New Results on Visual Cryptography

Stefan Droste

Hasenweg 7, 58239 Schwerte, Germany
E-mail: droste@ls2.informatik.uni-dortmund.de

Abstract. Naor and Shamir ([1]) defined the basic problem of visual cryptography by a visual variant of the k out of n secret sharing problem: how can an original picture be encoded by n transparencies so that less than k of them give no information about the original, but by stacking k of them the original can be seen? They described a solution to this problem by a structure called k out of n secret sharing scheme whose parameters directly correspond to quality and usability of the solution. In this paper a new principle of construction for such schemes is presented which is easy to apply and in most cases gives much better results than the former principles. New bounds on relevant parameters of k out of n schemes are developed, too. Furthermore, an extension of the basic problem is introduced and solved in which every combination of the transparencies can contain independent information.

Keywords: Visual Cryptography, Secret Sharing Problem, Secret Sharing Scheme

1 Introduction

Many cryptographic methods encrypt information represented as numbers by using one-way functions. The values of the used one-way function represent the encrypted information and to decrypt this information the original numbers have to be computed. Without a secret key this computation should require an enourmous amount of time to guarantee the security of the method. But even when the secret key is known in most cases the computation of the original information is very tedious, if not impossible, without computers.

In visual cryptography which was introduced by Naor and Shamir (see [1]) we are looking for ways to encrypt pictures, i.e. information which can be perceived directly by the human visual system. For easier formalization we assume that the pictures are black-and-white and rastered so that they consist of a finite set of pixels which are either black or white. The encoded information should have the form of n rastered black-and-white pictures. To decode the information it is necessary to have k pictures, print them on transparencies and stack them. Then the original picture shall be recognizable. Therefore, encoded information can be decoded simply by stacking k transparencies, i.e. without any computations. But less than k pictures shall give no information about the original picture even to an infinitely powerful cryptanalyst. Naor and Shamir have described this problem by a structure called k out of n secret sharing scheme. Finding

Copyright (c) 1998, Springer-Verlag

such a scheme directly results in a solution for the k out of n secret sharing problem whose quality and usability correspond to different parameters of the scheme.

In this paper a new construction principle for secret sharing schemes is given whose resulting schemes are in most cases much better than the previously known schemes, directly resulting in better solutions for the secret sharing problem. New structural results about k out of n schemes lead to new bounds on the size and quality of schemes which are dependent on k and n (the best formerly known bounds were dependent on k only). At the end of this paper an extension of the original problem is introduced: how can n transparencies be created so that each combination of them results in a different picture? Solutions for this problem which still guarantee the security of the scheme conclude this paper. Although the value of visual cryptography may be small in practice, this paper shows new interesting possibilities to encrypt information in a very easy but completely secure way.

2 The Basic Model

The solution of the visual variant of the k out of n secret sharing problem relies on encrypting each pixel of the original picture separately by m subpixels in each transparency. When printed in close proximity these subpixels are not seen separately by the human visual system which rather averages the number of black subpixels. Therefore, a black pixel of the original has to be represented by more black subpixels in the stack of every k transparencies than a white original pixel. The difference of the number of black subpixels determines the contrast of the stack of the transparencies and shall be as high as possible. But the required security rules out the more obvious model in which every white original pixel is represented by m white subpixels, as in this case a black subpixel in one transparency enforces a black original pixel.

The m subpixels of the n transparencies can be represented as a $n \times m$ Boolean matrix $B = [B_{ij}]$, where $B_{ij} = 1$, if and only if the j-th subpixel of the i-th transparency is black. The greyness of the stack of k transparencies is determined by the Hamming weight of the OR of the corresponding k rows of B. To ensure security original black pixels have to be represented by the same combinations of m subpixels as white original pixels when considering less than k transparencies. For this gives you no chance of determining the colour of any original pixel and you cannot even determine a probability of an original pixel being black or white. When all matrices representing black original pixels are named as a multi-set C_1 and all the others are named as a multi-set C_0, the following definition is straight-forward (see also [1]):

Definition 1. Two multi-sets C_0 and C_1 of $n \times m$ Boolean matrices are called a k out of n secret sharing scheme, if there are constants $\alpha \geq 1/m$ and $d \in \{1, \ldots, m\}$ so that the three following conditions are met:

1. For any $B \in C_1$, the OR of any k of the n rows of B has a Hamming weight of at least d.

Copyright (c) 1998, Springer-Verlag

such a scheme directly results in a solution for the k out of n secret sharing problem whose quality and usability correspond to different parameters of the scheme.

In this paper a new construction principle for secret sharing schemes is given whose resulting schemes are in most cases much better than the previously known schemes, directly resulting in better solutions for the secret sharing problem. New structural results about k out of n schemes lead to new bounds on the size and quality of schemes which are dependent on k and n (the best formerly known bounds were dependent on k only). At the end of this paper an extension of the original problem is introduced: how can n transparencies be created so that each combination of them results in a different picture? Solutions for this problem which still guarantee the security of the scheme conclude this paper. Although the value of visual cryptography may be small in practice, this paper shows new interesting possibilities to encrypt information in a very easy but completely secure way.

2 The Basic Model

The solution of the visual variant of the k out of n secret sharing problem relies on encrypting each pixel of the original picture separately by m subpixels in each transparency. When printed in close proximity these subpixels are not seen separately by the human visual system which rather averages the number of black subpixels. Therefore, a black pixel of the original has to be represented by more black subpixels in the stack of every k transparencies than a white original pixel. The difference of the number of black subpixels determines the contrast of the stack of the transparencies and shall be as high as possible. But the required security rules out the more obvious model in which every white original pixel is represented by m white subpixels, as in this case a black subpixel in one transparency enforces a black original pixel.

The m subpixels of the n transparencies can be represented as a $n \times m$ Boolean matrix $B = [B_{ij}]$, where $B_{ij} = 1$, if and only if the j-th subpixel of the i-th transparency is black. The greyness of the stack of k transparencies is determined by the Hamming weight of the OR of the corresponding k rows of B. To ensure security original black pixels have to be represented by the same combinations of m subpixels as white original pixels when considering less than k transparencies. For this gives you no chance of determining the colour of any original pixel and you cannot even determine a probability of an original pixel being black or white. When all matrices representing black original pixels are named as a multi-set C_1 and all the others are named as a multi-set C_0, the following definition is straight-forward (see also [1]):

Definition 1. Two multi-sets C_0 and C_1 of $n \times m$ Boolean matrices are called a k out of n secret sharing scheme, if there are constants $\alpha \geq 1/m$ and $d \in \{1, \ldots, m\}$ so that the three following conditions are met:

1. For any $B \in C_1$, the OR of any k of the n rows of B has a Hamming weight of at least d.

Copyright (c) 1998, Springer-Verlag

2. For any $B \in C_0$, the OR of any k of the n rows of B has a Hamming weight of at most $d - \alpha \cdot m$.
3. For any subset $\{i_1, \ldots, i_q\} \subset \{1, \ldots, n\}$ with $q < k$, the two multi-sets obtained by restricting each matrix in C_0 resp. C_1 to the rows $i_1, \ldots, i_q$ contain the same matrices with the same frequencies.

