9

SECRET SHARING AND VISUAL CRYPTOGRAPHY SCHEMES

A Randomness Preserving Transformation

Annalisa De Bonis and Alfredo De Santis

Dipartimento di Informatica ed Applicazioni
Università di Salerno, 84081 Baronissi (SA), Italy
{debonis,ads}@dia.unisa.it

Abstract A secret sharing scheme is a method for sharing a secret among a set P of n participants. The secret is encoded into n pieces called shares each of which is given to a distinct participant. Certain *qualified* subsets of participants can recover the secret by pooling together their information, whereas *forbidden* subsets of participants have no information on the secret. The specification of the qualified sets and the forbidden sets is called *access structure.*

A special kind of secret sharing schemes are visual cryptography schemes (VCSs), that is, schemes where the secret to share is an image and the shares consist of xeroxed transparencies which are stacked to recover the shared image.

In this paper we analyze the relationship between secret sharing schemes and VCSs, focusing our attention on the amount of randomness required to generate the shares. We show how to transform a secret sharing scheme for a given access structure into a VCS for the same access structure while preserving the randomness of the original scheme. An important consequence of this transformation is that lower bounds on the randomness of visual cryptography schemes apply to general secret sharing schemes. Our randomness preserving transformation has also been applied to derive a new upper bound on the randomness of (k, n)-threshold VCSs which dramatically improves on the previously known bounds. All VCSs obtained by applying our randomness preserving transformation allow a perfect reconstruction of black pixels.

Keywords: Cryptography, Randomness, Secret Sharing, Visual Cryptography.

Introduction

A secret sharing scheme is a method for sharing a secret among a set P of n participants. The secret is encoded into n pieces called shares each of

which is given to a distinct participant. Certain *qualified* subsets of participants can recover the secret by pooling together their information, whereas *forbidden* subsets of participants have no information on the secret. The specification of all qualified and forbidden subsets of participants constitutes an *access structure.*

Secret sharing schemes are especially useful in situations which require that several people cooperate in order to start an important action such as opening a bank vault or a safety deposit box, or launching a missile.

Shamir [14] and Blakley [5] have been the first to introduce secret sharing schemes. In particular, they considered (k, n)-threshold schemes, that is scheme where only subsets of P of size larger than or equal to a fixed integer k can reconstruct the secret. Ito, Saito, and Nishizeki [11] showed how to realize a secret sharing scheme for any access structure. Later, Benaloh and Leichter [4] proposed a simpler and more efficient way to realize secret sharing schemes. Other general techniques handling arbitrary access structures can be found in [12, 17].

An important issue in the implementation of secret sharing schemes is the amount of randomness required for generating the shares. Blundo *et al.* [7] have been the first to analyze the randomness of secret sharing schemes. Random bits are a natural computational resource which must be taken into account when designing cryptographic algorithms. Considerable effort has been devoted to reduce the number of bits used by probabilistic algorithms (see for example [10]) and to analyze the amount of randomness required in order to achieve a given performance. Motivated by the fact that "truly" random bits are hard to generate, it has also been investigated the possibility of using imperfect source of randomness in randomized algorithms [19]. In spite of the considerable effort devoted to analyzing the incidence of randomness in several areas of computer science, very few results have been obtained to quantify the amount of random bits required to solve classes of problems.

A special kind of secret sharing schemes are *visual cryptography schemes.* A visual cryptography scheme (VCS) is a method to secretly share an image among a given group of participants. A VCS for a set P of n participants encodes a secret image into n shadow images which constitute the shares given to the n participants. The shares given to participants in $X \subseteq P$ are xeroxed onto transparencies. If X is *qualified* then the participants in X can visually recover the secret image by stacking their transparencies without any cryptography knowledge and without performing any cryptographic computation.

In this paper we analyze the relationship between secret sharing schemes and visual cryptography schemes, with a special concern for the amount of randomness required to generate the shares. In this paper we only consider VCSs for black and white images. Visual cryptography schemes for black and white images have been defined by Naor and Shamir in [13]. They analyzed (k, n)-threshold visual cryptography schemes. Ateniese *at al.* [1,2] extended

the model by Naor and Shamir to general access structures. Since in a VCS an image is encoded pixel by pixel, then a VCS for black and white images is a special case of secret sharing scheme for a set of secrets of size two. We refer to such a secret sharing scheme with the term of *Binary Secret Sharing Scheme* (BSS). It follows that lower bounds on the randomness of BSSs apply also to VCSs. In this paper we prove that the converse implication holds as well, thus shading a new light on the study of secret sharing schemes. In other words, we prove that the number of random bits needed to secretly share a pixel is the same as that needed to share any secret chosen in a set of size two. Indeed, given a BSS Σ for an access structure Γ, we show how to construct a VCS for Γ with the same randomness as Σ. Such construction technique will be also applied to derive a new upper bound on the randomness of (k, n)-threshold VCSs. This upper bound dramatically improves on all previously known upper bounds and it is very close to the best known lower bound [9].

1. THE MODEL

Let $P = \{1, \ldots, n\}$ be a set of elements called *participants,* and let 2^P denote the set of all subsets of P. Let $\Gamma_{\mathrm{Qual}} \subseteq 2^P$ and $\Gamma_{\mathrm{Forb}} \subseteq 2^P$, where $\Gamma_{\mathrm{Qual}} \cap \Gamma_{\mathrm{Forb}} = \emptyset$. We refer to members Γ_{Qual} as *qualified sets* and we call members of Γ_{Forb} *forbidden sets.* The pair $\Gamma = (\Gamma_{\mathrm{Qual}}, \Gamma_{\mathrm{Forb}})$ is called the *access structure* of the scheme.

