

How to say yes, no and maybe with visual cryptography

Andreas Klein*

Ghent University

Dept. of Pure Mathematics and Computer Algebra

Krijgslaan 281-S22, 9000 Ghent, Belgium

January 11, 2008

Abstract

We present a version of a visual cryptography scheme in which a qualified set of participants is able to block the reconstruction of the secret.

1 Introduction

In [1] the concept of $(t; s)$ -threshold schemes was introduced as an extension of secret sharing schemes, in which each participant can say yes or no. Each t participants can reconstruct the secret if at most $s - 1$ participants say no, but if at least s participants say no it is impossible to reconstruct the secret. The scheme uses a trusted black box as combiner to prevent the participants who say yes from ignoring the vetos.

This article presents a secret sharing scheme in which some participants can block the reconstruction, which does not require a black box as combiner. The idea is the following:

Every person gets three shares: one for yes, one for no and one for maybe. The protocol forces every participant to submit one of his three shares. (We can sign the shares to make sure that a dishonest participant will not be able to submit a faked share. For the case of visual cryptography, such a signature is described in [4, 5].) The secret will be reconstructed if and only if a qualified set of participants says yes, but no qualified set of participants says no. Furthermore we require that no extra information of who says yes and no is revealed. The scheme must also make sure that a set of dishonest participants have no chance to learn the secret by mixing their shares.

*The research of the author takes place within the project "Linear codes and cryptography" of the Fund for Scientific Research Flanders (FWO-Vlaanderen) (Project nr. G.0317.06), and is supported by the Interuniversity Attraction Poles Programme-Belgian State-Belgian Science Policy: project P6/26-Bcrypt.

In this article we will use visual cryptography [7] to construct such a scheme. The work is organised as follows. In the next section we give a formal definition of the scheme and prove that every visual cryptography scheme that follows the specification has the required features. Then we show how to describe an optimal visual cryptography scheme with vetos as linear program. We will use this technique to find good solutions for cases with a small number of participants. In section 4 we use extended visual cryptography to prove that every access structure is realizable. Our proof is constructive and therefore we obtain a lower bound on the attainable contrast and an upper bound on the attainable pixel expansion. At the end of the article we will discuss possible extensions of the scheme.

2 The model

We identify the participants with the numbers $1, \dots, n$. An *access structure* is a proper subset Γ of $\mathcal{P}(\{1, \dots, n\})$ with the property: $A \in \Gamma \wedge A \subset B \implies B \in \Gamma$. The most important access structure is the *k-out-of-n* structure which consists of all sets of size at least k .

A scheme with vetos is described by two access structures Γ_{Yes} and Γ_{No} . These access structures must satisfy the *consistency* properties:

1. $A \notin \Gamma_{\text{Yes}} \implies \bar{A} \in \Gamma_{\text{No}}$. (I.e. if the coalition A is not able to reconstruct the secret then the complement of A can block the reconstruction.)
2. $A \notin \Gamma_{\text{No}} \implies \bar{A} \in \Gamma_{\text{Yes}}$.

In the case that Γ_{Yes} is an *l-out-of-n* and Γ_{No} is a *k-out-of-n* access structure the consistency conditions imply $l + k \leq n + 1$. In the case $l + k = n + 1$ the scheme with vetos reduces to a simple *l-out-of-n* scheme, since if at least k participants say no at most $n - k = l - 1$ participants can say yes and the secret would not be reconstructed any way. In general we must require that there exists an $A \in \Gamma_{\text{Yes}}$ and $B \in \Gamma_{\text{No}}$ with $A \cap B = \emptyset$ to obtain anything different from conventional secret sharing.

