On the Relation of Random Grid and Deterministic Visual Cryptography

Roberto De Prisco and Alfredo De Santis

***Abstract*— Visual cryptography is a special type of secret sharing. Two models of visual cryptography have been independently studied: 1) deterministic visual cryptography, introduced by Naor and Shamir, and 2) random grid visual cryptography, introduced by Kafri and Keren. In this paper, we show that there is a strict relation between these two models. In particular, we show that to any random grid scheme corresponds a deterministic scheme and vice versa. This allows us to use results known in a model also in the other model. By exploiting the (many) results known in the deterministic model, we are able to improve several schemes and to provide many upper bounds for the random grid model and by exploiting some results known for the random grid model, we are also able to provide new schemes for the deterministic model. A side effect of this paper is that future new results for any one of the two models should not ignore, and in fact be compared with, the results known in the other model.**

***Index Terms*— Cryptography, visual secret sharing, random grids, probabilistic visual cryptography.**

I. Introduction

VISUAL cryptography is a special type of secret sharing in which the secret is an image and the shares are random-looking images printed on transparencies. The captivating peculiarity of this type of secret sharing is that the reconstruction of the secret is performed without any computational machinery: it is enough to superpose the shares (transparencies) in order to reconstruct the secret. Visual cryptography has been introduced by Naor and Shamir [34] in 1994. Kafri and Keren [27] have introduced a similar technique, called *random grid encryption*, in 1987.

Roughly speaking, the model introduced by Naor and Shamir works as follows. A secret image, known by a trusted party called the *dealer*, has to be shared among a set of participants in such a way that some subsets of participants, called *qualified sets* are able to visually recover the images while others, called *forbidden sets*, do not have any information about the secret image. In order to share the image, the dealer creates a share for each participant. In a share each single pixel of the secret image is represented with a set of m, $m \geq 2$, pixels. Parameter m is the pixel expansion: the recovered secret image will be m times bigger than the original secret image. Limiting our discussion to black and white images, the shares are such that when we superpose shares of a qualified set of participants, among the m pixels that represent a secret pixels s, we will find at most ℓ black pixels if s is white and at least h black pixels if s is black, with $0 \leq \ell < h \leq m$. That is, in the recovered secret image, white secret pixels are reconstructed with at most ℓ black pixels out of m pixels, while black secret pixels are reconstructed with at least h black pixels. This difference makes up the *contrast*, which is a measure of the quality of the reconstructed image.

In the model used by Kafri and Keren, that exploits random grids, instead, there is no pixel expansion, that is to say, if we want still to use the parameter m, that we have $m = 1$. Clearly, with no pixel expansion, a secret pixel corresponds to one pixel in the reconstructed image. Using the thresholds ℓ and h, we have that for random grids we must use $\ell = 0$ and $h = 1$. It is not surprising that we cannot achieve such a reconstruction in a deterministic way. Indeed reconstruction in visual sharing based on random grids is guaranteed only with some probability: the *average light transmission* (white pixels) in the area of the reconstructed image that corresponds to the white area of the secret image is bigger than the average light transmission in the area of the reconstructed image that corresponds to the black area of the secret image. Such a difference makes up the contrast.

We will talk about *deterministic* visual cryptography to refer to the model introduced by Naor and Shamir and about *random grid* visual cryptography to refer to the model introduced by Kafri and Keren.

Deterministic visual cryptography has been widely studied. Many papers have explored various aspects: minimal pixel expansion (e.g., [4], [5], [21]), optimal contrast (e.g., [6], [8], [23], [28]), general access structures (e.g., [2], [33]), perfect reconstruction of black pixels (e.g., [5], [7], [38]) color images (e.g. [1], [13], [14], [19], [20], [24], [39], [48]), and other issues (e.g. [3], [9], [17], [25], [29], [31], [32], [37], [41], [42], [46], [47]). The book [16] contains a number of surveys about topics in visual cryptography.

In the context of the deterministic model, Yang [45] has introduced the *probabilistic* model. This model is very similar to the random grid model. The probabilistic model is strictly related to the deterministic model and such a relation has been studied by Cimato *et al.* [15]. In [15] the probabilistic model has been generalized to consider also pixel expansion and it is shown that the probabilistic factor β of a scheme, which is a measure of the quality of the reconstructed image and thus is the counterpart of the contrast, can be traded with the pixel expansion. That is, it is possible to use the probabilistic model using any pixel expansion m. For $m = 1$ we have the model of Yang, for m big enough we have the deterministic model of Naor and Shamir. The results of this paper imply that the probabilistic model of Yang is the same as the random

Manuscript received October 2, 2013; revised December 9, 2013; accepted February 3, 2014. Date of publication February 10, 2014; date of current version March 13, 2014. This work was supported by the Italian MIUR PRIN Projects. The associate editor coordinating the review of this manuscript and approving it for publication was Dr. Shantanu D. Rane.

The authors are with the Dipartimento di Informatica, Università di Salerno, Fisciano 84084, Italy (e-mail: robdep@di.unisa.it; ads@di.unisa.it).

Digital Object Identifier 10.1109/TIFS.2014.2305574

grid model of Kafri and Keren (see the "Summary of results" paragraph below and Section II-C).

Although the random grid model has been introduced before (1987) the deterministic model (1994) only in recent years many researchers have focused their attention on it. The paper by Kafri and Keren [27] provided only $(2, 2)$-threshold schemes for black and white secret images and suggested a generalization to gray-level images. In recent years, Shyu provided a generalization to color images [35] and a generalization to (n, n)-threshold schemes [36]; Chen and Tsao [11] provided $(2, n)$-threshold schemes and again (n, n)-threshold schemes [11] and also (k, n)-threshold schemes [12]; Chen and Lin [10] provided improved $(2, n)$-threshold schemes; Wu and Sun [43], [44] study random grid schemes with the `xor` operation for the decryption; in [40] "incremental" schemes are provided.

In this paper we show that there is a close relation between the random grid model and the deterministic model. More specifically we show that to any random grid scheme corresponds a deterministic scheme and viceversa. This allows us to use results known in a model also in the other model. Exploiting the (many) results known in the deterministic model we are able to improve several schemes and to provide many upper bounds for the random grid model. Exploiting some results known for the random grid model, we are also able to provide new schemes for the deterministic model. A side effect of this paper is that future new results for any one of the two models (random grid and deterministic) should not ignore, and in fact be compared to, the results known in the other model.

Related work. A recent paper by Fu and Yu [22] presents results related to the ones that we give in this paper. In particular, [22] proves that random grid schemes can be transformed into probabilistic schemes with no pixel expansion. Moreover it is observed that $\gamma_{\text{RG}} \leq \gamma_{\text{PR}}$, where γ_{RG} is the contrast used in the random grid model and γ_{PR} is the contrast used in the probabilistic model. The results presented in this paper are much more general that those presented in [22]. More specifically:

- We prove an *equivalence* between the *random grid* model and the *deterministic* model: any random grid scheme can be transformed into a deterministic scheme and *viceversa*. We also note that the above implies also that the random grid model is in fact *the same model* as the probabilistic model with no pixel expansion. This result alone implies the results of [22].
- We provide general theorems that allow us to *both* use schemes known in a model in the other model *and* to use *upper bounds* on the contrast known in a model in the other model.
- Beside proving relations about the contrast used in the different models, similar to the $\gamma_{\text{RG}} \leq \gamma_{\text{PR}}$ relation proved in [22], we prove the interesting result that $\gamma_{\text{RG}} = \gamma_{\text{ES}}$, that is, the contrast measure used in the random grid model is *equal* to one of the contrast measures proposed for the deterministic model (specifically the one by Eisen and Stinson [21]).

TABLE I
SUMMARY OF IMPLICATIONS

NEW BOUNDS FOR THE RANDOM GRID MODEL

	$(2, n)$	(k, n)	(n, n)
Bounds	$\gamma_{\text{RG}} \leq \frac{\lceil n/2 \rceil \lfloor n/2 \rfloor}{n(n-1)}$	$\gamma_{\text{RG}} \leq f(k, n)$	$\gamma_{\text{RG}} \leq \frac{1}{2^{n-1}}$

Function f is defined in Theorem 5.9.

NEW SCHEMES FOR THE RANDOM GRID MODEL

	$(3, n)$	$(n-1, n)$
Schemes	$\gamma_{\text{RG}} = f'(n) \geq \frac{1}{(n-1)^2}$	$\gamma_{\text{RG}} = \frac{1}{(n-2)2^{n-2}+1}$

Function f' is defined in Theorem 5.4.

NEW SCHEMES FOR THE DETERMINISTIC MODEL

	$(2, n)$	General Access Structures
Schemes	see Construction 5.2	see Section VI

- Finally, we do exploit the connection between the models both poviding new schemes for the deterministic model (starting from schemes for the random grid model) and providing new schemes and upper bounds on the contrast for the random grid model (starting from known results in the deterministic model).

Summary of results. The main result of this paper is the identification of a strong relation between random grid visual cryptography and deterministic visual cryptography. Such a strong relation could also be seen as an equivalence between the random grid model and the probabilistic model for which the strong relation with the deterministic model has been already studied. The main result has many implications in the sense that it allows to use results known for the deterministic model in the random grid model and viceversa. Table I summarizes the implications that we have analyzed in this paper.

Road map of the paper. In Section II we describe the formal model, providing the necessary definitions. Then we recall some relevant known results in Section III both for the random grid model and for the deterministic model. In Section IV we provide the theorems that show the connection between the random grid model and the deterministic model. Sections V and VI provide some consequences of the relationship established by the main results. Finally, in Section VII we provide concluding remarks and directions for future work.

II. THE MODEL

The secret image consists of black and white[1] pixels. We will use the symbols $\bullet$ and $\circ$ to denote, respectively, black and white pixels. In order to share the secret image among a set of participants $\mathcal{P} = \{1, 2, \ldots, n\}$, the owner of the secret, called the *dealer*, provides each of the n participants with a *share*, which is an image printed on a transparency.

An important parameter of a scheme is the pixel expansion m: each share is m times the size of the secret image, that is, each pixel of the secret image is expanded into m pixels. The deterministic model requires $m \geq 2$. For the random

[1]Notice that, for the shares, white should really be interpreted as transparent. So we use white as a synonymous for transparent.

grid model there is no pixel expansion, that is, $m = 1$. For the probabilistic model we have that $m \geq 1$, allowing both schemes with no pixel expansion ($m = 1$) and schemes with pixel expansion ($m \geq 2$).

An access structure $(\mathcal{Q}, \mathcal{F})$ is a specification of the *qualified* subsets of participants and of the *forbidden* subsets of participants. Qualified sets of participants have to be able to visually recover the secret image by superposing their shares. Forbidden sets of participants must not have any information about the secret image from the shares. In many cases, the forbidden sets of participants are those with strictly less than k participants, while the qualified sets are those with at least k participants. In such cases the access structure is a (k, n)-threshold access structure. The case of (k, n)-threshold schemes is the most widely studied one.

