A polarisation based Visual Crypto System and its Secret Sharing Schemes

P. Tuyls, H. D. L. Hollmann, J. H. v. Lint, L. Tolhuizen

December 19, 2002

Abstract

In this paper, we present a new visual crypto system based on the polarisation of light and investigate the existence and structure of the associated threshold visual secret sharing schemes. It is shown that very efficient (n, n) schemes exist and that $(2, n)$ schemes are equivalent to binary codes. The existence of (k, n) schemes is shown in general by two explicit constructions. Finally, bounds on the physical properties as contrast and resolution are derived.

Key words Light Polarisation, XOR, (MDS) codes, Threshold Visual Secret Sharing Schemes

1 Introduction

The idea of using the human visual system for security purposes was first mentioned in [1]. Independently of [1], the basic Visual Cryptography principles were studied by Naor, Shamir and Pinkas in [6, 7]. The main idea is to split an image into two random shares (printed on transparencies) which separately reveal no information on the original image. The original image can be reconstructed by superimposing the two shares. In [6, 7] it is shown that this system is equivalent to a One Time Pad encryption scheme based on the boolean OR function and therefore unconditionally secure. Moreover, they developped visual authentication schemes which together with a visual encryption scheme lead to a secure system. Later, the associated secret sharing problem and its physical properties as contrast, resolution and colour were extensively studied by Stinson [10] and by Verheul and Van Tilborg [11].

Although the above mentioned visual crypto systems can be made unconditionally secure, they are not satisfactory from a practical point of view. Firstly, because of the One Time Pad property of the scheme, a key can be used only once. Since transparencies are static objects, this implies that a user has to carry a pile of transparencies with him to update the keys. Secondly, the bad physical properties (colour, resolution, contrast) [6, 10, 11] make the system not very well suited for practical purposes.

In this paper we investigate threshold visual secret sharing schemes associated to a new visual encryption scheme. The new visual crypto system uses the polarisation of light and has good colour, contrast and resolution properties. It is based on two well-known physical principles: i) Polarisors only transmit light whose polarisation is aligned with the one of the polarisor (sunglasses) and ii) Liquid Crystal (LC) cells can be used to rotate the polarisation direction of incoming light.

This paper is organised as follows. In Sec. 2 we give a description of the physics behind the polarisation based visual crypto system and show that it can mathematically be described by an XOR. As such, the system has good brightness, resolution, contrast and colour properties and gives rise to a new interesting type of secret sharing problem based on the component wise addition of binary vectors, which is the main topic of this paper. This secret sharing problem is formally defined in Sec. 3. In this section we also give examples of some simple threshold visual secret sharing systems and show the equivalence between $(2, n)$ schemes and binary coding theory. The existence of general threshold visual secret sharing schemes based on polarisation is shown in Sec. 4. Finally, we derive bounds on resolution and contrast properties of these schemes in Sec. 5.

2 The Model

In this section, we explain the physical system and the model for black and white pictures. We also briefly sketch the situation for gray scales and colours but refer the reader for more details to a forthcoming publication.

In order to introduce the model, we briefly explain the physics of an LC display with backlight. An LC display consists mainly of four layers (Fig. 1). The first one has the backlight. The second layer consists of a polarisor, the third one is the LC layer and the fourth one consists again of a polarisor. The backlight emits circularly polarised light. The first polarisation layer projects the polarisation of the incident light on its polarisation direction. Depending on the voltage that is applied to a LC cell, this LC cell will rotate the polarisation of the light that enters it over a certain angle. If the polarisation direction of the light leaving the LC-layer matches that of the final polarisor, light comes out of the display. If on the other hand the polarisation of the light coming out of the LC layer is perpendicular to the polarisation direction of the final polariser, no light comes out. By applying voltages to the LC-cells such that the polarisation direction of the outcoming light makes an angle $\phi \leq \pi/2$ with the polarisation direction of the second polarisor, gray scales can be generated.

In order to build a visual crypto system based on LC displays we proceed as follows (Fig. 2). We have two displays consisting of an LC layer which have a polarisor at one side and no polarisor at the other side. We also assume that the first LC has the backlight and the second one has not. The second display has to be considered as a dedicated *trusted device* that a user is carrying with him. The *shares* of both users are then the two (or more) LC layers on which the dealer writes a certain pattern in terms of the angle of rotation of the various LC cells.

We will start with a model for black and white pixels. We assume that the direction of the first polarisor equals that of the second polarisor and is horizontal. Furthermore, we assume that two voltages can be applied to LC cells V_1 and V_2. When the voltage V_1 is applied, the LC cell will not rotate the polarisation direction of the incoming light, while when the voltage V_2 is applied, the polarisation direction is rotated over an angle of 90 degrees. When an LC consists of N pixels (LC cells), one share will basically consist of N voltages (corresponding to the angle of rotation of the different cells). Table 1 summarizes the physics for one pixel. It follows from Table 1 that when two superimposed LC cells apply the same rotation, this generates a white pixel and when they rotate the polarisation over a different angle this generates a black pixel.

Pol filter 1	$\rightarrow$	$\rightarrow$	$\rightarrow$	$\rightarrow$
LC1	$\parallel$	$\parallel$	$\circlearrowleft$	$\circlearrowleft$
LC2	$\parallel$	$\circlearrowleft$	$\parallel$	$\circlearrowleft$
Pol filter 2	$\rightarrow$	$\rightarrow$	$\rightarrow$	$\rightarrow$
Color	white	black	black	white

Table 1: This table summarizes the physics of a polarisation based visual crypto system. The arrows $\rightarrow$ indicate that the polarisor projects the polarisation direction of the incoming light on the horizontal. The symbols $\parallel$ and $\circlearrowleft$ stand for LC cells that do not and do rotate the polarisation direction of the light respectively.

