Visual Cryptography
Models, Issues, Applications and New Directions

Paolo D'Arco(✉) and Roberto De Prisco

Dipartimento di Informatica, University of Salerno,
Via Giovanni Paolo II, 132, 84084 Fisciano, SA, Italy
{pdarco,robdep}@unisa.it

Abstract. Since its introduction, visual cryptography has received considerable attention within the cryptographic community. In this paper we give a quick look at the salient moments of its history, focusing on the main models, on open issues, on its applications and on some prospectives.

Keywords: Visual cryptography · Models · Applications · Secure computation

1 Introduction

Visual Cryptography, in its simplest form, enables the sharing, in an unconditionally private way, of a black-and-white secret image among a set of parties.

In a sharing phase, each party receives a transparency containing a printed image, which looks like a collection of black and white random pixels. The transparency does not leak any information about the secret image. In a reconstruction phase, when a properly chosen subset of transparencies are superposed and perfectly aligned, the secret image is reconstructed.

The peculiarity of the technique is that the *human visual system* performs the reconstruction process: no machinery, computing mathematical operations, is required. Hence, it can be used by *everyone*: once the transparencies have been generated and privately distributed, cryptographic tools or skills are not needed to reconstruct the secret image.

Introduced by Naor and Shamir [44] in 1994 in the cryptographic community, due to its aesthetic attractiveness and to the elegant mathematical combinatorial structures underlying the design of the schemes, it has been the subject of active and extensive investigations. Currently, it is a sound research field with a large body of literature.

1.1 Superposing Transparencies

Let us look at a simple example in order to understand which problems need to be solved to produce a secure sharing. The secret image can be seen as a

I. Bica and R. Reyhanitabar (Eds.): SECITC 2016, LNCS 10006, pp. 20–39, 2016.
DOI: 10.1007/978-3-319-47238-6_2

matrix of black and white pixels[1]. Each transparency contains a random-looking collection of black pixels and white pixels. When two or more transparencies are superposed and perfectly aligned, in each position of the resulting image, there is a black pixel if in the corresponding position of the transparencies there is *at least* a black pixel. While, the pixel is equal to white if and only if in the corresponding position in *all* the transparencies the pixels are white. Fig. 1 summarizes the superposition law, while Fig. 2 reproduces the visual effect for two transparencies.

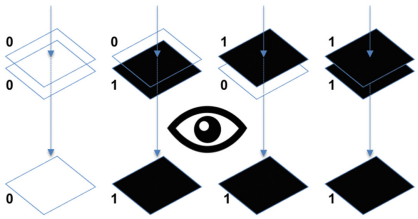

Fig. 1. Superposition law. The human eye performs the logical `or` operation.

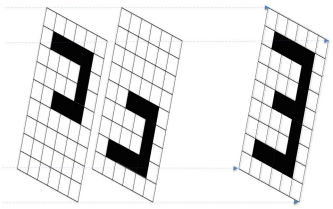

Fig. 2. Example of transparencies superposition.

Hence, for any privacy notion we could think about, it is clear that a *simple split* of the black pixels of the secret image among the pixels of the transparencies, in such a way that when superposed the secret image is reconstructed, *does not* work. It surely enables the reconstruction of the secret image but, at the same time, each transparency gives to his holder *partial information* about the secret image: each black pixel in the transparency corresponds to a black pixel in the reconstructed image.

Therefore, to avoid information leakage by each transparency, we need some non trivial sharing form. Fortunately, *two nice approaches* yield suitable solutions. To get the flavor, let us consider the basic case, in which a secret image is split in two transparencies. The first approach, by Naor and Shamir [44], encodes each pixel of the original image with a *collection* of black and white *subpixels* in each transparency, in such a way that each collection on each transparency could correspond to both a white pixel and a black pixel in reconstructed form.

[1] White pixels are actually transparent pixels, but we refer to them as to white pixels.

Only through the superposition the *nature* of the pixel is determined. With this encoding, a reconstructed white pixel of the original image has *always* some black subpixels, but it is still *visually distinguishable* from a black pixel because a black pixel has *more* black subpixels than a white one.

The second approach, due to Kafri and Keren [32], encodes a black pixel with a randomly chosen complementary pair of pixels on the two transparencies, i.e., black on the first and white on the second or vice versa, while it encodes a white pixel with two equal pixels on each transparency, i.e., either with a white pixel on both transparencies or with a black pixel on both transparencies, choosing, for each pixel, one of the two possibilities uniformly at random. Hence, a black pixel is always reconstructed correctly, while a white pixel is reconstructed *half of the times correctly* and *half of the times erroneously*. Even though half of the white pixels are erroneously reconstructed, the secret image, as a whole, is still *visually intelligible* when the transparencies are superposed but on a darker background compared to the original secret image, because half of the white pixels of the secret image have been turned to black.

Intuitively, it is clear that with both the encodings a transparency by itself does not provide any information, in an unconditionally secure way, on the corresponding secret image. Therefore, as we show in the following sections, in a *deterministic* way or in a *probabilistic* way, the secret image can be securely shared and visually recovered.

1.2 Organization of the Paper

We overview part of the large field of visual cryptography. More precisely, in Sect. 2 we describe Naor and Shamir's model and Kafri and Keren's model. We briefly discuss also Yang's model and its generalization due to Cimato et al. In Sect. 3 we provide a common framework for the formalization of the notion of visual cryptography scheme. Then, in Sect. 4, we discuss the main issues in the design: contrast, pixel expansion, randomness reduction. We survey some important results and point out open problems. Later on, is Sect. 5, we give a quick look at alternative models for visual cryptography: we consider models for grey and color images, for meaningful transparencies, for multiple secrets, as well as models using alternative properties for the physical superposition, and models robust against cheating. Then, in Sect. 6, we describe some classical applications proposed in the literature. This section offers to the reader some hints about potential uses of the techniques in real life. Finally, in Sect. 7, we focus on a new approach, which uses visual cryptography for general secure computation. Conclusions and final remarks are given in Sect. 8, which closes the paper.

2 Models for Visual Cryptography

In this section we introduce the models which implement the two ideas described before: the *deterministic* model, as we refer to the Naor and Shamir's model, and the *random grid* model, as we refer to the Kafri and Keren's model.

Deterministic Model. The deterministic model was introduced by Naor and Shamir [44]. In this model, each pixel of the secret image is expanded into a number $m \geq 2$ of subpixels in each transparency. Hence, the transparencies and the reconstructed secret image are larger than the original secret image. Consequently, the parameter m is referred to as the *pixel expansion*. Moreover, two thresholds ℓ and h, $0 \leq \ell < h \leq m$, together define the contrast, i.e., the visual quality, with which the secret image is reconstructed. More precisely, when the transparencies are superposed and aligned and the secret image is reconstructed, it is guaranteed that:

- if the secret pixel is *white*, then among the reconstructed m subpixels that correspond to the secret pixel, there are *at most* ℓ black subpixels
- if the secret pixel is *black*, then among the reconstructed m subpixels, there are *at least* h black subpixels.

Basically, the threshold ℓ quantifies the *maximal level of darkness* allowed in a collection of m subpixels which reconstructs a white pixel, while the threshold h quantifies the *minimal level of darkness* required in a collection of m subpixels which reconstructs a black pixel. Fig. 3 shows an example.

