NATIONAL KAPODISTRIAN UNIVERSITY OF ATHENS

Mathematics Department

Graduate Program in Logic, Algorithms and Computation

Visual Cryptography and Applications

Evie V. Economopoulou

Supervised by Aggelos Kiayias

M.Sc. Thesis

July 2015

Acknowledgments

I would like to express my great appreciation for the help, trust, and encouragement my supervisor, Aggelos Kiayias, showed me. Additionally, I would like to thank the members of the supervisory committee: Aris Pagourtzis who introduced me to the fascinating world of Cryptography and Evaggelos Raptis for his valuable guidance. Last but not least, I owe a special thanks to my sister Katerina Economopoulou and my friend Effie Stavraki for always being there for me.

To my late father

Chapter 1

Introduction

1.1 The Basic Model

Visual Cryptography is an encryption technique based on the secret sharing problem. In this case, visual information is shared, i.e., the message to be encrypted can be a black and white image, grey scale or a coloured one, printed text, etc. The encryption of the secret is done in such a way, that its decryption is very simple since there is no need for any mathematical calculations: it is done automatically by the human eye. What is more, the secret is completely safe, since it cannot be revealed by any unauthorized opponent, even one with infinite computational power.

B. Arazi, I. Dinstein and O. Kafri, in [1] were the first that mentioned the potentiality of a cipher algorithm which takes advantage of the visual human ability.

The first concrete definition of k out of n visual secret sharing schemes was stated in [2] by Moni Naor and Adi Shamir along with specific applications and extensions of the initial model.

Two more constructions and properties of k out of n visual secret sharing schemes, such as bounds on their parameters, are presented in[3] by Eric R. Verheul and Henk C. A. Van Tilborg. Additionally, an introduction to the notion of coloured visual secret sharing schemes is introduced and a general construction is given.

The definitions given and all the constructions and properties mentioned in [2] and [3] will be described in detail in the following Sections.

The basic model consists of two images of the same size that are composed of random looking black and white small squares. One can be considered as the ciphertext and the other as the key. When the key-image is placed on top of the ciphertext image, a secret message or picture is revealed. However, by inspecting each of the initial images separately, even an adversary with infinite computational resources cannot recover the encrypted message or any part of it. Both the ciphertext image and the key image are called *transparencies*. The reason is that each encrypted image must be printed on a transparent piece of paper for the decryption to succeed. Figure 1.1 from [22] depicts an example of the above-described model.

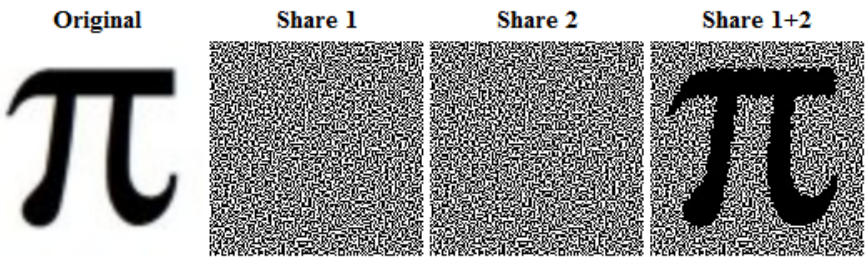


Figure 1.1: An example of a visual secret sharing scheme

One could say that it is a visual one-time pad scheme since each cypher-

text image can be decrypted only by a different key-image. What is more, its use is very simple since no mathematical calculations or cryptography skills are needed to disclose the secret message.

1.2 Visual Secret Sharing Schemes

Definition 1.2.1: *A k out of n visual secret sharing scheme* is an extension of the basic model: instead of 2, n different transparencies are produced. Any k of them reveal the secret message while fewer than k of them pass absolutely no information about it. As a result, the initial model can be considered as a 2 out of 2 visual secret sharing scheme.

As already mentioned, the basic model describes the share of a black and white image. The technique is based on the division of each pixel into b black and white subpixels which form a square or rectangle. In each transparency, or else *share*, each pixel is depicted in a different way.

When k transparencies are stacked together and the subpixels are aligned, the visual result for each subpixel is the boolean "or" of the k different versions of it: if all the k versions are white, then the result is white while in any other case the result is black. Additionally, the human eye perceives a pixel as white (respectively black) if there is a sufficient number of white (respectively black) subpixels. Hence, the contrast between the two colours must be as large as possible.

1.3 Mathematical Description of the Model

The mathematical description of a k out of n visual secret sharing scheme is described as follows: each pixel is divided into b subpixels. Since white subpixels do not block light, they are denoted by 0 while black subpixels are denoted by 1.

Each pixel is described by an $n \times b$ matrix A as shown in Figure 1.2. Each row of the matrix represents the different versions of the pixel in the n corresponding transparencies. Since each pixel is divided into b subpixels, the matrix A consists of b columns. If the j-th subpixel in the i-th transparency is white (respectively black), then $A[ij] = 0$ (respectively $Aij] = 1$).

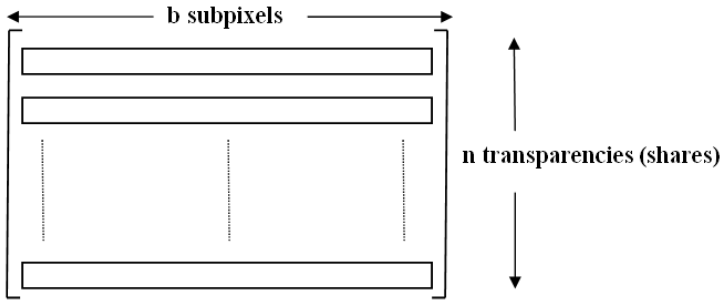


Figure 1.2: An $n \times b$ matrix which represents a visual secret sharing scheme

Definition 1.3.1: The parameter $b \in \mathbb{N}$ is called the *blocklength* of the scheme S and since it can be considered as the pixel expansion, we would like it to be as small as possible. In addition, b needs to be in the form of m^2 ($m \in \mathbb{N}$) if we want to preserve the aspect ratio of the original image.

When transparencies $i_1, i_2, \ldots, i_k$ from a matrix A are stacked together, the resulting pixel also consists of b subpixels. Each one of them is the

outcome of the boolean "or" of the k corresponding subpixels in $i_1, i_2, \ldots, i_k$ rows, as shown in Figure 1.3:

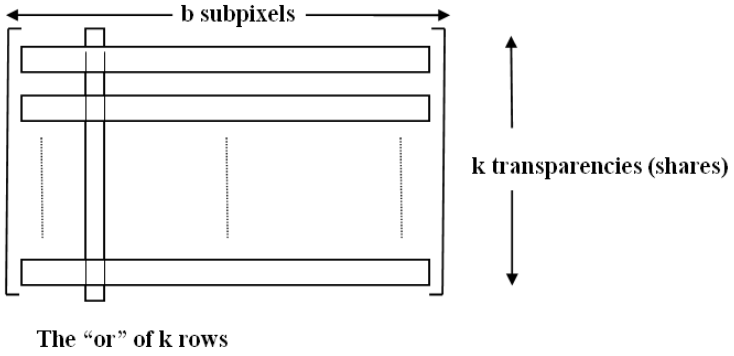


Figure 1.3: The boolean "or" of r transparencies

Let $\vec{v}$ be the boolean vector of length b that represents the "or" of k transparencies of a pixel. As already mentioned, whether the human eye interprets it as black or white depends on the number of black subpixels that it consists of, namely, of its Hamming weight (the one coordinates of vector $\vec{v}$), denoted $w(\vec{v})$. If $z(\vec{v})$ denotes the number of white subpixels, hence, the zero coordinates of vector $\vec{v}$, note that $b = z(\vec{v}) + w(\vec{v})$.

From the description above it is obvious that in this technique a white pixel does not consist of white subpixels only, and the same holds for a black pixel, too: some white subpixels may also be included. Hence, since a pixel is not purely white or black, the contrast between them is of great significance.

In [2], a threshold d ($1 \leq d \leq b$) and relative difference $a > 0$ are used to distinguish between the colours: a pixel is perceived by the visual system of the users as black if $w(\vec{v}) \geq d$ and as white if $w(\vec{v}) < d - a \cdot b$. Since the relative difference a is a way of expressing contrast, it must be as large as possible.

In [3], two non-negative numbers, h and l, are used to make the distinction between black and white. A pixel is perceived by the human eye as white if at least h subpixels are white, i.e., $z(\vec{v}) \geq h$. Similarly, a pixel is interpreted as black if at most l of its subpixels are white, i.e., $z(\vec{v}) \leq l$.

Two equivalent definitions of a visual secret sharing scheme follow, from [2] and [3] respectively:

Definition 1.3.2: *A k out of n visual secret sharing scheme* $S = (\mathcal{C}_0, \mathcal{C}_1)$ used to encrypt a black and white picture consists of two collections of $n \times b$ Boolean matrices $\mathcal{C}_0$ and $\mathcal{C}_1$. Collection $\mathcal{C}_0$ corresponds to white colour whereas collection $\mathcal{C}_1$ to black. The matrices that are contained in each collection $\mathcal{C}_0$ and $\mathcal{C}_1$ are the different versions of representing a white or a black pixel respectively. More specifically, the n rows of each matrix correspond to the n transparencies to be shared and the b elements of each row define the colour of the corresponding subpixels. The scheme must comply with the following three conditions:

According to [2]:

1. For any matrix A in the collection $\mathcal{C}_0$, the "or" $\vec{v}_0$ of any k out of its n rows must satisfy

$$w(\vec{v}_0) \leq d - a \cdot b \tag{1.1}$$

2. For any matrix A in the collection $\mathcal{C}_1$, the "or" $\vec{v}_1$ of any k out of its n rows must satisfy

$$w(\vec{v_1}) \geq d \tag{1.2}$$

According to [3]:

1. For any matrix A in $\mathcal{C}_0$ collection, the "or" $\vec{v}_0$ of any k out of its n rows must satisfy

$$z(\vec{v}_0) \geq h \tag{1.3}$$

2. For any matrix A in $\mathcal{C}_1$ collection, the "or" $\vec{v}_1$ of any k out of its n rows must satisfy

$$z(\vec{v}_1) \leq l \tag{1.4}$$

The parameters h and l, where $h, l \in \mathbb{N}$, must comply the following condition: $0 \leq l < h < b$: the condition $l = 0$ may hold, since there is a possibility that no white subpixel exists in a black pixel. The condition $l < h$ must hold since the contrast of the scheme is defined on this difference. Last but not least, $h < b$ holds because if $h = b$ the security of the scheme would be compromised.

The third requirement is the same in both papers:

3. The two collections $\mathcal{C}_0'$ and $\mathcal{C}_1'$ attained by limiting all the $n \times b$ matrices of $\mathcal{C}_0$ and $\mathcal{C}_1$ respectively to $s < k$ rows, $i_1, i_2, \ldots, i_s$, are identical, namely, the matrices that they contain are the same and appear in the same frequencies.

The first two conditions in [2] and [3] are two sides of the same coin: Naor and Shamir make the distinction between a white and a black pixel by counting the black subpixels whereas Verheul and Van Tilborg count the white ones. What is important about the two first conditions is the contrast between the stacked transparencies that comes from a white and a black pixel as well as the loss of contrast. In [2], the contrast is implicitly defined as $h - l = (b - w(\vec{v}_0)) - (b - w(\vec{v}_1)) = b - w(\vec{v}_0) - b + w(\vec{v}_1) = w(\vec{v}_1) - w(\vec{v}_0) = d - (d - a \cdot b) = d - d + a \cdot b = a \cdot b$, where $w(\vec{v}_0)$ ($w(\vec{v}_1)$ respectively) denotes

the Hamming weight of the "or" $\vec{v}$ of any k out of n rows of a matrix from $\mathcal{C}_0$ collection ($\mathcal{C}_1$ collection respectively) of the scheme S, i.e.,

$$contrast_{SN} = h - l = a \cdot b \tag{1.5}$$

The loss of contrast is defined as

$$contrastloss_{SN} = \frac{h-l}{b} = \frac{a \cdot b}{b} = a \tag{1.6}$$

,

where SN stands for Shamir Naor in equations 1.5 and 1.6.

As stated in [3], these definitions of contrast and loss of contrast are not really suitable. The following example shows in an intuitive way why: let us consider two buildings A and B at night. In the first case there are 100 lightened windows in A and 99 in B. In the second case, there is only one lightened window in A and none in B. In both cases the contrast if measured using formula (1.5) equals one. However, it is clear that the contrast in the first case is much less than in the second one. One can also check references in literature (see [4], p. 272 and [5], p.34). As a result, it is preferable to use the formulae stated in [3]:

$$contrast_{VVT} = \frac{h-l}{h+l} \tag{1.7}$$

is proposed as measure of contrast, and the loss of contrast as

$$contrastloss_{VVT} = \frac{h-l}{b \cdot (h+l)} \tag{1.8}$$

,

where VVT stands for Verheul and Van Tilborg in equations 1.7 and 1.8.

We want contrast to be as large as possible and the loss of contrast as small as possible.

According to the last condition the scheme is completely safe: even an unauthorized opponent with infinite computational power cannot make any deduction about the colour of a pixel when less than k transparencies are stacked.

Hence, the first two conditions define the *contrast of the scheme* and the third one its *security*.

The important parameters of a k out of n visual secret sharing scheme are the following:

- the blocklength of the scheme, denoted b.
- the minimum number of white subpixels in a white pixel, denoted h.
- the maximum number of white subpixels in a black pixel, denoted l.
- the number of matrices each collection $\mathcal{C}_0$ and $\mathcal{C}_1$ contain, denoted r.

We summarize these parameters as $[b; h, l; r]$.

1.4 Some Classifications

Definition 1.4.1: Let $S = (\mathcal{C}_0, \mathcal{C}_1)$ be a k out of n visual secret sharing scheme and $\vec{v}$ denote the "or" of any $s < k$ transparencies from a matrix either from $\mathcal{C}_0$ or $\mathcal{C}_1$. If there is a function f such that $f(s) = w(\vec{v})$ for every matrix, i.e., the Hamming weight of $\vec{v}$ depends only on the number of transparencies that are used and not from the collection that the matrix belongs, then S is called *uniform*.

As one can see, it is preferable to use schemes of high contrast and small blocklength (parameter b). As already mentioned, the two parameters that

define the contrast of a scheme are h and l. Since h and l are both positive numbers and $h > l$, contrast is maximal when $l = 0$, i.e. there are no white subpixels in a black pixel: $\frac{h-l}{h+l} = \frac{h-0}{h+0} = \frac{h}{h} = 1$.

Definition 1.4.2: The schemes of type $[b; h, l = 0]$ are called *maximal contrast* schemes.

Most of the schemes that are described in the following Sections are constructed using the following method: Let A_0 and A_1 be two $n \times b$ boolean matrices. Additionally, let h, l be two non-negative integers such that $h > l$. Then the following conditions must hold:

1. Let $\vec{v}_0$ denote the "or" of any k out of n rows of A_0.

   Then, $z(\vec{v}_0) \geq h$ must be satisfied.

2. Let $\vec{v}_1$ denote the "or" of any k out of n rows of A_1.

   Then, $z(\vec{v}_1) \leq l$ must be satisfied.

3. Let $s < k$ and $i_1 < i_2 < \ldots < i_s$ be any subset of $\{1, 2, \ldots, n\}$. The matrices A_0 and A_1 when restricted to rows $i_1, i_2, \ldots, i_s$ contain the columns, only in a different order. Mathematically, let $A_0 = [a_{ij}]$ and let $\sigma : \{1, \ldots, n\} \mapsto \{1, \ldots, n\}$. Then, $A_1 = \sigma(A_0) = [a_{i\sigma(j)}]$.

Definition 1.4.3: We call a k out of n scheme $S = (\mathcal{C}_0, \mathcal{C}_1)$ *generated by* A_0 *and* A_1 if the matrices contained in the collections $\mathcal{C}_0$ and $\mathcal{C}_1$ are obtained by all the permutations of the columns of A_0 and A_1 respectively. Such a scheme has parameters $[b; h, l; b!]$.

Definition 1.4.4: Let $S = (\mathcal{C}_0, \mathcal{C}_1)$ be a k out of n visual secret sharing scheme generated by matrices A_0 and A_1. We limit A_0 and A_1 to any s rows ($s < k$), namely, $i_1 < i_2 < \ldots < i_s$ and $j_1 < j_2 < \ldots < j_s$ in $\{1, \ldots, n\}$ respectively. If these two submatrices of A_0 and A_1 contain the same columns, but in a different order, we call A_0 and A_1 *systematic*. What is more, the scheme that is generated by them is called a *strong k out of n visual secret sharing scheme*.

Chapter 2

Visual Secret Sharing Schemes for fixed k and n

2.1 A 2 out of 2 Visual Secret Sharing Scheme

The very first scheme that was presented by Naor and Shamir in [2] is a 2 out of 2 visual secret sharing scheme. Although it can be solved by dividing a pixel into two subpixels, the aspect ratio of the image will be distorted. As a result, each pixel is divided into four subpixels to form a 2×2 square. In Figure 2.1 from [2] are depicted the different squares that can be used for the scheme.

As one can see, there are three different types of transparencies, horizontal, vertical and diagonal, each consisting of two squares which are complementary. In order to share a white pixel, two identical squares are chosen, whereas, to share a black one, two complementary squares are used.

The transition from the visual pattern of a pixel (a square consisting of 2×2 subpixels) to a row in a matrix is the following, where "*ul*" denotes the

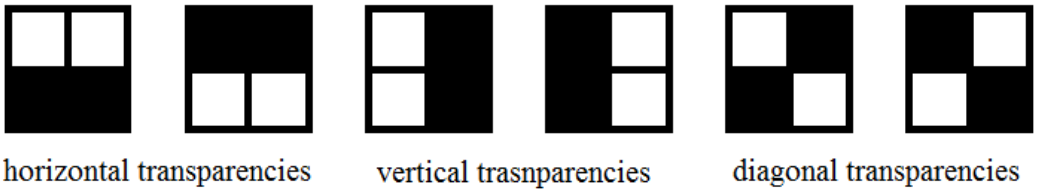


Figure 2.1: The different squares that are used for a 2 out of 2 scheme

upper left subpixel, "*ur*" the upper right, "*ll*" the lower left, and "*lr*" the lower right subpixel:

$$\begin{array}{|c|c|} \hline \text{ul} & \text{ur} \\ \hline \text{ll} & \text{lr} \\ \hline \end{array} \quad \rightsquigarrow \quad \begin{bmatrix} ul & ur & ll & lr \end{bmatrix}$$

As a result, collection $\mathcal{C}_0$ consists of the following set of matrices:

$$\mathcal{C}_0 = \left\{ \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \end{bmatrix} \right\}$$

Collection $\mathcal{C}_1$ consists of the following set of matrices:

$$\mathcal{C}_1 = \left\{ \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix} \begin{bmatrix} 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix} \right\}$$

Any single transparency (corresponding to a single row from an array of collection $\mathcal{C}_0$ or collection $\mathcal{C}_1$) consists of two black and two white subpixels arranged in all possible ways, and looks medium gray. Since the number of black (white respectively) subpixels is 2 in all the transparencies, the scheme is uniform.

As a result, the contrast of the scheme is $contrast_{SN} = h - l = 2 - 0 = 2$ and the relative difference between a black and a white pixel (i.e. the loss of contrast) is $contrastloss_{SN} = a = \frac{h-l}{b} = \frac{2}{4} = \frac{1}{2}$.

Respectively, $contrast_{VVT} = \frac{h-l}{h+l} = \frac{2-0}{2+0} = \frac{2}{2} = 1$ and $contrastloss_{VVT} = \frac{h-l}{b\cdot(h+l)} = \frac{2-0}{4\cdot(2+0)} = \frac{1}{4}$. The scheme is of type $[b; h, l = 0; r] = [4; 2, 0; 6]$ and thus is a maximal contrast scheme. So, when the two transparencies are stacked together, the visual outcome is either medium gray, which in this case represents white, or completely black, which represents black.

2.2 A 3 out of 3 Visual Secret Sharing Scheme

A 3 out of 3 visual secret sharing scheme can be generated by the 3×4 boolean matrices A_0 and A_1 as follows:

$$\mathcal{C}_0 = \{\text{all the matrices obtained by permuting the columns of } A_0 = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}\}$$

$$\mathcal{C}_1 = \{\text{all the matrices obtained by permuting the columns of } A_1 = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix}\}$$

As one may notice, the rows of A_0 and A_1 are the six different squares used in the 2 out of 2 visual scheme described in Section 2.1. More specifically, each one of them consists of one horizontal, one vertical, and one diagonal type of transparencies. As for the security of the scheme: Any single row contains two black and two white subpixels in any order and any two trans-

parencies consist of one common and two individual black subpixels, in any order, too. What is more, the "or" of any two rows consists of one white and three black subpixels. Hence, it is impossible to distinguish between a matrix from $\mathcal{C}_0$ and a matrix from $\mathcal{C}_1$ when less than three transparencies are inspected. Additionally, the scheme is uniform. However, if we stack three transparencies from a matrix in $\mathcal{C}_0$ one subpixel will be white and the rest three will be black, whereas when a matrix from $\mathcal{C}_1$ is chosen, it is completely black.

As a result, the contrast of the scheme is $contrast_{SN} = h - l = 1 - 0 = 1$ and the loss of contrast $contrastloss_{SN} = \frac{h-l}{b} = \frac{1}{4}$.

Respectively, $contrast_{VVT} = \frac{h-l}{h+l} = \frac{1-0}{1+0} = 1$ and the loss of contrast $contrastloss_{VVT} = \frac{h-l}{b\cdot(h+l)} = \frac{1-0}{4\cdot(1+0)} = \frac{1}{4}$. The scheme is of type $[b; h, l = 0; r] = [4; 1, 0; 24]$ and thus is a maximal contrast scheme. So, when three transparencies (shares) are stacked together, the result is either 3/4 gray (which represents white) or completely black (which represents black).

2.3 A 4 out of 4 Visual Secret Sharing Scheme

A 4 out of 4 visual secret sharing scheme can be generated by the permutation of the columns of the following two 4×9 boolean matrices A_0 and A_1:

$$A_0 = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \end{bmatrix} \quad A_1 = \begin{bmatrix} 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 \end{bmatrix}$$

The visual form of the 3×3 squares that represent a single pixel are

shown in Figure 2.2 from [2]:

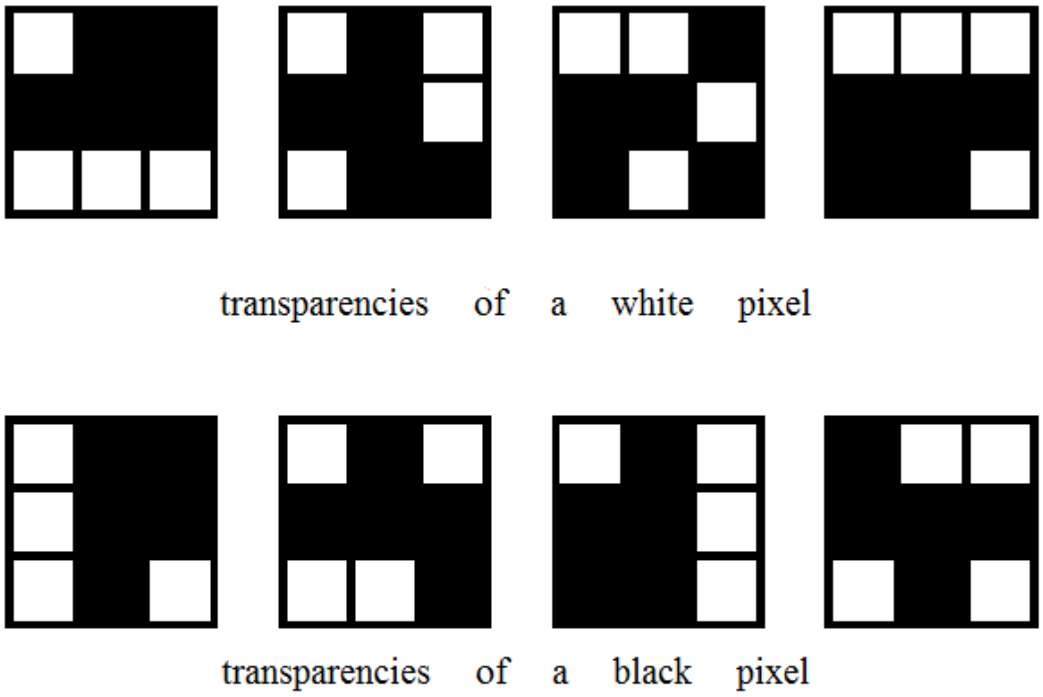


Figure 2.2: The 3×3 squares that represent a single pixel in a 4 out of 4 scheme

As one can see, each square contains 5 black subpixels, any stacked pair of transparencies contains 7 black ones, and any three of them 8 black subpixels. However, when four of them are stacked together, if the matrix belongs to $\mathcal{C}_0$ collection there exist one white and 8 black subpixels, whereas if it belongs to $\mathcal{C}_1$ all of the subpixels are black. It would be possible to use 8 instead of 9 subpixels, but then the aspect ratio would be distorted.

As a result, the contrast of the scheme is $contrast_{SN} = h - l = 1 - 0 = 1$ and the loss of contrast $contrastloss_{SN} = \frac{h-l}{b} = \frac{1}{9}$.

Respectively, $contrast_{VVT} = \frac{h-l}{h+l} = \frac{1-0}{1+0} = 1$ and $contrastloss_{VVT} =$

$\frac{h-l}{b\cdot(h+l)} = \frac{1-0}{9\cdot(1+0)} = \frac{1}{9}$. The scheme is of type $[b; h, l = 0; r] = [9; 1, 0; 9!]$ and thus is a maximal contrast scheme. So, when all four shares are stacked together, the result is either deep gray (i.e., 8/9 black subpixels), which represents white, or completely black, which represents black.