To reconstruct the secret image, participants superpose their shares, carefully aligning them. We will denote with $\mathtt{sup}(P)$ the superposition of the shares of the participants in $P \subseteq \mathcal{P}$. In the reconstructed image a pixel is white if and only if all the superposed pixels aligned to that pixel are white and black otherwise (that's an `or` operation if we represent white as 0 and black as 1). Since each pixel is expanded into $m \geq 1$ pixels, we have to infer the color of the secret pixel by the colors of the corresponding m pixels in the reconstruction.

For $m \geq 2$, the reconstruction relies on two thresholds, ℓ and h, with $0 \leq \ell < h \leq m$, such that when the secret pixel is white, we will have *at most* ℓ black pixels among the corresponding m pixels in the reconstructed image, and when the secret pixel is black, we will have *at least* h black pixels among the corresponding m pixels in the reconstructed image. For $m = 1$ the reconstruction relies on the the average light transmission, which we will define shortly, over the white and the black area of the secret image. The average light transmission is closely related to the above two thresholds. The case of schemes with no expansion is a special case for which $m = 1$. To use the thresholds ℓ and h also in this case, we must set $\ell = 0$ and $h = 1$.

In deterministic schemes the reconstruction must be always correct. In probabilistic and random grid schemes the reconstruction of some pixels can be wrong as long as, on average, there are not too many pixels erroneously reconstructed.

In all the cases (with and without pixel expansion), the quality of the reconstructed image depends on the scheme and is based on the fact that, on average, the areas of the reconstructed image that correspond to white areas in the secret image will contain less black pixels than those corresponding to the black areas of the secret image, making up the contrast.

For the deterministic and the probabilistic models the contrast is a function of both the thresholds ℓ and h and of the pixel expansion m. For the random grid model the contrast is defined by means of the average light transmissions which is the amount of light that a given region let pass through. More formally, given a region G of an image I, that is, a subset of the pixels of the image I, the average light transmission $\lambda(G)$ is

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

that is, the number of pixels in G that are white, divided by the total number of pixels in G. We remark that, in order for this measure to be meaningful, the distribution of the white pixels in G (and consequently also the distribution of the black pixels) has to be random. We will implicitly make this assumption when using the average light transmission.

Let I be a secret image and let $\mathcal{W}_I$ and $\mathcal{B}_I$ denote, respectively, the entire white area and the entire black area of I. Given another image R, with the same dimension of I, the notation $\mathcal{W}_I(R)$ (resp. $\mathcal{B}_I(R)$) denotes the area of R that corresponds to the white (resp. black) area of I, where the correspondence is given by the position of the pixels: pixel in position (i, j) of I corresponds to pixel in position (i, j) of R, for all i and j.

The random grid model evaluates schemes by assessing $\lambda(\mathcal{W}_I(R))$ and $\lambda(\mathcal{B}_I(R))$ where R is the reconstructed image. Clearly, the use of the average light transmission is not restricted to reconstructions obtained with a random grid scheme but can be used also to evaluate schemes with pixel expansion. In fact, the thresholds ℓ and h are just a different way of evaluating the average light transmission.

Rational probabilities. The construction of visual cryptography schemes involves the use of random choices. We assume that the random values used are rational numbers. This is not a big restriction since if a random choice has to be made with an irrational probability p_i, we can use a rational approximation p_r, as close as we wish to p_i.

A. The Random Grid Model

In the random grid model we have $m = 1$, and thus a share is an image having the same dimensions of the secret image I. To ease the notation we will use $\lambda_\circ(P)$ (resp. $\lambda_\bullet(P)$) to denote $\lambda(\mathcal{W}_I(\mathtt{sup}(P)))$ (resp. $\lambda(\mathcal{B}_I(\mathtt{sup}(P)))$), for a given set of participants P. Next we provide a formal definition of random grid schemes.

Definition 2.1: A random grid scheme for a secret image I, a set of participants $\mathcal{P} = \{1, 2, \ldots n\}$, and an access structure $(\mathcal{Q}, \mathcal{F})$, defines n shares, one for each participant, satisfying the following conditions.

1) (Contrast property) There exists two thresholds $\lambda_\circ$ and $\lambda_\bullet$, with $\lambda_\circ > \lambda_\bullet$, such that for any qualified set $Q \in \mathcal{Q}$ of participants, we have that $\lambda_\circ(R) \geq \lambda_\circ$ and $\lambda_\bullet \geq \lambda_\bullet(R)$, where $R = \mathtt{sup}(Q)$.
2) (Security property) For any forbidden set $F \in \mathcal{F}$ of participants, we have that $\lambda_\circ(R) = \lambda_\bullet(R)$, where $R = \mathtt{sup}(F)$.

Average light transmission parameters. $\lambda_\circ$ and $\lambda_\bullet$ are the average light transmission parameters of the scheme.

The first property is the contrast condition, which guarantees that the secret image will be visible when superposing the shares of a qualified set of participants. The second property is the security property: from a single share or from the superposition of (or any other computation on) the shares of a forbidden set of participants, we cannot infer any information about the secret image. Notice that the security property relies also on the implicit assumption that black and white pixels are uniformly distributed and thus the condition $\lambda_\circ(R) = \lambda_\bullet(R)$ is

sufficient to say that the (secret) white area is indistinguishable from the (secret) black area.

Uniform and generalized random grids. In [27] and in the formalization given in [35] it is also required that each share be a random grid where each pixel is chosen at random between white and black with uniform probability (1/2 for white and 1/2 for black). However this property is not necessary and only poses unnecessary limitations on the constructions of the schemes. What we really need, is that a single share does not provide any information on the secret and clearly this is a consequence of the fact that the share is a (uniform) random grid. However the fact that a single share does not give any information on the secret is also guaranteed by the security property[2]; hence there is no reason to require that a random grid be uniform. For example, a share might be the random distribution of white and black pixels where white appears with probability 2/3 and black with probability 1/3. To avoid confusion we will talk about *uniform random grids* when the distribution of white and black pixels is uniform and of *generalized random grids* when the distribution is not uniform. Some papers that deal with random grids, indeed, use generalized random grids, e.g. [12].

Contrast. The goodness of the reconstruction depends on the difference of the average light transmission between the white and the black areas of the secret image. Papers that have considered random grid schemes have used the following definition of contrast. Given a random grid scheme $\mathcal{S}$, with average light transmission parameters $\lambda_\circ$ and $\lambda_\bullet$, the contrast of $\mathcal{S}$ is:

$$\gamma_{\text{RG}}(\mathcal{S}) = \frac{\lambda_\circ - \lambda_\bullet}{1 + \lambda_\bullet}. \tag{1}$$

B. The Deterministic Model

To achieve a deterministic reconstruction we must *expand* the secret image: each pixel of the secret image will be represented as a collection of m pixels, $m \geq 2$. Parameter m is called the *pixel expansion* of the scheme. Deterministic schemes are described by means of two multisets of $n \times m$ *distribution* matrices, one for black secret pixels and one for white secret pixels. Each single element of the distribution matrices represents a pixel in a share. Each row in a distribution matrix represents a particular share, i.e., the m subpixels of the share. Each matrix represents a set of n shares, one per participant (row i represents the shares for participant i). Given a matrix M of n rows and a set of participants $P \subseteq \mathcal{P}$, we will denote by $M|P$ the restriction of M to the rows corresponding to participants in P. In the following we will denote with $w_\bullet(X)$ the number of black pixels in X, where X is an array of pixels.

Definition 2.2: A deterministic scheme for a secret image I, a set of participants $\mathcal{P} = \{1, 2, \ldots n\}$, and an access structure $(\mathcal{Q}, \mathcal{F})$, defines n shares, one for each participant, by means of two collections $\mathcal{C}_\circ$ and $\mathcal{C}_\bullet$ of $n \times m$ distribution matrices satisfying the following conditions.

1) (Contrast property) There exists two thresholds ℓ and h, with $\ell < h$, such that for any qualified set $Q \in \mathcal{Q}$ it holds: (i) for any $M \in \mathcal{C}_\circ$, we have that $w_\bullet(\texttt{sup}(M|Q)) \leq \ell$ and (ii) for any $M \in \mathcal{C}_\bullet$, we have that $w_\bullet(\texttt{sup}(M|Q)) \geq h$.
2) (Security property) For any forbidden set $F \in \mathcal{F}$, the two collections of $|F| \times m$ matrices, $\mathcal{D}_\circ = \{M|F$, for each $M \in \mathcal{C}_\circ\}$ and $\mathcal{D}_\bullet = \{M|F$, for each $M \in \mathcal{C}_\bullet\}$, are indistinguishable in the sense that they contain the same matrices with the same frequencies.

Contrast parameters. The thresholds ℓ and h are the *contrast parameters* of the scheme.

Cardinality parameters. In some cases, we will be interested in the cardinality of the distribution collections $\mathcal{C}_\circ$ and $\mathcal{C}_\bullet$. Hence we define the *cardinality parameters* of a scheme as $m_\circ = |\mathcal{C}_\circ|$ and $m_\bullet = |\mathcal{C}_\bullet|$.

Base matrices. 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 $B_\circ$ (resp. $B_\bullet$). For such schemes, the matrices $B_\circ$ and $B_\bullet$ are called the *base matrices* of the scheme.

Columns multiplicities. In some cases, it is possible to describe the base matrices in a very convenient way by means of column multiplicities. This is possible when a base matrix that contains a specific column, consisting of i black pixels and $n-i$ white pixels, with a multiplicity μ, contains also all the other possible columns that have exactly i black pixels and $n-i$ white pixels, each of them with the same multiplicity μ. When the above holds, the base matrices can be described simply by listing the multiplicities μ_i of the columns that have exactly i black pixels. The white base matrix will be specified by $\mu_0^\circ, \mu_1^\circ, \ldots, \mu_n^\circ$. The black base matrix will be specified by $\mu_0^\bullet, \mu_1^\bullet, \ldots, \mu_n^\bullet$.

Contrast. Various definitions of the contrast have been used for the deterministic model. In the original model by Naor and Shamir [34] the contrast of a scheme $\mathcal{S}$ with contrast parameters ℓ and h and pixel expansion m is defined as:

$$\gamma_{\text{NS}}(\mathcal{S}) = \frac{h - \ell}{m} \tag{2}$$

while Eisen and Stinson [21] have proposed

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

Alternative definitions of contrast have been given in [26] and [39]. Notice that the definition of the thresholds ℓ and h that we use in this paper is different from that used in [21] and [39]. If we denote with $\hat{\ell}$ and $\hat{h}$ the thresholds of [21] and [39] we have that $\hat{\ell} = m - h$ and $\hat{h} = m - \ell$. Thus the definition of contrast of [21], namely $\frac{\hat{h}-\hat{l}}{m+\hat{l}}$, becomes (3).