To generate the n transparencies from the original for every pixel of the original one simply chooses independently and equally distributed a matrix of the multi-set C_0 resp. C_1, depending on the colour of the pixel. The first two conditions, called *contrast*, ensure that the original can be seen when any k transparencies are stacked. The third condition, called *security*, ensures that less than k transparencies give no information about the original, as the expected value of appearances of a restricted matrix is the same, no matter if the original pixel is black or white. The parameter α, the *relative contrast*, is probably the most important, as it determines how well k transparencies reveal the original. The parameter m determines the number of subpixels which should be as small as possible. Without loss of generality one can assume that C_0 and C_1 have the same number r of elements (see Lemma 8); as $\log(r)$ is the number of random bits for each original pixel needed to generate the transparencies, r should be as small as possible. The threshold d determines the minimal greyness of black pixels; its value is less relevant so that one can allow it to vary depending on the chosen k transparencies. As this relaxed condition has not led to better schemes, it will be omitted.

3 Basic Results

Naor and Shamir ([1]) have shown how to construct a k out of k secret sharing scheme whose parameter m is as small as possible and whose parameter α is as large as possible. For easy specification, we call a column of a Boolean matrix with an even number of 1's *even* and otherwise *odd*. If B is a Boolean matrix, we say that $P(B)$ is the multi-set of matrices obtained by permuting the columns of B, i.e. each permutation corresponds exactly to one element of $P(B)$.

Lemma 2. *Let B_0 resp. B_1 be $k \times 2^{k-1}$ Boolean matrices whose columns are exactly all even resp. odd columns of length k. Then $P(B_0)$ and $P(B_1)$ are a k out of k secret sharing scheme with parameters $m = d = 2^{k-1}$ and $\alpha = 1/2^{k-1}$.*

Proof. The contrast is fulfilled, as B_0 has exactly one column that contains only 0's but B_1 has none such column. Therefore, the Hamming weight of the OR of all rows of B_0 is $2^{k-1} - 1$ while 2^{k-1} for B_1. To show the security consider restrictions of B_0 and B_1 to $k-1$ rows. Both of them contain the same columns, namely all Boolean vectors of length $k-1$, as there is exactly one possibility to extend such a column to an even resp. odd column of length k at a fixed position. This means that the restrictions of $P(B_0)$ and $P(B_1)$ to any $q < k$ rows contain the same matrices with the same frequencies, which ensures the security. □

Copyright (c) 1998, Springer-Verlag

Using a result of [2], it follows that in every k out of n scheme α is at most $1/2^{k-1}$ and m at least 2^{k-1}, showing the optimality of this construction. Naor and Shamir also have presented a basic construction principle for k out of n schemes with $m = l \cdot 2^{k-1}$, based on a set H of l functions from $\{1,\ldots,n\}$ to $\{1,\ldots,k\}$ with special properties. Choosing H as the set of all functions from $\{1,\ldots,n\}$ to $\{1,\ldots,k\}$ guarantees a k out of n scheme with $m = k^n \cdot 2^{k-1}$. Using Galois fields to construct H they claim $m = n^k \cdot 2^{k-1}$, although this seems to be only a lower bound. Using small-bias probability spaces to construct H results in $m = \log(n) \cdot 2^{O(k\log(k))}$ (see [1]). Apart from the complicateness of construction the resulting schemes are very large (for example, the resulting 4 out of 7 scheme has an m parameter of at least 19208 using Galois fields and 2^{45} using a small-bias probability space given in [3]).

4 A New Construction Principle for k out of n Schemes

The new construction principle is based on two rather simple results:

Lemma 3. *Let B_0 and B_1 be two Boolean matrices with m columns so that $P(B_0)$ and $P(B_1)$ are a k out of k secret sharing scheme with relative contrast α. Then for any Boolean matrix R with k rows and l columns the multi-sets $P([B_0R])$ and $P([B_1R])$ are a k out of k secret sharing scheme with relative contrast $\alpha \cdot m/(m+l)$ ($[B_0R]$ is the concatenation of B_0 and R).*

Proof. The contrast of the new structure follows directly from the contrast of the old, as the added Hamming weight is the same for matrices of both multi-sets. Analogously, as every restriction of $[B_0R]$ to $q < k$ rows contains the same columns as the restriction of $[B_1R]$ to these rows, the security is guaranteed, too. □

Lemma 4. *Let B_0 and B_1 be two $n \times m$ Boolean matrices so that for each subset $\{i_1,\ldots,i_k\} \subseteq \{1,\ldots,n\}$ the multi-sets of the restrictions of the elements of $P(B_0)$ and $P(B_1)$ to the rows $i_1,\ldots,i_k$ are a k out of k secret sharing scheme with constant parameters d and α. Then $P(B_0)$ and $P(B_1)$ are a k out of n secret sharing scheme with the same relative contrast α.*

Proof. The contrast is ensured, as the restrictions to k rows form a k out of k scheme and the parameters d and α are the same for all $\{i_1,\ldots,i_k\}$. The security only checks restrictions of $P(B_0)$ and $P(B_1)$ to $q < k$ rows which must contain the same matrices with the same frequencies, because these q rows belong to a k out of k scheme (strictly speaking to $\binom{n-q}{k-q}$ schemes). □

Putting these results together with Lemma 2, one obtains:

Lemma 5. *Let B_0 and B_1 be two $n \times m$ Boolean matrices so that there exist $m - 2^{k-1}$ column vectors $v_1,\ldots,v_{m-2^{k-1}} \in \{0,1\}^k$ with the following property: for every $\{i_1,\ldots,i_k\} \subseteq \{1,\ldots,n\}$ the restriction of B_0 (resp. B_1) to the rows $i_1,\ldots,i_k$ contains every even (resp. odd) column of length k exactly once and all*

Copyright (c) 1998, Springer-Verlag

columns $v_1, \ldots, v_{m-2^{k-1}}$. *Then* $P(B_0)$ *and* $P(B_1)$ *are a* k *out of* n *secret sharing scheme with relative contrast* $1/m$.