2.4 A 2 out of 6 Visual Secret Sharing Scheme

In this Section we describe a 2 out of 6 visual secret sharing scheme. The scheme is generated by two 6×4 boolean matrices, A_0 and A_1.

$$\mathcal{C}_0 = \{\text{all the matrices obtained by permuting the columns of } A_0 = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{bmatrix}\}$$

$$\mathcal{C}_1 = \{\text{all the matrices obtained by permuting the columns of } A_1 = \begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix}\}$$

In both A_0 and A_1, each row consists of two black and two white subpixels in any order. Hence, no conclusion can be made about the colour of the pixel and the scheme is secure.

As a result, the contrast of the scheme is $contrast_{SN} = h - l = 2 - 1 = 1$ and the loss of contrast $contrastloss_{SN} = a = \frac{h-l}{b} = \frac{1}{4}$.

Respectively, $contrast_{VVT} = \frac{h-l}{h+l} = \frac{2-1}{2+1} = \frac{1}{3}$ and $contrastloss_{VVT} = \frac{h-l}{b\cdot(h+l)} = \frac{2-1}{4\cdot(2+1)} = \frac{1}{12}$. The scheme is of type $[b; h, l; r] = [4; 2, 1; 24]$. When two transparencies are stacked together, the result is either medium gray (i.e., half subpixels white and half black), which represents white, or (almost) completely black (at least 3 subpixels back), which represents black (some cover all four).

Chapter 3

Visual Secret Sharing Schemes for fixed k

3.1 A 2 out of n Scheme and its Dual

In this Section a general 2 out of n visual secret sharing scheme is presented with blocklength $b = n$ using the following collections of $n \times n$ matrices:

$$\mathcal{C}_0 = \{\text{all the matrices obtained by permuting the columns of } A_0 = \begin{bmatrix} 100 & \dots & 0 \\ 100 & \dots & 0 \\ \dots & & \\ 100 & \dots & 0 \end{bmatrix}\}$$

$$\mathcal{C}_1 = \{\text{all the matrices obtained by permuting the columns of } A_1 = \begin{bmatrix} 100 & \dots & 0 \\ 010 & \dots & 0 \\ \dots & & \\ 000 & \dots & 1 \end{bmatrix}\}$$

As one can see, each row of a matrix in both collections consists of one black and $n-1$ white subpixels. As a result, the scheme complies with the security condition in Definition 1.3.2. When any two transparencies from a matrix in $\mathcal{C}_0$ are stacked together the "or"-ed vector still consists of one black and $n-1$ white subpixels. However, in $\mathcal{C}_1$, there exist two black and $n-2$ white subpixels, which looks relatively darker. By stacking more transparencies the difference between a black and a white pixel becomes more obvious. What is more, the scheme is uniform with parameters $[b; h, l; r] = [n; n-1, n-2; n!]$.

As a result, the contrast of the scheme is $contrast_{SN} = h - l = (n-1) - (n-2) = 1$ and the loss of contrast $contrastloss_{SN} = a = \frac{h-l}{b} = \frac{1}{n}$.

Respectively, $contrast_{VVT} = \frac{h-l}{h+l} = \frac{(n-1)-(n-2)}{(n-1)+(n-2)} = \frac{1}{2n-3}$ and $contrastloss_{VVT} = \frac{h-l}{b\cdot(h+l)} = \frac{1}{n\cdot(2n-3)}$. However, for large n the contrast of the scheme is nearly zero.

By switching 0 and 1 (i.e., by getting the complements of the matrices) a new 2 out of n visual secret sharing scheme is constructed with maximal contrast 1. In that case the two collections $\mathcal{C}_0$ and $\mathcal{C}_1$ are:

$$\mathcal{C}_0 = \{\text{all the matrices obtained by permuting the columns of } A_0 = \begin{bmatrix} 011 & \dots & 1 \\ 011 & \dots & 1 \\ \dots & & \\ 011 & \dots & 1 \end{bmatrix}\}$$

$$\mathcal{C}_1 = \{\text{all the matrices obtained by permuting the columns of } A_1 = \begin{bmatrix} 011 & \dots & 1 \\ 101 & \dots & 1 \\ \dots & & \\ 111 & \dots & 0 \end{bmatrix}\}$$

As one can see $l = 0$, so the scheme is a maximal contrast secret sharing scheme with parameters $[b; h, l; r] = [n; 1, 0; n!]$.

As a result, the contrast of the scheme is $contrast_{SN} = h - l = 1 - 0 = 1$ and the loss of contrast $contrastloss_{SN} = a = \frac{h-l}{b} = \frac{1}{n}$.

Respectively, $contrast_{VVT} = \frac{h-l}{h+l} = \frac{1-0}{1+0} = 1$ (maximal contrast scheme) and $contrastloss_{VVT} = \frac{h-l}{b\cdot(h+l)} = \frac{1}{n}$.

3.2 A second 2 out of n Visual Secret Sharing Scheme

The 2 out of 6 visual secret sharing scheme described in Section 2.4 can be used as a basis to construct a uniform 2 out of n scheme $S = (\mathcal{C}_0, \mathcal{C}_1)$. We choose a non-negative integer m such that $\binom{m}{m/2} \geq n$. Next, we choose a "ground set" (any set will do) of size m and consider all of its subsets of size $m/2$. As will become obvious later on, m must satisfy $\binom{m}{m/2} \geq n$ because in this way we ensure that there exist at least n different subsets, i.e., at least n different transparencies to be used to construct the scheme. Matrix A_1 then is constructed as follows: the ith row in A_1 corresponds to the ith subset, i.e., $A_1[i, j] = 1$ iff the jth element is in the ith subset. A_0 is the $n \times m$ matrix where each row is $1^{m/2}0^{m/2}$. Collections $\mathcal{C}_0$ and $\mathcal{C}_1$ are obtained from

all column permutations of A_0 and A_1 respectively.

The blocklength of the scheme is m and any single transparency contains an arbitrary collection of $m/2$ black and $m/2$ white subpixels. Hence, the scheme is uniform and perfectly secure. Any two stacked transparencies from $\mathcal{C}_0$ contain $m/2$ black subpixels whereas any two from $\mathcal{C}_1$ contain at least $\frac{m}{2}+1$ black subpixels, since the corresponding subsets cannot be the same. The parameters of the scheme are $[b; h, l; r] = [m; \frac{m}{2}, \frac{m}{2} - 1; m!]$.

As a result, the contrast of the scheme is $contrast_{SN} = h - l = w(\vec{v}_1) - w(\vec{v}_0) = \frac{m}{2} + 1 - \frac{m}{2} = 1$ and the loss of contrast $contrastloss_{SN} = a = \frac{h-l}{b} = \frac{1}{m}$.

Respectively, $contrast_{VVT} = \frac{h-l}{h+l} = \frac{1}{m-1}$ $contrastloss_{VVT} = \frac{h-l}{b\cdot(h+l)} = \frac{1}{m(m-1)}$.

Example 3.2.1: An example follows for $n = 5$:

We choose $m = 4$, because $\binom{m}{m/2} = \binom{4}{2} = 6 > 5$. In this case the ground set will be $J = \{j_1, j_2, j_3, j_4\}$ and all the subsets of size $\frac{m}{2} = 2$ are:

$$S_1 = \{j_1, j_2\}, \quad S_2 = \{j_1, j_3\}, \quad S_3 = \{j_1, j_4\},$$

$$S_4 = \{j_2, j_3\}, \quad S_5 = \{j_2, j_4\}, \quad S_6 = \{j_3, j_4\},$$

Matrix A_0 is the same as in the 2 out of 6 scheme described above. We choose S_1, S_2, S_3, S_4 and S_6 subsets for the $n = 5$ transparencies and we construct matrix A_1. As a result, matrices A_0 and A_1 are the following:

$$A_0 = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{bmatrix} \quad A_1 = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}$$

As a result, the contrast of this scheme is $contrast_{SN} = h - l = 1$ and the loss of contrast $contrastloss_{SN} = a = \frac{h-l}{b} = \frac{1}{4}$. Respectively, $contrast_{VVT} = \frac{h-l}{h+l} = \frac{1}{3}$ and the loss of contrast $contrastloss_{VVT} = \frac{h-l}{b\cdot(h+l)} = \frac{1}{12}$. The parameters of the scheme are $[b; h, l; r] = [4; 2, 1; 24]$.

3.3 A 3 out of n Visual Secret Sharing Scheme

The 3 out of 3 visual secret sharing scheme described in Section 2.2 can be used as a basis to construct a uniform 3 out of n scheme $S = (\mathcal{C}_0, \mathcal{C}_1)$. Consider an $n \times (n-2)$ matrix B whose elements are all ones (i.e., corresponds to all black subpixels) and the $n \times n$ identity matrix I whose elements are all zeros except for the diagonal whose values are ones. We denote BI the $n \times (2n-2)$ matrix which is the concatenation of the matrices B and I. Additionally, let $c(BI)$ be the boolean complement of BI. Then, we define

$\mathcal{C}_0 = \{$all the matrices obtained by permuting the columns of $A_0 = c(BI)\}$

$\mathcal{C}_1 = \{$all the matrices obtained by permuting the columns of $A_1 = BI\}$

Each transparency from any matrix consists of $n-1$ black and $n-1$ white subpixels. What is more, any two of them stacked on top of each other have two individual and $n-2$ common black subpixels. Hence, the scheme complies with the security condition in Definition 1.2.1.

The "or" vector of any three transparencies from any matrix in $\mathcal{C}_0$ contains n black subpixels, whereas in $\mathcal{C}_1$ collection contains $n+1$ black subpixels. As a result, the scheme is a uniform visual secret sharing scheme with parameters $[b; h, l; r] = [2n-2; n-2, n-3; n!]$.

As a result, the contrast of the scheme is $contrast_{SN} = h - l = w(\vec{v}_1) - w(\vec{v}_0) = n+1-n = 1$ and the loss of contrast is $contrastloss_{SN} = a = \frac{h-l}{b} = \frac{1}{2n-2}$.

Respectively, $contrast_{VVT} = \frac{h-l}{h+l} = \frac{1}{(n-2)+(n-3)} = \frac{1}{2n-5}$ and $contrastloss_{VVT} = \frac{h-l}{b\cdot(h+l)} = \frac{1}{(2n-2)(2n-5)}$. For large n the contrast of the scheme is nearly zero.

Example 3.3.1: An example for $n = 5$ follows:

The $n \times (n-2) = 5 \times 3$ dimensional matrix B and the $n \times n = 5 \times 5$ identity matrix I are:

$$B = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix} \quad I = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

The concatenated matrix BI then, and its Boolean complement $c(BI)$ will be:

$$BI = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \quad c(BI) = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{bmatrix}$$

The blocklength of the scheme is $b = 2n - 2 = 2 \cdot 5 - 2 = 8$. The contrast of the scheme is $contrast_{NS} = h - l = 3 - 2 = 1$ and the loss of contrast $contrastloss_{SN} = a = \frac{h-l}{b} = \frac{1}{2n-2} = \frac{1}{2 \cdot 3-2} = \frac{1}{4}$.

Respectively, $contrast_{VVT} = \frac{h-l}{h+l} = \frac{3-2}{2+3} = \frac{1}{5}$ and $contrastloss_{VVT} = \frac{h-l}{b \cdot (h+l)} = \frac{3-2}{8 \cdot (3+2)} = \frac{1}{40}$. The parameters of the scheme are $[b; h, l; r] = [8; 3, 2; 5!]$.

Chapter 4

k out of k Visual Secret Sharing Schemes

4.1 A k out of k scheme - Construction I

This k out of k visual secret sharing scheme $S = (\mathcal{C}_0, \mathcal{C}_1)$ was presented in [2] by Naor, Shamir: In order to construct the scheme we will use vectors of length k over the Galois field $GF(2)$, namely the Vector Space $V(k, 2)$. In particular, two sets of vectors are needed, denoted $J_1^0, J_2^0, \ldots, J_k^0$ and $J_1^1, J_2^1, \ldots, J_k^1$. Every $k-1$ vectors of the $J_1^0, J_2^0, \ldots, J_k^0$ are linearly independent whereas all k of them are not. An example of such a set is constructed as follows: $J_i^0 = 0^{i-1}10^{k-i}$ for $1 \leq i < k$ and $J_k^0 = 1^{k-1}0$. On the other hand, the vectors $J_1^1, J_2^1, \ldots, J_k^1$ are all linearly independent over $GF(2)$. As an example, we could use the following vectors: $J_i^1 = 0^{i-1}10^{k-i}$ for $1 \leq i \leq k$.

To construct matrix A_0 the following steps must be taken: we construct a $k \times k$ matrix B_0 whose rows are the k vectors $J_1^0, J_2^0, \ldots, J_k^0$. Additionally,

let F be a $k \times 2^k$ matrix whose columns consist of all the 2^k vectors in $V(k,2)$. Then, the multiplication $B_0 \cdot F$ results in a new $k \times 2^k$ boolean matrix A_0. Following the same procedure we construct matrix A_1, but vectors $J_1^1, J_2^1, \ldots, J_k^1$ are used as the rows of matrix B_1 respectively.

Lemma 4.1.1: *a. If B_t, $t \in \{0,1\}$ consists of $k-1$ linearly independent vectors, then A_t, when limited to $k-1$ rows contains exactly 2 all-zero columns.*

b. If the k vectors that B_1 consists of are linearly independent, then each vector in $V(k,2)$ occurs exactly once as a column of $B_1 \cdot F = A_1$.

Proof. a. Let us denote $null(B_t)$ the dimension of the null-space of B_t and $rank(B_t)$ the dimension of B_t. Then, it holds that $rank(B_t) + null(B_t) = k$. But $rank(B_t) = k-1$, hence, $null(B_t) = k - (k-1) = 1$. As a result, matrix A_t that is constructed by B_t and all the vectors in $V(k,2)$ will contain $2^{k-(k-1)} = 2$ all-zero columns.

b. Let us suppose that this is not the case, i.e., there exist $\vec{r}_1$ and $\vec{r}_2 \in V(k,2)$ that appear as columns in F, where $\vec{r}_1 \neq \vec{r}_2$, such that $B_1\vec{r}_1 = \vec{r}_3$ (equation I) and $B_1\vec{r}_2 = \vec{r}_3$ (equation II), $\vec{r}_3 \in V(k,2)$. But B_1 consists of linearly independent vectors, hence, it is invertible, i.e., B_1^{-1} exists. Then, from equations I and II it follows that $\vec{r}_1 = B_1^{-1}\vec{r}_3$ and $\vec{r}_2 = B_1^{-1}\vec{r}_3$, i.e., $\vec{r}_1 = \vec{r}_2$, which is a contradiction to the initial hypothesis. Hence, all the columns of $B_1 \cdot F = A_1$ consist of 2^k different vectors, i.e., each vector in $V(k,2)$ occurs exactly once as a column in A_1. □

Theorem 4.1.2: *The scheme described above is a k out of k visual secret sharing scheme with $b = 2^k$, $a = 1/2^k$, and $r = 2^k!$. Its parameters are*

$[b; h, l; r] = [2^k; 2, 1; 2^k!]$.

Proof. Both A_0 and A_1 are $k \times 2^k$ matrices, hence, the blocklength of the scheme is $b = 2^k$.

About the contrast of the scheme: As one can see, matrix A_0 contains two all-zero columns: one corresponds to the all-zero vector and the other one to vector $0^{k-1}1$ in F, hence, $h = 2$. However, from Lemma 4.1.1.b we get that matrix A_1 contains only one all-zero column, the one that corresponds to the all-zero vector in F, since all the k vectors are linearly independent, hence, $l = 1$. The same holds for all the matrices that are obtained from the column permutations of A_0 and A_1 respectively.

Hence, the contrast of the scheme is $contrast_{SN} = h - l = 2 - 1 = 1$ and $contrastloss_{SN} = a = (h - l)/b = (2 - 1)/2^k = 1/2^k$.

Respectively, $contrast_{VVT} = \frac{h-l}{h+l} = \frac{1}{2+1} = \frac{1}{3}$ and $contrastloss_{VVT} = \frac{h-l}{b\cdot(h+l)} = \frac{1}{3\cdot 2^k}$.

In order to show security, let us consider the following:

Note that the vectors corresponding to any $k-1$ rows in both B_0 and B_1 are linearly independent over $GF(2)$. By Lemma 4.1.1.a we get that when A_0 and A_1 are limited to any $k-1$ rows they both have two all-zero columns. Since this is the case for any $k-1$ rows, it will hold for less than $k-1$ rows, too. As a result, there cannot be a distinction between A_0 and A_1 when they are limited to less than k rows. The same will hold for all the column permutations of them and as a result, the scheme complies with the security condition of Definition 1.3.2.

Since the blocklength of the scheme is 2^k, it follows that the cardinality

of both collections $\mathcal{C}_0$ and $\mathcal{C}_1$ is $r = 2^k!$. □

Example 4.1.3: Consider $k = 4$, so the two lists of vectors will be:

$J_1^0 = 1000$, $J_2^0 = 0100$, $J_3^0 = 0010$, and $J_4^0 = 1110$

$J_1^1 = 1000$, $J_2^1 = 0100$, $J_3^1 = 0010$, and $J_4^1 = 0001$

As one can see, any $k-1$ vectors of list J_i^0 are linearly independent while all k are not. Additionally, all k vectors of list J_i^1 are linearly independent.

The vector space $V(4,2)$ consists of the following $2^k = 2^4 = 16$ vectors:

0000, 0001, 0010, 0011, 0100, 0101, 0110, 0111, 1000, 1001, 1010, 1011, 1100, 1101, 1110, and 1111.

To create A_0 we index its columns by the 16 vectors of $V(4,2)$ and calculate the inner product of each one of them with the vectors consisting list J_i^0. The result is the following:

$$A_0 = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix}$$

Similarly for A_1:

$$A_1 = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$$

In this scheme the contrast is $contrast_{SN} = h - l = 2 - 1 = 1$ and the loss of contrast $contrastloss_{SN} = a = \frac{1}{2^k} = \frac{1}{2^5}$.

Accordingly, $contrast_{VVT} = \frac{h-l}{h+l} = \frac{1}{2+1} = \frac{1}{3}$ and $contrastloss_{VVT} = \frac{h-l}{b\cdot(h+l)} = \frac{1}{3\cdot 2^k} = \frac{1}{3\cdot 2^5}$. The parameters of the scheme are $[b; h, l; r] = [16; 2, 1; 16!]$.

4.2 A k out of k scheme - Construction II

This k out of k visual secret sharing scheme $S = (\mathcal{C}_0, \mathcal{C}_1)$ generated by matrices A_0 and A_1 was also presented in [2] by Naor, Shamir: In order to construct it a ground set of k elements $W = \{e_1, e_2, \ldots, e_k\}$ will be used as a basis. Let us denote $\{\pi_1, \pi_2, \ldots, \pi_{2^{k-1}}\}$ the list of all the 2^{k-1} subsets of W of even cardinality and $\{\sigma_1, \sigma_2, \ldots, \sigma_{2^{k-1}}\}$ the list of all the subsets of W of odd cardinality.

Both A_0 and A_1 will be $k \times 2^{k-1}$ dimensional matrices. The elements of A_0 will be defined by the formula: $A_0[ij] = 1$ iff $e_i \in \pi_j$, where $1 \leq i \leq k$ and $1 \leq j \leq 2^{k-1}$. In exactly the same way, the elements of A_1 are defined by: $A_1[ij] = 1$ iff $e_i \in \sigma_j$, $1 \leq i \leq k$, and $1 \leq j \leq 2^{k-1}$.

By permuting the columns of matrices A_0 and A_1 in all possible ways we get the collections $\mathcal{C}_0$ and $\mathcal{C}_1$ of the scheme respectively.

Theorem 4.2.1: *The scheme described above is a k out of k visual secret sharing scheme with $b = 2^{k-1}$, $a = 1/2^{k-1}$, and $r = 2^{k-1}!$. Its parameters are $[b; h, l; r] = [2^{k-1}; 1, 0; 2^{k-1}!]$. What is more, it is a maximal contrast scheme.*

Proof. For each set W of k elements there exist 2^k different subsets, 2^{k-1} of even and 2^{k-1} of odd cardinality. Hence, both A_0 and A_1 consist of 2^{k-1} columns, i.e., the blocklength of the scheme is $b = 2^{k-1}$.

About the contrast of the scheme: There exists exactly one empty subset of W and it is contained in the list $\{\pi_1, \pi_2, \ldots, \pi_{2^{k-1}}\}$ of the even cardinality subsets. Hence, in matrix A_0 there exists an all-zero column, whereas in A_1 there is none. As a result, $h = 1$ and $l = 0$.

About the security of the scheme: The row of both A_0 and A_1 is defined by the element while the column by the subset. Since each element is in exactly half of the subsets, the number of zeros and ones is the same in each row, in both A_0 and A_1. Hence, a single row cannot reveal any secret about the colour of the pixel.

Additionally, when restricted to any $k-1$ rows, matrix A_0 has one all-zero column, and A_1 has one all-zero column, too. The latter corresponds to a subset that has only one element, the one which does not index any of the $k-1$ chosen rows, but it indexes the k-th.Using the same technique for less than $k-1$ rows, the same result follows.

As a result, the contrast of the scheme is $contrast_{SN} = h - l = 1 - 0 = 1$ and the loss of contrast $contrast_{SN} = a = \frac{h-l}{b} = \frac{1}{2^{k-1}}$.

Accordingly, $contrast_{VVT} = \frac{h-l}{h+l} = \frac{1-0}{1+0} = 1$ and $contrastloss_{VVT} = \frac{h-l}{b\cdot(h+l)} = \frac{1-0}{2^{k-1}\cdot(1+0)} = \frac{1}{2^{k-1}}$. Since $l = 0$, the scheme is of type $[b; h, l = 0] = [2^{k-1}; 1, 0]$ and thus is a maximal contrast scheme. So, when two shares are stacked together, the result is either deep gray (which represents white) or completely black (which represents black). □

Example 4.2.2: Let $k = 4$ and the ground set W be: $W = \{e_1, e_2, e_3, e_4\}$. Then the subsets of even cardinality are the $2^{k-1} = 2^{4-1} = 2^3 = 8$ following:

$\emptyset$, $\{e_1, e_2\}$, $\{e_1, e_3\}$, $\{e_1, e_4\}$, $\{e_2, e_3\}$, $\{e_2, e_4\}$, $\{e_3, e_4\}$, $\{e_1, e_2, e_3, e_4\}$

Accordingly, the subsets of odd cardinality are the $2^{k-1} = 2^{4-1} = 2^3 = 8$

following:

$\{e_1\}$, $\{e_2\}$, $\{e_3\}$, $\{e_4\}$, $\{e_1, e_2, e_3\}$, $\{e_1, e_2, e_4\}$, $\{e_1, e_3, e_4\}$, $\{e_2, e_3, e_4\}$

To construct A_0 we index the rows of the matrix by the elements of the ground set W, i.e. e_1, e_2, e_3 and e_4 and the columns by the subsets of even cardinality of W. Then we have:

$$A_0 = \begin{bmatrix} 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}$$

The construction of A_1 is similar with the exception that the columns of the matrix are indexed by the odd cardinality subsets of W. Thus, we have:

$$A_1 = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}$$

As a result, the contrast of this scheme is $contrast_{SN} = h - l = 1 - 0 = 1$ and the loss of contrast $contrastloss_{SN} = a = \frac{h-l}{b} = \frac{1}{2^{k-1}} = \frac{1}{2^3} = \frac{1}{8}$.

Accordingly, $contrast_{VVT} = \frac{h-l}{h+l} = 1$ and $contrastloss_{VVT} = \frac{h-l}{b\cdot(h+l)} = \frac{1}{2^3} = \frac{1}{8}$. The parameters of the scheme are $[b; h, l; r] = [8; 1, 0; 8!]$.

4.3 An upper bound on a for k out of k schemes

Theorem 4.3.1: *Let $S = (\mathcal{C}_0, \mathcal{C}_1)$ be any k out of k scheme visual secret sharing scheme. Then $a \leq \frac{1}{2^{k-1}}$ and $b \geq 2^{k-1}$.*

Proof. In order to prove that $a \leq \frac{1}{2^{k-1}}$ the following combinatorial fact will be used (see [6], [7]). Let us consider a ground set G and two lists of subsets of it, denoted $X_1, X_2, \ldots, X_k$ and $Y_1, Y_2, \ldots, Y_k$. If for every subset $U \subset \{1, \ldots, k\}$ of size less than k (i.e. $\leq k-1$) it holds that $|\cap_{i\in U} X_i| = |\cap_{i\in U} Y_i|$, then $|\cup_{i=1}^{k} X_i| \leq \frac{1}{2^{k-1}} \cdot |G| + |\cup_{i=1}^{k} Y_i|$. Namely, if all the intersections of less than k of the sets X_i and Y_i, $1 \leq i \leq k$, contain the same number of elements, then the difference in their union cannot be too large.

Let us consider a k out of k visual secret sharing scheme $S = (\mathcal{C}_0, \mathcal{C}_1)$. The ground set that will be used contains $b \cdot r$ elements which are indexed by (x, y), where $1 \leq x \leq r$ and $1 \leq y \leq b$. The two lists of subsets $X_1, X_2, \ldots, X_k$ and $Y_1, Y_2, \ldots, Y_k$ are constructed in the following way: element (x, y) of G is in X_i iff $A_x^0[i, y] = 1$. Symmetrically, it is in Y_i iff $A_x^1[i, y] = 1$. The idea is that, for each row i we count all the ones in all matrices of collection $\mathcal{C}_0$ ($\mathcal{C}_1$ respectively) and add the corresponding elements in X_i (Y_i respectively).