The definition of the contrast measure for deterministic schemes is an interesting point of discussion and has been the subject of several papers [18], [21], [26], [39]. We focus the attention on the γ_{NS} and γ_{ES} measures because the former is the one for which most results are known and the latter, as we will prove in this paper, is equal to γ_{RG}, the contrast measure used in random grid model. The result $\gamma_{\text{RG}} = \gamma_{\text{ES}}$, somehow supports this measure as the best one (see also the

[2]A singleton cannot be qualified. Indeed if a singleton $Q = \{i\}$ is qualified, then participant i knows the secret and it does not make sense that i "shares" the secret with other participants.

discussion in [21]), since it has been independently used in two mdoels. Moreover, both [18] and [21] give arguments to support the conclusion that γ_{ES} is better than γ_{NS}. The discussion about which measure is better goes beyond the scope of this paper and is an interesting research problem on its own already addressed, although not solved, in various papers. The goal of this paper is to prove the equivalence of the random grid model and the deterministic model (regardless of which measure is used to assess the contrast).

C. The Probabilistic Model

The probabilistic model allows both schemes having no pixel expansion and schemes with pixel expansion. In a probabilistic scheme the correct reconstruction is guaranteed only with some probability. We refer the reader to [15], [45] for a formal definition. Here we recall only some basic notions.

Let $p_{w|w}(Q)$, where Q is a qualified set of participants, be the probability of correctly reconstructing a white (secret) pixel when superposing the shares of Q, and $p_{b|b}(Q)$ be the probability of correctly reconstructing a black (secret) pixel. Clearly, we have $p_{b|w}(Q) = 1 - p_{w|w}(Q)$ and $p_{w|b}(Q) = 1 - p_{b|b}(Q)$. A probabilistic scheme is called β-probabilistic if for any qualified set Q it holds that

$$p_{b|b}(Q) - p_{b|w}(Q) \geq \beta$$

and

$$p_{w|w}(Q) - p_{w|b}(Q) \geq \beta.$$

Parameter β is a measure of the quality of the scheme and, roughly speaking, is the counterpart of the contrast.

Probabilistic schemes are important for the result of this paper. Indeed the main results presented in Section IV could be also restated in terms of probabilistic schemes and roughly speaking they would state that the random grid model is equivalent to the probabilistic model with no pixel expansion. Using a formal treatment of probabilistic schemes would introduce a lot of unnecessary details and the formalism used for the probabilistic model would cause also some difficulties with the handling of the contrast parameters. Because of this we directly relate random grid schemes to deterministic schemes. This choice is also motivated by the fact that, since the connections established in this paper allow to use results known for a given model in the other, our main goal is to use bounds and schemes for the random grid model in the deterministic model and viceversa, because for these two models many results are known.

D. On the Use of the Various Definitions of Contrast

Although the contrast for random grid schemes is defined as a function of the average light transmission and the contrast of deterministic schemes is defined as a function of the thresholds ℓ and h, it is not difficult to see that there is a strict correlation between the average light transmissions parameters and the contrast parameters. In Section IV the exact relation will be assessed. Here we only point out that one can use γ_{NS} and γ_{ES} also in the random grid model and γ_{RG} also in the deterministic model. We will see in Section IV, that, in fact, $\gamma_{RG} = \gamma_{ES}$.

E. Shares Description

In order to visually share a secret the dealer constructs the shares starting from the secret image and making random choices. In other words, the dealer uses a randomized algorithm $\mathcal{A}(I)$ that takes as input the secret image I, and gives in output n shares, where n is the number of participants.

The algorithm used to construct shares for schemes in the deterministic and probabilistic models, has a specific form: it uses two multisets of $n \times m$ *distribution* matrices $\mathcal{C}_\bullet$ and $\mathcal{C}_\circ$, one for black secret pixels and one for white secret pixels. Each matrix is a particular way of distributing the shares and given a matrix, each row represents one share. The algorithm $\mathcal{A}$ for the generation of the shares simply selects uniformly at random a distribution matrix from the multiset.

The shares construction algorithms for random grid schemes do not have a specific form and are usually described with pseudocode.

Clearly, the method used to describe the algorithm $\mathcal{A}$ is an aesthetic matter. Just to make formal this statement, we state the following facts.

Fact 2.3: Any scheme given by means of two collections of distribution matrices, can be described as pseudocode.

Proof: Trivial (The pseudocode is: if the secret pixel is black then select uniformly at random a matrix from $\mathcal{C}_\bullet$ while if the secret pixel is white then select uniformly at random a matrix from $\mathcal{C}_\circ$.) ■

It might seem that using pseudocode for the description of $\mathcal{A}$ is more general. But in fact using distribution matrices one can describe any algorithm for the generation of the shares, as stated in the following fact.

Fact 2.4: Any scheme given by means of an algorithm specified as pseudocode can be described by means of two collections of distribution matrices.

Proof: Let $\mathcal{A}$ be the algorithm that constructs the shares. For each pixel s of the secret image, algorithm $\mathcal{A}$ has to produce n shares as a function of the color of pixel s. The output of algorithm $\mathcal{A}$, beside depending on the secret pixel s depends also on random choices. The output of $\mathcal{A}$ can be represented as a $n \times m$ matrix with entries in $\{\circ, \bullet\}$. Let $v_1, v_2, \ldots, v_z$ be all possible outputs of $\mathcal{A}(\circ)$ and let p_i, $1 \leq i \leq z$, be the probability with which matrix v_i is given as output by $\mathcal{A}(\circ)$. Let w be the smallest integer such that $w \cdot p_1, \ldots, w \cdot p_z$ are all integers. Notice that w exists since (we assumed that) all the probabilities are rational numbers. Let $\mathcal{C}_\circ$ be the multiset of matrices where v_i appears $w \cdot p_i$ times. In a similar way define $\mathcal{C}_\bullet$ using $\mathcal{A}(\bullet)$. The scheme described by $\mathcal{C}_\circ$ and $\mathcal{C}_\bullet$ is the same scheme constructed by algorithm $\mathcal{A}$. ■

F. Examples

In this section we provide some examples. We consider the random grid schemes of Kafri and Keren: [27] provides 3 algorithms for the construction of $(2, 2)$-threshold schemes. Let us call these 3 schemes RG1, RG2 and RG3.

Scheme RG1. Scheme RG1 constructs the first share as a uniform random grid and the second share by assigning to pixel (i, j) the same color of the pixel (i, j) in the first share,

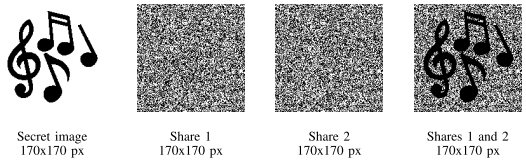

Fig. 1. Example of shares and superposition for scheme RG1.

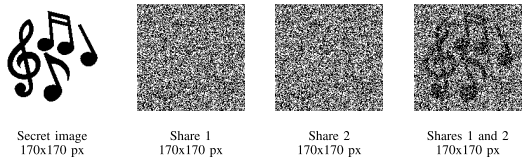

Fig. 2. Example of shares and superposition for scheme RG2.

if the secret pixel (i, j) is white, and the "opposite" color if the secret pixel (i, j) is black. The representation with distribution matrices of RG1, that is, the equivalent scheme in the probabilistic model, is described by

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

Fig. 1 shows the shares and the superposition of the two shares that reveals the secret image. The shares are uniform random grids, hence the average light transmission over each single share is $1/2$. In the reconstructed image R, the area that corresponds to black pixels of the secret image I, that is $\mathcal{B}_I(R)$, is reconstructed as a completely black area. Thus $\lambda_\bullet(RG1) = 0$. Hence, with RG1, black pixels are reconstructed in a perfect way. Instead $\mathcal{W}_I(R)$ consists of white and black pixels uniformly distributed over the region $\mathcal{W}_I(R)$, and thus $\lambda_\circ(RG1) = 1/2$. Hence, $\gamma_{\text{RG}} = 0.5$. If we see the scheme as a probabilistic scheme with $m = 1$, we have that $p_{w|w} = 1/2$ and $p_{b|b} = 1$ and thus $\beta = 0.5$.

Scheme RG2. Scheme RG2 generates again the first share as a uniform random grid. The second share is equal to the first when the secret pixel is white but if the secret pixel is black then also the second share is chosen at random. Scheme RG2 is described by the following collections:

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

Fig. 2 shows the shares and the superposition. The shares are again uniform random grids. However this time we have $\lambda_\circ(RG2) = 0.5$ and $\lambda_\bullet(RG2) = 0.25$ and thus the contrast is $\gamma_{\text{RG}} = (0.5 - 0.25)/1.25 = 0.2$. The white area $\mathcal{W}_I(R)$ is reconstructed as in the previous example, but the black area $\mathcal{B}_I(R)$ is not reconstructed perfectly but with, in average, 3 black pixels out of four pixels. If we see the scheme as a probabilistic scheme with $m = 1$, we have that $\beta = 0.25$. Indeed when the secret pixel is white the reconstruction provides either black or white with probability $1/2$, hence $p_{w|w} = p_{b|w} = 1/2$, while when the secret pixel is black the reconstruction provides black with probability $3/4$, that is $p_{b|b} = 3/4$, and white with probability $1/4$, that is $p_{w|b} = 1/4$. Thus $p_{b|b} - p_{b|w} = 1/4$.

Scheme RG3. In this scheme the first share is again generated at random while the second one is also generated at random

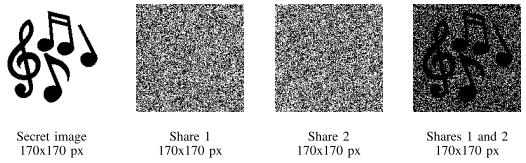

Fig. 3. Example of shares and superposition for scheme RG3.

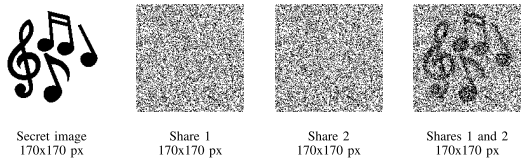

Fig. 4. Example of shares and superposition for scheme RG4.

if the secret pixel is white, and is the "opposite" of the first share if the secret pixel is black. Using distribution matrices, scheme RG3 is:

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

Fig. 3 shows the shares and the reconstruction. Again the shares are uniform random grids. We have $\lambda_\circ(RG3) = 0.25$ and $\lambda_\bullet(RG3) = 0$ and thus $\gamma_{\text{RG}} = 0.25$. If we see the scheme as a probabilistic scheme with $m = 1$, we have that $\beta = 0.25$.

Scheme RG4. Finally we present another example of a random grid $(2, 2)$-threshold scheme that uses generalized (non-uniform) random grids. Scheme RG4 is described by the following collections:

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

Fig. 4 shows the shares and the reconstruction. This time the shares are not uniform random grids but they are generalized random grids, since each single share has more white pixels (2/3) than black pixels (1/3). Hence we have $\lambda_\circ(RG4) = 2/3$ and $\lambda_\bullet(RG4) = 1/3$ and thus is $\gamma_{\text{RG}} = 1/4$. If we see the scheme as a probabilistic scheme with $m = 1$, we have that $\beta = 1/3$.

III. Previous Results

In this section we recall some known results that will be used later in the paper.

A. Deterministic VCS

In this section we recall some (relevant to this paper) results known for the deterministic visual cryptography model.

