Ca' Foscari
University
of Venice

Master's Degree programme

in Computer Science

"Software Dependability and
Cyber Security"

Final Thesis

Visual Cryptography Schemes with Multiple Secrets and Visual Key Derivation

Supervisor
Ch. Prof. Riccardo Focardi
Supervisor
Ch. Prof. Flaminia Luccio
Candidate
Nicolò Ghiotto, 846886
Academic Year
2017 / 2018

Abstract

Visual Cryptography was introduced in 1995 by Naor and Shamir to recover a secret image by overlapping two or more images. This scheme is secure and easy to implement and can be extended to a set of participants in order to recover the same secret image. In this thesis, we propose two new schemes that use a shared image to encode a different secret image for each participant. In the first scheme, we generate a *visual cyphertext* from a shared key for each participant. Since the shared key is computed a priori, we can add a new participant at any given time and generate her cyphertext, ensuring scalability. In the second scheme, we make the approach more practical by applying a *visual key derivation function* in order to let each participant derive her *visual cyphertext* from a different password for each participant. This is a joint work with colleague Tommaso Moretto, who has developed implementations and performed practical experiments on these new schemes applied to barcode confidentially [10].

Contents

1 Introduction

Visual Cryptography [11] is a cryptographic technique for securely encrypting images in such a way that the decryption does not need any computation. The secret image is split into two or more random noise images, that if overlapped, generate the secret image. While basic Visual Cryptography takes in consideration only black and white images, some schemes, e.g., [14], can also encrypt colored images. Visual Cryptography can also be extended by providing different secrets for a different set of users (e.g., [6]).
In this thesis, we propose two new schemes that use a shared image to encode a different secret image for each participant. In the first scheme, we generate a *visual cyphertext* from a shared key for each participant. In the second scheme, we make the approach more practical by applying a *visual key derivation function* in order to let each participant derive her *visual cyphertext* from a different password for each participant.

This thesis is structured as follows. In Section 2, we describe the basic model of Visual Cryptography, called n out of n scheme, which requires all the n images for the generation of the secret. This model is then extended into a k out of n scheme, requiring at least k images to generate the secret.
We then recall Access Structures, which are used in Cryptography and Security Systems where multiple users, called participants, need to share a specific resource [12]. Groups of participants that are granted access to the resource are called Qualified Sets. [1] and [2] extend Visual Cryptography with Access Structures. An Access Structure in a Visual Cryptography model allows each qualified set to overlap their image in order to recover the secret image.

Different Access Structures for Visual Cryptography Schemes can be unified in a unique Access Structure called Non-Connected, that preserves the same characteristics of a classic one.
Finally, in the last part of Section 2 we introduce extensions to Visual Cryptography in which each participant's image is not any more completely random, but it preserves the form of a predefined image. A qualified set of the Access Structure can recover the secret by overlapping their images. In this particular extension both the secret image and the the participants ones are meaningful. The number of images required for this model is therefore $n+1$, where n is the number of participants in the Access Structure, and the last one is the secret image the Qualified Sets can aquire.

In Section 3, we introduce two new methods to allow each participant to recover their secret, using a unique shared image. Each couple (participant, shared key) is a Qualified Set in the Access Structure and it has access to a unique secret image. This Access Structure can be seen as a union of many 2 out of 2 schemes, in which each scheme has a single participant and the shared image as members.
In order to ensure scalability, in the first model the shared image is precomputed and the images of the participants are generated starting from it. Moreover, in this scheme each participant image is meaningful. The shared images are randomly generated and it a random noise image.
In order to use the second model in real world applications, we have to consider usability. By exploiting a *visual key derivation function*, the images provided to each participant are generated starting from a password, so that

each user to recover the secret can provide the password instead of her image. The shared image is then computed starting from them. To make this model work, each subpixel of the shared image is divided in equal parts between each participant.

2 Visual Cryptography

Visual Cryptography was first introduced by Naor and Shamir in [11]. The idea is to recover a secret image by overlapping two or more images, called *transparencies*. E.g., an application that stores an image as secret key inside the application; when another image (the cyphertext) arrives by email, the two images are overlapped to generate a new secret image.
Let us now formally define what a Visual Cryptography Scheme is.

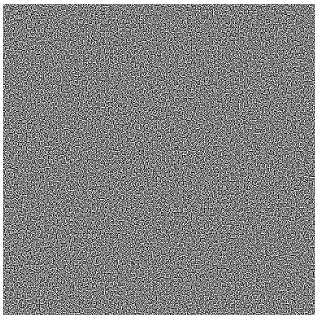
Definition 2.1 *[11] A* ***n out of n Visual Cryptography Scheme*** *is a scheme in which n transparencies are generated from a secret image in a way that the secret image is visible if exactly n transparencies are overlapped.*

The previous model can be extended to define a k out of n scheme, in which at least k transparencies are neeeded to recover the secret image.

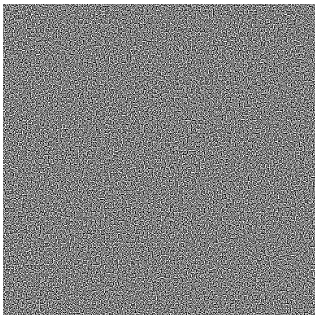
Definition 2.2 *[11] A* ***k out of n Visual Cryptography Scheme****, with $k \leq n$, is a scheme in which n transparencies are generated from a secret image in a way that the secret image is visible if any k or more transparencies are overlapped.*

In Figures 1, 2 and 3, we show a simple example of a 2 out of 2 Visual Cryptography Scheme.

Figure 1: Secret image.



(a) Transparency 1



(b) Transparency 2

Figure 2: Two Transparencies that overlapped produce Figure 3.

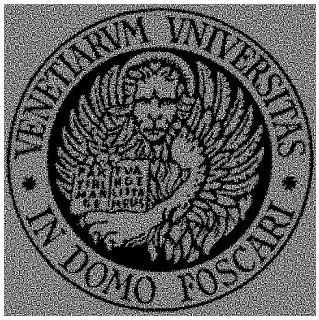


Figure 3: The overlapped transparencies of Figure 2 produce this new image.

2.1 Visual Cryptography model

In the evaluated model, the secret image is generated starting from its orginal pixels. Each pixel can be either black or white and it appears in n modified versions, called *shares*, one for each transparency. These shares are subpixels generated starting from a set of m white and black *subpixels* combined to contribute to the color of the original pixel. Let us now define the matrix S needed to construct the shares.

Definition 2.3 *$S = [s_{ij}]$ is an $n \times m$ matrix such that each element $s_{ij} = 1$ if and only if the jth subpixel in the ith transparency is black, $s_{ij} = 0$ otherwise.*

The *Hamming Weight* of the shares is calculated to define the original color of a pixel.

Definition 2.4 *Given a binary string s of length n, the **Hamming Weight** of s is the number of bits of S that are different from 0.*

S_0 and S_1 are respectively the *basis matrices* that contain a set of shares that define white and black pixels.
Starting from the basis matrices S_0 and S_1, we generate the collections of all the possibile shares C_0 and C_1.

Definition 2.5 *C_0 is the set of $n \times m$ matrices obtained by permuting the columns of S_0, while C_1 is the set of $n \times m$ matrices obtained by permuting the columns of S_1.*

The overlap of the transparencies generates a unique share that is an expanded version of the original secret image, in which the color of each origi-

nal pixel depends on the Hamming Weight H of the OR operations of each transparency's subpixel.

Definition 2.6 *Given a set of transparencies* $\{i_1, .., i_k\}$*, the combined share obtained by overlapping them, has as many black subpixel as the string obtained by computing the binary OR of transparencies* $i_1, ..., i_k$*, and its grey level is defined by its Hamming weight* H*.*
A combined share is considered black if the Hamming Weight H *of the OR operation of the transparencies is* $H \geq d$ *and white if* $H < d - \alpha m$ *for some fixed threshold* $1 \leq d \leq m$ *and chosen* α *that determines which level of grey maps to a white pixel and which maps to a black pixel.*

The shares that have to be overlapped to reconstruct a white (respectively, black) pixel are generated starting from the $n \times m$ basis matrix S_0 (respectively, S_1). The Hamming Weight H of the OR operation of $k \leq n$ rows in S_0 give a white pixel in the reconstructed secret image, as described in Definition 2.6.

Example 2.1 In Figure 4, with $m = 2$ subpixels for each pixel, $d = 2$ and $0 < \alpha < 1/2$, so that, in the final image a black pixel will have 2 black subpixels, and a white pixel will have 1 black subppixel and 1 white subpixel.

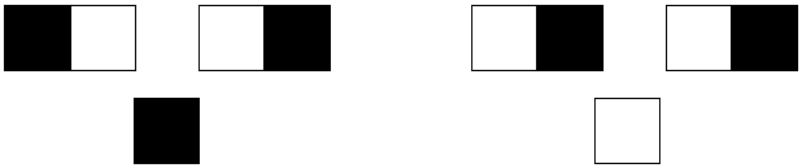


Figure 4: On the right, two shares are generated starting from a black pixel. On the left, two shares are generated starting from a white pixel.

We now require two important conditions: the *contrast* between a white and a black pixel, is the difference between a set of subpixels for a black pixel with a set of subpixels for a white pixel, and the *security* of the scheme, in particular we want that by inspecting less than k transparencies, even with an infinitely powerful computer, the secret image cannot be guessed.

Definition 2.7 *[11] For the k out of n secret scheme,with $k \leq n$, we choose one matrix from C_0 to define a white pixel and a matrix from C_1 to define a black pixel. The chosen matrix from the collection defines the m subpixels for the n transparencies. The conditions are the following:*

1. ***Contrast**:*

   - *For any S in C_0, the OR operation of any k of the n rows satisfies $H \leq d - \alpha m$.*
   - *For any S in C_1, the OR operation of any k of the n rows satisfies $H \geq d$.*

2. ***Security:***

- *For any subset* $\{i_1, .., i_q\}$ *of* $\{i_1, .., i_n\}$ *with* $q < k$*, the two collections of* $q \times m$ *matrices* D_0 *and* D_1*, obtained by removing the row of the missing participants from* C_0 *and* C_1*, are indistinguishable meaning that the Hamming Weight of the shares taken from a matrix in* D_0 *is euqal to the Hamming weight of the sares taken fro ma matrix in* D_1*.*

In [11] various constructions for specific values of k and n are proposed. The one we are interested in is:

Theorem 2.1 *[11] For any k out of k problem, given the number of transparencies k there is a Visual Cryptography Scheme with the length of a share* $m \leq 2^{k-1}$ *and the relative difference* $\alpha \geq \frac{1}{2^{k-1}}$*. The scheme is optimal when* $m = 2^{k-1}$ *and* $\alpha = \frac{1}{2^{k-1}}$*.*

Example 2.2 Simple 2 out of 2 scheme. The 2 out of n secret scheme problem can be solved by the following collections of $n \times n$ matrices:

$$C_0 = \{\textit{columns permutation of } S_0\}$$
$$C_1 = \{\textit{columns permutation of } S_1\}$$

with:

$$S_0 = \begin{bmatrix} 100...0 \\ 100...0 \\ ... \\ 100...0 \end{bmatrix}, \; S_1 = \begin{bmatrix} 100...0 \\ 010...0 \\ ... \\ 000...1 \end{bmatrix}$$

Any share in the collections is a random choice of one black and $n-1$ white subpixels. The difference between two shares taken from C_0 and C_1 is in the Hamming weight: two shares from C_0 have the Hamming weight of 1 and two shares from C_1 have the Hamming weight of 2. By overlapping additional shares, the gap between a black and a white pixel becomes more recognizable.