Proof. Lemmata 2 and 3 yield that for all $\{i_1, \ldots, i_k\} \subseteq \{1, \ldots, n\}$ the multi-sets of the restrictions of $P(B_0)$ and $P(B_1)$ to the rows $i_1, \ldots, i_k$ are a k out of k scheme with relative contrast $1/m$. As the columns $v_1, \ldots, v_{m-2^{k-1}}$ are the same for all restrictions, the parameters d and α are the same, too, so Lemma 4 can be applied, stating that $P(B_0)$ and $P(B_1)$ are a k out of n scheme. □

Hence, to construct a k out of n scheme one just has to construct two $n \times m$ Boolean matrices B_0 and B_1 with the property that their restrictions to k rows contain the same columns in addition to all even resp. odd columns. The number of columns of both matrices should be as small as possible, as the relative contrast is exactly $1/m$. The main idea for construction is to start with an empty matrix (which has no columns) and, for various $q \in \{0, \ldots, n\}$, add all $\binom{n}{q}$ columns which have exactly q 1's. Because of the symmetry of this construction with respect to rows, all restrictions of such a matrix to k rows contain the same columns. And one can exactly determine which columns they contain:

Lemma 6. *For* $q \in \{0, \ldots, n\}$ *let* B *be an* $n \times \binom{n}{q}$ *Boolean matrix which contains every column with* q 1*'s exactly once. Then every restriction of* B *to* k *rows (with* $k \leq n$*) contains every column with* p 1*'s exactly* $\binom{n-k}{q-p}$*-times (where* $p \in \{\max(0, q-(n-k)), \ldots, \min(q, k)\}$*).*

Proof. A column of length k with exactly p 1's can be expanded to a column of length n with exactly q 1's on $\binom{n-k}{q-p}$ different ways if the positions of expansion are fixed. Hence, the restriction of B contains every column with p 1's exactly $\binom{n-k}{q-p}$-times. In order to let this value be greater than zero p must not be less than $q-(n-k)$, because otherwise the whole column contains too many 1's to have a restriction containing only p 1's. As p cannot be negative and greater than q or k, it has to be between $\max(0, q-(n-k))$ and $\min(q, k)$. □

Lemma 6 shows a possibility to expand a matrix, if you want to add to all its restrictions (restrictions always stand for restrictions to k rows, if not stated otherwise) every column with p 1's exactly once: just add all columns with $q = p$ or $q = p + n - k$ 1's to the entire matrix, because in these cases $\binom{n-k}{q-p}$ is one. Choosing $q = p$ when $p \leq k - p$ and $q = p + n - k$ otherwise guarantees that the smaller number of columns is added. So a subroutine $ADD(p, B)$ can be formulated, which adds to each restriction of B every column with p 1's by adding columns to the entire matrix:

ADD(p,B)

1. If $p \leq k - p$, add every column with $q = p$ 1's to B.
2. If $p > k - p$, add every column with $q = p + n - k$ 1's to B.

This subroutine makes it easy to construct matrices B_0 resp. B_1 whose restrictions always contain every even resp. odd column. But besides these

Copyright (c) 1998, Springer-Verlag

columns, every restriction of B_0 and B_1 can contain remaining columns (which are the same for all restrictions of one matrix because of the construction principle). To be appropriate for a k out of n scheme these remaining columns have to be the same for B_0 and B_1 (see Lemma 5). So the remaining columns of every restriction of B_0 which are not remaining columns of every restriction of B_1, called the *rest* of B_0, have to be added to every restriction of B_1 and vice versa. In most cases these added columns will create new rests which cause new columns to be added.

The criterion for choosing q in $ADD(p, B)$ guarantees that this process stops after finitely many steps: If $p \leq k - p$, every column with $q = p$ 1's is added, otherwise every column with $q = p + n - k$ 1's. Both decisions add each column with p 1's to every restriction by adding all columns with q 1's to the entire matrix. In the first case the new remaining columns of every restriction have less than p 1's and in the second more than p 1's (see Lemma 6). So the adjustment of these remaining columns is done by adding columns with even less resp. more 1's to the entire matrix. As the column which contains only 0's resp. 1's creates no new remaining columns in the restrictions, the adjustment uses at most $\lfloor k/2 \rfloor$ steps. So the algorithm has the following form:

Algorithm 7.

1. *For all even $p \in \{0, \ldots, k\}$, add every column with p 1's to each restriction of B_0 by calling $ADD(p, B_0)$.*
2. *For all odd $p \in \{0, \ldots, k\}$, add every column with p 1's to each restriction of B_1 by calling $ADD(p, B_1)$.*
3. *While the rests of B_0 and B_1 are not empty:*
   (a) Add to B_0 all columns adjusting the rest of B_1 by calling ADD.
   (b) Add to B_1 all columns adjusting the rest of B_0 by calling ADD.

For $k = 4$ and $n = 5$ the algorithm works as follows: in the first step every column with zero, two and five 1's is added to B_0 and in the second step every column with one and four 1's to B_1. Now every restriction of B_0 resp. B_1 contains every even resp. odd column and besides that every column with one resp. zero and four 1's. So in the first run of step 3 every column with zero and five 1's is added to B_0 and every column with one 1 to B_1. Now every restriction of B_0 contains every even column and every column with zero, one and four 1's, while every restriction of B_1 contains every odd column and every column with one and four 1's and two columns without 1's. To adjust the rests in the second run of step 3 a column without 1's is added to B_0, resulting in matrices which fulfill the conditions of Lemma 5.

This algorithm can be implemented very easily and although the parameter m of the resulting schemes is hard to describe by a formula depending on k and n, its results are far better than those of Naor and Shamir for realistic values of k and n with $k < n$. For example, it generates a 4 out of 7 scheme with $m = 35$ in comparison to at least 19208 and 2^{45} when using the former methods. An overview for $k \leq n \leq 10$ is given by Table 1 in the appendix.