Let Γ_0 consist of all the minimal qualified sets:

$$\Gamma_0 = \{A \in \Gamma_{\mathrm{Qual}} : A' \notin \Gamma_{\mathrm{Qual}} \text{ for all } A' \subset A\}.$$

A participant $p \in P$ is an *essential* participant if there exists a set $X \subseteq P$ such that $X \cup \{p\} \in \Gamma_{\mathrm{Qual}}$ but $X \notin \Gamma_{\mathrm{Qual}}$. A non-essential participant does not need to participate "actively" in the reconstruction of the secret, since the information she has is not needed by any set in P in order to recover the shared image. In any secret sharing scheme having non-essential participants, these participants do not require any information in their shares.

In the case where Γ_{Qual} is monotone increasing, Γ_{Forb} is monotone decreasing, and $\Gamma_{\mathrm{Qual}} \cup \Gamma_{\mathrm{Forb}} = 2^P$, the access structure is said to be *strong,* and Γ_0 is termed a *basis.* In a strong access structure,

$$\Gamma_{\mathrm{Qual}} = \{C \subseteq \mathcal{P} : B \subseteq C \text{ for some } B \in \Gamma_0\},$$

and we say that Γ_{Qual} is the *closure* of Γ_0.

In the following we formally define secret sharing schemes for a strong access structure $(\Gamma_{\mathrm{Qual}}, \Gamma_{\mathrm{Forb}})$. Indeed, in traditional secret sharing schemes the access structures are always assumed to be strong.

A secret sharing scheme Σ for a set of secrets $S = \{s_0, \ldots, s_{h-1}\}$ on a set P of participants for the strong access structure $(\Gamma_{\mathrm{Qual}}, \Gamma_{\mathrm{Forb}})$ is a method to

secretly share a secret chosen in S among the members of P in such a way that only subsets of participants which are in Γ_{Qual} can recover the secret. The secret sharing scheme Σ consists of h collections of *distribution functions* $C_0, \ldots, C_{h-1}$. A *distribution function* $f \in C_i$, $i = 0, \ldots, h-1$, is a function which associates to each participant $p \in P$ a share. When the secret to share is s_i, $i = 0, \ldots, h-1$, the dealer randomly chooses a distribution function $f \in C_i$ and assigns to each $p \in P$ the share $f(p)$.

Definition 1 *Let* $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}})$ *be a strong access structure on a set P of participants. The collections of distribution functions* $C_0, \ldots, C_{h-1}$ *realize a secret sharing scheme for a set of secrets of size h if the following conditions hold:*

1. Any subset $X \subseteq P$ of participants qualified to recover the secret can compute the secret.
   Formally, if $X \in \Gamma_{\mathsf{Qual}}$, *then it is* $\{(p, f(p))\}_{p \in X} \neq \{(p, g(p))\}_{p \in X}$, *for all* $f \in C_i$ *and* $g \in C_j$ *with* $i, j \in \{0, \ldots, h-1\}$ *and* $i \neq j$.

2. Any subset $X \subseteq P$ of participants non-qualified to recover the secret has no information on the secret value.
   Formally, if $X = \{p_{v1}, \ldots, p_{va}\} \in \Gamma_{\mathsf{Forb}}$, *then for any possible choice* $sh_{v1} \ldots, sh_{va}$ *of the shares given to participants* $p_{v1}, \ldots, p_{va}$, *it results*
   $$\frac{|\{f \in C_i : (f(p_{v_1}) \ldots, f(p_{v_a})) = (sh_{v_1}, \ldots, sh_{v_a})\}|}{|C_i|} = \frac{|\{f \in C_j : (f(p_{v_1}) \ldots, f(p_{v_a})) = (sh_{v_1}, \ldots, sh_{v_a})\}|}{|C_j|},$$
   for any $i, j \in \{0, \ldots, h-1\}$.

The first property is related to the reconstruction of the secret. It states that the for any pair of distinct secrets s_i and s_j, the group of shares assigned to a qualified group of participants when the encoded secret is s_i is different from that assigned to the same group of participants when the encoded secret is s_j.

The second property is called *security*, since it implies that, even by inspecting all their shares, a forbidden set of participants cannot gain any information on the shared secret.

Notice that in the previous definition C_i, $i = 0, \ldots, h-1$, is a multiset of distribution functions, therefore we allow a function to appear more than once in C_i, $i = 0, \ldots, h-1$. Moreover, the sizes of the collections $C_0, \ldots, C_{h-1}$ do not need to be the same.