LC1	0	0	1	1
LC2	0	1	0	1
Color	0	1	1	0

Table 2: Mathematical model of Table 1.

If an LC does not rotate the polarisation of the incoming light, then we will denote this by a 0. If on the other hand the polarisation is rotated over 90 degrees by the LC cell, this will be denoted by a 1. This means that the mathematical structure of the system we described is that of binary addition as follows from Table 2. The visual encryption scheme corresponds then to the physical implementation on LC layers of the One Time Pad based on an XOR operation. As LC layers can be driven electronically (as in LCD's), the key can be easily updated (using pseudo random number generators), which leads to a practical updating mechanism.

Finally, we mention that recently another visual crypto system using an XOR process has been introduced in [2]. Their system is based on interferometric techniques and needs a Mach-Zehnder interferometer making the system less practical and more expensive.

3 Threshold Visual Secret Sharing Schemes

3.1 Definitions

In this section, we will construct Threshold Visual Secret Sharing (TVSS) schemes based on the polarisation rotation technique as explained in Sec. 2. We will restrict ourselves to images consisting of black or white pixels. Since images consist of pixels, it suffices to give schemes for sharing a black or white pixel only. In order to share a complete image, the pixel scheme has to be applied as many times as there are pixels in the image.

By a (k, n) TVSS scheme, we mean a scheme in which a secret (the colour: black or white) is divided into n shares which are given to the n users. Any subgroup of k users out of these n, can reconstruct the secret but any subgroup consisting of less than k users does not have any information on the secret.

We introduce the notion of a *share matrix*. A k-share matrix is an $n \times b$ (n: number of users, b: length of the shares) matrix whose rows are the shares that are distributed to the users. Any arbitrary subset of k rows out of the set of n rows generates the secret when the shares

are superimposed. We denote by $\mathcal{C}_0$ the set of $n \times b$ k-share matrices that generate a white pixel. By $\mathcal{C}_1$ we denote the set of k-share matrices that generate a black pixel.

We will follow the definitions of Verheul and Van Tilborg [11] to give rigorous definitions of a visual secret sharing scheme, contrast and resolution. For a vector $\mathbf{v} \in \mathrm{GF}(2)^b$, we denote by $z(\mathbf{v})$ the number of zero entries in the vector $\mathbf{v}$ (note that $z(\mathbf{v}) + w(\mathbf{v}) = b$, where $w(\mathbf{v})$ denotes the Hamming weight of the vector $\mathbf{v}$).

A k out of n TVSS scheme $\mathsf{S} = (\mathcal{C}_0, \mathcal{C}_1)$ consists of two collections of $n \times b$ binary share matrices $\mathcal{C}_0$ and $\mathcal{C}_1$. To share a white (black) pixel, the dealer randomly chooses one of the matrices in $\mathcal{C}_0$ ($\mathcal{C}_1$) and distributes its rows (shares) under the n participants of the system. More precisely,

Definition 1 *Let k, n, b, h, l be positive integers satisfying $1 \leq k \leq n$ and $b \geq h > l$. A $[(k, n); b, h, l]$ TVSS scheme consists of two collections of $n \times b$ boolean matrices $\mathcal{C}_0$ and $\mathcal{C}_1$ such that:*

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

h is called the white level *of the system and l is called the* black level. *The parameter b is called the* block length *and determines the resolution of the scheme.*

For a good scheme one needs that $h > l$. In [11] the contrast c is defined as $c = (h-l)/(h+l)$ which is also the definition that we will take here. Note that $c \in [0, 1]$ and that c is maximal, when $l = 0$. Schemes with $l = 0$ are called *maximal contrast schemes.* In general, one is interested in schemes with b as small as possible but with the contrast c as large as possible.

The following symmetry property follows very easily and is therefore stated without proof.

Proposition 1 *Let $\mathsf{S} = (\mathcal{C}_0, \mathcal{C}_1)$ be a $[(k, n); b, h, l]$ TVSS scheme with k odd and let $\hat{\mathcal{C}}_i$ be obtained from $\mathcal{C}_i$ by replacing zeroes by ones and vice versa. Then, the scheme $\hat{\mathsf{S}} = (\hat{\mathcal{C}}_0, \hat{\mathcal{C}}_1)$ is a $[(k, n); b, b-l, b-h]$ scheme with contrast $\hat{c}$,*

$$\hat{c} = (h - l)/(2b - l - h).$$

It follows that $\hat{c} > c$ whenever $l + h > b$.

■

The following proposition gives a bound on the distance between the different shares and its proof is given in appendix A.

Proposition 2 *Let $\mathsf{S} = (\mathcal{C}_0, \mathcal{C}_1)$ be a $[(k, n); b, h, l]$ TVSS scheme with $k \geq 3$ and let c_1 and c_2 be two rows of a share matrix in $\mathcal{C}_0$ and hence also two rows of a share matrix in $\mathcal{C}_1$. Then,*

$$d(c_1, c_2) \leq \min\{2l, 2(b - h)\},$$

where $d(.,.)$ denotes the Hamming distance.