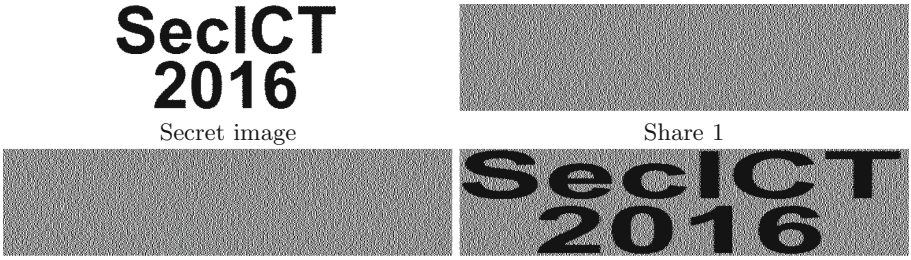

Fig. 3. Example in the deterministic model.

Random Grid Model. The random grid model was introduced by Kafri and Keren [32]. Historically, this is the first model for visual cryptography, found independently and before the deterministic model [44]. Nevertheless, it received attention only after the deterministic model had been discovered and presented at the cryptographic community, when a large number of researchers started investigating the subject[2]. The model introduced by Kafri and Keren is called *random grid* because it uses random black and white images as building blocks for sharing secret images. In this model there is *no pixel expansion*, i.e., the parameter m is equal to 1. Therefore, the shares and the reconstructed image have the *same*

[2] Kafri and Keren proposed three constructions for sharing a secret image between two parties. Naor and Shamir, on the other hand, gave a general model, formalizing the properties that visual cryptography schemes need to satisfy, and constructions and bounds for threshold schemes. They also coined the term *Visual Cryptography*.

sizes of the original image. As we have explained before, the reconstruction is a probabilistic process since errors may occur: some white pixels are reconstructed as black pixels[3] but the original image is still visually intelligible. Fig. 4 shows an example.

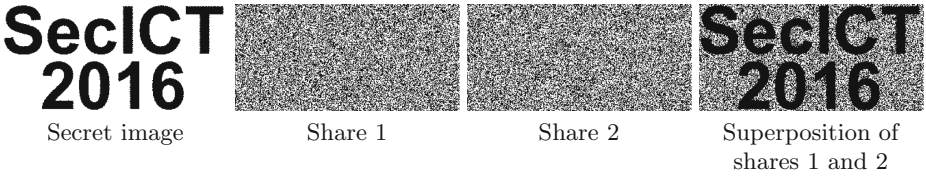

Fig. 4. Example in the random grid model.

Probabilistic Model. The probabilistic model was introduced by Yang [50] and generalized by Cimato et al. [13]. Each pixel of the secret image can be represented with a number $m \geq 1$ of pixels in each transparency. There still exist thresholds ℓ and h, $0 \leq \ell < h \leq m$, which together define the contrast.

For $m > 1$ (Cimato et al.'s model), it can be seen as a variant of the deterministic model, where the warranty about the reconstruction holds *only with*

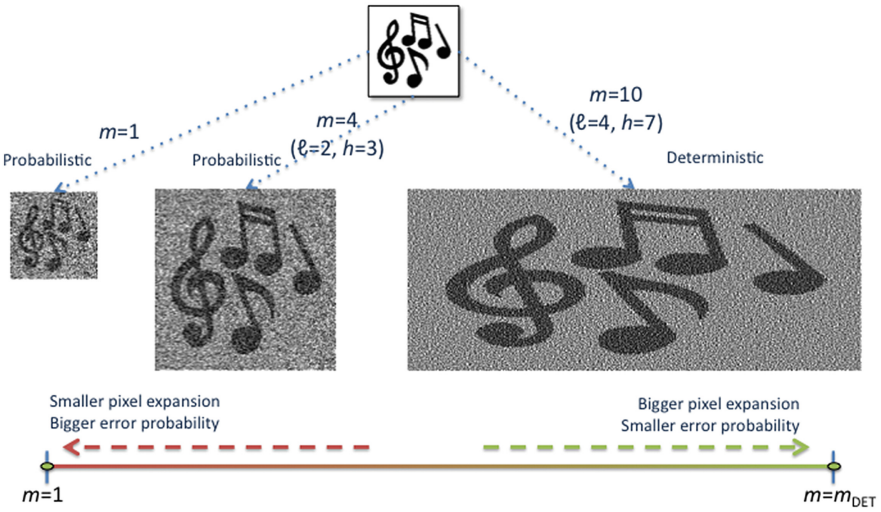

Fig. 5. Models

[3] In the other two constructions proposed by Kafri and Keren there are errors of both types, i.e., white pixels are reconstructed as black and black pixels are reconstructed as white. However, reconstruction is still possible as long as the errors are "not too many".

high probability. Precisely, occasionally the reconstruction can be wrong, allowing a reconstructed white pixel to have more than ℓ black subpixels, and a reconstructed black pixel to have less than h black subpixels.

Models Equivalence. In [23] it has been proved that all of the above models are strongly tied together. More specifically, for $m = 1$ (Yang's model), the probabilistic model is the same as the random grid model, while for m big enough the probabilistic model becomes deterministic. Hence, all the models described can be thought of as parameterized on the pixel expansion m, and on one extreme ($m = 1$) we have the random grid/probabilistic model, while on the other extreme (m big enough) we have the deterministic model. In between the two extremes we have the generalized probabilistic model; the intermediate probabilistic models trade the pixel expansion with the error probability, as depicted in Fig. 5.

3 Visual Cryptography Schemes

Independently of the choice, the models can be described by using a common framework. Let us introduce it.

3.1 Collections of Matrices

Let I be a secret image that needs to be visually shared among a set $\mathcal{P} = \{1, 2, \ldots, n\}$ of n parties. A trusted party, called the *dealer*, in order to share I, generates n images, printed on transparencies, called *shares*, and distributes them to the parties, giving in a private way one share to each party. Some subsets of parties, called *qualified*, are able to reconstruct the secret by pooling together and superposing their shares. All other subsets of parties, called *forbidden*, do not infer any information about the secret image neither by superposing their shares nor by any other computation on them.

A *visual cryptography scheme* (*VCS*, for short) is a method for encoding the secret image I into the n shares. The encoding process associates, to each pixel of the secret image I, a collection[4] of m subpixels that collectively represent a pixel of the secret image, in each of the n shares.

A *distribution matrix* M is an $n \times m$ matrix which represents the encoding of a single pixel by means of n shares. More precisely, row i of M represents the collection of subpixels printed on share i, which is used to encode a secret pixel of I. We use 0 to denote a white subpixel and 1 to denote a black subpixel. With this notation, the matrices are binary matrices and the superposition of subpixels corresponds to the logical `or` operation (see Fig. 1). However, since the symbols ∘ and • are self-explanatory, where convenient, we also use ∘ and • to denote, respectively, white and black.

[4] We stress that for deterministic visual cryptography it must be $m \geq 2$, i.e., the pixel *expansion* is unavoidable. The probabilistic and the random grid visual cryptography models instead allow $m = 1$.

