ELSEVIER

Theoretical Computer Science 240 (2000) 471–485

Theoretical Computer Science

www.elsevier.com/locate/tcs

in visual cryptography

Thomas Hofmeister[a], Matthias Krause[b,*], Hans U. Simon[a]

[a] *Lehrstuhl Informatik 2, Universität Dortmund, D-44221 Dortmund, Germany*
[b] *Fachbereich Informatik, Universität Mannheim, D-68131 Mannheim, Germany*

Abstract

Visual cryptography and (k,n)-visual secret sharing schemes were introduced by Naor and Shamir (Advances in Cryptology — Eurocrypt 94, Springer, Berlin, 1995, pp. 1–12). A sender wishing to transmit a secret message distributes n transparencies amongst n recipients, where the transparencies contain seemingly random pictures. A (k,n)-scheme achieves the following situation: If any k recipients stack their transparencies together, then a secret message is revealed visually. On the other hand, if only $k-1$ recipients stack their transparencies, or analyze them by any other means, they are not able to obtain any information about the secret message. The important parameters of a scheme are its contrast, i.e., the clarity with which the message becomes visible, and the number of subpixels needed to encode one pixel of the original picture. Naor and Shamir constructed (k,k)-schemes with contrast $2^{-(k-1)}$. By an intricate result from Linial (Combinatorica 10 (1990) 349–365), they were also able to prove the optimality of these schemes. They also proved that for all fixed $k \leqslant n$, there are (k,n)-schemes with contrast $(2e)^{-k}/\sqrt{2\pi k}$. For $k = 2,3,4$ the contrast is approximately $\frac{1}{105}$, $\frac{1}{698}$ and $\frac{1}{4380}$. In this paper, we show that by solving a simple linear program, one is able to compute *exactly* the best contrast achievable in any (k,n)-scheme. The solution of the linear program also provides a representation of a corresponding scheme. For small k as well as for $k = n$, we are able to analytically solve the linear program. For $k = 2,3,4$, we obtain that the optimal contrast is at least $\frac{1}{4}$, $\frac{1}{16}$ and $\frac{1}{64}$. For $k = n$, we obtain a very simple proof of the optimality of Naor's and Shamir's (k,k)-schemes. In the case $k = 2$, we are able to use a different approach via coding theory which allows us to prove an optimal tradeoff between the contrast and the number of subpixels.

Keywords: Visual cryptography; Secret sharing schemes; Linear programming

1. Introduction

We recall the definition of visual secret sharing schemes given in [6]. In the sequel, we simply refer to them under the notion *scheme*. For a 0–1-vector v, let $H(v)$ denote

* Corresponding author.
E-mail addresses: hofmeist@ls2.informatik.uni-dortmund.de (T. Hofmeister), krause@pi3.informatik.uni-mannheim.de (M. Krause), simon@ls2.informatik.uni-dortmund.de (H.U. Simon).

0304-3975/00/$ - see front matter
PII: S0304-3975(99)00243-1

the Hamming weight of v, i.e., the number of ones in v. Throughout the paper, the notion "matrix" always refers to a matrix with entries from $\{0,1\}$. Let us begin with an informal description of how visual cryptography works. Given are two collections $\mathscr{C}_0$ and $\mathscr{C}_1$ of $n \times m$-matrices. The sender translates every pixel of the secret image into n sets of subpixels, in the following way: If the sender wishes to transmit a white pixel, then she chooses one of the matrices from $\mathscr{C}_0$ according to the uniform distribution. In the case of a black pixel, one of the matrices from $\mathscr{C}_1$ is chosen. For all $1 \leqslant i \leqslant n$, recipient i obtains the ith row of the chosen matrix as an array of subpixels, where a 1 in the row corresponds to a black subpixel and a 0 corresponds to a white subpixel. The subpixels are arranged in a fixed pattern, e.g. a rectangle. Note that in this model, stacking transparencies corresponds to "computing" the OR of the subpixel arrays.

In designing a visual cryptographic scheme, we have to achieve "security" and "contrast". Both aspects are covered in the following definition, in which the third property is often referred to as the "security property". This property guarantees that any set of $q < k$ recipients cannot distinguish whether a subpixel pattern that they see on their transparencies was created from a transmitted black pixel or from a transmitted white pixel. In this sense, they are not able to obtain any information about the original picture. (Except for the size of the picture, of course.)

The "contrast property" is represented by Conditions (1) and (2). Condition (2) guarantees that the k recipients see at least d black subpixels in a subpixel array representing a black pixel. Condition (1) guarantees that in the case of a white pixel, at most $d - \alpha \cdot m$ subpixels are black. Together, k recipients can recognize a transmitted black pixel visually since the corresponding subpixel array appears to be "more black". The larger α is, the easier it is to recognize the black pixels.

Definition 1. A (k,n)-scheme $\mathscr{C} = (\mathscr{C}_0, \mathscr{C}_1)$ *with* m *subpixels*, *contrast* $\alpha > 0$ *and threshold* d consists of two collections of $n \times m$-matrices $\mathscr{C}_0 = [C_{0,1}, \ldots, C_{0,r}]$ and $\mathscr{C}_1 = [C_{1,1}, \ldots, C_{1,s}]$, such that the following properties are valid:

1. For any matrix $S \in \mathscr{C}_0$, the OR v of any k out of the n rows of S satisfies $H(v) \leqslant d - \alpha \cdot m$.
2. For any matrix $S \in \mathscr{C}_1$, the OR v of any k out of the n rows of S satisfies $H(v) \geqslant d$.
3. For any $q < k$ and any q-element subset $\{i_1, \ldots, i_q\} \subseteq \{1, \ldots, n\}$, the two collections of $q \times m$ matrices $\mathscr{D}_0$ and $\mathscr{D}_1$ obtained by restricting each $n \times m$-matrix in $\mathscr{C}_0$ and $\mathscr{C}_1$ to rows $i_1, \ldots, i_q$ are indistinguishable in the sense that they contain the same matrices with the same relative frequencies.

