Constructions and Properties of k out of n visual secret sharing schemes *

Eric R. Verheul
Ministry of the Interior
P.O. Box 20010
2500 EA, the Hague, the Netherlands
E-mail Eric.Verheul@pobox.com
and
Henk C.A. van Tilborg
Department of Mathematics and Computing Science
Eindhoven University of Technology
P.O. Box 513 5600 MB, Eindhoven, the Netherlands
E-mail henkvt@win.tue.nl

Abstract

The idea of visual k out of n secret sharing schemes was introduced in [**?**]. Explicit constructions for $k = 2$ and $k = n$ can be found there. For general k out of n schemes bounds have been described.

Here, two general k out of n constructions are presented. Their parameters are related to those of maximum size arcs or MDS codes. Further, results on the structure of k out of n schemes, such as bounds on their parameters, are obtained. Finally, the notion of coloured visual secret sharing schemes is introduced and a general construction is given.

Key words Visual cryptography, Secret sharing schemes, MDS codes, Arcs

*To appear in *Codes, Designs and Cryptography.*

1 Introduction

The possibility of using human visual intelligence as part of a symmetrical cipher algorithm, was first discussed in [**?**]. Independently, the notion of visual k out of n secret sharing schemes is introduced [**?**]. The idea is that an image (e.g. picture or text) is transformed into n transparencies (shares), in such a way that if one puts any k-tuple of transparencies on top of each other, the original image is again visible, while with any $(k-1)$-tuple of transparencies no information about the original image is released (in the sense that any possibility is equally likely). Actually, the concept of a visual 2 out of 2 secret sharing scheme constitutes to a visual symmetrical cipher, earlier described in [**?**, p.1019].

The technique, explained in [**?**], divides any pixel of the original image into b subpixels. On each transparency some subpixels of any pixel are white while the others are black.
When held to the light, white subpixels let through light and black subpixels stop it. So when several transparencies on top of each other are held to the light, one sees the "or" result of the transparencies, i.e. a subpixel is seen as white if all underlying subpixels are white, otherwise it is seen as black. A pixel (the total of the b subpixels) will be observed as white if sufficiently many subpixels (at least h) are white, while it will be observed as black if not to many of them (at most l) are white. Here $h > l$ are some non-negative integers.
In the mathematical model of this technique, white (sub)pixels are represented with 0 ("they form *no* obstruction to light") and black (sub)pixels are represented with 1 ("they stop light"). To give a formal definition, let $z(\underline{v})$ denote the number of zero coordinates of a vector $\underline{v}$ (note that $z(\underline{v}) + w(\underline{v}) = b$, where $w(\underline{v})$ denotes the Hamming weight of $\underline{v}$). From [**?**] we now quote - with some notational changes- the following definition of a k out of n secret sharing scheme, or k out of n scheme for short.

Definition 1.1 *A k out of n visual secret sharing system $S = (\mathcal{C}_0, \mathcal{C}_1)$ consists of two collections of $n \times b$ Boolean matrices $\mathcal{C}_0$ and $\mathcal{C}_1$. To share a white pixel, the dealer randomly chooses one of the matrices in $\mathcal{C}_0$, and to share a black pixel, the dealer randomly chooses one of the matrices in $\mathcal{C}_1$. The n transparencies (rows) are distributed over the n users (participants of the* *system). The chosen matrix defines the colour of the b subpixels of that particular pixel in each one of the n transparencies (a 1 stands for black and 0 for white). The solution is considered valid if the following three conditions are met:*

1. *For any S in $\mathcal{C}_0$, the "or" $\underline{v}$ of any k of the n rows satisfies $z(\underline{v}) \geq h$.*
2. *For any S in $\mathcal{C}_1$, the "or" $\underline{v}$ of any k of the n rows satisfies $z(\underline{v}) \leq l$.*
3. *For any $i_1 < i_2 < \ldots < i_s$ in $\{1, 2, \ldots, n\}$ with $s < k$, the two collections of $s \times b$ matrices $\mathcal{D}_j$ for $j \in \{0, 1\}$ obtained by restricting each $n \times b$ matrix in $\mathcal{C}_j$ (where $j = 0, 1$) to rows $i_1, i_2, \ldots, i_s$ are indistinguishable in the sense that they contain the same matrices with the same frequencies.*

Here $h > l$ and b is called the blocklength of the scheme S. By the third property, the first rows of the matrices in $\mathcal{C}_0$, and $\mathcal{C}_1$ give rise to the same frequency-tables. Hence, the cardinality of $\mathcal{C}_0$, must coincide with the cardinality of $\mathcal{C}_1$ and will be denoted with r. The parameters of a scheme will be denoted by $[b; h, l; r]$ or $[b; h, l]$ when r is not relevant.
In [**?**] the contrast between combined shares that come from a white pixel and a black pixel is implicitly defined as $h - l$, and the loss of contrast as $(h - l)/b$. This concept of contrast is not really suitable. For an intuitive justification: consider the contrast of two adjacent buildings A and B in the night, formed by the number of illuminated windows. Then the contrast formed by 100 illuminated windows in A and 99 in B, is much less than 1 illuminated window in A and 0 in B. Aside from intuition, also references in literature suggest that the contrast between two optical regions is characterised by the *relative* difference of the irradiance within the regions. See [**?**, p.272] and [**?**, p.34] (Willem van den Bosch is thanked for pointing out these references). In the present circumstances we therefore would like to propose $(h - l)/(h + l)$ as measure of contrast, and the loss of contrast as $(h - l)/b(h + l)$.
Usually one is interested in schemes of high contrast and low blocklength. Observe that contrast is maximal when $l = 0$, which is a motivation to call schemes of type $[b; h, l = 0]$ *maximal contrast* schemes.
In [**?**] constructions can be found of k out of n visual secret sharing systems with parameters:

k	n	b	h	l	r
2	n	n	$n-1$	$n-2$	$n!$
k	k	2^k	2	0	$2^k!$
k	k	2^{k-1}	1	0	$2^{k-1}!$

Further, existence proofs for two types of general k out of n visual secret sharing systems are given by means of hash functions. The first system has blocklength $b = n^k 2^{k-1}$ and the second $b = log(n)2^{O(klogk)}$. Due to a different concept of "contrast" only the quantities $\alpha = (h-l)/b$ are given in [**?**]; in the first system this equals $(2\exp)^{-k}/\sqrt{2\pi k}$, in the second this equals $2^{-\Omega(k)}$. Many schemes in [**?**] are examples of a generic method to construct k out of n schemes that we shall describe now. Let A_0 and A_1 be Boolean $n \times b$ matrices and $h > l$ integers, such that:

1-2. The "or" $\underline{v}$ of any k out of n rows of A_0 (resp. A_1) satisfies $z(\underline{v}) \geq h$ (resp. $z(\underline{v}) \leq l$).

3. For any $i_1 < i_2 < \ldots < i_s$ in $\{1, \ldots, n\}$ with $s < k$, the matrices A_0 and A_1 restricted to rows $i_1, i_2, \ldots i_s$ are equal modulo a permutation of the columns.