A visual cryptography scheme is specified by *two collections* of distribution matrices, denoted with $\mathcal{C}_\circ = \{M_\circ^1, M_\circ^2, \ldots, M_\circ^{r_0}\}$ and $\mathcal{C}_\bullet = \{M_\bullet^1, M_\bullet^2, \ldots, M_\bullet^{r_1}\}$. To share a secret pixel of I, the dealer operates as follows: if the secret pixel is white, then he randomly chooses a distribution matrix from $\mathcal{C}_\circ$, and gives row i to party i; while, if the secret pixel is black, he randomly chooses a distribution matrix from $\mathcal{C}_\bullet$ and gives row i to party i. The sharing process is repeated for *every* pixel of the secret image.

An *access structure* $\mathcal{A} = (\mathcal{Q}, \mathcal{F})$ is a specification of the qualified subsets of parties $\mathcal{Q}$ and of the forbidden subsets of parties $\mathcal{F}$. Notice that if $Q \in \mathcal{Q}$, then any superset Q' of Q must belong to $\mathcal{Q}$. Another natural requirement is that any subset P of parties is either qualified or forbidden[5]. In most cases the access structure is a *threshold* access structure: $\mathcal{Q}$ consists of all the subsets of at least k parties, while $\mathcal{F}$ consists of all the subsets with at most $k-1$ parties, with $2 \leq k \leq n$. Such structures are referred to as (k, n)-*threshold* access structures.

Given a distribution matrix M and a set of parties P, we denote with M_P the submatrix of M consisting only of the rows corresponding to parties in P. Moreover, we denote with $\texttt{Sup}(M)$ the superposition of the shares represented by the rows of M. Notice that $\texttt{Sup}(M)$ is a binary vector where the i^{th} element is equal to the `or` of the i^{th} column of M. Hence, $\texttt{Sup}(M_Q)$ is the pixel reconstructed by the parties of a qualified set Q. Given a vector v, we denote with $w(v)$ the Hamming weight of v, the number of 1s (i.e., the number of black subpixels) in v.

Definition 1. *A $(\mathcal{Q}, \mathcal{F})$ deterministic visual cryptography scheme $\mathcal{S}$ consists of two collections $\mathcal{C}_\circ$ and $\mathcal{C}_\bullet$ of $n \times m$ distribution matrices such that there exists two integers ℓ and h, such that $0 \leq \ell < h \leq n$, for which the following conditions are satisfied.*

1. **Reconstructability.** *For any qualified set Q it holds that: for any $M \in \mathcal{C}_\circ$, we have that $w(\texttt{Sup}(M_Q)) \leq \ell$ while, for any $M \in \mathcal{C}_\bullet$, we have that $w(\texttt{Sup}(M_Q)) \geq h$.*
2. **Security.** *For any forbidden set F, it holds that the two collections $\mathcal{C}_\circ[F] = \{M_F | M \in \mathcal{C}_\circ\}$ and $\mathcal{C}_\bullet[F] = \{M_F | M \in \mathcal{C}_\bullet\}$ are indistinguishable in the sense that they contain the same matrices with the same frequencies.*

The first condition guarantees that reconstructed white and black pixels are visually distinguishable. The second essentially says that a pixel reconstructed by a forbidden subset of parties can correspond to a white pixel or to a black pixel with exactly the same probability. We refer to ℓ and h as to the *contrast thresholds*.

Notice that, in many schemes, the collection $\mathcal{C}_\circ$ (resp. $\mathcal{C}_\bullet$) consists of all the matrices that can be obtained by permuting all the columns of a matrix B° (resp. $B^\bullet$). Therefore, the matrices B° and $B^\bullet$ are called the *base matrices*.

[5] In a more general form, it is possible to consider access structures where there are some subsets that are neither qualified nor forbidden; in such a case we simply don't care about what those subsets of parties can do with the shares.

When a scheme is described with base matrices the reconstructability and the security conditions can be simplified to the following:

1. **Reconstructability.** For any qualified set Q, we have that $w(\mathtt{Sup}(B^{\circ}_{Q})) \leq \ell$ and that $w(\mathtt{Sup}(B^{\bullet}_{Q})) \geq h$.
2. **Security.** For any forbidden set F, the two matrices B°_{F} and $B^{\bullet}_{F}$ are the same up to a permutation of the columns.

For the random grid model the contrast is defined by means of the *average light transmission*, which is the amount of light that can pass through a part of an image[6] Instead of considering a single pixel, the definition considers the whole image. More precisely, given a subset G of pixels of an image I, the average light transmission $\lambda(G)$ of G is

$$\lambda(G) = \frac{\#\text{white-pixels(G)}}{\#\text{pixels(G)}},$$

the number of white pixels in G, divided by the total number of pixels in G. Let $\mathcal{W}_I$ and $\mathcal{B}_I$ be, respectively, the entire white and black regions of I, and let $\mathcal{W}_I(R)$ and $\mathcal{B}_I(R)$ be the corresponding white and black regions of R, the reconstructed version of I. Denoting with $\lambda_{\circ}(R) = \lambda(\mathcal{W}_I(R))$ and $\lambda_{\bullet}(R) = \lambda(\mathcal{B}_I(R))$ the following definition holds.

Definition 2. *A $(\mathcal{Q}, \mathcal{F})$ random grid visual cryptography scheme $\mathcal{S}$ consists of two collections $\mathcal{C}_{\circ}$ and $\mathcal{C}_{\bullet}$ of $n \times 1$ distribution matrices such that, denoting with R the reconstructed version of I, the following two conditions are satisfied:*

1. **Reconstructability.** *There exists two thresholds, $\lambda_{\circ}$ and $\lambda_{\bullet}$, with $\lambda_{\circ} > \lambda_{\bullet}$, such that, for any qualified set Q, it holds that $\lambda_{\circ}(R) \geq \lambda_{\circ}$ and $\lambda_{\bullet} \geq \lambda_{\bullet}(R)$.*
2. **Security.** *For any forbidden set F, it holds that $\lambda_{\circ}(R) = \lambda_{\bullet}(R)$.*

The first condition guarantees that reconstructed white and black areas are visually distinguishable. The second essentially says that in the image reconstructed by a forbidden subset of parties the white and black areas are perfectly indistinguishable.

3.2 Examples of Schemes

To get some confidence with the framework, let us consider some simple examples. Assume that the set S of secret images contains all black-and-white square images I of $n \times n$ pixels. Let use denote with $Shr(\cdot)$ the algorithm used in the sharing phase by the dealer, and with $Rec(\cdot)$ the algorithm used in the reconstruction phase by a set of qualified parties. We consider collections consisting of exactly two distribution matrices, that is, $\mathcal{C}_{\circ} = \{\mathcal{C}_{\circ,0}, \mathcal{C}_{\circ,1}\}$, and $\mathcal{C}_{\bullet} = \{\mathcal{C}_{\bullet,0}, \mathcal{C}_{\bullet,1}\}$. The $Shr(\cdot)$ and $Rec(\cdot)$ algorithms are:

[6] Recall that in the model, for sharing a secret image, a random black and white image (a random grid) is used as starting point.