The parameter d/m will also be called "relative threshold" in the sequel. Two remarks are in place: First, given a scheme, the above definition does not uniquely define the contrast α and the threshold d of a scheme. One can do so by choosing d as the largest possible value such that condition (2) is true and then choosing the largest α which keeps condition (1) fulfilled. Second, note that by duplicating matrices appropriately often, we can always assume that $\mathscr{C}_0$ and $\mathscr{C}_1$ contain the same number of matrices.

The notion of a scheme can also be generalized in such a way that certain subsets of recipients can work successfully together, whereas other subsets will gain no information. If the two classes of subsets are the sets of at most $k-1$ recipients and the sets of at least k recipients, respectively, we obtain the schemes considered in this paper. Generalized schemes are investigated in [1]. Another model for (2,2)-schemes involving more than two colors is presented in [7]. Visual cryptography provides a simple method of transmitting perfectly secret information. In particular, the decoding process requires no special computing devices, only the human eye. A (k,n)-scheme can, for example, be used for splitting some password into n parts and delivering the parts to n people. Any action requiring the password can only take place whenever at least k of the n people approve. The approval can be verified without a computer.

A good contrast is vital for decoding the messages. As shown in [6], the optimal contrast for a (k,n)-scheme cannot exceed $2^{-(k-1)}$. But even for small values of k and arbitrary n, the contrasts achieved by the schemes in [6] are so small that they can hardly be visualized. A first step into the direction of analyzing the best-possible contrast was taken in [2], where a method of computing an upper bound was described. The main contribution of our paper is that for *general* k and n, we are not only able to compute upper bounds, but to compute the *exact* value of the maximum possible contrast. Surprisingly, there is a uniform procedure which constructs such a contrast-optimal scheme for arbitrary values of k and n (see Section 4). This procedure solves a (carefully designed) linear program, denoted by $L(k,n)$, whose solutions implicitly represent a contrast-optimal scheme. Moreover, the optimal value $L_{\mathrm{opt}}(k,n)$ of the target function of $L(k,n)$ coincides with the maximal possible contrast. For specific values of k, the optimal solution to $L(k,n)$ and $L_{opt}(k,n)$ can be analytically described (see Section 5). As a nice byproduct, we obtain a much simpler proof of the optimality of Naor's and Shamir's (k,k)-scheme.

We stress however that for a practical application of the schemes, a good contrast α is not the only criterion, but one also has to take care of the values m and d, i.e., one might prefer to have

(a) smaller values of m corresponding to smaller pixel expansion, and
(b) a smaller relative threshold d/m, corresponding to less "background noise" in the picture.

Point (b) stems from the subjective empirical observation that even at the same contrast α, the human eye might perceive the picture easier to decode if the whole picture is lighter. Analyzing the interplay of those three parameters, e.g. questions like "what is the optimal contrast achievable if d and m are fixed at certain values?" is a difficult problem.

Our results yield the optimal contrast achievable if there is no condition on the size of d and m. This also means that the schemes resulting from $L(k,n)$ are far from being optimal with respect to the number of subpixels. We address this problem for $k=2$ in Section 3 where we give a more elegant construction of contrast-optimal $(2,n)$-schemes which takes also care of the number of subpixels. This construction makes use of Hadamard matrices.

Some of the results on $(2,n)$-schemes in Section 3 have already been obtained by a different approach in [1]. (See e.g. Theorem 23 in [1] which states that the maximum possible contrast for a $(2,n)$-scheme is $(\lfloor n/2\rfloor\lceil n/2\rceil)/n(n-1)$.)

Nevertheless, our approach also allows to obtain the result that for any contrast below $\frac{1}{4}$, much less subpixels are needed than for contrast at least $\frac{1}{4}$.

2. Basic notions and definitions

For $v,w\in\{0,1\}^m$ let $d(v,w)=\#\{i\colon v_i\neq w_i\}$ denote the Hamming distance between v and w. The *minimum Hamming distance* $d(S)$ and the contrast $\alpha(S)$ of a matrix S are given by $d(S):=\min_{v\neq w\in row(S)} d(v,w)$ and

$$\alpha(S):=\frac{1}{m}\left(\min_{v\neq w\in row(S)} H(v\,OR\,w)-\max_{v\in row(S)} H(v)\right).$$

A $\{0,1\}$-matrix is called *balanced* if each row contains the same number of ones. For two $\{0,1\}$-matrices A and B (with appropriate dimensions), we denote by $[A|B]$ the matrix obtained by "horizontally concatenating" A and B and by $\left[\begin{smallmatrix}A\\B\end{smallmatrix}\right]$ the "vertical concatenation". $\bar{A}$ denotes the matrix obtained from A by negating the entries of A. For a subset I of the rows, we denote by $A|_I$ the matrix which contains only those rows i of A which are in I. Also recall the notion of Hadamard matrices H_n which are recursively defined by

$$H_1=[1]\quad\text{and}\quad H_{2\cdot n}=\begin{bmatrix}H_n & H_n\\ H_n & \bar{H}_n\end{bmatrix}.$$

3. Optimal $(2,n)$-schemes

3.1. Contrast is related to Hamming distance

In this subsection, we reduce the problem of finding a $(2,n)$-scheme with maximal contrast to the problem of finding a balanced matrix with maximal minimum Hamming distance (see Lemma 3).