Copyright (c) 1998, Springer-Verlag

5 Structural Results

The following two results are rather simple, but nevertheless important:

Lemma 8. *If C_0 and C_1 are a k out of n scheme with $|C_0| \neq |C_1|$, a new k out of n scheme C_0' and C_1' with $|C_0'| = |C_1'|$ can be constructed, which has the same parameters d, α and m.*

Proof. Let r be the least common multiple of $|C_0|$ and $|C_1|$ and define C_0' (resp. C_1') as the union of $r/|C_0|$ (resp. $r/|C_1|$) copies of C_0 (resp. C_1). Then both multi-sets contain r elements and neither the contrast nor the security of the new scheme is lost. □

Lemma 9. *Let $k > k' \geq 2$ and C_0 and C_1 be a k out of k scheme with $|C_0| = |C_1|$ and parameters d, α and m. For a subset $\{i_1, \ldots, i_{k-k'}\} \subset \{1, \ldots, k\}$ delete in every matrix of C_0 (resp. C_1) every row $i_1, \ldots, i_{k-k'}$ and every column of this matrix which has a 1 in one of these rows. If the multi-set $C_0(i)$ (resp. $C_1(i)$) contains all of these new matrices with i columns ($i \in \{1, \ldots, m\}$), then all non-empty multi-sets $C_0(i)$ and $C_1(i)$ are a k' out of k' scheme with relative contrast $\alpha \cdot m/i$ and $|C_0(i)| = |C_1(i)|$.*

Proof. The Hamming weight of the OR of k' rows of an element of $C_0(i)$ (resp. $C_1(i)$) is at most $d - \alpha \cdot m - (m - i)$ (resp. at least $d - (m - i)$). Therefore, the new relative contrast is $\alpha \cdot m/i$.

To show the security of $C_0(i)$ and $C_1(i)$ consider $q < k'$ rows $j_1, \ldots, j_q$ of an element of $C_0(i)$, which are derived from q rows of an element of C_0. By adding the rows $i_1, \ldots, i_{k-k'}$ the total number of rows is at most $k - 1$. Hence, the restriction of this element of C_0 to these $k - k' + q$ rows has an equivalent in the restriction of C_1 to these rows. As the frequencies of the elements do not change, the restrictions of $C_0(i)$ and $C_1(i)$ to fixed $q < k'$ rows are the same. Therefore, the security is guaranteed. □

If C_0 and C_1 are a k out of n scheme, let $B(C_0)$ (resp. $B(C_1)$) be the concatenation of all matrices of C_0 (resp. C_1) in arbitrary order.

Theorem 10. *If C_0 and C_1 are a k out of k scheme with $r := |C_0| = |C_1|$, then $B(C_0)$ (resp. $B(C_1)$) contains every even (resp. odd) column of length k at least $r \cdot \alpha \cdot m$-times.*

Proof. First of all, every element of C_0 has to contain $\alpha \cdot m$ columns with zero 1's, as otherwise the contrast cannot be fulfilled. For every row i and every matrix of C_1 there have to be $\alpha \cdot m$ columns in which the matrix has its only 1 in row i, because otherwise the Hamming weight of the OR of all the other rows would not increase when adding the ith row. But this must happen, as the Hamming weight of all rows has to be at least d and of $k - 1$ rows at most $d - \alpha \cdot m$.

Furthermore, if k is even, $B(C_0)$ has to contain $r \cdot \alpha \cdot m$ columns filled with 1's and, if k is odd, $B(C_1)$ has to contain $r \cdot \alpha \cdot m$ such columns. To show this

Copyright (c) 1998, Springer-Verlag

we define sets $R_i^t \subseteq \{1,\ldots,m\} \times \{1,\ldots,r\}$ for $t \in \{0,1\}$ and $i \in \{1,\ldots,k\}$ by $(j,l) \in R_i^t$, if and only if the l-th matrix of C_t has a 1 in the section of its i-th row and j-th column. The Hamming weight of the OR of all k rows of $B(C_t)$ is now equal to $|R_1^t \cup \ldots \cup R_k^t|$. The principle of inclusion-exclusion says:

$$|R_1^t \cup \ldots \cup R_k^t| = \sum_{i=1}^{k} |R_i^t| - \sum_{i<j} |R_i^t \cap R_j^t| + \ldots + (-1)^{k+1} |R_1^t \cap \ldots \cap R_k^t|.$$

As the restrictions of $B(C_0)$ and $B(C_1)$ to less than k rows contain the same columns, the sections of less than k sets have to be of the same size for $t = 0$ and $t = 1$, i.e.:

$$|R_1^1 \cup \ldots \cup R_k^1| - |R_1^0 \cup \ldots \cup R_k^0| = (-1)^{k+1} |R_1^1 \cap \ldots \cap R_k^1| - (-1)^{k+1} |R_1^0 \cap \ldots \cap R_k^0|.$$

As the size of the union of all sets is the Hamming weight of the OR of all rows of $B(C_t)$, their difference has to be at least $r \cdot \alpha \cdot m$. Hence, if k is even, $B(C_0)$ has to contain $r \cdot \alpha \cdot m$ columns filled with 1's and, if k is odd, $B(C_1)$ has to contain $r \cdot \alpha \cdot m$ columns filled with 1's. Using Lemma 9 by deleting the rows which correspond to the 0's, it follows that $B(C_0)$ (resp. $B(C_1)$) contains every even (resp. odd) column at least $r \cdot \alpha \cdot m$-times. □

As every restriction of a k out of n scheme to k rows is a k out of k scheme and observing Lemma 8, one can easily conclude:

Corollary 11. *Let C_0 and C_1 be a k out of n scheme and C_0' (resp. C_1') be a restriction of C_0 (resp. C_1) to k rows. Then $B(C_0')$ (resp. $B(C_1')$) contains every even (resp. odd) column of length k at least $|C_0| \cdot \alpha \cdot m$-times (resp. $|C_1| \cdot \alpha \cdot m$-times).*

Analogously, for k out of n schemes $P(B_0)$ and $P(B_1)$ every element of a restriction of $P(B_0)$ (resp. $P(B_1)$) to k rows contains every even (resp. odd) column at least $\alpha \cdot m$-times.

6 New Bounds on the Values of α and m

If C_0 and C_1 are a k out of n scheme with $r := |C_0| = |C_1|$, Corollary 11 can be applied by counting the restrictions of $B(C_0)$ and $B(C_1)$ to k rows and the columns with q 1's in these restrictions: there are $\binom{n}{k}$ possible restrictions of $B(C_0)$ (resp. $B(C_1)$) and the number of columns with q 1's has to be at least $\binom{k}{q} \cdot r \cdot \alpha \cdot m$, when q is even (resp. odd). Therefore, the sum over all restrictions of $B(C_0)$ (resp. $B(C_1)$) to k rows of the number of different columns with q 1's in this restriction has to be at least $\binom{n}{k} \cdot \binom{k}{q} \cdot r \cdot \alpha \cdot m$, when q is even (resp. odd).