The security condition of all visual secret sharing schemes implies that for any $U \subset \{1, \ldots, k\}$ of size $s < k$ it holds that $|\cap_{i\in U} X_i| = |\cap_{i\in U} Y_i|$ since there can be no distinction between matrices from $\mathcal{C}_0$ and $\mathcal{C}_1$ when limited to less than k rows. Then from the combinatorial fact described in the first paragraph we get that

$|\cup_{i=1}^{k} Y_i| \leq \frac{1}{2^{k-1}} \cdot rb + |\cup_{i=1}^{k} X_i|$

Namely, the difference of the Hamming weight of the "or" of any k rows of a matrix in $\mathcal{C}_0$ and one in $\mathcal{C}_1$ is at most $\frac{1}{2^{k-1}} \cdot b$, which implies that $w(\vec{v}_1) - w(\vec{v}_0) \leq \frac{1}{2^{k-1}} \cdot b$. Since $a = \frac{h-l}{b} = \frac{w(v_1)-w(v_0)}{b}$, from the previous formula if we divide by b we get: $a \leq \frac{1}{2^{k-1}}$.

The contrast condition of the scheme implies that the difference between the Hamming weight of the "or" of the k rows of a matrix in $\mathcal{C}_0$ and the Hamming weight of the "or" of the k rows of a matrix in $\mathcal{C}_1$ must be at least 1. Hence, from the same formula we conclude that: $1 \leq \frac{1}{2^{k-1}} \cdot b$, namely, $b \geq 2^{k-1}$. □

Chapter 5

General k out of n Visual Secret Sharing Schemes

5.1 A k out of n Scheme - Construction I

The following k out of n scheme was presented in [2] by Naor, Shamir. In particular, a given k out of k scheme is used in the construction of a k out of n scheme:

We consider a uniform k out of k scheme $\mathcal{S} = (\mathcal{C}_0, \mathcal{C}_1)$ with parameters b, a, and r. Each collection $\mathcal{C}_0$ and $\mathcal{C}_1$ consists of r $k \times b$ matrices $T_1^d, T_2^d, \ldots, T_r^d$, $d \in \{0, 1\}$.

We recall that a scheme is uniform when the number of zeros of the "or" of any $q < k$ rows, in any matrix T_i^d, $1 \leq i \leq r$ and $d \in \{0, 1\}$ depends only on the number q. Consequently, a function $f(q)$ can be used to describe it for both collections and as a result there is no way to decide if it is about a white or a black pixel. All the visual secret sharing schemes that are described so

far have this property.

In order to transform a k out of k scheme to a k out of n scheme a collection H of ℓ (hash) functions must be used with the following properties:

1. For every $h \in H$ it holds: $h : \{1, \ldots, n\} \mapsto \{1, \ldots, k\}$
2. If $Y = |\{h(i_1), h(i_2), \ldots, h(i_k)\}|$, $i \in \{1, \ldots, n\}$, is a random variable and β_q is the probability that $Prob[Y = q]$, then β_q is the same for every $h \in H$.

Let us name $\mathcal{S}' = (\mathcal{C}'_0, \mathcal{C}'_1)$ the new k out of n scheme.

Each collection $\mathcal{C}'_0$ and $\mathcal{C}'_1$ consists of r^ℓ different $n \times b \cdot \ell$ matrices. Each matrix is indexed by a vector t, where $t = (t_1, t_2, \ldots, t_\ell)$, $1 \leq t_i \leq r$. The elements of the matrices are calculated by the formula $A^d_t[i, (j, h)] = T^d_{t_h}[h(i), j]$, $d \in \{0, 1\}$, $0 \leq i \leq n-1$, $1 \leq j \leq b$, and $1 \leq h \leq \ell$. Additionally, t_h denotes the h-th entry in vector t, and $T^d_{t_h}[h(i), j]$ the corresponding element of matrix $T^d_{t_h}$ in $\mathcal{C}_d$ collection. As one can see, the blocklength of the scheme is $b \cdot \ell$.

Lemma 5.1.1: *By using a k out of k visual secret sharing scheme with parameters b, a, and r, one can construct a k out of n visual secret sharing scheme $\mathcal{S}'$ with parameters $b' = b \cdot \ell$, $a' = a \cdot \beta_k$, and $r' = r^\ell$, where ℓ denotes the number of the hash functions in the H family.*

Proof. From the construction above, it is obvious that each matrix A^d_t has blocksize ℓ times the blocksize of the matrices T^d_i, $1 \leq i \leq r$, namely, $b \cdot \ell$.

We have already mentioned that β_q denotes the probability that $Prob[Y = q]$, where $Y = |\{h(i_1), h(i_2), \ldots, h(i_k)\}|$ is a random variable, $i \in \{1, \ldots, n\}$.

By definition, β_q is the same for every $h \in H$. From the security of $\mathcal{S}$ it is ensured that if $q < k$ then the number of black subpixels (i.e., the Hamming weight of the "or"-ed q rows) is equal to $f(q)$ for all matrices in both $\mathcal{C}_0$ and $\mathcal{C}_1$ collections. Hence, only when h is limited to any k values is $1 - 1$, i.e., yields k different values, there is a distinction between a white and a black pixel. If we denote by β_k the probability that this event takes place, then, $\beta_k = \frac{k!}{k^k} \geq \frac{(k/e)^k}{k^k\sqrt{2\pi k}} = \frac{e^{-k}}{\sqrt{2\pi k}}$.

Considering all the above mentioned, the Hamming weight of an "or" of k rows of a white pixel (a matrix from $\mathcal{C}'_0$ collection) is **at most**

$$w(\vec{v_0}) \leq \ell(\beta_k \cdot (d - ab) + \sum_{q=1}^{k-1} \beta_q \cdot f(q)),$$

and the weight of a black pixel (a matrix from $\mathcal{C}'_1$ collection) is **at least**

$$w(\vec{v_1}) \geq \ell(\beta_k \cdot d + \sum_{q=1}^{k-1} \beta_q \cdot f(q)).$$

The above mentioned relation holds for $w(\vec{v_0})$ because when k out of n shares are chosen, one of the following will happen: (a) they will be mapped to k different values, with probability β_k, and then, there will be at most $b - ad$ black subpixels in a white pixel. In this case it will be clear that it is a white pixel. (b) they will be mapped to $q < k$ values, with probability β_q, and as stated in the definition of uniformity, the number of the black subpixels in this case is described by a function $f(q)$, i.e., it depends only on the number of rows q. Hence, there are q different events that may take place with β_q probability each. In such a case there is no way to tell if the shares describe a white or a black pixel.

The same applies to $w(\vec{v_1})$: when k out of n shares are chosen, one of the following will happen: (a) they will be mapped to k different values, with probability β_k, and as a result there will be at least d black subpixels in a

black pixel. It will be clear that it is a black pixel. (b) they will be mapped to $q < k$ values, with probability β_q, and again the number of the black subpixels is described by a function $f(q)$. Similarly, there are q different events that may take place with β_q probability each. It is again impossible to decide the colour of the pixel.

If we do the calculations, $w(\vec{v_1}) - w(\vec{v_0}) \geq \ell \cdot \beta_k \cdot a \cdot b$.

Then, the contrast of the scheme is $contrast_{SN} = h - l = w(\vec{v_1}) - w(\vec{v_0}) = \ell \cdot \beta_k \cdot a \cdot b$ and the relative difference (i.e., loss of contrast of the scheme) is $contrastloss_{SN} = a' = \frac{w_1(\vec{v}) - w_0(\vec{v})}{b'} = \frac{\ell \cdot \beta_k \cdot a \cdot b}{b \cdot \ell} = a \cdot \beta_k$.

As for the security of the scheme, as mentioned in the beginning of the Proof, each matrix A_t^d consists of ℓ matrices from the corresponding $\mathcal{C}_d$ collection. Hence, the security of the k out of k scheme implies the security of the new k out of n scheme. □

5.1.1 Construction of H

In order to create this family of hash functions the following must be taken under consideration:

Definition 5.1.1.1: A family H of hash functions $H = \{h : \mathcal{U} \mapsto [m]\}$ is *k-wise independent* if for every $h \in H$, and for all distinct values $x_1, x_2, \cdots, x_k \in \mathcal{U}$ and any k (not necessarily distinct) values $y_1, y_2, \ldots, y_k \in [m]$, it holds:

$Pr[h(x_1) = y_1 \ \& \ h(x_2) = y_2 \ \& \ \ldots \ \& \ h(x_k) = y_k] = \frac{1}{m^k}$

Alternatively we could say:

1. For any random $h \in H$ and for a fixed $x \in \mathcal{U}$, any value in $[m]$ is equally likely to represent $h(x)$, namely, $h(x)$ is uniformly distributed

in $[m]$.

2. If h is chosen randomly from H, then for any fixed distinct values $x_1, \ldots, x_k \in \mathcal{U}$ the outcomes $h(x_1), \ldots, h(x_k) \in [m]$ are independent random variables, i.e., they have the same probability distribution which cannot be influenced by the occurrence of the other values.

Such constructions are described in [8], [9], and [10].

For a general k out of n scheme, we want to construct H in such a way that for every $h \in H$ if we choose k different values $x_1, x_2, \ldots, x_k$ from $\{1, \ldots, n\}$ then $h(x_1), h(x_2), \ldots, h(x_k)$ are completely independent and as a result the probability β_q is the same for all of them.

A simple construction of such a family H follows:

We take k to be a prime and find a number p such that $k^p \geq n$. Then, there exist $(k^p)^k$ different polynomials $q(x)$ of degree $k-1$ over $GF(k^p)$. We take for every $h \in H$, $h(x) = w(q(x))$ and construct the H collection, where $w : GF(k^p) \mapsto GF(k)$. Since $|H| = (k^p)^k$ and $k^p \geq n$, $|H| \geq n^k$.

Combining Lemma 5.1.1 with the above described construction the following Theorem holds:

Theorem 5.1.1.2: *A visual secret sharing scheme with parameters* $b' = n^k \cdot 2^{k-1}$, $a' = 2(2e)^{-k}/\sqrt{2\pi k}$, *and* $r' = (2^{k-1}!)^{n^k}$ *can be constructed for any* n *and any* k.

Proof. This k out of n construction is based on a k out of k visual secret sharing scheme. Let us assume that the latter is the second k out of k scheme described earlier in Section 4.2, with $b = 2^{k-1}$, $a = \frac{1}{2^{k-1}}$, and $r = 2^{k-1}!$.

From Lemma 5.1.1 we get that $b' = b \cdot \ell$, $a' = a \cdot \beta_k$, and $r' = r^\ell$ are the parameters for the new k out of n scheme. Since $\ell = n^k$ and $\beta_k = \frac{e^{-k}}{\sqrt{2\pi k}}$, we get $b' = 2^{k-1} \cdot n^k$, $a' = \frac{1}{2^{k-1}} \cdot \frac{e^{-k}}{\sqrt{2\pi k}} = \frac{2 \cdot (2e)^{-k}}{\sqrt{2\pi k}}$, and $r = (2^{k-1}!)^{n^k}$. □

In the case of a 2 out of n visual scheme, a construction of a pairwise independent family of hash functions which is presented in [9] can be used. In this case, the construction is described as follows: Let us assume that we want to create a family of hash functions H such that for each $h \in H$ it holds that: $h : A \mapsto B$, where $A = \{0, \ldots, n-1\}$, $B = \{0, \ldots, k-1\}$, and $n > k$. We choose the smallest prime p such that $p \geq n$ and the family of hash functions is constructed using the formula $h(x) = ((cx + w) \bmod p) \bmod k$, where $c, w \in Z_p$ and $c \neq 0$. Hence, $|H| = p(p-1) \simeq n^2$.

Example 5.1.1.2: An example will enlighten the details of the construction of the scheme:

We will create a 2 out of 3 visual secret sharing scheme starting from a 2 out of 2 scheme, whose collections $\mathcal{C}_0$ and $\mathcal{C}_1$ are created by the permutations of the following two matrices:

$$T_0 = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix} \quad T_1 = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \end{bmatrix}$$

The above 2 out of 2 visual secret sharing scheme is uniform. Each collection, $\mathcal{C}_0$ and $\mathcal{C}_1$, consists of $r = 4! = 24$ matrices, so, the parameters of the scheme are $[b; h, l; r] = [4; 2, 0; 24]$.

Since $k = 2$, in order to create H we will use the construction from [9], which was described above. Then, collection H will consist of the following 6 hash functions, i.e., $\ell = 6$:

$h_1(n) = (n \bmod 3) \bmod 2$

$h_2(n) = ((n+1) \bmod 3) \bmod 2$

$h_3(n) = ((n+2) \bmod 3) \bmod 2$

$h_4(n) = (2n \bmod 3) \bmod 2$

$h_5(n) = ((2n+1) \bmod 3) \bmod 2$

$h_6(n) = ((2n+2) \bmod 3) \bmod 2$

As one can see, all of them fulfill the requirements stated before:

- For all of them we have: $h_i : \{1..3\} \mapsto \{1..2\}$ and
- If $Y = |\{h(i_1), h(i_2), h(i_3)\}|$, $i \in \{1, \ldots, 3\}$, is a random variable and β_q is the probability that $Prob[Y = q]$, then β_q is the same for every $h \in H$.

The vectors that will index the matrices of the collections $\mathcal{C}'_0$ and $\mathcal{C}'_1$ are $[1,1,1,1,1,1]$ up to $[24,24,24,24,24,24]$, i.e., each collection consists of 24^6 matrices.

In the new 2 out of 3 scheme each matrix $A^d_{[t_1,t_2,t_3]}$ has 3 rows, since $n = 3$, and $\ell \cdot b = 6 \cdot 4 = 24$ columns.

Its elements are calculated by the formula $A^d_t[i,(j,h)] = T^d_{t_h}[h(i),j]$. Applying this formula, $A^0_{[1,1,1,1,1,1]}$ and $A^1_{[1,1,1,1,1,1]}$ matrices of the new scheme will be the following:

$$A^0_{[1,1,1,1,1,1]} = \begin{bmatrix} 0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&1&1&1&1&1&1&1&1&1 \\ 0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&1&1&1&1&1&1&1&1&1 \\ 0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&1&1&1&1&1&1&1&1&1 \end{bmatrix}$$

$$A^1_{[1,1,1,1,1,1]} = \begin{bmatrix} 0&1&0&0&1&0&0&1&0&0&1&0&1&0&1&1&0&1&1&0&1&1&0&1 \\ 1&0&0&0&0&1&1&0&0&0&0&1&0&1&1&1&1&0&0&1&1&1&1&0 \\ 0&0&1&1&0&0&0&0&1&1&0&0&1&1&0&0&1&1&1&1&0&0&1&1 \end{bmatrix}$$

Each single line either from matrix $A^0_{[1,1,1,1,1,1]}$ or matrix $A^1_{[1,1,1,1,1,1]}$ consists of 12 zeros and 12 ones. Hence, there there is no way to decide if the matrix belongs to either $\mathcal{C}'_0$ or $\mathcal{C}'_1$ judging from only one transparency. The boolean "or" of any 2 rows of matrix $A^0_{[1,1,1,1,1,1]}$ consist of 4 zeros while in $A^1_{[1,1,1,1,1,1]}$ consist of 12 zeros.

As a result, the contrast of the scheme is $contrast_{SN} = h - l = 12 - 4 = 8$ and the loss of contrast $contrastloss_{SN} = a = \frac{h-l}{b} = \frac{8}{24} = \frac{1}{3}$.

Accordingly, $contrast_{VVT} = \frac{h-l}{h+l} = \frac{8}{16} = \frac{1}{2}$ and $contrastloss_{VVT} = \frac{h-l}{b(h+l)} = \frac{8}{16 \cdot 24} = \frac{1}{48}$.

Collections $\mathcal{C}'_0$ and $\mathcal{C}'_1$ consist of all the 24^6 matrices.

As a result, the parameters of the new scheme $\mathcal{S}'$ are: $[b'; h', l'; r'] = [24; 12, 4; 24^6]$.

5.2 A k out of n Scheme - Construction II

5.2.1 Relaxing the conditions on H

As the size of collection H is very big, it is about n^k as mentioned in the previous section, it would be preferable to reduce it since it affects the block-length and the size of the collections $\mathcal{C}_0$ and $\mathcal{C}_1$ of the scheme. In order to accomplish this, we could modify condition 2 from Section 5.1 of H as follows: the probability b_q that k different values from $\{1, \ldots, n\}$ to $\{1, \ldots, k\}$ are mapped to q different values is the same for a randomly chosen function $h \in H$ to within $\pm\epsilon$. Namely,

$\forall q \ \exists \beta_q$ such that $\forall x_{i1}, x_{i2}, \ldots x_{ik}$, where $i_1, i_2, \ldots, i_k \in \{1, \ldots, n\}$,

$|Prob[|\{h(x_1), \ldots, h(x_k)\}| = q] - \beta_q| \leq \epsilon$, for a randomly chosen $h \in H$.

In such a case it is possible to construct H in such a way that its size can be significantly smaller. If we apply such a family in the construction of the previous section we observe the following:

The Hamming weight of an "or" of k rows of a white pixel is **at most:**

$$w(\vec{v_0}) \leq \ell((\beta_k + \epsilon) \cdot (d - ab) + \sum_{q=1}^{k-1} (\beta_q + \epsilon) \cdot f(q))$$

and the weight of a black pixel is **at least**:

$$w(\vec{v_1}) \geq \ell((\beta_k - \epsilon) \cdot d + \sum_{q=1}^{k-1} (\beta_q - \epsilon) \cdot f(q))$$

As a result, the difference between a black and a white pixel is therefore **at least:**

$$w(\vec{v_1}) - w(\vec{v_0}) = \ell(\beta_k ab + eab - 2\epsilon d - 2\epsilon \sum_{q=1}^{k-1} f(q)) \geq \ell(\beta_k ab - 2\epsilon d - 2\epsilon \sum_{q=1}^{k-1} f(q))$$

But $f(q) \leq d - ab$, hence, $\sum_{q=1}^{k-1} f(q)) \leq (k-1)(d-ab)$, and as a result,

$w(\vec{v_1}) - w(\vec{v_0}) \geq \ell(\beta_k ab - 2\epsilon kd - 2\epsilon b)$

Hence, it follows that the relative difference of the new scheme will be

$a' \geq \beta_k a - 2\epsilon(1 + kd/b)$.

Since fewer than k transparencies never result in k different values, the security of the scheme is ensured.

5.2.2 Construction of relaxed H:

In order to reduce the size of H we will use the concept of small-bias sample spaces. *A small-bias sample space* (also defined as δ-biased sample space, δ-biased generator, or small-bias probability space) is a probability distribution that is very similar to the uniform distribution, to within a factor δ (in the bibliography it can be found as ϵ-biased but since ϵ is used in another way -see previous section- it is denoted by δ). One can consult [8], [11], and [12]

for constructions of such sample spaces.

Let $x_1, \ldots, x_n$ be n random variables that take values from $\{0, 1\}$ and let D denote their joint probability distribution.

Definition 5.2.2.2: We define

$$bias_D(S) = \left| Prob_D \left[\left(\sum_{i \in S} x_i = 0 \right) \bmod 2 \right] - Prob_D \left[\left(\sum_{i \in S} x_i = 1 \right) \bmod 2 \right] \right|$$

to be the *bias of a subset* $S \subseteq \{1, \ldots, n\}$ for some distribution D. Then, the above mentioned variables $x_1, \ldots, x_n$ are *δ-biased* if for every subset $S \subseteq \{1, \ldots, n\}$ it holds that $bias_D(S) \leq \delta$. What is more, we define them as *k-wise δ-biased* if for every subset S such that $|S| \leq k$, $bias_D(S) \leq \delta$.

We will construct a collection H of smaller size, namely, a collection that grows logarithmically with the number of tranparencies n, according to [11]: we choose k to be a power of 2 and we will use a $k \log k$-wise δ-bias probability space R on $n \log k$ random variables. Each function h corresponds to an element of R. Then, as stated in [11], the size of such a probability space is $2^{O(k \log k)} \log n$, i.e., $|H| = 2^{O(k \log k)} \log n$.

We now define the collection H: The $n \log k$ random variables of the sample space are denoted by Y_{ij}, $1 \leq i \leq n$, $1 \leq j \leq \log k$, and take values in $\{0, 1\}$. The choice of the function h determines the values of all random variables Y_{ij}. Each function h is defined as $h(x) = Y_{x1} Y_{x2} \ldots Y_{x \log k}$. Since each Y_{xi} is equal to 0 or 1, for a fixed x, $Y_{x1} Y_{x2} \ldots Y_{x \log k}$ can be viewed as a number between 0 and $k-1$. Namely, each h maps values from $\{1, \ldots, n\}$ to $\{0, \ldots, k-1\}$. This is the case because x takes values from $\{1, \ldots, n\}$ and $Y_{x1} Y_{x2} \ldots Y_{x \log k}$ is treated as a number which takes values from $\{0, \ldots, k-1\}$.

As it was stated previously in Definition 5.1.1.1, a family H of hash

functions $H = \{h : \mathcal{U} \mapsto [m]\}$ is k-wise independent if for every $h \in H$, and for all distinct $x_1, x_2, \cdots, x_k \in \mathcal{U}$ and any k (not necessarily distinct) values $y_1, y_2, \ldots, y_k \in [m]$, it holds:

$Pr[h(x_1) = y_1 \ \& \ h(x_2) = y_2 \ \& \ \ldots \ \& \ h(x_k) = y_k] = m^{-k}$.

Additionally, it can be shown:

$\forall q \ \exists \beta_q$ such that $\forall x_{i1}, x_{i2}, \ldots x_{ik}$, where $i_1, i_2, \ldots, i_k \in \{1, \ldots, n\}$,

$Prob[|\{h(x_1), \ldots, h(x_k)\}| = q] = \beta_q$, for a randomly chosen $h \in H$.

In our case where $m = k$, according to [2] it can be proved that for a k-wise δ-bias family of hash functions and for all $x_1, x_2, \ldots, x_k \in \{1, \ldots, n\}$ and for all $y_1, y_2, \ldots, y_k \in \{0, \ldots, k-1\}$ we have:

$\frac{1}{k^k} - \delta \cdot k^k \leq Prob[h(x_1) = y_1, h(x_2) = y_2, \ldots, h(x_k) = y_k] \leq \frac{1}{k^k} + \delta \cdot k^k$.

We will prove that condition 2 stated in Section 5.2.1 holds, i.e.:

The probability β_q that k different values from $\{1, \ldots, n\}$ to $\{1, \ldots, k\}$ are mapped to q different values is the same for a randomly chosen function $h \in H$ to within $\pm\epsilon$. Namely,

Proposition 5.2.2.6: $\forall q \ \exists \beta_q$ such that $\forall x_{i1}, x_{i2}, \ldots x_{ik}$, where $i_1, i_2, \ldots, i_k \in \{1, \ldots, n\}$, $|Prob[|\{h(x_1), \ldots, h(x_k)\}| = q] - \beta_q| \leq \epsilon$, for a randomly chosen $h \in H$.

Proof. Let us denote by h a k-wise independent hash function. Then as already mentioned, for every $y_1, \ldots, y_k \in \{1, \ldots, k\}$ it holds:

$Pr\left[h(x_1) = y_1, \ldots, h(x_k) = y_k\right] = \frac{1}{k^k}$ Equation (I)

Additionally, let $\tilde{h}$ denote a δ-bias k-wise independent hash function.

Then, for every $y_1, \ldots, y_k \in \{1, \ldots, k\}$ it holds:

$Pr\left[\tilde{h}(x_1) = y_1, \ldots, \tilde{h}(x_k) = y_k\right] \leq \frac{1}{k^k} + \delta \cdot k^k$ Equation (II)

Let us denote:

$h(x_1) = y_1, \ldots, h(x_k) = y_k$ as $h_{1\ldots k}$ and

$\tilde{h}(x_1) = y_1, \ldots, \tilde{h}(x_k) = y_k$ as $\tilde{h}_{1\ldots k}$.

As a result, Equation (I) now is $Pr\left[h_{1\ldots k}\right] = \frac{1}{k^k}$.

Respectively, Equation (II) is $Pr\left[\tilde{h}_{1\ldots k}\right] \leq \frac{1}{k^k} + \delta \cdot k^k$

Then, $Pr\left[|\{\tilde{h}(x_1), \ldots, \tilde{h}(x_k)\}| = q\right] =$

$\sum_{y_1,\ldots,y_k} Pr\left[|\{y_1, \ldots, y_k\}| = q | \tilde{h}_{1\ldots k}\right] \cdot Pr\left[\tilde{h}_{1\ldots k}\right]$ Equation (III)

Let us denote $I^q_{y_1,\ldots,y_k} = \begin{cases} 1 & \text{if } |\{y_1, \ldots, y_k\}| = q \\ 0 & \text{otherwise} \end{cases}$

By substituting in Equation (III) the previous formula and Equation (II) we get:

$Pr\left[|\{\tilde{h}(x_1), \ldots, \tilde{h}(x_k)\}| = q\right] \leq \sum_{y_1,\ldots,y_k} I^q_{y_1,\ldots,y_k} \cdot (\frac{1}{k^k} + \delta \cdot k^k) =$

$\sum_{y_1,\ldots,y_k} I^q_{y_1,\ldots,y_k} \cdot (Pr\left[h_{1\ldots k}\right] + \delta \cdot k^k) =$

$\sum_{y_1,\ldots,y_k} I^q_{y_1,\ldots,y_k} \cdot Pr\left[h_{1\ldots k}\right] + \delta \cdot k^k \cdot \sum_{y_1,\ldots,y_k} I^q_{y_1,\ldots,y_k} =$

$\sum_{y_1,\ldots,y_k} Pr\left[|y_1, \ldots, y_k| = q | h_{1\ldots k}\right] \cdot Pr\left[h_{1\ldots k}\right] + \delta \cdot k^k \cdot \sum_{y_1,\ldots,y_k} I^q_{y_1,\ldots,y_k} =$

$Pr\left[|h(x_1), \ldots, h(x_k)| = q\right] + \delta \cdot k^k \cdot \sum_{y_1,\ldots,y_k} I^q_{y_1,\ldots,y_k} =$

$\beta_q + \delta \cdot k^k \cdot \sum_{y_1,\ldots,y_k} I^q_{y_1,\ldots,y_k} = \beta_q + \delta \cdot k^{2k}$, i.e.,

$Pr\left[|\{\tilde{h}(x_1), \ldots, \tilde{h}(x_k)\}| = q\right] \leq \beta_q + \delta \cdot k^{2k}$

Combining the above result with the following formula that must hold:

$\forall q\ \exists \beta_q$ such that $\forall x_{i1}, x_{i2}, \ldots x_{ik}$, where $i_1, i_2, \ldots, i_k \in \{1, \ldots, n\}$,

$|Prob[|\{h(x_1), \ldots, h(x_k)\}| = q] - \beta_q| \leq \epsilon$, for a randomly chosen $h \in H$,

we get: $\epsilon = \delta \cdot k^{2k}$. If we choose δ to equal $\frac{1}{(2k)^{2k}}$ we get: $\epsilon = \frac{k^{2k}}{(2k)^{2k}} = \frac{1}{2^{2k}}$, which is small. $\square$

Since $|H| = 2^{O(k \log k)} \log n$ in the scheme we constructed, the blocklength of the scheme b grows only logarithmically with the number of shares (transparencies) n.