Lemma 2. *Each $n\times m$-matrix S satisfies the inequality $\alpha(S)\leqslant d(S)/2m$. If S is balanced, then equality holds.*

Proof. Choose v,w such that $d(S)=d(v,w)$ and $H(v)\leqslant H(w)$. By definition, $\alpha(S)\leqslant (H(v\,OR\,w)-H(w))/m$. $f(v,w):=H(v\,OR\,w)-H(w)$ counts the number of positions where $v_i=1$ and $w_i=0$. Since $H(v)\leqslant H(w)$, the number of positions where $w_i=1$ and $v_i=0$ is also at least that number. Hence, $d(S)=d(v,w)\geqslant 2f(v,w)\geqslant 2\cdot m\cdot\alpha(S)$. If S is balanced, i.e., every row has Hamming weight t, then for all v,w, $H(v\,OR\,w)=t+d(v,w)/2$, hence $\alpha(S)=d(v,w)/2m$. □

Lemma 3. (a) *Let $\mathscr{C}=(\mathscr{C}_0,\mathscr{C}_1)$ be a $(2,n)$-scheme with m subpixels and contrast α. Then $\alpha\leqslant \min_{S\in\mathscr{C}_1} d(S)/2m$.*

(b) *Given a balanced $n\times m$-matrix S, one can define a $(2,n)$-scheme $\mathscr{C}(S)$ with contrast $d(S)/2m$ and m subpixels.*

Proof. (a) $\alpha\leqslant(1/m)(\min_{\substack{S\in\mathscr{C}_1,\\ v\neq w\in row(S)}} H(v\ OR\ w)-\max_{\substack{S\in\mathscr{C}_0,\\ v\neq w\in row(S)}} H(v\ OR\ w))$ (by definition) which is $\leqslant(1/m)(\min_{\substack{S\in\mathscr{C}_1,\\ v\neq w\in row(S)}} H(v\ OR\ w)-\max_{\substack{S\in\mathscr{C}_0,\\ v\in row(S)}} H(v))$. By the security property, $\max_{\substack{S\in\mathscr{C}_0,\\ v\in row(S)}} H(v)=\max_{\substack{S\in\mathscr{C}_1,\\ v\in row(S)}} H(v)$. Consequently, $\alpha\leqslant\min_{S\in\mathscr{C}_1}\alpha(S)\leqslant\min_{S\in\mathscr{C}_1}(d(S)/2m)$ (by Lemma 2).

(b) Choose $\mathscr{C}_0(S)$ to consist of matrices $A_1,\ldots,A_n$, where A_i is obtained from S by taking n copies of the ith row in S. Choose $\mathscr{C}_1(S)$ to consist of the matrices $S,\pi(S),\pi^2(S),\ldots,\pi^{n-1}(S)$, where, for each $n\times m$-matrix A, $\pi(A)$ is obtained by permuting the rows of A according to the cyclic shift permutation $\pi=(12\ldots n)$. Clearly, the security property is fulfilled. The contrast property is also fulfilled since the OR of any two rows out of a matrix in $\mathscr{C}_0$ corresponds to a row from S, whereas the OR of two matrices in $\mathscr{C}_1$ corresponds to an OR of two rows in S. Thus, the contrast of the scheme is equal to the contrast $\alpha(S)$ which, by Lemma 2, is equal to $d(S)/(2m)$. □

We call a scheme $\mathscr{C}$ *balanced* if $\mathscr{C}=\mathscr{C}(S)$ for some balanced matrix S.

3.2. Contrast-optimal $(2,n)$-schemes and a subpixel tradeoff

Due to the connection between the Hamming distance of a matrix and $(2,n)$-schemes, we are able to apply results from coding theory, for example the so-called "Plotkin bound", see e.g. [5].

Lemma 4 (Plotkin's bound). *Let S be an $n\times m$-matrix with entries from $\{0,1\}$. If $d(S)>m/2$, then $n\leqslant 2d(S)/2d(S)-m$. The following are corollaries*:

(i) $d(S)\leqslant(n/2(n-1))m$.
(ii) *If* $d(S)\geqslant m/2$, *then* $n\leqslant 2m$.
(iii) *If* $d(S)\geqslant m/2$ *and* S *is balanced, then* $n\leqslant 2m-1$.

Proof. The first statement follows directly. The second statement can be proved by considering the submatrix S_1 (S_0, resp.) of S which consists of those rows which have a 1 (0, resp.) in the first column. Deleting the first column of S_0 and S_1 and then applying Plotkin's bound, we obtain $n\leqslant 4d(S)/(2d(S)-m+1)$. For $d(S)\geqslant m/2$, this gives $n\leqslant 2m$.

For the third statement, assume w.l.o.g. that every row in S has Hamming weight exactly $t\leqslant m/2$. We can add a constant 1-row to S and obtain a matrix S' which still has minimum Hamming distance $m/2$. We apply part (ii) to S'. □

Theorem 5. (a) *The contrast of a $(2,n)$-scheme is at most $n/4(n-1)$.*

(b) *For all* $n=2^k$, $k\geqslant 1$, *there is a* $(2,n)$*-scheme with contrast* $n/4(n-1)$ *and* $m=2n-2$ *subpixels.*

Proof. (a) is proved by Lemma 3, part (a), and Lemma 4, part (i). For the proof of (b), we note that the Hadamard matrix H_n has a constant 1 column as well as a constant 1 row, all other rows have Hamming weight $n/2$. Furthermore, $d(H_n)=n/2$. Define the $n\times 2(n-1)$-matrix S_n by $S_n=[B_n\,|\,\bar{B}_n]$, where B_n is obtained from H_n by deleting the constant 1 column. S_n is balanced, and $d(S_n)=n$. By Lemma 3, part (b), this matrix leads to the desired scheme. □

3.2.1. Schemes with contrast $\frac{1}{4}$ *and the minimal number of subpixels*

Here, we derive bounds on the number m of subpixels needed to construct a $(2,n)$-scheme with contrast at least $\frac{1}{4}$. Remember that if the contrast α of a scheme $\mathscr{C}$ is at least $\frac{1}{4}$, then the minimum Hamming distance of the matrices in $\mathscr{C}_1$ is at least $m/2$.