A column with exactly i 1's can be restricted in $\binom{n-i}{k-q} \cdot \binom{i}{q}$ different ways such that the restricted column contains q 1's: there are $\binom{n-i}{k-q}$ ways to choose the 0's and $\binom{i}{q}$ ways to choose the 1's. If i is less than q or if i is greater than $n-k+q$, this number is zero. Letting m_i^t be the number of columns in $B(C_t)$ with exactly

Copyright (c) 1998, Springer-Verlag

i 1's, one can compute the sum over all columns of the number of restrictions to k rows such that the actual column has exactly q 1's in these restrictions:

$$\sum_{i=q}^{n-k+q} \binom{n-i}{k-q} \cdot \binom{i}{q} \cdot m_i^t.$$

As the sum over all columns of the number of different restrictions is equal to the sum over all restrictions of the number of different columns, the above sum has to be at least $\binom{n}{k} \cdot \binom{k}{q} \cdot r \cdot \alpha \cdot m$ for all even q, if $t = 0$, and for all odd q, if $t = 1$. Because restrictions of $B(C_0)$ and $B(C_1)$ to fixed $k-1$ rows contain the same columns, the above sum has the same value for $t = 0$ and $t = 1$ when replacing k by $k-1$. As the number $r \cdot m$ of columns of $B(C_t)$ is the sum of all m_i^t over $i \in \{0, \ldots, n\}$, a lower bound on $r \cdot m$ is given by the minimum of a linear integer program. By allowing real values for m_i^t all values can be divided by $r \cdot m$ resp. r, resulting in the following bounds on the parameters α and m of k out of n schemes (which are valid for schemes with $|C_0| \neq |C_1|$ because of Lemma 8):

Theorem 12. *If C_0 and C_1 are a k out of n secret sharing scheme, α is at most $1/MIN(k,n)$ and m is at least $\lceil MIN(k,n) \rceil$, where $MIN(k,n)$ is the minimal value of the objective function of the following linear programming problem:*

$$\begin{gathered}
\textit{Minimize } m_0^0 + \ldots + m_n^0 \textit{ under the constraints:} \\
m_0^0 + \ldots + m_n^0 = m_0^1 + \ldots + m_n^1 \\
m_0^0, \ldots, m_n^0, m_0^1, \ldots, m_n^1 \geq 0 \\
\textit{For all even } q \in \{0, \ldots, k\} : \sum_{i=q}^{n-k+q} \binom{n-i}{k-q} \cdot \binom{i}{q} \cdot m_i^0 \geq \binom{n}{k} \cdot \binom{k}{q} \\
\textit{For all odd } q \in \{0, \ldots, k\} : \sum_{i=q}^{n-k+q} \binom{n-i}{k-q} \cdot \binom{i}{q} \cdot m_i^1 \geq \binom{n}{k} \cdot \binom{k}{q} \\
\textit{For all } q \in \{0, \ldots, k-1\} : \sum_{i=q}^{n-k+1+q} \binom{n-i}{k-1-q} \cdot \binom{i}{q} \cdot (m_i^0 - m_i^1) = 0
\end{gathered}$$

As $MIN(k,k)$ is exactly 2^{k-1}, the bounds of Naor and Shamir also can be concluded from this theorem. An overview of $\lceil MIN(k,n) \rceil$ for $k \leq n \leq 10$ is given in the appendix. Furthermore, it is possible to construct linear integer programming problems with $2^{n+1} + \binom{n}{k} + 1$ variables, whose solutions describe optimal k out of n schemes $P(B_0)$ and $P(B_1)$ with respect to m.

7 S-Extended n out of n Schemes

The so far used model of visual cryptography is the visual variant of the secret sharing problem. The only given information here is the information of the original picture; it is not possible to construct the n transparencies in such a way that they reveal pictures, too. Now an extended model is introduced offering the possibility to give the stack of each combination of the n transparencies a different information without any hints of the resulting pictures when stacking further transparencies. A subset $S \subseteq \mathcal{P}(\{1, \ldots, n\}) \setminus \{\emptyset\}$, i.e. a set of non-empty subsets of $\{1, \ldots, n\}$, defines which combinations shall reveal a picture, i.e. the stack of the transparencies $i_1, \ldots, i_q$ reveals one, if and only if $\{i_1, \ldots, i_q\} \in S$.

Copyright (c) 1998, Springer-Verlag

Again the construction of the n transparencies will be done pixel-wise, assuming that all pictures have the same resolution in pixels. To construct the transparencies for each pixel a matrix will be chosen of an appropriate multi-set, where this matrix determines the subpixels of the n transparencies. As there are $|S|$ combinations of the transparencies to consider, there are $2^{|S|}$ different combinations of black and white pixels. To handle these $2^{|S|}$ combinations of pixels one has to deal with $2^{|S|}$ different multi-sets C^T of matrices. They are indexed by subsets $T \subseteq S$, where the meaning of an index T is the following: for every element $\{i_1, \ldots, i_q\} \in T$ the stack of the transparencies $i_1, \ldots, i_q$ shall appear black, while the other stacks shall appear white. So the Hamming weight of the OR of the rows $i_1, \ldots, i_q$ of a matrix $B \in C^T$ has to be greater for $\{i_1, \ldots, i_q\} \in T$ than for $\{i_1, \ldots, i_q\} \notin T$.

To guarantee the security one has to demand that the restrictions of the sets C^T to the rows $i_1, \ldots, i_q$ (with $q < n$) have to contain the same elements with the same frequencies for all $T \subseteq S$ which are equal when restricted to subsets of $\{i_1, \ldots, i_q\}$. If T contains a subset of $\{i_1, \ldots, i_q\}$ which T' does not, the stack of the corresponding transparencies has to appear black when using C^T and white when using $C^{T'}$, so the restrictions of C^T and $C^{T'}$ cannot contain the same elements. But if T and T' contain the same subsets of $\{i_1, \ldots, i_q\}$, the colour of the stack of every subset of the transparencies $i_1, \ldots, i_q$ is independent of using C^T or $C^{T'}$. So the equality of the restrictions of C^T and $C^{T'}$ to these rows guarantees that no one can determine whether the subpixels come from a matrix of C^T or of $C^{T'}$.