■

We will denote the set of $n \times b$ boolean matrices ($M^{n\times b}(\mathrm{GF}(2))$) briefly by $M^{n\times b}$.

3.2 n out of n visual secret sharing

In this section, we show that (n, n) TVSS schemes can have maximal contrast ($c = 1$) with minimal block length ($b = 1$). This stands in sharp contrast to the Naor Shamir case [6] where for the simplest non-trivial case ($n = 2$) at least two subpixels ($b = 2$) are needed.

Proposition 3 *Let $\mathcal{C}_0$ and $\mathcal{C}_1$ be two sets of $n \times 1$ matrices defined as follows,*

$$\mathcal{C}_0 = \{s \in (GF(2))^n \mid \bigoplus_{i=1}^{n} s_i = 0\}, \quad \mathcal{C}_1 = \{s \in (GF(2))^n \mid \bigoplus_{i=1}^{n} s_i = 1\}. \tag{1}$$

Then, the scheme $\mathsf{S} = (\mathcal{C}_0, \mathcal{C}_1)$ is a $[(n, n); 1, 1, 0]$ TVSS scheme.

Proof. From the definition of $\mathcal{C}_0$ and $\mathcal{C}_1$, it follows immediately that $b = 1$, $h = 1$ and $l = 0$. Furthermore, one derives easily that $|\mathcal{C}_0| = |\mathcal{C}_1| = 2^{n-1}$. Clearly any restriction of a share matrix $s \in \mathcal{C}_0$ to any $t < n$ rows (shares) can also be obtained as a restriction of a share matrix $\hat{s} \in \mathcal{C}_1$ and vice versa. It follows moreover that those restrictions occur with the same frequencies in $\mathcal{C}_0$ and $\mathcal{C}_1$. Therefore, the conditions of Def. 1 are satisfied.

■

Hence, in this set-up there exist visual encryption schemes with good contrast and resolution properties. This stands in sharp contrast with OR-based visual crypto systems where maximal contrast schemes can only exist if $b > 1$ [11].

3.3 $(2, n)$ TVSS schemes

A general construction for $(2, n)$ TVSS schemes is given by the following theorem. It shows that $(2, n)$ TVSS schemes are equivalent to binary codes. By a (b, n, d) code, we mean a binary code of length b, n words and minimum Hamming distance d.

Theorem 1 *Let b, l be natural numbers with $b > 1$ and $0 \leq l \leq b$. A $[(2, n); b, b, l]$ TVSS scheme exists if and only if there exists a binary $(b, n, b - l)$ code $\mathcal{C}$.*

Proof. The theorem is proved by construction. Let S be a $[(2, n); b, b, l]$ TVSS scheme. Take a share matrix $A_1 \in \mathcal{C}_1$ and define a set $\mathcal{C}$ whose words $c_1, \ldots, c_n$ are given by the rows of A_1. As the sets $\mathcal{C}_0$ and $\mathcal{C}_1$ define a $[(2, n); b, b, l]$ TVSS scheme, the minimal distance between those words is $b - l$. Consequently, $\mathcal{C}$ defines a code of length b, consisting of n words and with minimal distance $d = b - l$.

Conversely, let $\mathcal{C}$ be a (b, n, d) code over GF(2). Define the boolean matrices $A_i \in M^{n\times b}$, $i = 1, \ldots, n$ as matrices whose n rows contain the same codeword c_i and define the boolean matrix $B \in M^{n\times b}$ consisting of n different rows containing the code words c_i, $i = 1, \ldots, n$. Furthermore, define the boolean matrices $\hat{A}_i = \Gamma_n^i(B) \in M^{n\times b}, i = 1, \ldots, n$ where the cyclic shift on n points, Γ_n, is applied to the rows of B. Define the sets $\mathcal{C}_0 = \{A_1, \ldots, A_n\}$ and $\mathcal{C}_1 = \{\hat{A}_1, \ldots, \hat{A}_n\}$. We prove that the secret sharing scheme $\mathsf{S} = (\mathcal{C}_0, \mathcal{C}_1)$ is a $[(2, n); b, b, b-d]$ TVSS scheme.

Without loss of generality, we start from considering the matrices $A_i, \hat{A}_i, i = 1, \ldots, n$. It is clear that the sum of two arbitrary rows of the matrices $A_i, i = 1, \ldots, n$ gives the all zero vector. It follows that $h = b$. As $\mathcal{C}$ has minimum distance d, for any two rows σ^j, σ^k from $\hat{A}_i$ $(i = 1, \ldots, n)$, we have $z(\sigma^j \oplus \sigma^k) \geq b - d$. Equality holds if σ^j and σ^k have Hamming distance d, so $l = b - d$. The contrast c of the scheme S is hence given by,

$$c = \frac{d}{2b - d}.$$

From the construction it follows that $|\mathcal{C}_0| = |\mathcal{C}_1|$ and also that the collections $\mathcal{D}_0$ and $\mathcal{D}_1$ which are obtained by restricting the elements of the collections $\mathcal{C}_0$ and $\mathcal{C}_1$ to an arbitrary row are indistinguishable. Therefore, the scheme $\mathsf{S} = (\mathcal{C}_0, \mathcal{C}_1)$ is a $[(2, n); b, b, b - d]$ TVSS scheme.