Then, by letting $\mathcal{C}_0$ (resp. $\mathcal{C}_1$) consist of all matrices obtained by permutations of the columns of A_0 (resp. A_1) one obtains a k out of n scheme (with parameters $[b; h, l; b!]$). Such schemes we call *generated* by A_0 and A_1. Observe that the implementation of schemes of these types require little (computer) memory, as the collections $\mathcal{C}_0$ and $\mathcal{C}_1$ are fully determined by A_0, A_1 and permutations of b elements.
As an example, in [**?**] the following 2 out of n visual secret sharing scheme with $b = n$ and $h = n-1, l = n-2$ is generated by:

$$A_0 = \begin{pmatrix} 1 & 0 & . & . & . & 0 \\ 1 & 0 & . & . & . & 0 \\ . & . & . & . & . & . \\ 1 & 0 & . & . & . & 0 \end{pmatrix} \quad ; \quad A_1 = \begin{pmatrix} 1 & 0 & . & . & . & 0 \\ 0 & 1 & . & . & . & 0 \\ . & . & . & . & . & . \\ 0 & 0 & . & . & . & 1 \end{pmatrix}.$$

Observe that the contrast of this scheme equals $1/(2n-3)$ which for large n is nearly zero; by interchanging 0 and 1 one obtains a 2 out of n scheme with *maximal* contrast 1!
Next, suppose that A_0 and A_1 satisfy the following strengthing of 3:

3' For each any $i_1 < i_2 < \ldots < i_s$ and $j_1 < j_2 < \ldots < j_s$ in $\{1, ..., n\}$ with $s < k$, the matrix A_0 restricted to rows $i_1, i_2, ..., i_s$ and A_1 restricted to rows $j_1, j_2, ..., j_s$ are equal modulo a permutation of the columns.

Then the pair A_0, A_1 is called *systematic* and the k out of n scheme they generate is called a *strong* k out of n scheme. Finally, we note that strong schemes are an example of the *uniform* schemes of [**?**], which are schemes for which $z(\underline{v})$ of the "or" $\underline{v}$ of any $s < k$ transparencies in $\mathcal{C}_0$ or $\mathcal{C}_1$ only depends on the number s. Actually, one of our results (Theorem **??**) states that uniform schemes give rise to strong schemes in a very canonical way.

In Sections **??** and **??** we propose two explicit strong k out of n visual secret sharing systems. Their parameters are connected to notions in finite geometry and coding theory. To this end we first review the theory that we need for these constructions.

2 Some facts about arcs and MDS codes

Let $V_m(q)$ denote the m-dimensional vectorspace over the Galois field $GF(q)$. As usual, the cardinality of a set A will be denoted by $|A|$. A (sub)set of cardinality k will be called a k-(sub)set.

Definition 2.1 *For fixed q and $m \geq 1$, an n-*arc *is defined as an n-subset $\mathcal{A}$ of $V_m(q)$ with the property that each m elements in $\mathcal{A}$ are linearly independent.*
The maximum n for which an n-arc in $V_m(q)$ exists will be denoted by $r(q, m)$.

Quite clearly, $r(q, 1) = q - 1$ for all q. From now on we assume that $m \geq 2$. There is a well-known relation between the $r(q, m)$-function and the existence of q-ary Maximum Distance Separable (MDS) codes, i.e. q-ary $[n, m, d]$ codes with $d = n - m + 1$. For definitions and proofs, we refer the reader to [**?**] (in particular to Ch. 11, §2).

Theorem 2.2 *Let q be some prime power and n and m integers, where $m \geq 2$. Then the following statements are equivalent.*

1. *An n-arc exists in $V_m(q)$,*
2. *$n \leq r(m, q)$,*

3. A q-ary $[n, n-m, m+1]$ MDS code exists,

4. A q-ary $[n, m, n-m+1]$ MDS code exists.

Lemma 2.3 *For all $m \geq 2$,*

$$r(q, m+1) \leq r(q, m) + 1. \tag{1}$$

Proof: Consider an n-arc $\mathcal{A} = \{\underline{a}_1, \underline{a}_2, \ldots, \underline{a}_n\}$ in $V_{m+1}(q)$. By simple basis manipulations, we may assume that $\underline{a}_1 = (0, \ldots, 0, 1)$. Remove the last coordinate from the other $n-1$ vectors in the arc. Since $\mathcal{A}$ is an n-arc in $V_{m+1}(q)$, it follows that these $n-1$ shortened vectors (in $V_m(q)$) have the property that any m-tuple of them is linearly independent. In other words, we have found an $(n-1)$-arc in $V_m(q)$. It follows that $n - 1 \leq r(q, m)$. Substitution of $n = r(q, m+1)$ yields (**??**). □

Theorem 2.4 *The following relations hold for $r(q, m)$:*

$$r(q, 2) = q + 1 \tag{2}$$

$$q + 1 \leq r(q, m) \leq q + m - 1 \quad \textit{if} \quad 2 \leq m \leq q - 1, \tag{3}$$

$$r(q, m) = m + 1 \quad \textit{if} \quad m \geq q. \tag{4}$$

Proof: Although known from the literature, we show all the above statements.
Relation (**??**) is just a particular case of (**??**).
The left most inequality in (**??**) again follows from an explicit construction. Indeed, the vectors $(0, \ldots, 0, 1)$ and $(1, \omega^1, \ldots, \omega^{m-1})$ with ω in $GF(q)$ form an $(q+1)$-arc, as follows readily with a Vandermonde matrix argument.
The second inequality in (**??**) is a direct consequence of Lemma **??**.
To prove that $r(q, m) \geq m + 1$, one can take any basis $\underline{a}_1, \underline{a}_2, \ldots, \underline{a}_m$ in $V_m(q)$ and add the vector $\underline{a}_{m+1} = \sum_{i=1}^{m} \underline{a}_i$ to obtain an $(m+1)$-arc. On the other hand, if $r(q, m) = m + 2$ (or more) and $m \geq q$ we get a contradiction from Theorem **??** 4), because the Hamming bound implies that an $[m+2, m, 3]$ code does not exist. Indeed, $q^m\left(1 + (m+2)(q-1)\right) \geq q^m\left(1 + (q+2)(q-1)\right) > q^{m+2}$, for $m \geq q$. □

It is a well-known conjecture that for $2 \leq m \leq q - 1$ the actual value of $r(q, m)$ is $q + 1$, except when q is even and $m = 3$ or $q - 1$, in which case $r(q, m) = q + 2$. The conjecture has been proven for many cases. For an overview of the current situation we refer to [?] or [?].

3 A k out of n scheme

To construct k out of n visual secret sharing schemes we shall make use of linearly independent functionals defined on $V_m(q)$. For any given basis of $V_m(q)$ there is a one-to-one correspondence between functionals $F(\underline{x})$ on $V_m(q)$ and vectors $\underline{f}$ in $V_m(q)$ which is given by

$$F(\underline{x}) = (\underline{f}, \underline{x}) = f_1x_1 + f_2x_2 + \ldots + f_mx_m.$$

Clearly, functionals $F_i(\underline{x}),\ 1 \leq i \leq l$, are linearly independent if and only if the corresponding vectors $\underline{f}_i,\ 1 \leq i \leq l$, are linearly independent.
Consider a numbering of the vectors in $V_m(q)$, say $\underline{u}_1, \underline{u}_2, \ldots, \underline{u}_{q^m}$. The $n \times q^m$ *representation matrix* S of n functionals $F_i(\underline{x}),\ 1 \leq i \leq n$, with respect to the vectors $\underline{u}_i,\ 1 \leq i \leq q^m$, is defined by

$$S_{i,j} \ = \ F_i(\underline{u}_j), \qquad 1 \leq i \leq n,\ 1 \leq j \leq q^m. \tag{5}$$

Elementary linear algebra shows the following lemmas.