The *randomness* of a secret sharing scheme represents the number of random bits used by the dealer to share a secret among the participants. Let Σ be a secret sharing scheme for a set of h secrets $s_0, \ldots, s_{h-1}$ realized by the collections $C_0, \ldots, C_{h-1}$. For $i = 0, \ldots, h-1$, let p_i denote the probability that the shared secret is s_i. The randomness of Σ has been defined by Blundo *et al.* [7] as

$$\mathcal{R}^{(C_0, \ldots, C_{h-1}), \mathbf{p}} = \sum_{i=0}^{h-1} \mathrm{p}_i \log |C_i|,$$

where $\mathbf{p} = (p_0, ..., p_{h-1})$. Let $\Gamma = (\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}})$ be a given access structure. In accordance with [7], the dealer's randomness for the access structure Γ is defined as

$$\mathcal{R}_\Gamma = \inf_{\mathcal{A},\mathcal{I}} \mathcal{R}^{(\mathcal{C}_0,\ldots,\mathcal{C}_{h-1}),\mathbf{p}},$$

where A denotes the set of all h-tuple of collections $C_0, \ldots, C_{h-1}$ realizing a secret sharing scheme for Γ for the set of secrets $\{s_0, \ldots, s_{h-1}\}$, and I is the set of all probability vectors of length h with non-zero entries. Indeed, we assume that the secret have non-zero probability of being any of $s_0, \ldots, s_{h-1}$. In [7] the above definition has been proved to be equivalent to the following

$$\mathcal{R}_\Gamma = \min_{\mathcal{A}} \log(\min\{|\mathcal{C}_0|, \ldots, |\mathcal{C}_{h-1}|\}).$$

The above definition implies that, given h function collections $C_0, \ldots, C_{h-1}$ realizing a secret sharing scheme for a set of h secrets for the access structure Γ, we are mainly concerned with the quantity $\log(\min\{|C_0|, \ldots, |C_{h-1}|\})$. Hence, we define the randomness $R(C_0, ..., C_{h-1})$ of a secret sharing scheme for a set of h secrets realized by $C_0, \ldots, C_{h-1}$ as

$$\mathcal{R}(\mathcal{C}_0, \ldots, \mathcal{C}_{h-1}) = \log(\min\{|\mathcal{C}_0|, \ldots, |\mathcal{C}_{h-1}|\}). \tag{1}$$

1.1. VISUAL CRYPTOGRAPHY SCHEMES

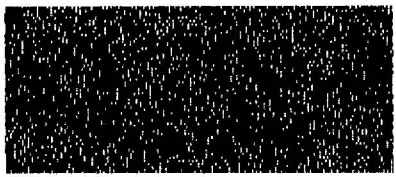
We assume that the image to be encoded consists of a collection of black and white pixels. The image is encoded pixel by pixel. A pixel is encoded into n pixels which constitute the shares for the n participants associated with that pixel. For each participant the shares associated with the pixels of the whole secret image are xeroxed onto a transparency which constitutes the share assigned to that participant. The participants of a qualified set can visually recover the secret image by stacking their transparencies.

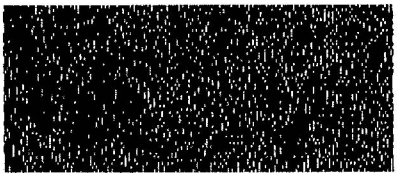
As an example, consider the image representing the acronym "SEC2001".

SEC2001

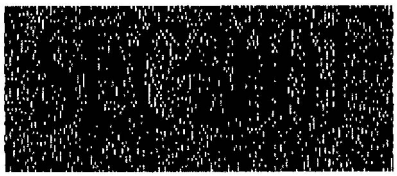
The two shares generated by a (2, 2)-threshold VCS are given below.

Share of participant 1 Share of participant 2





The following is the image obtained by stacking the shares of both participants



Each of the n shares associated with a single pixel is a collection of m black and white subpixels. The resulting structure can be described by an $n \times m$ boolean matrix $S = [s_{ij}]$ where $s_{ij} = 1$ iff the j-th subpixel in the i-th transparency is black. Therefore the grey level of the combined shares, obtained by stacking the transparencies $i_1, \ldots, i_s$ is proportional to the Hamming weight $w(V)$ of the m-entry vector $V = OR(R_{i_1}, \ldots, R_{i_s})$, where $R_{i_1}, \ldots, R_{i_s}$ are the rows of S associated with the transparencies we stack. This grey level is interpreted by the visual system of the users as black or as white according with some rule of contrast.

Definition 2 *Let* $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}})$ *be an access structure on a set of n participants. Two collections (multisets) of* $n \times m$ *boolean matrices* $\hat{\mathcal{C}}_0$ *and* $\hat{\mathcal{C}}_1$ *constitute a* visual cryptography scheme $(\Gamma_{\mathsf{Qual}}, \Gamma_{\mathsf{Forb}})$-VCS *if there exist a value* $\alpha(m)$ *and a collection* $\{(X, t_X)\}_{X \in \Gamma_{\mathsf{Qual}}}$ *satisfying:*

1 Any (qualified) set $X = \{i_1, i_2, \ldots, i_p\} \in \Gamma_{\mathsf{Qual}}$ can recover the shared image by stacking their transparencies.
Formally, for any $M \in \hat{\mathcal{C}}_0$, *the "or" V of rows* $i_1, i_2, \ldots, i_p$ *satisfies* $w(V) \leq t_X - \alpha(m) \cdot m$; *whereas, for any* $M \in \hat{\mathcal{C}}_1$ *it results that* $w(V) \geq t_X$.

2 Any (forbidden) set $X = \{i_1, i_2, \ldots, i_p\} \in \Gamma_{\mathsf{Forb}}$ has no information on the shared image.
Formally, the two collections of $p \times m$ *matrices obtained by restricting the* $n \times m$ *matrices of* $\hat{\mathcal{C}}_0$ *and* $\hat{\mathcal{C}}_1$ *to rows* $i_1, i_2, \ldots, i_p$ *are indistinguishable, in the sense that they contain the same matrices with the same frequencies.*

Each pixel of the original image will be encoded into n pixels, each of which consists of m subpixels. To share a white (black, resp.) pixel, the dealer randomly chooses one of the matrices in $\hat{C}_0$ ($\hat{C}_1$ resp.) and distributes row i to participant i.