■

We note that the construction of Theorem 1 does not allow to construct maximal contrast schemes. The impossibility of such a construction for (k, n) schemes with $1 < k < n$, will be shown in generality in Sec. 5. In fact, since we showed in Theorem 1 that $(2, n)$ TVSS schemes are equivalent to binary codes, bounds for c, h and l can be derived from bounds for (b, n, d) codes. Using the Singleton bound, we obtain the following corollary.

Corollary 1 *The contrast of a $[(2, n); b, b, l]$ TVSS scheme is at most*

$$(b - \log_2 n + 1)/(b + \log_2 n - 1). \tag{2}$$

Proof. The proof follows from the Singleton bound [3, Thm. 5.2.1] and Theorem 1.

■

In the same way, a lower bound for the contrast of a $(2, n)$ TVSS scheme follows from the Gilbert-Varshamov bound [3, Thm. 5.1.7].

4 General k out of n visual secret sharing schemes

In this section, we show two constructions of (k, n) TVSS schemes for all $3 \leq k \leq n - 1$. The first construction is recursive, the second one is a direct construction and based on so-called MDS codes known from algebraic coding theory. We realize that more efficient constructions are possible, but post those as an open problem.

4.1 Construction 1

The first construction that we propose is a recursive construction. We will first describe a $(3, n)$ TVSS scheme, and derive a $(4, n)$ TVSS scheme from it. It will then be clear how more general schemes can be derived.

4.1.1 Introduction

We first emphasize that in all of the following constructions we produce two classes of share matrices consisting of n rows called $\mathcal{C}_0$ and $\mathcal{C}_1$. In each step of the construction we will let the permutation group $\mathcal{S}_n$ act on the n rows of the share matrices in $\mathcal{C}_0$ and $\mathcal{C}_1$. The appropriate permutation group $\mathcal{S}$ will act on the columns of the share matrices in $\mathcal{C}_0$ and $\mathcal{C}_1$.

This ensures the indistinguishability property according to Def. 1 for the sets $\mathcal{C}_0$ and $\mathcal{C}_1$. In all constructions, we assume that this is done without mentioning this.

The idea of the construction is the following. Denote by a_i the weight of the sum of any $1 \leq i \leq k$ rows of a matrix $A \in \mathcal{C}_0$ and similarly we use the notation b_i for the weight any i rows for $B \in \mathcal{C}_1$. The construction will guarantee that $a_i = b_i$ as long as $i < k$ and that $a_k \neq b_k$ as required by the indistinguishability property.

4.1.2 (3,n) TVSS schemes

Let $B \in M^{n\times(2n-2)}$ be a matrix defined as follows,

$$B = (I_n J_{n,n-2}),$$

where I_n stands for the $n \times n$ identity matrix and $J_{n,n-2}$ is the all one matrix with n rows and $n-2$ columns. The matrix $A \in M^{n\times(2n-2)}$ is defined as the complement of B. We build the sets of share matrices $\mathcal{C}_0$ and $\mathcal{C}_1$ by letting the appropriate permutation groups act on the rows and the columns of the matrices A and B respectively, as explained in Sec. 4.1.1.

Proposition 4 *The scheme $\mathsf{S} = (\mathcal{C}_0, \mathcal{C}_1)$ as defined in the previous paragraph is a $[(3, n); 2n-2, n+1, n-3]$ TVSS scheme with contrast $c = 4/(2n-2)$.*

Proof. Let $a_i, b_i, i = 1, \ldots, n$ be as defined in Sec 4.1.1. Then, it follows that

$$a_1 = b_1 = n-1,\ a_2 = b_2. \tag{3}$$

The permutation of the columns applied to the matrices A and B guarantees together with Eqs (3) that the scheme S satisfies the indistinguishability property of Def. 1. Furthermore, it follows immediately, that $h = n+1$ and $l = n-3$ and therefore $c = 4/(2n-2)$.

■

4.1.3 (4,n) TVSS schemes

We present the construction for n even (for n odd, the construction is similar). First, we introduce some more notation. Let $\mathcal{O}_{n,l}$ denote the all-zero matrix consisting of n rows and l columns. We construct a sequence of matrices $A^1, A^2, \ldots$ which will lead to the set $\mathcal{C}_0$ and a sequence of matrices $B^1, B^2, \ldots$ which will lead to the set $\mathcal{C}_1$. Moreover, for all i, the matrices A^i will have the same number of columns as well as the matrices B^i. If these numbers are different we adjoin matrices $\mathcal{O}_{n,l}$ to all members of one of the classes to make the number of columns equal.

Construction 1

1. Define binary matrices B^1 that contain every column of weight two exactly once. It follows from some computations that:

$$b_1 = n-1,\ b_2 = 2n-4,\ b_3 = 3(n-3),\ b_4 = 4(n-4). \tag{4}$$

2. Define binary matrices A^1 that contain every column of weight three exactly once. Then,

$$a_1 = \binom{n-1}{2},\ a_2 = 2\binom{n-2}{2},\ a_3 = 3\binom{n-3}{2} + 1,\ a_4 = 4\binom{n-4}{2} + 4. \tag{5}$$