Example 2.3 Efficient 2 out of 2 scheme. We could solve this case with two subpixels for each share, in fact by taking the number of required transparencies $k = 2$, the length of a share $m = 2^{k-1}$ we get $m = 2$. In order to preserve the square aspect of the pixel we use 4 subpixels as 2×2 matrix. With $H \geq d$ for black pixels and $H \leq d - \alpha m$ for white pixels, by setting $d = 4$ and $\alpha = \frac{1}{2}$ we have that 2 rows of one matrix from C_0 give $H = 4$ which represents a black pixel, and 2 rows of one matrix from C_1 give $H = 2$ which represents a grey pixel.

$$S_0 = \begin{bmatrix} 1100 \\ 1100 \end{bmatrix}, \; S_1 = \begin{bmatrix} 1100 \\ 0011 \end{bmatrix}$$

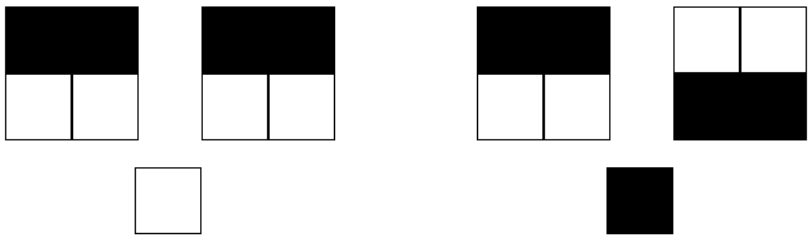


Figure 5: S_0 and S_1 for a 2 out of 2 scheme

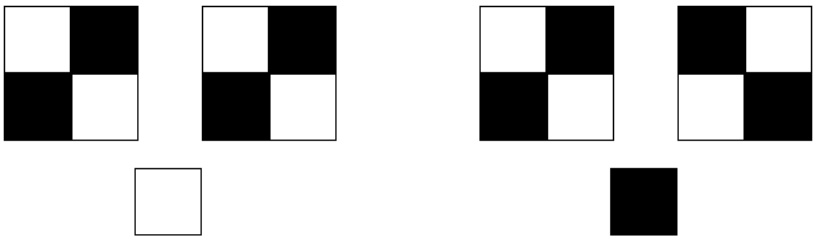


Figure 6: Two shares taken from C_0 and C_1 for a 2 out of 2 scheme

Example 2.4 Efficient 3 out of 3 scheme. This scheme requires $m = 4$ and $\alpha = \frac{1}{4}$ to be optimal and so by putting $d = 4$ we get $H = 4$ for the generation of a black pixel and $H = 3$ for the generation of a white pixel.

$$S_0 = \begin{bmatrix} 1100 \\ 1010 \\ 0110 \end{bmatrix}, \; S_1 = \begin{bmatrix} 1100 \\ 1010 \\ 1001 \end{bmatrix}$$

In this case, a single analysis of one or two shares makes it impossible to distinguish C_0 from C_1 and viceversa. However, three shares stacked together from C_0 generate a pixel which is only 3/4 black, while three shares from C_1 generate a completely black pixel.

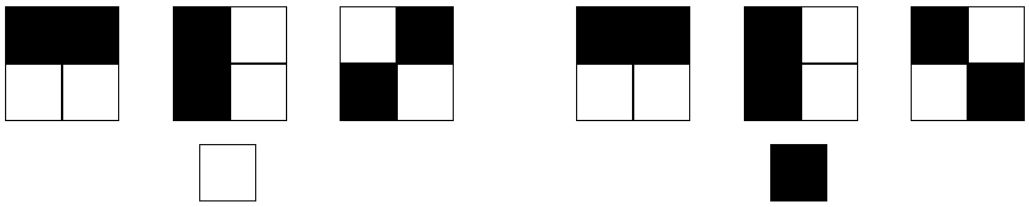


Figure 7: S_0 and S_1 for a 3 out of 3 scheme

Example 2.5 Efficient 4 out of 4 scheme. The 4 out of 4 problem can be optimally solved with $m = 8$ and $\alpha = \frac{1}{8}$, but as we would lose the square aspect of the pixel, we need $m = 9$ so that each share can be seen as 3×3 matrix.

$$S_0 = \begin{bmatrix} 011111000 \\ 010110011 \\ 001110101 \\ 000111110 \end{bmatrix}, \; S_1 = \begin{bmatrix} 011011010 \\ 010111001 \\ 010110110 \\ 100111010 \end{bmatrix}$$

In this case: any single share has $H = 5$, two shares have $H = 7$, three shares have $H = 8$ and four shares have $H = 8$, if the original pixel is white, or $H = 9$, if it is black.

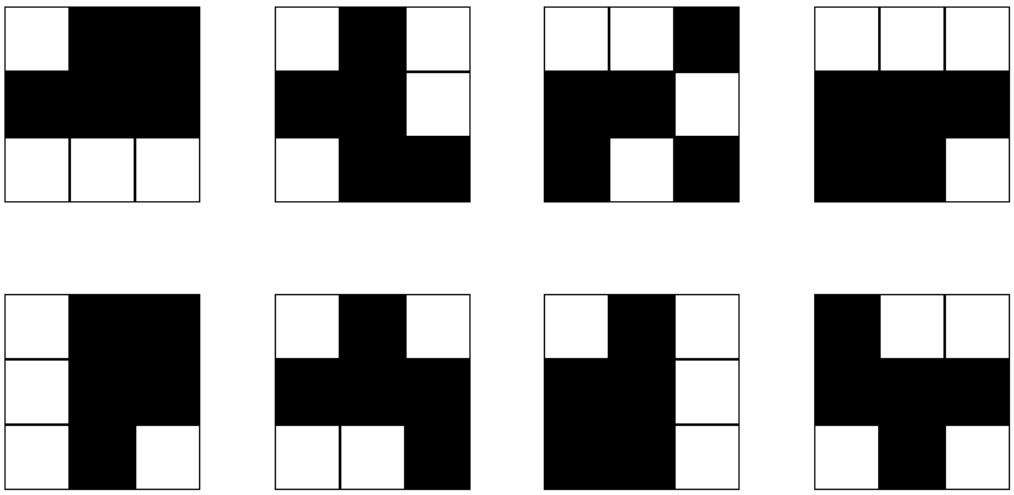


Figure 8: S_0 and S_1 for a 4 out of 4 scheme

2.2 General Access Structures

In [1] and [2] Visual Cryptography is extended to a set $\mathscr{P}$ of n participants in which each member receives a transparency for the secret image and some qualified subsets of $\mathscr{P}$ are able to recover the secret image by overlapping their transparencies, while some others, called forbidden subsets, cannot.

Definition 2.8 *A **qualified set** p is a subset of $\mathscr{P}$ such that by overlapping the transparencies of the participants in p it is possible to recover the secret image. A **forbidden set** f is a subset of $\mathscr{P}$ such that by overlapping the transparencies of the participants in f, it is not possible to recover the secret image.*

The two sets containing these subsets are respectively called Γ_{qual} and Γ_{forb}.

Definition 2.9 *Γ_{qual} is the set containing all the qualified sets for the set $\mathscr{P}$. Γ_{forb} is the set containing all the forbidden sets for the set $\mathscr{P}$.*

A member p in $\mathscr{P}$ is called *essential* if it is required in a subset of Γ_{qual} to recover the secret image.

Definition 2.10 *A member $p \in \mathscr{P}$ is called **essential** if for any subset $Q \subseteq \mathscr{P}$ we have $Q \cup \{p\} \in \Gamma_{qual}$ and $Q \notin \Gamma_{qual}$.*

Members of $\mathscr{P}$ that are not present in Γ_{qual} can have a completely white transparency as they are not relevant for the reconstruction of the secret image.

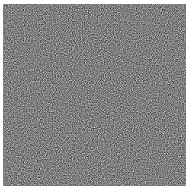
In [13] and [2] a technique which exploit Access Structures for the construction of a Visual Cryptography Scheme which achieve higher constrast is proposed.

Example 2.6 Consider $\mathscr{P} = \{1, 2, 3, 4\}$ where we want at least two members $\{1, 2\}$, $\{2, 3\}$ or $\{3, 4\}$ to recover the secret image and all the remaining subsets of participants $\{1, 3\}$, $\{1, 4\}$, $\{2, 4\}$ are forbidden:

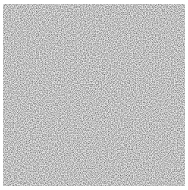
$$\Gamma_{qual} = \{\{1, 2\}, \{2, 3\}, \{3, 4\}, \{1, 2, 3\}, \{1, 2, 4\}, \{2, 3, 4\}, \{1, 2, 3, 4\}\}$$

This example is shown in Figures 9, 10, 11, 12, 13.

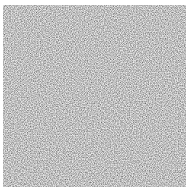
Figure 9: secret image



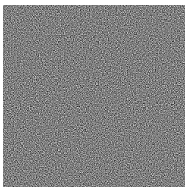
(a) transparency 1



(b) transparency 2



(c) transparency 3



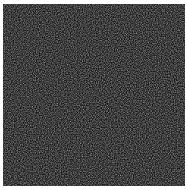
(d) transparency 4

Figure 10: Participants in the Access Structure

(a) 1 and 2 overlapped

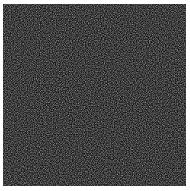
(b) 2 and 3 overlapped

(c) 3 and 4 overlapped

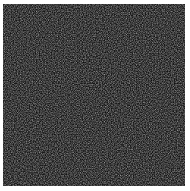


(d) 1 and 3 overlapped

Figure 11: Part 1 of the Access Structure



(a) 1 and 4 overlapped



(b) 2 and 4 overlapped

(c) 1,2 and 3 overlapped

(d) 1, 2 and 4 overlapped

Figure 12: Part 2 of the Access Structure

(a) 1, 3 and 4 overlapped

(b) 2, 3 and 4 overlapped

(c) 1, 2, 3 and 4 overlapped

Figure 13: Part 4 of the Access Structure

2.2.1 General Access Structure Model

Starting from a set $\mathscr{P}$ of *participants* and its power set $P(\mathscr{P})$, it follows that $\Gamma_{qual} \subseteq P(\mathscr{P})$, $\Gamma_{forb} \subseteq P(\mathscr{P})$ and $\Gamma_{qual} \cap \Gamma_{forb} = \emptyset$.

Definition 2.11 *The pair* $(\Gamma_{qual}, \Gamma_{forb})$ *is called* ***Access Structure****.*

All the minimal qualified sets of Γ_{qual} can be expressed as:

$$\Gamma_0 = \{Q \in \Gamma_{qual} : Q' \notin \Gamma_{qual} \; \forall \; Q' \subset Q\}$$

The most frequently used setting for Visual Cryptography is based on *strong* Access Structures.