The first property of Definition 2 is related to the contrast of the image. It states that when a qualified set of users stack their transparencies they can correctly recover the shared image. Observe that this property implies Property 1. of Definition 1. The value $\alpha(m)$ is called *relative difference,* the number $\alpha(m) \cdot m$ is referred to as the *contrast* of the image, the set $\{(X, t_X)\}_{X \in \Gamma_{\text{Qual}}}$ is called the *set of thresholds,* and t_X is the threshold associated to $X \in \Gamma_{\text{Qual}}$. We want the contrast to be as large as possible and at least one, that is, $\alpha(m) \geq 1/m$. The second property, as well as Property 2. of Defination 1, is related to the security of the scheme.

The model of visual cryptography we consider is the same as that described in [1,2]. This model is a generalization of the one proposed in [13], since with each set $X \in \Gamma_{\text{Qual}}$ we associate a (possibly) different threshold t_X. Further, the access structure is not required to be strong in our model.

Notice that if a set of participants X is a superset of a qualified set X', then they can recover the shared image by considering only the shares of the set X'. This does not in itself rule out the possibility that stacking all the transparencies of the participants in X does not reveal any information about the shared image.

In accordance with definition (1), the randomness $R(\hat{C}_0, \hat{C}_1)$ of a visual cryptography scheme realized by $\hat{C}_0$ and $\hat{C}_1$ is given by

$$\mathcal{R}(\hat{C}_0, \hat{C}_1) = \log(\min\{|\hat{C}_0|, |\hat{C}_1|\}).$$

The randomness of a VCS represents the number of random bits per pixel required by the VCS to share a secret image.

2. A RANDOMNESS PRESERVING TRANSFORMATION FROM BSSs TO VCSs

In this section we will show how to transform a BSS for a strong access structure Γ into a VCS for Γ with the same randomness as the original BSS.

Let $C_0 = \{f_1^0, \ldots, f_{c_0}^0\}$ and $C_1 = \{f_1^1, \ldots, f_{c_1}^1\}$ be two function collections realizing a BSS for an access structure on the set of participants $P = \{1, \ldots, n)$. Two tables, T_0 and T_1, will be used to represent the shares assigned to each participant by the distribution functions of C_0 and C_1. For any $b \in \{0, 1\}$, $i = 1, \ldots, n$ and $j = 1, \ldots, c_b$, it is $T_b[i, j] = f_j^b(i)$. A share will be symbolically represented by a literal indexed with the associated participant. For a given participant $i \in (1, \ldots, n\}$, distinct literals indexed with i denote distinct shares. Notice that Property 1. of Definition 1 implies that if we restrict T_0 and T_1 to

the rows corresponding to a set $X \in \Gamma_{\text{Qual}}$, we obtain two tables having no common column. Moreover, Property 2. of Definition 1 implies that if we restrict T_0 and T_1 to the rows corresponding to a set $X \in \Gamma_{\text{Forb}}$, we obtain two tables whose multisets of columns are indistinguishable, in the sense that they contain the same columns with the same frequencies.

The following example illustrates the randomness preserving transformation. For any n-row matrix M and any set $X \subseteq \{1, \ldots, n\}$, we will denote with $M[X]$ the matrix obtained by restricting M to the rows with indices in X. The rows appear in $M[X]$ in the same order they appear in M.

The initial BSS

Let us consider the strong access structure Γ on the set of participants $\{1, 2, 3, 4\}$ with basis $\Gamma_0 = \{\{1, 3, 4\}, \{1, 2\}, \{2, 3\}, \{2, 4\}\}$. Let us assume that $C_0 = \{f_1^0, f_2^0, f_3^0, f_4^0\}$ and $C_1 = \{f_1^1, f_2^1, f_3^1, f_4^1\}$ be two collections af distribution functions realizing a BSS for Γ and that the shares assigned to each participant by the distribution functions of C_0 and C_1 be given by the following two tables

$T_0 =$

	f_1^0	f_2^0	f_3^0	f_4^0
1	x_1	x_1	y_1	y_1
2	x_2	y_2	z_2	w_2
3	x_3	y_3	x_3	y_3
4	x_4	y_4	y_4	x_4

$T_1 =$

	f_1^1	f_2^1	f_3^1	f_4^1
1	x_1	y_1	y_1	x_1
2	w_2	x_2	y_2	z_2
3	x_3	y_3	x_3	y_3
4	y_4	y_4	x_4	x_4

Construction of the Matrix collections $\hat{C}_0$ and $\hat{C}_1$

We associate to each function $f_j^b, j = 1, 2, 3, 4$ and $b \in \{0, 1\}$, a 4×4 matrix M_j^b. For $j = 1, 2, 3, 4$, and $b = 0, 1$, we construct the matrix M_j^b as follows. For any $i = 1, 2, 3, 4$ and $l = 1, 2, 3, 4$, we set the i-th entry of the l-th column of M_j^b equal to

$$M_j^b[i, \ell] = \begin{cases} 0 & \text{if } f_j^b(i) = f_\ell^0(i), \\ 1 & \text{otherwise.} \end{cases}$$