$(2,2)$-VCS
Shr(I) For every $i,j = 1,\ldots,n$, Choose uniformly at random $r_{i,j} \in \{0,1\}$ Use row k of $\mathcal{C}_{I(i,j),r_{i,j}}$ to set $sh_k(i,j)$, for $k = 1,2$. Output (sh_1, sh_2)
Rec(sh_1, sh_2) Return $I = \mathtt{Sup}(sh_1, sh_2)$.

The collections of distribution matrices, $\mathcal{C}_\circ = \{\mathcal{C}_{\circ,0}, \mathcal{C}_{\circ,1}\}$ and $\mathcal{C}_\bullet = \{\mathcal{C}_{\bullet,0}, \mathcal{C}_{\bullet,1}\}$, given by

$$\mathcal{C}_\circ = \left\{ \begin{bmatrix} \circ & \bullet \\ \circ & \bullet \end{bmatrix}, \begin{bmatrix} \bullet & \circ \\ \bullet & \circ \end{bmatrix} \right\} \qquad \mathcal{C}_\bullet = \left\{ \begin{bmatrix} \circ & \bullet \\ \bullet & \circ \end{bmatrix}, \begin{bmatrix} \bullet & \circ \\ \circ & \bullet \end{bmatrix} \right\}$$

realize a $(2,2)$-VCS in the deterministic model. Indeed, both the Reconstructability and Security conditions hold.

- The contrast thresholds are $\ell = 1$ and $h = 2$. A white pixel is always reconstructed as a white subpixel and a black subpixel. A black pixel is always reconstructed as two black subpixels
- The restrictions of the collections $\mathcal{C}_\circ$ and $\mathcal{C}_\bullet$ to submatrices of one row contain the same submatrices with the same frequencies.

The scheme is a special case ($k = n = 2$) of the (k,n)-VCS threshold scheme, given by Naor and Shamir in [44]. This scheme has been used to generate the example in Fig. 3.

Similarly, the following two collections of distribution matrices $\mathcal{C}_\circ = \{\mathcal{C}_{\circ,0}, \mathcal{C}_{\circ,1}\}$, and $\mathcal{C}_\bullet = \{\mathcal{C}_{\bullet,0}, \mathcal{C}_{\bullet,1}\}$, where

$$\mathcal{C}_\circ = \left\{ \begin{bmatrix} \circ \\ \circ \end{bmatrix}, \begin{bmatrix} \bullet \\ \bullet \end{bmatrix} \right\} \qquad \mathcal{C}_\bullet = \left\{ \begin{bmatrix} \circ \\ \bullet \end{bmatrix}, \begin{bmatrix} \bullet \\ \circ \end{bmatrix} \right\}$$

realize a $(2,2)$-VCS in the random grid model (or the probabilistic model with $m = 1$). Indeed, both the Reconstructability and Security conditions hold.

- The two thresholds $\lambda_\circ$ and $\lambda_\bullet$ are $\lambda_\circ = \frac{1}{2}$ and $\lambda_\bullet = 0$. Indeed, $\lambda_\circ(R) = \frac{1}{2}$ while $\lambda_\bullet(R) = 0$.
- For each share sh it holds that $\lambda_\circ(sh) = \lambda_\bullet(sh) = \frac{1}{2}$.

The scheme is the first one of the three $(2,2)$-VCS schemes, given by Kafri and Keren in [32]. This scheme has been used to generate the example in Fig. 4.

4 Issues

Constructions for (k,n)-VCS threshold schemes, for any integer k and n, such that $k \leq n$, and for general access structures are known both for the deterministic model and the random grid (probabilistic) model, e.g., [2,10,11,23,44,57]. However, some issues are still open. Let us have a quick look at them.

4.1 Contrast

For deterministic schemes, three main measures of contrast have appeared in the literature: γ_{NS} (Naor and Shamir [44]), γ_{VV} (Verheul and van Tilborg [48]) and γ_{ES} (Eisen and Stinson [24]). The measure introduced by Naor and Shamir [44]) is defined by:

$$\gamma_{\mathrm{NS}}(\mathcal{S}) = \frac{h-\ell}{m}. \tag{1}$$

Verheul and van Tilborg [48], on the other hand, defined:

$$\gamma_{\mathrm{VV}}(\mathcal{S}) = \frac{h-\ell}{m(2m-h-\ell)}, \tag{2}$$

while, Eisen and Stinson [24], used:

$$\gamma_{\mathrm{ES}}(\mathcal{S}) = \frac{h-\ell}{2m-h}. \tag{3}$$

Other notions have also been proposed by other authors, e.g., [18,40]. The constructions for threshold and general access structures in the deterministic model [2,44] have been evaluated according to γ_{NS}, e.g., [2,5,6,27,36,37,44]. However, Eisen and Stinson have provided convincing arguments in support of γ_{ES}, which currently seems to be the notion with the best match with the real world. Hence, we need to understand whether γ_{ES} is actually the optimal notion and, if this is the case, how to construct contrast-optimal schemes with respect to such a notion.

4.2 Pixel Expansion

In the deterministic model, pixel expansion and contrast are strictly related. Hence, some lower bounds which hold for γ_{NS} e.g., [4,44], might need to be revised with respect to the new notion γ_{ES}. Currently, we have lower bounds only for $(2, n)$-VCS threshold schemes with respect to γ_{ES} (see [24]).

4.3 Randomness Reduction

The issue of reducing the randomness the dealer needs to generate a scheme has been addressed in few papers, e.g., [20]. Recently, a new strategy for reducing randomness by encoding group of pixel has been outlined in [19]. There is room for findings and further investigations.

5 Alternative Models: Miscellaneous

Apart the three models briefly described before, many variants have been introduced and studied throughout the years. A detailed overview is out of the scope of this short abstract, but a few words about some of them are worthy, especially

to give an idea of the breadth of the area: the interested reader can then use the references for deepening the aspects he is more curious about.

Visual Cryptography for Color Images. The three models concern with black-and-white images. Grey images and color images have also been considered. Grey images are treated by naturally extending the black-and-white image model: grey levels are represented with different quantities of black subpixels in the reconstructed pixels, obtained through superposition. Color images are not easy to deal with: indeed, some tricky questions arise from the complex behavior of color superposition. In the literature several models have been proposed but no agreement on a reference one has been achieved. In some of them, pixels of different colors cannot be superposed. Others exploit color superposition and the laws of color composition. The notion of contrast is not easy to define as well. However, in all of them, constructions have been proposed and the respective performances have been compared, e.g., [1,12,14,22,29,34,53].

Visual Cryptography with Meaningful Shares. Shares of a visual cryptography scheme are normally random looking images. Special sharing schemes have the capability of producing shares which are not random looking images but instead contain meaningful images; such schemes have been called *extended*[7]. In an extended visual cryptography scheme in each transparency is visible a different image; obviously, the images visible in the transparencies are unrelated to the secret image, and the security property still holds. The images on the transparencies provide a way to identify each transparency as belonging to a specific part. Extended visual cryptography schemes have been introduced in [3,44] and studied in other papers, e.g., [9,25,38].