Lemma 3.1 *Let, in the above notation, k be the dimension of the linear span of n functionals. Then the representation matrix S of these functionals will contain exactly q^{m-k} all-zero columns.*
If $n = k = m$ (exactly m linearly independent functionals are considered) each vector in $V_m(q)$ occurs exactly once as a column in S.

Proof: The null-space of k independent functionals of $V_m(q)$ has dimension $m - k$. □

Lemma 3.2 *Let $F_i,\ 1 \leq i \leq k$, be a set of linearly independent functionals on $V_m(q)$ (so $k \leq m$) and let S be the representation matrix of this set with respect to the vectors $\underline{u}_j,\ 1 \leq j \leq q^m$.*
Let $G_i,\ 1 \leq i \leq k$, be a second set of linearly independent functionals on $V_m(q)$. Then a (second) numbering $\underline{v}_1, \underline{v}_2, \ldots, \underline{v}_{q^m}$ of the vectors in $V_m(q)$ exists such that the representation matrix T of the functionals G_i's with respect to the vectors $\underline{v}_j,\ 1 \leq j \leq q^m$, is identical to S.

Proof: It suffices to prove the lemma for $k = m$ (otherwise add suitable linearly independent functionals to both sets).

Consider the two $m \times q^m$ matrices $S = (F_i(\underline{u}_j))_{ij}$ and $S' = (G_i(\underline{u}_j))_{ij}$. By Lemma **??**, S and S' have the same column set, so there exists a permutation π of $\{1, 2, \ldots, q^m\}$ with induced permutation matrix P such that $S = S'P$. Equivalently,

$$F_i(\underline{u}_j) = G_i(\underline{u}_{\pi(j)}) \qquad \text{for all } 1 \leq i \leq m,\ 1 \leq j \leq q^m.$$

Putting $\underline{v}_j = \underline{u}_{\pi(j)},\ 1 \leq j \leq q^m$, one gets that

$$T_{ij} = G_i(\underline{u}_{\pi(j)}) = F_i(\underline{u}_j) = S_{ij}.$$

□

The lemmas above make it possible to prove that the scheme below yields a k out of n visual secret sharing scheme. In the construction, the value of q has to be sufficiently large.

Construction 3.3 *A strong k out of n visual secret sharing scheme with parameters $b = (q^k - 1)/(q - 1)$, $h = 1$, $l = 0$, $|\mathcal{C}_0| = |\mathcal{C}_1| = q^k!$ can be obtained from the following steps.*

1. *Choose a finite field size q with $r(q, k - 1) \geq n$ and $r(q, k) \geq n$.*

   Identify the vectors in $V_m(q)$ that are a scalar multiple of each other and discard $\underline{0}$. One obtains $PG_{m-1}(q)$, the $(m - 1)$-dimensional projective space over $GF(q)$. It contains $(q^m - 1)/(q - 1)$ vectors. Consider any numbering of the vectors in $V_m(q)$, say $\underline{u}_1, \underline{u}_2, \ldots, \underline{u}_{q^m}$ and let $\underline{v}_1, \underline{v}_2, \ldots, \underline{v}_{(q^m-1)/(q-1)}$, be the reduced set of vectors constituting $PG_{m-1}(q)$.

2. *Choose functionals $F_1, F_2, \ldots, F_n$ on $V_k(q)$, such that any k of them are linearly independent. This is possible by the definition of $r(q, k)$.*

   Let S be the representation matrix of the functionals F_i, $1 \leq i \leq n$, with respect to the numbering $\underline{u}_j$, $1 \leq j \leq q^k$. Let S' be the restriction of S to the columns indexed by $\underline{v}_j$, $1 \leq j \leq (q^m - 1)/(q - 1)$. Replace all non-zero elements in S' by 1.

   The $n \times (q^m - 1)/(q - 1)$ binary matrices generated by S' form the class $\mathcal{C}_1$.

3. *Choose n functionals, say $G'_1, G'_2, \ldots, G'_n$ defined on $V_{k-1}(q)$, such that any $(k-1)$ of them are linearly independent. Extend their definition in the canonical way to obtain the functionals $G_1, G_2, \ldots, G_n$ on $V_k(q)$ (so $G_i(x_1, \ldots, x_{k-1}, x_k) := G'_1(x_1, \ldots, x_{k-1})$). Any $k-1$ of them are linearly independent, but any k-tuple is linearly dependent, because the dimension of $V_{k-1}(q)$ is $k-1$.*

   Convert the representation matrix T of the functionals G_i in the same way as above to a binary $n \times (q^m-1)/(q-1)$ matrix T'. The $n \times (q^m - 1)/(q-1)$ binary matrices generated by T' form the class $\mathcal{C}_0$.

Proof: The "or" of any k rows of a matrix in $\mathcal{C}_1$ consists of only ones, because by Lemma **??** (2-nd statement) the q-ary representation matrix from which it is obtained, when restricted to these k rows, contains each possible column exactly once and the $\underline{0}$ column was removed.
The "or" of any k rows of a matrix in $\mathcal{C}_0$ contains 1 zero and $(q^k-q)/(q-1)$ ones, because by Lemma **??** (1-st statement) the q-ary representation matrix from which it is obtained, when restricted to these k rows, contains each possible column exactly once. The security of the scheme (see Definition **??**) also follows from Lemma **??**. $\square$

To construct a k out of k scheme in the above way, it suffices to take $q = 2$ (see (**??**)). In this case, Construction **??** reduces to what amounts to a modest improvement of Construction I in [**?**].
If $n-1$ is a prime power, one can take $q = n-1$ (see (**??**)). The blocklength of this k out of n scheme equals $((n-1)^k - 1)/(n-2)$.
Let us compare our scheme with the two corresponding schemes of [**?**] - also mentioned in Section **??**. The first scheme has a larger blocklength, the second one has a much smaller blocklength. Both schemes have less contrast than the above scheme. Also, the first scheme in [**?**] has more loss of contrast. We were not able to compare the loss of contrast of the second scheme of [**?**] with ours.

4 A second k out of n scheme

As in the previous section, we start with some general considerations. Let $G(\underline{x})$ and $F_1(\underline{x}), F_2(\underline{x}), \ldots, F_n(\underline{x})$ be functionals defined on $V_m(q)$. Let $\underline{u}_j$, $1 \leq$

$j \leq q^{m-1}$, be a numbering of the vectors $\underline{x}$ in $V_m(q)$ for which $G(\underline{x}) = 0$ and $\underline{v}_j,\ 1 \leq j \leq q^{m-1}$, likewise for the vectors $\underline{x}$ in $V_m(q)$ for which $G(\underline{x}) = 1$. These numberings define the $n \times q^{m-1}$ representation matrices S and T by

$$S_{ij} = F_i(\underline{u}_j), \quad 1 \leq i \leq n,\ 1 \leq j \leq q^{m-1}, \tag{6}$$
$$T_{ij} = F_i(\underline{v}_j), \quad 1 \leq i \leq n,\ 1 \leq j \leq q^{m-1}. \tag{7}$$

It is again a matter of elementary linear algebra to prove the following lemma.