Given these conditions the same algorithm to generate the transparencies can be used: pixel for pixel a matrix is chosen independently and equally distributed from the multi-set C^T where T matches the combination of the black pixels and this $n \times m$ matrix determines the m subpixels of the n transparencies. When given less than n transparencies even with infinite computing power one cannot gain information about any picture that reveals when stacking further transparencies. As these schemes make it possible to give only the combinations of transparencies represented by S an information, they are called *S-extended n out of n schemes*:

Definition 13. Let S be a subset of $\mathcal{P}(\{1, \ldots, n\}) \setminus \{\emptyset\}$. Multi-sets C^T (for all $T \subseteq S$) of $n \times m$ Boolean matrices are called an S-extended n out of n secret sharing scheme, if the following three properties are met:

1. For all $\{i_1, \ldots, i_q\} \in S$, there is an $d(\{i_1, \ldots, i_q\}) \in \mathbb{N}^+$ such that the Hamming weight of the OR of the rows $i_1, \ldots, i_q$ is at least $d(\{i_1, \ldots, i_q\})$ for all matrices of C^T where $\{i_1, \ldots, i_q\} \in T$.
2. For all $\{i_1, \ldots, i_q\} \in S$, there is an $\alpha(\{i_1, \ldots, i_q\}) \in \mathbb{R}^+$ such that the Hamming weight of the OR of the rows $i_1, \ldots, i_q$ is at most $d(\{i_1, \ldots, i_q\}) - \alpha(\{i_1, \ldots, i_q\}) \cdot m$ for all matrices of C^T where $\{i_1, \ldots, i_q\} \notin T$.
3. For all $\{i_1, \ldots, i_q\} \subset \{1, \ldots, n\}$, the restrictions of the multi-sets C^T to the rows $i_1, \ldots, i_q$ contain the same elements with the same frequencies for all T which are the same when restricted to subsets of $\{i_1, \ldots, i_q\}$.

Copyright (c) 1998, Springer-Verlag

Again the first two conditions guarantee the contrast of the scheme while the third one ensures the security. Naor and Shamir gave an example of an $\{\{1\},\{2\},\{1,2\}\}$-extended 2 out of 2 scheme (see [1]):

$$C^{\{\}} := P(\begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \end{bmatrix}), \quad C^{\{\{1,2\}\}} := P(\begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix})$$

$$C^{\{\{1\}\}} := P(\begin{bmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \end{bmatrix}), \quad C^{\{\{1\},\{1,2\}\}} := P(\begin{bmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix})$$

$$C^{\{\{2\}\}} := P(\begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 \end{bmatrix}), \quad C^{\{\{2\},\{1,2\}\}} := P(\begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix})$$

$$C^{\{\{1\},\{2\}\}} := P(\begin{bmatrix} 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 \end{bmatrix}), \quad C^{\{\{1\},\{2\},\{1,2\}\}} := P(\begin{bmatrix} 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix})$$

This was the previously only known real extended scheme (when choosing $S = \{\{1,\ldots,n\}\}$ an S-extended n out of n scheme is equivalent to a "normal" n out of n scheme). Now a construction principle for S-extended n out of n schemes $C^T = P(B^T)$ is presented, using the q out of q schemes $P(B_0^q)$ and $P(B_1^q)$ for all $q \in \{1,\ldots,n\}$ which are obtained by Lemma 2 (where $B_0^1 := [0]$ and $B_1^1 := [1]$).

For any $\{i_1,\ldots,i_q\} \in S$ and $t \in \{0,1\}$ the Boolean matrix $B_t(i_1,\ldots,i_q)$ is defined as follows: it has n rows and its i_p-th row is the p-th row of B_t^q (for all $p \in \{1,\ldots,q\}$) while all other rows consist only of 1's. As B_t^q has 2^{q-1} columns, $B_t(i_1,\ldots,i_q)$ has 2^{q-1} columns, too. For any $T \subseteq S$ and $\{i_1,\ldots,i_q\} \in S$, the matrix $B(T,\{i_1,\ldots,i_q\})$ is defined as:

$$B(T,\{i_1,\ldots,i_q\}) := \begin{cases} B_0(i_1,\ldots,i_q) & \text{, if } \{i_1,\ldots,i_q\} \notin T \\ B_1(i_1,\ldots,i_q) & \text{, if } \{i_1,\ldots,i_q\} \in T \end{cases}$$

For fixed n and $S \subseteq \mathcal{P}(\{1,\ldots,n\}) \setminus \{\emptyset\}$ and any $T \subseteq S$ the Boolean matrix B^T is defined as the concatenation of the matrices $B(T,\{i_1,\ldots,i_q\})$ for all $\{i_1,\ldots,i_q\} \in S$ (in arbitrary order). Therefore, the number of columns of B^T is $\sum_{q=1}^{n} 2^{q-1} \cdot b_q$ where b_q is the number of elements of S which contain exactly q elements.

The rather technical proof of the correctness of this construction is omitted to clarify the idea of this principle. The new matrices B^T consist of $|S|$ matrices $B(T,\{i_1,\ldots,i_q\})$, which contain the matrices B_t^q expanded by $n-q$ rows consisting only of 1's. Such a matrix is responsible for the stack of the transparencies $i_1,\ldots,i_q$ and as the appropriate t is chosen dependent on T, the contrast of the stack of these transparencies is guaranteed. The security of the extended scheme follows directly from the security of the old ones.

To give a concrete example two matrices B^T of the $\{\{1\},\{2\},\{3\},\{1,2\},\{1,3\},\{2,3\},\{1,2,3\}\}$-extended 3 out of 3 scheme will be constructed, using the 2 out of 2 and 3 out of 3 scheme given by Lemma 2 (the only purpose of the lines is a better general view of the construction):

$$B^{\{\{1\},\{2,3\},\{1,2,3\}\}} = \left[\begin{array}{c|c|c|cc|cc|cc|cccc} 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{array}\right]$$

Copyright (c) 1998, Springer-Verlag

$$B^{\{\{1\},\{3\},\{1,3\}\}} = \left[\begin{array}{c|c|c|cc|cc|cc|cccc} 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \end{array}\right]$$

Another example is given by Naor and Shamir's $\{\{1\},\{2\},\{1,2\}\}$-extended 2 out of 2 scheme, as the above principle constructs the given multi-sets of matrices.

Acknowledgements

I thank Ingo Wegener for his help and his encouragement to write this paper.