Definition 2.12 *An Access Structure is called* ***strong*** *when* Γ_{qual} *is monotone increasing and* $\Gamma_{qual} \cup \Gamma_{form} = P(\mathscr{P})$. Γ_0 *is called basis and* Γ_{qual} *is its closure.*

We can now define $(\Gamma_{qual}, \Gamma_{forb}, m)$-VCS, that is a *Visual Cryptography Scheme* with an Access Structure, where α is the relative difference and d_Q is a specific d for the subset Q, both described in 2.1:

Definition 2.13 *The two collections of* $n \times m$ *matrices* C_0 *and* C_1 *define a Visual Cryptography Scheme* $(\Gamma_{qual}, \Gamma_{forb}, m)$*-VCS with the relative difference* α *and its set* $\{(Q, d_Q)\}_{Q \in \Gamma_{qual}}$*, if the following constrast and security properties are satisfied:*

1. *Contrast, for any* $Q = \{i_1, i_2, ..., i_n\} \in \Gamma_{qual}$*:*

- *If $Q \in C_0$ the OR operation of rows $i_1, i_2, ..., i_n$ satisfies $H \leq d_Q - \alpha m$*
- *If $Q \in C_1$ the OR operation of rows $i_1, i_2, ..., i_n$ satisfies $H \geq d_Q$*

2. *Security:*

   - *The two collections of $p \times m$ matrices D_0 and D_1, obtained by restricting each $n \times m$ matrices in C_0 and C_1 to rows $\{i_1, i_2, ..., i_n\}$, are indistinguishable in the sense that they contain the same matrices with the same frequencies.*

Each pixel of the original image is encoded into n shares, each of which contains m subpixels. To choose a white or a black pixel, one matrix is randomly chosen respectively from C_0 or C_1 and the rows are distributed between the participants.

This structure is a generalization of the Visual Cryptography Scheme proposed in [11], since a different threshold d_Q can be associated to each set $Q \in \Gamma_{qual}$.

Although C_0 and C_1 could also have different sizes, for simplicity and without being a restriction, both in [11] and [2], the authors consider that C_0 and C_1 have the same size $|C_0| = |C_1|$.

We can now define the construction of a $(\Gamma_{qual}, \Gamma_{forb}, m)$-VCS starting from the basis matrices S_0 and S_1:

Definition 2.14 *A visual cryptography Scheme $(\Gamma_{qual}, \Gamma_{forb})$-VCS, with the relative difference α and the set $\{(Q, d_Q)\}_{Q \in \Gamma_{qual}}$ is such that the basis matrices S_0 and S_1, satisfy the following properties:*

1. *Constrast, if* $Q = \{i_1, ..., i_n\} \in \Gamma_{qual}$*:*

   - *The OR operation of rows* $i_1, i_2, ..., i_n$ *of* S_0 *satisfies* $H \leq d_Q - \alpha m$
   - *The OR operation of rows* $i_1, i_2, ..., i_n$ *of* S_1 *satisfies* $H \geq d_Q$

2. *Security, if* $Q = \{i_1, ..., i_n\} \in \Gamma_{forb}$*:*

   - *The two collections of* $p \times m$ *matrices* D_0 *and* D_1*, obtained by restricting* S_0 *and* S_1 *to rows* $\{i_1, i_2, ..., i_n\}$ *are equal up to a column permutation.*

Moreover, [2] extends Theorem 2.1, where in a k out k problem $m \geq 2^{k-1}$ and $\alpha \leq \frac{1}{2^{k-1}}$.
In particular, we are interested in minimizing m for a given Access Structure. Hence, $m^*(\Gamma_{qual}, \Gamma_{forb})$ is defined as the smallest value of m for which $(\Gamma_{qual}, \Gamma_{forb}, m)$-VCS exists.
Let $\mathscr{P}' \subseteq \mathscr{P}$ and let us define:

$$\Gamma[\mathscr{P}']_{qual} = \{X \in \Gamma_{qual} : X \subseteq \mathscr{P}'\},$$
$$\Gamma[\mathscr{P}']_{forb} = \{Y \in \Gamma_{forb} : Y \subseteq \mathscr{P}'\}.$$

If follows that:

Lemma 2.1 *[2] In an Access tructure* $(\Gamma_{qual}, \Gamma_{forb})$ *with a set* $\mathscr{P}$ *of participants and* $(\Gamma[\mathscr{P}']_{qual}, \Gamma[\mathscr{P}']_{forb})$*. Then*

$$m^*(\Gamma[\mathscr{P}']_{qual}, \Gamma[\mathscr{P}']_{forb}) \leq m^*(\Gamma_{qual}, \Gamma_{forb}).$$

The previous lemma and theorem 2.1 imply:

Corollary 2.1 *[2] Let* $(\Gamma_{qual}, \Gamma_{forb})$ *be an Access Structure. starting from* $X \in \Gamma_0$ *and* $Y \in \Gamma_{forb}$ *for all* $Y \subseteq X$*, with* $Y \neq X$*:*

$$m^*(\Gamma_{qual}, \Gamma_{forb}) \geq 2^{|X|-1}.$$

Example 2.7 $(\Gamma_{qual}, \Gamma_{forb}, 3)$**-VCS with 4 participants.** Consider $\mathscr{P} = \{1, 2, 3, 4\}$. We want a $(\Gamma_{qual}, \Gamma_{forb}, 3)$-VCS with:

$$\Gamma_{qual} = \{\{1, 2\}, \{2, 3\}, \{3, 4\}, \{1, 2, 3\}\},$$
$$\Gamma_{forb} = \{\{1\}, \{2\}, \{3\}, \{4\}, \{1, 3\}, \{1, 4\}, \{2, 4\}\}$$

Then, we can set:

$$\Gamma_0 = \{\{1, 2\}, \{2, 3\}, \{3, 4\}\}$$

By recalling that $m \geq 2^k - 1$ and $\alpha \leq 1/(2^k - 1)$, we choose $m = 3$, $\alpha = 1/3$ and we can set S_0 and S_1 as follows (see also Figure 14):

$$S_0 = \begin{bmatrix} 101 \\ 100 \\ 100 \\ 110 \end{bmatrix}, \; S_1 = \begin{bmatrix} 011 \\ 100 \\ 001 \\ 110 \end{bmatrix}$$

By calculating d for each subset of Γ_{qual}, we can see that *contrast* properties for Γ_{qual} are fulfilled:

$$d_{\{1,2\}} = 3,$$
$$d_{\{2,3\}} = 2,$$
$$d_{\{3,4\}} = 3,$$
$$d_{\{1,2,3\}} = 3.$$

The Security property of Γ_{forb} is also fulfilled.

Moreover, there are subsets of $\mathscr{P}$ that are neither in Γ_{qual} nor in Γ_{forb}, meaning that this is not a *strong* Access Structure. In particular, these subsets are $\{1,2,4\}$, $\{1,3,4\}$, $\{2,3,4\}$.

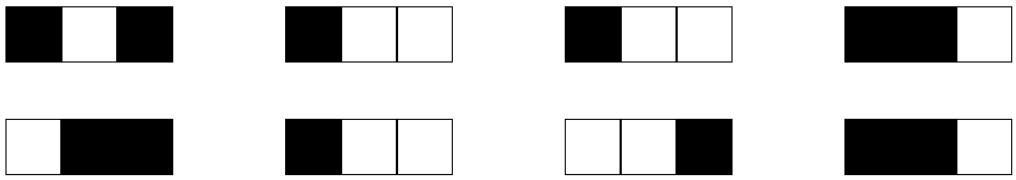


Figure 14: S_0 (on top) and S_1 (on bottom)

Example 2.8 Strong Access Structure with 6 participants. Let $\mathscr{P} = \{1,2,3,4,5,6\}$. Consider the strong Access Structures with basis $\Gamma_0 = \{\{i,j\} \mid i,j \in \mathscr{P} \wedge i \neq j\}$. This structure is equal to a 2 out of 6 scheme.

$$S_0 = \begin{bmatrix} 1100 \\ 1100 \\ 1100 \\ 1100 \\ 1100 \\ 1100 \end{bmatrix}, \; S_1 = \begin{bmatrix} 1010 \\ 1001 \\ 1100 \\ 0110 \\ 0101 \\ 0011 \end{bmatrix}$$

In this case the Access Structure is *strong*, in fact:

$\Gamma_{forb} = \{\{1\},\{2\},\{3\},\{4\},\{5\},\{6\}\}$ *and* $\Gamma_{qual} \cup \Gamma_{forb} = P(\mathscr{P})$.

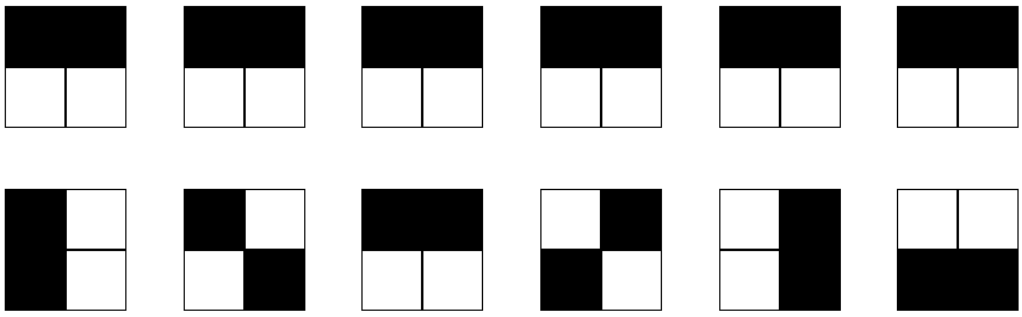


Figure 15: S_0 and S_1 for a strong Access Structure with 6 participants

2.2.2 Construction of Access Structures

We are now interested in the construction techniques to realize a visual cryptography for an Access Structure. In [2] three types of constructions are presented, the first one bases on *Cumulative Array*, the second one based on smaller schemes and the third one based on *perfect hashing* [4, 9, 7].
We will now describe the approach based on Cumulative Array as it is the one we have used during the experiments made for this study.

2.2.3 Construction using Cumulative Arrays

This construction is based on the method of Cumulative Arrays, introduced in [8].
A map of the relations between the sets in Γ_{qual}, called Cumulative Map, is needed to calculate the array that preserves the Access Structure, called Cumulative Array. From this array, S_0 and S_1 are generated.

Definition 2.15 *A* ***Cumulative Map*** (β, T) *for* Γ_{qual} *is a finite set* T *along*

with a mapping $\beta : \mathscr{P} \to 2^T$ *such that for* $Q \subseteq \mathscr{P}$*:*

$$\bigcup_{a \in Q} \beta(a) = T \iff Q \in \Gamma_{qual}$$

A cumulative map (β, T) for any Γ_{forb} can be constructed starting from the collection of the maximal forbidden sets $Z_M = \{F_1, ..., F_t\}$, which is:

$$Z_M = \{B \in \Gamma_{forb} : B \cup \{i\} \in \Gamma_{qual} \forall i \in \mathscr{P} \backslash B\}$$

By taking $T = \{T_1, ..., T_t\}$ and any $i \in \mathscr{P}$ let:

$$\beta(i) = \{T_j \mid i \notin F_j, 1 \leq j \leq t\}$$

for any $X \in \Gamma_{qual}$, holds that:

$$\bigcup_{i \in X} \beta(i) = T,$$

while any $X \in \Gamma_{forb}$ misses at least one element $T_j \in T$. From the cumulative mapping $\beta(i)$ for Γ_{qual}, a Cumulative Array for Γ_{qual} can be created.