Lemma 4.1 *Consider functionals G and $F_i,\ 1 \leq i \leq n$, on $V_m(q)$. The following three statements are equivalent:*

1. *For each numbering $\underline{v}_j,\ 1 \leq j \leq q^{m-1}$, of $G^{-1}(1)$ a numbering $\underline{u}_j,\ 1 \leq j \leq q^{m-1}$, of $G^{-1}(0)$ exists (and the other way around) such that the representation matrices S and T, defined by (**??**) and (**??**) are the same.*
2. $\left(\bigcap_{i=1}^{n} F_i^{-1}(0)\right) \cap G^{-1}(1) \neq \emptyset$,
3. *G is not in the span of $F_1, F_2, \ldots, F_n$.*

Proof:
2) $\Rightarrow$ 1): Let a be an element in the left hand side of statement 2. above. Further, let $\underline{v}_j,\ 1 \leq j \leq q^{m-1}$ be a numbering of $G^{-1}(1)$ with representation matrix T. Then $\underline{u}_j = \underline{v}_j - \underline{a},\ 1 \leq j \leq q^{m-1}$ is a numbering of $G^{-1}(0)$ and its representation matrix T equals S, because $F_i(\underline{u}_j) = F_i(\underline{v}_j - \underline{a}) = F_i(\underline{v}_j) - F_i(\underline{a}) = F_i(\underline{v}_j),\ 1 \leq j \leq q^{m-1}$, and $G(\underline{u}_j) = G(\underline{v}_j - \underline{a}) = G(\underline{v}_j) - G(\underline{a}) = 1 - 1 = 0$.
The proof of the "other way around" in condition 1) (i.e. the role of $G^{-1}(0)$ and $G^{-1}(1)$ are interchanged) goes the same way.

1) $\Rightarrow$ 2): Choose numberings of the elements in $G^{-1}(0)$ and $G^{-1}(1)$ such that the corresponding representation matrices S and T are identical. Since S contains the all-zero column at least once, there must be a vector in $G^{-1}(1)$, say $\underline{a}$, for which $F_i(\underline{a}) = 0$, for all $1 \leq i \leq n$. This means that $\underline{a} \in \left(\bigcap_{i=1}^{n} F_i^{-1}(0)\right) \cap G^{-1}(1)$.

2) $\Leftrightarrow$ 3): This equivalence is well-known (compare for instance with [**?**, Lemma 3.9]). $\square$

Construction 4.2 *A strong k out of n visual secret sharing scheme with parameters $b = q^{k-1}$, $h = 1$, $l = 0$, $|\mathcal{C}_0| = |\mathcal{C}_1| = q^{k-1}!$ can be obtained from the following steps.*

1. *Choose a finite field size q such that $r_q(k) \geq n + 1$.*

2. *Choose $n + 1$ functionals on $V_k(q)$, to be called $F_1, F_2, \ldots, F_n$ and G, such that any k of them are linearly independent (so, the intersection of the kernel of any k of them is just $\{\underline{0}\}$).*

3. *Let S be the representation matrix of the functionals F_i, $1 \leq i \leq n$, with respect to a numbering $\underline{u}_j$, $1 \leq j \leq q^{k-1}$, of $G^{-1}(0)$. Replace all non-zero elements in S by 1.*

   The $n \times q^{k-1}$ matrices generated by S form the class $\mathcal{C}_1$.

4. *Let T be the representation matrix of the functionals F_i, $1 \leq i \leq n$, with respect to a numbering $\underline{v}_j$, $1 \leq j \leq q^{k-1}$, of $G^{-1}(1)$. Replace all non-zero elements in T by 1.*

   The $n \times q^{k-1}$ matrices generated by T form the class $\mathcal{C}_0$.

Proof: By Lemma **??**, the "or" of k rows of T has no zeroes and q^{k-1} ones. The "or" of k rows of S has precisely 1 zero and $q^{k-1} - 1$ ones. The rest of the proof also follows from Lemma **??**. □

When $k = n$ one can take $q = 2$ and the above scheme reduces to Construction II in [**?**].
If n is a prime power, one can take $q = n$ (see (**??**)). The blocklength of this k out of n scheme equals n^{k-1}. The comparison of our scheme with the two corresponding schemes of [**?**] - also mentioned in Section **??** - is similar to the comparison at the end of Section **??**.
In many cases, Construction **??** gives k out of n schemes with smaller blocklength than Construction **??** (e.g. if $k = n$). However there are situations where the opposite is true. For instance, if $n - 1$ is a prime power, then Construction **??** gives a blocklength of $((n-1)^k - 1)/(n-2)$. On the other hand, it can be easily shown that the blocklength of Construction **??** is at least n^{k-1}, which is larger than the first blocklength.

5 Bounds on k out of n schemes

In this section we will obtain some results on the structure of k out of n secret sharing schemes. In order to prove these results we develop a method of decomposing a k out of n secret sharing scheme into two $k-1$ out of $n-1$ schemes. The significance of this method lies in the fact that it enables proofs by induction. Let us first mention some of our results.

Theorem 5.1 *For any k out of n secret sharing scheme with parameters $[b; h, l]$ we have $b \geq (h-l)2^{k-1}$.*

Theorem 5.2 *Let $b(k,n)$ be the minimal blocklength of any uniform k out of n scheme, then $b(k,n) \geq 2 \cdot b(k-1, n-1)$. Moreover, if g is minimal with respect to $\binom{g}{\lfloor g/2 \rfloor} \geq n-k+2$, then $b(k,n) \geq g \cdot 2^{k-2}$. In particular, the blocklength of any uniform k out of n scheme with $k \neq n$ is at least $3 \cdot 2^{k-2}$.*

Theorem 5.3 *Let $S = (\mathcal{C}_0, \mathcal{C}_1)$ be a uniform k out of n scheme with parameters $[b; h, l]$. Then any A_0 in $\mathcal{C}_0$ and A_1 in $\mathcal{C}_1$ are systematic and the scheme generated by A_0 and A_1 yields a strong k out of n scheme with parameters $[b; h, l]$.*

Theorem **??** is an improvement of [**?**, Theorem 1] of Naor and Shamir. Moreover, contrary to the proof of Naor and Shamir, ours is given within the context of visual sharing schemes. From Theorem **??** one easily deduces that the loss of contrast of any k out of k scheme $[b; h, l]$ is at least $1/(h+l)2^{k-1}$. Hence the k out of k scheme with parameters $[2^{k-1}; 1, 0]$ mentioned in Section **??** has minimal loss of contrast.

We first introduce some convenient notions. Let A be an $n \times b$ Boolean matrix and $\underline{r}$ the i-th row in A. Then the *1-restriction*, (resp. *0-restriction*) matrix of A with respect to the i-th row is the restriction of A to the column where $\underline{r}$ has 1-coordinates (resp. 0-coordinates). Observe that the number of rows in these restrictions equals $n-1$. Their number of columns depends on the weight of $\underline{r}$, however their sum equals b.

This notion can be naturally extended to a collection $\mathcal{C}$ of $n \times b$ Boolean matrices that all have an i-th row of the same weight. Hence in this situation we can also speak of the 0-restriction and 1-restriction of $\mathcal{C}$ with respect to the (fixed) i-th row.

Now suppose that $S = (\mathcal{C}_0, \mathcal{C}_1)$ is a $k(>1)$ out of n scheme with parameters $[b; h, l]$. Let $i \in \{1, 2, ..., n\}$ and let $\underline{r}$ be a vector which occurs as an i-th row in a matrix of $\mathcal{C}_0$ (and hence in $\mathcal{C}_1$). Also let b_0 (resp. b_1) be the number of zeros (resp. ones) in $\underline{r}$. We now decompose S in three steps.