Theorem 6. (a) *A* $(2,n)$*-scheme* $\mathscr{C}$ *with contrast* $\alpha\geqslant\frac{1}{4}$ *uses at least* $\lceil n/2\rceil$ *subpixels. Moreover, if* $\mathscr{C}$ *is balanced, it uses at least* $\lceil (n+1)/2\rceil$ *subpixels.*

(b) *If* $n=2^k-2$ *for some* $k\geqslant 2$, *then there exists a balanced* $(2,n)$*-scheme* $\mathscr{C}$ *with contrast* $\frac{1}{4}$ *and* $\lceil (n+1)/2\rceil$ *subpixels.*

Proof. (a) By Lemma 4, part (ii), $m\geqslant n/2$. If $\mathscr{C}=\mathscr{C}(S)$ is balanced, we apply part (iii) to the balanced matrix S.

(b) For m a power of 2, let C_m be the $(m-1)\times m$-matrix obtained from the Hadamard matrix H_m by deleting the constant-1 row.

$$S_n := \left[\frac{C_n}{C_n}\right]$$

is a balanced $(2m-2)\times m$-matrix, and it is easy to see that it has minimum Hamming distance $m/2$. The scheme $\mathscr{C}=\mathscr{C}(S_n)$ has the desired properties. □

3.2.2. The subpixel number of schemes with contrast smaller than 1/4

For every $\alpha<\frac{1}{4}$, one can construct $(2,n)$-schemes with contrast at least α and much less than $n/2$ subpixels:

Theorem 7. *For any fixed* $\alpha<\frac{1}{4}$, *there is a balanced* $(2,n)$*-scheme with* $m=$ $\mathrm{O}(\log n)$ *subpixels and contrast at least* α.

Proof. In the theory of linear codes, the Gilbert–Varshamov bound (see e.g. [3, Theorem 8.27]), gives a sufficient condition for the existence of "linear (m,k)-codes". For our purposes, it is enough to know that a linear (m,k)-code S over the field $\mathbb{F}_q$ is a linear subspace of $\mathbb{F}_q^m$. It is of dimension k, hence $|S|=q^k$, and fulfills some additional properties. The minimum distance of such a code S is defined as $\min_{v\neq w\in S}|\{i\,|\,v_i\neq w_i\}|$ and coincides with the Hamming distance which we have defined earlier (for the case $q=2$).

Gilbert–Varshamov bound: There exists a linear (m,k)-code over $\mathbb{F}_q$ with minimum distance at least d whenever

$$q^{m-k} > \sum_{i=0}^{d-2} \binom{m-1}{i} (q-1)^i. \tag{1}$$

Assume now that we have chosen $q=2$ and the parameters k,d and m such that the Gilbert–Varshamov bound guarantees the existence of a linear (m,k)-code. It follows that there is a subset of $\{0,1\}^m$ of cardinality 2^k with minimum Hamming distance d. These 2^k vectors can be arranged as the rows of a matrix showing that there is a $(2^k \times m)$-matrix F with minimum Hamming distance $d(F) \geqslant d$. Let us now choose the parameters k,d and m appropriately. The right-hand side of (1) is

$$\sum_{i=0}^{d-2} \binom{m-1}{i} \leqslant \sum_{i=0}^{d-2} \binom{m}{i} \leqslant 2^m \sum_{i=0}^{d-2} \binom{m}{i} (1/2)^i (1/2)^{m-i}.$$

We can interpret the last expression as 2^m times the probability that an unbiased coin comes up HEAD at most $d-2$ times in m independent trials, hence by Chernov's bound we can upper bound it by $2^m e^{-(m/4)(1-2(d-1)/m)^2}$. If we let $d := \lceil 2m\alpha \rceil$, i.e., $d-1 \leqslant 2m\alpha$, then this bound is at most $2^m e^{-(m/4)\cdot(1-4\alpha)^2}$. Thus, the Gilbert–Varshamov bound is applicable if $2^{-k} > e^{-(m/4)\cdot(1-4\alpha)^2}$ which is fulfilled for

$$m > 4k \ln 2/(1-4\alpha)^2.$$

If we let $k = \lceil \log n \rceil$ and choose m as above, then we obtain an $n \times m$-matrix F with $d(F) \geqslant d$. Let $B = [F \mid \bar{F}]$. B is balanced and $d(B) = 2d(F) \geqslant 2d$. By Lemma 2, $\alpha(B) = d(B)/4m \geqslant d/2m \geqslant \alpha$. This yields the desired balanced $(2,n)$-scheme $\mathscr{C}(B)$. □

Note that subpixel number $\Omega(\log n)$ is necessary since in every $\mathscr{C}_1$-matrix of a scheme, no two rows can be the same.

4. Contrast-optimal (k,n)-schemes for general k

4.1. Considering "totally symmetric" schemes is sufficient

Given a (k,n)-scheme $\mathscr{C}$, consisting of collections $\mathscr{C}_0$ and $\mathscr{C}_1$ of $n \times m$-matrices, we will say that $\mathscr{C}$ is *generated by $n \times m$-matrices* G_0 and G_1 if for $j \in \{0,1\}$: $\mathscr{C}_j = [\pi(G_j) \mid \pi$ is a permutation of the columns$]$.

Observe that collections $\mathscr{C}_0$ and $\mathscr{C}_1$ generated by G_0 and G_1 form a (k,n)-scheme if and only if G_0 and G_1 fulfill the following conditions:

(I) The weight obtained by OR-ing k rows of G_1 is at least d, while the weight obtained by OR-ing k rows of G_0 is at most $d - \alpha \cdot m$.

(II) For each set I of $k-1$ row indices, each $v \in \{0,1\}^{k-1}$ occurs with the same frequency as column in $G_0|_I$ and in $G_1|_I$.

The key to our results will be the observation that optimal contrast values can always be achieved by schemes of a very special form.

Definition 8. An $n \times m$-matrix A is *totally symmetric* if all $v, w \in \{0,1\}^n$ of equal weight, say j, occur with the same frequency $f_j(A)$ as columns of A.