Definition 2.16 *A* ***Cumulative Array*** *is a* $|\mathscr{P}| \times |T|$ *matrix* CA*, such that* $CA(i, j) = 1$ *if and only if* $i \notin F_j$*.*

Example 2.9 Let

$$\mathscr{P} = \{1, 2, 3, 4\},$$

$$\Gamma_0 = \{\{1, 2\}, \{2, 3\}, \{3, 4\}\},$$

$$Z_M = \{\{1, 4\}, \{1, 3\}, \{2, 4\}\}, \textit{ with}$$

$$F_1 = \{1, 4\},\ F_2 = \{1, 3\},\ F_3 = \{2, 4\}$$

In this case we have $|T|= 3$, because $|Z_M|= 3$, and CA is:

$$CA = \begin{bmatrix} 001 \\ 110 \\ 101 \\ 010 \end{bmatrix}$$

At this point, we have to use both the Cumulative Array and the basis matrices for a $|T|$ out of $|T|$ scheme, $\hat{S}_0$ and $\hat{S}_1$. For any fixed i let $j_{i,1}, ...j_{i,g_i}$ be the j such that $CA(i, j) = 1$. S_0 and S_1 are made from the OR operation of the rows $j_{i,1}, ...j_{i,g_i}$ of $\hat{S}_0$ and $\hat{S}_1$.

Theorem 2.2 *[2] In any strong Access Structure* $(\Gamma_{qual}, \Gamma_{forb})m$ *with the collection of the maximal forbidden sets* Z_M*, there exists a* $(\Gamma_{qual}, \Gamma_{forb}, m)$*-VCS with* $m = 2^{|Z_m|-1}$ *and* $t_x = m$*.*

Example 2.10 By extending the Example 2.9, consider:

$$\hat{S}_0 = \begin{bmatrix} 0011 \\ 0101 \\ 0110 \end{bmatrix}, \ \hat{S}_1 = \begin{bmatrix} 1100 \\ 1010 \\ 1001 \end{bmatrix}$$

The operation to generate the basis matrix S_0 from $\hat{S}_0$ and CA are the

following:

$$\begin{aligned} \textit{Third row of } \hat{S}_0 &= \begin{bmatrix} 0110 \end{bmatrix} \\ \textit{First row of } \hat{S}_0 \textit{ OR Second row of } \hat{S}_0 &= \begin{bmatrix} 0111 \end{bmatrix} \\ \textit{First row of } \hat{S}_0 \textit{ OR Third row of } \hat{S}_0 &= \begin{bmatrix} 0111 \end{bmatrix} \\ \textit{Second row } \hat{S}_0 &= \begin{bmatrix} 0101 \end{bmatrix} \end{aligned}$$

then, S_0 and S_1 are:

$$S_0 = \begin{bmatrix} 0110 \\ 0111 \\ 0111 \\ 0101 \end{bmatrix}, \; S_1 = \begin{bmatrix} 1001 \\ 1110 \\ 1101 \\ 1010 \end{bmatrix}$$

2.2.4 Non-Connected Access Structures

Access structures described so far are said to be *connected*.

Definition 2.17 *An Access Structure is* ***connected*** *if there is no partition of $\mathscr{P}$ into two non-empty sets $\mathscr{P}'$ and $\mathscr{P}''$ such that $\Gamma_0 \subseteq P(\mathscr{P}') \cup P(\mathscr{P}'')$.*

In this section we look deep into *non-connected* Access Structures, as they are required in the next chapters. This specific type of structure is useful because we can merge different Access Structures into a single one.
In [2] there is a proof of construction of Visual Cryptography Schemes for *non-connected* Access Structures, given the schemes for their connected parts.

In particular, given two different Access Structures $(\Gamma'_{qual}, \Gamma'_{forb})$ and $(\Gamma''_{qual}, \Gamma''_{forb})$ we would like to have a single Access Structure $(\Gamma_{qual}, \Gamma_{forb})$ such that:

$$\Gamma_{qual} = \Gamma'_{qual} \cup \Gamma''_{qual},$$
$$\Gamma_{forb} = \{X \cup Y \mid X \in \Gamma'_{forb}, Y \in \Gamma''_{forb}\}.$$

To verify the existance of this property, we need to be able to extend C_0 and C_1 of any $(\Gamma_{qual}, \Gamma_{forb}, m)$-VCS by a $n \times p$ boolean matrix D.
By concatenating D with $M \in C_0 \cup C_1$, we have that *constrast* and *security* properties for general Access Structures are satisfied and in particular $\{Q, d_Q\}_{Q \in \Gamma_{qual}}$ do not change from C_0 and C_1 to C'_0 and C'_1. The only change is the relative difference $\alpha' = \frac{(\alpha \cdot m)}{(m+t)}$.
The next theorem holds:

Theorem 2.3 *[2] Let C_0 and C_1 be the matrices for the Access Structure $(\Gamma_{qual}, \Gamma_{forb}, m)$-VCS, and let D be any $n \times p$ boolean matrix. $\circ$ is the operation for matrix concatenation. It follows that $C'_0 = \{M \circ D \mid D \in C_0\}$ and $C'_1 = \{M \circ D \mid D \in C_1\}$ constitute a $(\Gamma_{qual}, \Gamma_{forb}, m + p)$-VCS.*

Example 2.11 Consider a 2 out of 2 environment with $m = 2$:

$$C_0 = \left\{ \begin{bmatrix} 10 \\ 10 \end{bmatrix}, \begin{bmatrix} 01 \\ 01 \end{bmatrix} \right\} C_1 = \left\{ \begin{bmatrix} 10 \\ 01 \end{bmatrix}, \begin{bmatrix} 01 \\ 10 \end{bmatrix} \right\}$$

with $D = \begin{bmatrix} 1 \\ 1 \end{bmatrix}$, we obtain a 2 out of 2 scheme with $m = 3$:

$$C'_0 = \left\{ \begin{bmatrix} 101 \\ 101 \end{bmatrix}, \begin{bmatrix} 011 \\ 011 \end{bmatrix} \right\} C'_1 = \left\{ \begin{bmatrix} 101 \\ 011 \end{bmatrix}, \begin{bmatrix} 011 \\ 101 \end{bmatrix} \right\}$$

Theorem 2.4 *[2] Let* $(\Gamma'_{qual}, \Gamma'_{forb})$ *and* $(\Gamma''_{qual}, \Gamma''_{forb})$ *be two Access Structures of two different sets* $\mathscr{P}'$ *and* $\mathscr{P}''$*, and let* $(\Gamma_{qual}, \Gamma_{forb})$ *be their sum. If there exists a* $(\Gamma'_{qual}, \Gamma'_{forb}, m')$*-VCS and a* $(\Gamma''_{qual}, \Gamma''_{forb}, m'')$*-VCS, then there exists a* $(\Gamma_{qual}, \Gamma_{forb}, m)$*-VCS, with* $m = max\{m', m''\}$.

To prove this theorem, let C'_0 and C'_1 for $(\Gamma'_{qual}, \Gamma'_{forb})$, C''_0 and C''_1 for $(\Gamma''_{qual}, \Gamma''_{forb})$. We have that:

$$|C'_0| = |C'_1| = r',$$
$$|C''_0| = |C''_1| = r'',$$
$$m' > m''.$$

For Theorem 2.3, there exists a $(\Gamma''_{qual}, \Gamma''_{forb}, m')$-VCS.
Let C'''_0 and C'''_1 be the two collections of matrices for $(\Gamma''_{qual}, \Gamma''_{forb}, m')$-VCS.
The collections of matrices C_0 and C_1 for $(\Gamma_{qual}, \Gamma_{forb})$ are:

$$C_0 = \{M \mid M[\mathscr{P}'] \in C'_0, M[\mathscr{P}''] \in C'''_0\}$$
$$C_1 = \{M \mid M[\mathscr{P}'] \in C'_1, M[\mathscr{P}''] \in C'''_1\}$$

From any matrix in C'_0, there are r'' matrices to insert in C_0, and so we have that $|C_0| = |C_1| = r = r' \cdot r''$.
The two *contrast* properties for general Access Structures are easily verified.
To prove *security* property, let $X \in \Gamma'_{forb}$ and $M \in C'_0 \cup C'_1$.
η^0_X and η^1_X are the number of times that matrix $M[X]$ appears in the collections $\{A[X] \mid A \in C'_0\}$ and $\{A[X] \mid A \in C'_1\}$. From the *security* property for a general Access Structure, we have that $\eta^0_X = \eta^1_X$. We can deduce the same conclusion for $X \in \Gamma'''_{forb}$ and $M \in C'''_0 \cup C'''_1$, with μ^0_X and μ^1_X.

For $M \in C_0 \cup C_1$, γ_X^0 and γ_X^1 are the number of times that matrix $M[X]$ appears in the collections $\{A[X] \mid A \in C_0\}$ and $\{A[X] \mid A \in C_1\}$. We need to prove that for any $X \in \Gamma_{forb}$, $\gamma_X^0 = \gamma_X^1$ must be true.
If we consider $X \in \Gamma_{forb}$ and $X \subseteq \mathscr{P}' \setminus \mathscr{P}''$, then:

$$\gamma_X^0 = \eta_X^0 \cdot r'' = \eta_X^1 \cdot r'' = \eta_X^1$$

If $X \in \Gamma_{forb}$, $Y \in \Gamma'_{forb}$, $Z \in \Gamma''_{forb}$ and $X = Y \cup Z$, then:

$$\gamma_X^0 = \eta_Y^0 \cdot \mu_Z^0 = \eta_Y^1 \cdot \mu_Z^1 = \gamma_X^1$$

Hence, the property is proved.

Example 2.12 Suppose that $(\Gamma'_{qual}, \Gamma'_{forb})$ is a 2 out of 2 scheme with $\mathscr{P}' = \{1, 2\}$ and $(\Gamma''_{qual}, \Gamma''_{forb})$ is a 2 out of 2 scheme with $\mathscr{P}'' = \{3, 4\}$. The sum of this two Access Structure is:

$$\Gamma_{qual} = \{\{1, 2\}, \{3, 4\}\},$$
$$\Gamma_{forb} = \{\{1\}, \{2\}, \{3\}, \{4\}, \{1, 3\}, \{1, 4\}, \{2, 3\}, \{2, 4\}\}.$$

A scheme for $(\Gamma_{qual}, \Gamma_{forb})$ is obtained with:

$$C_0 = \left\{ \begin{bmatrix} 10 \\ 10 \\ 10 \\ 10 \end{bmatrix}, \begin{bmatrix} 01 \\ 01 \\ 01 \\ 01 \end{bmatrix}, \begin{bmatrix} 10 \\ 10 \\ 01 \\ 01 \end{bmatrix}, \begin{bmatrix} 01 \\ 01 \\ 10 \\ 10 \end{bmatrix} \right\}$$

$$C_1 = \left\{ \begin{bmatrix} 10 \\ 01 \\ 10 \\ 01 \end{bmatrix}, \begin{bmatrix} 01 \\ 10 \\ 10 \\ 01 \end{bmatrix}, \begin{bmatrix} 10 \\ 01 \\ 01 \\ 10 \end{bmatrix}, \begin{bmatrix} 01 \\ 10 \\ 01 \\ 10 \end{bmatrix} \right\}$$

2.3 Extensions for Visual Cryptography

In [3] the Visual Cryptography Scheme with Access Structure $(\Gamma_{qual}, \Gamma_{forb})$ on a set of participants $\mathscr{P}$ is extended with n images, one for each participant, that are encoded into transparencies. The transparencies generated are still meaningful, which means the participants can still recognize the original images. An example is provided in Figures 16, 17, 18 and 19.

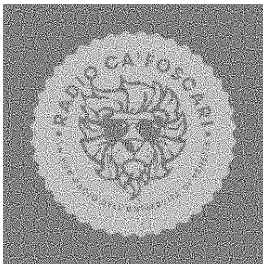
Figure 16: Secret image.

(a) Image 1.

(b) Image 2.

Figure 17: Participants in the Access Structure.

(a) Transparency 1.



(b) Transparency 2.

Figure 18: Transparencies

Figure 19: Secret image.