We say that a participant i *can say yes* if there is a set A with $A \notin \Gamma_{\text{Yes}}$, but $A \cup \{i\} \in \Gamma_{\text{Yes}}$, i.e. i is a member of at least one minimal yes-coalition. With P_{Yes} we denote the set of all participants that can say yes. In the same manner we define the set P_{No} of all participants who *can say no*. A participant who can say neither yes nor no is not needed in the scheme, so we can restrict ourselves to *non degenerated* schemes with $P_{\text{Yes}} \cup P_{\text{No}} = \{1, \dots, n\}$.

We define now a visual cryptography scheme with vetos. As usual in visual cryptography [7] we describe the scheme as two multisets Γ_W (the encoding rule for a white pixel) and Γ_B (the encoding rule for a black pixel) of boolean matrices. The rows of the matrices describe the different participants and the columns describe the different subpixels.

Definition 1

Let Γ_{Yes} and Γ_{No} be two access structures that satisfy the restrictions described above and let $N = n + |P_{\text{Yes}}| + |P_{\text{No}}|$.

A visual cryptography scheme with veto consists of two multisets Γ_B and Γ_W of binary $N \times m$ matrices with the following properties.

1. The N rows of each matrix are indexed by (i, M) ($i \in \{1, \dots, N\}$), (i, Y) ($i \in P_{\text{Yes}}$) and (i, N) ($i \in P_{\text{No}}$). For the rest of the article we assume that the order of rows is $(1, Y)$, $(1, M)$, $(1, N)$, $(2, Y)$, \dots , (n, N) .
2. If we delete the rows with index of the form $(i, *)$ we obtain either a multiset of $(N - 2) \times m$ or $(N - 3) \times m$ matrices, depending on whether i lies only in one or both sets P_{Yes} and P_{No} .

These matrices satisfy:

- (a) We obtain the same multiset if we apply this operation to the matrices in Γ_B on Γ_W , respectively.
 - (b) Furthermore if we interchange in all those matrices two rows with indices of the form $(j, *)$, $(j, *')$ then the multiset does not change.
3. If we choose n rows with indices $(1, *)$, \dots , $(n, *)$ and restrict the matrices to that rows we obtain multisets Γ'_W and Γ'_B . Each matrix in Γ'_W contains the same number N_W of zero columns and each matrix in Γ'_B contains the same number N_B of zero columns. Furthermore the multisets Γ'_W and Γ'_B satisfy the properties:
 - (a) If either the row indices of the form $(i_1, N), \dots, (i_k, N)$ satisfy $\{i_1, \dots, i_k\} \in \Gamma_{\text{No}}$ or the row indices of the form $(i_1, Y), \dots, (i_l, Y)$ do not satisfy $\{i_1, \dots, i_l\} \in \Gamma_{\text{Yes}}$ then the multisets Γ'_W and Γ'_B equal the same multiset Γ . This multiset is independent of the choice of the row indices $(1, *)$, \dots , $(n, *)$ as long as the conditions stated above are satisfied.
 - (b) If the row indices of the form $(i_1, Y), \dots, (i_l, Y)$ satisfy $\{i_1, \dots, i_l\} \in \Gamma_{\text{Yes}}$ and the row indices of the form $(i_1, N), \dots, (i_k, N)$ do not satisfy $\{i_1, \dots, i_k\} \in \Gamma_{\text{No}}$, then $N_W < N_B$. Furthermore the multisets Γ'_W and Γ'_B are independent from the choice of $(1, *)$, \dots , $(n, *)$ as long as the condition stated above is satisfied.

The dealer will encode an image by the following operation. He divides every pixel in m subpixels and chooses a random element C of Γ_W or Γ_B depending on whether the point is white or black. He colours the subpixel number j on transparency i black if and only if the element in the i -th row and j -th column of C is 1.