Visual Cryptography for Multisecret. In a standard VCS parties share one secret image. It is possible to construct schemes for sharing more than one image, in such a way that each specific subset of qualified parties recovers a different image. In [42] a construction for the case when qualified subsets are pairs corresponding to adjacent nodes in a graph is provided; the scheme is also an "extended" scheme, in the sense explained in the previous paragraph. Several schemes for the special case of two parties have been proposed; in such schemes, the parties can recover more than one image by rotating the shares, so that different superpositions are produced. With square shaped shares only 4 possible rotations are possible; with circular shaped shares any rotation degree can be used (e.g., [26,45,55,56]). In some schemes the shares are translated instead of rotated; translation reduces the overall size of the reconstructed image, e.g., [26]. A suitable model and secure constructions for threshold and general access structures are interesting open problems.

Visual Cryptography with Alternative Approaches. The basic property of visual cryptography is that the reconstruction operation is performed by the human

[7] We remark that the adjective "extended" has been used also to denote other types of visual cryptography schemes with different additional properties; for example, in [33], "extended" schemes allow to share different secrets, one for each qualified subset.

eye. As remarked before, if we think of white as 0 and black as 1, the superposition operation corresponds to the logical `or` operation. Several researchers have considered visual cryptography schemes where the reconstruction operation is the `xor` operation. The use of the `xor` is justified by the fact that, for a special type of transparencies that exploit the light polarization, the superposition of the transparencies let the human eye perceives an `xor` as a result of the superposition. The idea and some schemes were proposed in [7]; several papers, e.g. [41,47], have provided schemes in this model. In [39] an interferometric encryption technique is used.

Visual Cryptography with Reversing. Some papers have considered the possibility of exploiting an extra operation in the reconstruction phase. This operation is called *reversing* and, as the name suggests, changes black pixels into white ones and vice versa. Some copy machines are able to reverse an image. The idea was introduced in [49] and other papers, e.g., [15,30,54] have considered this model.

Visual Cryptography Robust Against Cheating. In standard schemes, it is assumed that all parties are honest. Taking into consideration the possibility that some parties might be malicious, then precautions to avoid problems are needed. A cheater or a group of cooperating cheaters, by using fake shares could, for example, fool other parties by having them reconstruct a wrong secret. Several papers have considered this problem and proposed schemes that allow to detect cheaters, e.g., [21,28,31].

6 Applications

Visual cryptography has been proposed for several applications. Let us briefly look at some of them.

Educational Tool. Visual cryptography is quite a powerful tool for introducing to a general audience the basic ideas of *encryption* and *secure sharing* in an unconditional secure way. Throughout the years many presentations of the techniques and introductory articles have been written, e.g., starting from [46].

Identification and Authentication. Naor and Pinkas in [43] were the first ones to propose applications for visual identification and for visual authentication. The first, allow a human user to prove his identity to a verifier without using any computational device. The second, ensures that an adversary cannot convince a human recipient to accept any fake message. Concerning the latter, a real-life setting is the following: the user, when opening a new bank account, receives a set of transparencies, each with a unique identifier. Later on, when he makes an on-line transaction and asks the bank to credit a certain amount of money, for example, to an Internet seller, the bank to be sure of the source of the message sends to the user a transparency, which appears on the screen. The user, by superposing to it one of the transparencies previously received, precisely, the one with the same identifier which is shown on the transparency on the screen, is able to visually reconstruct as secret image an authorization code, which has

to be typed on the keyboard and sent to the bank, in order to convince the bank that the money transfer request is an original one and comes from him (and it does not come from a malicious party). Compared to a similar and currently used method (give the user directly the series of codes needed to authenticate a transaction) this method has the advantage that codes are reconstructed only when the user needs to use them and thus cannot be stolen.

Access Control. Any public or private institution might give out visual shares of the password of a vault to two people who are supposed to be both present when the vault needs to be opened. A threshold scheme might also be used for generalizing the approach to more people, adding some flexibility. The same strategy can be applied to other similar access control problems in which human users are involved.

Electronic Voting: Chaum's Scheme. The most interesting application came from Chaum [8]. He designed a sophisticated voting scheme in which a voter gets a receipt satisfying two seemingly conflicting properties: the anonymous receipt allows her or anyone else on her behalf to check that the vote was counted in the final tally but, at the same time, it does not allow to use the receipt to prove what her vote was for. The receipt is one of two transparencies generated in the voting booth, when the vote choice is made (details in [8]).

Other applications have also been suggested to fight phishing, by merging together captchas and visual cryptography, and for watermarking and more generally for copyright protection of multimedia data. We refer the interested reader to Chapter 12 of [16], which overviews with more details some applications of visual cryptography.

7 New Directions

As pointed out in [17], the design of secure protocols which can be used *without the aid of a computer* and *without cryptographic knowledge* is an interesting and challenging research task. Indeed, protocols enjoying these features could be useful in a variety of settings where computers cannot be used or where people feel uncomfortable to interact with or trust a computer. Visual cryptography might play an important role in that respect.

Indeed, a novel method for performing secure two-party computations that merges together in a suitable way Yao's garbled circuit construction and visual cryptography has been proposed in [17]. It enables Alice and Bob to securely evaluate a function $f(\cdot, \cdot)$ of their inputs, x and y, through a *pure physical* process. Once Alice has prepared a set of properly constructed transparencies, Bob computes the function value $f(x, y)$ by applying a sequence of simple steps which require the use of a pair of scissors, superposing transparencies, and the human visual system. Let us briefly describe it.

7.1 Tool for Secure Computation

Yao's Construction. Yao's construction enables two parties, Alice and Bob, to privately evaluate a boolean function $f(\cdot, \cdot)$ on their inputs, x and y, in such a

way that each party gets the result and, at the same time, *preserves* the privacy of its own input, apart from what can be inferred about it by the other party from its input and the function value $f(x, y)$, e.g., if the function $f(\cdot, \cdot)$ is the `xor` function, given x `xor` y and x there is no way to preserve the other input y.

The construction works as follows: the boolean function $f(\cdot, \cdot)$ is represented through a boolean circuit $C(\cdot, \cdot)$ for which, for each x, y, it holds that $C(x, y) = f(x, y)$. Yao's idea is to use the circuit as a *conceptual guide* for the computation which, instead of a sequence of `and`, `or` and `not` operations on strings of bits x and y, becomes a *sequence of decryptions* on sequences of ciphertexts. More precisely, one of the party, say Alice, given $C(\cdot, \cdot)$, computes a new object $\tilde{C}$, which is usually referred to as the *garbled circuit*, where:

- to each wire w of $C(\cdot, \cdot)$, are associated in $\tilde{C}$ two random keys, k_w^0 and k_w^1, which (secretly, the correspondence is not public) represent 0 and 1, and,
- to each gate $G(\cdot, \cdot)$ of $C(\cdot, \cdot)$, corresponds in $\tilde{C}$ a *gate table* $\tilde{G}$ with four rows, each of which is a *double encryption*, obtained by using two different keys $k_{w_1}^a$ and $k_{w_2}^b$, for $a, b \in \{0, 1\}$, of a message which is itself a random key $k_{w_3}^c$, for $c \in \{0, 1\}$. In details, each double encryption $E_{ab}{=}E_{k_{w_2}^b}(E_{k_{w_1}^a}(k_{w_3}^c))$ uses *one of the four* possible pairs of keys $(k_{w_1}^a, k_{w_2}^b)$, associated to the input wires (w_1, w_2) of gate $G(\cdot, \cdot)$, and the message which is encrypted is the random key $k_{w_3}^c$, associated to the wire w_3 of output of the gate $G(\cdot, \cdot)$ *if and only if* $G(a, b) = c$. The four double encryptions E_{00}, E_{01}, E_{10} and E_{11} are stored in the gate table rows in *random* order.