2.3.1 Extended Visual Cryptography model

In the Visual Cryptography Scheme for an Access Structure $(\Gamma_{qual}, \Gamma_{forb})$ with n participants, the secret image is encoded into n transparencies.
In this model the n images transparencies have to be meaningful. Therefore, $n+1$ images are needed; the first n images are associated with the n participants, the last one is the secret image. Any user must be able to recognize its starting image from its generated transparency.
To generate this kind of scheme, we need to take into consideration the color

of the pixels of the original n images. In particular, C_0 and C_1 of the previous schemes are extended to $C_0^{p_1,\ldots,p_n}$ and $C_1^{p_1,\ldots,p_n}$, where $p_i \in \{0,1\}$, $\forall\ i \in \{1,..,n\}$. To obtain the pixel c of the secret image, n pixels $p_1,..,p_n$ need to be considered, one for each image. Hence, the collections of matrix to be generated are $(C_0^{p_0,\ldots,p_n}, C_1^{p_0,\ldots,p_n})$, one for each combination of black and white pixel in the n original images. S_0 and S_1 are respectively the *basis matrices* that contain a set of shares that defines white and black pixels.

Definition 2.18 *$C_0^{p_1,\ldots,p_n}$ is the set of $n \times m$ matrices obtained by permuting the columns of $S_0^{p_1,\ldots,p_n}$. $C_1^{p_1,\ldots,p_n}$ is the set of $n \times m$ matrices obtained by permuting the columns of $S_1^{p_1,\ldots,p_n}$.*

The shares that have to be overlapped to reconstruct a white (respectively, black) pixel and preserve the color of the their respective original image pixel, are generated starting from the $n \times m$ basis matrix $S_0^{p_1,\ldots,p_n}$ (respectively, $S_1^{p_1,\ldots,p_n}$). The Hamming Weight H of the OR operation of $k \leq n$ rows in $S_0^{p_1,\ldots,p_n}$ (respectively, $S_1^{p_1,\ldots,p_n}$) gives a white (respectively, black) pixel in the reconstructed secret image, as described in Definition 2.6.
Formally, this extended Visual Cryptography model can be defined as follows:

Definition 2.19 *Let $(\Gamma_{qual}, \Gamma_{forb})$ be an Access Structure for n participants. 2^n pairs of collections of $n \times m$ boolean matrices $\{(C_0^{p_1,\ldots,p_n}, C_1^{p_1,\ldots,p_n})\}_{p_1,..,p_n \in \{0,1\}}$ constitute a $(\Gamma_{qual}, \Gamma_{forb}, m)$-EVCS, if there exist a relative difference for the transparencies α_T, a relative difference for the recover of the secret image α_S, and $\{Q, d_Q\}_{Q \in \Gamma_{qual}}$, such that the following contrast, security and preservation properties are satisfied:*

1. *Contrast, for any* $Q \in \Gamma_{qual}$ *and for any* $p_1, ...p_n \in \{0,1\}$*:*

   - *For any* $M \in C_0^{p_1,...,p_n}$, $H(M_Q) \leq d_Q - \alpha_T \cdot m$.
   - *For any* $M \in C_1^{p_1,...,p_n}$, $H(M_Q) \geq d_Q$.

2. *Security, for any* $p_1, ...p_n \in \{0,1\}$*:*

   - *the two collections of* $q \times m$ *matrices* $D_0^{p_1,..,p_n}$ *and* $D_1^{p_1,..,p_n}$*, obtained by removing the row of the missing participants from* C_0 *and* C_1*, are indistinguishable.*

3. *Preservation*

   - *Any participant can recognize the image of its transparency, i.e,* $\forall\ i \in \{1, ..., n\}$ *and* $\forall\ c_1, ..., c_{i-1}, c_{i+1}, ..., c_n \in \{0,1\}$*:*

$$\min_{M \in \mathscr{M}_0} H(M_i) - \max_{M \in \mathscr{M}_1} H(M_i) \geq \alpha_S \cdot m$$

$$\text{where } \mathscr{M}_0 = \bigcup\nolimits_{p_1,...,p_{i-1},p_{i+1},...,p_n \in \{0,1\}} C_0^{p_1,...,p_{i-1},0,p_{i+1},...,p_n}$$

$$\text{and } \mathscr{M}_1 = \bigcup\nolimits_{p_1,...,p_{i-1},p_{i+1},...,p_n \in \{0,1\}} C_0^{p_1,...,p_{i-1},1,p_{i+1},...,p_n}$$

Constrast and Security properties are similar to the ones of the previous models.

Preservation is a property which ensures that any user will recognize the image of its transparency.

Theorem 2.5 *[3] In a k out of k scheme extended VCS, the upper bound on*

m, α_F and α_S is:

$$2^{k-1}\alpha_F + \frac{k}{k-1}\alpha_S \leq 1,$$
$$m \geq 2^{k-1} + 2.$$

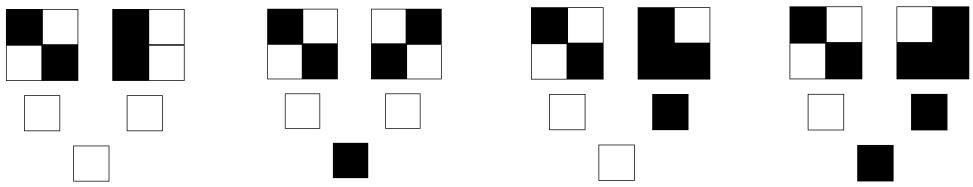
Example 2.13 2 out of 2 scheme. Let $\mathscr{P} = \{1, 2\}$. The collections $C_c^{p_1,p_2}$, where $c, p_1, p_2 \in \{0, 1\}$, are obtained by permuting the columns of the following matrices, with $\alpha_T = \alpha_S = \frac{1}{4}$:

$$S_0^{00} = \begin{bmatrix} 1001 \\ 1010 \end{bmatrix} \text{ and } S_1^{00} = \begin{bmatrix} 1001 \\ 0110 \end{bmatrix},$$

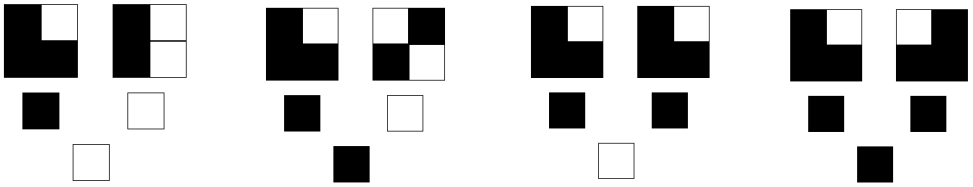
$$S_0^{01} = \begin{bmatrix} 1001 \\ 1011 \end{bmatrix} \text{ and } S_1^{01} = \begin{bmatrix} 1001 \\ 0111 \end{bmatrix},$$

$$S_0^{10} = \begin{bmatrix} 1011 \\ 1010 \end{bmatrix} \text{ and } S_1^{10} = \begin{bmatrix} 1011 \\ 0110 \end{bmatrix},$$

$$S_0^{11} = \begin{bmatrix} 1011 \\ 1011 \end{bmatrix} \text{ and } S_1^{11} = \begin{bmatrix} 1011 \\ 0111 \end{bmatrix}.$$



(a) S_0^{00} (b) S_1^{00} (c) S_0^{01} (d) S_1^{01}



(e) S_0^{10} (f) S_1^{10} (g) S_0^{11} (h) S_1^{11}

Figure 20: EVCS: 2 out of 2 scheme. In each Figure, the first row represents the shares, the second row represents participant pixel and the third one represents the secret pixel.

2.3.2 Construction for k out of k EVCS

The following section describes the algorithm of [3] for the generation of a k out of k Extended Visual Cryptography Scheme, starting from an admissibile region for the relative differences between a black and a white pixel in the transaprencies (α_t) and in the resulting secret image (α_s).

Definition 2.20 *An **admissible region** $\mathscr{AR}$ for α_T and α_S is:*

$$\mathscr{AR} = \left\{ (\alpha_F, \alpha_S) \mid \alpha_F > 0, \alpha_S > 0, \text{ and } 2^{k-1}\alpha_F + \frac{k}{k-1}\alpha_S \leq 1 \right\}.$$

Theorem 2.6 *[3] For any pair of rational numbers* $(\alpha_T, \alpha_S) \in \mathscr{AR}$*, a* k *out of* k *ECVS scheme with* α_T *and* α_s *exists.*

The proof of the previous theorem follows.
Let $(\alpha_T, \alpha_S) \in \mathscr{AR}$ and consider $(\alpha_T, \alpha_S) = (\frac{a}{b}, \frac{c}{d})$. Let also

$$h = bd(k-1) - 2^{k-1}ad(k-1) - kbc.$$

Since $(\alpha_T, \alpha_S) \in \mathscr{AR}$, $h \geq 0$. Now, let T be a $k \times h$ 0-matrix, S_0 and S_1 the *basis* matrices of the k out of k scheme, where the columns of S_0 are all the boolean k-vectors with even number of 1, and the columns of S_1 are all the boolean k-vectors with odd number of 1.
A k ouf of k EVCS is generated by Algorithm 1, iterated for each pixel of the original image:

Algorithm 1: Basic algorithm to generate a k out of k EVCS [3]

Input :

- The basis matrices S_0, S_1
- The $k \times h$ matrix T
- $p_1, \ldots, p_k \in \{0, 1\}$, colours of the pixel in the original k images
- $c \in 0, 1$, colour of the pixel of the secret image

Output:

- The matrix M

Construct a $k \times k$ matrix D:

for $i = 1$ **to** k **do**

  if $p_i = 1$ **then**
    set all the entries of row i of D to 1

  else
    set the entry (i, i) of D to 1 and all remaining entries of row i to 0.

  end

end

$C_c^{p_1,\ldots,p_k}$ is constructed by permuting the columns of:

$$S_c^{p_1,\ldots,p_k} = \begin{cases} \underbrace{S_0 \circ \ldots \circ S_0}_{(k-1)ad} \circ \underbrace{D \circ \ldots \circ D}_{bc} \circ T & \text{if } c = 0 \\ \underbrace{S_1 \circ \ldots \circ S_1}_{(k-1)ad} \circ \underbrace{D \circ \ldots \circ D}_{bc} \circ T & \text{if } c = 1 \end{cases}$$

M is a matrix randomly chosen from $C_c^{p_1,\ldots,p_k}$

$S_O^{p_1,\ldots,p_n}$ and $S_1^{p_1,\ldots,p_n}$, generated by the previous algorithm, are basis matrices of a k out of k EVCS with $\alpha_T = a/b$ and $\alpha_S = c/d$. Let $Q = \{1, \ldots, k\}$, for any $p_1, \ldots, p_k \in \{0, 1\}$, for any $M \in C_0^{p_1,\ldots,p_k}$ and for any $M' \in C_1^{p_1,\ldots,p_k}$. We have that:

$H(M_Q) = 2^{k-1}(k-1)ad + kbc,$
$H(M'_Q) = (2^{k-1} - 1)(k-1)ad + kbc = H(M_Q) - (k-1)ab = H(M_Q) - \alpha_T \cdot m.$

Consequently, by setting $d_Q = H(M_Q)$, *constrast* properties are satisfied. It is easy to see that also *security* and *preservation* properties are satisfied.
As well it holds that for any $p_1, \ldots p_k \in \{0, 1\}$, $i \in Q$, $M \in C_c^{p_1,\ldots,p_{i-1},0,p_{o+1},\ldots,p_k}$ and $M' \in C_c^{p_1,\ldots,p_{i-1},1,p_{o+1},\ldots,p_k}$:

$$H(M_i) - H(M'_i) = bc(k-1) = \alpha_s \cdot m.$$

2.3.3 General construction for EVCS

We now explain the algorithm used in this study for the construction of an Extended Visual Cryptography Scheme. A first attempt to implement Visual Cryptography with the use of hypergraph colorings is given in [5]. We show the general construction of [3], which is an extension of the previous work.