Thus, up to column permutations, a totally symmetric matrix A is completely characterized by the values $f_0(A), \ldots, f_n(A)$. Obviously, the following relation holds:

$$\sum_{j=0}^{n} \binom{n}{j} f_j(A) = m. \tag{2}$$

We also note the following simple property:

Proposition 9. *Let A be a totally symmetric $n \times m$-matrix, and let I and I' be subsets of $\{1, \ldots, n\}$ with $|I| = |I'|$. Then the following holds: The matrices $A|_I$ and $A|_{I'}$ are also totally symmetric and the parameters of $A|_I$ and $A|_{I'}$ are the same, i.e., $f_i(A|_I) = f_i(A|_{I'})$ for $i \in \{0, \ldots, |I|\}$.*

Proof. Consider a pattern $v \in \{0,1\}^{|I|}$ which contains i ones. If we consider all possibilities of adding patterns v' from $\{0,1\}^{n-|I|}$ with t ones to obtain a vector from $\{0,1\}^n$, we find that v occurs exactly $\sum_{t=0}^{n-|I|} \binom{n-|I|}{t} \cdot f_{t+i}(A)$ times in $A|_I$. The dependence of this number on v is only via i, the number of ones in v, hence $A|_I$ is totally symmetric. Its dependence on I is only via the cardinality $|I|$, hence, the parameters are the same for I' since $|I'| = |I|$. □

We assign to an arbitrary $n \times m$-matrix A a totally symmetric $n \times (n! \cdot m)$-matrix $symm(A) := [\sigma_1(A) \mid \sigma_2(A) \mid \cdots \mid \sigma_{n!}(A)]$, where for a permutation $\sigma \in \Sigma_n$ we denote by $\sigma(A)$ the matrix obtained from A by permuting its rows according to σ and where σ_i runs through all permutations.

We call a (k,n)-scheme $\mathscr{C} = (\mathscr{C}_0, \mathscr{C}_1)$ *totally symmetric* if it is generated by totally symmetric matrices G_0 and G_1.

Theorem 10. *For each (k,n)-scheme $\mathscr{C} = (\mathscr{C}_0, \mathscr{C}_1)$ with contrast $\alpha > 0$ there is a totally symmetric (k,n)-scheme which has contrast at least α.*

Proof. Let m denote the number of subpixels of $\mathscr{C}$. As indicated earlier, we can w.l.o.g. assume that $\mathscr{C}_0$ consists of the same number r of matrices as $\mathscr{C}_1$. Denote by H_0 and H_1 the $n \times (rm)$-matrices obtained by "horizontally concatenating" all matrices in $\mathscr{C}_0$ and $\mathscr{C}_1$, respectively. Now consider the scheme generated by the matrices $symm(H_0)$ and $symm(H_1)$. It is easy to check that we obtain a totally symmetric (k,n)-scheme of contrast not smaller than α and threshold $d' = dn!r$. Each matrix in the scheme has $m' = mrn!$ many columns. □

Note that the "relative threshold value" is not changed by this construction, i.e., we have $d'/m' = d/m$.

4.2. A linear program for computing schemes of maximal contrast

We have seen in the previous subsection that for analyzing the best-possible contrast in (k,n)-schemes, we may restrict ourselves to schemes which are generated by totally symmetric matrices G_0 and G_1.

First, we transform the security and the contrast property into conditions on the parameters of G_0 and G_1.

Definition 11. Let A be a totally symmetric $n \times m$-matrix. For $t=1,\dots,n$ and $l=0,\dots,t$, define $c_l^t(A)=f_l(A|_I)$, where I is an arbitrarily fixed subset of $\{1,\dots,n\}$ of cardinality t.

Note that the parameters $c_l^t(A)$ are well defined since for two different subsets I and I' of $\{1,\dots,n\}$ with $|I|=|I'|=t$, the matrices $A|_I$ and $A|_{I'}$ are totally symmetric and are characterized by the same parameters f_l. (See Proposition 9.) The parameter $c_l^t(A)$ counts how often each vector with l ones occurs as column in an arbitrary submatrix of A which has t rows. Observe that

$$c_l^t(A)=\sum_{j=l}^{n-t+l} f_j(A)\binom{n-t}{j-l}. \tag{3}$$

Let us illustrate the definitions by a small example: Let

$$A=\begin{bmatrix} 0 & 0 & 1 & 1 & 1 & 0\\ 0 & 0 & 1 & 1 & 0 & 1\\ 0 & 0 & 1 & 0 & 1 & 1\\ 0 & 0 & 0 & 1 & 1 & 1 \end{bmatrix}.$$

Then we have $f_0(A)=2$, $f_1(A)=f_2(A)=f_4(A)=0$, $f_3(A)=1$ and $c_0^1(A)=3$, $c_1^1(A)=3$, $c_0^2(A)=2$, $c_1^2(A)=1$, $c_2^2(A)=2$, etc.

Theorem 12. *Given two totally symmetric $n \times m$-matrices G_0 and G_1 with $\beta := (c_0^k(G_0)-c_0^k(G_1))/m>0$.*

G_0 and G_1 generate a (k,n)-scheme of contrast β if and only if:

$$\forall_{l=0,\dots,k-1}:\ c_l^{k-1}(G_0)=c_l^{k-1}(G_1). \tag{4}$$

Proof. Condition (4) is obviously equivalent to the security condition (II). In order to investigate the contrast, consider the OR of k rows of G_0. The resulting vector contains $c_0^k(G_0)$ zeroes, i.e., $m-c_0^k(G_0)$ ones. Similarly, the OR of k rows of G_1 contains $m-c_0^k(G_1)$ ones. Thus, the contrast is $(c_0^k(G_0)-c_0^k(G_1))/m$. The threshold of the scheme is $m-c_0^k(G_1)$. □

Observe that the relation for $l=0$ in (4) can be omitted as the weighted sum (see (2)) of the c_l^k is the same for G_0 and G_1.

For all natural numbers $2\leqslant k\leqslant n$, let us define the following linear program $L(k,n)$ over the variables $(x_0,\dots,x_n,y_0,\dots,y_n)\in\mathbb{Q}^{2n+2}$. The target function corresponds to the

contrast of the schemes and the conditions express the security property. The variables x_j and y_j correspond to the values $f_j(G_0)\binom{n}{j}/m$ and $f_j(G_1)\binom{n}{j}/m$, respectively.