Theorem 5.2.2.7: *A k out of n visual secret sharing scheme with parameters $b = \log n \cdot 2^{O(k \log k)}$, $a = 2^{-\Omega(k)}$, and $r' = (2^{k-1}!)^{2^{O(k \log k)} \log n}$ can be constructed for any k and any n.*

Proof. This k out of n construction is based on any k out of k visual secret sharing scheme. Let us assume that the latter is the second k out of k scheme described earlier in Section 4.2, with $b = 2^{k-1}$, and $a = \frac{1}{2^{k-1}}$. From Lemma 5.1.1 and Subsection 5.2.1 we get that $b' = b \cdot \ell$ and $a' = a \cdot \beta_k - 2\epsilon(1 + kd/b)$ are the parameters for the new k out of n scheme. Since $\ell = \log n \cdot 2^{O(k \log k)}$, $\beta_k = \frac{e^{-k}}{\sqrt{2\pi k}}$, and $\epsilon \leq \frac{1}{2^{2k}}$ from Proposition 5.2.2.6, we get $b' = 2^{k-1} \cdot \log n \cdot 2^{O(k \log k)} = \log n \cdot 2^{O(k \log k)}$, and $a' = 2^{-\Omega(k)}$. Similarly, since $r = 2^{k-1}!$ and $r' = r^{\ell}$, by substitution it results that $r' = (2^{k-1}!)^{2^{O(k \log k)} \log n}$. □

5.3 A k out of n Scheme - Construction III

5.3.1 Some Preliminaries

Before describing the following constructions of visual secret schemes, let us state some terminology, definitions, and theorems that will prove useful later on.

Definition 5.3.1.1: A *vector space* $V(k, q)$ over the Galois Field $GF(q)$ is the set of all possible k-dimensional vectors over $GF(q)$. As a result,

$|V(k,q)| = q^k$.

Definition 5.3.1.2: Algebraically speaking, a *projective space* over $GF(q)$ denoted $PG(k,q)$ consists of all the non-zero subspaces of $V(k+1,q)$. In a geometric point of view, a *projective space* over a vector space V includes sets of points, lines, planes, and hyperplanes.

A *hyperplane* in a $k+1$-dimensional vector space is a subset of k dimensions which is "flat", i.e., it is described by a degree-one algebraic equation. Sometimes it is called *codimension 1 subspace*. The term dimension refers to the number of vectors the basis of the subspace consists of. If V is finite dimensional then points and hyperplanes are in a 1-1 correspondence as will become clear later on. This is the reason why a hyperplane can be represented by a $(k+1)$-tuple, too, just like a point.

When the vector space V is defined over the Galois Field $GF(q)$, i.e., $V(k+1,q)$, then the *projective space* denoted as $PG(k,q)$ consists of finite sets of the above mentioned elements.

Homogeneous coordinates are a system of coordinates used in Projective Geometry. All the elements of a Projective Geometry can be given homogeneous coordinates and these will be used in the following Sections. Using homogeneous coordinates, if $(x_0, x_1, \ldots, x_k)$ is a point in $PG(k,q)$, then $(\lambda \cdot x_0, \lambda \cdot x_1, \ldots, \lambda \cdot x_k)$ is the same point, where λ is any non-zero element (also called scalar) of $GF(q)$, and $x_i \in GF(q)$. Since there exist $q^{k+1}-1$ non-zero $(k+1)$-tuples, and each point appears $q-1$ times (there are $q-1$ non-zero scalars in $GF(q)$), the number of points is $(q^{k+1}-1)/(q-1) = 1+q+\ldots+q^k$.

One important concept in Projective Geometry is that of *Duality*: as far

as the elements of a Projective Geometry are concerned, there is a certain "symmetry" in definitions and theorems: a point is dual with a hyperplane. As an example, let us assume the projective plane, which is 2-dimensional, where the lines are the hyperplanes: points and lines are dual and can be interchanged in any valid statement to yield another. In 3-dimensional Projective Geometry a point is dual with a plane. In this case, the planes are the hyperplanes of the 3-space.

The property of containment holds when the inner product of the corresponding point and hyperplane, i.e., their homogeneous coordinates, is zero. As an example, in a plane, a point is on a line, or symmetrically, a line passes through a point, if and only if their inner product is zero. In general, we say a point $p = (x_0, \ldots, x_k)$ is **on** a hyperplane $L = (y_0, \ldots, y_k)$ if and only if $x_0 \cdot y_0 + x_1 \cdot y_1 + \ldots + x_k \cdot y_k = 0$.

Since in $PG(k, q)$ the terms hyperplane and point can be interchanged, there are $(q^{k+1} - 1)/(q - 1) = 1 + q + \ldots + q^k$ hyperplanes, too. Additionally, there are $(q^k - 1)/(q - 1)$ points in any hyperplane and respectively, each point is contained in $(q^k - 1)/(q - 1)$ hyperplanes.

Definition 5.3.1.4: In $V(k, q)$ vector space, an *n-arc* is a set of n vectors $(n \geq k + 1)$ with the property that any k of them are linearly independent. An arc is called *complete* when n takes the maximum possible value.

An Alternative Definition for arc 5.3.1.5: In Projective Geometry $PG(k, q)$ an *n-arc* is a set of n points with $n \geq k+1$ such that no $k+1$ points lie on a hyperplane, i.e., at most k points lie on a hyperplane. Symmetrically, it is a set of n hyperplanes no $k + 1$ of which pass through a single point.

In an intuitive way, they form "curved" figures. Loosely speaking, they are sets of points that are not straight -like lines are- in a plane, or "flat" in a three-dimensional space. An n-arc is called *complete* if it is not properly contained in a larger arc and is denoted by $r(k,q)$.

The size of a complete arc has been a major open problem for a long time in Finite Geometry. Some results of research work on this topic are shown in the following table:

$V(k,q)$	k	q	$r(k,q)$
$V(3,q)$	3	*odd*	$q+1$
$V(3,q)$	3	*even*	$q+2$
$V(k,q)$	$3,4,5$	$\neq 3$	$q+1$
$V(k,q)$	$3,4,5$	3	$k+3$
$V(4,q)$	4	>2	$q+1$

For more results and a more detailed inspection of the problem one can refer to [13].

A $(k+1)$-arc in $V(k,q)$ if $k \geq q$ can be constructed in the following way: Let us assume that a basis for $V(k,q)$ consists of the following k vectors: $\vec{a}_1, \vec{a}_2, \ldots, \vec{a}_k$, where $\vec{a}_i = (\omega_{i1}, \omega_{i2}, \ldots, \omega_{ik})$, $\omega_{ij} \in GF(q)$. These k vectors are linearly independent. We construct a new vector, $\vec{a}_{k+1}$, such that $\vec{a}_{k+1} = \sum_{i=1}^{k} \vec{a}_i = (\sum_{i=1}^{k} x_{i1}, \sum_{i=1}^{k} x_{i2}, \ldots, \sum_{i=1}^{k} x_{ik})$. Then, the set $\{\vec{a}_1, \vec{a}_2, \ldots, \vec{a}_k, \vec{a}_{k+1}\}$ consists of $k+1$ vectors any k of them are linearly independent, i.e., we created a $(k+1)$-arc.

In order to create a $(q+1)$-arc in $V(k,q)$ if $k < q$, we use the following method: we take the vectors $(0, \ldots, 0, 1)$ and $(1, \omega_i^1, \ldots, \omega_i^{k-1})$ with ω_i in

$GF(q)$, $1 \leq i \leq q$, as columns in a matrix. Without the first column, this is just a Vandermonde matrix. As is well known, the columns of a Vandermonde matrix consist of q linearly independent vectors. By adding vector $(0, \ldots, 0, 1)$, we have found a (q + 1)-arc.

The following visual secret sharing scheme is described in [3]. Some new concepts must be defined, as well:

Definition 5.3.1.6: In a vector space $V(k, q)$ a *functional* $F(x)$ is defined by the formula $F(\vec{x}) = (\vec{f}, \vec{x}) = f_1x_1 + f_2x_2 + \cdots + f_kx_k$, where $\vec{f} = (f_1, f_2, \ldots, f_k)$ is the corresponding to F vector in $V(k, q)$, and $\vec{x} \in V(k, q)$.

Let us consider k functionals, denoted F_i, $1 \leq i \leq k$. If $\vec{f_i}$, their corresponding vectors in $V(k, q)$, are linearly independent, then, the functionals F_i are also linearly independent. Since the k-dimensional vector space $V(k, q)$ consists of q^k vectors, let us denote a numbering of all the vectors in $V(k, q)$, say $\vec{u}_1, \vec{u}_2, \ldots, \vec{u}_{q^k}$.

Definition 5.3.1.7: Let $n \geq k$. The $n \times q^k$ *representation matrix* S of n functionals $F_i(\vec{u_j})$, for all the vectors in $V(k, q)$, is defined by

$$S_{i,j} = F_i(\vec{u}_j), \quad 1 \leq i \leq n, \quad \textit{and} \quad 1 \leq j \leq q^k. \tag{5.1}$$

In order to construct a representation matrix we do the following: we construct an $n \times k$ matrix B whose rows are the n functionals and another matrix F, with dimension $k \times q^k$, whose columns consist of all the q^k vectors in $V(k, q)$. Then, the multiplication of B and F results in a new $n \times q^k$ matrix named S, which is the representation matrix of these functionals.

Lemma 5.3.1.8: *(a) Let n $(n \geq k)$ functionals in $V(k,q)$, and m $(m \leq k)$ of them be linearly independent, hence, the dimension of their linear span on $V(k,q)$ is m. Then, their corresponding representation matrix S will contain exactly q^{k-m} all-zero columns.*

(b) If $k = m$, and any k out of n functionals are linearly independent, when their representation matrix S is limited to any k rows, then, each vector in $V(k,q)$ occurs exactly once as a column in S.

Proof. a. Let us construct an $n \times k$ matrix B whose rows are the n functionals, where each m $(m \leq k)$ are linearly independent vectors in $V(k,q)$. Additionally, let us denote $null(B)$ the dimension of the null-space of B (i.e., the dimension of the set of all vectors $\vec{r}$ in $V(k,q)$ for which $B\vec{r} = \vec{0}$) and $rank(B)$ the dimension of B. Then, according to the Rank - Nullity Theorem it holds that $rank(B) + null(B) = k$. But $rank(B) = m$, hence, $null(B) = k - m$. As a result, the representation matrix S that is constructed by B and all the vectors in $V(k,q)$ will contain q^{k-m} all-zero columns.

b. Let us construct the two matrices B and F as described earlier which are used for the construction of the representation matrix S and limit matrix B to any k rows, named B'. We will show by contradiction that each vector in $V(k,q)$ occurs exactly once as a column in S.

Let us suppose that this is not the case, i.e., there exist $\vec{r}_1$ and $\vec{r}_2 \in V(k,q)$ that appear as columns in F, where $\vec{r}_1 \neq \vec{r}_2$, such that $B'\vec{r}_1 = \vec{r}_3$ (equation I) and $B'\vec{r}_2 = \vec{r}_3$ (equation II), $\vec{r}_3 \in V(k,q)$. But B' consists of linearly independent vectors, hence, it is invertible, i.e., $(B')^{-1}$ exists. Then, from equations I and II it follows that $\vec{r}_1 = (B')^{-1}\vec{r}_3$ and $\vec{r}_2 = (B')^{-1}\vec{r}_3$, i.e., $\vec{r}_1 = \vec{r}_2$, which is a contradiction to the initial hypothesis. Hence, all the

columns of S when limited to any k rows consist of q^k different vectors, i.e., each vector in $V(k,q)$ occurs exactly once as a column in S. □

5.3.2 A k out of n scheme construction:

In order to create a strong k out of n visual secret sharing scheme (see Definition 1.4.4) we do the following:

1. We choose k, q such that $r(k-1,q) \geq n$ and $r(k,q) \geq n$ for $V(k-1,q)$ and $V(k,q)$ respectively.

2. Let $V(k,q)$ consist of the vectors $\vec{u}_1, \vec{u}_2, \ldots, \vec{u}_{q^k}$. We discard the all-zero vector as well as all the vectors that are scalar multiples of each other. Geometrically speaking, in that way the remaining vectors are all the distinct $(q^k-1)/(q-1)$ hyperplanes in $PG(k-1,q)$. Let $\vec{v}_1, \vec{v}_2, \ldots, \vec{v}_{(q^k-1)/(q-1)}$ be that reduced set of vectors.

3. We choose n functionals on $V(k,q)$, i.e., $F_1, F_2, \ldots, F_n$, such that any k of them are linearly independent. This is the reason why we chose $r(k,q) \geq n$.

4. We name S the $n \times q^k$ representation matrix of the functionals F_i, $1 \leq i \leq n$ on all the q^k vectors of $V(k,q)$ $\vec{u}_1, \vec{u}_2, \ldots, \vec{u}_{q^k}$. By A_1 we denote the $n \times (q^k-1)/(q-1)$ representation matrix of the reduced set of vectors $\vec{v}_1, \vec{v}_2, \ldots, \vec{v}_{(q^k-1)/(q-1)}$.

5. We replace all the non-zero values in A_1 by 1. The matrices that are obtained by permuting the columns of A_1 form the collection $\mathcal{C}_1$. Since

A_1 is an $n \times (q^k - 1)/(q-1)$-dimension matrix, $|\mathcal{C}_1| = (q^k - 1)/(q-1)!$.

6. Accordingly, we choose n functionals $G'_1, G'_2, \ldots, G'_n$ on $V(k-1, q)$ with the property that any $(k-1)$ of them are linearly independent. We increase the number of their dimension by 1, by adding the zero value and get functionals $G_1, G_2, \ldots, G_n$ i.e., $G_i(x_1, \ldots, x_{k-1}, 0) := G'_i(x_1, \ldots, x_{k-1})$, $1 \leq i \leq n$. The dimension of $V(k-1, q)$ is $k-1$, hence, any $k-1$ of the functionals G_i, $q \leq i \leq n$ are linearly independent, whereas any k of them are linearly dependent.

7. We name T the $n \times q^k$ representation matrix of the functionals G_i, $1 \leq i \leq n$ on all the q^k vectors of $V(k, q)$ $\vec{u}_1, \vec{u}_2, \ldots, \vec{u}_{q^k}$. By A_0 we denote the $n \times (q^k - 1)/(q-1)$ representation matrix of the reduced set of vectors $\vec{v}_1, \vec{v}_2, \ldots, \vec{v}_{(q^k-1)/(q-1)}$.

8. We replace all the non-zero values in A_0 by 1. The matrices that are obtained by permuting the columns of A_0 form the collection $\mathcal{C}_0$. Since A_0 is an $n \times (q^k - 1)/(q-1)$-dimension matrix, $|\mathcal{C}_0| = (q^k - 1)/(q-1)!$.

Theorem 5.3.2.1: *The above scheme is a maximal contrast k out of n visual secret scheme with parameters $b = (q^k - 1)/(q-1)$, $h = 1$, $l = 0$, $r = |\mathcal{C}_0| = |\mathcal{C}_1| = (q^k - 1)/(q-1)!$, and contrast $a = 1$.*

Proof. In order to get S we constructed the representation matrix of functionals F_i, $1 \leq i \leq n$, which have the property that each k of them are linearly independent. Because of that, according to Lemma 5.3.1.8, each vector in $V(k, q)$ occurs exactly once as a column of the representation matrix, when limited to any k rows. The same applies to the all-zero vector, as well, which

is the result of the dot product of the functionals and the all-zero vector in $V(k,q)$. However, in order to obtain A_1 from S we remove the all-zero vector, hence, A_1 does not have an all-zero column when limited to any k rows. As a result, $l = 0$.

As already mentioned, the functionals G_i, $1 \leq i \leq n$, used for the construction of T have the property that each $k-1$ of them are linearly independent but any k of them is not. Hence, the dimension of the linear span of any k functionals of them is $k-1$. By Lemma 5.3.1.8, the representation matrix T of these functionals when limited to any k rows will contain exactly $q^{k-m} = q^{k-(k-1)} = q$ all-zero columns.

In order to create a column of matrix A_0, we calculate the inner product of a vector in $V(k,q)$ to all the functionals $G_1, G_2, \ldots, G_n$. Therefore, an all-zero column in matrix A_0 is obtained as follows: since the last coordinate of the functionals is zero, the vectors that their inner product with the functionals is zero are of the form $(0,\ldots,0,x)$, where $x \in GF(q)$. But in order to obtain A_0 we remove all scalar multiples, all but one of these vectors, i.e., we remove $q-1$ vectors, including the all-zero one. As a result, there is only one column that is all zeros in matrix A_0 when limited to any k rows, i.e., $h = 1$.

As a result, the contrast of the scheme is $contrast_{SN} = a = h - l = 1 - 0 = 1$ and the loss of contrast $contrastloss_{SN} = \frac{h-l}{b} = \frac{q-1}{q^k-1}$.

Respectively, $contrast_{VVT} = \frac{h-l}{h+l} = 1$ and $contrastloss_{VVT} = \frac{h-l}{b(h+l)} = \frac{q-1}{q^k-1}$.

About the security of the scheme:

The $(q^k-1)/(q-1)$ vectors indexing the columns of A_0 and A_1 can be considered as the hyperplanes of $PG(k-1,q)$ and the n functionals indexing

their rows respectively as n points in $PG(k-1,q)$. As mentioned before, each point is contained in $(q^{k-1}-1)/(q-1)$ hyperplanes, i.e., their corresponding inner products will produce exactly $(q^{k-1}-1)/(q-1)$ zeros. As a result, the number of zeros in each row of both A_0 and A_1 is a fixed number.

According to Definition 5.3.1.5, functionals F_i, $1 \leq i \leq n$, form an n-arc, i.e., a set $\mathcal{A}$ of n points in $PG(k-1,q)$ with the property that every hyperplane is incident with at most $k-1$ points. Hence, if we restrict A_1 to any $k-1$ rows there will be exactly one all-zero column. This holds because the hyperplanes are distinctly represented, i.e., they are represented only once and each $k-1$ points are incident with only one hyperplane.

Algebraically speaking now, if we limit A_0 in any $k-1$ rows, since the dimension of the span of the functionals is $k-1$, each vector will appear in the columns of A_0 exactly once, hence, there is exactly one all-zero column in it, too. Since for all $(k-1) \times (q^k-1)/(q-1)$ submatrices of A_0 and A_1 the above facts hold, there is no way that someone can conclude that any $k-1$ shares come from a white or a black pixel. The same holds for shares that correspond to less than $k-1$ rows. □

As we will later see in Theorem 7.1.11, the blocklength of the scheme is almost optimal.

Example 5.3.2.2: Let us create a 3 out of 4 visual secret sharing scheme according to the above described construction: we choose $q=5$, $k=3$ and $n=4$. As a result, the vector space will be $V(k,q)=V(3,5)$, and in such a case, since $k<q$ and q odd, $r(k,q)=q+1=6$. Hence, we can find $n=4$ vectors in $V(3,5)$ such that any 3 of them are linearly independent. These

vectors will be the functionals F_i $(1 \leq i \leq 4)$ of the construction. We will use $F_1 = [001]$, $F_2 = [010]$, $F_3 = [100]$, and $F_4 = [111]$.

In $V(3,5)$ vector space there are $q^k = 5^3 = 125$ vectors. By discarding the all-zero vector and the vectors that are a scalar multiple of each other we get $(q^k - 1)/(q - 1) = (5^3 - 1)/(5 - 1) = 31$ vectors, which are the points of $PG(k-1, q) = PG(2, 5)$. These are: (001), (010), (011), (012), (013), (014), (100), (101), (102), (103), (104), (110), (111), (112), (113), (114), (120), (121), (122), (123), (124), (130), (131), (132), (133), (134), (140), (141), (142), (143), and (144).

As for the vector space $V(k-1, q) = V(2, 5)$, the same holds for $r(k - 1, q) = r(2, 5)$, i.e., since $k - 1 \leq q - 1$ and q odd, $r(k-1, q) = q + 1 = 6$. Hence, we can find $n = 4$ vectors in $V(2, 5)$ such that each 2 of them are linearly independent. These vectors will be the functionals G_i $(1 \leq i \leq 4)$ of the construction. We will use $G'_1 = [01]$, $G'_2 = [11]$, $G'_3 = [21]$, and $G'_4 = [31]$. We extend them by one coordinate and we get $G_1 = [010]$, $G_2 = [110]$, $G_3 = [210]$, and $G_4 = [310]$. Each three of these new functionals are linearly dependent, while each two of them are linearly independent.

In order to construct matrix A_1 we index its rows by the F_i functionals and its columns by the 31 vectors that were not discarded in the previous step, i.e., the points of $PG(2, 5)$. Hence, A_1 has dimension $n \times (q^k - 1)/(q - 1) = 4 \times 31$. Each element of $A_1[i, j]$, $1 \leq i \leq 4$ and $1 \leq j \leq 31$ is the inner product of the corresponding vector-row and the corresponding vector-column:

$$A_1 = \begin{bmatrix} 1\,0\,1\,2\,3\,4\,0\,1\,2\,3\,4\,0\,1\,2\,3\,4\,0\,1\,2\,3\,4\,0\,1\,2\,3\,4\,0\,1\,2\,3\,4 \\ 0\,1\,1\,1\,1\,1\,0\,0\,0\,0\,0\,1\,1\,1\,1\,1\,2\,2\,2\,2\,2\,3\,3\,3\,3\,3\,4\,4\,4\,4\,4 \\ 0\,0\,0\,0\,0\,0\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1 \\ 1\,1\,2\,3\,4\,0\,1\,2\,3\,4\,0\,2\,3\,4\,0\,1\,3\,4\,0\,1\,2\,4\,0\,1\,2\,3\,0\,1\,2\,3\,4 \end{bmatrix}$$

By substituting all non-zero elements by 1 we get:

$$A_1 = \begin{bmatrix} 1\,0\,1\,1\,1\,1\,0\,1\,1\,1\,1\,0\,1\,1\,1\,1\,0\,1\,1\,1\,1\,0\,1\,1\,1\,1\,0\,1\,1\,1\,1 \\ 0\,1\,1\,1\,1\,1\,0\,0\,0\,0\,0\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1 \\ 0\,0\,0\,0\,0\,0\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1 \\ 1\,1\,1\,1\,1\,0\,1\,1\,1\,1\,0\,1\,1\,1\,0\,1\,1\,1\,0\,1\,1\,1\,0\,1\,1\,1\,0\,1\,1\,1\,1 \end{bmatrix}$$

The $n \times (q^k - 1)/(q - 1) = 4 \times 31$ binary matrices generated by the permutation of A_1 form the collection $\mathcal{C}_1$. As one can see, $|\mathcal{C}_1| = (q^k - 1)/(q - 1)! = 31!$.

The same procedure is followed to get collection $\mathcal{C}_0$: In order to construct matrix A_0 we index its rows by the G_i functionals and its columns by the 31 vectors that were not discarded, i.e., the points of $PG(2, 5)$. Hence, A_0 has dimension $n \times (q^k - 1)/(q - 1) = 4 \times 31$. Each element of $A_0[i, j]$, $1 \leq i \leq 4$ and $1 \leq j \leq 31$ is the inner product of the corresponding vector-row and the corresponding vector-column.

$$A_0 = \begin{bmatrix} 0\,1\,1\,1\,1\,1\,0\,0\,0\,0\,0\,1\,1\,1\,1\,1\,2\,2\,2\,2\,2\,3\,3\,3\,3\,3\,4\,4\,4\,4\,4 \\ 0\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,2\,2\,2\,2\,2\,3\,3\,3\,3\,3\,4\,4\,4\,4\,4\,0\,0\,0\,0\,0 \\ 0\,1\,1\,1\,1\,1\,2\,2\,2\,2\,2\,3\,3\,3\,3\,3\,4\,4\,4\,4\,4\,0\,0\,0\,0\,0\,1\,1\,1\,1\,1 \\ 0\,1\,1\,1\,1\,1\,3\,3\,3\,3\,3\,4\,4\,4\,4\,4\,0\,0\,0\,0\,0\,1\,1\,1\,1\,1\,2\,2\,2\,2\,2 \end{bmatrix}$$

By substituting all non-zero elements by 1 we get:

$$A_0 = \begin{bmatrix} 0\,1\,1\,1\,1\,1\,0\,0\,0\,0\,0\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1 \\ 0\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,0\,0\,0\,0\,0 \\ 0\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,0\,0\,0\,0\,0\,1\,1\,1\,1\,1 \\ 0\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,0\,0\,0\,0\,0\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1 \end{bmatrix}$$

The $n \times (q^k - 1)/(q - 1) = 4 \times 31$ binary matrices generated by the permutation of A_0 form the collection $\mathcal{C}_0$. As one can see, $|C_0| = (q^k - 1)/(q - 1)! = 31!$.