The matrices resulting from the above construction for our running example are:

$$M_1^0 = \begin{bmatrix} 0011 \\ 0111 \\ 0101 \\ 0110 \end{bmatrix} \quad M_2^0 = \begin{bmatrix} 0011 \\ 1011 \\ 1010 \\ 1001 \end{bmatrix} \quad M_3^0 = \begin{bmatrix} 1100 \\ 1101 \\ 0101 \\ 1001 \end{bmatrix} \quad M_4^0 = \begin{bmatrix} 1100 \\ 1110 \\ 1010 \\ 0110 \end{bmatrix}$$

$$M_1^1 = \begin{bmatrix} 0011 \\ 1110 \\ 0101 \\ 1001 \end{bmatrix} \quad M_2^1 = \begin{bmatrix} 1100 \\ 0111 \\ 1010 \\ 1001 \end{bmatrix} \quad M_3^1 = \begin{bmatrix} 1100 \\ 1011 \\ 0101 \\ 0110 \end{bmatrix} \quad M_4^1 = \begin{bmatrix} 0011 \\ 1101 \\ 1010 \\ 0110 \end{bmatrix}$$

The reader can quickly verify by a simple inspection of the collections $\{M_1^0, M_2^0, M_3^0, M_4^0\}$ and $\{M_1^1, M_2^1, M_3^1, M_4^1\}$ that the above construction yields a VCS for the access structure $(\Gamma_{\text{Qual}}, \Gamma_{\text{Forb}})$.

In the following we describe an algorithm which transforms an arbitrary BSS for a given access structure into a VCS for the same access structure. Let $C_0 = \{f_1^0, \ldots, f_{c0}^0\}$ and $C_1 = \{f_1^1, \ldots, f_{c1}^1\}$ be two collections of distribution functions realizing a BSS for a given strong access structure Γ. The input of the algorithm consists of the two tables T_0 and T_1 representing the shares assigned to each participant by the distribution functions of C_0 and C_1.

Generate-VCS(T_0, T_1)
  $n \leftarrow$ number of rows of T_0
  $c_0 \leftarrow$ number of columns of T_0
  $c_1 \leftarrow$ number of columns of T_1
    for $b \leftarrow 0$ **to** 1
      for $j \leftarrow 1$ **to** c_b
        for $i \leftarrow 1$ **to** n
          for $l \leftarrow 1$ **to** c_0
            if $f_j^b(i) = f_l^0(i)$
              then $M_j^b[i, l] \leftarrow 0$
              else $M_j^b[i, l] \leftarrow 1$
  output$(\{M_1^0, \ldots, M_{c_0}^0\}, \{M_1^1, \ldots, M_{c_1}^1\})$

Figure 1 A randomness preserving transformation from a BSS to a VCS

The proof of the following theorem, which has been omitted due to space constraints, can be found in the journal version of the present paper.

Theorem 3 *Let* $C_0 = \{f_1, \ldots, f_{c0}\}$ *and* $C_1 = \{f_1, \ldots, f_{c1}\}$ *realize a BSS for a sting access structure* Γ *on the set of n participants* $P = \{1, \ldots, n\}$. *The algorithm described in Figure 1 generates a VCS on P for* Γ *with pixel expansion equal to* $|C_0| = c_0$, *contrast equal to one, and having the same randomness as the original BSS.*

Notice that by replacing each matrix M in the VCS of Theorem 3 with the matrix obtained by concatenating h copies of M, we obtain a VCS with contrast h and pixel expansion $h \cdot |C_0|$.

2.1. LOWER BOUNDS ON THE RANDOMNESS OF SECRET SHARING SCHEMES

Since visual cryptography schemes are a particular kind of binary secret sharing schemes, then any lower bound on the randomness of BSSs for a given access structure Γ is a lower bound on the randomness of any VCS for the

same access structure. Theorem 3 shows that the reverse implication holds as well, that is, any lower bound on the randomness of VCSs for the strong access structure Γ is also a lower bound on the randomness of any BSS for Γ. It follows that the techniques introduced in [8, 9] to derive lower bounds on the randomness of VCSs apply also to BSSs and consequently to secret sharing schemes for any set of secrets. In particular, the following lower bound [9] on the randomness of (k, n)-threshold VCS extends to any (k, n)-threshold secret sharing scheme:

$$(k-1)\log(n-k+2). \tag{2}$$

In [7] it has been proved that a (k, n)-threshold secret sharing scheme for a set of s secrets has randomness at least $(k-1)\log s$. For set of secrets of size $s > n$, Shamir [14] has provided a scheme which achieves this bound. Then, one has that the following theorem holds.

Theorem 4 *For $n \geq k \geq 2$, the randomness of any (k, n)-threshold secret sharing scheme for a set of s secrets is at least $(k-1)\max\{\log s, \log(n-k+2)\}$.*

2.2. VCSs WITH PERFECT RECONSTRUCTION OF BLACK PIXELS

An important property of the VCSs obtained by applying the transformation of Figure 1 is that for any $X = \{i_1, i_2, \ldots, i_p\} \in \Gamma_{\mathrm{Qual}}$ and any $M \in \hat{\mathcal{C}}_1$, the "or" V of rows $i_1, i_2, \ldots, i_p$ consists of an all-one vector. VCSs with this property generate high quality images since they allow a perfect reconstruction of black pixels (see [6] for bounds on the pixel expansion of such VCSs). Given any VCS for the strong access structure Γ, we can construct a VCS with perfect reconstruction of black pixels for the same access structure as follows. We construct the distribution function collections C_0 and C_1 corresponding to the given VCS. Then, we apply the transformation of Figure 1 to obtain a VCS for Γ with perfect reconstruction of black pixels. By replacing each matrix $M \in \hat{\mathcal{C}}_0 \cup \hat{\mathcal{C}}_1$ with the matrix obtained by concatenating h copies of M, we obtain two matrix collections realizing a VCS with contrast h and with perfect reconstruction of black pixels. Hence, one has that the following theorem holds.