The linear program $L(k,n)$

max	$\sum_{j=0}^{n-k} \frac{\binom{n-k}{j}}{\binom{n}{j}}(x_j - y_j)$	
(1)	$x_j, y_j \geqslant 0$	$\forall j = 0,\ldots,n$
(2)	$\sum_{j=0}^{n} x_j = \sum_{j=0}^{n} y_j = 1$	
(3)	$\sum_{j=l}^{n-k+l+1} \frac{\binom{n-k+1}{j-l}}{\binom{n}{j}}(x_j - y_j) = 0$	$\forall l = 0,\ldots,k-1$

We denote by L_{target} the target function of $L(k,n)$, and by L_{opt} the optimal value of the target function. It is not hard to show that $L_{\text{opt}} > 0$.

We show now that solving this linear program provides us with a scheme of optimal contrast. For a totally symmetric (k,n)-scheme (generated by H_0 and H_1), let us denote by a_j the fraction of columns in H_0 with weight exactly j. Similarly, define b_j for H_1, i.e.,

$$a_j = \frac{f_j(H_0)\cdot\binom{n}{j}}{m} \quad \text{as well as } b_j = \frac{f_j(H_1)\cdot\binom{n}{j}}{m} \quad \text{for } j = 0,\ldots,n.$$

Lemma 13. (a) *The parameters a_j and b_j of a totally symmetric (k,n)-scheme $\mathscr{C}$ satisfy $L(k,n)$ if we let $x_j = a_j$ and $y_j = b_j$. The value of the target function is then equal to the contrast of $\mathscr{C}$.*

(b) *Given a feasible solution $\underline{a},\underline{b}$ of $L(k,n)$, where the target function is larger than* 0, *there is a (k,n)-scheme $\mathscr{C}$ with contrast equal to the target function.*

Proof. (a) Conditions (1) and (2) are trivially fulfilled. For proving Condition (3), we observe that by (4), the security property for $\mathscr{C}$ implies that $c_l^{k-1}(H_0) = c_l^{k-1}(H_1)$ for $l = 0,\ldots,k-1$. Using relation (3), we obtain that for all $l = 0,\ldots,k-1$, it holds that

$$\sum_{j=l}^{n-k+l+1} \binom{n-k+1}{j-l} \frac{a_j - b_j}{\binom{n}{j}} \cdot m = 0$$

which we can divide by m to obtain equality (3) of the linear program. Also by (4), it follows that the contrast of $\mathscr{C}$ is exactly

$$(c_0^k(H_0) - c_0^k(H_1))/m = \sum_{j=0}^{n-k} \binom{n-k}{j} (a_j - b_j)/\binom{n}{j} = L_{\text{target}}(\underline{a},\underline{b}).$$

(b) Since the a_j and b_j are rational numbers, we can bring them into the form $a_j = \binom{n}{j} A_j/m$ and $b_j = \binom{n}{j} B_j/m$, respectively, where $m, A_0,\ldots,A_n, B_0,\ldots,B_n$ are natural numbers. We then construct totally symmetric $n \times m$-matrices G_0 and G_1 which contain

each column vector of Hamming weight j exactly A_j and B_j times, respectively. The scheme generated by G_0 and G_1 has the desired properties. □

Since we have shown in Section 4.1 that for computing the maximal possible contrast, it suffices to investigate totally symmetric schemes, Lemma 13 implies:

Theorem 14. *Let $2 \leqslant k \leqslant n$. For all (k,n)-schemes the contrast is at most $L_{\mathrm{opt}}(k,n)$. Furthermore, there is a (k,n)-scheme with contrast $L_{\mathrm{opt}}(k,n)$, and a description of this optimal scheme can be computed in time polynomial in n.*

Finally, we note a property of an optimal solution $(\underline{a},\underline{b})$ of the linear program. Namely, we can always guarantee the following behavior: For all j, we have that $a_j = 0$ or $b_j = 0$. The reason is the following: Condition (3) as well as the target function only depend on $x_j - y_j$. For the sake of contradiction assume an optimal solution where $a_j, b_j > 0$. Assume w.l.o.g. $a_j \geqslant b_j$. Note that $b_j < 1$ because, otherwise, $a_j = b_j = 1$, implying $L_{\mathrm{opt}}(k,n) = 0$ (a contradiction). We can replace a_j by $a_j - b_j$ and b_j by 0. The target function does not change, and Condition (3) still holds. In order to satisfy Condition (2) again, we multiply all a_i and b_i by $1/(1-b_j) > 1$ which strictly increases the value of the target function and yields a feasible solution. This is a contradiction to the optimality of $\underline{a},\underline{b}$.

Remark. As we have noted earlier, it might be desirable to have a scheme with small relative threshold value d/m. According to the remark after Theorem 10, the relative threshold value does not change if we turn a given scheme into a totally symmetric scheme, hence the linear program can also be used to compute the best contrast which can be achieved if we want an upper bound on the relative threshold. The relative threshold can be computed in the variables of the linear program as

$$\frac{m - c_0^k(G_1)}{m} = 1 - \sum_{j=0}^{n-k} x_j \frac{\binom{n-k}{j}}{\binom{n}{j}}.$$

Thus, by adding to the linear program the constraint

$$1 - \sum_{j=0}^{n-k} x_j \frac{\binom{n-k}{j}}{\binom{n}{j}} \leqslant C$$

for a desired upper bound C, we can compute the best achievable contrast if the relative threshold is at most C. (If there is such a scheme at all.)

5. The linear program for concrete values of k and n

In this section, we show how the previously described linear program can be used to obtain much simpler proofs of already known results on the optimal contrast as well as new results on previously untackled parameters.