The quality of a visual cryptography scheme is measured by three values: the contrast $\alpha = \frac{N_B - N_W}{m}$ which is the relative difference between the number of black subpixels needed to represent a black and white pixel, the pixel expansion m and the randomness $r = |\Gamma_W| = |\Gamma_B|$. The contrast is considered to be

the most important parameter and the randomness is considered to be the least important parameter. Therefore almost all constructions of visual cryptography schemes aim at maximising the contrast before trying to minimise the pixel expansion. Most schemes use the trivial bound $r \leq m!$ for the randomness. There are only few results on the randomness (see [2]) and these deal mostly with finding the minimal randomness in the class of all schemes with optimal contrast and minimal pixel expansion. In this paper we will focus on existence results and the contrast.

We summarise the properties of the scheme in the following theorem.

Theorem 2

The visual cryptography scheme described by Definition 1 has the following properties. If less than n participants meet they obtain no information on the secret image. Furthermore no one can prove to the other persons which of his transparencies is the yes, no or maybe transparency.

If each one of the n participants submits exactly one of his transparencies the secret image is revealed if and only if a coalition described in Γ_{yes} submits their yes transparencies and the set $\{i_1, \dots, i_k\}$ of persons which submit their no transparencies is not in Γ_{No} . If the secret image is not revealed the n transparencies do not contain any information about the secret image.

In addition to the fact whether the image is reconstructed or not no participant gain any information on the decisions of the other participants.

Proof. Condition 3b of Definition 1 says that in the stack of an allowed coalition a white pixel will be represented by N_W white subpixels and a black pixel will be represented by N_B black subpixels. Since $N_W < N_B$ we can see the secret image. If the stack does not belong to an allowed coalition the distribution of black subpixels is independent from the colour of the corresponding pixel (Condition 3a of Definition 1), i.e. we do not see the image.

Now we have to investigate the security of the system. A group of up to $n - 1$ attackers can digitalize their slides. By this operation they learn per pixel a $k \times m$ matrix G which must be either a submatrix of some matrix in Γ_W or Γ_B . Let m_W be the number of matrices in Γ_W which contain G as submatrix and let m_B be the number of matrices in Γ_B which contain G . Then we obtain the conditional probability that the pixel is black as

$$p(B|G) = \frac{p(B)m_B}{p(B)m_B + p(W)m_W} ,$$

where $p(B)$ and $p(W)$ denotes the probability that the pixel is black or white, respectively. Condition 2a of Definition 1 states that $m_B = m_W$ and thus $p(B|G) = p(B)$ which means that the attackers do not gain information on the encoded image.

Similarly Condition 2b of Definition 1 states that if participant number j presents the other attackers a (random) permutation of his slides the a posteriori distribution of the permutation is equal the a priori distribution, i.e. the others do not learn which of his slides is for yes, no and maybe.

The requirement $\Gamma'_W = \Gamma'_B$ (Condition 3a in Definition 1) guarantees us that the slides of a forbidden collation contain no information on the colour of the encoded image.

The requirement that the multisets Γ'_W and Γ'_B are independent from the choice of $(1, *)$, \dots , $(n, *)$ as long as the outcome (reconstruction of the image or not) stays the same in Condition 3a and 3b of Definition 1 guarantees that the decisions of the different participants remain secret. \square

3 Formulation as a linear program

We will now show how to find an optimal visual cryptography scheme with vetos via linear programming.

We will not care about the randomness of the scheme, therefore we may assume that Γ_W and Γ_B contain together with a matrix C also all column permutations of C . Thus we must only consider the fraction of dark subpixels.

By $x_T^{(W)}$, $\emptyset \neq T \subseteq \{(1, Y), \dots, (n, N)\}$ we denote the fraction of subpixels of a white pixel that are black on the transparencies denoted by the elements of T and white on the other transparencies. By $g_T^{(W)}$ we denote the fraction of black subpixels in a white pixel in the stack of the transparencies described by T . For black pixels we describe the corresponding fractions by $x_T^{(B)}$ and $g_T^{(B)}$. The variables $x_T^{(W)}$, $g_T^{(W)}$, $x_T^{(B)}$ and $g_T^{(B)}$ describe fractions, i.e. they lie in the interval $[0, 1]$.