Theorem 5 *Let $\hat{\mathcal{C}}_0$ and $\hat{\mathcal{C}}_1$ be two matrix collections realizing a VCS for the strong access structure Γ. Then, for any arbitrary $h \geq 1$, there exists a VCS for Γ with perfect reconstruction of black pixels, having pixel expansion equal to $h \cdot |\hat{\mathcal{C}}_0|$, contrast equal to h, and the same randomness as the original VCS.*

The following example illustrates the above theorem.

Example 6 *Let us consider the strong access structure Γ on the set of participants $\{1,2,3,4\}$ with basis $\Gamma_0 = \{\{1, 2\}, \{1, 3\}, \{2, 3\}, \{2, 4\}, \{3, 4\}\}$. The following matrix collections realize a VCS for Γ.*

$$\hat{C}_0 = \left\{ \begin{bmatrix} 10000 \\ 10001 \\ 10001 \\ 00001 \end{bmatrix}, \begin{bmatrix} 01000 \\ 01001 \\ 01001 \\ 00001 \end{bmatrix}, \begin{bmatrix} 00100 \\ 00101 \\ 00101 \\ 00001 \end{bmatrix}, \begin{bmatrix} 10000 \\ 10010 \\ 10010 \\ 00010 \end{bmatrix}, \begin{bmatrix} 01000 \\ 01010 \\ 01010 \\ 00010 \end{bmatrix}, \begin{bmatrix} 00100 \\ 00110 \\ 00110 \\ 00010 \end{bmatrix} \right\}$$

$$\hat{C}_1 = \left\{ \begin{bmatrix} 10000 \\ 01001 \\ 00101 \\ 00010 \end{bmatrix}, \begin{bmatrix} 01000 \\ 00101 \\ 10001 \\ 00010 \end{bmatrix}, \begin{bmatrix} 00100 \\ 10001 \\ 01001 \\ 00010 \end{bmatrix}, \begin{bmatrix} 10000 \\ 01010 \\ 00110 \\ 00001 \end{bmatrix}, \begin{bmatrix} 01000 \\ 00110 \\ 10010 \\ 00001 \end{bmatrix}, \begin{bmatrix} 00100 \\ 10010 \\ 01010 \\ 00001 \end{bmatrix} \right\}$$

The distribution function collections associated with this VCS are represented by the following two tables. For i = 1,2,3,4, *the shares for participant i are denoted by a literal indexed with i. For a fixed index i, distinct literals indicates distinct shares.*

$T_0 =$

	f_1^0	f_2^0	f_3^0	f_4^0	f_5^0	f_6^0
1	u_1	v_1	x_1	u_1	v_1	x_1
2	u_2	v_2	x_2	y_2	z_2	w_2
3	u_3	v_3	x_3	y_3	z_3	w_3
4	u_4	u_4	u_4	v_4	v_4	v_4

$T_1 =$

	f_1^1	f_2^1	f_3^1	f_4^1	f_5^1	f_6^1
1	u_1	v_1	x_1	u_1	v_1	x_1
2	v_2	x_2	u_2	z_2	w_2	y_2
3	x_3	u_3	v_3	w_3	y_3	z_3
4	v_4	v_4	v_4	u_4	u_4	u_4

Now we apply the randomness preserving transformation of Figure 1 to obtain a VCS for Γ *with perfect reconstruction of the black pixels.*

$$\hat{C}_0 = \left\{ \begin{bmatrix} 011011 \\ 011111 \\ 011111 \\ 000111 \end{bmatrix}, \begin{bmatrix} 101101 \\ 101111 \\ 101111 \\ 000111 \end{bmatrix}, \begin{bmatrix} 110110 \\ 110111 \\ 110111 \\ 000111 \end{bmatrix}, \begin{bmatrix} 011011 \\ 111011 \\ 111011 \\ 111000 \end{bmatrix}, \begin{bmatrix} 101101 \\ 111101 \\ 111101 \\ 111000 \end{bmatrix}, \begin{bmatrix} 110110 \\ 111110 \\ 111110 \\ 111000 \end{bmatrix} \right\}$$

$$\hat{C}_1 = \left\{ \begin{bmatrix} 011011 \\ 101111 \\ 110111 \\ 111000 \end{bmatrix}, \begin{bmatrix} 101101 \\ 110111 \\ 011111 \\ 111000 \end{bmatrix}, \begin{bmatrix} 110110 \\ 011111 \\ 101111 \\ 111000 \end{bmatrix}, \begin{bmatrix} 011011 \\ 111101 \\ 111110 \\ 000111 \end{bmatrix}, \begin{bmatrix} 101101 \\ 111110 \\ 111011 \\ 000111 \end{bmatrix}, \begin{bmatrix} 110110 \\ 111011 \\ 111101 \\ 000111 \end{bmatrix} \right\}$$

By concatenating h copies of each matrix in the above collections $\hat{C}_0$ *and* $\hat{C}_1$ *we obtain a VCS with contrast h.* Δ