1. $\tilde{\mathcal{C}_0}$ (resp. $\tilde{\mathcal{C}_1}$) consists of all matrices in $\mathcal{C}_0$ (resp. $\mathcal{C}_1$), whose i-th row has the same weight as $\underline{r}$ (cf. condition 3 of a visual sharing scheme).
2. Let $\mathcal{D}_0$ (resp. $\mathcal{D}_1$) be the 0-restriction of $\tilde{\mathcal{C}_0}$ (resp. $\tilde{\mathcal{C}_1}$) with respect to the i-th row.
3. Let $\mathcal{E}_0$ (resp. $\mathcal{E}_1$) be the 1-restriction of $\tilde{\mathcal{C}_1}$ (resp. $\tilde{\mathcal{C}_0}$) with respect to the i-th row (note the interchange of 0 and 1).

Lemma 5.4 *In the above context:*
$(\mathcal{D}_0, \mathcal{D}_1)$ *is a* $k-1$ *out of* $n-1$ *scheme with parameters* $[b_0; h, l]$.

Let z_{max} *be the maximal value of* $z(\underline{v})$ *over all* $\underline{v}$, *where* $\underline{v}$ *is the "or" of any* $k-1$ *rows different from* i *of any matrix in either* $\tilde{\mathcal{C}_0}$ *or* $\tilde{\mathcal{C}_1}$. *The integer* z_{min} *is obtained similarly by replacing "maximal" with "minimal".*

If $z_{max} - z_{min} < h - l$, *then* $(\mathcal{E}_0, \mathcal{E}_1)$ *yields a* $k-1$ *out of* $n-1$ *scheme with parameters* $[b_1; z_{min} - l, z_{max} - h]$. *Moreover, if* S *is uniform then* $z_{max} = z_{min}$ *and the schemes* $(\mathcal{D}_0, \mathcal{D}_1)$ *and* $(\mathcal{E}_0, \mathcal{E}_1)$ *are also uniform.*

Proof: The proof of the first assertion of the lemma is a straightforward verification. In the proof of the second part (about $(\mathcal{E}_0, \mathcal{E}_1)$), the assertions about the blocksize being b_1 and that the third condition of a visual secret sharing scheme is satisfied, follow also with a straightforward verification. Thus only the two separation properties remain to be proven for this part.
To show the first separation property, let E be a $(k-1) \times b_1$ submatrix of an element in $\mathcal{E}_0$. Then E can be obtained by the 1-restriction to the i-th row of a $k \times b$ submatrix C of an element in $\mathcal{C}_1$. Denote the i-th row of C by $\underline{r}$. Also, let $\hat{C}$ denote the $(k-1) \times b$ submatrix of C obtained by removing the i-th row from C. So E is a submatrix of $\hat{C}$ and $\hat{C}$ is a submatrix of C.
Now let z be the number of zero columns in $\hat{C}$, i.e. the "or" $\underline{u}$ of $\hat{C}$ satisfies $z(\underline{u}) = z$. Each such column has either a zero or a one on the corresponding position in $\underline{r}$, giving rise to two types of columns in C. Hence if the numbers of these columns in C are denoted by respectively z_0 and z_1, then $z = z_0 + z_1$.

Observe that the "or" $\underline{v}$ of C satisfies $z(\underline{v}) = z_0$ and that the "or" $\underline{w}$ of E satisfies $z(\underline{w}) = z_1$. Moreover, $z \leq z_{max}$ by construction and $z_0 \geq h$ by definition. Hence, $z_1 \leq z_{max} - h$.
In a similar fashion one proves that the "or" $\underline{w}$ of E in $\mathcal{E}_1$ satisfies $z(\underline{w}) \geq z_{min} - l$. As $z_{min} - l > z_{max} - h$ by assumption, this concludes the proof that $(\mathcal{E}_0, \mathcal{E}_1)$ is a secret sharing scheme.

Let us now turn to the last statement of the lemma. That $z_{max} = z_{min}$ if S is uniform follows directly. The verification of the uniformity of $(\mathcal{D}_0, \mathcal{D}_1)$ is once again straightforward. To verify that $(\mathcal{E}_0, \mathcal{E}_1)$ is uniform, let $s < k$ and let E be an $s \times b_1$ submatrix in $\mathcal{E}_0$ or $\mathcal{E}_1$. Then E can be obtained by the 1-restriction of an $(s+1) \times b_1$ submatrix C of an element in $\mathcal{C}_0$ or $\mathcal{C}_1$ to the i-th row $\underline{r}$. Also, let $\hat{C}$ denote the $s \times b$ submatrix of C obtained by removing the i-th row from C. So E is a submatrix of $\hat{C}$ and $\hat{C}$ is a submatrix of C.
Now let z be the number of zero columns in $\hat{C}$, i.e. the "or" $\underline{u}$ of $\hat{C}$ satisfies $z(\underline{u}) = z$. Each such column has either a zero or a one on the corresponding position in $\underline{r}$, giving rise to two types of columns in C. Hence, if the numbers of these columns in C are denoted by respectively z_0 and z_1, then $z = z_0 + z_1$.
Observe that the "or" $\underline{v}$ of C satisfies $z(\underline{v}) = z_0$ and that the "or" $\underline{w}$ of D satisfies $z(\underline{w}) = z_1$. Moreover, by uniformity, z and z_0 only depend on s, hence so does z_1. $\square$

We remark that there exist examples of k out of n schemes (even generated ones) in which $(\mathcal{E}_0, \mathcal{E}_1)$, is *not* a visual secret sharing scheme (i.e. does not satisfy the first two conditions of a visual secret sharing scheme).
As an illustration of the above technique, let $(\mathcal{C}_0, \mathcal{C}_1)$ be the following [7;1,0] 3 out of 3 visual sharing scheme, where $\mathcal{C}_0$ and $\mathcal{C}_1$ are respectively generated by:

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

When restricting this scheme to the third row, we have $z_{min} = z_{max} = 1$. Then, the [3;1,0] 2 out of 2 scheme $(\mathcal{D}_0, \mathcal{D}_1)$ and the [4;1,0] 2 out of 2 scheme $(\mathcal{E}_0, \mathcal{E}_1)$ are generated by

$$\begin{pmatrix} 0 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix} ; \quad \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}$$

respectively by

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

Proof of Theorem ??: As taking k transparencies of a k out of n scheme yields a k out of k scheme, it suffices to prove the theorem for k out of k schemes. To this end, we will use induction to k. Observe that the result for $k = 1$ is evident. Now assume the validity of of Theorem **??** for all $k-1$ out of $k-1$ schemes.

As an intermediate result we shall prove the result for schemes generated by two Boolean $k \times b$ matrices A_0, A_1 with parameters $[b; h, l]$. Note that - in the context of Lemma **??** - for any row index i (say $i = 1$) we have $z = z_{max} = z_{min}$. Hence taking the 0-restrictions and 1-restrictions to the first row, yields two $k-1$ out of $k-1$ schemes with respective parameters $[b_0; h, l]$ and $[b_1; z-l, z-h]$. By induction $b_0 \geq (h-l)2^{k-2}$ and $b_1 \geq (z-l-(z-h))2^{k-2} = (h-l)2^{k-2}$. Hence $b = b_0 + b_1 \geq (h-l)2^{k-1}$, as desired.

For a proof for general k out of k schemes $(\mathcal{C}_0, \mathcal{C}_1)$ we will use the following nice trick from [?]. Let $r = |\mathcal{C}_0| = |\mathcal{C}_1|$ and form the Boolean $n \times (b \cdot r)$ matrices A_0 (resp. A_1) by concatenating all matrices in $\mathcal{C}_0$ (resp. $\mathcal{C}_1$). Then A_0 and A_1 generate a k out of k scheme with parameters $[r \cdot b; r \cdot h, r \cdot l]$. Hence by the intermediate result $r \cdot b \geq r(h-l)2^{k-1}$, or $b \geq (h-l)2^{k-1}$. $\square$

Proof of Theorem ??: The first part of Theorem **??** follows directly from the last part of Lemma **??**.