We can compute $g_T^{(W)}$ from the corresponding $x_*^{(W)}$ via

$$g_T^{(W)} = \sum_{S, S \cap T \neq \emptyset} x_S^{(W)} .$$

In matrix notation we write

$$g^{(W)} = Mx^{(W)} \tag{1}$$

where $g^{(W)} = (g_T^{(W)})_{T \subseteq \{(1, Y), \dots, (n, N)\}}$, $x^{(W)} = (x_T^{(W)})_{T \subseteq \{(1, Y), \dots, (n, N)\}}$ and $M = (m_{T, S})_{T, S \subseteq \{(1, Y), \dots, (n, N)\}}$ with

$$m_{T, S} = \begin{cases} 1 & T \cap S \neq \emptyset \\ 0 & T \cap S = \emptyset \end{cases} .$$

Similarly we obtain

$$g^{(B)} = Mx^{(B)} . \tag{2}$$

In [6] it was proved that M is invertible and M^{-1} contains only 0 and ± 1 as entry.

Condition 2a of Definition 1 says that we can not distinguish a white pixel from a black pixel without using a transparency from person i . That means that the following gray levels have to be equal:

$$g_T^{(W)} = g_T^{(B)} \quad \text{for all } T \text{ with } T \cap \{(i, Y), (i, M), (i, N)\} = \emptyset. \tag{3}$$

In addition (Condition 2b of Definition 1) we should not be able to tell whether two rows of the form $(j, *)$ are swapped or not. We can formulate this as: Let T be a set with

$$T \cap \{(i, Y), (i, M), (i, N), (j, Y), (j, M), (j, N)\} = \emptyset$$

then the following equations hold

$$g_{T \cup \{(j, Y)\}}^{(W)} = g_{T \cup \{(j, M)\}}^{(W)} = g_{T \cup \{(j, N)\}}^{(W)} \quad (4)$$

and

$$g_{T \cup \{(j, Y), (j, M)\}}^{(W)} = g_{T \cup \{(j, Y), (j, N)\}}^{(W)} = g_{T \cup \{(j, M), (j, N)\}}^{(W)}. \quad (5)$$

Note that by (3) we have $g_{T \cup \{(j, Y)\}}^{(W)} = g_{T \cup \{(j, Y)\}}^{(B)}$ and so on, so we must not consider the values of $g^{(B)}$ in the equations (4) and (5).

We can express Condition 3a of Definition 1 as

$$g_T^{(W)} = g_T^{(B)} = g \quad (6)$$

for all T of the form $T = \{(1, *), \dots, (n, *)\}$ where either a qualified set says no or no qualified set says yes.

Condition 3b is expressed as

$$g_T^{(W)} = g^{(W)} \quad \text{and} \quad g_T^{(B)} = g^{(B)} \quad (7)$$

for all T of the form $T = \{(1, *), \dots, (n, *)\}$ where a qualified set says yes but no qualified set says no.

The goal is to maximise the contrast which is $g^{(B)} - g^{(W)}$.

3.1 A small example

In this subsection we use the linear program to solve the case of two participants where Γ_{Yes} and Γ_{No} are the 1-out-of-2 access structure. In this particular simple case the contrast will be $\frac{1}{3}$ which makes it an ideal example.

The linear program consists of 255 variables and 163 constraints. With the computer we find the optimal solution in less than a second. For the given example the contrast is $\alpha = \frac{1}{3}$. It is a bit more difficult to find a solution with minimal pixel expansion. To do this we declare the variables $x_T^{(W)}$, $g_T^{(W)}$, $x_T^{(B)}$ and $g_T^{(B)}$ to be integers and add the constraint

$$g^{(B)} - g^{(W)} = \alpha g_{\{(1, Y), \dots, (n, N)\}}^{(B)}. \quad (8)$$

The new goal is to minimise the pixel expansion $m = g_{\{(1, Y), \dots, (n, N)\}}^{(B)}$. This integer program is more difficult to solve. In the case of the example it is still very fast, but for more complicated access structures the determination of the optimal m can take several hours.