Definition 2.21 *A **hypergraph** is a pair $(X, \mathscr{B})$, where $\mathscr{B} \subseteq P(\mathscr{B})$, that is the powerset of $\mathscr{B}$. X is the set of vertices of the hypergraph, and $\mathscr{B}$ is the set of edges.*

A ***q-colouring*** *for a hypergraph* $H = (X, \mathscr{B})$ *is a function* $\phi : X \to \{1, \ldots, q\}$*:*

$$|\{\phi(x) : x \in B\}| \geq 2, \quad \forall B \in \mathscr{B} : |B| \geq 2.$$

The ***chromatic number*** *of* H*,* $\chi(H)$*, is the minimum integer* q *under which a* q*-colouring of* H *exists.*

To generate a EVCS, we will use an arbitrary *q-colouring* ϕ of $(\mathscr{P}, \Gamma_0)$.
To encode the whole image, we iterate the following algorithm to all the pixel of the secret image.

Algorithm 2: Algorithm to generate the shares for EVCS

Input :

- $(\Gamma_{qual}, \Gamma_{forb})$ for a set $\mathscr{P}$ of n participants
- S_0 and S_1
- $p_1, \ldots, p_k \in \{0, 1\}$, colours of the pixel in the original k images
- $c \in 0, 1$, colour of the pixel of the secret image
- ϕ for $(\mathscr{P}, \Gamma_0)$

Output:

- The matrix M

Construct a $n \times q$ matrix D:

for $i = 1$ **to** n **do**

  if $p_i = 1$ **then**
    set all the entries of row i of D to 1

  else
    set the entry $(i, \phi(i))$ of D to 0 and all remaining entries of row i to 1.

  end

end

$C_c^{p_1,\ldots,p_k}$ is constructed by permuting the columns of:

$$S_c^{p_1,\ldots,p_k} = \begin{cases} S_0 \circ D & \text{if } c = 0 \\ S_1 \circ D & \text{if } c = 1 \end{cases}$$

M is a matrix randomly chosen from $C_c^{p_1,\ldots,p_k}$

In [3], the authors prove that the previous algorithms produce an EVCS. We first observe that $(C_0^{p_1,\ldots,p_n}, C_1^{p_1,\ldots,p_n})$ constitutes a VCS for the Access Structure $(\Gamma_{qual}, \Gamma_{forb})$, and so *constrast* and *security* properties are verified. To verify the *preservation* property, consider the ith participant. If its pixel is white, it is encoded into $m+q$ subpixels, and $H(S_i^0)+q-1$ are black. If the pixel is black, it is encoded into $m+q$ subpixels, and $H(S_i^1)+q$ are black. So, we have that $\alpha_S = 1/m$. Therefore, participant i is able to distinguish his initial image from the transparency.

Theorem 2.7 *[3] If there exists a* $(\Gamma_{qual}, \Gamma_{forb}, m)$*-VCS with* S_0 *and* S_1 *and a* ***q-colouring*** *for a hypergraph* $(\mathscr{P}, \Gamma_0)$*, then there exists* $(\Gamma_{qual}, \Gamma_{forb}, m+q)$*-EVCS.*

Example 2.14 Generation of a 2 out of 2 EVCS. For this example we use a *2-colouring* of the hypergraph $(\{1,2\},\{1,2\})$. For the basic 2 out of 2 example, we have:

$$S_0 = \begin{bmatrix} 10 \\ 10 \end{bmatrix},\ S_1 = \begin{bmatrix} 10 \\ 01 \end{bmatrix}$$

The generated matrix D, is:

$$D = \begin{cases} \begin{bmatrix} 01 \\ 10 \end{bmatrix} & \text{if } p_1 = p_2 = 0 \\ \begin{bmatrix} 01 \\ 11 \end{bmatrix} & \text{if } p_1 = 0 \text{ and } p_2 = 1 \\ \begin{bmatrix} 11 \\ 10 \end{bmatrix} & \text{if } p_1 = 1 \text{ and } p_2 = 0 \\ \begin{bmatrix} 11 \\ 11 \end{bmatrix} & \text{if } p_1 = p_2 = 1 \end{cases}$$

Example 2.15 General Access Structure. Let $\mathscr{P} = \{1, 2, 3, 4, 5\}$, $\Gamma_{qual} = \{\{1, 2, 3, 4\}, \{1, 5\}\}$ and $\Gamma_{forb} = P(\mathscr{P}) \setminus \Gamma_{qual}$. A Visual Cryptography for $(\Gamma_{qual}, \Gamma_{forb})$ can be obtained by the following matrices:

$$S_0 = \begin{bmatrix} 00001111 \\ 00110011 \\ 01010101 \\ 01101001 \\ 00001111 \end{bmatrix}, \; S_1 = \begin{bmatrix} 00001111 \\ 00110011 \\ 01010101 \\ 10010110 \\ 11110000 \end{bmatrix}.$$

Let the *hypergraph* $H = (\mathscr{P}, \Gamma_0)$. We have $\chi(H) = 2$.

We can define a 2-colouring, in which $\phi(1) = 1$, $\phi(2) = \phi(3) = \phi(4) = \phi(5) = 2$.

By applying the algorithm for a general EVCS for S_0^{01000} and S_1^{10111}, we can

generate the 5×2 matrix D:

$$D = \begin{bmatrix} 01 \\ 11 \\ 10 \\ 10 \\ 10 \end{bmatrix}.$$

Therefore, S_0^{01000} is:

$$S_0^{01000} = \begin{bmatrix} 00001111 \\ 00110011 \\ 01010101 \\ 01101001 \\ 00001111 \end{bmatrix} \circ \begin{bmatrix} 01 \\ 11 \\ 10 \\ 10 \\ 10 \end{bmatrix} = \begin{bmatrix} 0000111101 \\ 0011001111 \\ 0101010110 \\ 0110100110 \\ 0000111110 \end{bmatrix},$$

and S_1^{01000} is:

$$S_1^{01000} = \begin{bmatrix} 00001111 \\ 00110011 \\ 01010101 \\ 10010110 \\ 11110000 \end{bmatrix} \circ \begin{bmatrix} 01 \\ 11 \\ 10 \\ 10 \\ 10 \end{bmatrix} = \begin{bmatrix} 0000111101 \\ 0011001111 \\ 0101010110 \\ 1001011010 \\ 1111000010 \end{bmatrix}$$

.

3 Shared image extensions for Visual Cryptography

So far, the described schemes rely on at least two participants to recover a specific secret image. In [6] the author considers the problem of sharing different secrets between a set of participants, but they do not consider the possiblity of having a unique shared image.

We now propose an Access Structure $(\Gamma_{qual}, \Gamma_{forb})$, such that each participant has her specific secret, starting from a unique shared image k. In particular, we want to prove that the Access Structure $(\Gamma_{qual}, \Gamma_{forb})$, such that Γ_{qual} contains each couple (participant, shared image), preserves the characteristics of a Visual Cryptography Model, being a Non-Connected Access Strucure.

We know formally define the Access Structure:

Definition 3.1 *Let* $\mathscr{P} = \{1, ..., n\}$ *be the set of participants and* $\mathscr{S} = \{s_1, ..., s_n\}$ *be the set of secret images. Consider the union of* $\mathscr{P}$ *with a new participant* k, $\mathscr{P}^* = \mathscr{P} \cup \{k\}$.

$\forall i \in \mathscr{P}\ \exists\ (\Gamma^i_{qual}, \Gamma^i_{forb})$ *s.t.* $s_i \in \mathscr{S}$ *can be recovered by* Γ^i_{qual}.

Each Access Structure $(\Gamma^i_{qual}, \Gamma^i_{forb})$ *for participant* $i \in \mathscr{P}$ *to recover sercret image* s_i, *can be seen as an indipendent* 2 *out of* 2 *model, with* $\Gamma^i_{qual} = \{\{i, k\}\}$ *and* $\Gamma_{qual} = \{\{i\}, \{k\}\}$, *where* k *is the shared participant for* $\mathscr{P}$. *Then, by overlapping transparency of* i *and* k, s_i *is obtained.*

At this point, consider $(\Gamma_{qual}, \Gamma_{forb})$*, defined over* $\mathscr{P}$ *as:*

$$\Gamma_{qual} = \bigcup_{\forall i \in \mathscr{P}} \Gamma^i_{qual}$$
$$\Gamma_{forb} = \bigcup_{\forall i \in \mathscr{P}} \Gamma^i_{forb}$$

For Theorem 2.3, $(\Gamma_{qual}, \Gamma_{forb})$ coincides with the union of indipendet Non-Connected Access Structure and consequently can be considered as a unique 2 out of n $(\Gamma_{qual}, \Gamma_{forb}, m)$-VCS.
It is important to stress the fact that the Theorem 2.3 does not introduce any constraint on the secret of the n Access Structures, so even with a different secret for each qualified set the Theorem holds. This result is a consequence of the fact that this theorem does not consider the secret of the Access Structure but only the definition of the Basis Matrices.

We now discuss some characteristics we would like to have in our ideal Shared Image Visual Cryptography Model. An important property we would like to have is scalability, in fact we would like to add as much participants as we want even after the creation of the shared key, e.g., during a train journey we want to be able to generate tickets at any time. Moreover, in a real world scenario, the overlap of two images with no structure is not an easy task. To take advantage of Visual Cryptography, a user should be able to recover the secret easily, e.g., by using a smartphone application to scan the transparencies. The main problem is the difficulty of scanning a transparency,

which in reality is undistinguishable from a random noise image and so it has no structure at all. In this section we discuss two different models that overcome these two problems.

In particular, the first model defines a pre-computed shared image and at each time, a new participant can generate her specific secret starting from the shared image and her starting image. In the second model, we loose the scalability property in order to improve usability, by letting each participant derive her share from a password.

3.1 A pre-computed shared key model

In the first model, called pre-computed shared key model, we first generate the secret image, and starting from both it and the secret associated to the participant, we generate the transparencies. In this model, the transparencies have to be meaningful.

By using the Access Structure proposed at the beginning of this section, each qualified set is formed by a participant and the secret image.Then, we need to verify the *constrast*, *security* and *preservation* properties for a single subscheme of a single participant with the precomputed shared key k.

But first, we require the computation to generate k. With equal m to each submodel, an easy algorithm is to random generate shares that are valid for the set of collections $C_m^{p_0,p_1}$.