Theorem 3.1: [8], [23] For $n \geq 2$, in any deterministic $(2, n)$-threshold scheme we have that $\gamma_{\text{NS}} \leq \frac{\lceil n/2 \rceil \lfloor n/2 \rfloor}{n(n-1)}$.

We can construct $(2, n)$-threshold schemes that achieve optimal γ_{NS} contrast by using a black base matrix whose columns are all the binary vectors of weight $\lfloor n/2 \rfloor$ and a white base matrix consisting of n equal rows each with weight $\binom{n-1}{\lfloor n/2 \rfloor - 1}$. The pixel expansion is $m = \binom{n}{\lfloor n/2 \rfloor}$.

Theorem 3.2: [34] For $n \geq 2$, in any deterministic (n, n)-threshold scheme we have that $\gamma_{\text{NS}} \leq \frac{1}{2^{n-1}}$ and $m \geq 2^{n-1}$.

We can construct (n, n)-threshold schemes that achieve optimal γ_{NS} contrast by using a black base matrix whose

columns are all the binary vectors with an even weight (that is, $\mu^{\bullet}_{2i} = 1$ and $\mu^{\bullet}_{2i+1} = 0$ for $i = 0, 1, \ldots \lfloor n/2 \rfloor$) and a white base matrix whose columns are all the binary vectors with an odd weight (that is, $\mu^{\circ}_{2i} = 0$ and $\mu^{\circ}_{2i-1} = 1$ for $i = 0, 1, \ldots \lceil n/2 \rceil$). The pixel expansion is $m = 2^{n-1}$.

Bounds on γ_{NS} for $(3, n)$-threshold schemes and $(n-1, n)$-threshold schemes are provided in Blundo et al. [6]. Krause and Simon [28] have provided a general (for any k) formula:

Theorem 3.3: [28] For $k \geq 2$ and $n \geq k$, in any deterministic (k, n)-threshold scheme we have that

$$\gamma_{\text{NS}} \leq 4^{-(k-1)} \frac{n^k}{n(n-1)\cdots(n-(k-1))}.$$

A number of papers have considered the problem of finding schemes for which the reconstruction of black pixels is perfect, that is schemes for which $h = m$. In particular we recall the following two constructions of $(3, n)$-threshold schemes.

Construction 3.4: [7] Construction of a $(3, n)$-threshold scheme, with $n \geq 3$: The white base matrix is described by $\mu^{\circ}_0 = 1$ and $\mu^{\circ}_{n-1} = n-2$ (and the remaining μ°s are equal to 0). The black base matrix is described by $\mu^{\bullet}_n = \frac{(n-1)(n-2)}{2}$ and $\mu^{\bullet}_{n-2} = 1$ (and the remaining $\mu^{\bullet}$s are equal to 0).

Theorem 3.5: [7] For $n \geq 3$, Construction 3.4 yields deterministic $(3, n)$-threshold scheme with $m = (n-1)^2$, $\ell = m - 1$ and $h = m$ and thus $\gamma_{\text{NS}} = \frac{1}{n^2-1}$.

Construction 3.6: [6] Construction of a $(3, n)$-threshold scheme, with $n \geq 3$: The white base matrix is described by

$$\mu^{\circ}_0 = \binom{n-1}{\lfloor \frac{n+1}{4} \rfloor} - \binom{n-1}{\lfloor \frac{n+1}{4} \rfloor - 1}, \quad \mu^{\circ}_{n-\lfloor \frac{n+1}{4} \rfloor} = 1$$

and all remaining $\mu^{\bullet}$s are 0. The black base matrix is described by

$$\mu^{\bullet}_n = \binom{n-1}{\lfloor \frac{n+1}{4} \rfloor} - \binom{n-1}{\lfloor \frac{n+1}{4} \rfloor - 1}, \quad \mu^{\circ}_{\lfloor \frac{n+1}{4} \rfloor} = 1$$

and all remaining μ°s are 0.

Theorem 3.7: [6] For $n \geq 3$, Construction 3.6 (see Section 4.2 and Theorem 4.7 of [6]) yields a deterministic $(3, n)$-threshold scheme with that $m = 2\binom{n-1}{\lfloor \frac{n+1}{4} \rfloor}$ ands $\gamma_{\text{NS}} = \frac{(n-2)\lfloor \frac{n+1}{4} \rfloor \lfloor \frac{n+1}{4} \rfloor}{2(n-1)(n-2)}$.

Finally we recall the following construction of $(n-1, n)$-threshold schemes.

Construction 3.8: [7] Construction of a $(n-1, n)$-threshold scheme, with $n \geq 3$: The white base matrix is described by $\mu^{\circ}_0 = 1$ and $\mu^{\circ}_{2i+1} = 2i$, for $1 \leq i \leq (n-1)/2$ (and the remaining μs are equal to 0). The black base matrix is described by $\mu^{\bullet}_{2i} = 1$, for $1 \leq i \leq n/2$ (and the remaining μs are equal to 0).

Theorem 3.9: [7] For $n \geq 3$, Construction 3.4 yields deterministic $(n-1, n)$-threshold schemes with $m = (n-2)2^{n-2}+1$, $\ell = m-1$ and $h = m$, and thus $\gamma_{\text{NS}} = \frac{1}{(n-2)2^{n-2}+1}$.

B. Random Grid VCS

In this section we recall some (relevant to this paper) results for the random grid model. The following result has been proved by Shyu [36].

Construction 3.10: [36] For any $n \geq 2$, there exists random grid (n, n)-threshold schemes with $\lambda_{\bullet} = 0$ and $\lambda_{\circ} = \frac{1}{2^{n-1}}$ (thus with $\gamma_{\text{RG}} = \frac{1}{2^{n-1}}$).

The following has been proved by Chen and Lin [10].

Construction 3.11: [10] For any $n \geq 2$, there exists random grid $(2, n)$-threshold schemes with contrast $\gamma_{\text{RG}} = \frac{c/n - (c/n)^2}{1 + (c/n)^2 - 1/n(1+c/n)}$, where $c \in \{\lfloor n(\sqrt{2}-1) \rfloor, \lceil n(\sqrt{2}-1) \rceil\}$ is the integer that maximizes γ_{RG}.

Moreover in [10] it is proved (Theorem 4 of [10]) that the schemes of Construction 3.11 are such that $\gamma_{\text{RG}} \leq \frac{3-2\sqrt{2}}{-2+2\sqrt{2}-1/n}$. Notice that this bound applies only to schemes that have a particular form (the one used by Construction 3.11).

Also, [10] provides an extension of the $(2, n)$-threshold schemes yielding a $(2, \infty)$-threshold scheme with $\gamma_{\text{RG}} = (\sqrt{2}-1)/2 \simeq 0.2071$. Among the schemes with the same form of Construction 3.11, the $(2, \infty)$-threshold scheme is asymptotically optimal because

$$\lim_{n \to \infty} \frac{3 - 2\sqrt{2}}{-2 + 2\sqrt{2} - 1/n} = (\sqrt{2}-1)/2.$$

Chen and Tsao [12] provide constructions of random grid (k, n)-threshold schemes whose contrast is given in the next theorem.

Construction 3.12: [12] For any $k \geq 2$ and $n \geq k$, there exists (k, n)-threshold random grid schemes with contrast[3]

$$\gamma_{\text{RG}} = \frac{2}{(2^k+1)\binom{n}{k} - 1}.$$

IV. The Connection Between the Random Grid and the Deterministic Model

In this section we present the main results of this paper. We prove that there is a strong connection between the random grid model and the deterministic model: for every random grid scheme there exists a corresponding deterministic scheme with similar characteristics and viceversa. This allows us to use results known in a model in the other model. As we have already pointed out it would have been possible to cast the same result by stating that the random grid model is equivalent to the probabilistic model with no pixel expansion. We have explained in Section II-C why we preferred not to pass through the probabilistic model.

Theorem 4.1: Every random grid scheme $\mathcal{S}$ with average light transmissions parameters $\lambda_{\circ}$ and $\lambda_{\bullet}$ and cardinality parameters $m_{\circ}$ and $m_{\bullet}$, can be transformed into a deterministic scheme $\mathcal{S}'$ with $m = \text{LCM}(m_{\circ}, m_{\bullet})$, $\ell = m(1-\lambda_{\circ})$ and $h = m(1-\lambda_{\bullet})$.

Proof: By Fact II-E we have that scheme $\mathcal{S}$ can be described by two distribution collections $\mathcal{C}_{\circ}$ and $\mathcal{C}_{\bullet}$. Let $m_{\circ}$ and $m_{\bullet}$ be the cardinality parameters of $\mathcal{S}$. Construct scheme $\mathcal{S}'$ with the following base matrices. Let m be the least common multiple $\text{LCM}(m_{\circ}, m_{\bullet})$ of $m_{\circ}$ and $m_{\bullet}$. Base matrix $B_{\circ}$ is obtained by concatenating $m/m_{\bullet}$ copies of each

[3] In [12] it is proved that when superposing $t \geq k$ shares the contrast is $\gamma_{\text{RG}} = \frac{2 \cdot \binom{t}{k}}{(2^t+1)\binom{n}{k} - \binom{t}{k}}$. We have to consider the worst case contrast which is obtained with the minimum number of shares which is $t = k$.

of the vectors in $\mathcal{C}_\circ$ while base matrix $B_\bullet$ is obtained by concatenating $m/m_\circ$ copies of each of the vectors in $\mathcal{C}_\bullet$.

Since $\mathcal{S}'$ is obtained by concatenating matrices of $\mathcal{S}$, the security property of $\mathcal{S}'$ derives directly from the security property of $\mathcal{S}$. Moreover, by the definition of $\lambda_\circ$ and $\lambda_\bullet$ we have that $\ell = m(1-\lambda_\circ)$ and $h = m(1-\lambda_\bullet)$. ∎

Theorem 4.2: Every deterministic scheme $\mathcal{S}$ with pixel expansion m and contrast parameters ℓ and h, can be transformed into a random grid scheme $\mathcal{S}'$ with average light transmission parameters $\lambda_\circ = 1 - \frac{\ell}{m}$ and $\lambda_\bullet = 1 - \frac{h}{m}$.

Proof: Let $\mathcal{C}_\circ$ and $\mathcal{C}_\bullet$ be the distribution collections of $\mathcal{S}$. Construct $\mathcal{C}'_\circ$ from $\mathcal{C}_\circ$ by taking all the columns that appear in any of the matrices of $\mathcal{C}_\circ$. Notice that $\mathcal{C}'_\circ$ is a multiset if there are repeated columns. Similarly construct $\mathcal{C}'_\bullet$ from $\mathcal{C}_\bullet$. Scheme $\mathcal{S}'$ is the random grid scheme described by $\mathcal{C}'_\circ$ and $\mathcal{C}'_\bullet$ (see Fact 2.3).