The final solution is that Γ_W consists of all column permutations of

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

and that Γ_B consists of all column permutations of

$$C_B = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}.$$

Lets us check the multisets defined by this describe indeed a visual cryptography scheme with vetos.

First we observe that every row in C_W and C_B has six nonzero entries. Thus on every transparency the fraction of black subpixels is $\frac{6}{12}$ and we can not tell which transparency has which role.

Furthermore if we restrict the matrices C_W and C_B to the first three rows (encoding the yes, maybe and no transparency of the first participant), we see in both cases a column permutation of

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

Thus the first participant alone obtains no information on the encoded image. Similarly we check that the second participant obtains no information on the encoded image.

Now check for example that the first participant says yes (first row) and the second participant says maybe (fifth row). The matrix C_W contains 5 columns with zero entry in both rows, so the fraction of black subpixels in a white pixel will be $\frac{7}{12}$. The matrix C_B contains only one column which has zero entry in both rows, i.e. the fraction of black subpixels in a black pixel will be $\frac{11}{12}$. This gives a contrast of $\alpha = \frac{11}{12} - \frac{7}{12} = \frac{1}{3}$.

Now let us check the case that the first participant says no (third row) and the second participant says yes (fourth row). In this case we see that in C_W and C_B there are exactly 3 columns with zero entry in both rows, i.e. no image is reconstructed.

4 Proof of existence

In this section we will use extended visual cryptography to construct veto schemes for any given access structure. In this way we prove that the linear

program found in the previous section always has a feasible solution.

In extended visual cryptography every of the $2^n - 1$ possible stacks of n slides may reveal an different image. In [7] the possibility of an extended visual cryptography scheme with two slides is shown. In [3] the problem was solved for every number of slides. In general (no relation between the different images every stack of transparencies shows an image) an extended visual cryptography scheme with n slides needs $m = \frac{1}{2}(3^n - 1)$ subpixels and has a contrast of $\alpha = \frac{1}{m}$. In [6] this was shown to be optimal.

We will use the construction described in [3]. This construction works as follows.

Let $\mathfrak{S} \subseteq \mathcal{P}(\{1, \dots, n\}) \setminus \{\emptyset\}$ and assume that for every $T \in \mathfrak{S}$ the stack the corresponding slides reveals an (different) image. Such a scheme is called a \mathfrak{S} -extended visual cryptography scheme.

It is possible to construct extended visual cryptography schemes from k -out-of- k schemes.

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 the transparency i will be black. The \mathfrak{S} -extended visual cryptography scheme is achieved by putting all these schemes together.

A more detailed description and a proof of correctness can be found in [3].

To construct a veto-scheme we need one n -out-of- n scheme for every possible choice of yes, no and maybe. If every participant has all three choices this means that we need 3^n different n -out-of- n schemes. For simplicity we assume that this is the case. Thus our scheme with vetos will use $m = 3^n \cdot 2^{n-1}$ subpixels and the contrast will be $\alpha = \frac{1}{m}$.

For each of 3^n possible choices of yes, no and maybe we use the corresponding 2^{n-1} subpixels to construct an n -out-of- n scheme. If the choice is allowed to reconstruct the image we use the n -out-of- n scheme to encode the secret image. If the choice is not allowed to reconstruct the image we use the n -out-of- n scheme to encode a completely white image. On the $2n$ other transparencies we colour these 2^{n-1} subpixels black.

Before we prove that this extended visual cryptography scheme satisfies the definition of a veto scheme (Definition 1), we give an example of the construction.

Example 3

We use now extended visual cryptography to construct a scheme with Γ_{Yes} and Γ_{No} being the 1-out-of-2 access structure.