Once $\tilde{C}$ has been computed, Alice sends to Bob all the gate tables $\tilde{G}$ associated to the circuit gates $G(\cdot, \cdot)$, and *reveals* the random keys k_w^0 and k_w^1, associated to all the *output* wires w, and their correspondences with the values 0 and 1. Moreover, for the input wires of the circuit, she sends to Bob the random keys $k_{w_1}^{x_1}, k_{w_2}^{x_2}, \ldots, k_{w_n}^{x_n}$ corresponding to the bit-values of her own input $x = x_1 x_2 \ldots x_n$. To perform the computation represented by $\tilde{C}$, then Bob needs only the keys associated to the input wires corresponding to *his own* input. This issue can be solved by means of *executions* of 1-out-of-2 *oblivious transfer* protocols, through which Bob receives the random keys $k_{w_{n+1}}^{y_1}, k_{w_{n+2}}^{y_2}, \ldots, k_{w_{2n}}^{y_{2n}}$ corresponding to the bit-values of his own input $y = y_1 y_2 \ldots y_n$ and nothing else, while Alice from the transfer does not know which specific keys Bob has recovered.

Finally Bob, according to the topology of the original circuit $C(\cdot, \cdot)$, level after level, decrypts[8] *one and only one* entry from each gate table $\tilde{G}$ in $\tilde{C}$, until he computes *one and only one* random key associated to each output wire. The binary string which corresponds to the sequence of computed random keys, associated to the output wires, is the value $C(x, y)$. Bob sends the result of the computation to Alice.

Koleshnikov Approach. Kolesnikov [35] showed that a different approach to the function evaluation process in Yao's construction can be pursued. Roughly

[8] An encryption scheme allowing to verify whether a decryption is successful, providing a correctly decrypted value, or fails, providing garbage, is used.

speaking, instead of constructing the garbled circuit $\tilde{C}$ by using for each gate $G(\cdot,\cdot)$ a gate table $\tilde{G}$, containing a double encryption for each possible input pair of keys, it is possible to use *secret sharing schemes* designed to realize the functionalities implemented by the logical gates. Such schemes were referred to as *gate evaluation secret sharing schemes* (GESS, for short) [35]. Using a GESS, any time that two shares, say $sh^a_{w_1}$ and $sh^b_{w_2}$, associated to the input wires w_1 and w_2 of gate $G(\cdot,\cdot)$, are combined through the reconstruction function of the GESS, the secret s_{w_3}, associated to the output wire w_3 of gate $G(\cdot,\cdot)$ is recovered. It follows that an *explicit representation* $\tilde{G}$ of $G(\cdot,\cdot)$ is *not* needed any more, because all the information required to reconstruct the secret value associated to w_3, depending on the functionality of the target gate $G(\cdot,\cdot)$, is coded and, hence, *implicitly represented*, into the shares $sh^a_{w_1}$ and $sh^b_{w_2}$. Therefore, given the circuit $C(\cdot,\cdot)$, and by applying a bottom-up process, which starts from the circuit output wires and ends when the circuit input wires are reached, Alice can construct shares associated to the circuit input wires which encode *all the information* needed to evaluate $C(\cdot,\cdot)$ on every pair of inputs (x, y). Then, as in Yao's construction, Alice sends directly to Bob the shares corresponding to the bit-values of her own input x, while Bob, by means of *executions* of 1-out-of-2 *oblivious transfer* protocols, receives the shares corresponding to the bit-values of his own input y. Finally, Bob applies iteratively the GESS reconstruction functions, until the secrets associated to the output wires, which correspond to the value $C(x, y)$, are obtained.

A Visual Construction. In [17] it was shown how to build on Kolesnikov's idea in order to produce a circuit implementation by using visual cryptography, i.e., in such a way that the evaluation process ends up in a sequence of transparency superpositions. The first crucial step is to set up a *physical oblivious transfer*.

Let Alice's secrets be n-bit strings z_0 and z_1, let σ be Bob's bit-choice, and let $\perp$ denote no output. The 1-out-of-2-OT functionality is specified by $((z_0, z_1, \sigma) \rightarrow (\perp, z_\sigma))$. The construction proposed is partially inspired to the approach pursued in [8], when the voter comes out from the booth. Let us assume that the two secrets z_0 and z_1 are represented in form of transparencies, and Alice has two *indistinguishable envelopes* which *perfectly hide* the transparency inside. Alice and Bob proceed as follows:

1. Alice puts the two transparencies in the two envelopes, one in the first and one in the second, and closes both of them. She also adds to each envelope a paper post-it with number 0 and number 1, depending on the transparency which is inside. Then, she hands the two envelopes to Bob.
2. Bob turns his shoulders to Alice, checks that the envelopes are identical, takes the envelopes with the post-it corresponding to the secret he is interested in, removes the post-it from both envelopes, turns again in front of Alice, and inserts under Alice surveillance the remaining envelope in a paper-shredder which reduces the envelop and its content in dust.

In such a way, Bob gets one and only one transparency, while Alice does not know which one.

The second step is to produce a *visual equivalent* of a $GESS$ scheme. In [17] it is showed how to do it, introducing the notion of $VGESS$, i.e., *visual gate evaluation secret sharing*.

With these tools, the visual protocol ends up in the same reduction of secure function evaluation to 1-out-of-2 OT given via Construction 1 in [35], but with $VGESSs$ and physical OTs instead of $GESSs$ and a digital OTs. It consists in a *Shares construction phase*, performed by Alice, and a *Computation phase*, performed by Alice and Bob.

To get an idea of how the protocol works, let us look at an example. The function f is equal to $f(x, y) = (x_1 \wedge y_1) \vee (x_2 \wedge y_2)$. The output values are represented through a totally white image (0) and a totally black image (1). Notice that, in the *Computation phase*, and specifically in the visual computation performed by Bob, any image with *at least* a white pixel corresponds to 0, while the *totally black* image corresponds to 1. In Fig. 6, Alice has completed the *Shares construction phase* and all the shares that are needed for the computation have been computed and have been associated to the input wires. For example, for the left input wire of G_1, the value 0 corresponds to share Sh_1^C, while the value 1 corresponds to the share Sh_1^D. The prepended bits, implemented by using a visual cryptography scheme too, says to which half of the right share the left share has to be superposed. For details, the reader is referred to [17].

Figure 7 shows an example of the *Computation phase*, with input values $x_1 = 0, x_2 = 1, y_1 = 1$ and $y_2 = 0$. Once Bob has received from Alice the shares associated to her input and, through two instances of the OT protocol, the shares associated to his input, then he can perform the computation. The reconstructed value as shown in the figure is correctly zero.