Let Q be a forbidden set of participants. Then by the security property of $\mathcal{S}$ we have that the sets $\mathcal{D}_\circ = \{M|X, \text{ for each } M \in \mathcal{C}_\circ\}$ and $\mathcal{D}_\bullet = \{M|X, \text{ for each } M \in \mathcal{C}_\bullet\}$ are indistinguishable in the sense that they contain the same matrices with the same frequencies. This implies that the sets $\mathcal{D}'_\circ = \{M|X, \text{ for each } M \in \mathcal{C}'_\circ\}$ and $\mathcal{D}'_\bullet = \{M|X, \text{ for each } M \in \mathcal{C}'_\bullet\}$ are equal. Hence we have that $\lambda_\circ(Q) = \lambda_\bullet(Q)$.

Let Q be a qualified set of participants. Then by the contrast property, for any $M \in \mathcal{C}_\circ$, we have that $w_\bullet(\sup(M|Q)) \leq \ell$ and for any $M \in \mathcal{C}_\bullet$, we have that $w_\bullet(\sup(M|X)) \geq h$. Since $\mathcal{C}'_\circ$ (resp. $\mathcal{C}'_\bullet$) has been obtained by simply concatenating (a number of copies of) the matrices $M \in \mathcal{C}_\circ$ (resp. $M \in \mathcal{C}_\bullet$) we have that $\lambda_\circ(Q) \leq (m - m\ell)/m$ (resp. $h \geq (m - mh)/m$). Hence we can set $\lambda_\circ = 1 - \frac{\ell}{m}$ and $\lambda_\bullet = 1 - \frac{h}{m}$ for scheme $\mathcal{S}'$. ∎

What Theorems 4.1 and 4.2 say is that there is a strong correspondence between the random grid model and the deterministic model.

Given a random grid scheme $\mathcal{S}$ and a deterministic scheme $\mathcal{S}'$ related by Theorem 4.1 (or by Theorem 4.2, swapping the names), we have that

$$\gamma_{\text{ES}}(\mathcal{S}') = \frac{h-\ell}{2m-h} = \frac{m(1-\lambda_\bullet) - m(1-\lambda_\circ)}{2m - m(1-\lambda_\bullet)} = \frac{\lambda_\circ - \lambda_\bullet}{1+\lambda_\bullet} = \gamma_{\text{RG}}(\mathcal{S})$$

and

$$\gamma_{\text{NS}}(\mathcal{S}') = \frac{h-\ell}{m} = \frac{m(1-\lambda_\bullet) - m(1-\lambda_\circ)}{m} = \lambda_\circ - \lambda_\bullet.$$

Since γ_{ES}, used in the deterministic model, is the same as γ_{RG}, used in the random grid model, we have the following theorems.

Theorem 4.3: Let $f(n)$ be an upper bound on γ_{NS} in the deterministic model (resp. random grid model). Then we have that $f(n)$ is an upper bound on γ_{NS} also in the random grid model (resp. deterministic model).

Proof: Assume that $f(n)$ is an upper bound on γ_{NS} in the deterministic model and assume by contradiction that the theorem does not hold and thus that there exists a random grid scheme $\mathcal{S}$ with $\gamma_{\text{NS}}(\mathcal{S}) > f(n)$. Then by Theorem 4.1 we can construct a deterministic scheme $\mathcal{S}'$ with $\gamma_{\text{NS}}(\mathcal{S}') = \gamma_{\text{NS}}(\mathcal{S}) > f(n)$. This contradicts the fact that $f(n)$ is an upper bound on γ_{NS} in the deterministic model.

Similarly, assume that $f(n)$ is an upper bound on γ_{NS} in the random grid model. The proof is as before swapping "random model" with "deterministic" and using Theorem 4.2 instead of Theorem 4.1. ∎

Theorem 4.4: Let $f(n)$ be an upper bound on γ_{ES} (resp. γ_{RG}) in the deterministic model (resp. random grid model). Then we have that $f(n)$ is un upper bound on γ_{RG} (resp. γ_{ES}) also in the random grid model (resp. deterministic model).

Proof: Assume that $f(n)$ is an upper bound on γ_{ES} in the deterministic model and assume by contradiction that the theorem does not hold and thus that there exists a random grid scheme $\mathcal{S}$ with $\gamma_{\text{RG}}(\mathcal{S}) > f(n)$. Then by Theorem 4.1 we can construct a deterministic scheme $\mathcal{S}'$ with $\gamma_{\text{ES}}(\mathcal{S}') = \gamma_{\text{RG}}(\mathcal{S}) > f(n)$. This contradicts the fact that $f(n)$ is an upper bound on γ_{ES} in the deterministic model.

Similarly, assume that $f(n)$ is an upper bound on γ_{RG} in the random grid model. The proof is as before swapping "random model" with "deterministic", swapping ES with RG and using Theorem 4.2 instead of Theorem 4.1. ∎

Notice that, by the definitions, we have that $\gamma_{\text{ES}} \leq \gamma_{\text{NS}}$ hence an upper bound on γ_{NS} is also an upper bound on γ_{ES} (and on γ_{RG}, since $\gamma_{\text{RG}} = \gamma_{\text{ES}}$). This observation can be used to prove the following theorem.

Theorem 4.5: Let $f(n)$ be an upper bound on γ_{NS} in the deterministic model then we have that $f(n)$ is un upper bound on γ_{RG} also in the random grid model.

Proof: Assume that $f(n)$ is an upper bound on γ_{NS} in the deterministic model and assume by contradiction that the theorem does not hold and thus that there exists a random grid scheme $\mathcal{S}$ with $\gamma_{\text{RG}}(\mathcal{S}) > f(n)$. Then by Theorem 4.1 we can construct a deterministic scheme $\mathcal{S}'$ with $\gamma_{\text{ES}}(\mathcal{S}') = \gamma_{\text{RG}}(\mathcal{S}) > f(n)$. Since $\gamma_{\text{ES}}(\mathcal{S}') \leq \gamma_{\text{NS}}(\mathcal{S}')$ we have that $\gamma_{\text{NS}}(\mathcal{S}') > f(n)$. This contradicts the fact that $f(n)$ is an upper bound on γ_{NS} in the deterministic model. ∎

V. Threshold Schemes

In this section we focus the attention on (k, n)-threshold schemes and provide new results in the random grid model (resp. in the deterministic model) starting from known results in the deterministic model (resp. random grid model).

A. $(2, n)$-Threshold Schemes

Theorem 5.1: For any $n \geq 2$, in any random grid $(2, n)$-threshold scheme $\mathcal{S}$ we have that $\gamma_{\text{RG}}(\mathcal{S}) \leq \frac{\lceil n/2 \rceil \lfloor n/2 \rfloor}{n(n-1)}$.

Proof: Immediate consequence of Theorems 3.1 and 4.5. ∎

Notice that the bound of Theorem 5.1 is general while the bound of Chen and Lin (see paragraph after Construction 3.11), applies only to a particular class of schemes.

Fig. 5 shows the bound of Theorem 5.1 and the contrast of the schemes of Construction 3.11. For $n = 2, 3$ the value of the contrast of the scheme matches the upper bound, hence the $(2, 2)$-threshold and the $(2, 3)$-threshold schemes are optimal with respect to γ_{RG}. It remains an open problem to either find schemes with an improved contrast γ_{RG} or to prove a sharper upper bound (for example proving that the bound of

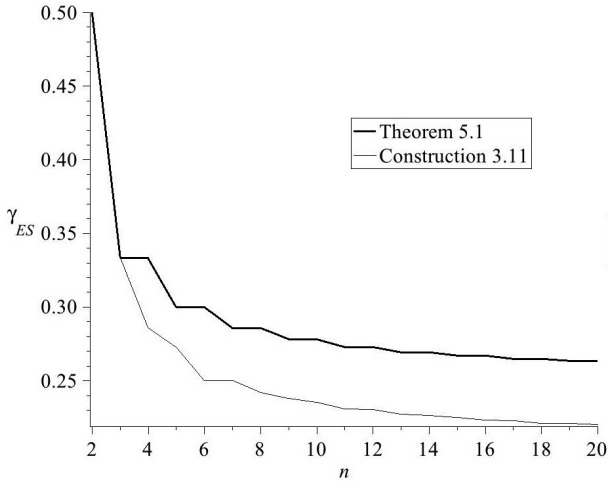

Fig. 5. Upper bound on γ_{RG} (thick line) and value of contrast of schemes of Construction 3.11 (thin line) for $(2, n)$-threshold schemes.

Chen and Lin in fact holds for any type of scheme and not just for those that have the same form of the schemes of Construction 3.11).

We can exploit the random grid $(2, n)$-threshold schemes of [10] to obtain new deterministic schemes that improve the contrast γ_{ES}. First we give a construction very similar to that of [10].

Construction 5.2: Construction of a $(2, n)$-threshold random grid scheme, with $n \geq 2$: Let $c \in \{\lfloor n(\sqrt{2}-1)\rfloor, \lceil n(\sqrt{2}-1)\rceil\}$. The collection $\mathcal{C}_\bullet$ consists of all the possible $\binom{n}{c}$ vectors having c elements equal to $\circ$ and $n-c$ elements equal to $\bullet$. The collection $\mathcal{C}_\circ$ is given by the multiset of vectors consisting of $\binom{n-1}{c-1}$ vectors with all elements equal to $\circ$ and $\binom{n}{c} - \binom{n-1}{c-1}$ vectors with all elements equal to $\bullet$. Among the two possible values for c, choose the one that maximizes γ_{ES}.

Notice that this construction is slightly different from that of [10]. Our construction ensures that the cardinality parameters are equal, that is $m_\circ = m_\bullet$. This helps in constructing deterministic schemes with a smaller pixel expansion.

Example. Let us consider an example. For $n = 5$ we have that $c = 2$ and

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

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

Construction 5.2 (see Theorem 1 of [10]) gives a random grid $(2, n)$-threshold scheme and (by the proof of Theorem 2 in [10]) we have that the parameters are $\lambda_\circ = c/n$ and $\lambda_\bullet = \frac{c}{n}\frac{c-1}{n-1}$.

By Theorem 4.1, starting from schemes obtained with Construction 5.2, we can construct deterministic schemes, that we denote with A_n. We have that for scheme A_n

$$m = \binom{n}{c}, \quad \ell = m\left(1 - \frac{c}{n}\right), \quad h = m\left(1 - \frac{c(c-1)}{n(n-1)}\right).$$

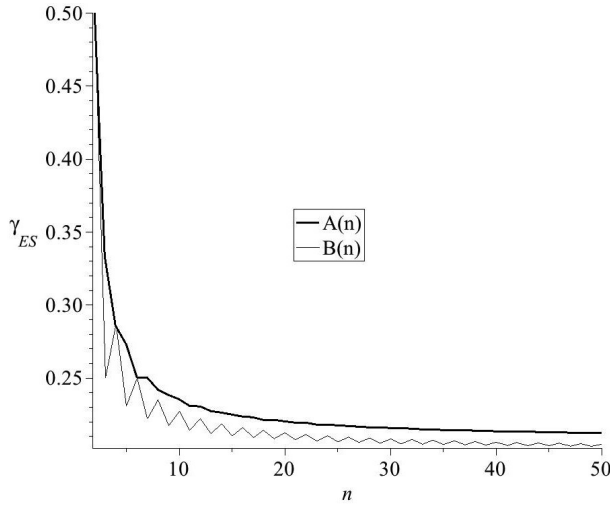

Fig. 6. Comparison of the contrast $\gamma_{ES}(A_n)$ (thick line) with $\gamma_{ES}(B_n)$ (thin line) for $(2, n)$-threshold schemes.