As a result, the contrast of the scheme is $contrast_{SN} = a = h - l = 1$ and the loss of contrast $contrastloss_{SN} = \frac{q-1}{q^k-1} = \frac{1}{31}$. Respectively, $contrast_{VVT} = \frac{h-l}{h+l} = 1$ and $contrastloss_{VVT} = \frac{h-l}{b(h+l)} = \frac{1}{31}$.

The above scheme has parameters $b = 31$, $h = 1$, $l = 0$, $a = 1$, and $r = 31!$. It is a maximal contrast visual secret sharing scheme.

If $n - 1$ is a prime power, hence can be used as a Galois field basis, one can take $q = n - 1$. In such a case, the blocklength of this k out of n scheme equals $((n - 1)^k - 1)/(n - 2)$.

The above scheme can be used to construct a maximal (i.e., $l = 0$) k out of k visual secret sharing scheme, too. In this case one can take $q = 2$, since $r(k, q) = k + 1$ if $k \geq q$. In this case, by substituting q by 2 we get: $b = (q^k - 1)/(q - 1) = (2^k - 1)/(2 - 1) = 2^k - 1$, $a = \frac{h-l}{b} = \frac{1}{2^k-1}$, and $r = b! = (2^k - 1)!$. The parameters of the first k out of k construction presented in Section 4.1, were $b = 2^k$, $a = \frac{1}{2^k}$, and $r = 2^k!$. Hence, the parameters in this construction are slightly improved compared to the ones of the k out of k scheme described in Section 4.1.

Example 5.3.2.3: We will construct a 3 out of 3 visual secret sharing scheme for $k = n = 3$ and $q = 2$ following the above instructions:

Let $F_1 = [001]$, $F_2 = [010]$, and $F_3 = [100]$ whose corresponding vectors are linearly independent in $V(k, q) = V(3, 2)$. Let $G'_1[01]$, $G'_2 = [10]$, and $G'_3 = [11]$, any two of them are linearly independent vectors in $V(k-1, q) = V(2, 2)$. We increase their coordinates by one and get $G_1 = [010]$, $G_2 = [100]$, and $G_3 = [110]$.

The $V(3, 2)$ vector space consists of the following $2^3 = 8$ vectors: (000), (001), (010), (011), (100), (101), (110), and (111). Since there are no scalar multiples we remove only the all-zero vector (000). The rest $(q^k-1)/(q-1) = (2^3-1)/(2-1) = 7$ vectors will be used to construct A_0 and A_1. Since there no other elements except 0 and 1 in $GF(2)$ there in no need for any substitution, hence:

$$A_0 = \begin{bmatrix} 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 \end{bmatrix} \quad A_1 = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

As one can see, its blocklength is $b = \frac{q^k-1}{q-1} = 7$, $h = 1$, $l = 0$, $r = \frac{q^k-1}{q-1}! = 7!$. Hence, the parameters of the scheme are $[b; h, l; r] = [7; 1, 0; 7!]$ and it is a maximal contrast scheme.

As a result, its contrast is $contrast_{SN} = a = h - l = 1$ and the loss of contrast $contrastloss_{SN} = \frac{h-l}{b} = \frac{1}{7}$. Respectively, $contrast_{VVT} = \frac{h-l}{h+l} = 1$ and $contrastloss_{VVT} = \frac{h-l}{b(h+l)} = \frac{1}{7}$.

5.4 A k out of n Scheme - Construction IV

5.4.1 A k out of n scheme construction:

In order to create a strong k out of n visual secret sharing scheme (see Definition 1.4.4) we do the following:

1. We choose k, q such that $r(k,q) \geq n+1$.

2. Similarly to Construction II, we choose $n+1$ functionals on $V(k,q)$, i.e., $G, F_1, F_2, \ldots, F_n$, such that any k of them are linearly independent. This is the reason why we chose $r(k,q) \geq n+1$.

3. Let $\vec{u}_j$, $1 \leq j \leq q^{k-1}$ be the vectors on $V(k,q)$ such that $G(\vec{u}_j) = 0$. We construct the $n \times q^{k-1}$ representation matrix A_0 by using these $\vec{u}_j$ vectors and the following formula:

$$S_{ij} = F_i(\vec{u}_j), \quad 1 \leq i \leq n, \quad 1 \leq j \leq q^{k-1} \tag{5.2}$$

4. We replace all the non-zero values in A_0 by 1. The matrices that are obtained by permuting the columns of A_0 form the collection $\mathcal{C}_0$. Since A_0 is an $n \times q^{k-1}$-dimensional matrix, $|\mathcal{C}_0| = q^{k-1}!$.

5. Accordingly, let $\vec{v}_j$, $1 \leq j \leq q^{k-1}$ be the vectors on $V(k,q)$ such that $G(\vec{v}_j) = 1$. We construct the $n \times q^{k-1}$ representation matrix A_1 by using these $\vec{u}_j$ vectors and the following formula:

$$T_{ij} = F_i(\vec{v}_j), \quad 1 \leq i \leq n, \quad 1 \leq j \leq q^{k-1} \tag{5.3}$$

6. We replace all the non-zero values in A_1 by 1. The matrices that are obtained by permuting the columns of A_1 form the collection $\mathcal{C}_1$. Since A_1 is an $n \times q^{k-1}$-dimensional matrix, $|\mathcal{C}_1| = q^{k-1}!$.

Theorem 5.4.2.1: The above scheme is a maximal contrast k out of n visual secret sharing scheme with parameters $b = q^{k-1}$, $h = 1$, $l = 0$, $a = h - l = 1$, and $|\mathcal{C}_0| = |\mathcal{C}_1| = q^{k-1}!$.

Proof. Let us consider a vector $\vec{x} = (x_1, x_2, \ldots, x_k)$ in $V(k, q)$, and let us suppose that we want to calculate the inner product of it with all the q^k vectors in $V(k, q)$, denoted $\vec{y} = (y_1, y_2, \ldots, y_k)$, $y_i \in GF(q)$. For every q vectors in a row, i.e., vectors $(y_1, y_2, \ldots, y_{k-1}, 0)$ to $(y_1, y_2, \ldots, y_{k-1}, q-1)$ this function is injective, hence, each number $\{0, \ldots, q-1\}$ appears exactly once. Since there are q^{k-1} such "cycles" of q vectors in $V(k, q)$, each number in $GF(q)$ appears q^{k-1} times as the result of the inner product of $\vec{x}$ with all the q^k vectors in $V(k, q)$. This means that matrices A_0 and A_1 are $n \times q^{k-1}$ dimensional, hence, $b = q^{k-1}$.

From Lemma 5.3.1.8 we get that each vector appears exactly once as a column when the dot product of k linearly independent functionals with all the vectors of $V(k, q)$ is calculated. In the construction of A_0, its columns are indexed by the vectors $\vec{x}$ in $V(k, q)$ that $G(\vec{x}) = 0$ whereas in A_1, the vectors that index the columns of it are those in $V(k, q)$ that $G(\vec{x}) = 1$. There cannot be a vector $\vec{x}$ such that $G(\vec{x}) = 0$ and $G(\vec{x}) = 1$. Hence, since the all-zero vector indexes one column in A_0, an all-zero column appears in A_0, and there is no all-zero column in A_1, i.e., $h = 1$ and $l = 0$.

As a result, the contrast of the scheme is $contrast_{SN} = h - l = 1$ and the

loss of contrast $contrastloss_{SN} = \frac{h-l}{b} = \frac{1}{q^{k-1}}$. Respectively, $contrast_{VVT} = \frac{h-l}{h+l} = 1$ and $contrastloss_{VVT} = \frac{h-l}{b(h+l)} = \frac{1}{q^{k-1}}$.

For the security of the scheme: The vectors that index the rows of A_0 are k linearly independent, and as a result they are $k-1$ linearly independent, too. What is more, as already mentioned, A_0 and A_1 consist of q^{k-1} columns. Hence, when A_0 is limited to $k-1$ rows, from Lemma 5.3.1.8 we get that each vector in $V(k-1,q)$ is calculated exactly once as a column of the matrix. The same holds for A_1, too. Hence, the two matrices, A_0 and A_1, when restricted to any $k-1$ rows, they both consist of the same columns. Since this fact holds for any $k-1$ rows, it follows that A_0 and A_1 consist of the same columns, but in a different order.

Since A_0 and A_1 are $n \times q^{k-1}$-dimensional matrices, $|\mathcal{C}_0| = |\mathcal{C}_1| = q^{k-1}!$. □

As we will later see in Theorem 7.1.11, the blocklength of the scheme is almost optimal.

Example 5.4.2.2: We will construct a 3 out of 4 scheme and we choose $k = 3$, $n = 4$, and $q = 4 = 2^2$. As a result, the vector space will be $V(k,q) = V(3,4)$, and in such a case, since $k < q$ and q even, $r(k,q) = q+2 = 4+2 = 6$. Hence, we can find $n+1 = 4+1 = 5$ vectors in $V(3,4)$ such that any 3 of them are linearly independent. These vectors will be the functionals G, F_i, $1 \leq i \leq 4$ of the construction. We will use $G = (001)$, $F_1 = (010)$, $F_2 = (100)$, $F_3 = (11a)$, and $F_4 = (baa)$. Galois Field $GF(4) = GF(2^2)$ consists of the following elements $\{0, 1, a, b = a^2\}$ and the addition and multiplication tables respectively are depicted below:

$+$	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

$*$	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

The $q^{k-1} = 4^{3-1} = 4^2 = 16$ vectors $\vec{x}$ in $V(3,4)$ such that $G(\vec{x}) = 0$ are the following: (000),(010), $(0a0)$, $(0b0)$, (100), (110), $(1a0)$, $(1b0)$, $(a00)$, $(a10)$, $(aa0)$, $(ab0)$, $(b00)$, $(b10)$, $(ba0)$, and $(bb0)$.

The $q^{k-1} = 4^{3-1} = 4^2 = 16$ vectors $\vec{x}$ in $V(3,4)$ such that $G(\vec{x}) = 1$ are the following: (001),(011), $(0a1)$, $(0b1)$, (101), (111), $(1a1)$, $(1b1)$, $(a01)$, $(a11)$, $(aa1)$, $(ab1)$, $(b01)$, $(b11)$, $(ba1)$, and $(bb1)$.

In order to construct matrix A_0 we index its rows by the F_i, $1 \leq i \leq 4$, functionals and its columns by the 16 vectors $\vec{x}$ in $V(3,4)$ with the property that $G(\vec{x}) = 0$. Hence, A_0 has dimensions $n \times q^{k-1} = 4 \times 16$. Each element of $A_0[i,j]$, $1 \leq i \leq 4$, $1 \leq j \leq 16$ is the inner product of the corresponding vector-row and the corresponding vector-column:

$$A_0 = \begin{bmatrix} 0 & 1 & a & b & 0 & 1 & a & b & 0 & 1 & a & b & 0 & 1 & a & b \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & a & a & a & a & b & b & b & b \\ 0 & 1 & a & b & 1 & 0 & b & a & a & b & 0 & 1 & b & a & 1 & 0 \\ 0 & a & b & 1 & b & 1 & 0 & a & 1 & b & a & 0 & a & 0 & 1 & b \end{bmatrix}$$

By substituting all non-zero elements by 1 we get:

$$A_0 = \begin{bmatrix} 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

The $n \times q^{k-1} = 4 \times 16$ binary matrices generated by the permutation of A_0 form the collection $\mathcal{C}_0$. As one can see, $|\mathcal{C}| = q^{k-1}! = 16!$.

The same procedure is followed to get collection $\mathcal{C}_1$: In order to construct matrix A_1 we index its rows by the F_i, $1 \leq i \leq 4$ functionals, and its columns by the 16 vectors $\vec{x}$ in $V(3,4)$ with the property that $G(\vec{x}) = 1$. Hence, A_1 has dimensions $n \times q^{k-1} = 4 \times 16$. Each element of $A_1[i,j]$, $1 \leq i \leq 4$, $1 \leq j \leq 16$ is the inner product of the corresponding vector-row and the corresponding vector-column:

$$A_1 = \begin{bmatrix} 0 & 1 & a & b & 0 & 1 & a & b & 0 & 1 & a & b & 0 & 1 & a & b \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & a & a & a & a & b & b & b & b \\ a & b & 0 & 1 & b & a & 1 & 0 & 0 & 1 & a & b & 1 & 0 & b & a \\ a & 0 & 1 & b & 1 & b & a & 0 & b & 1 & 0 & a & 0 & a & b & 1 \end{bmatrix}$$

By substituting all non-zero elements by 1 we get:

$$A_1 = \begin{bmatrix} 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}$$

The $n \times q^{k-1} = 4 \times 16$ binary matrices generated by the permutation of A_0 form the collection $\mathcal{C}_0$. As one can see, $|\mathcal{C}| = q^{k-1}! = 16!$.

As a result, the contrast of the scheme is $contrast_{SN} = h - l = 1$ and the loss of contrast $contrastloss_{SN} = a = \frac{h-l}{b} = \frac{1}{16}$. Respectively, $contrast_{VVT} = \frac{h-l}{h+l} = 1$ and $contrastloss_{VVT} = \frac{h-l}{b(h+l)} = \frac{1}{16}$.

The above scheme has parameters $b = 16$, $h = 1$, $l = 0$, $a = \frac{1}{16}$, and $r = 16!$. It is a maximal contrast visual secret sharing scheme.

Remarks 5.4.2.3: If $k = n$ and $q = 2$ the scheme that is constructed has the same parameters as the k out of k visual secret sharing scheme in Construction II, described in [2]. What is more, if n is a prime power, we can choose $q = n$. In such a case, the blocklength of the scheme will equal $q^{k-1} = n^{k-1}$.

Chapter 6

Summary of the Schemes presented so far:

A table with the parameters of all the visual secret sharing schemes for specific values of n and k that were presented in [2] follows:

k	n	b	h	l	r	a	Described in
2	2	4	2	0	6	1/2	2.1
3	3	4	1	0	4!	1/4	2.2
4	4	9	1	0	9!	1/9	2.3
2	6	4	2	1	6	1/4	2.4

A table with the parameters of all the visual secret sharing schemes for specific values of k described in [2] and [3] is the following:

k	n	b	h	l	r	a	Described in	Remarks
2	n	n	$n-1$	$n-2$	n	$1/n$	3.1	
2	n	n	1	0	n	$1/n$	3.1	
2	n	m	$\frac{m}{2}$	$\frac{m}{2}-1$	$m!$	1/m	3.2	m s.t. $\binom{m}{m/2} \geq n$
3	n	$2n-2$	n	$n-1$	$(2n-2)!$	$\frac{1}{2n-2}$	3.3	

A table with the parameters of all the k out of k visual secret sharing schemes presented in [2] and [3] follows:

k	n	b	h	l	r	a	Described in	Remarks
k	k	2^k	2	1	$2^k!$	$\frac{1}{2^k}$	4.1	
k	k	2^{k-1}	1	0	$2^{k-1}!$	$\frac{1}{2^{k-1}}$	4.2	
k	k	2^{k-1}	1	0	$2^{k-1}!$	$\frac{1}{2^{k-1}}$	5.3	special case of a k out of n scheme

A table with the parameters of the four k out of n visual secret sharing schemes that were described in [2] and [3] follows:

k	n	b	h	l	r	a	Described in
k	n	$n^k 2^{k-1}$	*	*	$(2^{k-1}!)^{n^k}$	$2(2e)^{-k}/\sqrt{2\pi k}$	5.1
k	n	$\log n \cdot 2^{O(k \log k)}$	*	*	$(2^{k-1}!)^{2^{O(k \log k)} \log n}$	$2^{-\Omega(k)}$	5.2
k	n	$\frac{q^{k-1}}{q-1}$	1	0	$\frac{q^{k-1}}{q-1}!$	$\frac{q-1}{q^k-1}$	5.3
k	n	q^{k-1}	1	0	$q^{k-1}!$	$\frac{1}{q^{k-1}}$	5.4

* Since in both constructions different families of hash functions can be used, it is not possible to calculate the number of the white subpixels in the schemes

Chapter 7

Bounds on k out of n Visual Secret Sharing Schemes

7.1 Some General Concepts

In this Section several properties of k out of n visual secret sharing schemes will be introduced. In order to prove them, we will use the method of induction, i.e., the break of a k out of n scheme into two $k-1$ out of $n-1$ schemes. Before the theorems that define bounds about the blocklength are presented, some definitions much be given:

Definition 7.1.1: Let A be an $n \times b$ matrix and i one of its rows, any one will do. Then the *1-restriction* (respectively *0-restriction*) matrix of A considering a row i of it, is a new matrix $\tilde{A}_1$ (respectively $\tilde{A}_0$) which is obtained by removing the i-th row and by limiting the rest of the matrix to the columns where row i has value 1 (respectively 0). As a result, $\tilde{A}_1$ (respectively $\tilde{A}_0$) is a submatrix of A consisting of $n-1$ rows, whereas its

number of columns depends on the weight of row i. It is obvious that the sum of the number of columns in both $\tilde{A}_1$ and $\tilde{A}_0$ equals b.

Let us now consider a k out of n visual secret sharing scheme $S = (\mathcal{C}_0, \mathcal{C}_1)$ with parameters $[b; h, l]$. In all matrices in both $\mathcal{C}_0$ and $\mathcal{C}_1$, each i-th row, $i \in \{1, 2, \ldots, n\}$, can be considered as a binary vector $\vec{v}$. Then, the concepts of *0-restriction* and *1-restriction* can be extended to each collection $\mathcal{C}_0$ and $\mathcal{C}_1$: they can be defined as the subsets containing the corresponding submatrices. What is more, if we denote b_0 the number of zeros in $\vec{v}$, and b_1 the number of ones respectively, then it follows that $b = b_0 + b_1$.

In order to decompose S the following procedure is followed:

1. Let a k out of n scheme $S = (\mathcal{C}_0, \mathcal{C}_1)$ with parameters $[b; h, l]$.

2. We fix a vector $\vec{v}$ that appears as an i-th row in a matrix of $\mathcal{C}_0$ and hence of $\mathcal{C}_1$.

3. Let us consider all the matrices in $\mathcal{C}_0$ (respectively $\mathcal{C}_1$) that their i-th row has the same weight as $\vec{v}$. We denote this subset $\tilde{\mathcal{C}}_0$ (respectively $\tilde{\mathcal{C}}_1$).

4. We denote D_0 (respectively D_1) the 0-restriction of $\tilde{\mathcal{C}}_0$ (respectively $\tilde{\mathcal{C}}_1$).

5. Symmetrically, we denote E_0 (respectively E_1) the 1-restriction of $\tilde{\mathcal{C}}_1$ (respectively $\tilde{\mathcal{C}}_0$). Note that in this case we have swapped 0 with 1.

Lemma 7.1.2: *The above construction is a $k-1$ out of $n-1$ visual secret sharing scheme denoted $S_1 = (D_0, D_1)$ with parameters $[b_0; h, l]$.*

Proof. By construction, the submatrices D_0 and D_1 have b_0 columns and $n-1$ rows, namely, the blocklength of the scheme is b_0.

Since the newly formed matrix is a 0-restriction, it does not matter if the i-th row is included or not in the k rows that are chosen each time; the "or" of any $k-1$ rows is not affected and there will be h zeros in D_0 and l zeros in D_1.

About the security of the scheme: By the definition of S it holds that for each matrix in $\mathcal{C}_0$, when limited to less than k rows, there exists one exactly the same in $\mathcal{C}_1$, with the same frequency. Let us denote A_0 and A_1 these matrices.

Case 1: The i-th row is included in the $k-1$ or less rows: when we remove it from both A_0 and A_1, the new matrices are also indistinguishable when limited to $k-2$ (or less) rows.

Case 2: The i-th row is not included in the $k-1$ or less rows: then, A_0 and A_1 are also indistinguishable when limited to $k-2$ or less rows.

Hence, $S_1 = (D_0, D_1)$ is a $k-1$ out of $n-1$ visual secret sharing scheme with parameters $[b_0; h, l]$. □

Definition 7.1.3: Let us consider a k out of n visual secret sharing scheme $S = (\mathcal{C}_0, \mathcal{C}_1)$ with parameters $[b; h, l]$ and its restrictions $\tilde{\mathcal{C}_0}$ and $\tilde{\mathcal{C}_1}$. Let $\vec{u}$ be the "or" of any $k-1$ rows (except the i-th row) of any matrix in either $\tilde{\mathcal{C}_0}$ or $\tilde{\mathcal{C}_1}$. We denote z_{max} the maximal number of $z(\vec{u})$, i.e., the largest number of zeros obtained by the "or" of any $k-1$ rows of any matrix in either $\tilde{\mathcal{C}_0}$ or $\tilde{\mathcal{C}_1}$. Respectively, let z_{min} denote the minimal number of $z(\vec{u})$. If the scheme is uniform, then it holds that $z_{max} = z_{min}$.

Lemma 7.1.4: *Let us consider a k out of n visual secret sharing scheme $S = (\mathcal{C}_0, \mathcal{C}_1)$ with parameters $[b; h, l]$, which is generated by A_0 and A_1. If*

$z_{max} - z_{min} < h - l$, then the scheme $S_2 = (E_0, E_1)$ as defined above is a a $k-1$ out of $n-1$ visual secret sharing scheme with parameters $[b_1; z_{min} - l, z_{max} - h]$. Additionally, if the original scheme S is uniform, i.e., $z_{max} = z_{min}$, then the scheme (E_0, E_1) is also uniform.

Proof. By construction, the submatrices in E_0 and E_1 have b_1 columns and $n - 1$ rows, namely, the blocklength of the scheme is b_1.

As already stated, E_0 is the 1-restriction of the set $\tilde{\mathcal{C}}_1$. Let $\tilde{E}_0$ be a member of $\mathcal{E}_0$. If we follow this procedure step by step, we can denote $\tilde{A}_1$ the $n - 1 \times b$ matrix that is obtained if we remove the i-th row from A_1, a matrix in $\tilde{\mathcal{C}}_1$. Then, we get $\tilde{E}_0$ by restricting $\tilde{A}_1$ to the columns that in the i-th row of A_1 are ones. As one can see, $\tilde{A}_1$ is an $(n - 1) \times b$ submatrix of $n \times b$ A_1 and in turn, $\tilde{E}_0$ is an $(n - 1) \times b_1$ submatrix of $\tilde{A}_1$.

Let us denote z the number of zeros in the "or" of any $k - 1$ rows in $\tilde{A}_1$. Some of them correspond to zero coordinates in the i-th row, denoted z_0, and some to one coordinates respectively, denoted z_1. Hence, $z = z_0 + z_1$.

As one can see, z_0 is the number of zeros in the "or" of any k rows in A_1. What is more, z_1 is the number of zeros in the "or" of any $k - 1$ rows in $\tilde{E}_0$.

By definition $z_{min} \leq z$, hence $z_{min} \leq z_0 + z_1$. Additionally, from the definition of the visual secret sharing scheme, for any matrix in $\mathcal{C}_1$ it holds that $z_0 \leq l$. Hence, $z_{min} \leq l + z_1$, i.e., $z_{min} - l \leq z_1$. This means that the number of zeros of the "or" of any $k - 1$ rows of $\tilde{E}_0$ is at least $z_{min} - l$, i.e., it complies with condition 1 of a visual secret sharing scheme (*Result 1*).

Respectively, let E_1 be the 1-restriction of the set $\tilde{\mathcal{C}}_1$. Let $\tilde{E}_1$ be a member of $\mathcal{E}_1$. We denote $\tilde{A}_0$ the $n - 1 \times b$ matrix that is obtained if we remove the i-th row from A_0. Then, we get $\tilde{E}_1$ by restricting $\tilde{A}_0$ to the columns that in

the i-th row of A_0 were ones. As one can see, $\tilde{A}_0$ is an $n-1 \times b$ submatrix of $n \times b$ A_0 and in turn, $\tilde{E}_1$ is an $n-1 \times b_1$ submatrix of $\tilde{A}_0$.

We denote z the number of zeros in the "or" of any $k-1$ rows in $\tilde{A}_0$. Some of them correspond to zero coordinates in the i-th row, denoted z_0, and some to one coordinates respectively, denoted z_1. Hence, $z = z_0 + z_1$.

As one can see, z_0 is the number of zeros in the "or" of any k rows in A_0. What is more, z_1 is the number of zeros in the "or" of any $k-1$ rows in $\tilde{E}_1$.

By definition $z \leq z_{max}$, hence $z_0 + z_1 \leq z_{max}$. Additionally, from the definition of the visual secret sharing scheme, for any matrix in $\mathcal{C}_0$ it holds that $h \leq z_0$. Hence, $h + z_1 \leq z_{max}$, i.e., $z_1 \leq z_{max} - h$. This means that the number of zeros of the "or" of any $k-1$ rows of $\tilde{E}_1$ is at most $z_{max} - h$, i.e., it complies with condition 2 of a visual secret sharing scheme (*Result 2*).

Taking into account Results 1 and 2, and if $z_{max} - z_{min} < h - l$, then, $S_2 = (\mathcal{E}_0, \mathcal{E}_1)$ satisfy the first two conditions of a visual secret sharing scheme.

About the security of the scheme: By the definition of S it holds that for each matrix in $\mathcal{C}_0$, when limited to less than k rows, there exists one in $\mathcal{C}_1$, with the same frequency. Let us denote A_0 and A_1 these matrices.