References

[1] M. Naor and A. Shamir, *Visual cryptography*, in "Advances in Cryptology - Eurocrypt '94", Springer-Verlag, Berlin, pp. 1-12, 1995

[2] N. Linial and N. Nisan, *Approximate inclusion-exclusion*, Combinatorica **10**, pp. 349-365, 1990

[3] N. Alon, O. Goldreich, J. Hastad and R. Peralta, *Simple constructions of almost k-wise independent random variables*, Random Structures and Algorithms **3**, pp. 289-304, 1992

Appendix

To elucidate the good results of the algorithm presented in Section 4 a table of the parameter m of the k out of n schemes which were computed by the algorithm follows. As one can easily show that columns of length n contained by both matrices B_0 and B_1 can be deleted, this improvement has been added to the algorithm. So this table shows slightly better results as a concrete implementation of the algorithm in Section 4 would do. In parentheses the values $\lceil MIN(k,n) \rceil$ according to Theorem 12 are given for comparison (which are printed in italics, if $MIN(k,n)$ is no integer). As the relative contrast of the schemes is exactly

$k \backslash n$	2	3	4	5	6	7	8	9	10
2	2 (2)	3 (3)	4 (3)	5 (*4*)	6 (*4*)	7 (*4*)	8 (*4*)	9 (*4*)	10 (*4*)
3	-	4 (4)	6 (6)	8 (6)	10 (7)	12 (7)	14 (7)	16 (7)	18 (*8*)
4	-	-	8 (8)	15 (*13*)	24 (*14*)	35 (14)	48 (*15*)	63 (15)	80 (15)
5	-	-	-	16 (16)	30 (25)	48 (27)	70 (*30*)	96 (*30*)	126 (*31*)
6	-	-	-	-	32 (32)	70 (*53*)	128 (*59*)	210 (*61*)	320 (*62*)
7	-	-	-	-	-	64 (64)	140 (105)	256 (*117*)	420 (*121*)
8	-	-	-	-	-	-	128 (128)	315 (217)	640 (238)
9	-	-	-	-	-	-	-	256 (256)	630 (434)
10	-	-	-	-	-	-	-	-	512 (512)

Table 1. The parameter m of the resulting k out of n schemes (and $\lceil MIN(k,n) \rceil$).

$1/m$, this table also gives information about the quality of the corresponding solution of the secret sharing problem. As $1/\lfloor MIN(k,n) \rfloor$ is an upper bound on α, an overview of the best possible relative contrast is given, too.

The next three pages give an example of an $\{\{1,2\},\{1,3\},\{2,3\}\}$-extended 3 out of 3 scheme: when copied on transparencies and stacked carefully each combination of two transparencies reveals a different picture.