Hence we have

$$\gamma_{ES}(A_n) = \frac{h-\ell}{2m-h} = \frac{\frac{c}{n}\left(1 - \frac{c-1}{n-1}\right)}{1 + \frac{c}{n}\frac{c-1}{n-1}}$$

In the deterministic model optimal contrast schemes have been studied only with respect to γ_{NS}. Thus the best comparison we can make is with the schemes that are optimal with respect to γ_{NS} (see Theorem 3.1 and the subsequent paragraph). Denote with B_n such schemes. Obviously we have to compare the contrast $\gamma_{ES} = \gamma_{RG}$ of such schemes. For schemes B_n we have:

$$m = \binom{n}{\lfloor n/2\rfloor}, \quad \ell = \binom{n-1}{\lfloor n/2\rfloor - 1},$$

and

$$h = \binom{n}{\lfloor n/2\rfloor} - \binom{n-2}{\lfloor n/2\rfloor}.$$

Hence we have

$$\gamma_{ES}(B_n) = \frac{h-\ell}{2m-h} = \frac{\binom{n-1}{\lfloor n/2\rfloor} - \binom{n}{\lfloor n/2\rfloor}}{\binom{n}{\lfloor n/2\rfloor} + \binom{n-2}{\lfloor n/2\rfloor}}.$$

Fig. 6 shows a comparison of the contrast $\gamma_{ES}(A_n)$ (thick line) with $\gamma_{ES}(B_n)$ (thin line). As can be seen from the figure, the contrast γ_{ES} of the schemes of Construction 5.2 is better that the contrast γ_{ES} of the schemes that have optimal contrast γ_{NS}.

B. $(3, n)$*-Threshold Schemes*

We provide two constructions for new random grid schemes based on two different deterministic $(3, n)$-threshold schemes. The first construction allows an easy analytical comparison with previous random grid schemes. The comparison shows that the new schemes have a better contrast. The second construction gives better schemes but the analytical comparison becomes more complicated. We provide empirical evidence that this second construction provides an improved contrast.

Theorem 5.3: The random grid $(3, n)$-threshold schemes obtained by using Construction 3.4 and the transformation of Theorem 4.2 has contrast

$$\gamma_{RG} = \frac{1}{(n-1)^2}.$$

Proof: By Theorem 3.5 we have that Construction 3.4 gives a deterministic $(3,n)$-threshold scheme with $m=(n-1)^2$, $h=m$ and $\ell=m-1$. By Theorem 4.2 we can transform such a scheme into a random grid scheme with $\lambda_\circ=\frac{1}{(n-1)^2}$ and $\lambda_\bullet=0$. ∎

The contrast provided by the schemes of Theorem 5.3 is better than the contrast of the schemes of Construction 3.12. Indeed the $(3,n)$-threshold scheme of Chen and Tsao [12] have contrast $\frac{2}{(2^3+1)\binom{n}{3}-1}$. A simple algebra shows that $\frac{1}{(n-1)^2}$ is always bigger than $\frac{2}{(2^3+1)\binom{n}{3}-1}$ for $n\geq 3$. Indeed the condition $\frac{1}{(n-1)^2}>\frac{2}{(2^3+1)\binom{n}{3}-1}$ is equivalent to $3n^3-10n^2+8n-3>0$, which is true for $n\geq 3$.

Next we provide another construction with an improved contrast.

Theorem 5.4: The random grid $(3,n)$-threshold scheme obtained using Construction 3.6 and Theorem 4.2 has contrast

$$\gamma_{\text{RG}}=\frac{(n-1)(n-2)(n-2\alpha)-\psi(n-\alpha)+\psi(\alpha)}{2(n-1)(n-2)(n-\alpha)+\psi(n-\alpha)}$$

where $\alpha=\lfloor\frac{n+1}{4}\rfloor$ and $\psi(x)=x(x-1)(x-2)$.

Proof: By Theorem 3.7 we have that Construction 3.6 yields a deterministic $(3,n)$-threshold scheme with $m=2\binom{n-1}{\lfloor\frac{n+1}{4}\rfloor}$ and $\gamma_{\text{NS}}=\frac{(n-2)\lfloor\frac{n+1}{4}\rfloor\lfloor\frac{n+1}{4}\rfloor}{2(n-1)(n-2)}$. Unfortunately, Theorem 3.7 does not explicitly provide the value of ℓ and h.

In order to evaluate γ_{RG} we need to find ℓ and h. Let Q be a qualified set of three participants. Parameter ℓ (resp. h), that is the number of black pixels in $\texttt{sup}(B_\circ|Q)$ (resp. $\texttt{sup}(B_\bullet|Q)$) is given by m minus the number of the 3-white-pixel columns in $B_\circ|Q$ (resp. $B_\bullet|Q$).

To find ℓ notice that in $B_\circ$ we have μ_0° all-white columns and thus these columns will count for μ_0° 3-white-pixel columns in $B_\circ|Q$. In the remaining part of $B_\circ$ we have all the columns with exactly $n-\lfloor\frac{n+1}{4}\rfloor$ black pixels. Hence among these columns in $B_\circ|Q$, there will be exactly $\binom{n-3}{n-\lfloor\frac{n+1}{4}\rfloor}$ 3-white-pixel columns. Since ℓ is equal to m minus the number of 3-white-pixel columns, we have that $\ell=m-\mu_0^\circ-\binom{n-3}{n-\lfloor\frac{n+1}{4}\rfloor}$.

To find h notice that in $B_\bullet$ we have $\mu_n^\bullet$ all-black columns and thus among these columns in $B_\bullet|Q$ there will be no 3-white-pixel columns. In the remaining $m-\mu_n^\bullet$ columns of $B_\bullet$ we have all the columns with exactly $\lfloor\frac{n+1}{4}\rfloor$ black pixels. Hence among these columns in $B_\bullet|Q$, there will be exactly $\binom{n-3}{\lfloor\frac{n+1}{4}\rfloor}$ 3-white-pixel columns. Since h is equal to m minus the number of 3-white-pixel columns of $B_\circ|Q$, we have that $h=m-\binom{n-3}{\lfloor\frac{n+1}{4}\rfloor}$.

Now we have ℓ,h and m so we can assess $\gamma_{\text{RG}}=\frac{h-\ell}{2m-h}$ and, recalling that $\mu_0^\circ=\binom{n-1}{\lfloor\frac{n+1}{4}\rfloor}-\binom{n-1}{\lfloor\frac{n+1}{4}\rfloor-1}$ we get

$$\gamma_{\text{RG}}=\frac{\binom{n-1}{\lfloor\frac{n+1}{4}\rfloor}-\binom{n-1}{\lfloor\frac{n+1}{4}\rfloor-1}-\binom{n-3}{\lfloor\frac{n+1}{4}\rfloor}+\binom{n-3}{n-\lfloor\frac{n+1}{4}\rfloor}}{2\binom{n-1}{\lfloor\frac{n+1}{4}\rfloor}+\binom{n-3}{\lfloor\frac{n+1}{4}\rfloor}}.$$

To provide a closed form for the above expression, let us recall some well-known equalities involving binomial coefficients. The symmetry relation

$$\binom{a}{b}=\binom{a}{a-b}, \tag{4}$$

the addition formula

$$\binom{a}{b}=\binom{a-1}{b-1}\binom{a-1}{b}, \tag{5}$$

the equalities

$$\binom{a}{b}=\frac{a}{b}\binom{a-1}{b-1}, \tag{6}$$

and

$$\binom{a}{c}\binom{a-c}{b}=\binom{a}{b}\binom{a-b}{c}. \tag{7}$$

From (5) used with $a=n$, $b=\lfloor\frac{n+1}{4}\rfloor$, we have that

$$\binom{n-1}{\lfloor\frac{n+1}{4}\rfloor}-\binom{n-1}{\lfloor\frac{n+1}{4}\rfloor-1}=\frac{n-2\lfloor\frac{n+1}{4}\rfloor}{n}\binom{n}{\lfloor\frac{n+1}{4}\rfloor} \tag{8}$$

From (7) used with $a=n$, $b=\lfloor\frac{n+1}{4}\rfloor$ and $c=1$, we have that

$$\binom{n-1}{\lfloor\frac{n+1}{4}\rfloor}=\frac{n-\lfloor\frac{n+1}{4}\rfloor}{n}\binom{n}{\lfloor\frac{n+1}{4}\rfloor} \tag{9}$$

Again from (7) used with $a=n$, $b=\lfloor\frac{n+1}{4}\rfloor$ and $c=3$, we have that

$$\binom{n-3}{\lfloor\frac{n+1}{4}\rfloor}=\frac{\psi(n-\lfloor\frac{n+1}{4}\rfloor)}{\psi(n)}\binom{n}{\lfloor\frac{n+1}{4}\rfloor} \tag{10}$$

From (4) used with $a=n-3$, $b=n-\lfloor\frac{n+1}{4}\rfloor$ we have that

$$\binom{n-3}{n-\lfloor\frac{n+1}{4}\rfloor}=\binom{n-3}{\lfloor\frac{n+1}{4}\rfloor-3}$$

while using three times (6) we have that

$$\binom{n}{\lfloor\frac{n+1}{4}\rfloor}=\frac{n(n-1)(n-2)}{\lfloor\frac{n+1}{4}\rfloor(\lfloor\frac{n+1}{4}\rfloor-1)(\lfloor\frac{n+1}{4}\rfloor-2)}\binom{n-3}{\lfloor\frac{n+1}{4}\rfloor-3}.$$

Combining the previous two equalities we get

$$\binom{n-3}{n-\lfloor\frac{n+1}{4}\rfloor}=\frac{\psi(\lfloor\frac{n+1}{4}\rfloor)}{\psi(n)}\binom{n}{\lfloor\frac{n+1}{4}\rfloor} \tag{11}$$

Using Equations (8)–(11), with some tedious but simple algebraic transformations we get the theorem. ∎

Corollary 5.5: The random grid $(3,n)$-threshold scheme obtained using Construction 3.6 and Theorem 4.2 has contrast

$$\gamma_{\text{RG}}=\begin{cases}\frac{2(n^2-1)}{41n^2-138n+109} & \text{if } n=3 \bmod 4\\ \frac{2(n+2)}{41n-38} & \text{if } n=2 \bmod 4\\ \frac{2(n+1)}{41n-85} & \text{if } n=1 \bmod 4\\ \frac{2n^2}{41n^2-132n+96} & \text{if } n=0 \bmod 4\end{cases}$$

Proof: By Theorem 5.4 we have that

$$\gamma_{\text{RG}}=\frac{(n-1)(n-2)(n-2\alpha)-\psi(n-\alpha)+\psi(\alpha)}{2(n-1)(n-2)(n-\alpha)+\psi(n-\alpha)}$$

where $\alpha=\lfloor\frac{n+1}{4}\rfloor$ and $\psi(x)=x(x-1)(x-2)$. Observing that for $n=3 \bmod 4$ we have $\alpha=\frac{n+1}{4}$, that for $n=2 \bmod 4$ we

have $\alpha = \frac{n-2}{4}$, that for $n = 1 \bmod 4$ we have $\alpha = \frac{n-1}{4}$, and that for $n = 0 \bmod 4$ we have $\alpha = \frac{n}{4}$, it will be enough to substitute the appropriate value in the above formula for γ_{RG}, and after some tedious but simple algebraic transformations we get the corollary. ∎

From the above corollary it is evident that for $n \to \infty$ the value of γ_{RG} approaches $2/41$.