We need $m = 2 \cdot 3^2 = 18$ subpixels for the construction. For each possible choice of yes, no and maybe we must choose two subpixels. For example choose the first two subpixels for (Y, Y) . The other choices follow in the order (Y, M) , (Y, N) , (M, Y) , \dots , (N, N) .

Then we obtain that Γ_W consists of all column permutations of

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

and that Γ_B consists of all column permutations of

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

To understand the construction look at the first two columns. They should encode the image that is visible if both participants submit their yes transparency. On the maybe and no transparencies the subpixels are both black (entry 1,1 in the rows 2, 3, 5 and 6). On the yes slides we see a simple 2-out-of-2 scheme described by the matrices $\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}$ and $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ for a white and a black pixel, respectively.

Now look on the fifth and sixth column. These two columns corresponds to participant 1 says yes, but participant 2 says no. Here we see 1,1 in the rows 2, 3, 4 and 5 corresponding to the maybe and no transparency of participant 1 and the yes and maybe transparency of participant 2. In the rows 1 and 6 we see a 2-out-of-2 scheme, but since participant 2 says no the image is not reconstructed, which means that we see the same submatrix $\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}$ in C_W and C_B .

Now we prove that the extended visual cryptography scheme is indeed a veto scheme.

Theorem 4

The extended visual cryptography scheme described above satisfies the conditions of Definition 1.

Proof. Let us recall some basic properties of an n -out-of- n scheme defined in [7]. The pixel expansion is 2^{n-1} and in a stack of $k < n$ slides exactly $2^{n-1} - 2^{n-k-1}$ subpixels are black.

Now look at the extended visual cryptography scheme. Since we assume that Γ_{Yes} and Γ_{No} contain with a matrix all its column permutations, we must only check the fraction of black subpixels.

By definition the stack of two transparencies that belongs to one participant is completely black. (Remember that the 2^{n-1} subpixels that correspond to a choice $(1, *)$, \dots , $(n, *)$ are black on the other $2n$ transparencies.)

Thus we must investigate only the cases in which k participants submit one transparency τ_1, \dots, τ_k each. If $k < n$ then the $n - k$ remaining participants have 3^{n-k} different possibilities to choose one transparency each. For each of these 3^{n-k} choices there exists an n -out-of- n scheme. In the stack of τ_1, \dots, τ_k exactly $2^{n-1} - 2^{n-k-1}$ of the 2^{n-1} subpixels in such an n -out-of- n scheme are black.

By the construction of the extended visual cryptography scheme we know that in the stack of τ_1, \dots, τ_k every subpixel that does not belong to one of these 3^{n-k} n -out-of- n schemes is black any way. Therefore the number of black subpixels in the stack of τ_1, \dots, τ_k is $3^n 2^{n-1} - 3^{n-k} 2^{n-k-1}$.

The number of black subpixels depends only on k , but not on the choice (Yes, No or Maybe) of the k participants, nor on the colour of the encoded pixel. This proves that $k < n$ participants gain no information on the encoded image and that no information on the choice (Yes, No or Maybe) of the k participants is leaked.

If every person submits one slide the following happens. The $(3^n - 1)2^{n-1}$ subpixels which do not belong to the selection will be black. In the remaining 2^{n-1} subpixels we see an n -out-of- n scheme. If the selection is not allowed to reconstruct the secret the scheme encodes a white pixel, i.e. exactly one of the $3^n 2^{n-1}$ subpixel remains white. In this case we gain no information on the secret image.