Case 1: The i-th row is included in the $k-1$ or less rows: when we remove it from both A_0 and A_1, the new matrices are also indistinguishable when limited to $k-2$ (or less) rows.

Case 2: The i-th row is not included in the $k-1$ or less rows: then, A_0 and A_1 are also indistinguishable when limited to $k-2$ or less rows.

Hence, $S_2 = (\mathcal{E}_0, \mathcal{E}_1)$ is a $k-1$ out of $n-1$ visual secret sharing scheme with parameters $[b_1; z_{min} - l, z_{max} - h]$.

Let us suppose that $S = (\mathcal{C}_0, \mathcal{C}_1)$ is *uniform*, i.e., the Hamming weight

of any $s < k$ transparencies depends only on the number of transparencies that are used and not from the collection that the matrix belongs to. So, let $s < k$ and C be a $(s+1) \times b$ matrix, submatrix of collection $\mathcal{C}_0$. Let $\tilde{\mathcal{C}}$ denote a $s \times b$ 1-restriction submatrix of C and E a $s \times b_1$ submatrix of $\tilde{\mathcal{C}}$. Let z denote the number of zeros of the "or" of the s rows of $\tilde{\mathcal{C}}$. In the C matrix, some of these z zeros correspond to zero coordinates in the i-th row, denoted z_0, and some to one coordinates respectively, denoted z_1. Hence, $z = z_0 + z_1$. As one can see, z_0 is the number of zeros in the "or" of any s rows in C. What is more, z_1 is the number of zeros in the "or" of any s rows in E. But z and z_0 depend only on s since S is uniform. As a result, z_1 depends only on s and $S_2 = (\mathcal{E}_0, \mathcal{E}_1)$ is uniform, too. □

An example follows:

Example 7.1.5: Let a 3 out of 5 scheme $S = (\mathcal{C}_0, \mathcal{C}_1)$ with parameters $[8; 3, 2]$ that is generated by the following A_0 and A_1 matrices respectively:

$$A_0 = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{bmatrix} \quad A_1 = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

The 0-restriction of the above matrices will be constructed by considering the second row, i.e., $i = 2$. Then, the sets $\mathcal{D}_0$ and $\mathcal{D}_1$ are obtained by the permutation of the columns of the following submatrices:

$$\tilde{D}_0 = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix} \quad \tilde{D}_1 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

A 2 out of 4 visual secret sharing scheme $S_1 = (\mathcal{D}_0, \mathcal{D}_1)$ is constructed with parameters $[4; 3, 2]$.

Similarly, the sets $\mathcal{E}_0$ and $\mathcal{E}_1$ are obtained by the permutation of the columns of the following submatrices:

$$\tilde{E}_0 = \begin{bmatrix} 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 \end{bmatrix} \quad \tilde{E}_1 = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix}$$

A 2 out of 4 visual secret sharing scheme $S_2 = (\mathcal{E}_0, \mathcal{E}_1)$ is constructed with parameters $[4; 1, 0]$.

Theorem 7.1.6: *For any k out of n visual secret sharing scheme with parameters $[b; h, l]$ it holds that $b \geq (h - l)2^{k-1}$.*

Proof. This Theorem will be proved for a k out of k uniform scheme, since one can take any k out of the n rows of a k out of n scheme in order to construct a k out of k one. Hence, a k out of k visual secret sharing scheme $S = (\mathcal{C}_0, \mathcal{C}_1)$ will be used, which has parameters $[b; h, l; r]$. We will use induction in k in order to prove the Theorem:

For $k = 1$ it holds that $b \geq (h - l)2^{k-1}$, since $b \geq (h - l)$.

Let us assume that the statement holds for any $k - 1$ out of $k - 1$ visual secret sharing scheme, i.e., $b \geq (h - l)2^{(k-1)-1}$, or $b \geq (h - l)2^{k-2}$.

Let us assume a k out of k scheme with parameters $[b; h, l]$ that is generated by two boolean matrices A_0 and A_1. According to Lemmas 7.1.2 and 7.1.4, if we take the 0-restriction and 1-restriction of these two matrices, for example on the first row of them, two $k-1$ out of $k-1$ schemes are generated with parameters $[b_0; h, l]$ and $[b_1; z-l, z-h]$, respectively.

From the induction step we get that $b_0 \geq (h-l)2^{k-2}$ and $b_1 \geq (z-l-(z-h))2^{k-2}$, or $b_1 \geq (h-l)2^{k-2}$. From the construction of the two $k-1$ out of $k-1$ visual secret sharing schemes it holds that $b = b_0 + b_1$. Using the above relations we get that $b \geq (h-l)2^{k-2} + (h-l)2^{k-2}$, hence, $b \geq (h-l)2^{k-1}$.

In order to prove the Theorem for any k out of k scheme S, and not only for schemes that are generated by two matrices, the following technique is used:

From the collections $\mathcal{C}_0$ and $\mathcal{C}_1$ of S we construct two boolean $n \times (b \cdot r)$ matrices A'_0 and A'_1 which are the concatenation of all the matrices in these collections respectively. Then, a new scheme S' is generated by them, with parameters $[r \cdot b; r \cdot h, r \cdot l]$ and the Theorem holds since $r \cdot b \geq r \cdot (h-l) \cdot 2^{k-1}$, which implies that $b \geq (h-l) \cdot 2^{k-1}$. □

Theorem 7.1.7: *1. Let $S = (\mathcal{C}_0, \mathcal{C}_1)$ be a uniform k out of n scheme with parameters $[b; h, l]$. If we denote $b(k, n)$ the minimal blocklength of S, then $b(k, n) \geq 2 \cdot b(k-1, n-1)$.*

2. Additionally, if g is the smallest integer such that $\binom{g}{\lfloor g/2 \rfloor} \geq n - k + 2$, then $b(k, n) \geq g \cdot 2^{k-2}$.

3. If $k \neq n$ then $b(k, n) \geq 3 \cdot 2^{k-2}$.

Proof. From Lemmas 7.1.2 and 7.1.4 we already know that a k out of n

visual secret sharing scheme S with parameters $[b; h, l]$ can be decomposed into two $k-1$ out of $n-1$ visual secret sharing schemes with parameters $[b_0; h, l]$ and $[b_1; z-l, z-h]$. If $b(k-1, n-1) = min\{b_0, b_1\}$, i.e., the minimal blocklength of the two $k-1$ out of $n-1$ schemes that are produced by S. Since $b = b_0 + b_1$, then $b(k, n) \geq 2 \cdot b(k-1, n-1)$.

In order to prove the second statement, the method of induction will be used. For $k = 2$ the statement is:

If g is minimal with respect to $\binom{g}{\lfloor g/2 \rfloor} \geq n$, then $b(2, n) \geq g$.

Hence, we consider a 2 out of n visual secret sharing scheme $S = (\mathcal{C}_0, \mathcal{C}_1)$. Its blocklength will be denoted by b. The security of the scheme implies that for any row in a matrix A_0 in collection $\mathcal{C}_0$ there exists a matrix A_1 in collection $\mathcal{C}_1$ containing the same row. Additionally, by the definition of the scheme, for any matrix A_0 (respectively A_1) in $\mathcal{C}_0$ (respectively $\mathcal{C}_1$) collection, the "or" denoted by $\vec{v}_0$ (respectively $\vec{v}_1$) of any k out of its n rows must satisfy $z(\vec{v}_0) \geq h$ (respectively $z(\vec{v}_1) \leq l$). Two identical rows produce the maximum value of $z(\vec{v}_i)$, $i \in \{0, 1\}$. Since the contrast of the scheme is defined by the equation $contrast = \frac{h-l}{h+l}$, there cannot be two identical rows in any matrix of the $\mathcal{C}_1$ collection, or else there would be no distinction between a white and a black pixel (recall that this is a 2 of out of 2 visual secret sharing scheme). Let us denote by x the number of ones in each row (transparency) of a matrix in A_1. Then it must hold $\binom{b}{x} \geq n$. We can safely assume that x can take any value from 1 to $b-1$ depending on the scheme. Since $\binom{b}{\lfloor b/2 \rfloor} \geq \binom{b}{x}$ for every $1 \leq x \leq b$, implies that the number g will be the minimal one to satisfy the relation $\binom{g}{\lfloor g/2 \rfloor} \geq n$, hence, g is less or equal to b, and for $k = 2$ the statement holds.

Let us assume that the statement holds for $k-1$, $n-1$, i.e., if g is the smallest integer such that $\binom{g}{\lfloor g/2 \rfloor} \geq (n-1)-(k-1)+2$, then $b(k-1,n-1) \geq g \cdot 2^{k-1-2}$, namely, if g is the smallest integer such that $\binom{g}{\lfloor g/2 \rfloor} \geq n-k+2$, then $b(k-1,n-1) \geq g \cdot 2^{k-3}$.

For a k out of n scheme, using statement 1, we get: if g is the smallest integer such that $\binom{g}{\lfloor g/2 \rfloor} \geq n-k+2$, then $b(k,n) \geq 2 \cdot b(k-1,n-1)$. From the inductive step it holds that if g is minimal with respect to $\binom{g}{\lfloor g/2 \rfloor} \geq n-k+2$, then $b(k-1,n-1) \geq g \cdot 2^{k-3}$. By combining the two relations we get that if g is minimal with respect to $\binom{g}{\lfloor g/2 \rfloor} \geq n-k+2$, then $b(k,n) \geq g \cdot 2^{k-2}$.

About the third statement: If $k \neq n$, then $n-k+2$ equals at least 3, hence, $\binom{g}{\lfloor g/2 \rfloor} \geq 3$. The minimal g for the latter inequality to hold is 3, hence, $b(k,n) \geq 3 \cdot 2^{k-2}$. □

We repeat the following definition before stating the next Theorem:

Definition 7.1.8: Let a k out of n visual secret sharing scheme generated by matrices A_0 and A_1. We limit A_0 and A_1 to any s rows ($s < k$), namely, $i_1 < i_2 < \ldots < i_s$ and $j_1 < j_2 < \ldots < j_s$ in $\{1, \ldots, n\}$ respectively. If these two submatrices of A_0 and A_1 contain the same columns in a different order, we call A_0 and A_1 *systematic*. What is more, the scheme that is generated by them is called a *strong* k out of n visual secret sharing scheme.

Theorem 7.1.9: *If a k out of n visual secret sharing scheme $S = (\mathcal{C}_0, \mathcal{C}_1)$ with parameters $[b; h, l]$ is uniform, then any pair of matrices A_0 and A_1 in $\mathcal{C}_0$ and $\mathcal{C}_1$ respectively are systematic. What is more, the scheme that is constructed by the permutation of the columns of A_0 and A_1 is a strong k out*

of n visual secret sharing scheme with the same parameters as S.

Proof. In order to prove the Theorem, induction in k will be used.

For $k = 2$: Since the scheme is uniform, by definition the number of ones in the "or" of any $s < k$ rows depends only on the number s. Hence, for $s = 1$, the number of ones is the same in all the rows of any matrix in either collection $\mathcal{C}_0$ or $\mathcal{C}_1$. This means, that if we choose any two matrices, e.g., A_0 from $\mathcal{C}_0$ and A_1 from $\mathcal{C}_1$, they contain the same elements when limited to only one row (any single row), only in a different order. Hence, in this case the pair A_0 and A_1 is systematic.

As an inductive step, let us assume that the Theorem holds for any uniform $k-1$ out of $n-1$ scheme.

Next, we will prove the Theorem for any uniform k out of n visual secret sharing scheme. Let $S = (\mathcal{C}_0, \mathcal{C}_1)$ be a uniform k out of n scheme, and let A_0 be a matrix in the collection $\mathcal{C}_0$ and A_1 a matrix in the collection $\mathcal{C}_1$ respectively.

At first, let us consider that A_0 and A_1 have a common row, denoted i. From Lemmas 7.1.2 and 7.1.4 we get that S can be decomposed with respect to row i into two $k-1$ out of $n-1$ visual secret sharing schemes. As a result, A_0 will be decomposed into two matrices, D_0 and E_1, and A_1 into D_1 and E_0, respectively. By the inductive step we get that D_0 and D_1 are systematic. The same holds for E_0 and E_1. Since A_0 (respectively A_1) can be reconstructed from D_0 and E_1 (respectively D_1 and E_0), by adding the common i row, the A_0 and A_1 pair is also systematic.

If A_0 and A_1 do not have a common row, we will proceed as follows: two subsets of matrices can be used, one from $\mathcal{C}_0$ and one from $\mathcal{C}_1$. Let

$A_{0.1}, A_{0.2}, \ldots, A_{0.t}$ be the subset of $\mathcal{C}_0$ and $A_{1.1}, A_{1.2}, \ldots, A_{1.t}$ the one from $\mathcal{C}_1$ respectively. The matrix $A_{0.1}$ to be A_0 and matrix $A_{1.t}$ to be A_1. The security of the scheme implies that for any row in a matrix A_0 in collection $\mathcal{C}_0$ there exists a matrix A_1 in collection $\mathcal{C}_1$ containing the same line. Taking this under consideration, the matrices that the collections consist of have the following property: the $A_{1.j}$ matrix, $j \in \{1, \ldots, t\}$, has at least one common row with $A_{0.j}$ and $A_{0.j+1.}$. In this way, a chain of matrices with common rows is created starting from A_0 and ending with A_1. Figure 7.1 depicts the described method.

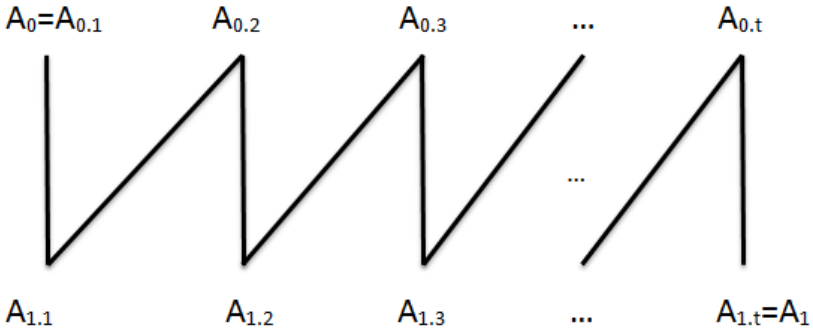


Figure 7.1: A chain of matrices with common rows

Since each pair of matrices $A_{0.j}$ and $A_{1.j}$, $i \in \{1, \ldots, t\}$ have at least one row in common, the statement holds for each pair of them, i.e., the corresponding pair of matrices is systematic. This property is transitive, hence, the original pair A_0 and A_1 is systematic.

As a result, if a k out of n scheme $S = (\mathcal{C}_0, \mathcal{C}_1)$ is uniform, then, any two matrices from collection $\mathcal{C}_0$ and $\mathcal{C}_1$ are systematic. As a result, the scheme that they generate is a strong k out of n scheme with the same parameters as S. □

The next Theorem gives a bound on the blocklength of maximal contrast visual secret sharing schemes, i.e., schemes with parameters $[b; h, 0]$.

Theorem 7.1.10: *Consider a maximal contrast k out of n visual secret sharing scheme $S = (\mathcal{C}_0, \mathcal{C}_1)$ with parameters $[b; h, 0]$. Then, it holds that $b \geq h \cdot \binom{n}{k-1}$.*

Proof. From the definition of the scheme we know that when limited to k (or less) rows any matrix in $\mathcal{C}_0$ consists of at least h all-zero columns. Hence, from the security of the scheme we get that when restricted to $k-1$ rows, all matrices from both $\mathcal{C}_0$ and $\mathcal{C}_1$ collections will have at least h all-zero columns.

What is more, since $l = 0$ it follows that in any matrix in $\mathcal{C}_1$ there are no more than $k-1$ zeros in any of their columns. Considering all the above mentioned, the blocklength b of the scheme must be at least h times the number of combinations of $(k-1)$-subsets of $\{1, \ldots, n\}$, i.e., $b \geq h \cdot \binom{n}{k-1}$. □

Remark 7.1.11: If we fix k, for large n, $\binom{n}{k-1}$ is approximately equal to $n^{k-1}/(k-1)!$. As a result, the maximal contrast schemes described in Constructions III and IV (Sections 5.3.2 and 5.4.2 respectively) are quite optimal as far as the blocklength of the scheme is concerned.

Constructions III and IV of k out of n visual secret sharing schemes (Sections 5.3.2 and 5.4.2, respectively) are both based on Projective Geometry, which is characterized, as mentioned, by the Principle of Duality. What is more, we have already created in Section 3.1 the dual of a 2 out of n visual secret sharing scheme. However, the dual of a k out of n scheme is not always a visual secret sharing scheme itself. As an example, let us consider two 2 out of 2 visual secret sharing schemes $S^1 = (\mathcal{C}_0^1, \mathcal{C}_1^1)$ and $S^2 = (\mathcal{C}_0^2, \mathcal{C}_1^2)$, both

with parameters $[4; 2, 1; 4!]$, which are generated by the following matrices respectively:

$$A_0^1 = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix} \qquad A_1^1 = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{bmatrix}$$

and

$$A_0^2 = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix} \qquad A_1^2 = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \end{bmatrix}$$

The union of S_1 and S_2 denoted $S = (\mathcal{C}_0, \mathcal{C}_1)$ is a valid 2 out of 2 visual secret sharing scheme with parameters $[4; 2, 1; 2 \cdot 4!]$. Let us consider now the dual scheme of it, $S^* = (\mathcal{C}_0^*, \mathcal{C}_1^*)$. This is not a valid visual secret sharing scheme: the dual of A_0^2 which is in the $\mathcal{C}_0^*$ collection and the dual of A_1^1 which is in the $\mathcal{C}_1^*$ collection are the following:

$$A_0^* = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \end{bmatrix} \in \mathcal{C}_0^* \qquad A_1^* = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \end{bmatrix} \in \mathcal{C}_1^*$$

As one can see, the "or" of the 2 rows in both matrices yield one zero and three ones, i.e., they are exactly the same, hence, there is no difference between a black and a white pixel.

However, when the scheme is uniform this is not the case as Theorem 7.1.9 states. In order to prove it, the following Lemma is needed:

Lemma 7.1.12: *Let us consider a uniform k out of n visual secret sharing scheme $S = (\mathcal{C}_0, \mathcal{C}_1)$ with parameters $[b; h, l]$. We denote by A a $k \times b$ submatrix of any matrix in $\mathcal{C}_0$ or $\mathcal{C}_1$. Additionally, let us denote $\vec{u}_1$, $\vec{u}_2$ two vectors in $V(k, 2)$ that appear as columns in A. If w is the number of coordinates*

that $\vec{u}_1$, $\vec{u}_2$ differ, and $e(\vec{u}_i)$, $i \in \{1,2\}$ is the number of times $\vec{u}_i$ appears as a column in A, then the expression $e(\vec{u}_1) + (-1)^{1+w} e(\vec{u}_2)$ is independent of A.

Proof. We will use induction in w.

For $w = 1$, i.e., the two vectors differ in only one coordinate (an example is shown in Figure 7.2): without loss of generality let us consider that $\vec{u}_1$ and $\vec{u}_2$ differ in their first coordinate. If we remove the first row from A, we get a $k-1 \times b$ matrix A'. In this case, $e(\vec{u}_1) + e(\vec{u}_2)$ is the number of times the $k-1$ common coordinates that are left appear as columns in A'. Since the scheme is uniform, from Theorem 7.1.8 we know that all of its matrices are systematic, and hence, $e(\vec{u}_1) + e(\vec{u}_2)$ depends only on $k-1$, i.e., is independent of A.

For $w = 2$: Without loss of generality, let $\vec{u}_1$ and $\vec{u}_2$ differ in the first two coordinates - an example is depicted in the following figure. Additionally, let us denote by $\vec{u}_3$ another vector in $V(k,2)$, which differs in the first coordinate with $\vec{u}_1$ and in the second coordinate with $\vec{u}_2$. Since $\vec{u}_3$ differs by only one coordinate with $\vec{u}_1$ and $\vec{u}_2$ respectively, from step 1 we get that $e(\vec{u}_1) + e(\vec{u}_3)$ and $e(\vec{u}_2) + e(\vec{u}_3)$ are independent of A. The same holds for their difference, $e(\vec{u}_1) + e(\vec{u}_3) - e(\vec{u}_2) - e(\vec{u}_3)$, i.e., $e(\vec{u}_1) - e(\vec{u}_2)$ is independent of A.

Inductive step: Let us consider that the formula is true for $w = 2i+1$ and for $w = 2i+2$.

Then, for $w = 2i+3$ we get: as done for $w = 1$ and $w = 2$ we assume that $\vec{u}_1$ and $\vec{u}_2$ differ in the first three coordinates. Let us consider another vector, $\vec{u}_3$ in $V(k,2)$ that differs in the first two coordinates with $\vec{u}_1$ and in one coordinate (the third one) with $\vec{u}_2$. From the two first steps of the induction

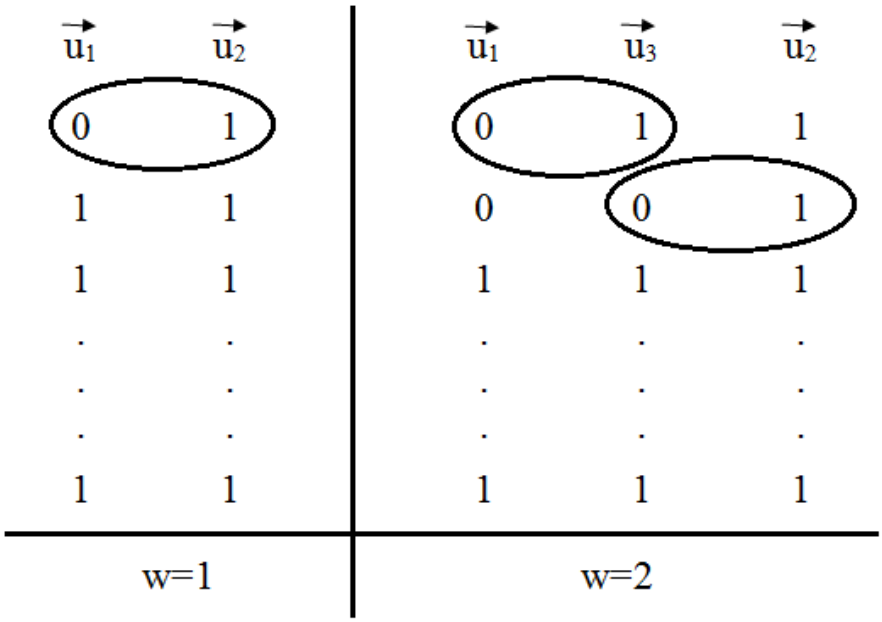


Figure 7.2: Visual representation for $w = 1$ and $w = 2$

we get that $e(\vec{u}_1) - e(\vec{u}_3)$ is independent of A and $e(\vec{u}_2) + e(\vec{u}_3)$ is independent of A, too. As a result, their sum, $e(\vec{u}_1) - e(\vec{u}_3) + e(\vec{u}_2) + e(\vec{u}_3) = e(\vec{u}_1) + e(\vec{u}_2)$ is independent of A. Hence, for $w = 2i + 3$ the formula holds.

For $w = 2i + 4$ we get: as done in all previous cases we assume that $\vec{u}_1$ and $\vec{u}_2$ differ in the first four coordinates. Let us consider another vector, $\vec{u}_3$ in $V(k, 2)$ that differs in the first two coordinates with $\vec{u}_1$ and in two coordinates (the third and forth one) with $\vec{u}_2$. From the induction step we get that $e(\vec{u}_1) - e(\vec{u}_3)$ is independent of A and $e(\vec{u}_3) - e(\vec{u}_2)$ is independent of A, too. As a result, their sum, $e(\vec{u}_1) - e(\vec{u}_3) + e(\vec{u}_3) - e(\vec{u}_2) = e(\vec{u}_1) - e(\vec{u}_2)$ is independent of A. Hence, for $w = 2i + 4$ the formula holds.

As a result, the expression $e(\vec{u}_1) + (-1)^{1+w} e(\vec{u}_2)$ is independent of A. □

Theorem 7.1.14: *Consider a k out of n uniform visual secret sharing*

scheme $S = (\mathcal{C}_0, \mathcal{C}_1)$. Let $\mathcal{F}$ (respectively $\mathcal{G}$) denote the set of all the matrices in $\mathcal{C}_0$ (respectively $\mathcal{C}_1$) in which we have replaced the ones by zeros and vice versa.

a. For k even, the scheme $(\mathcal{F}, \mathcal{G})$ is a uniform k out of n visual secret sharing scheme with parameters $[b; z + h, z + l]$.

b. For k odd, the scheme $(\mathcal{G}, \mathcal{F})$ is a uniform k out of n visual secret sharing scheme with parameters $[b; z - l, z - h]$.

Proof. a. For k even: Let A_0 denote a matrix in $\mathcal{C}_0$ and A_1 a matrix in $\mathcal{C}_1$. Additionally, let A'_0 and A'_1 be their limitations to any k rows. By $\vec{u}_1$ we denote the "all-one" vector and by $\vec{u}_2$ the "all-zero" vector in $V(k, 2)$ which may appear as columns in A'_0 and A'_1. Since k is even, from Lemma 7.1.10 we get that $z = e(\vec{u}_1) - e(\vec{u}_2)$ is independent of A'_0 and A'_1.

Since the number of zeros in the "or" of the rows in A'_0 is at least h, the same holds for the number of all-zero vectors in it, i.e., the number of all-zero vectors in A'_0 is at least h, i.e., $e(\vec{u}_2) \geq h$. Hence, the number of all-ones columns in A'_0 is at least $z + h$.

Symmetrically, since the "or" of the rows in A'_1 is at most l, the same holds for the number of all-zero vectors in it, i.e., the number of all-zero vectors in A'_1 is at most l, i.e., $e(\vec{u}_2) \leq l$. Hence, the number of all-ones columns in A'_1 is at most $z + l$.