Example. Next we provide an example that will clarify the construction of the random grid schemes of Theorem 5.4. Let $n = 4$. Construction 3.6 gives the scheme where the non-zero μ's are $\mu_0^\circ = 2, \mu_3^\circ = 1, \mu_1^\bullet = 1, \mu_4^\bullet = 2$. Hence the base matrices are:

$$B_\circ = \begin{bmatrix} \circ\circ\bullet\bullet\bullet\circ \\ \circ\circ\bullet\bullet\circ\bullet \\ \circ\circ\bullet\circ\bullet\bullet \\ \circ\circ\circ\bullet\bullet\bullet \end{bmatrix} \quad B_\bullet = \begin{bmatrix} \bullet\bullet\bullet\circ\circ\circ \\ \bullet\bullet\circ\bullet\circ\circ \\ \bullet\bullet\circ\circ\bullet\circ \\ \bullet\bullet\circ\circ\circ\bullet \end{bmatrix}$$

By using Theorem 4.2 we can transform such a scheme into a random grid scheme which is given by

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

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

The contrast provided by the schemes of Theorem 5.4 improves on that of the schemes of Theorem 5.3. Fig. 7 shows empirical evidence. The figure includes also the contrast of schemes of Construction 3.12.

C. $(n-1, n)$-Threshold Schemes

Theorem 5.6: The random grid $(n-1, n)$-threshold schemes obtained by using Construction 3.4 and the transformation of Theorem 4.2 has contrast $\gamma_{\text{RG}} = \frac{1}{(n-2)2^{n-2}+1}$.

Proof: By Theorem 3.5 we have that Construction 3.4 gives a deterministic $(n-1, n)$-threshold scheme with $m = (n-2)2^{n-2} + 1$, $h = m$ and $\ell = m - 1$. By Theorem 4.2 we can transform such a scheme into a random grid scheme with $\lambda_\circ = \frac{1}{(n-2)2^{n-2}+1}$ and $\lambda_\bullet = 0$. ∎

The contrast provided by the schemes of Theorem 5.6 is better than the contrast of schemes of Construction 3.12. Indeed the $(n-1, n)$-threshold scheme of Chen and Tsao [12] have contrast $\frac{2}{(2^{n-1}+1)\binom{n}{n-1}-1}$. If we compute the difference we can easily see that it is always positive. Indeed

$$\frac{1}{(n-2)2^{n-2}+1} - \frac{2}{(2^{n-1}+1)\binom{n}{n-1}-1} > 0$$

is equivalent to

$$(2^{n-1}+1)\binom{n}{n-1} - 1 - 2((n-2)2^{n-2}+1) > 0$$

and a simple algebra shows that the above is true for all $n \geq 2$.

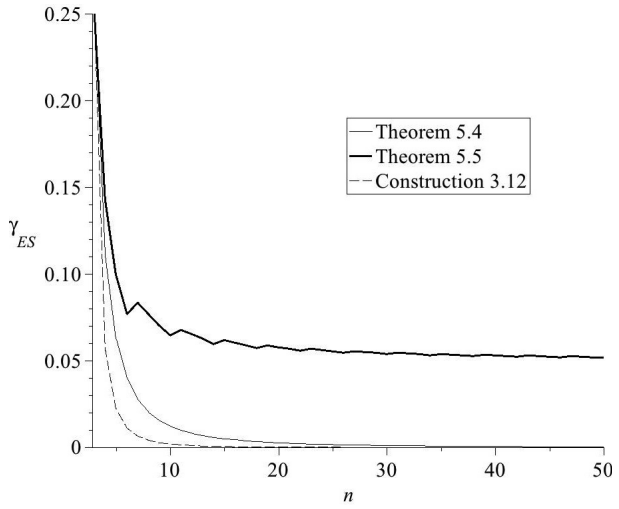

Fig. 7. Comparison of the contrast for $(3, n)$ schemes, Theorem 5.4 (thick line), Theorem 5.3 (thin line) and Construction 3.12 (dashed line).

D. (n, n)-Threshold Scheme

In this section we focus the attention on (n, n)-threshold schemes.

Theorem 5.7: For any $n \geq 2$, in any random grid (n, n)-threshold scheme $\mathcal{S}$ we have that $\gamma_{\text{RG}}(\mathcal{S}) \leq 1/2^{n-1}$.

Proof: Immediate consequence of Theorems 3.2 and 4.5. ∎

The bound of Theorem 5.7 matches the contrast of the random grid (n, n)-threshold schemes of Shyu [36], hence:

Corollary 5.8: The random grid (n, n)-threshold scheme by Shyu is optimal with respect to the contrast γ_{RG} (and also with respect to γ_{NS} since the schemes have perfect reconstruction of black pixels and thus $\gamma_{\text{RG}} = \gamma_{\text{NS}}$).

The optimal (n, n)-threshold schemes by Shyu are the same as the ones we can get starting from the deterministic (n, n)-threshold schemes of Naor and Shamir.

Roughly speaking, the construction of Shyu [36] is as follows: the first $n-1$ shares $S_1, \ldots, S_{n-1}$ are generated as independent random grids. The last share S_n is a function of $S_1, \ldots, S_{n-1}$. Although cast with a different formalism, this function sets the pixel of the last share in such a way that the total number of black pixels in the n shares is even if the secret bit is white and odd if the secret pixel is black. Hence Shyu's random grid (n, n)-threshold scheme is in fact the same as the random grid (n, n)-threshold scheme that can be obtained by taking as possible distribution vectors all the vectors of the base matrices of the Naor and Shamir's (n, n)-threshold scheme.

Example. Consider the case $n = 3$. The base matrices of Naor and Shamir $(3, 3)$-threshold schemes are.

$$B_\circ = \begin{bmatrix} \circ\circ\bullet\bullet \\ \circ\bullet\circ\bullet \\ \circ\bullet\bullet\circ \end{bmatrix} \quad B_\bullet = \begin{bmatrix} \bullet\circ\circ\bullet \\ \circ\bullet\circ\bullet \\ \circ\circ\bullet\bullet \end{bmatrix}$$

The corresponding random grid $(3, 3)$ scheme is

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

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

The above scheme is the same one that is constructed by the construction of Shyu [36].

E. (k, n)-Threshold Schemes

Finally we give an upper bound on γ_{RG} valid for any value of k.

Theorem 5.9: For any $k \geq 2$ and $n \geq k$, in any random grid (k, n)-threshold scheme we have that

$$\gamma_{\text{RG}} \leq 4^{-(k-1)} \frac{n^k}{n(n-1)\cdots(n-(k-1))}.$$

Proof: Immediate consequence of Theorems 3.3 and 4.5. ∎

We have already considered upper bounds for the cases $k = 2, n$ (Theorems 5.1 and 5.7). The general form provided above does not improve on the specific cases $k = 2$ and $k = n$. However it gives bounds for the other values of k for which no bounds on γ_{RG} were known.

VI. General Access Structure

Theorems 4.1 and 4.2 apply also to schemes with general access structures. Hence we can construct new random grid schemes for general access structures starting from deterministic schemes. Paper [2] shows a general technique that can be used to construct deterministic schemes for non-connected access structures. The same technique can be applied to random grid schemes.

Let $\mathcal{A}_1 = (\mathcal{Q}_1, \mathcal{F}_1)$ and $\mathcal{A}_2 = (\mathcal{Q}_2, \mathcal{F}_2)$ be two access structures on disjoint sets of participants. Let $\mathcal{A} = (\mathcal{Q}, \mathcal{F})$ be the *sum* of $\mathcal{A}_1$ and $\mathcal{A}_2$, given by

$$\mathcal{Q} = \mathcal{Q}_1 \cup \mathcal{Q}_2$$

and

$$\mathcal{F} = \{X \cup Y | X \in \mathcal{F}_1, Y \in \mathcal{F}_2\}.$$

Given a scheme $\mathcal{S}_1 = \{\mathcal{C}^1_\circ, \mathcal{C}^1_\bullet\}$ for $\mathcal{A}_1$ and a scheme $\mathcal{S}_2 = \{\mathcal{C}^2_\circ, \mathcal{C}^2_\bullet\}$ for $\mathcal{A}_2$, Theorem 5.5 of [2] shows that there exists a scheme $\mathcal{S} = \{\mathcal{C}_\circ, \mathcal{C}_\bullet\}$ with access structure $\mathcal{A}$. The scheme is obtained by letting

$$\mathcal{C}_\circ = \left\{ \begin{bmatrix} M' \\ M'' \end{bmatrix} : M' \in \mathcal{C}^1_\circ, M'' \in \mathcal{C}^2_\circ \right\}$$

and

$$\mathcal{C}_\bullet = \left\{ \begin{bmatrix} M' \\ M'' \end{bmatrix} : M' \in \mathcal{C}^1_\bullet, M'' \in \mathcal{C}^2_\bullet \right\}.$$

For the construction of Theorem 5.5 of [2] it is shown that one can assume, without loss of generality, that both scheme $\mathcal{S}_1$ and $\mathcal{S}_2$, have cardinality parameters that are equal, that is for each $\mathcal{S}_i$, $|\mathcal{C}^i_\circ| = |\mathcal{C}^i_\circ|$. Although this assumption is without loss of generality, because we can replicate matrices in each collection in order to have distribution collections of the same size, it increases the total number of matrices to consider and consequently the amount of randomness needed. It is not hard to see that the construction works even if we relax this requirement.

VII. Conclusion

In this paper we have shown that deterministic and random grid visual cryptography are strictly related. As a consequence many results known for the deterministic model can be used in the random grid model and viceversa. In the current literature papers that deal with random grid ignore results known for the deterministic model and viceversa.

Although the connection established in this paper allows to re-use many known results, it also opens up new directions. For example, given the fact that the measure of contrast γ_{RG} used in the random grid model corresponds to the measure of contrast γ_{ES} given in [21] for the deterministic model, it becomes interesting to further study γ_{ES} in the deterministic model. Almost all the papers that studied the contrast in the deterministic model have used the definition of contrast γ_{NS} given in [34] and little is known for γ_{ES}.

Many problems remain open. For example it is possible to find better random grid (k, n)-threshold schemes? For $k = n$ we have proved that the known random grid schemes are optimal with respect to γ_{RG}. However for the other cases there is still a gap between the contrast of known schemes and the upper bound. For the case of $k = 2$, the schemes match the upper bound only for $n = 2, 3$. Clearly the same question can be recast in the deterministic model: which is the optimal contrast γ_{ES}? Which are the optimal, with respect to γ_{ES}, schemes?