Notice that an investigation of a different approach to secure multiparty computation by using visual cryptography has been recently proposed in [19]. Indeed, in the general solutions for unconditionally secure multiparty computation, in order to compute new shares for the subsequent steps, parties process their input shares interactively or non-interactively. Along the same line, [19] looks at how transparencies can be efficiently manipulated in such a way that when the newly produced transparencies are superposed, the result of the function evaluation is obtained, while the input privacy is still preserved.

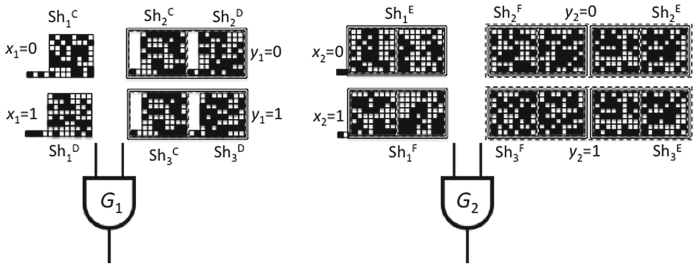

Fig. 6. Shares for evaluating function f

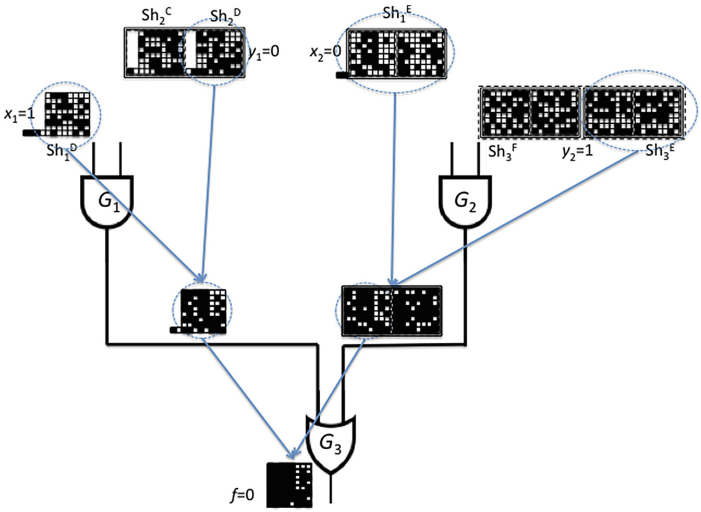

Fig. 7. Visual evaluation of f with input $((0,1),(1,0))$

8 Conclusions

We have proposed a brief excursus in the large field of visual cryptography. Starting from Naor and Shamir's and Kafri and Keren's models, we have described a common framework for visual cryptography schemes, and we have given a look at alternative models: for grey and color images, for meaningful transparencies, for multiple secrets, as well as models that exploit special properties for the superposition of transparencies and models robust against cheating. We have also described some classical applications and, finally, we have focused on a new approach, which uses visual cryptography for general secure computation. Along the way, we have pointed out issues and open problems, which could be objects of attention and further investigations in the next years. Years in which visual cryptography seems to be still a potentially useful technique.

References

1. Adhikari, A., Sikdar, S.: A new (2,n)-visual threshold scheme for color images. In: Johansson, T., Maitra, S. (eds.) INDOCRYPT 2003. LNCS, vol. 2904, pp. 148–161. Springer, Heidelberg (2003)
2. Ateniese, G., Blundo, C., De Santis, A., Stinson, D.R.: Visual cryptography for general access structures. Inf. Comput. **129**(2), 86–106 (1996)
3. Ateniese, G., Blundo, C., De Santis, A., Stinson, D.R.: Extended schemes for visual cryptography. Theoret. Comput. Sci. **250**(1–2), 143–161 (2001)
4. Blundo, C., Cimato, S., De Santis, A.: Visual cryptography schemes with optimal pixel expansion. Theoret. Comput. Sci. **369**(1–3), 169–182 (2006)
5. Blundo, C., D'Arco, P., De Santis, A., Stinson, D.R.: Contrast optimal threshold visual cryptography schemes. SIAM J. Discrete Math. **16**(2), 224–261 (2003)

6. Blundo, C., De Santis, A., Stinson, D.R.: On the contrast in visual cryptography schemes. J. Cryptol. **12**(4), 261–289 (1999)
7. Biham, E., Itzkovitz, A.: Visual cryptography with polarization. In: The Dagstuhl Seminar on Cryptography (1997) and Crypto 1998 RUMP Session (1998)
8. Chaum, D.: Secret-ballot receipts: true voter-verifiable elections. IEEE Secur. Priv. 38–47 (2004)
9. Chen, T.-H., Lee, Y.-S.: Yet another friendly progressive visual secret sharing scheme. In: 5th International Conference Intelligent Information Hiding and Multimedia Signal Processing, pp. 353–356 (2009)
10. Chen, T.-H., Tsao, K.-H.: Visual secret random grids sharing revisited. Pattern Recogn. **42**(9), 2203–2217 (2009)
11. Chen, T.-H., Tsao, K.-H.: Threshold visual secret sharing by random grids. J. Syst. Softw. **84**(7), 1197–1208 (2011)
12. Cimato, S., De Prisco, R., De Santis, A.: Optimal colored threshold visual cryptography schemes. Des. Codes Crypt. **35**, 311–335 (2005)
13. Cimato, S., De Prisco, R., De Santis, A.: Probabilistic visual cryptography schemes. Comput. J. **49**(1), 97–107 (2006)
14. Cimato, S., De Prisco, R., De Santis, A.: Colored visual cryptography without color darkening. Theoret. Comput. Sci. **374**(1–3), 261–276 (2007)
15. Cimato, S., De Santis, A., Ferrara, A.L., Masucci, B.: Ideal contrast visual cryptography schemes with reversing. Inf. Process. Lett. **93**(4), 199–206 (2005)
16. Cimato, S., Yang, C.-N.: Visual Cryptography and Secret Image Sharing. CRC Press, Boca Raton (2012). ISBN: 978-1-4398-3721-4
17. D'Arco, P., Prisco, R.: Secure two-party computation: a visual way. In: Padró, C. (ed.) ICITS 2013. LNCS, vol. 8317, pp. 18–38. Springer, Heidelberg (2014). doi:10.1007/978-3-319-04268-8_2
18. D'Arco, P., De Prisco, R., De Santis, A.: Measure-independent characterization of contrast optimal visual cryptography schemes. J. Syst. Softw. **95**, 89–99 (2014)
19. D'Arco, P., De Prisco, R., Desmedt, Y.: Private visual share-homomorphic computation and randomness reduction in visual cryptography. In: ICITS 2016, 9–12 August 2016, Tacoma, Washington, USA (2016)
20. De Bonis, A., De Santis, A.: Randomness in secret sharing and visual cryptography schemes. Theoret. Comput. Sci. **314**(3), 351–374 (2004)
21. De Prisco, R., De Santis, A.: Cheating immune threshold visual secret sharing. Comput. J. **53**(9), 1485–1496 (2009)
22. De Prisco, R., De Santis, A.: Color visual cryptography schemes for black and white secret images. Theoret. Comput. Sci. **510**(28), 62–86 (2013)
23. De Prisco, R., De Santis, A.: On the relation of random grid and deterministic visual cryptography. IEEE Trans. Inf. Forensics Secur. **9**(4), 653–665 (2014)
24. Eisen, P.A., Stinson, D.R.: Threshold visual cryptography schemes with specified whiteness levels of reconstructed pixels. Des. Cods Crypt. **25**, 15–61 (2002)
25. Fang, W.P.: Friendly progressive visual secret sharing. Pattern Recogn. **41**(4), 1410–1414 (2008)
26. Feng, J.-B., Wu, H.-C., Tsai, C.-S., Chang, Y.-F., Chu, Y.-P.: Visual secret sharing for multiple secrets. Pattern Recogn. **41**(12), 3572–3581 (2008)
27. Hofmeister, T., Krause, M., Simon, H.U.: Contrast-optimal k out of n secret sharing schemes in visual cryptography. Theoret. Comput. Sci. **240**(2), 471–485 (2000)
28. Horng, G., Chen, T.-H., Tsai, D.-S.: Cheating in visual cryptography. Des. Codes Crypt. **38**(2), 219–236 (2006)
29. Hou, Y.-C.: Visual cryptography for color images. Pattern Recognit. **36**(7), 1619–1629 (2003)