Copyright (c) 1998, Springer-Verlag

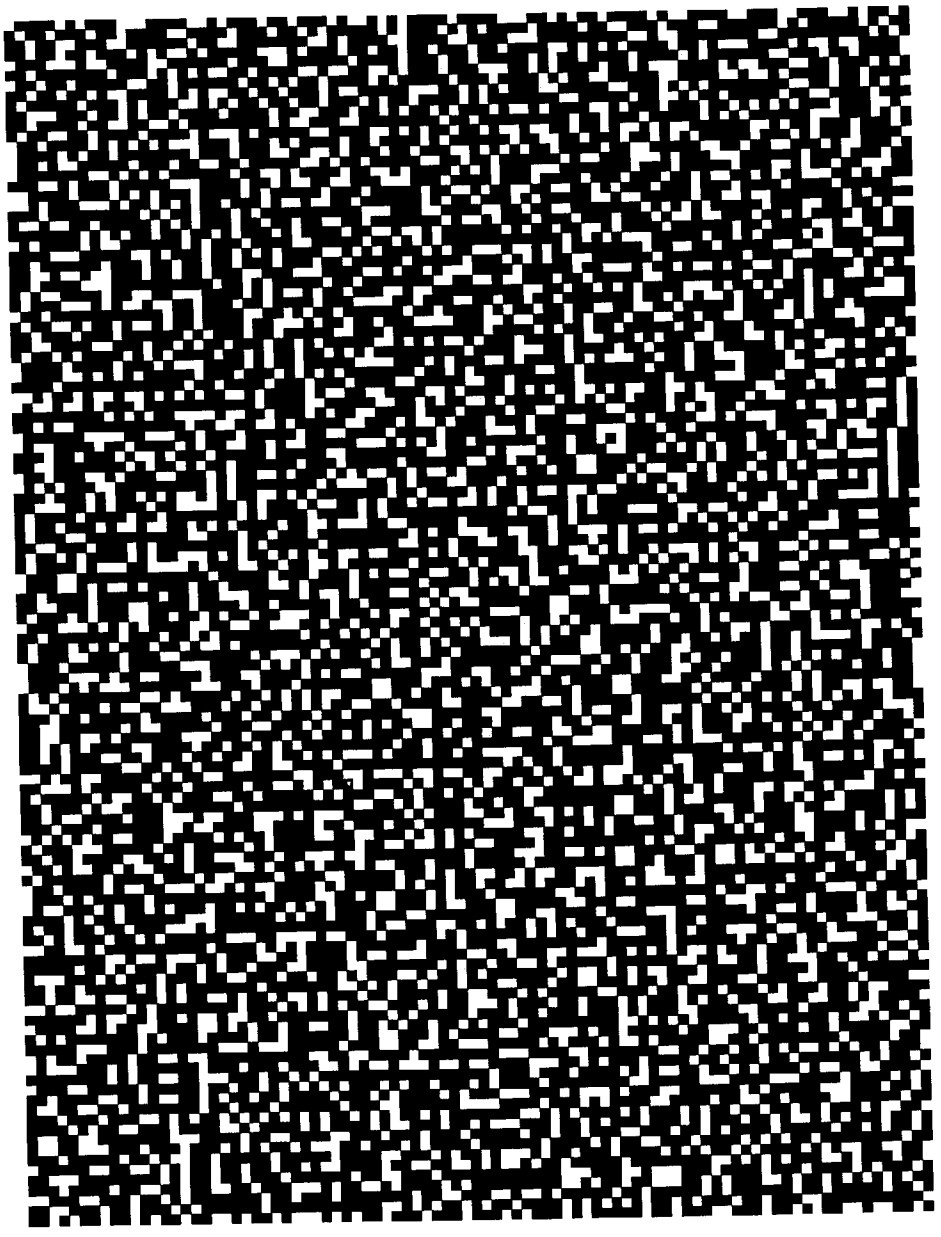

Fig. 1. Transparency 1

Copyright (c) 1998, Springer-Verlag

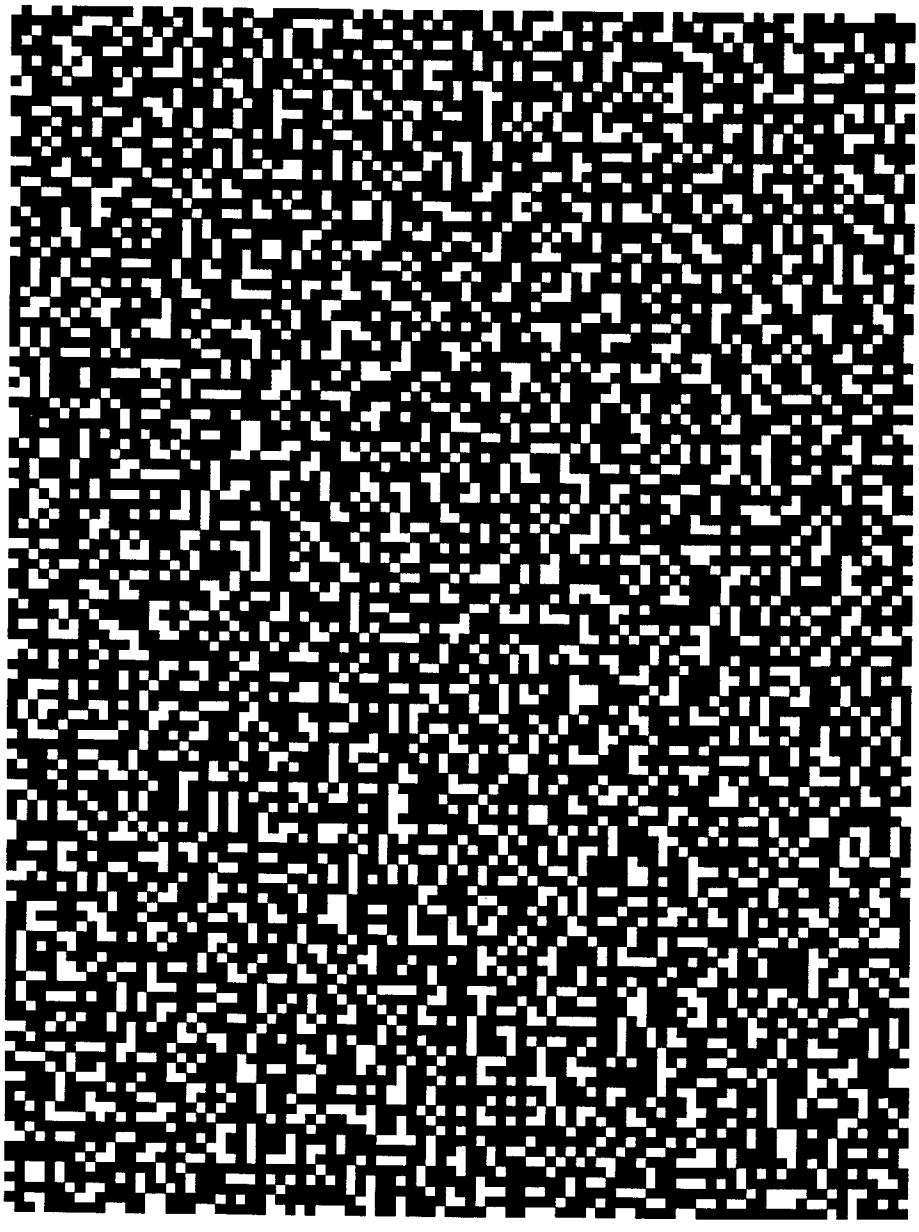

Fig. 2. Transparency 2

Copyright (c) 1998, Springer-Verlag

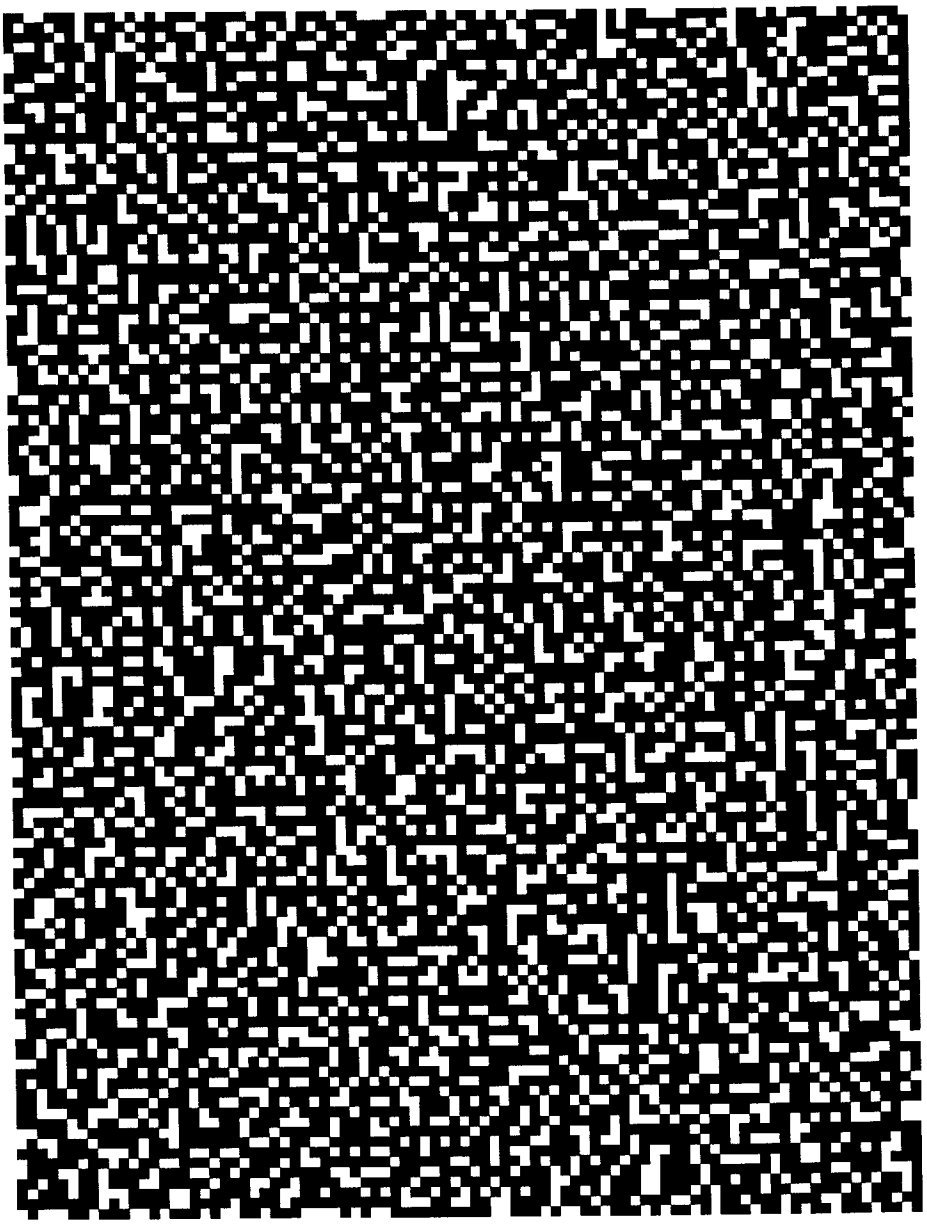

Fig. 3. Transparency 3

Copyright (c) 1998, Springer-Verlag