We interchange the one coordinates with zero and vice versa in all matrices of $\mathcal{C}_0$ and $\mathcal{C}_1$ and get the sets $\mathcal{F}$ and $\mathcal{G}$ respectively. Then, all the matrices in $\mathcal{F}$ when limited to k rows have at least $z + h$ all-zero columns, hence, the "or" of any k rows results is at least $z + h$ zeros. Similarly, all the matrices in $\mathcal{G}$ when limited to k rows have at most $z + l$ all-zero columns, hence, the

"or of any k rows results is at most $z + l$ zeros. Since $z + h > z + l$ and considering all the above mentioned, it follows that $(\mathcal{F}, \mathcal{G})$ is a k out of n uniform visual secret sharing scheme with parameters $[b; z + h, z + l]$.

b. For k odd: Let A_0 denote a matrix in $\mathcal{C}_0$ and A_1 a matrix in $\mathcal{C}_1$. Additionally, let A'_0 and A'_1 be their limitations to any k rows. By $\vec{u}_1$ we denote the "all-one" vector and by $\vec{u}_2$ the "all-zero" vector in $V(k, 2)$ which appear as columns in A'_0 and A'_1. Since k is odd, from Lemma 7.1.10 we get that $z = e(\vec{u}_1) + e(\vec{u}_2)$ is independent of A'_0 and A'_1.

Since the number of zeros in the "or" of the rows in A'_0 is at least h, the same holds for the number of "all-zero" vectors in it, i.e., the number of "all-zero" vectors in A'_0 is at least h, i.e., $e(\vec{u}_2) \geq h$. Hence, the number of "all-one" columns in A'_0 is at most $z - h$.

Symmetrically, since the "or" of the rows in A'_1 is at most l, the same holds for the number of "all-zero" vectors in it, i.e., the number of "all-zero" vectors in A'_1 is at most l, i.e., $e(\vec{u}_2) \leq l$. Hence, the number of "all-one" columns in A'_1 is at least $z - l$.

We interchange the one coordinates with zero and vice versa in all matrices of $\mathcal{C}_0$ and $\mathcal{C}_1$ and get the sets $\mathcal{F}$ and $\mathcal{G}$ respectively. Then, all the matrices in $\mathcal{F}$ when limited to any k rows have at most $z - h$ all-zero columns, hence, the "or" of any k rows results is at most $z - h$ zeros. Similarly, all the matrices in $\mathcal{G}$ when limited to any k rows have at least $z - l$ "all-zero" columns, and as a result, the "or of any k rows results is at least $z - l$ zeros. Since $z - l > z - h$ and considering all the above mentioned, it follows that $(\mathcal{G}, \mathcal{F})$ is a k out of n uniform visual secret sharing scheme with parameters $[b; z - l, z - h]$.

□

Chapter 8

Extensions

The basic model of considering only black and white messages (written texts or images) can be further extended to continuous tone images, coloured images, etc. What is more, efficient techniques can be used to conceal the very fact of the use of Visual Cryptography. Some of these techniques are explained in the following Sections.

8.1 Continuous Tone Visual Encryption Problem

In the case of a continuous tone image where pixels have gray scaling ranging from 0 to 255, one first technique can be followed: For each pixel with g level of gray, a $16 \times 16 (= 256)$ array can be used which will consist of g black and $256 - g$ white subpixels. Each one of them, in turn, can be encrypted using one of the techniques mentioned in the previous chapters.

However, a more efficient solution can be used. It is a 2 out of 2 scheme.

This time each original pixel is not divided into subpixels, but it is represented by a circle which is half black and half white. It is the relative angle between the circles in the two transparencies that determines the colour of each pixel. It ranges from medium gray which represents white (when the two circles have zero relative angle) to completely black, representing black (their relative angle is 180^o). Figure 8.1 from [2] depicts an example of the sharing of a medium gray coloured pixel:

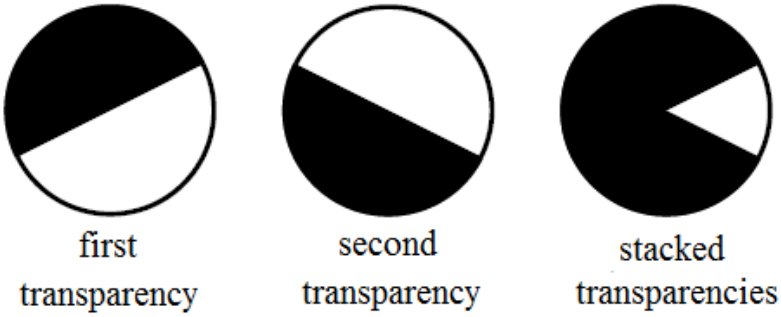


Figure 8.1: Sharing a medium gray coloured pixel

Additionally, a random absolute angle is used for each circle in both transparencies while preserving the specified relative angle between them. As a result, each transparency will look gray and can reveal no information about the original hidden message. The only effect of the encryption is that when the message is revealed, it will look darker than the original one.

8.2 Extended Visual Cryptography

An interesting version of the original problem is the following: the two transparencies that are required to reveal the hidden message are not random

looking patterns but ordinary - black and white - images with a visual meaning. In this way, it is difficult for someone to even imagine that putting these two images on top of one another a hidden message is disclosed. What is more, it is easier for the dealer to recognize each transparency. This problem is solved by the use of Extended Visual Cryptography, an example of which one can see in Figure 8.2 taken from [30].

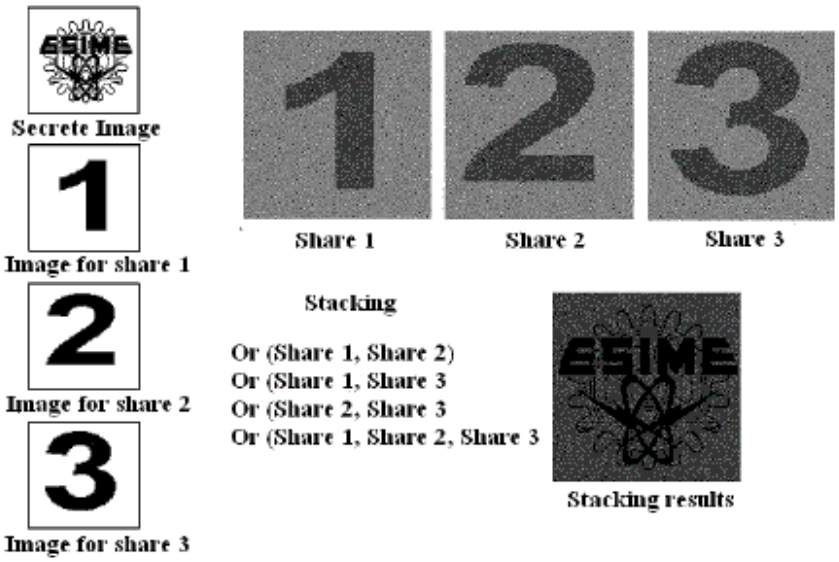


Figure 8.2: A 2 out of 3 scheme of extended visual cryptography

A 2 out of 2 extended visual scheme is described: Each pixel is divided into 4 subpixels, hence, we consider 2×4 matrices. Since the two transparencies to be combined are common images like a cat or a boat, the colour of their pixels must be taken under consideration, too.

As a result, in order to represent a white pixel, one of the top row combinations of Figure 8.3 (taken from [2]) must be used, depending on the colour of the pixels of the two image-transparencies. In order to represent a black pixel, a choice from the bottom row combinations must be used. For exam-

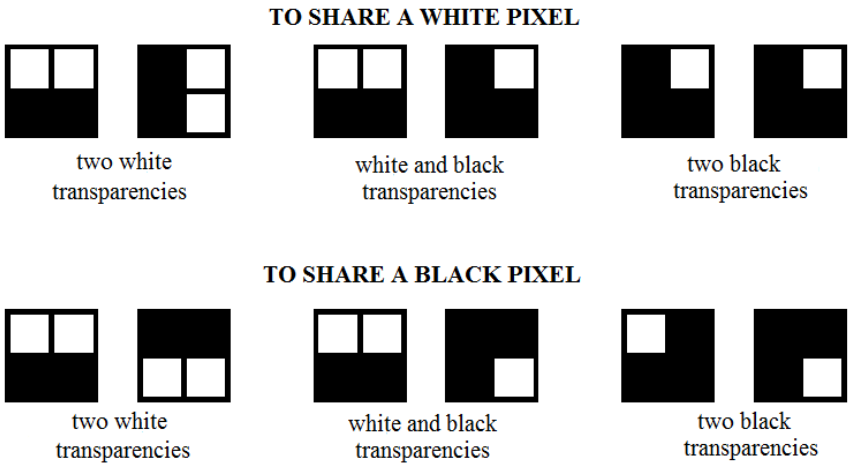


Figure 8.3: To share a black or a white pixel

ple, if the colour of the final pixel is white and the corresponding pixels are white, too, then the upper left combination of subpixels is used.
The matrices that represent a white pixel are the permutations of the following:

$$\begin{bmatrix} 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix} \qquad \begin{bmatrix} 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 \end{bmatrix} \qquad \begin{bmatrix} 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 \end{bmatrix}$$

two white shares white and black shares two black shares

Similarly, the matrices that represent a black pixel are the permutations of the following:

$$\begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix} \qquad \begin{bmatrix} 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix} \qquad \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix}$$

two white shares white and black shares two black shares

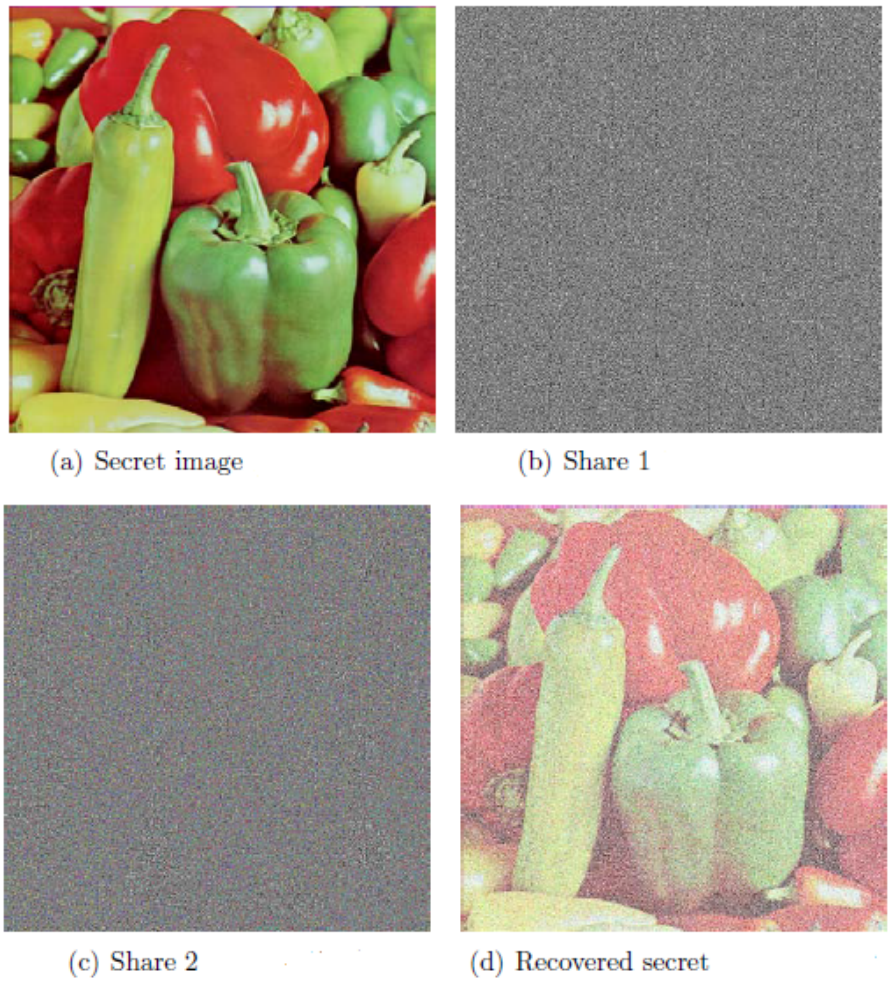
As one can see, in the two transparencies a white pixel is represented by two black and two white subpixels, whereas a black pixel is represented by three black and one white subpixel. In the resulting image, a white pixel is represented by one white and three black subpixels, i.e., $h = 1$, and a black one by four black subpixels, i.e., $l = 0$. What is more, it is obvious that not any of the two transparencies alone uncover any information about the hidden message. Hence, this is a maximal contrast scheme with parameters $[b; h, l] = [4; 1, 0]$.

8.3 Coloured k out of n Secret Sharing Schemes

8.3.1 Introduction

Let us consider a coloured image where c colours are used, and we will denote them $k_0, k_1, \ldots, k_{c-1}$. In an analogous way, a gray tone image with c levels of grayness can be considered as a coloured image where $g_0, g_1, \ldots, g_{c-1}$ denote the different tones of gray that are used in it. An example of such a scheme is shown in Figure 8.4 taken from [31].

In the general model, in each transparency, every pixel is divided into b subpixels. The reason why we divide a pixel in subpixels is to define its colour via a collection of basic colour components (red, green, blue). Each one of them can take any one of the c colours. This time it is the subpixels that are depicted as circles of small radius. Each one of them is divided into c equal slices $0, 1, \ldots, c-1$. When the subpixel is of colour c_i, then the corresponding slice is coloured c_i and the remaining area of the circle is black. As a result, when the shares are placed on top of each other in a way



(a) Secret image (b) Share 1

(c) Share 2 (d) Recovered secret

Figure 8.4: Example of a coloured visual secret sharing scheme from [31]

that the corresponding subpixels align, if all of them are of the same colour c_i then the resulting colour is c_i. In any other case it is black.

Figure 8.5 (taken from [3]) shows the subpixels of such a scheme using $k = 3$ colours.

In the mathematical model of this technique, the following must be mentioned: First of all, the number c of the colours consisting the image must

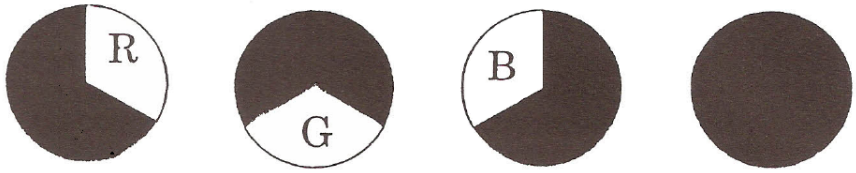


Figure 8.5: Example of the pixels that can be used for a 3-colour scheme (taken from [3])

be a prime or a prime power, and hence, the colours $k_0, k_1, \ldots, k_{c-1}$ are represented by elements of a Galois field. As one can deduce from the figure above, if all of them are of the same colour k_i, then k_i will be the colour of the resulted subpixel. By $\bullet$ we denote the result of *differently* coloured subpixels placed on top of each other. More specifically, $\bullet$ does not refer to any of the $k_0, k_1, \ldots, k_{c-1}$ colours, even if black is one of them. What is more, if a vector's $\vec{u}$ coordinates are in $\{k_0, k_1, \ldots, k_{c-1}\} \cup \{\bullet\}$, then we denote by $z_i(\vec{u})$, $(i = 0, 1, \ldots, c-1)$ the number of its coordinates that are equal to colour k_i.

Definition 8.3.1.1: *A k out of n c-coloured visual secret sharing scheme* $S = (\mathcal{C}_0, \mathcal{C}_1, \ldots, \mathcal{C}_{c-1})$ used to encrypt a coloured image is a set of collections of $n \times b$ matrices whose elements are in a Galois field $GF(q)$, $c \leq q$. Each collection corresponds to one of the colours that are used in the image. The matrices that are contained in a collection $\mathcal{C}_i$, $0 \leq i \leq c-1$, are the different versions of representing a subpixel of colour c_i. More specifically, the n rows of each matrix correspond to the n transparencies that are distributed to the participants of the scheme and the b elements of each row define the colour of its subpixels. The scheme must comply with the following three conditions:

1. For any matrix in a collection $\mathcal{C}_i$, $0 \leq i \leq c-1$, the "or" of any k out of its n rows must satisfy $z_i(\vec{u}) \geq h$.

2. For any matrix in a collection $\mathcal{C}_i$, $0 \leq i \leq c-1$, the "or" of any k out of its n rows must satisfy $z_j(\vec{u}) \leq l$, for every $j \neq i$.

3. The collections $\mathcal{C}'_j$, $0 \leq j \leq c-1$, obtained by limiting all the $n \times b$ matrices in the corresponding $\mathcal{C}_j$ to $s < k$ rows, $i_1 < i_2 < \ldots < i_s$, are identical, namely, the matrices that they contain are the same and appear in the same frequencies.

As already mentioned in the definition of a black and white visual secret sharing scheme, the parameters h and l ($h, l \in \mathbb{N}$) must comply the following condition: $0 \leq l < h < b$: the condition $l = 0$ may hold, since there is a possibility that no white subpixel exists in a black pixel. The condition $l < h$ must hold since the contrast of the scheme is defined on this difference. Last but not least, $h < b$ holds because if $h = b$ the security of the scheme would be compromised.

The parameters of such a c-coloured visual secret sharing scheme $S = (\mathcal{C}_0, \mathcal{C}_1, \ldots, \mathcal{C}_{c-1})$ will be $[c; b; h, l; r]$, where c is the number of the colours, b the blocklength of the scheme, i.e., the number of subpixels a pixel is divided into, and r the cardinality of the collections. It holds that $h > l$ and $|\mathcal{C}_0| = |\mathcal{C}_1| = \ldots = |\mathcal{C}_{c-1}| = r$.

In order to construct a c-coloured visual secret sharing scheme the following are necessary:

Definition 8.3.1.2: An *n-arc of functionals* $G, F_1, F_2, \ldots, F_{n-1}$ on $V(k, q)$ is called *coinciding with respect to* G if for every k-subset K of $\{1, 2, \ldots, n-1\}$ it holds that

$$\left(\bigcap_{i\in K} F_i^{-1}(1)\right) \cap G^{-1}(1) \neq \emptyset. \tag{8.1}$$

We denote $s(k,q)$ the maximum n for which a coinciding n-arc of functionals with respect to G exists in $V(k,q)$.

Lemma 8.3.1.3: *Let $s(k,q)$ denote the maximum coinciding n-arc of functionals in $V(k,q)$. Then, for any Galois field $GF(q)$ and k-dimensional space $V(k,q)$ the following statements hold:*

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

Proof. 1. Let us consider as functionals $G, F_1, \ldots, F_{q-1}$ the vectors in $V(k,q)$ of the form $(1, \omega_i^1, \ldots, \omega_i^{k-1})$, where $\omega_i \in GF(q)$, $1 \leq i \leq q-1$ and all the vectors from the permutations of the ω_i^j elements. It can be easily verified that the relation $\left(\bigcap_{i\in K} F_i^{-1}(1)\right) \cap G^{-1}(1) \neq \emptyset$ holds, since there exists at least one vector in $V(k,q)$, the vector $[1,0,\ldots,0]$, that fulfills it. Hence, $s(k,q) \geq |GF(q)| = q$.

2. Let us add vector $(0,0,\ldots,1)$ to the above described q-arc $s(k,q)$ and obtain a $q+1$ set of functionals. If $k-1$ and $q-1$ are not relatively prime, then the mapping $\omega \mapsto \omega^{k-1}$ is not surjective, and hence, there exists at least one element $x \in GF(q)$ such that $\omega^{k-1} \neq x$ for every $\omega \in GF(q)$. Since this holds, the inner product of the functionals in $s(k,q)$ with the vector $(-x,0,0,\ldots,1)$ is non-zero. In order to make this inner product equal 1, we do the following: we calculate the values y_i, $1 \leq i \leq q$ which are the

results of each one of the functionals to the vector $(-x, 0, 0, \ldots, 1)$. Next, we divide the members of $s(k, q)$ by their corresponding non-zero value y_i, i.e., we multiply by $-y_i$. As a result, the outcome of all the functionals to vector $(-x, 0, 0, \ldots, 1)$ equals 1 and we have constructed a coinciding arc of functionals of size $q + 1$. Hence, $s(k, q) \geq q + 1$.

3. Let us consider the set $s(k, q)$ to consist of all the unit vectors of $V(k, q)$, i.e., $(1, 0, \ldots, 0)$, $(0, 1, 0, \ldots, 0)$, etc. The inner product of each one of them with the vector $(1, 1, \ldots, 1)$ equals 1, hence, we have created a k-arc of coinciding functionals, i.e., $s(k, q) \geq k$.

4. If $q > 2$, or if $q = 2$ and k is odd, we can find a non-zero element t in $GF(q)$ such that the equation $\lambda = k - 1 + t \neq 0$. Then, the inner product of the vector $\lambda^{-1}(1, \ldots, 1, t)$ to vector $(1, \ldots, 1)$ equals $\lambda^{-1}(k-1+t) = \lambda^{-1} \cdot \lambda = 1$. We add vector $\lambda^{-1}(1, \ldots, 1, t)$ to the k-arc above, and get a $k + 1$-arc of coinciding functionals. Hence, $s(k, q) \geq k + 1$ if $q > 2$ or $q = 2$ and k is odd. □

8.3.2 A k out of n c-colour scheme construction

In order to construct a k out of n c-colour visual secret sharing scheme $S = (\mathcal{C}_0, \mathcal{C}_1, \ldots, \mathcal{C}_{c-1})$ we do the following steps:

1. Let us choose a Galois field $GF(q)$ such that $q \geq c$ and $s(k, q) \geq n+1$. Then, we select any c-subset $\{k_0, k_1, \ldots, k_{c-1}\}$ of elements in $GF(q)$.

2. We create an $n + 1 = (q + 1)$-arc of coinciding functionals in $V(k, q)$ using Lemma 8.3.1.3.

3. For each k_i, $0 \leq i \leq c-1$, we form the representation matrices A_i of the

functionals F_j, $1 \leq j \leq n$ using only the vectors $\vec{u}$ in $V(k,q)$ such that $G(\vec{u}) = k_i$ as follows: we construct an $n \times k$ matrix B whose rows are the n functionals and another matrix F, with dimension $k \times q^{k-1}$, whose columns consist of all the q^{k-1} vectors in $V(k,q)$ such that $G(\vec{u}) = k_i$. Then, the multiplication of B and F results in a new $n \times q^{k-1}$ matrix named A_i, which is the representation matrix of these functionals. It holds

$$\left(\bigcap_{i \in K} F_j^{-1}(k_i) \right) \cap G^{-1}(k_i) \neq \emptyset \tag{8.2}$$

for any k subset K of $\{1, \ldots, n\}$ and $i \in \{0, \ldots, c-1\}$.

4. The collections $\mathcal{C}_i$, $0 \leq i \leq c-1$ of S consist of all the matrices generated by permuting the columns of the corresponding A_i matrices created in the previous step.

Theorem 8.3.2.1: *The above scheme is a maximal contrast c-colour k out of n visual secret sharing scheme with parameters* $b = q^{k-1}$, $h = 1$, $l = 0$, *and* $r = q^{k-1}!$.

Proof. Without loss of generality let us consider $c = q$. As already mentioned in Section 5.4.1, the result of a functional in $V(k,q)$ with all the q^k different vectors in $V(k,q)$ equals q^{k-1} times the q different elements of $GF(q)$. Hence, the blocklength of the scheme is $b = q^{k-1}$.

From equation 8.2 we conclude that in each of these matrices, when limited to any k rows, there exists at least one "all-k_i" column. Since the vectors that correspond to the functionals are linearly independent, from Lemma 5.3.1.8 we get that each k-length vector appears exactly once. Hence, $h = 1$.

It is obvious that each representation matrix is created considering different vectors in $GF(q)$, since, there is no $\vec{u} \in GF(q)$ such that its image via $G(\vec{u})$ takes two different values, say k_i, k_j, $0 \leq i, j \leq k-1$, at the same time. Let us create a matrix $\tilde{A}$ which is the concatenation of all the representation matrices A_i, $0 \leq i \leq q-1$. Since each A_i consists of q^{k-1} columns, $\tilde{A}$ will consist of $q \cdot q^{k-1} = q^k$ columns. What is more, as mentioned in 5.3.1, the set that is constructed by the vectors $(0, 0, \ldots, 1)$ and $(1, \omega_i^1, \ldots, \omega_i^{k-1})$, where $\omega_i \in GF(q)$, $0 \leq i \leq q-1$, constitutes a $(q+1)$-arc, i.e., an $(n+1)$-arc. This implies that the n functionals that are used to create $\tilde{A}$ are k-wise linearly independent and as a result, from Lemma 5.3.1.8 when $\tilde{A}$ is limited to any k rows we get that each vector in $V(k, q)$ occurs exactly once as a column in $\tilde{A}$. Hence, the all-k_i columns appear exactly once, each in its corresponding matrix A_i. For example, since the all-zero vector appears as a column in matrix A_0, no such vector appears as a column in the rest of the A_i matrices. As a result, for the scheme it holds that $l = 0$.