3. A NEW UPPER BOUND ON THE RANDOMNESS OF (*k*, *n*)-THRESHOLD VCSs

In this section we provide a construction for (*k*, *n*)-threshold VCSs which improves on the randomness of all previously known VCSs and is very close to lower bound (2). The idea of the construction consists of applying Theorem 3 to Shamir's (*k*, *n*)-threshold secret sharing scheme [14]. Shamir's scheme shares a secret *s*, uniformly chosen in $GF(2^r)$, among a set of $n < 2^r$ participants. To share a secret *s*, the dealer uniformly and independently chooses $k-1$ elements $a_1, a_2, \ldots, a_{k-1}$ in $GF(2^r)$ and then constructs the polynomial $p(x) = s + a_1x + a_2x^2 + \ldots + a_{k-1}x^{k-1}$. The share assigned to participant *i* is $p(i)$. It is easy to see that if at least *k* participants join together then they can interpolate the polynomial $p(x)$ and calculate the secret $s = f(0)$, whereas any set of less than *k* participants has no information on the secret. The dealer uses

$(k-1)r$ random bits to choose the coefficients $a_1, a_2, \ldots, a_{k-1}$. The collection of distribution functions associated to a secret $s \in GF(2^r)$ is $C_s = \{p(x) = s + a_1x + a_2x^2 + \ldots + a_{k-1}x^{k-1} : a_i \in GF(2^r),\ i = 1, \ldots, k-1\}$.

Given a Shamir's secret sharing scheme to share a secret $s \in GF(2^r)$ among a set of n participants, with $n < 2^r$, we can obtain a (k,n)-threshold BSS $\sum$ as follows. Below, we will assume w.l.o.g. that the binary secret be chosen in $\{0, 1\}$. We assume that all secrets in $GF(2^r) \setminus \{0, 1\}$ be chosen with probability 0 and that the secrets 0 and 1 occur with probability $\frac{1}{2}$ each. To share a secret $s \in \{0, 1\}$, the dealer uniformly chooses a polynomial $p(x)$ in $C_s = \{p(x) = s + a_1x + a_2x^2 + \ldots + a_{k-1}x^{k-1} : a_i \in GF(2^r),\ i = 1, \ldots, k-1\}$ and for $i = 1, \ldots, n$, distributes to participant i the share $p(i)$. By applying the randomness preserving transformation of Figure 1 to $\sum$ we obtain a VCS with randomness $(k-1)r$. We can increase the contrast of the resulting VCS by replacing each matrix with h concatenated copies of that matrix. Since it must be $2^r > n$, then r can be as small as $\lceil \log(n+1) \rceil$. Hence, the following theorem holds.

Theorem 7 *For any $n \geq k \geq 2$ and $h \geq 1$, there exists a (k,n)-threshold VCS with pixel expansion $h \cdot 2^{(k-1)\lceil \log(n+1) \rceil}$, contrast h, and randomness $(k-1)\lceil \log(n+1) \rceil$.*

Table 1 summarizes some known upper bounds on the randomness of (k, n)-threshold VCSs. Notice that the bound of Theorem 7 greatly improves on all other bounds. Indeed, all other bounds, except that of Corollary 2 of [9] which holds only for constant values of the threshold k, are exponential in k. Moreover, the upper bound of Theorem 7 is very close to lower bound (2).

Naor *et al.* [13]	$n^k \log(2^{k-1}!)$
Ateniese *et al.* [1]	$\log\left((O(k(2e)^k)\log n)!\right)$
Thm. 6 [9]	$\binom{n}{k-1} - 1$
Thm. 9 [9]	$(k-1)\binom{n}{k}$
Cor. 1 [9]	$O(k^2e^k)\log n$
Cor. 2 [9]	$O(k^{2\log^* n}\log n)$, for k constant
Thm. 7	$(k-1)\lceil \log(n+1) \rceil$

Table 1 Upper bounds on the randomness of (k, n)-threshold VCSs.

3.1. MINIMUM RANDOMNESS (*k, k*)-THRESHOLD VCSs

In this section we show how to obtain a minimum randomness (*k, k*)-threshold VCS using the following well known construction for minimum randomness (*k, k*)-threshold BSSs (see for example [16]). To share a secret $s \in \{0, 1\}$ the dealer randomly chooses $k - 1$ random bits $b_1, \ldots, b_{k-1}$ and computes $b_k = s \oplus b_1 \oplus \ldots \oplus b_{k-1}$, where "⊕" denotes the "xor" operator. For $i = 1, \ldots, k$, the share for participant i is b_i. It is easy to see that if k participants join together then they can recover the secret s by calculating the "xor" of their shares, whereas less than k participants have no information on s. The randomness of this BSS is $k - 1$. Hence, by applying the randomness preserving construction we obtain a VCS with pixel expansion 2^{k-1}, contrast 1 and randomness $k - 1$. By concatenating h copies of each matrix in the resulting VCS we obtain a minimum randomness (*k, k*)-threshold VCS with pixel expansion $h \cdot 2^{k-1}$ and contrast h.

The following example shows a (3,3)-threshold VCS obtained by applying the above construction.