For a proof of the second part of the theorem, we will use induction to k, n. Observe that if the integer g satisfies the condition mentioned in the theorem for any k, n, then it also satisfies this condition for $k-1, n-1$. Hence, if the result is valid for $k-1, n-1$ then the validity for k, n follows directly from the first part of Theorem **??**. It therefore suffices to prove the "basis" of the induction, i.e. the situation where $k = 2$. To this end, let $(\mathcal{C}_0, \mathcal{C}_1)$ be a uniform 2 out of n scheme, and let S in $\mathcal{C}_1$.

Let g be minimal with respect to $\binom{g}{\lfloor g/2 \rfloor} \geq n$. Observe that the n rows of S must be (pairwise) different. Hence if the weight of any row (transparency) is denoted by h, then b must satisfy $\binom{b}{h} \geq n$ (consider the rows as subsets of $\{1, \ldots k\}$). As the last left hand side is less or equal to $\binom{b}{\lfloor b/2 \rfloor}$ the (minimal) number g will be less than b, proving the result for $k = 2$. $\square$

Proof of Theorem ??: For a proof of Theorem **??** we will use induction to k. Observe that the result for $k = 1$ is evident. Now assume the validity of Theorem **??** for all (uniform) $k-1$ out of n schemes. Let $S = (\mathcal{C}_0, \mathcal{C}_1)$ be a k out of n scheme and let A_0 (resp. A_1) be an $s \times b$ submatrix ($s < k$) of an element C_0 in $\mathcal{C}_0$ (resp. C_1 in $\mathcal{C}_1$). If $s = 1$ then A_0 and A_1 are evidently systematic, hence we may assume that $s \geq 2$.
As an intermediate result we shall show that A_0 and A_1 are systematic if C_0 and C_1 have a common row number i. Indeed, by decomposing S to the i-th row into $k-1$ out of $n-1$ symmetric schemes (Lemma **??**), the matrix A_0 (resp. A_1) decomposes into two $\dot{A}_0$ and $\ddot{A}_0$ (resp. $\dot{A}_1$ and $\ddot{A}_1$). By the induction hypothesis both $\dot{A}_0$, $\dot{A}_1$ and $\ddot{A}_0$, $\ddot{A}_1$ are systematic. Now as the i-th row of A_0 equals the i-th row of A_1 modulo a permutation of b elements (they have the same weight), this means that A_0 and A_1 are also systematic.
The general case follows from the intermediate result by considering two chains $A_{0,1}, A_{0,2}, \ldots, A_{0,t}$ and $A_{1,1}, A_{1,2} \ldots, A_{1,t}$ of $s \times b$ submatrices of C_0 and C_1 respectively with $A_{0,0} = A_0$ and $A_{1,t} = A_1$ such that each $A_{0,j}, A_{1,j}$ and $A_{0,j+1}, A_{0,j}$ and $A_{0,j}, A_{1,j+1}$ have a common row. □

With respect to Theorem **??**: one can find k out of n schemes $(\mathcal{C}_0, \mathcal{C}_1)$ in which *no* selection of matrices in $\mathcal{C}_0$ and $\mathcal{C}_1$ generates a k out of n (sub-)-scheme. We next give a bound on the blocklength of high-contrast visual secret sharing schemes, i.e. schemes of type $[b; h, 0]$.

Theorem 5.5 *For any k out of n scheme with parameters $[b; h, 0]$ we have $b \geq h \cdot \binom{n}{k-1}$.*

Proof: Consider such a scheme and let C be any matrix from the accompanying collection of Boolean matrices $\mathcal{C}_1$. It follows from the first and third condition of a visual secret sharing scheme that each submatrix of C consisting of $k-1$ rows of C has at least h zero columns. Moreover, it follows from $l = 0$ that C has no columns with more than $k-1$ zeros. Hence the blocklength b must be as least as big as the number of h times the number of $(k-1)$-subsets of $\{1, ..., n\}$, i.e. $h \cdot \binom{n}{k-1}$

□

For fixed k and large n, the expression $\binom{n}{k-1}$ is approximately equal to $n^{k-1}/(k-1)!$. Hence, the previous result at least indicates that the blocklengths of the high-contrast k out of n schemes constructed in Sections **??** and **??** are fairly optimal.

It seems like a natural question whether interchanging zeros and ones in any k out of n scheme yields another (the "dual") k out of n scheme. Alas, one can construct 2 out of 2 schemes whose "dual" is not a 2 out of 2 scheme. To this end, consider the $[4; 2, 1; 4!]$ 2 out of 2 schemes $(\mathcal{C}_0^1, \mathcal{C}_1^1)$ and $(\mathcal{C}_0^2, \mathcal{C}_1^2)$ respectively generated by

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

and

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

Now let $(\mathcal{C}_0, \mathcal{C}_1)$ be the "union" of these schemes, i.e. $\mathcal{C}_0 = \mathcal{C}_0^1 \cup \mathcal{C}_0^2$ and $\mathcal{C}_1 = \mathcal{C}_1^1 \cup \mathcal{C}_1^2$, then this yields a $[4; 2, 1; 2 \cdot 4!]$ 2 out of 2 scheme. However, if $(\mathcal{C}_0^*, \mathcal{C}_1^*)$ denotes the "dual" of this scheme, then

$$\begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \end{pmatrix} \in \mathcal{C}_0^* \quad ; \quad \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \end{pmatrix} \in \mathcal{C}_1^*.$$

Hence, $(\mathcal{C}_0^*, \mathcal{C}_1^*)$ can never yield a 2 out of 2 scheme. The following result, however, settles the above question for uniform schemes.

Theorem 5.6 *Let $S = (\mathcal{C}_0, \mathcal{C}_1)$ be a uniform k out of n scheme and let $\mathcal{F}$ (resp. $\mathcal{G}$) be constructed from $\mathcal{C}_0$ (resp. $\mathcal{C}_1$) by interchanging zero and one. Then, ($\mathcal{F}$, $\mathcal{G}$) yields an uniform k out of n scheme for n even, and ($\mathcal{G}$, $\mathcal{F}$) yields a uniform k out of n scheme for n odd.*

For the proof of this theorem we need the following lemma.

Lemma 5.7 *Let $S = (\mathcal{C}_0, \mathcal{C}_1)$ be a uniform k out of n scheme with parameters $[b; h, l]$ and let A be a $k \times b$ submatrix of an element in $\mathcal{C}_0$ or $\mathcal{C}_1$. Also for each $\underline{v}$ in $V_2(k)$ let $e(\underline{v})$ be the number of columns in A equal to v. Then for $\underline{v}_1, \underline{v}_2$ in $V_2(k)$:*

$$e(\underline{v}_1) + e(\underline{v}_2)(-1)^{1+weight(\underline{v}_1 - \underline{v}_2)},$$

is independent of A.