3. Define $\Delta_i = b_i - a_i$ at each step of the construction.

4. New binary matrices B^2 are defined by taking $\frac{n-2}{2}$ copies of the matrix B^1. At this step, we have

$$\Delta_1 = 0,\ \Delta_2 = n-2,\ \Delta_3 = 3n-10,\ \Delta_4 = 6n-28.$$

5. Define binary matrices B^3 by adjoining the matrix $J_{n,(n-2)/2}$ to the matrices B^2. Define also binary matrices A^2 by adjoining $(n-2)/2$ copies of I_n to the matrices A_1. At this step, one then has

$$\Delta_1 = 0,\ \Delta_2 = 0,\ \Delta_3 = 2n-8,\ \Delta_4 = 4n-24.$$

6. Define binary matrices B^4 by adjoining to the matrices B^3, $(n-4)/2$ copies of the matrices from the set $\mathcal{C}_1$ of the $(3,n)$ schemes as constructed in Sec. 4.1.2. Similarly, define binary matrices A^3 by adjoining $(n-4)/2$ copies of share matrices of the class $\mathcal{C}_0$ of the $(3,n)$ scheme constructed in Sec. 4.1.2 to the matrices A^2. From the construction of the matrices in the $(3,n)$ schemes, it still follows that $\Delta_1 = \Delta_2 = 0$. But for Δ_3 we have

$$\Delta_3 = (2n-8) - 4\frac{n-4}{2} = 0.$$

   On the other hand, this construction clearly has no impact on Δ_4. For $n \neq 6$, we have that $\Delta_4 \neq 0$.

7. Define the sets $\mathcal{C}_0$ and $\mathcal{C}_1$ from the matrices A^2 and B^4 respectively according to the action of the appropriate permutation groups as explained in the Sec. 4.1.1.

Proposition 5 *The scheme* $\mathsf{S} = (\mathcal{C}_0, \mathcal{C}_1)$ *with* $\mathcal{C}_0$ *and* $\mathcal{C}_1$ *as constructed in construction 1 is a* $[(4,n); b, h, l]$ *TVSS scheme for* $n > 6$ *where*

$$b = \frac{n^3 + 3n^2 - 22n + 16}{4},\ \ h = b - 2n^2 + 16n - 40,\ \ l = b - 2n^2 + 12n - 16.$$

Proof. The indistinguishability property follows from the fact that $\Delta_1 = \Delta_2 = \Delta_3 = 0$ and the application of the permutation group on the columns of the share matrices. The values for b, h and l follow from some tedious calculations.

■

4.2 Construction 2

In this section, we assume that $2 < k < n$. In order to construct (k,n) TVSS schemes we make use of MDS codes over GF(q), the finite field with q elements. We recall that an $[n, k, n-k+1]$ MDS code over GF(q) exists if $q+1 \geq n$ as follows from Theorem 9 in Ch. 11 of [4]. Therefore, we choose $q \geq n-1$.

We start by constructing the set $\mathcal{C}_1$. Let A be a $n \times q^k$ matrix over GF(q). The columns of A consist of the q^k words of an $[n, k, n-k+1]$ code $\mathcal{C}$ over GF(q).

Lemma 1 *Denote by A^s the restriction of the matrix A to the first s rows. The columns of the matrix A^k contain each vector of the vector space $GF(q)^k$ exactly once. Moreover, the restriction A^{k-1} contains each vector of $GF(q)^{k-1}$ exactly q times.*

Proof. Since the columns of A belong to a code $\mathcal{C}$ whose words differ in at least $n-k+1$ positions, the columns of a restricted matrix A^k differ in at least one position. Hence, all q^k columns of A^k are distinct and so A^k contains each vector of $\mathrm{GF}(q)^k$ exactly once.

Hence, it also follows that the restriction of A to any $k-1$ rows contains every possible column (elements of $\mathrm{GF}(q)^{k-1}$) exactly q times.

■

Lemma 1 holds for the restriction of A to any k rows, as one sees by inspection of its proof.

We derive a binary matrix $\hat{A} \in M^{n \times q^k}$ from the matrix A by replacing all non-zero entries of A by the element 1.

Lemma 2 *Let $A^{i_1,\ldots,i_k}$ denote the restriction of the matrix A to the rows $i_1,\ldots,i_k$ and denote by $v^{\oplus}_{i_1,\ldots,i_k} \in GF(2)^{q^k}$ the sum of the k rows of the associated binary matrix $\hat{A}^{i_1,\ldots,i_k}$. Then,*

$$z(v^{\oplus}_{i_1,\ldots,i_k}) = \frac{q^k + (2-q)^k}{2}.$$

Proof. Choose k arbitrary rows $i_1,\ldots,i_k$. By construction of the matrix $\hat{A}^{i_1,\ldots,i_k}$, this matrix contains every possible column exactly once, hence the number of columns of weight w equals

$$\binom{k}{w}(q-1)^w.$$

Therefore, the number of zeros in $v^{\oplus}_{i_1,\ldots,i_k}$ equals

$$z(v^{\oplus}_{i_1,\ldots,i_k}) = \sum_{w=0 \,(\mathrm{mod}2)} \binom{k}{w}(q-1)^w = \frac{q^k + (2-q)^k}{2}.$$

■

Since the number $z(v^{\oplus}_{i_1,\ldots,i_k})$ does not depend on the rows $i_1,\ldots,i_k$, we will further denote this number simply by $z(v^{\oplus}_b)$.

Put $A_1 = \hat{A}$ and define the set $\mathcal{C}_1$ as the set of share matrices obtained by letting the permutation group $\mathcal{S}_{q^k}$ act on the columns of the matrix $\hat{A}$.