Example 8 *A minimum randomness* (3,3)*-threshold VCS with contrast* $h = 1$.

$$\hat{C}_0 = \left\{ \begin{bmatrix} 0011 \\ 0101 \\ 0110 \end{bmatrix}, \begin{bmatrix} 0011 \\ 1010 \\ 1001 \end{bmatrix}, \begin{bmatrix} 1100 \\ 0101 \\ 1001 \end{bmatrix}, \begin{bmatrix} 1100 \\ 1010 \\ 0110 \end{bmatrix} \right\},$$

$$\hat{C}_1 = \left\{ \begin{bmatrix} 0011 \\ 0101 \\ 1001 \end{bmatrix}, \begin{bmatrix} 0011 \\ 1010 \\ 0110 \end{bmatrix}, \begin{bmatrix} 1100 \\ 0101 \\ 0110 \end{bmatrix}, \begin{bmatrix} 1100 \\ 1010 \\ 1001 \end{bmatrix} \right\}.$$

△

It is interesting to notice that the minimum randomness (*k, k*)-threshold VCS obtained in this section is also obtainable by using the construction for minimum randomness (*k, k*)-threshold VCSs provided in [9]. We recall that in [9] it has been shown that any (*k, k*)-threshold VCS with contrast h has pixel expansion larger than or equal to $h \cdot 2^{k-1}$ and that, for any value of the contrast h, our construction is the only one providing a (*k, k*)-threshold VCS with both minimum randomness and pixel expansion $h \cdot 2^{k-1}$.

4. CONCLUSIONS

In this paper we have provided a technique to transform a BSS into a VCS having the same randomness, thus proving that BSSs and VCSs are equivalent with respect to the randomness. Another consequence of our result is that any lower bound on the randomness of VCSs applies also to secret sharing schemes

for any set of secrets. A nice property of the VCSs obtained by applying our randomness preserving transformation is that they allow a perfect reconstruction of black pixels.

Our randomness preserving transformation has also been used to obtain a construction for (k, n)-threshold VCSs whose randomness is significantly smaller than the randomness of all previously known (k, n)-threshold VCSs and is very close to the known lower bound. An interesting open problem would be to further reduce the gap between the lower bound and the upper bound on the randomness of these VCSs.

References

[1] G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson, *Visual Cryptography for General Access Structures. Information and Computation,* **129-2,** 86–106 (1996).

[2] G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson, *Constructions and Bounds for Visual Cryptography. Proc. 23rd International Colloquium on Automata, Languages and Programming,* LNCS **1099,** 416–428 (1996).

[3] A. Beimel and B. Chor, *Universally Ideal Secret Sharing Schemes. IEEE Trans. on Info. Theory.* **40**(3), 786–794 (1994) (Extended abstract in CRYPTO '92).

[4] J. Benaloh and J. Leichter, *Generalized Secret Sharing and Monotone Functions.* Lecture Notes in Computer Science, **403,** 27–35 (1990).

[5] G. R. Blakley, *Safeguarding Cryptographic Keys. AFIPS Conference Proceedings,* **48,** 313–317 (1979).

[6] C. Blundo and A. De Santis, *Visual Cryptography Schemes with Perfect Reconstruction of Black Pixels. Journal for Computers & Graphics,* Special Issue: "Data Security in Image Communication and Network", **22-4,** 449–455 (1998).

[7] C. Blundo, A. De Santis, and U. Vaccaro, *Randomness in Distribution Protocols. Information and Computation,* **131,** 111–139 (1996).

[8] A. De Bonis and A. De Santis, *New Results on the Randomness of Visual Cryptography, Proc. of Workshop on Cryptography and Computational Number Theory, CCNT'99,* Birkhauser, 187–201.

[9] A. De Bonis and A. De Santis, *Randomness in Visual Cryptography. Proc. 17th International Symposium on Theoretical Aspects of Computer Science, STACS 2000,* LNCS **1770,** 626–638 (2000).

[10] R. Impagliazzo and D. Zuckerman, *How to Recycle Random Bits. Proc. 21st Annual ACM Symp. on Theory of Computing,* 248–255 (1989).

[11] M. Ito, A. Saito, and T. Nishizeki, *Secret Sharing Scheme Realizing General Access Structure. Proc. IEEE Global Telecommunications Conf., Globecom 87,* 99–102 (1987).

[12] K. M. Martin, *New Secret Sharing Schemes from Old. J. of Combin. Math. and Combin. Comput.,* **14,** 65–77 (1993).

[13] M. Naor and A. Shamir, *Visual Cryptography. Advances in Cryptology – EUROCRYPT '94,* LNCS **950,** 1–12 (1995).

[14] A. Shamir, *How to Share a Secret. Commun. of the ACM,* **22,** 612–613 (1979).

[15] D. R. Stinson, *An Introduction to Visual Cryptography.* Presented at *Public Key Solutions '97,* Toronto, Canada, April 28–30 (1997). Available as `http://bibd.unl.edu/ stinson/VKS-PKS.ps`.

[16] D. R. Stinson, *Cryptography, Theory and Practice,* 1995, CRC Press, Inc., Boca Raton, Florida.

[17] G. J. Simmons, W. Jackson, and K. Martin, *The Geometry of Shared Secret Schemes.* Bulletin of the ICA, **1**,71–88 (1991).

[18] E. R. Verheul and H. C. A. van Tilborg, *Constructions and Properties of k out of n Visual Secret Sharing Schemes. Designs, Codes, and Cryptography* **11-2,** 179–196 (1997).

[19] D. Zuckerman, *Simulating BPP Using a General Weak Random Source. Proc. 32nd IEEE Symp. on Foundations of Comp. Science,* 79–89 (1991).