30. Hu, C.-M., Tzeng, W.-G.: Compatible ideal contrast visual cryptography schemes with reversing. In: Zhou, J., Lopez, J., Deng, R.H., Bao, F. (eds.) ISC 2005. LNCS, vol. 3650, pp. 300–313. Springer, Heidelberg (2005). doi:10.1007/11556992_22
31. Hu, C., Tzeng, W.G.: Cheating prevention in visual cryptography. IEEE Trans. Image Process. **16**(1), 36–45 (2007)
32. Kafri, O., Keren, E.: Encryption of pictures and shapes by random grids. Opt. Lett. **12**(6), 377–379 (1987)
33. Klein, A., Wessler, M.: Extended visual cryptography schemes. Inf. Comput. **205**(5), 716–732 (2007)
34. Koga, H., Yamamoto, H.: Proposal of a lattice-based visual secret sharing scheme for color and gray-scale images. IEICE Trans. Fundam. Electron. Commun. Comput. Sci. **81**–**A**(6), 1262–1269 (1998)
35. Kolesnikov, V.: Gate evaluation secret sharing and secure one-round two-party computation. In: Roy, B. (ed.) ASIACRYPT 2005. LNCS, vol. 3788, pp. 136–155. Springer, Heidelberg (2005). doi:10.1007/11593447_8
36. Krause, M., Simon, H.U.: Determining the optimal contrast for secret sharing schemes in visual cryptography. Comb. Probab. Comput. **12**(3), 285–299 (2003)
37. Kuhlmann, C., Simon, H.U.: Construction of visual secret sharing schemes with almost optimal contrast. In: 11th ACM-SIAM Symposium on Discrete Algorithms, San Francisco, USA, pp. 262–272 (2000)
38. Lee, K.-H., Chiu, P.-L.: An extended visual cryptography algorithm for general access structures. IEEE Trans. Inf. Forensics Secur. **7**(1), 219–229 (2012)
39. Lee, S.-S., Na, J.-C., Sohn, S.-W., Park, C., Seo, D.-H., Kim, S.-J.: Visual cryptography based on interferometric encryption technique. ETRI J. **24**(5), 373–380 (2002)
40. Liu, F., Wua, C., Lin, X.: A new definition of the contrast of visual cryptography scheme. Inf. Process. Lett. **110**(7), 241–246 (2010)
41. Liu, F., Wu, C.K.: Optimal XOR based (2,n)-visual cryptography schemes. In: Shi, Y.-Q., Kim, H.J., Pérez-González, F., Yang, C.-N. (eds.) IWDW 2014. LNCS, vol. 9023, pp. 333–349. Springer, Heidelberg (2015)
42. Lu, S., Manchala, D., Ostrovsky, R.: Visual cryptography on graphs. J. Comb. Optim. **21**(1), 47–66 (2011)
43. Naor, M., Pinkas, B.: Visual authentication and identification. In: Kaliski, B.S. (ed.) CRYPTO 1997. LNCS, vol. 1294, pp. 322–336. Springer, Heidelberg (1997). doi:10.1007/BFb0052245
44. Naor, M., Shamir, A.: Visual cryptography. In: Santis, A. (ed.) EUROCRYPT 1994. LNCS, vol. 950, pp. 1–12. Springer, Heidelberg (1995). doi:10.1007/BFb0053419
45. Shyu, S.-J., Huang, S.-Y., Lee, Y.-K., Wang, R.-Z., Chen, K.: Sharing multiple secrets in visual cryptography. Pattern Recogn. **40**(12), 3633–3651 (2007)
46. Stinson, D.: Visual cryptography and threshold schemes. Dr. Dobbs J. (1998). http://www.drdobbs.com/visual-cryptography-threshold-schemes/184410530
47. Tulys, P., Hollman, H.D., van Lint, J.H., Tolhuizen, L.: XOR-based visual cryptography schemes. Des. Codes Crypt. **27**, 169–186 (2005)
48. Verheul, E.R., van Tilborg, H.C.A.: Constructions and properties of k out of n visual secret schemes. Des. Codes Crypt. **11**, 179–196 (1997)
49. Viet, D.Q., Kurosawa, K.: Almost ideal contrast visual cryptography with reversing. In: Okamoto, T. (ed.) CT-RSA 2004. LNCS, vol. 2964, pp. 353–365. Springer, Heidelberg (2004). doi:10.1007/978-3-540-24660-2_27
50. Yang, C.-N.: New visual secret sharing schemes using probabilistic method. Pattern Recogn. Lett. **25**(4), 481–494 (2004)

51. Yang, C.-N., Chen, T.-S.: Size-adjustable visual secret sharing schemes. IEICE Trans. Fundam. Electron. Commun. Comput. Sci. **E88–A**(9), 2471–2474 (2005)
52. Yang, C.-N., Chen, T.-S.: Aspect ratio invariant visual secret sharing schemes with minimum pixel expansion. Pattern Recogn. Lett. **26**(2), 193–206 (2005)
53. Yang, C.-N., Laih, C.-S.: New colored visual secret sharing schemes. Des. Codes Crypt. **20**, 325–335 (2000)
54. Yang, C.-N., Wang, C.-C., Chen, T.-S.: Visual cryptography schemes with reversing. Comput. J. **51**(6), 710–722 (2008)
55. Wu, H.C., Chang, C.C.: Sharing visual multi-secrets using circle shares. Comput. Stand. Interfaces **134**(28), 123–135 (2005)
56. Wu, C.-C., Chen, L.-H.: A study on visual cryptography. Master thesis, Institute of Computer and Information Science, National Chiao Tung University, Taiwan, R.O.C. (1998)
57. Wu, X., Sun, W.: Random grid-based visual secret sharing for general access structures with cheat-preventing ability. J. Syst. Softw. **85**(5), 1119–1134 (2012)

http://www.springer.com/978-3-319-47237-9

Innovative Security Solutions for Information Technology and Communications
9th International Conference, SECITC 2016, Bucharest, Romania, June 9-10, 2016, Revised Selected Papers
Bica, I.; Reyhanitabar, R. (Eds.)
2016, X, 287 p. 86 illus., Softcover
ISBN: 978-3-319-47237-9