Proof: It suffices to prove the lemma in the case that $weight(\underline{v}_1 - \underline{v}_2) = 1$. The general case can then be shown by an inductive argument. Moreover, without loss of generality we may assume that $\underline{v}_1$ and $\underline{v}_2$ only differ in their first coordinate. Then the remaining $k-1$ elements give rise to an element $\underline{v}$ in $V_2(k-1)$. By removing the first row of A we obtain a $(k-1)\times b$ submatrix A'. Now, $e(\underline{v}_1) + e(\underline{v}_2)$ is precisely the number of columns in A' equal to $\underline{v}$. By Theorem **??** this number only depends on $k-1$, i.e. is independent of A.

□

The previous lemma and its proof can be readily generalized to $s \times b$ submatrices for $s < k$.

Proof of Theorem ??: Let n be odd. Also let $S = (\mathcal{C}_0, \mathcal{C}_1)$ be a uniform k out of n scheme and let A be a $k \times b$ submatrix of an element in $\mathcal{C}_0$ or $\mathcal{C}_1$. By Lemma **??** the number z defined as the number of all-zero vectors plus all-one vectors is independent of A. As the number of all-zero vectors in A is at least h, the number of all-one vectors in A is at most $z - l$. Similarly, if A is a submatrix of an element of a member of $\mathcal{C}_1$, then the number of one vectors in A is at least $z - l$. Hence the interchanging of zeros and ones yields a $[b; z-l, z-h]$ scheme. The proof for n even is similar.

□

We remark that the dual (in the sense of Theorem **??**) of any 1 out of n scheme yields once again such a scheme (trivial). Moreover, by arguing similarly as in the proof of Theorem **??**, one can show that the same is true for any 2 out of 2 scheme generated by two matrices. This explains why the 2 out of 2 counterexample preceding Theorem **??** is not of this type.

6 Coloured k out of n Secret Sharing Schemes

The secret sharing schemes as proposed in [**?**] only deal with secretly sharing black & white images. It seems only natural to develop a method of secretly sharing coloured images (or images with grey-levels). In this section we will (briefly) describe such a method. At the end of this section we will indicate some applications.

A coloured image is seen as an array of pixels, each of which is of *colour* $k_0, k_1, \ldots, k_{c-1}$. Here c is the number of colours and k_i is called the i-th colour. Clearly, we can look upon a tone image with grey-levels $g_0, \ldots, g_{r-1}$

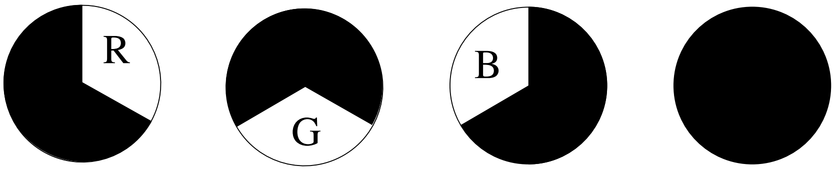

Figure 1: Representation of three colours

as a coloured picture with colours $g_0, \ldots, g_{r-1}$.
Each pixel is divided into b subpixels of colour $0, 1, \ldots, c-1$. These subpixels interrelate which each other in the following way. When subpixels are put on top of each other and held to the light, one sees a "generalized" or, i.e. if all subpixels are of colour i then one sees light of colour i, otherwise one sees no light at all (i.e. black).
These "special" properties of subpixels can be constructed as follows. Consider a circle (of small radius) divided in c equal circle-sectors $0, 1, \ldots, c-1$. Then a subpixel of colour i corresponds with such a circle where sector i has colour k_i and all other sectors are black. Compare Figure 1.
Before giving a formal definition of a colour secret sharing scheme, or colour scheme for short, we introduce some convenient notations. First, we shall always assume that the c colours are elements of a Galois field. Second, we denote black by $\bullet$. Moreover, the sign $\bullet$ is always distinguishable from the c colours, although of course the colour black might be one of the c colours. Next, the generalized "or" of elements in $\{k_0, \ldots, k_{c-1}\}$ equals k_i if all elements are equal to k_i, otherwise it equals $\bullet$. Finally, for a vector $\underline{v}$ with coordinates in $\{k_0, k_1, \ldots, k_{c-1}\} \cup \{\bullet\}$ we let $z_i(\underline{v})$ $(i = 0, \ldots, c-1)$ denote the number of coordinates in $\underline{v}$ equal to colour i.

Definition 6.1 *A k out of n c-colour visual secret sharing system*

$$S = (\mathcal{C}_0; \mathcal{C}_1, \ldots, \mathcal{C}_{c-1}),$$

consists of c collections of $n \times b$ q-ary matrices, in which the c colours are elements of the Galois field $GF(q)$ To share a pixel of colour i, the dealer randomly chooses one of the matrices in $\mathcal{C}_i$. The chosen matrix defines the colour of the b subpixels in each one of the n transparencies. The solution is considered valid if the following three conditions are met for all $0 \leq i \leq c-1$:

1 *For any S in $\mathcal{C}_i$, the generalized "or" $\underline{v}$ of any k of the n rows satisfies $z_i(\underline{v}) \geq h$.*

2 For any S in $\mathcal{C}_i$, the generalized "or" $\underline{v}$ of any k of the n rows satisfies $z_j(\underline{v}) \leq l$, for $j \neq i$.

3 For any $i_1 < i_2 < \ldots < i_s$ in $\{1, 2, \ldots, n\}$ with $s < k$, the collections of $s \times b$ matrices $\mathcal{D}_j$ for $j \in \{0, 1, \ldots, c-1\}$ obtained by restricting each $n \times b$ matrix in $\mathcal{C}_j$ to rows $i_1, i_2, \ldots, i_s$ are indistinguishable in the sense that they contain the same matrices with the same frequencies.

As before, $h > l$ and b is called the blocklength of the scheme. Also, the cardinalities of the $\mathcal{C}_i$, must coincide and are denoted with r. In our construction of colour schemes a particular form of n-arcs of functionals plays a prominent role.

Definition 6.2 *An n-arc of functionals $G, F_1, F_2, \ldots, F_{n-1}$ on $V_m(q)$ is called coinciding (with respect to G) provided for each $m-$subset M of $\{1, 2, \ldots n-1\}$*

$$\left(\bigcap_{i \in M} F_i^{-1}(1)\right) \cap G^{-1}(1) \neq \emptyset.$$

The maximum n for which an coinciding n-arc of functionals in $V_m(q)$ exists will be denoted by $s(q, m)$.

Lemma 6.3 *The following relations hold for $s(q, m)$:*

1. *$s(q, m) \geq q$. If $m-1$ and $q-1$ are not relatively prime then $s(q, m) \geq q+1$.*
2. *$s(q, m) \geq m$. If $q > 2$ or m is odd, then $s(q, m) \geq m+1$.*

Proof: For a proof of the first statement, one can easily verify that the functionals $G, F_1, F_2, \ldots, F_{q-1}$ on $V_m(q)$ corresponding with - any permutation of - the vectors $(1, \omega^1, \ldots, \omega^{m-1})$ with ω in $GF(q)$ form a coinciding q-arc. Now suppose that $k-1$ and $q-1$ are not relatively prime. Let us try - cf. the proof of Theorem **??** - to make this arc one larger by adding the functional corresponding to $(0, \ldots, 0, 1)$. Under the stated condition the mapping $x \rightarrow x^{m-1}$ is not surjective. Hence there exists a (non-zero) $y \in GF(q)$ not occuring as last coordinate in any of the $q+1$ vectors determining the functionals. This implies that all functionals take a non-zero value on $(-y, 0, \ldots, 0, 1)$. Hence,

by dividing the functionals by their value on $(-y, 0, \ldots, 0, 1)$ we obtain a coinciding $(q+1)$-arc.
For a proof of the second statement, one can easily verify that the functionals $G, F_1, F_2, \ldots, F_{m-1}$ on $V_m(q)$ corresponding with - any permutation of - the unit vectors of $V_m(q)$ constitute a coinciding m-arc. If $q > 2$ or m odd, then there exists a non-zero $t \in GF(q)$ such that $\lambda = t + m - 1 \neq 0$. Now expand the last m-arc with the functional corresponding to the vector $\lambda^{-1}(1, \ldots, 1, t)$. Then one clearly obtains an $(m+1)$-arc of functionals which all take the value 1 on $(1, \ldots, 1)$.