For the security of the scheme: As already mentioned, the vectors that index the rows of A_i are k linearly independent, and as a result they are $k-1$ linearly independent, too. What is more, as already mentioned, each matrix A_i consists of q^{k-1} columns. Hence, when they are limited to $k-1$ rows, from Lemma 5.3.1.8 we get that each vector in $V(k-1, q)$, $|V(k-1, q)| = q^{k-1}$, is calculated exactly once as a column of the matrix. As a result, all the matrices A_i, $0 \leq i \leq q-1$, when restricted to any $k-1$ rows consist of the same columns, namely, they are indistinguishable. □

Remark 8.3.2.2: If c is a prime power and $c = q$, then the following types of schemes can be constructed taking Lemma 8.3.1.3 under consideration:

1. A k out of k c-colour visual secret sharing scheme for all k.

2. A k out of $c-1$ c-colour visual secret sharing scheme for $k < c$. As one can see, in this case $n = c - 1$.

3. A k out of c c-colour visual secret sharing scheme when $k-1$ and $c-1$ are relatively prime.

The following construction depicts the above-described model, case 3 in particular:

Example 8.3.2.3: We will construct a 3 out of 5 5-colour visual secret sharing scheme. Let us choose $q = c = 5$ and as a result $GF(5)$ will be used. Additionally, we choose $V(k, q) = V(3, 5)$. Since $k - 1 = 2$ and $q - 1 = 4$ are not relatively prime, we can create a 6-arc of coinciding functionals, according to Lemma 8.3.1.3 - 2nd part: We take the vectors created by the formula $(1, \omega, \ldots, \omega^{k-1})$, for every $\omega \in GF(5)$. These are the vectors $(1, 0, 0)$, $(1, 1, 1)$, $(1, 2, 4)$, $(1, 3, 4)$, and $(1, 4, 1)$. To these 5 vectors we add vector $(0, 0, 1)$. As one can see, element $\omega \mapsto \omega^{k-1} \neq 2$ for every $\omega \in GF(q)$. Hence, the value of the inner product of $(-2, 0, 1) = (3, 0, 1)$ with any of the 6 vectors is non-zero. In order for this result to equal one, we divide each vector by this result. Then the 6-arc of coinciding functionals will be: $F_1 = (2, 0, 0)$, $F_2 = (4, 4, 4)$, $F_3 = (3, 1, 2)$, $F_4 = (3, 4, 2)$, $F_5 = (4, 1, 4)$, and $G = (0, 0, 1)$. As one can see, the inner product of all these 6 vectors with the vector $(3, 0, 1)$ equal 1.

We now create the 5 representation matrices:

Functional $G = (0, 0, 1)$ equals 0 for the following vectors in $V(3, 5)$: $(0, 0, 0)$, $(0, 1, 0)$, $(0, 2, 0)$, $(0, 3, 0)$, $(0, 4, 0)$, $(1, 0, 0)$, $(1, 1, 0)$ $(1, 2, 0)$, $(1, 3, 0)$, $(1, 4, 0)$, $(2, 0, 0)$, $(2, 1, 0)$, $(2, 2, 0)$, $(2, 3, 0)$, $(2, 4, 0)$, $(3, 0, 0)$, $(3, 1, 0)$, $(3, 2, 0)$, $(3, 3, 0)$ $(3, 4, 0)$, $(4, 0, 0)$, $(4, 1, 0)$, $(4, 2, 0)$, $(4, 3, 0)$, and $(4, 4, 0)$.

Hence, the representation matrix for the zero value is the following:

$$A_0 = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 2 & 2 & 2 & 2 & 2 & 4 & 4 & 4 & 4 & 4 & 1 & 1 & 1 & 1 & 1 & 3 & 3 & 3 & 3 & 3 \\ 0 & 4 & 3 & 2 & 1 & 4 & 3 & 2 & 1 & 0 & 3 & 2 & 1 & 0 & 4 & 2 & 1 & 0 & 4 & 3 & 1 & 0 & 4 & 3 & 2 \\ 0 & 1 & 2 & 3 & 4 & 3 & 4 & 0 & 1 & 2 & 1 & 2 & 3 & 4 & 0 & 4 & 0 & 1 & 2 & 3 & 2 & 3 & 4 & 0 & 1 \\ 0 & 4 & 3 & 2 & 1 & 3 & 2 & 1 & 0 & 4 & 1 & 0 & 4 & 3 & 2 & 4 & 3 & 2 & 1 & 0 & 2 & 1 & 0 & 4 & 3 \\ 0 & 1 & 2 & 3 & 4 & 4 & 0 & 1 & 2 & 3 & 3 & 4 & 0 & 1 & 2 & 2 & 3 & 4 & 0 & 1 & 1 & 2 & 3 & 4 & 0 \end{bmatrix}$$

Functional $G = (0, 0, 1)$ equals 1 for the following vectors in $V(3, 5)$: $(0, 0, 1)$, $(0, 1, 1)$, $(0, 2, 1)$, $(0, 3, 1)$, $(0, 4, 1)$, $(1, 0, 1)$, $(1, 1, 1)$ $(1, 2, 1)$, $(1, 3, 1)$, $(1, 4, 1)$, $(2, 0, 1)$, $(2, 1, 1)$, $(2, 2, 1)$, $(2, 3, 1)$, $(2, 4, 1)$, $(3, 0, 1)$, $(3, 1, 1)$, $(3, 2, 1)$, $(3, 3, 1)$ $(3, 4, 1)$, $(4, 0, 1)$, $(4, 1, 1)$, $(4, 2, 1)$, $(4, 3, 1)$, and $(4, 4, 1)$.

Hence, the representation matrix for value one is the following:

$$A_1 = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 2 & 2 & 2 & 2 & 2 & 4 & 4 & 4 & 4 & 4 & 1 & 1 & 1 & 1 & 1 & 3 & 3 & 3 & 3 & 3 \\ 4 & 3 & 2 & 1 & 0 & 3 & 2 & 1 & 0 & 4 & 2 & 1 & 0 & 4 & 3 & 1 & 0 & 4 & 3 & 2 & 0 & 4 & 3 & 2 & 1 \\ 2 & 3 & 4 & 0 & 1 & 0 & 1 & 2 & 3 & 4 & 3 & 4 & 0 & 1 & 2 & 1 & 2 & 3 & 4 & 0 & 4 & 0 & 1 & 2 & 3 \\ 2 & 1 & 0 & 4 & 3 & 0 & 4 & 3 & 2 & 1 & 3 & 2 & 1 & 0 & 4 & 1 & 0 & 4 & 3 & 2 & 4 & 3 & 2 & 1 & 0 \\ 4 & 0 & 1 & 2 & 3 & 3 & 4 & 0 & 1 & 2 & 2 & 3 & 4 & 0 & 1 & 1 & 2 & 3 & 4 & 0 & 0 & 1 & 2 & 3 & 4 \end{bmatrix}$$

Functional $G = (0, 0, 1)$ equals 2 for the following vectors in $V(3, 5)$: $(0, 0, 2)$, $(0, 1, 2)$, $(0, 2, 2)$, $(0, 3, 2)$, $(0, 4, 2)$, $(1, 0, 2)$, $(1, 1, 2)$ $(1, 2, 2)$, $(1, 3, 2)$, $(1, 4, 2)$, $(2, 0, 2)$, $(2, 1, 2)$, $(2, 2, 2)$, $(2, 3, 2)$, $(2, 4, 2)$, $(3, 0, 2)$, $(3, 1, 2)$, $(3, 2, 2)$, $(3, 3, 2)$ $(3, 4, 2)$, $(4, 0, 2)$, $(4, 1, 2)$, $(4, 2, 2)$, $(4, 3, 2)$, and $(4, 4, 2)$.

Hence, the representation matrix for value two is the following:

$$A_2 = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 2 & 2 & 2 & 2 & 2 & 4 & 4 & 4 & 4 & 4 & 1 & 1 & 1 & 1 & 1 & 3 & 3 & 3 & 3 & 3 \\ 3 & 2 & 1 & 0 & 4 & 2 & 1 & 0 & 4 & 3 & 1 & 0 & 4 & 3 & 2 & 0 & 4 & 3 & 2 & 1 & 4 & 3 & 2 & 1 & 0 \\ 4 & 0 & 1 & 2 & 3 & 2 & 3 & 4 & 0 & 1 & 0 & 1 & 2 & 3 & 4 & 3 & 4 & 0 & 1 & 2 & 1 & 2 & 3 & 4 & 0 \\ 4 & 3 & 2 & 1 & 0 & 2 & 1 & 0 & 4 & 3 & 0 & 4 & 3 & 2 & 1 & 3 & 2 & 1 & 0 & 4 & 1 & 0 & 4 & 3 & 2 \\ 3 & 4 & 0 & 1 & 2 & 2 & 3 & 4 & 0 & 1 & 1 & 2 & 3 & 4 & 0 & 0 & 1 & 2 & 3 & 4 & 4 & 0 & 1 & 2 & 3 \end{bmatrix}$$

Functional $G = (0, 0, 1)$ equals 3 for the following vectors in $V(3, 5)$: $(0, 0, 3)$, $(0, 1, 3)$, $(0, 2, 3)$, $(0, 3, 3)$, $(0, 4, 3)$, $(1, 0, 3)$, $(1, 1, 3)$ $(1, 2, 3)$, $(1, 3, 3)$, $(1, 4, 3)$, $(2, 0, 3)$, $(2, 1, 3)$, $(2, 2, 3)$, $(2, 3, 3)$, $(2, 4, 3)$, $(3, 0, 3)$, $(3, 1, 3)$, $(3, 2, 3)$, $(3, 3, 3)$ $(3, 4, 3)$, $(4, 0, 3)$, $(4, 1, 3)$, $(4, 2, 3)$, $(4, 3, 3)$, and $(4, 4, 3)$.

Hence, the representation matrix for value three is the following:

$$A_3 = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 2 & 2 & 2 & 2 & 2 & 4 & 4 & 4 & 4 & 4 & 1 & 1 & 1 & 1 & 1 & 3 & 3 & 3 & 3 & 3 \\ 2 & 1 & 0 & 4 & 3 & 1 & 0 & 4 & 3 & 2 & 0 & 4 & 3 & 2 & 1 & 4 & 3 & 2 & 1 & 0 & 3 & 2 & 1 & 0 & 4 \\ 1 & 2 & 3 & 4 & 0 & 4 & 0 & 1 & 2 & 3 & 2 & 3 & 4 & 0 & 1 & 0 & 1 & 2 & 3 & 4 & 3 & 4 & 0 & 1 & 2 \\ 1 & 0 & 4 & 3 & 2 & 4 & 3 & 2 & 1 & 0 & 2 & 1 & 0 & 4 & 3 & 0 & 4 & 3 & 2 & 1 & 3 & 2 & 1 & 0 & 4 \\ 2 & 3 & 4 & 0 & 1 & 1 & 2 & 3 & 4 & 0 & 0 & 1 & 2 & 3 & 4 & 4 & 0 & 1 & 2 & 3 & 3 & 4 & 0 & 1 & 2 \end{bmatrix}$$

Functional $G = (0, 0, 1)$ equals 4 for the following vectors in $V(3, 5)$: $(0, 0, 4)$, $(0, 1, 4)$, $(0, 2, 4)$, $(0, 3, 4)$, $(0, 4, 4)$, $(1, 0, 4)$, $(1, 1, 4)$ $(1, 2, 4)$, $(1, 3, 4)$, $(1, 4, 4)$, $(2, 0, 4)$, $(2, 1, 4)$, $(2, 2, 4)$, $(2, 3, 4)$, $(2, 4, 4)$, $(3, 0, 4)$, $(3, 1, 4)$, $(3, 2, 4)$, $(3, 3, 4)$ $(3, 4, 4)$, $(4, 0, 4)$, $(4, 1, 4)$, $(4, 2, 4)$, $(4, 3, 4)$, and $(4, 4, 4)$.

Hence, the representation matrix for value four is the following:

$$A_4 = \begin{bmatrix}
0 & 0 & 0 & 0 & 0 & 2 & 2 & 2 & 2 & 2 & 4 & 4 & 4 & 4 & 4 & 1 & 1 & 1 & 1 & 1 & 3 & 3 & 3 & 3 & 3 \\
1 & 0 & 4 & 3 & 2 & 0 & 4 & 3 & 2 & 1 & 4 & 3 & 2 & 1 & 0 & 3 & 2 & 1 & 0 & 4 & 2 & 1 & 0 & 4 & 3 \\
3 & 4 & 0 & 1 & 2 & 1 & 2 & 3 & 4 & 0 & 4 & 0 & 1 & 2 & 3 & 2 & 3 & 4 & 0 & 1 & 0 & 1 & 2 & 3 & 4 \\
3 & 2 & 1 & 0 & 4 & 1 & 0 & 4 & 3 & 2 & 4 & 3 & 2 & 1 & 0 & 2 & 1 & 0 & 4 & 3 & 0 & 4 & 3 & 2 & 1 \\
1 & 2 & 3 & 4 & 0 & 0 & 1 & 2 & 3 & 4 & 4 & 0 & 1 & 2 & 3 & 3 & 4 & 0 & 1 & 2 & 2 & 3 & 4 & 0 & 1
\end{bmatrix}$$

As one can see, in each one of the matrices A_i, $0 \leq i \leq 4$, there is a column whose elements are all equal to number i. The parameters of the scheme are $[c; b; h, l; r] = [5; 25; 1, 0; 25!]$.

Chapter 9

Applications of Visual Cryptography

Although Visual Cryptography has some advantages compared to other cryptographic schemes, practical applications based on it took a while to evolve. Two were the main reasons: the visual noise added at the printing process, and the difficulty in the correct alignment of the transparencies. Some solutions to the latter were developed, such as a frequency domain alignment scheme [18].

Another problem of Visual Cryptography is that because of the expansion of the original image, the schemes are not effective when the hidden message is longer than a single word or a small phrase. The same holds for images to be shared with high resolution.

One field where Visual Cryptography can be used is e-voting: Since everything is handled by a computer program and there is no physical substance of a vote, there must be some way for all voters to verify that their voting decision is counted correctly. However, a receipt that clearly declares the identity

of the voter along with their voting choices may cause coercion or vote selling problems. Some solutions using Visual Cryptography are proposed.

For example, Chaum in [19] presents a secret-ballot receipt system. In this case, after a voter has made their choices, a two-layer (two transparencies) receipt is created using a 2 out of 2 visual secret sharing scheme and then is printed. When these two layers are put on top of each other, the choices of the voter are shown. However, when separated, an unreadable pattern of random black and white subpixels is only visible in the place of the vote. One layer is kept by the voter while the other is destroyed by a poll worker before the voter. A serial number that is printed on the layer the voter keeps enables him to verify that his voting decisions was correctly counted by the system. In figure 9.1 from [19] one can see the initial representation of the letter "e", the two layers (transparencies) produced using the visual secret sharing scheme and their representation when they are stacked together in Chaum's secret ballot receipt system. What is more, electronic voting schemes have been proposed that combine visual cryptography and digital processing [18]. In [34], Visual Cryptography is used in a remote Internet voting scheme as assistance to transform the construction into a verification protocol.

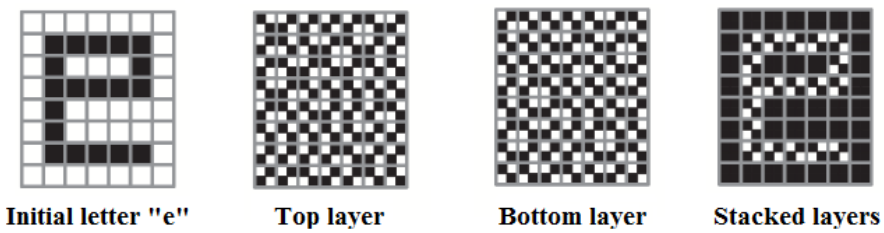


Figure 9.1: Chaum's secret-ballot receipt

Another field where Visual Cryptography can be applied is Biometric Au-

thentication. As an example, ID cards using fingerprints as an authentication medium can be constructed as follows: a fingerprint image of an eligible person is divided into two shares. One is placed on their ID card while the other is stored in a centralized database. During the authentication phase, the two images are superimposed and from the resulting fingerprint the minutiae (small details) of the finger are extracted. Next, a fresh image of the fingerprint is obtained with the help of any fingerprint scanner and the minutiae of the latter are compared with the minutiae of the secret fingerprint image. If they match, the authentication succeeds. An example of such a construction is presented in Figure 9.2 from [23]. Since Visual Cryptography Schemes are perfectly secure, ID card spoofing can be avoided. What is more, the side effects of a potential database compromise are eliminated.

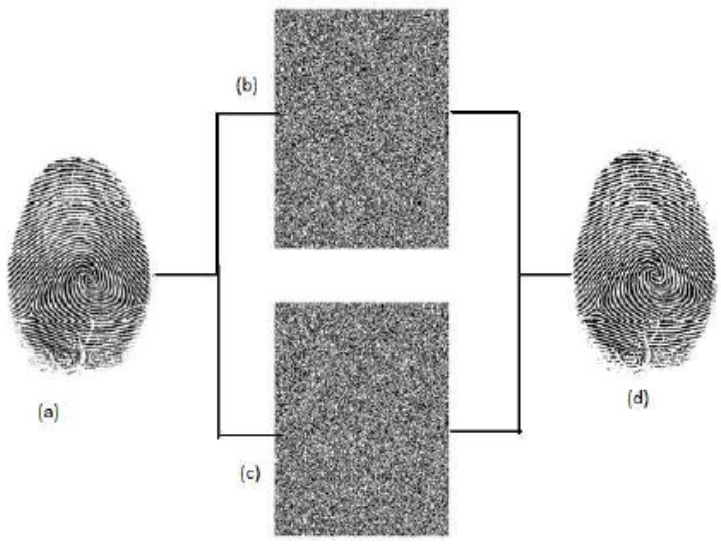


Figure 9.2: (a) Original image, (b) First share, (c) Second share, (d) Superimposed shares

Many other constructions and improvements have been presented, regarding authentication using visual cryptography schemes. Examples can be found in [24], [25], [26] and [27]. Additionally, methods for creating image copyright protection and watermarking using Visual Cryptography are presented in [32] and [33]. An important use of Extended Visual Cryptography could be the transfer over the Internet of military maps or commercial secrets.

Several enhancements involving security have been presented, too: in [28] for example, the use of Digital Watermarking is introduced in visual secret sharing schemes. Other approaches involve encoding without pixel expansion, as described in [29]. Additionally, the concept of sharing multiple secrets is described in [35] and [36]. The general technique that is used is that the first secret message is revealed by stacking the transparencies, while the second one by first rotating one of them. Research is also done regarding the combination of Coloured and Extended Visual Cryptography (an example in [37]), where two meaningful ordinary coloured images are used to encrypt a secret coloured image.

An application of a coloured visual secret sharing scheme can be the share of special short messages whose symbols are colours and not alphanumerical characters, for example passwords or combinations to safes. Exactly like all the other techniques described in previous sections, no calculations of any form are necessary since the decryption is very simple and is accomplished by the human visual system.

Chapter 10

Conclusion

From 1994, where the first paper was presented by Shamir and Naor, Visual Cryptography has never stopped being a field of research with steadily growing interest. Its basic model is still being enhanced in different ways: many innovative ideas and extensions are proposed. The special properties that make Visual Cryptography an interesting field of study are its perfect safety, effectiveness, and simplicity. These properties are fulfilled because its constructions are based on special mathematical models. As digital technology becomes more and more part of our lives, Visual Cryptography may play a significant role in the future.

Notation List

$S = (\mathcal{C}_0, \mathcal{C}_1)$	A visual secret sharing scheme consisting of two collections of matrices, $\mathcal{C}_0$ and $\mathcal{C}_1$
$\mathcal{C}_0$:	A collection of matrices each one of which represent the shares of a white pixel
$\mathcal{C}_1$:	A collection of matrices each one of which represent the shares of a black pixel
A_0	A matrix from which collection $\mathcal{C}_0$ is constructed via permutation of its columns
A_1	A matrix from which collection $\mathcal{C}_1$ is constructed via permutation of its columns
b	The blocklength of the scheme, i.e., the number of subpixels a pixel is divided
$w(\vec{v})$	The Hamming weight, i.e., the number of non-zero coordinates of a vector $\vec{v}$
$z(\vec{v})$	The number of zero coordinates of a vector $\vec{v}$
h	The minimum number of white subpixels in a white pixel. Alternatively, the minimum number of zeros required in the blocklength of a matrix to represent a white pixel

l	The maximum number of white subpixels in a black pixel. Alternatively,the maximum number of zeros allowed in the blocklength of a matrix to represent a black pixel
a	The relative difference between a black and a white pixel. Defined in [2] as $a = (h - l)/b$. Must be as large as possible
r	The cardinality of $\mathcal{C}_0$ and $\mathcal{C}_1$ ($r = \|\mathcal{C}_0\| = \|\mathcal{C}_1\|$)
$GF(k)$	The Galois Field of order k, where k is a prime or a prime power
$V(k, q)$	A vector space over the Galois Field $GF(q)$, i.e., the set of all possible k-dimensional vectors over $GF(q)$. As a result, $\|V(k, q)\| = q^k$
$PG(k, q)$	A projective space over $GF(q)$ which consists of all the non-zero subspaces of $V(k + 1, q)$ with respect to inclusion
$r(k, q)$	The maximum n for which an n-arc exists in $V(k, q)$
$s(k, q)$	The maximum n for which a coinciding n-arc **of functionals** exists in $V(k, q)$

Bibliography

[1] B. Arazi, I. Dinstein and O. Kafri, *Intuition, perception, and secure communication*, IEEE Transactions on Systems, Man, and Cybernetics, Vol. 19 (1989) pp. 1016-1020.

[2] M. Naor and A. Shamir, *Visual Cryptography*, Preproceedings of Eurocrypt '94 (1994) pp. 1-11.

[3] Eric R. Verheul and Henk C. A. Van Tilborg, *Constructions and Properties of k out of n Visual Secret Sharing Schemes*, Designs, Codes and Cryptography, 11, 179-196, (1997).

[4] F. van der Heijden, *Image Based measurement Systems*, John Wiley & Sons, Chichester (1994).

[5] W. K. Pratt, *Digital Image Processing*, John Wiley & Sons, Chichester (1991).

[6] J. Kahn, N. Linial and A. Samorodnitsky, *Inclusion - exclusion: exact and approximate*, manuscript.

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

[8] N. Alon and J. Spencer, *The Probabilistic Method*, Wiley, 1992.

[9] J. L. Carter and M. N. Wegman, *Universal classes of hash functions*, Journal of Computer and System Sciences 18 (1979), pp. 143-154.

[10] M. N. Wegman and J. L. Carter, *New hash functions and their use in authentication and set equality*, Journal of Computer and System Sciences 22, pp. 265-279 (1981).

[11] J. Naor and M. Naor, *Small bias probability spaces: efficient constructions and applications*, SIAM J. on Computing, vol. 22, 1993, pp. 838-856.

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

[13] 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 (1993) pp. 139-154.

[14] T. L. Alderson, A. A. Bruen, and R. Silverman, *Maximum Distance Separable Codes and Arcs in Projective Spaces.*

[15] W. Rudin, *Functional Analysis*, MacGraw-Hill Series in Higher Mathematics, MacGraw-Hill, New York (1973).

[16] J. A. Thas, *Projective Geometry over a finite field*, Chapter 7 in Handbook of Incidence Geometry (F. Buuekenhout, ed.), Elsevier Science, Amsterdam (1995).

[17] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North Holland, Amsterdam etc., 1977.

[18] Wei-Qi Yan, Duo Jin, and Mohan S.Kankanhalli, *Visual Cryptography for print and scan applications*, Proceedings of International Symposium on Circuits and Systems, pages 572-575, May 2004.

[19] David Chaum *Secret Ballot Receipts: True Voter Verifiable Elections*, IEEE Security and Privacy 38-47, Jan.-Feb. 2004.

[20] Jim Cai, *A short survey on Visual Cryptographic Schemes*

[21] *http://www.wikipedia.org*

[22] *http://marc-stevens.nl/vck/*

[23] Nazanin Askari, Cecilia Moloney, Howard M. Heys, *Application of Visual Cryptography to Biometric Authentication*

[24] A. Jain, L. Hong, S. Pankanti, R. Bolle, *An Identity Authentication System Using Fingerprints*, Department of Computer Science, Michigan State University, USA. 1- 66, 1997.

[25] Y.V. Subba Rao, Yulia Sukonkina, Chakravarthy Bhagwati, Umesh Kumar Singh, *Fingerprint based authentication application using visual cryptography methods (Improved ID card)*, Proc.IEEE Region 10 Conf, pp.1-5, Nov 2008.

[26] T. Monoth and B.A., *Tamperproof transmission of fingerprints using visual cryptography schemes*, Procedia Computer Science,vol. 2, pp. 143-148, 2010.

[27] P.S.Revenkar, Anisa Anjum, W .Z.Gandhare, *Secure Iris Authentication Using Visual Cryptography.*

[28] Shyamalendu Kandar, Arnab Maiti, Bibhas Chandra Dhara *Visual Cryptography Scheme for Color Image Using Random Number with Enveloping by Digital Watermarking.*

[29] N. Gowdham, S.D. Libin Raja, M. Sornalakshmi, M. Navaneetha Krishnan *Two Step Share Visual Cryptography Algorithm for Secure Visual Sharing* .

[30] Angelina Espejel Trujill, Mariko Nakano Miyatake, Mitsugu Iwamoto, Hector Perez Meana *A cheating prevention EVC scheme using watermarking techniques.*

[31] Jonathan Weir, WeiQi Yan *Visual Cryptography and its Applications.*

[32] Adel Hammad Abusitta, *A Visual Cryptography Based Digital Image Copyright Protection.*

[33] Mahmoud A. Hassan, and Mohammed A. Khalili , *Self Watermarking based on Visual Cryptography.*

[34] Aggelos Kiayias, Anthi A. Orfanou, *Voter Verifiable Internet Voting Protocols.*

[35] Shyong Jian Shyu, Shih-Yu Huang,Yeuan-Kuen Lee, Ran-Zan Wang, Kun Chen, *Sharing multiple secrets in visual cryptography.*

[36] Mustafa Ulutas, R. Yazici, Vasif V. Nabiyev, GG'Ozin Ulutas, *Secret Sharing scheme with improved share randomness.*

[37] C. Chang, C. Tsai, and T. Chen, *A new scheme for sharing secret color images in computer network.*