5.1. The case $n = k$

In [6] it is shown that for all $k \geqslant 2$ the maximal contrast achievable by a (k,k)-scheme is $2^{-(k-1)}$. A contrast-optimal (k,k)-scheme with the minimal number of subpixels can be obtained as follows:

(I) Take the scheme which is generated by the $k \times 2^{(k-1)}$-matrices G_0 and G_1, where the columns of G_0 and G_1 consist of all k-vectors of even and odd Hamming weight, respectively.

The proof of contrast-optimality in [6] uses an intricate result of [4] known as the principle of approximate inclusion–exclusion. Our approach gives a very straightforward proof for the contrast-optimality of scheme (I).

For $n = k$ the linear program $L(n,k)$ reads as follows. We have to maximize $x_0 - y_0$ for all $\underline{x} \geqslant 0$ and $\underline{y} \geqslant 0$ from $\mathbb{Q}^{k+1}$ fulfilling $\sum_{j=0}^{n} x_j = \sum_{j=0}^{n} y_j = 1$, and for all

$$l = 0, \ldots, k-1 : \frac{x_l - y_l}{\binom{k}{l}} + \frac{x_{l+1} - y_{l+1}}{\binom{k}{l+1}} = 0.$$

Since $L_{\mathrm{opt}}(k,n) > 0$, it follows that $x_0 > y_0$, and since one of them needs to be 0, it follows that $y_0 = 0$. For $l = 0$, we obtain $(x_1 - y_1)/\binom{k}{1} = -x_0/\binom{k}{0}$, hence $x_1 = 0$ and $y_1 = (\binom{k}{1}/\binom{k}{0})/x_0$. Proceeding in this fashion, and exploiting that $\sum_i x_i = \sum_i y_i = 1$, we obtain that in the optimal solution

$$x_i = \begin{cases} 0 & \text{if } i \text{ is odd,} \\ 2^{-(k-1)} \binom{k}{i} & \text{otherwise.} \end{cases}$$

The same holds for y with "odd" replaced by "even". This yields exactly scheme (I).

5.2. $(2,n)$-schemes revisited

The optimal contrast achievable by $(2,n)$-schemes is

$$L_{\mathrm{opt}} = \frac{\lceil n/2 \rceil \lfloor n/2 \rfloor}{n(n-1)}.$$

This can be proved by analyzing the linear program, as we shall see now. The target function for $k = 2$ is

$$\sum_{j=0}^{n-2} \frac{(n-j)(n-j-1)}{n(n-1)}(x_j - y_j) = \sum_{j=0}^{n} \frac{(n-j)(n-j-1)}{n(n-1)}(x_j - y_j).$$

Condition (3) in the linear program can be rewritten as

$$\sum_{j=0}^{n-1} (n-j)(x_j - y_j) = 0 \quad \text{and} \quad \sum_{j=1}^{n} j(x_j - y_j) = 0. \tag{5}$$

Eq. (5) imply that, for any linear function $h(j) = c_1 j + c_2$, the following holds:

$$\sum_{j=0}^{n} (h(j)(x_j - y_j)) = \sum_{j=0}^{n} (c_1 j(x_j - y_j)) + \sum_{j=0}^{n} (c_2(x_j - y_j)) = 0. \tag{6}$$

We first show the lower bound on the contrast by considering a particular solution of the linear program. If n is even, we choose

$$b_j = \begin{cases} 1 & \text{if } j = \frac{n}{2}, \\ 0 & \text{otherwise.} \end{cases}$$

If n is odd, we choose

$$b_j = \begin{cases} 1/2 & \text{if } j \in \{\frac{n-1}{2}, \frac{n+1}{2}\}, \\ 0 & \text{otherwise.} \end{cases}$$

In both cases, we let

$$a_j = \begin{cases} \frac{1}{2} & \text{if } j \in \{0, n\}, \\ 0 & \text{otherwise.} \end{cases}$$

It is straightforward to verify that the conditions of the linear program are fulfilled and that the value of the target function is $\lceil n/2 \rceil \lfloor n/2 \rfloor / n(n-1)$. In order to prove the upper bound on the contrast, observe that the target function can be written as

$$\frac{1}{n(n-1)} \sum_{j=0}^{n} (j^2 + g(j))(x_j - y_j),$$

where $g(j)$ is a linear function in j. Eq. (6) implies that we can replace $g(j)$ by any linear function in j. We choose as the new target function

$$\frac{1}{n(n-1)} \sum_{j=0}^{n} (j - \lfloor n/2 \rfloor)(j - \lceil n/2 \rceil)(x_j - y_j).$$

The term $(j - \lfloor n/2 \rfloor)(j - \lceil n/2 \rceil)$ for $j \in \{0, \ldots, n\}$ is never negative and never larger than $\lceil n/2 \rceil \lfloor n/2 \rfloor$, hence the value of the target function is bounded by $\lceil n/2 \rceil \lfloor n/2 \rfloor / n(n-1)$. This proves the upper bound on the contrast.

For n even, the totally symmetric matrix H_0 corresponding to the above chosen solution consists of $\binom{n}{n/2}/2$ constant-0 and constant-1 columns, respectively. H_1 consists of all $\binom{n}{n/2}$ columns of Hamming weight $n/2$. H_0 and H_1 generate a contrast-optimal $(2, n)$-scheme with $\binom{n}{n/2}$ subpixels. (This is inferior to our Hadamard constructions in Section 3.2, which were also contrast-optimal, but used $2n - 2$ subpixels only.)

5.3. $(3, n)$-schemes, where n is divisible by 4

For n divisible by 4, we can choose $a_0 = b_n = 1/3$ and $a_{3n/4} = b_{n/4} = 2/3$, and $a_j = b_j = 0$ otherwise. For this choice, the value of the target function becomes

$$L_{\text{target}}(\underline{a}, \underline{b}) = \frac{1}{3} + \frac{2}{3}\left(\binom{n-3}{3n/4} - \binom{n-3}{n/4}\right) = \frac{n^2}{16(n-1)(n-2)}.$$

We only remark that with methods similar to the one which we have applied in the case $k = 2$, one can also prove the optimality of the corresponding scheme. (Nevertheless, we omit these tedious computations.)