Next, we describe the construction of the set $\mathcal{C}_0$. Denote by B_0 an $n \times q^{k-1}$ matrix over $\mathrm{GF}(q)$ whose columns are the words of an $[n, k-1, n-k+2]$ (MDS) code over $\mathrm{GF}(q)$ (this code exists since $n \leq q+1$). The matrix B consists of q copies of the matrix B_0 and is hence an $n \times q^k$ matrix over $\mathrm{GF}(q)$.

Lemma 3 *Denote by $B^{i_1,\ldots,i_k}$ the restriction of the matrix B to the rows $i_1,\ldots,i_k$. Then, the columns of the matrix $B^{i_1,\ldots,i_k}$ contain each vector of $GF(q)^k$ either zero or q times. The columns of the matrix $B^{i_1,\ldots,i_{k-1}}$ contain each vector of the space $GF(q)^{k-1}$ exactly q times.*

Proof. Since the columns of the matrix B belong to an $[n, k-1, n-k+2]$ MDS code over $\mathrm{GF}(q)$, the columns of the restricted matrix $B^{i_1,\ldots,i_{k-1}}$ differ in at least one position. Hence, the columns of $B^{i_1,\ldots,i_{k-1}}$ contain all the vectors $\mathrm{GF}(q)^{k-1}$ exactly once.

The fact that the matrix $B^{i_1,\ldots,i_k}$ contains each vector of $\mathrm{GF}(q)^k$ either zero or q times follows then immediately from the construction.

■

We define the binary matrix $\hat{B}$ by replacing in the matrix B each non-zero entry by one. Put $A_0 = \hat{B}$.

Lemma 4 *Let $A_0^{i_1,\ldots,i_k}$ denote the restriction of the matrix A_0 to the rows $i_1,\ldots,i_k$. Then, the number of zeroes in the sum vector $v^{\oplus}_{i_1,\ldots,i_k}$ is given by*

$$z(v^{\oplus}_{i_1,\ldots,i_k}) = z(v_b^{\oplus}) + (q-1)2^{k-1}.$$

Proof. Consider the matrix $B_0^{i_1,\ldots,i_k}$ which is a restriction of the matrix B_0 to the rows $i_1,\ldots,i_k$. The columns of this matrix are the words of an $[k, k-1, 2]$ MDS code over $\mathrm{GF}(q)$. By Theorem 6 in Ch. 11 of [4], it follows that b_w the number of columns of weight w in the matrix $B_0^{i_1,\ldots,i_k}$, is given by

$$\begin{aligned} b_w &= \binom{k}{w}(q-1)\sum_{j=0}^{w-2}(-1)^j\binom{w-1}{j}q^{w-2-j} \\ &= \binom{k}{w}(q-1)\left(\frac{(q-1)^{w-1}-(-1)^{w-1}}{q}\right). \end{aligned} \tag{6}$$

As B consists of q copies of B_0, it follows that in $\hat{B}$ and hence in A_0 every column of weight w occurs qb_w times and so

$$z(v^{\oplus}_{i_1,\ldots,i_k}) = qb_w = z(v_b^{\oplus}) + (q-1)\sum_{w=0 \bmod 2}\binom{k}{w} = z(v_b^{\oplus}) + (q-1)2^{k-1}.$$

■

Again, we remark that the number $z(v^{\oplus}_{i_1,\ldots,i_k})$ does not depend on the rows $i_1,\ldots,i_k$. Therefore, we denote this number by $z(v_w^{\oplus})$.

The set $\mathcal{C}_0$ is then defined by letting the permutation group $\mathcal{S}_{q^k}$ act on the columns of A_0.

Construction of a general (k,n) scheme: construction 2

1. Choose q (power of a prime) with $q \geq n-1$.
2. Define the sets of share matrices $\mathcal{C}_0$ and $\mathcal{C}_1$ as earlier in this section.
3. Define the scheme $\mathsf{S} = (\mathcal{C}_0, \mathcal{C}_1)$.

Theorem 2 *The scheme $\mathsf{S} = (\mathcal{C}_0, \mathcal{C}_1)$ as defined in construction 2, is a $[(k,n); q^k, z(v_w^{\oplus}), z(v_b^{\oplus})]$ TVSS scheme.*

Proof. The fact that $b = q^k$ follows from the definition of construction 2. The equalities $h = z(v_w^{\oplus})$ and $l = z(v_b^{\oplus})$ follow from lemmas 4 and 2. The indistinguishability property follows from the observation that the matrices $A_0^{i_1,\ldots,i_t}$ and $A_1^{i_1,\ldots,i_t}$, with $t < k$, obtained by restricting the matrices A_0 and A_1 to t arbitrary rows, are constructed in the same way.

They are obtained from the indistinguishable matrices $B^{i_1,\cdots,i_t}$ and $A^{i_1,\cdots,i_t}$ as follows from lemmas 3 and 1.

■

Finally, note that the contrast c of $[(k,n);b,h,l]$ schemes in construction 2 is given by

$$c = ((q-1)2^{k-1})/(q^k + (-1)^k(q-2)^k + (q-1)2^{k-1}).$$

5 Bounds on the parameters b, h and l

Lemma 5 *Let k be an even integer. Let B be a binary matrix with n rows such that the sum (XOR) of any k rows from B differs from $\mathbf{0}$. Then B has at least $n-k+2$ distinct rows.*

Proof. By induction on k. The result is obvious for $k=2$. Now assume that $k \geq 4$, and that B has two equal rows (otherwise we are done). By removing these two rows from B, we obtain a matrix B^* with $n-2$ rows. The sum of any $k-2$ rows from B^* differs from $\mathbf{0}$ as otherwise these $k-2$ rows and the two removed rows would add up to $\mathbf{0}$. The induction hypothesis implies that B^* (so surely B) has at least $(n-2)-(k-2)+2 = n-k+2$ distinct rows.