Algorithm 3: Algorithm to generate the shared key

Input :

- size of the secret image s
- size of share m
- set of collections $\{C_c^{00}, C_c^{01}, C_c^{10}, C_c^{11}\}$

Output:

- shared key k

Generate shared key k of size $s \cdot m$

for *each pixel in the secret image* **do**

Generate a random share contained the set of the collections

Assign the share to key k

end

We need now to verify the three properties only for the collections of $2 \times m$ matrices $C_0^{p,0}$,$C_0^{p,1}$,$C_1^{p,0}$,$C_1^{p,1}$, where $p \in \{0, 1\}$. Recall that, like in Description 2.3.1, we still require the relative difference α_T to recover the image of participant i, the relative difference α_S to recover the secret image and the threshold d:

1. Contrast
   - The OR operation of the pair $M \in C_0^{p,0} \cup C_0^{p,1}$, where one of the two shares is equal to the share of k, has $H \leq d - \alpha_T \cdot m$
   - The OR operation of the pair $M \in C_1^{p,0} \cup C_1^{p,1}$, where one of the two shares is equal to the share of k, has $H \geq d$
2. Security

- The only share of the participant is not enough to recover the secret, in particular a share taken from $M \in C_0^{p,0} \cup C_0^{p,1}$ is indistinguishable from a pixel taken from $M \in C_1^{p,0} \cup C_1^{p,1}$
- The only shared key is not enough to recover the secret, in particular a share taken from $M' \in C_0^{p,0} \cup C_0^{p,1}$ is indistinguishable from a share taken from $M'' \in C_1^{p,0} \cup C_1^{p,1}$

3. Preservation

   - The participant can recognize the image of its transparency, as in extended Visual Cryptography properties in Description 2.3.1.

This model is then a particular case of the model explained in Description 2.3.1, preserving all its characteristics, with the only difference that each Access Structure have access to a different secret, but this property does not affect the basis matrices.

Definition 3.2 *Let* $(\Gamma_{qual}, \Gamma_{forb})$ *be an Access Structure for* n *participants in the set* $\mathscr{P}$*, and* $\mathscr{P}^* = \mathscr{P} \cup \{k\}$ *such that* $\Gamma_{qual} = \{(p,k)\}, \forall p \in \mathscr{P}$*,* $\Gamma_{forb} = P(\mathscr{P}) \setminus \Gamma_{qual}$ *and* k *the shared image. 4 pairs of collections of* $2 \times m$ *boolean matrices* $\{(C_0^{p_1,p_k}, C_1^{p_n,\ldots,p_k})\}_{p_1,..,p_n,p_k \in \{0,1\}}$ *constitute a* $(\Gamma_{qual}, \Gamma_{forb}, m)$*-pre-computed shared image EVCS, if there exist a relative difference for the transparencies* α_T*, a relative difference for the recover of the secret image* α_S*, and* $\{Q, d_Q\}_{Q \in \Gamma_{qual}}$*, such that the following contrast, security and preservation properties are satisfied:*

1. *Contrast, for any* $p_1, \ldots p_n \in \{0,1\}$*:*

- *For any* $M \in C_0^{p_i,k}$, $H(M) \leq d_Q - \alpha_T \cdot m$.
- *For any* $M \in C_1^{p_i,k}$, $H(M) \geq d_Q$.

2. *Security, for any* $p_1, ...p_n \in \{0,1\}$*:*

   - *the two collections of* $q \times m$ *matrices* $D_0^{p_i,k}$ *and* $D_1^{p_i,k}$*, obtained by removing the row of the missing participants from* $C_0^{p_i,k}$ *and* $C_1^{p_i,k}$*, are indistinguishable.*

3. *Preservation*

   - *Any participant can recognize the image of its transparency, i.e,* $\forall\ i \in \{1, ..., n\}$ *and* $\forall\ c_1, ..., c_{i-1}, c_{i+1}, ..., c_n \in \{0,1\}$*:*

$$\min_{M \in \mathscr{M}_0} H(M_i) - \max_{M \in \mathscr{M}_1} H(M_i) \geq \alpha_S \cdot m$$

$$\text{where } \mathscr{M}_0 = \bigcup\nolimits_{p_1,...,p_{i-1},p_{i+1},...,p_n \in \{0,1\}} C_0^{p_1,...,p_{i-1},0,p_{i+1},...,p_n}$$

$$\text{and } \mathscr{M}_1 = \bigcup\nolimits_{p_1,...,p_{i-1},p_{i+1},...,p_n \in \{0,1\}} C_0^{p_1,...,p_{i-1},1,p_{i+1},...,p_n}$$

The generation of the transparency t for participant i, with shared key k is described by the following algorithm, and its results are shown in figures 21, 22 and 23.

Algorithm 4: Algorithm to generate the transparency for participant i

Input :

- size of secret image s
- size of share m
- shared key k
- starting image for participant i
- secret image for participant i
- set of collections $\{C_c^{00}, C_c^{01}, C_c^{10}, C_c^{11}\}$

Output:

- transparency t for i

Generate transparency t of size $s \cdot m$

for *each pixel in the secret image* **do**

  if *secret image pixel is white* **then**

    if *shared key pixel is white* **then**

      Search in C_0^{00} and C_0^{01} for a pair with shared key share

    else

      Search in C_0^{10} and C_0^{11} for a pair with shared key share

    end

  else

    if then

      Search in C_1^{00} and C_1^{01} for a pair with shared key share

    else

      Search in C_1^{00} and C_1^{01} for a pair with shared key share

    end

  end

  Assign the share that in the pair is not the one of k, to t

end

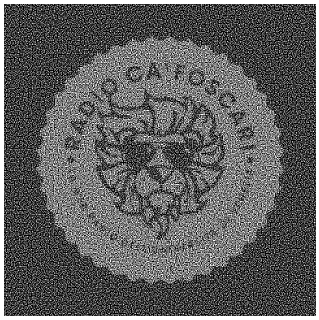
(a) Secret image for participant 1

(b) Secret image for participant 2

(c) Image for participant 1

(d) Image for participant 2

(e) transparency for participant 1



(f) transparency for participant 2

Figure 21: Images

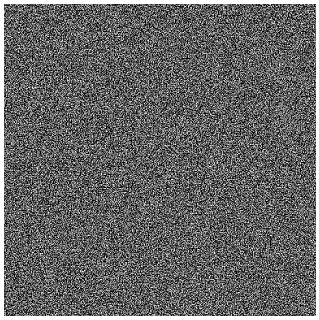
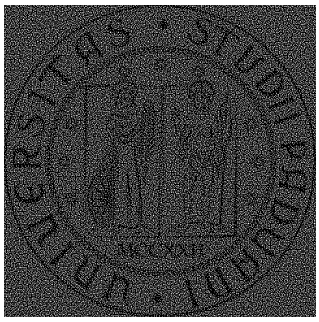


Figure 22: Shared key k

(a) transparency 1 and k overlapped



(b) transparency 2 and k overlapped

Figure 23: Example of a priori Shared key extended Visual Cryptography with two participants

Example 3.1 Generation of transparencies.

Let $\mathscr{P} = \{1, 2\}$ with shared key k, $m = 2$ and $\alpha_T = \alpha_S = 1/4$.

At iteration i of the algorithm, the pixel of the starting image for participant 1 is white, the pixel of the starting image for participant 2 is black, the share of the key is 1001, the secret image pixel for 1 is black and the secret image pixel for 2 is white.

A possible share for 1 is 0110 and for 2 is 1101. In fact:

$$H(1) = 1001 \ OR \ 0110 = 1111$$

$$H(2) = 1001 \ OR \ 1101 = 1101$$

Remind that the generation of transparency for each participant can be done independently from the others.

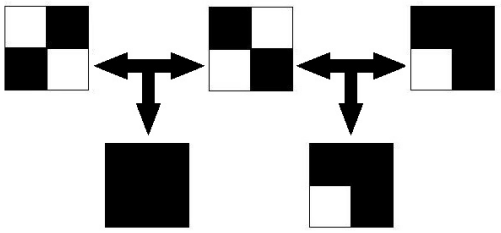


Figure 24: Transparencies of participant 1, shared key and participant 2 give access to two different secret pixels

3.1.1 Problems of the model

In theory, this model is really powerful, but in reality it is impossible to scan a transparency, as it is indistinguishable from a random noise and so it has

no structure.

We would like to have a transparency that maintains a structure of a barcode such that it can be easily scanned by any mobile device. But, by giving it a structure, we would lose the *Security* property of the model.

3.2 A pre-computed cyphertext model

To overcome the problems presented in the previous scheme, we introduce a model in which the cyphertexts can be pre-computed so that we can exploit a "visual key derivation" function [10] in order to recover the image starting from a password. The shared image is then computed starting from all the transparencies of the participants. The idea behind the "visual key derivation" function is to generate randomly the transparencies of each participant through the use of PBKDF2 (Password-Based Key Derivation Function 2).
Let $\mathscr{P}$ be the set of n participants, each one with its respective secret image. We want to generate the shared key k starting from n random generated transparencies, such that each participant's transparency overlapped with it, generates the secret image for that participant.
In our model, each pixel in the secret image becomes a set of $n \times m$ subpixels in the transparencies. In this way, we can generate the shared key k by giving importance to m specific subpixels for each participant, such that by overlapping them, we get information of the ith secret image. An intuition is given in Figure 25.

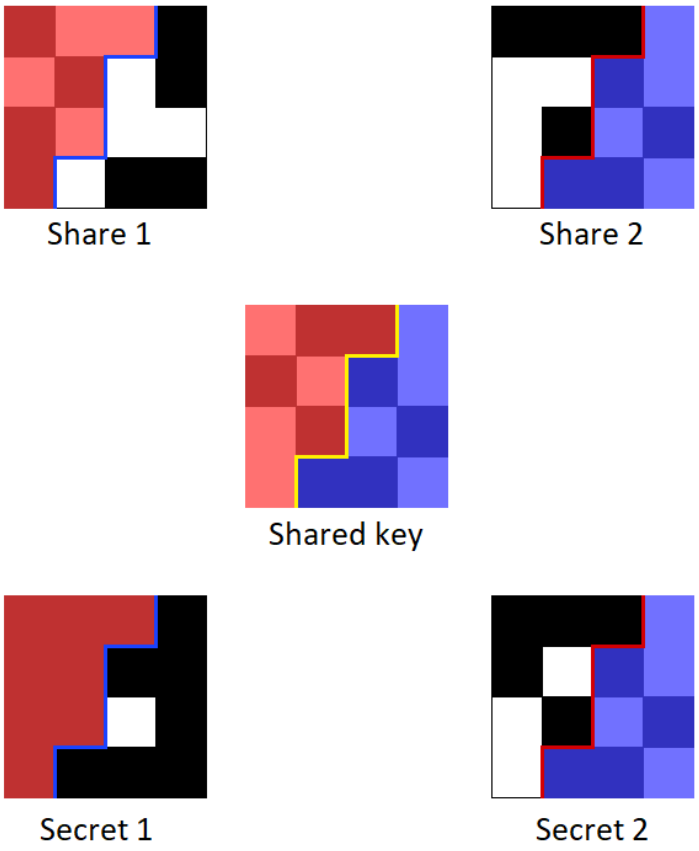


Figure 25: example of pre-computed cyphertext model with 2 participants and $m = 8$. Red subpixels are related to secret of participant 1. Blue subpixels are related to secret of participant 2.

The size of the transparencies is at least $n \times m \times$size of secret images. In practice, we want the transparencies to preserve the structure of the image and so we need each pixel to become the smallest square root that is greater than $n \times m$. For example by having $m = 4$, $n = 2$ and $m \times n = 8$, each pixel in the transparency will have size $m' = 9$.

By overlapping a transparency with k, the secret image for participant i is

preserved in the $\frac{100}{n}\%$ of the image, while the rest of the image are random pixels. By inspecting the resulting image we can recognize the secret.
The main problem of this implementation is that with the increasing of participants, the difficult to visually recognize the image increases.
The overall method can be then seen as a basic Visual Cryptography Scheme described in 2.1 with n participants and size of shares m'.
Security property of this model is in fact equal to the one in 2.1.
Contrast property consider a specific pattern p of subpixels for a participant:

- for any white pixel in the secret image and for any chosen pattern p of subpixels, of size $m < m'$,in the transparency t and in the shared key k, $p(t)$ OR $p(k) \leq d - \alpha m$;
- for any black pixel in the secret image and for any chosen pattern p of subpixels, of size $m < m'$,in the transparency t and in the shared key k, $p(t)$ OR $p(k) \geq d$.