$\square$

Theorem 6.4 *Let q be a finite field size such that $q \geq c$ and $s(q,k) \geq n+1$. Then a k out of n colour visual secret sharing scheme with c colours exists with parameters $b = q^{k-1}$, $h = 1$, $l = 0$, $r = q^{k-1}$!*

Proof: Let $\{k_0, \ldots, k_{c-1}\}$ be any c-subset of $GF(q)$. Also choose an coinciding $(n+1)$-arc of functionals $G, F_1, \ldots, F_n$ on $V_k(q)$. Now proceed similar to Construction **??**: for each $j = 0, \ldots c-1$ construct the representation matrices S_j of the functionals F_i, $1 \leq i \leq n$, with respect to a numbering of $G^{-1}(k_j)$.
Now for each $j = 0, \ldots, c-1$ let $\mathcal{C}_j$, be generated by S_j. Observe that for any k-subset K of $\{1, \ldots, n\}$ and $j \in \{0, \ldots, c-1\}$

$$\left(\bigcap_{i \in K} F_i^{-1}(k_j) \right) \cap G^{-1}(k_j) \;\neq\; \emptyset. \tag{8}$$

This implies the first condition of a colour visual secret sharing scheme.
For a proof of the second condition, we argue by contradiction. Suppose that S in $\mathcal{C}_i$, is such that the generalized “or” $\underline{v}$ of any k of the n rows satisfies $z_j(\underline{v}) > 0$ for $j \neq i$. Without loss of generality we may assume that these rows are $1, \ldots k$. This then implies the existence of an $x \in V_k(q)$ with $F_1(x) = \ldots = F_k(x) = k_j$, while $G(x) = k_i \neq k_j$. Let y be any element in the left hand side of Equation **??**, then

$$\frac{y-x}{k_j - k_i} \in \left(\bigcap_{i=1}^{k} F_i^{-1}(0) \right) \cap G^{-1}(1) \;\neq\; \emptyset.$$

This contradicts the dimension k of $V_k(q)$ by Lemma **??**.

Finally, also the security condition of a colour scheme follows from Lemma **??**. $\square$

As an illustration, below are the three matrices belonging to colours 0, 1, 2 respectively, generating a 3 out of 3 scheme with three colours.

$$\begin{pmatrix} 0&0&0&1&1&1&2&2&2\\ 0&1&2&0&1&2&0&1&2\\ 0&1&2&1&2&0&2&0&1 \end{pmatrix} \quad \begin{pmatrix} 0&0&0&1&1&1&2&2&2\\ 0&1&2&0&1&2&0&1&2\\ 2&0&1&0&1&2&1&2&0 \end{pmatrix} \quad \begin{pmatrix} 0&0&0&1&1&1&2&2&2\\ 0&1&2&0&1&2&0&1&2\\ 1&2&0&2&0&1&0&1&2 \end{pmatrix}.$$

Let $c > 2$ be a prime power. Then by taking $q = c$ (cf. Lemma **??**) the above construction produces: a k out of k scheme with c colours for all k; a k out of $c-1$ scheme with c colours for $k < c$; a k out of c scheme with c colours for $k < c$ if $k-1$ and $c-1$ are not relatively prime.

The above proof actually shows a special property of the k out of n colour visual schemes of Theorem **??**: when putting k transparencies on top of each other and held to the light *precisely* one colour (the shared one) is shown. We remark that this property can - at least in principle - be used to securely (and cheaply!) share short messages (e.g. passwords, combinations of safes) represented in the "alphabet" of the used colors. That is, passwords or safe-combination consist of colours (e.g. "blue green red red green blue") instead of alpha-numerical characters. This, for instance, can be applied in situations where no computer-assistance is available (e.g. as a back-up) or desirable.
It is mentioned in [**?**] that in black & white visual cryptography one can send one of the shares by fax. Similarly, in coloured visual cryptography one can send one of the coloured shares by email, and use the (colour) computer screen as one as the shares. One could also print the share on a colour printer. In this fashion one can make use of information technology without having to entrust anybody with the resulting, final secret information. Indeed, the final computation is done by the human visual system.

For example, let us assume that we are using dots of diameter 0.5 cm with 9 colours. A 3 out of 9 visual sharing scheme with 9 colours will use $9^2 = 81$ coloured dots for each colour of the password. As there is room for roughly $20 \cdot 30/0.25 = 2400$ dots on an A4 overhead sheet, we can use such a sheet to construct a 3 out of 9 visual sharing scheme for a $29 \cdot \log 9 \approx 90$ bit safe-combination.

7 Summary

We have introduced a notion of contrast of a visual secret sharing scheme that is more physically justifiable than the one given in [**?**]. Moreover, we have presented two new constructions for k out of n visual secret sharing schemes which are both of maximal contrast, contrary to the two schemes constructed in [**?**]. The blocklengths of our schemes are within the blocklengths of schemes of the same parameters k and n in [**?**].

We have also presented some theoretical results on visual secret sharing schemes. One result is on decomposing one visual secret sharing scheme into two other ones with smaller parameters. Several bounds on the blocklengths of schemes are derived, improving [**?**, Theorem 1]. A further result shows that $(k-1) \times b$ submatrices of k out of n uniform schemes, as introduced in [**?**], are essentially equal to each other (modulo a column permutation). A final result states that the "dual" of a uniform scheme (formed by interchanging one and zero) is once again a uniform scheme.

Finally, we have presented a construction for coloured visual secret sharing schemes, sharing coloured images instead of black & white ones as in [**?**]. We have also indicated some applications for it.

References

[1] B. Arazi, I. Dinstein, O. Kafri, *Intuition, Perception, and Secure Communication*, IEEE Transactions on Systems, Man, and Cybernetics, Vol. 19, pp. 1016-1020, 1989.

[2] F. van der Heijden, *Image based measurement systems*, John Wiley & Sons, Chichester, 1994.

[3] F.J. MacWilliams and N.J.A. Sloane, *The theory of error-correcting codes,* North Holland, Amsterdam etc., 1977.

[4] M. Naor and A.Shamir, Visual cryptography, *Preproceedings of Eurocrypt '94*, pp. 1–11, 1994.

[5] W.K. Pratt, *Digital image processing*, John Wiley & Sons, Chichester, 1991.

[6] W. Rudin, *Functional analysis*, MacGraw-Hill Series in Higher Mathematics, MacGraw-Hill, New York, 1973.

[7] L. Storme and J.A. Thas, M.D.S. codes and arcs in $PG(n, q)$ with q even: an improvement of the bounds of Bruen, Thas and Blokhuis, *Journal of Combinatorial Theory, Series A*, Vol. 62, pp. 139-154, 1993.

[8] J.A. Thas, Projective geometry over a finite field, Chapter 7 in *Handbook of incidence geometry* (ed. F. Buekenhout), Elsevier Science, Amsterdam, 1995.