■

Proposition 6 *Let k be even, $k \geq 4$ and let $\mathcal{S} = (\mathcal{C}_0, \mathcal{C}_1)$ be a $[(k,n);b,h,l]$ TVSS scheme. Then we have that*

$$n-k+1 \leq \sum_{i=0}^{\min(l,2(b-h))} \binom{b}{i}.$$

Proof. Let B be a share matrix in $\mathcal{C}_1$. As $l \neq b$, no k rows of B add to the all-zero word. Lemma 5 implies that B has at least $n-k+2$ distinct rows. As all rows from B have Hamming distance at most $2(b-h)$ to its top row (see Proposition 2),

$$n-k+2 \leq \sum_{i=0}^{2(b-h)} \binom{b}{i}.$$

Now, we assume without loss of generality that the top $n-k+1$ rows of B are distinct. Let $\mathbf{c}$ be the sum of the $k-1$ bottom rows of B. For $1 \leq i \leq n-k+1$, the sum of $\mathbf{c}$ and the i-th row of B contains at most l ones; that is to say, the i-th row of B has Hamming distance at most l to the complement of $\mathbf{c}$. As the $n-k+1$ top rows of B are distinct, $n-k+1$ is at most the number of vectors at distance at most l from the complement of $\mathbf{c}$, so

$$n-k+1 \leq \sum_{i=0}^{l} \binom{b}{i}.$$

■

We are investigating the structure of the possible schemes in this set-up. In particular, we prove that maximal contrast schemes ($l=0$) do not exist.

Proposition 7 *$[(k,n);b,h,0]$ TVSS schemes with $1<k<n$ do not exist. Furthermore, $[(k,n);b,b,l]$ TVSS schemes with $2<k<n$ do not exist either.*

Proof. For $k=2$ the first statement has already been proven in Corollary 1. Therefore, we assume w.l.o.g. that $k\geq 3$. Let $\mathsf{S}=(\mathcal{C}_0,\mathcal{C}_1)$ be a $[(k,n);b,h,0]$ TVSS scheme and let B be a share matrix in $\mathcal{C}_1$. Denote by σ^1,σ^2 two arbitrary rows in B. Since $n-2\geq k-1$, there are still $k-1$ rows left in the share matrix B. We denote these rows by $\sigma^3,\ldots,\sigma^{k+1}$. Since S is a threshold scheme with $l=0$, the XOR of $\sigma^1,\sigma^3,\sigma^4,\ldots,\sigma^{k+1}$ is the all-one vector, as is the XOR of $\sigma^2,\sigma^3,\sigma^4,\ldots,\sigma^{k+1}$. It follows that $\sigma^1=\sigma^2$, so all rows of $B\in\mathcal{C}_1$ are equal.

Next, let $A\in\mathcal{C}_0$ and consider row i and j of A. As $k\geq 3$, the indistinguishability property of Def. 1 implies that there is a $B\in\mathcal{C}_1$ that agrees with A in these rows. As all rows of B are equal, the i-th and j-th row of A are equal. Since i and j are arbitrary, all rows of A are equal, so A equals B, a contradiction.

The second statement follows from an analogous reasoning.

■

Note that Proposition 7 implies that $[(k,n);1,h,l]$ TVSS schemes do not exist for $1<k<n$. Moreover, it is note worthy that $[(2,n);b,b,l]$ TVSS schemes with $l>0$ exist while $[(2,n);b,h,0]$ TVSS schemes do not exist.

It follows from Def. 1 that one is interested in schemes with small l. The following Proposition shows that for even k, l/b can not be arbitrarily small.

Proposition 8 *Let $\mathsf{S}=(\mathcal{C}_0,\mathcal{C}_1)$ be a $[(k,n);b,h,l]$ TVSS scheme with $1<k<n$ and k even. Then, the white level l satisfies the following inequality,*

$$l\geq\frac{b}{k+1}.$$

Proof. Choose a share matrix $B\in\mathcal{C}_1$. Let $\hat{B}$ be a set of $k+1$ arbitrarily chosen rows in B. Let α_1 denote the number of positions in which the shares of $\hat{B}$ all have the same coordinate. Let α_2 denote the number of positions in which not all of the $k+1$ shares of $\hat{B}$ have the same coordinate. Note that $\alpha_1+\alpha_2=b$. Consider the $k+1$ subsets of k elements of $\hat{B}$ and compute the sum vector of each of the subsets of k elements. The total number of zeroes z in the concatenation of these sum vectors satisfies

$$(k+1)l\geq z\geq(k+1)\alpha_1+\alpha_2\geq\alpha_1+\alpha_2=b.$$

■

It follows from Proposition 8 that for even $k>3$ the contrast c of $[(k,n);b,h,l]$ TVSS schemes is bounded by

$$c\leq((k+1)(b-1)-b)/((k+1)(b-1)+b). \tag{7}$$

For odd k on the other hand, l/b can be arbitrarily small. Indeed, in Construction 2 of Sec. 4.2, the white level l satisfies (for fixed odd k)

$$\frac{l}{b}=\frac{1}{2}(1-(1-\frac{2}{q})^k)\stackrel{\text{large } q}{\longrightarrow}\frac{k}{q}+O(q^{-2}),$$

which becomes arbitrarily small with increasing q. Together with Proposition 1, these results indicate that (k, n) schemes with k odd are fundamentally different from (k, n) schemes with k even.
Finally, we mention that if $k = 2$, h can be as large as b (see Sec. 3.3). For larger k, Construction 2 (combined with Proposition 1, if k is odd) yields (k, n) schemes with h/b arbitrarily close to 1.