Definition 3.3 *Let $\mathscr{P} = \{1, ..., n\}$ and $\mathscr{P}^* = \mathscr{P} \cup \{k\}$. The two collections of $n \times m$ matrices C_0 and C_1 define a pattern p for a $(\Gamma_{qual}, \Gamma_{forb}, m)$-precomputed cyphertext VCS with the relative difference α and its set $\{(Q, d_Q)\}_{Q \in \Gamma_{qual}}$, if the following constrast and security properties are satisfied:*

1. *Contrast, for any $(i, k) \in \Gamma_{qual}$:*
   - *$\forall$ white pixels in the secret image of participant i, chosen a pattern p in each subpixel for i, of size $m \leq m'$, given the transparency t_i and the shared key k, $H(p(t)\ OR\ p(k)) \leq d_Q - \alpha m$*

- $\forall$ *black pixels in the secret image of participant* i*, chosen a pattern* p *in each subpixel for* i*, of size* $m \leq m'$*, given the transparency* t_i *and the shared key* k*,* $H(p(t)\ OR\ p(k)) \geq d_Q$

2. *Security:*

   - *The two collections of* $q \times m$ *matrices* D_0 *and* D_1*, obtained by restricting each* $n \times m$ *matrices in* C_0 *and* C_1 *to rows* $\{i_1, i_2, ..., i_n\}$*, are indistinguishable in the sense that they contain the same patterns with the same frequencies.*

The following algorithm shows the computation fo the shared key.

Algorithm 5: Algorithm to generate the shared key

Input :

- shared key k
- transparencies $1, ..., n$
- secret image for participant i, s_i
- patterns $p_1, ..., p_n$
- C_0, C_1

Output:

- Shared image for $\mathscr{P}$

for *each* $i \in \mathscr{P}$ **do**

  for *each pixel in the secret image* s_i **do**

    if *secret image pixel for* i *is white* **then**

      Search in C_0 for a pair with transparency pattern p_i of the subpixel i

    else

      Search in C_1 for a pair with transparency pattern p_i of the subpixel i

    end

    Assign the share that in the pair is not the one of p_i, to k in the pattern p_i

  end

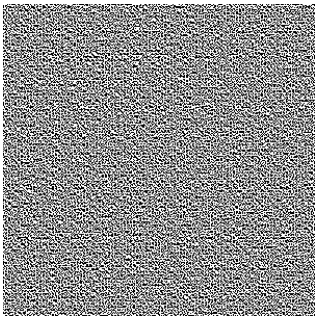
end

In figures 26, 27, 28 and 29 we show the results of the implementation of this method with two participants.

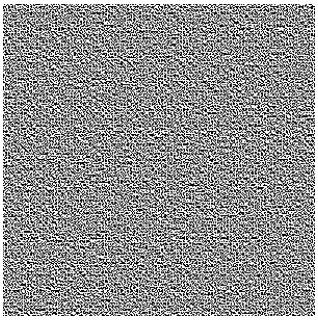
(a) Secret image 1

(b) Secret image 2

Figure 26: Secret images



(a) transparency 1



(b) transparency 2

Figure 27: Transparencies

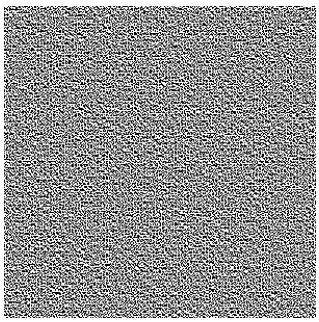
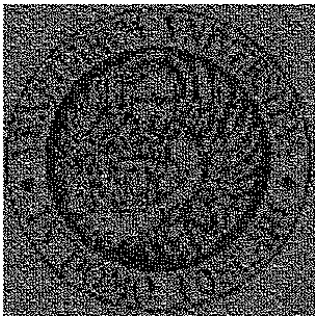
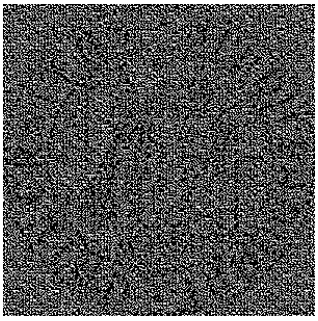


Figure 28: Shared key



(a) Secret image 1 overlapped



(b) Secret image 2 overlapepd

Figure 29: Secret images overlapped

Example 3.2 2 participants. The following example with 2 participants can better explain this implementation.

Let $\mathscr{P} = \{1, 2\}$, $m = 4$, size of each share equal to 9, $S_0 = \begin{bmatrix} 1100 \\ 1100 \end{bmatrix}$ and $S_1 = \begin{bmatrix} 1100 \\ 0011 \end{bmatrix}$.

Each transparency is randomly generated by taking subpixels from C_0 and C_1.

At iteration i, secret image pixel for 1 is black and its share is 101010011 and

secret image pixel for 2 is white, with share equal to 110010101.
The shared key generated is 010110110. Indeed, if we look at the first 4 subpixels of transparency for 1 and k, we have 1010 OR 0101 = 1111, which is a black pixel. If we look at the last 4 subpixels of 2 ORed with k, 0011 OR 0110 = 1110, which is a white pixel. The 5th pixel is 1 for each trasparecy, and it is added to preserve the original form of the secrets.

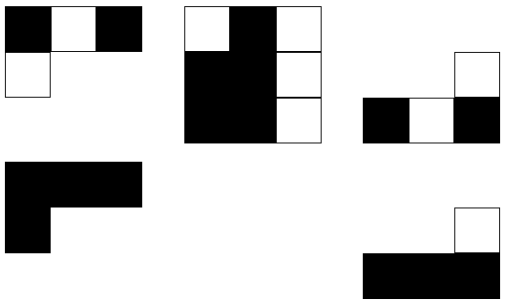


Figure 30: first row, significant share of 1, shared key, significant share of 2. Second row, share 1 OR k, share 2 OR k.

3.2.1 Problems of the model

While the previous model is scalable, this one requires the exact number of participant to generate each cyphertext. Moreover, to generate the final shared key, each cyphertext is required.
Another problem is that the secret image recovered is not completely visible, as a part of that is still random noise. One way to overcome this obstacle, is to save the position of the significant position of the participant in the cyphertext. By doing that, we can entirely recognize the secret image for

that participant by taking only the overlap of the significant parts.

In a real case scenario, a 2D-barcode could contain both the password to generate the cyphertext and the position of the significant position in the cyphertext for a specific participant.

4 Conclusions

In this thesis we implemented two models for Visual Cryptography that use a unique shared image to recover a specific secret image for each participant. These two models can be seen as an alternative to Classic Cryptography, that uses only images and that do not require any computation to recover the secret.

In the basic Visual Cryptography model, a secret image is recovered by the overlap of two images that are indistinguishable from random noise. This model can be extended to more than two images, called k out of k scheme, or in at least k participants between a set of n participants, with $k \leq n$, called k out of n scheme.

In order to let only a specific set of participants recover a secret, Access Structures for Visual Cryptography are required. In the literature, Visual Cryptography is extended in a way that some qualified subsets of the set of participants are able to recover the secret image by overlapping their transparencies, while some others cannot. This scheme is called General Access Structure. One of the two implemented models needed a way to give a meaning to the images that are overlapped. In literature, an extension for Visual Cryptography that exploits Access Structures, gives to each transparency the shape of a specific images chosen by the owner of the transparency. Both methods can be seen as an union of separated Access Structures, one for each participant. Different Access Structures can be merged into a unique one, called Non-Connected Access Structure. This specific structure preserves the characteristics of a classic one.

The first model we implemented considers scalability issues. The shared im-

age is first computed. While it looks like a random noise, the specific image for each participant is meaningful. We can then consider each couple (participant, shared image) as a separate Access Structure that recover a different secret. The union of this Access Structure is a Non-Connected Access Structure. Thanks to the pre-computation of the shared image, we can add as much participants as we want, at any time. The main problem of this implementation is that participant images cannot be scanned. A possible solution to this problem is to generate them starting from a key derivation function. The second model, starting from a specific number of participants, first generates the participant images from a key derivation function. The shared image is then computed starting from all the images. To make this model work, each subpixel of the shared image is divided by each participant, and each of them take in consideration a portion of it to recover the secret. While this model is more usable, it lacks of scalability and with more participants the images become bigger.

Future work should focus on finding a model that is at the same time scalable and usable, in order to make it relevant in real-world applications. For what concerns the first model, while it is unlikely to find a function that generates the participants images starting from the shared image, a possible solution to this problem could be finding a structure for the images in order to let them be scannable by a barcode reader. In the second model, a possible study could be made on the division of the subpixels between the participants. It would be interesting to answer to these questions. Is it possible to share a part of the subpixels between more than one participant? Can we then reduce the size of the images based on the number of participants?

References

[1] G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson. Constructions and bounds for visual cryptography. In F. Meyer and B. Monien, editors, *Automata, Languages and Programming*, pages 416–428, Berlin, Heidelberg, 1996. Springer Berlin Heidelberg.

[2] G. Ateniese, C. Blundo, A. D. Santis, and D. R. Stinson. Visual cryptography for general access structures. *Information and Computation*, 129(2):86 – 106, 1996.

[3] G. Ateniese, C. Blundo, A. D. Santis, and D. R. Stinson. Extended capabilities for visual cryptography. *Theoretical Computer Science*, 250(1):143 – 161, 2001.

[4] M. Atici, S. Magliveras, D. R. Stinson, and W. d. Wei. Some recursive constructions for perfect hash families. *Journal of Combinatorial Designs*, 4, 04 1996.

[5] C. Blundo, A. De Santis, and D. R. Stinson. Extended schemes for visual cryptography. preprint, 10 1996.

[6] S. Droste. New results on visual cryptography. In N. Koblitz, editor, *Advances in Cryptology — CRYPTO '96*, pages 401–415, Berlin, Heidelberg, 1996. Springer Berlin Heidelberg.

[7] M. L. Fredman and J. Komls. On the size of separating systems and families of perfect hash functions. *SIAM Journal on Algebraic Discrete Methods*, 5(1):61–68, 1984.

[8] K. Martin, G. Simmons, and W.-A. Jackson. The geometry of shared secret schemes. *Bulletin of the ICA*, 1:71–88, 1991.

[9] K. Mehlhorn. On the program size of perfect and universal hash functions. In *23rd Annual Symposium on Foundations of Computer Science (sfcs 1982)*, pages 170–175, Nov 1982.

[10] T. Moretto. Secure 2d barcode based on visual cryptography. Master's thesis, Univeristy Ca'Foscari of Venice, 2018.

[11] M. Naor and A. Shamir. Visual cryptography. In A. De Santis, editor, *Advances in Cryptology — EUROCRYPT'94*, pages 1–12, Berlin, Heidelberg, 1995. Springer Berlin Heidelberg.

[12] A. Shamir. How to share a secret. *Commun. ACM*, 22(11):612–613, Nov. 1979.

[13] D. R. Stinson. Decomposition constructions for secret-sharing schemes. *IEEE Transactions on Information Theory*, 40(1):118–125, Jan 1994.

[14] E. R. Verheul and H. C. A. van Tilborg. Constructions and properties of k out of n visual secret sharing schemes. *Designs, Codes and Cryptography*, 11(2):179–196, May 1997.