Thus, for arbitrary n divisible by 4, a contrast-optimal $(3,n)$-scheme is generated by G_0 and G_1 where G_0 contains each column of Hamming weight $3n/4$ exactly once, and $\binom{n}{n/4}/2$ constant-0 columns; G_1 contains each column of Hamming weight $n/4$ exactly once, and $\binom{n}{n/4}/2$ constant-1 columns. (Observe that $\binom{n}{n/4}$ is always even.) E.g., we obtain a contrast-optimal $(3,4)$-scheme with contrast $1/6$ and $m=6$ subpixels if we generate it by G_0 and G_1, where

$$G_0=\begin{bmatrix}0&0&1&1&1&0\\0&0&1&1&0&1\\0&0&1&0&1&1\\0&0&0&1&1&1\end{bmatrix} \quad \text{and} \quad G_1=\begin{bmatrix}1&1&1&0&0&0\\1&1&0&1&0&0\\1&1&0&0&1&0\\1&1&0&0&0&1\end{bmatrix}.$$

6. Conclusion

For general $2\leqslant k\leqslant n$, we have shown that the optimal achievable contrast in any (k,n)-scheme can be computed exactly by solving a linear program. We have demonstrated that for special values of k, an analytical solution of the linear program can be provided.

The variables belonging to the optimal solution of the linear program also provide us with a description of the corresponding scheme, unfortunately, the pixel expansion, i.e., the number m of subpixels needed in the schemes is extremely large.

For this reason, we have presented for the special case $k=2$ a more elegant approach. This approach allowed us to come up with $(2,n)$-schemes which have a linear (in n) pixel expansion and optimal contrast at least $\frac{1}{4}$. We have complemented this result by showing that every $(2,n)$-scheme with contrast at least $\frac{1}{4}$ actually needs a linear number of subpixels. We then have also been able to show that for any contrast smaller than $\frac{1}{4}$, there are $(2,n)$-schemes which only use a logarithmic (in n) number of subpixels. This number of subpixels is also optimal.

For general k, it remains open to construct contrast-optimal (k,n)-schemes which have also an efficient number of subpixels. Nevertheless, the optimal solution of our linear program provides a tool of analyzing the contrast quality of any (k,n)-scheme that one might come up with.

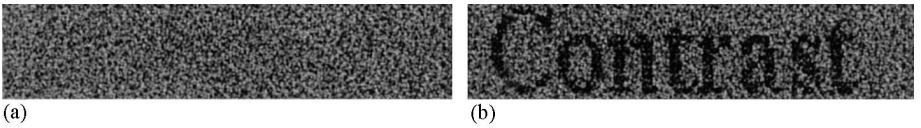
Besides reducing the pixel expansion, one might also consider it useful to have a small relative threshold. We have seen that by a slight modification of the linear program, it is still able to compute the optimal contrast under the restriction that the relative threshold is bounded by some value C.

7. Final remarks

For $(4,n)$-schemes, we are able to provide for every even n a solution to the linear program where the target function takes a value which converges to $\frac{1}{64}$ as $n\to\infty$. We omit these computations.

Table 1

$k\backslash n$	2	3	4	5	6	7	8	9	10	...	50	...	100
2	1/2	1/3	1/3	3/10	3/10	2/7	2/7	5/18	5/18		25/98		25/99
3		1/4	1/6	1/8	1/10	1/10	2/21	5/56	1/12		13/196		625/9702
4			1/8	1/15	1/18	3/70	3/80	2/63	1/35		1161/65800		425/25608



(a) (b)

Fig. 1.

It would be nice to have a general closed-form solution for $L_{\text{opt}}(k,n)$ and a corresponding optimal (k,n)-scheme for arbitrary $2 \leqslant k \leqslant n$.

We conjecture that, for all $k \geqslant 2$, $\lim_{n\to\infty} L_{\text{opt}}(k,n) = 4^{-(k-1)}$. Computer solutions to the linear program yield some evidence for this conjecture. It would also be interesting to prove that like in the case $k=2$, also for all $k>2$ and $\alpha < 4^{-(k-1)}$, there are (k,n)-schemes of contrast α which use only $O(\log n)$ subpixels.

Using a computer algebra system, we have computed for some values of k and n the optimal solution $L_{\text{opt}}(k,n)$. Some results are listed in the following Table 1.

Finally, let us give an example of a $(2,64)$-scheme, constructed according to Theorem 5, part (b), with contrast $\frac{64}{63\cdot 4}$ and 126 subpixels, arranged in a 9×14-pattern. Fig. 1(a) shows a typical picture of the kind that the 64 recipients obtain. Fig. 1(b) depicts the typical picture that emerges when any two recipients stack their transparencies.

References

[1] G. Ateniese, C. Blundo, A. De Santis, D.R. Stinson, Visual cryptography for general access structures, Proc. ICALP 96, Springer, Berlin, 1996, pp. 416–428.
[2] S. Droste, New results on visual cryptography, in: "Advances in Cryptology" — CRYPTO '96, Springer, Berlin, 1996, pp. 401–415.
[3] R. Lidl, H. Niederreiter, Introduction to Finite Fields and their Applications, Cambridge University Press, Cambridge, 1994.
[4] N. Linial, N. Nisan, Approximate inclusion–exclusion, Combinatorica 10 (1990) 349–365.
[5] J.H. van Lint, R.M. Wilson, A Course in Combinatorics, Cambridge University Press, Cambridge, 1996.
[6] M. Naor, A. Shamir, Visual Cryptography, in: "Advances in Cryptology — Eurocrypt 94", Springer, Berlin, 1995, pp. 1–12.
[7] M. Naor, A. Shamir, Visual cryptography II: improving the contrast via the cover base, in: Proc. of "Security Protocols: International Workshop 1996", Lecture Notes in Computer Science, vol. 1189, Springer, Berlin, 1997, pp. 69–74.