \subseteq \mathcal{P}(T')$ for some proper subset T' of T.
(2) An even harder problem is a full characterization of $\mathfrak{S}$-extended visual cryptography schemes with minimal pixel expansion for arbitrary subsets $\mathfrak{S}$ of $\mathcal{P}(\{1,\ldots,n\})$, i.e., to find a formula for the minimal pixel expansion $M(\mathfrak{S})$ depending on $\mathfrak{S}$.

References

[1] G. Ateniese, C. Blundo, A. De Santis, D.R. Stinson, Constructions and bounds for visual cryptography, in: ICALP, Lect. Notes Comput. Sci., vol. 1099, Springer, Berlin, 1996, pp. 416–428.
[2] G. Ateniese, C. Blundo, A. De Santis, D.R. Stinson, Visual cryptography for general access structures, Inform. Comput. 195 (2) (1996) 86–106.
[3] G. Ateniese, C. Blundo, A. De Santis, D.R. Stinson, Extended capabilities for visual cryptography, Theor. Comput. Sci. 250 (1–2) (2001) 143–161.
[4] S. Droste, New results in visual cryptography, in: Advances inCryptology—CRYPTO'96, Lect. Notes Comput. Sci., vol. 1109, Springer, Berlin, 1996, pp. 401–415.
[5] M. Naor, A. Shamir, Visual cryptography, in: A. De Santis (Ed.), Advances inCryptology—EUROCRYPT'94, Lect. Notes Comput. Sci., vol. 950, Springer, Berlin, 1994, pp. 1–12.