Given the connection established in this paper, it will be enough to solve any of these open problems either in the random grid model with respect to γ_{RG}, or in the deterministic model with respect to γ_{ES}.

Acknowledgment

The authors would like to thank an anonymous referee for letting them know about [22], and Fu and Yu for providing them the paper that was not yet publicly available at the time of submission of the final version of this paper.

References

[1] A. Adhikari and S. Sikdar, "A new (2,n)-visual threshold scheme for color images," in *Proc. 4th Int. Conf. Cryptol.*, Dec. 2005, pp. 148–161.
[2] G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson, "Visual cryptography for general access structures," *Inf. Comput.*, vol. 129, no. 2, pp. 86–106, Sep. 1996.
[3] G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson, "Extended schemes for visual cryptography," *Theoretical Comput. Sci.*, vol. 250, pp. 143–161, Aug. 2001.
[4] C. Blundo, S. Cimato, and A. De Santis, "Visual cryptography schemes with optimal pixel expansion," *Theoretical Comput. Sci.*, vol. 369, nos. 1–3, pp. 169–182, Dec. 2006.
[5] C. Blundo, A. De Bonis, and A. De Santis, "Improved schemes for visual cryptography," *Des., Codes Cryptogr.*, vol. 24, no. 3, pp. 255–278, Dec. 2001.
[6] C. Blundo, P. D'Arco, A. De Santis, and D. R. Stinson, "Contrast optimal threshold visual cryptography schemes," *SIAM J. Discrete Math.*, vol. 16, no. 2, pp. 224–261, 2003.
[7] C. Blundo and A. De Santis, "Visual cryptography schemes with perfect reconstruction of black pixels," *J. Comput. Graph.*, vol. 22, pp. 449–455, Jan. 1998.
[8] C. Blundo, A. De Santis, and D. R. Stinson, "On the contrast in visual cryptography schemes," *J. Cryptol.*, vol. 12, no. 4, pp. 261–289, Sep. 1999.
[9] C.-C. Chang, C.-C. Lin, T. H. N. Le, and H. B. Le, "Self-verifying visual secret sharing using error diffusion and interpolation techniques," *IEEE Trans. Inf. Forensics Security*, vol. 4, no. 4, pp. 790–801, Dec. 2009.

[10] S.-K. Chen and S.-J. Lin, "Optimal $(2, n)$ and $(2, \infty)$ visual secret sharing by generalized random grids," *J. Vis. Commun. Image Represent.*, vol. 23, no. 4, pp. 677–684, May 2012.
[11] T.-H. Chen and K.-H. Tsao, "Visual secret sharing revisited," *Pattern Recognit.*, vol. 42, no. 9, pp. 2203–2217, Sep. 2009.
[12] T.-H. Chen and K.-H. Tsao, "Threshold visual secret sharing by random grids," *J. Syst. Softw.*, vol. 84, no. 7, pp. 1197–1208, Jul. 2011.
[13] S. Cimato, R. De Prisco, and A. De Santis, "Colored visual cryptography without color darkening," *Theoretical Comput. Sci.*, vol. 374, nos. 1–3, pp. 261–276, 2007.
[14] S. Cimato, R. De Prisco, and A. De Santis, "Optimal colored threshold visual cryptography schemes," *Des., Codes Cryptogr.*, vol. 35, no. 3, pp. 311–335, Jun. 2005.
[15] S. Cimato, R. De Prisco, and A. De Santis, "Probabilistic visual cryptography schemes," *Comput. J.*, vol. 49, no. 1, pp. 97–107, 2006.
[16] S. Cimato and C.-N. Yang, *Visual Cryptography and Secret Image Sharing*. Boca Raton, FL, USA: CRC Press, 2012.
[17] P. D'Arco and R. De Prisco, "Secure two-party computation: A visual way," in *Information Theoretic Security* (Lecture Notes in Computer Science). New York, NY, USA: Springer-Verlag, 2014, pp. 18–38.
[18] P. D'Arco, R. De Prisco, and A. De Santis, "Measure-independent characterization of contrast optimal visual cryptography schemes," in *Information Theoretic Security* (Lecture Notes in Computer Science). New York, NY, USA: Springer-Verlag, 2014, pp. 39–55.
[19] R. De Prisco and A. De Santis, "Using colors to improve visual cryptography for black and white images," in *Information Theoretic Security* (Lecture Notes in Computer Science). New York, NY, USA: Springer-Verlag, 2011, pp. 182–201.
[20] R. De Prisco and A. De Santis, "Color visual cryptography schemes for black and white secret images," *Theoretical Comput. Sci.*, vol. 510, pp. 62–86, Oct. 2013.
[21] P. A. Eisen and D. R. Stinson, "Threshold visual cryptography schemes with specified whiteness levels of reconstructed pixels," *Des., Cods Cryptogr.*, vol. 25, no. 1, pp. 15–61, Jan. 2002.
[22] Z.-X. Fu and B. Yu, "Visual cryptography and random grids schemes," in *Proc. 12th Int. Workshop Dig., Forensics Watermarking*, Oct. 2013, pp. 1–6.
[23] T. Hofmeister, M. Krause, and H. U. Simon, "Contrast-optimal k out of n secret sharing schemes in visual cryptography," *Theoretical Comput. Sci.*, vol. 240, no. 2, pp. 471–485, Jun. 2000.
[24] Y.-C. Hou, "Visual cryptography for color images," *Pattern Recognit.*, vol. 36, pp. 1619–1629, Jul. 2003.
[25] M. Iwamoto, "A weak security notion for visual secret sharing schemes," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 2, pp. 372–382, Apr. 2012.
[26] F. Liu, C. Wua, and X. Lin, "A new definition of the contrast of visual cryptography scheme," *Inf. Process. Lett.*, vol. 110, no. 7, pp. 241–246, Mar. 2010.
[27] O. Kafri and E. Keren, "Encryption of pictures and shapes by random grids," *Opt. Lett.*, vol. 12, no. 6, pp. 377–379, 1987.
[28] M. Krause and H. U. Simon, "Determining the optimal contrast for secret sharing schemes in visual cryptography," *Combinatorics, Probab. Comput.*, vol. 12, no. 3, pp. 285–299, 2003.
[29] K.-H. Lee and P.-L. Chiu, "An extended visual cryptography algorithm for general access structures," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 1, pp. 219–229, Feb. 2012.
[30] S.-J. Lin and W.-H. Chung, "A probabilistic model of visual cryptography scheme with dynamic group," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 1, pp. 197–207, Jan. 2012.
[31] F. Liu, C. Wu, and X. Lin, "Step construction of visual cryptography schemes," *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 1, pp. 27–38, Mar. 2010.
[32] F. Liu and C. Wu, "Embedded extended visual cryptography schemes," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 2, pp. 307–322, Jun. 2011.
[33] S. Lu, D. Manchala, and R. Ostrovsky, "Visual cryptography on graphs," *J. Combinat. Optim.*, vol. 21, no. 1, pp. 47–66, Jan. 2011.
[34] M. Naor and A. Shamir, "Visual cryptography," in *Advances in Cryptology* (Lecture Notes in Computer Science), vol. 950. New York, NY, USA: Springer-Verlag, 1994, pp. 1–12.
[35] S.-J. Shyu, "Image encryption by random grids," *Pattern Recognit.*, vol. 40, no. 3, pp. 1014–1031, Mar. 2007.
[36] S.-J. Shyu, "Image encryption by multiple random grids," *Pattern Recognit.*, vol. 42, no. 7, pp. 1582–1596, Jul. 2009.
[37] S.-J. Shyu and H.-W. Jian, "General constructions for threshold multiple-secret visual cryptographic schemes," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 5, pp. 733–743, May 2013.
[38] H. U. Simon, "Perfect reconstruction of black pixels revisited," in *Fundamentals of Computation Theory* (Lecture Notes in Computer Science). New York, NY, USA: Springer-Verlag, 2005, pp. 221–232.
[39] E. R. Verheul and H. C. A. van Tilborg, "Constructions and properties of k out of n visual secret sharing schemes," *Des., Codes, Cryptogr.*, vol. 11, no. 2, pp. 179–196, May 1997.
[40] R.-Z. Wang, Y.-C. Lan, Y.-K. Lee, S. S.-J. Huang, and T.-L. Chia, "Incrementing visual cryptography using random grids," *Opt. Commun.*, vol. 283, no. 21, pp. 4242–4249, Nov. 2010.
[41] D. Wang, D. Lin, and X. Li, "Towards shift tolerant visual secret sharing schemes," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 2, pp. 323–337, Jun. 2011.
[42] D. Wang, T. Song, L. Dong, and C. Yang, "Optimal contrast grayscale visual cryptography schemes with reversing," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 12, pp. 2059–2072, Dec. 2013.
[43] X. Wu and W. Sun, "Random grid-based visual secret sharing with abilities of OR and XOR decryptions," *J. Vis. Commun. Image Represent.*, vol. 24, no. 1, pp. 48–62, Jan. 2013.
[44] X. Wu and W. Sun, "Generalized random grid and its applications in visual cryptography," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 9, pp. 1541–1553, Sep. 2013.
[45] C.-N. Yang, "New visual secret sharing schemes using probabilistic method," *Pattern Recognit. Lett.*, vol. 25, no. 4, pp. 481–494, 2004.
[46] C.-N. Yang and T.-S. Chen, "Size-adjustable visual secret sharing schemes," *IEICE Trans. Fundam. Electron., Commun. Comput. Sci.*, vol. E88-A, no. 9, pp. 2471–2474, Sep. 2005.
[47] C.-N. Yang and T.-S. Chen, "Aspect ratio invariant visual secret sharing schemes with minimum pixel expansion," *Pattern Recognit. Lett.*, vol. 26, no. 2, pp. 193–206, Jan. 2005.
[48] C.-N. Yang and C.-S. Laih, "New colored visual secret sharing schemes," *Des., Codes, Cryptogr.*, vol. 20, no. 3, pp. 325–335, Jul. 2000.

Roberto De Prisco is an Associate Professor of Computer Science with the University of Salerno, Italy. He received the M.Sc. and Ph.D. degrees in computer science from the Massachusetts Institute of Technology, USA, in 1997 and 2000, respectively, and the Diploma of Pianoforte degree from the Music Conservatory of Salerno in 2007. From 1999 to 2001, he has been a Research Scientist with Akamai Technologies. His current research interests include algorithms, distributed systems, networks, cryptography and security, data compression, and computer music

Alfredo De Santis is a Professor of Computer Science with the University of Salerno, Italy. From 1991 to 1995 and from 1998 to 2001, he was the Director with the Dipartimento di Informatica ed Applicazioni, University of Salerno. Since 2013, he has been an Associate Editor of the IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY. His current research interests include algorithms, data security, digital forensics, cryptography, communication networks, information theory, and data compression.