If the choice is allowed to reconstruct the image, then either $2^{n-1} - 1$ or 2^{n-1} of the 2^{n-1} subpixels in the n -out-of- n scheme are black, i.e. we see the image with a contrast of $\frac{1}{m}$. \square

Finally one word on the randomness of the scheme. We assume for simplicity that Γ_{Yes} and Γ_{No} contain with a matrix all its column permutations. This would lead to a randomness of $r = m! = (3^n 2^{n-1})!$. But it is enough to choose for each participant i a cyclic permutation π_i which maps the subpixels corresponding to his yes choices to the subpixels corresponding to his maybe choices, the maybe choices, to the no choices and the no choices back to the yes choices. Then we have to choose a random element of $\langle \pi_1, \dots, \pi_n \rangle$ to obtain a permutation of the 3^n different n -out-of- n schemes. Each of these schemes has a randomness of 2^{n-1} (see [2]), which leads to an overall randomness of $r = 3^n (2^{n-1})^{3^n}$. We need a random number between 1 and 2^{n-1} for each of the 3^n different n -out-of- n schemes (which gives us the factor $(2^{n-1})^{3^n}$) and a random number between 1 and 3^n to choose a random element of $\langle \pi_1, \dots, \pi_n \rangle$ (which gives us the factor 3^n).

5 Variants of veto schemes

We can extend the concept of a veto scheme as follows. Every participant gets k shares. The protocol forces him to submit exactly one of his shares. An

access function $\Gamma : \{1, \dots, k\}^n \rightarrow \{0, 1\}$ describes which selection of shares can reconstruct the secret. The schemes with vetos are a special case with $k = 3$. But there are other access structures like: The secret is reconstructed if and only if an even number of participants say yes.

The construction of Section 4 works for this extension without modification; we need $m = k^n \cdot 2^{n-1}$ subpixels and the contrast will be $\alpha = \frac{1}{m}$.

A further extension of the concept scheme with vetos is the following. We allow a reconstruction, if not every participant submits a share. Formally we have an access structure Γ and for each $S \in \Gamma$ we have an access function $\Gamma_S : \{1, \dots, k\}^{|S|} \rightarrow \{0, 1\}$. The only restriction that must be satisfied is that $\Gamma_S(a_1, \dots, a_{|S|}) = 1$ implies $\Gamma_{S \cup \{s'\}}(a_1, \dots, a_{|S|}, x) = 1$ for every x , i.e. if the persons from S have made a choice which reconstructs the image, then the choice of other participants can not block the reconstruction. This restriction is unavoidable, since we do not use a black box as combiner.

The construction of such a scheme can be done with extended visual cryptography as we used it in Section 4. For each $S \in \Gamma$ we reserve $k^{|S|}$ groups of $2^{|S|-1}$ subpixels. In each group we build a $|S|$ -out-of- $|S|$ scheme which either encodes the secret image if $\Gamma_S(a_1, \dots, a_{|S|}) = 1$ or a totally white image if $\Gamma_S(a_1, \dots, a_{|S|}) = 0$. The proof of Theorem 4 actually shows that such a scheme works.

6 Conclusion

We have introduced a new variant of secret sharing in which a qualified minority can prohibit a reconstruction. We have used visual cryptography to construct examples of such schemes.

References

- [1] A. Beutelspacher. How to say “no”. In *EuroCrypt '89*, volume 434 of *LNCS*, pages 491–496, 1989.
- [2] A. De Bonis and A. De Santies. Randomness in secret sharing and visual cryptography schemes. *Theoretical Computer Science*, 314(3):351–374, 2004.
- [3] S. Droste. New results in visual cryptography. In *Advances in cryptology – CRYPTO '96*, volume 1109 of *Lect. Notes Comput. Sci.*, pages 401–415. Springer, Berlin, 1996.
- [4] G. Horng, T. Chen, and D.-S. Tsai. Cheating in visual cryptography. *Des. Codes Cryptogr.*, 38(2):219–236, 2006.
- [5] A. Klein. *Visuelle Kryptographie*. Springer, 2007.
- [6] A. Klein and M. Wessler. Extended visual cryptography schemes. *Information and Computation*, 205(5):716–732, 2007.

- [7] Moni Naor and Adi Shamir. Visual cryptography. In Alfredo De Santis, editor, *Advances in cryptology - EUROCRYPT '94*, volume 950 of *Lect. Notes Comput. Sci.*, pages 1–12. Springer-Verlag, 1995.