References

[1] B. Arazi, I. Dinstein, O. Kafri, *Intuition, perception and secure communication*, IEEE Transactions on Systems, Man and Cybernetics, Vol. 19 (1989), 1016-120.

[2] S-S. Lee, J-C. Na, S-W. Sohn, C. Park, D-H. S. and S-J. Kim, *Visual Cryptography based on an Interferometric Encryption Technique*, ETRI Journal, Vol. 24, 5, 2002, 373-380.

[3] J.H. van Lint, *Introduction to Coding Theory*, Springer-Verlag, 1998.

[4] F.J. MacWilliams and N.J.A. Sloane, *The theory of Error-Correcting Codes*, Amsterdam-New York-Oxford, North Holland, 1977.

[5] A. Menezes, P. van Oorschot, S. Vanstone, *Handbook of Applied Cryptography*, 1996.

[6] M. Naor, A. Shamir, *Visual Cryptography*, Eurocrypt 94, Springer-Verlag LNCS Vol. 950, 1-12.

[7] M. Naor, B. Pinkas, *Visual Authentication and Identification*, Crypto 97.

[8] V. Rijmen, B. Preneel, *Efficient colour visual encryption or 'shared colors of Benetton'*, Presented at the rump session of Eurocrypt '96. Also available at `http://d-n-mj--.jollibee-ood.restat.kuleuven.ac.be/ rijmen/vc/` .

[9] G. Simmons, *A survey of information authentication*, in Contemporary Cryptography - The science of information integrity, IEEE Press, 379-419.

[10] D.R. Stinson, *An introduction to visual cryptography*, presented at Public Key solutions '97. Available at `http://e-h---u--at`

Proof. Let B be a share matrix in $\mathcal{C}_1$ containing the rows c_1, c_2 and let c denote the (XOR) sum of $k-1$ other rows. Then, we have

$$\begin{aligned} d(c_1, 1 \oplus c) &= z(c \oplus c_1) \leq l, \\ d(c_2, 1 \oplus c) &= z(c \oplus c_2) \leq l. \end{aligned}$$

From the triangle inequality, it then follows that

$$d(c_1, c_2) \leq 2l. \tag{8}$$

An analogous reasoning on a share matrix $A \in \mathcal{C}_0$ containing the shares c_1, c_2 and $\hat{c}$, then gives

$$d(c_1, c_2) \leq 2(b-h). \tag{9}$$

Adding Eq. 8 and Eq. 9 then leads also to the following bound

$$d(c_1, c_2) \leq b - h + l.$$

■

B Figures

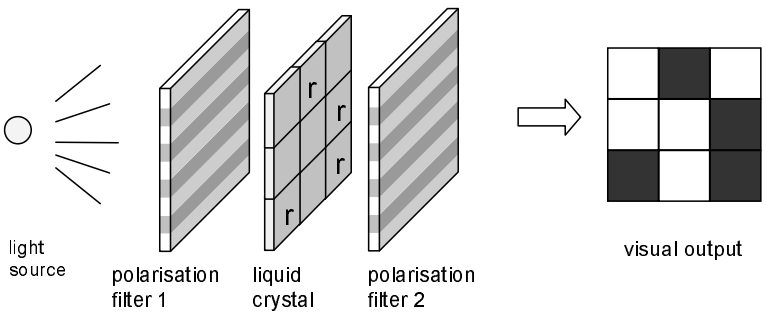

Figure 1: *Structure and principle of an LC Display. The symbol* r *in a cell means that this LC cell rotates the polarisation of the incoming light.*

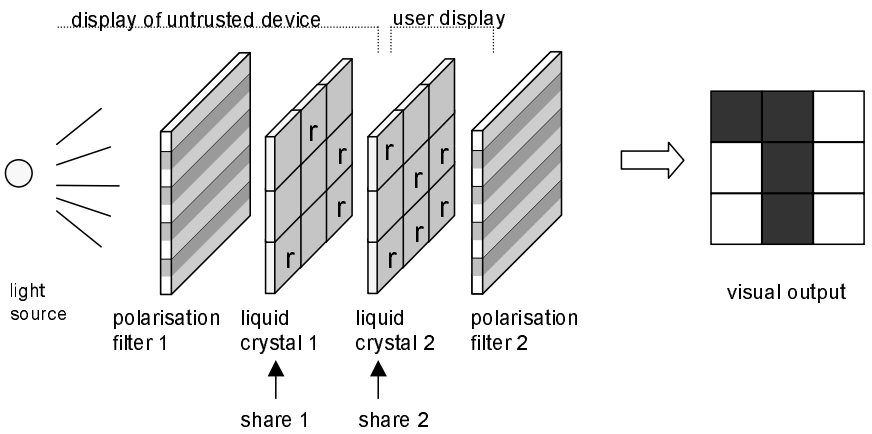

Figure 2: *Visual crypto system by superimposing two LC layers. The symbol* r *in a cell means that this LC cell rotates the polarisation of the incoming light.*