Designs, Codes and Cryptography, 27, 207–227, 2002

A New Approach for Visual Cryptography*

WEN-GUEY TZENG† tzeng@cis.nctu.edu.tw
Department of Computer and Information Science, National Chiao Tung University, Hsinchu, Taiwan 30050
Tel.: 886-3-5712121 ext. 56608, Fax: 886-3-5721490

CHI-MING HU
Department of Computer and Information Science, National Chiao Tung University, Hsinchu, Taiwan 30050

Communicated by: P. Wild

Received March 6, 2000; Revised May 10, 2001; Accepted August 14, 2001

Abstract. Visual cryptography is to encrypt a secret image into some shares (transparencies) such that any qualified subset of the shares can recover the secret "visually." The conventional definition requires that the revealed secret images are always darker than the backgrounds. We observed that this is not necessary, in particular, for the textual images.

In this paper, we proposed an improved definition for visual cryptography based on our observation, in which the revealed images may be darker or lighter than the backgrounds. We studied properties and obtained bounds for visual cryptography schemes based on the new definition. We proposed methods to construct visual cryptography schemes based on the new definition. The experiments showed that visual cryptography schemes based on our definition indeed have better pixel expansion in average.

Keywords: visual cryptography, secret sharing, access structure

1. Introduction

Due to fantastic development of computers, powerful cryptographic algorithms and protocols are designed to meet security requirements of various applications. However, almost all of those need computing power of computers. In some situations it may not be possible or necessary to use computers, for example, a security guard checks the security badge of a personnel. Obviously, the security guard uses his visual system to authenticate the badge. We can see that the human visual system is one of the most convenient tools to decrypt the information. Therefore, Naor and Shamir [13] invents the visual cryptography in which a written material (secret image) is encrypted in a perfectly secure way such that the human visual system can easily decrypt the image with some special arrangement.

*Research supported in part by the Ministry of Education grant 89-E-FA04-1-4, Taiwan, ROC.
†Corresponding author.

In visual cryptography, a dealer encodes the secret image into n special transparencies (shares) and gives each participant a transparency. Each transparency reveals absolutely no information about the secret image. Nevertheless, a qualified set of participants can decode the image by stacking their transparencies together so that the darker secret image appears and the participants read it directly. On the other hand, a forbidden set of participants can not get any information about the secret image from their transparencies even with infinite computing power.

There are quite many new results and extensions of the original work [1–8,12,14,17]. All those work use the definition of Naor and Shamir, i.e., when recovered, the secret image is darker than the background. However, in many situations, what the human visual system cares about is "contrast," no matter whether the image is darker or lighter than the background. For example, we can get the textual secret image "5" from either ⑤ or ❺. Therefore, we give a new definition for visual cryptography based on the above observation. With this new definition, we propose various visual cryptographic schemes. Our schemes have better pixel expansion than previous results in some cases. In this paper, we obtain the following results:

- We propose an improved definition for visual cryptography.
- We study properties and obtain bounds for visual cryptography schemes based on the new definition.
- We propose methods to construct visual cryptography schemes based on the new definition. The experiment results show that our constructions provide better pixel expansion in average.

1.1. Previous Work

Naor and Shamir [13] defined visual cryptography formally and proposed an optimal visual cryptography scheme for the (n, n)-threshold access structure. They also extended the work for the (k, n)-threshold access structures. More results along this line with higher contrast were proposed in [2,4–7,18]. Hofmeister et al. [7] proposed a visual cryptography scheme for (k, n)-threshold access structures, which achieves the best contrast by solving a simple linear program. Ateniese et al. [2] proposed an efficient technique to construct visual cryptography schemes. They analyzed structures of visual cryptography schemes and proved bounds for the size of the shares. Visual cryptography schemes for colour images were given in [11,15,18].

Extended visual cryptography defines that each share shows an image, but their combinations show the real secret image. Naor and Shamir [13] proposed an extended visual cryptography scheme for the (2, 2)-threshold access structure. Droste [6] proposed a very general method to construct an extended visual cryptography scheme for an arbitrary access structure, which is not necessarily monotonic. Ateniese et al. [3] proposed a hyper-coloring technique to construct extended visual cryptography schemes. It is possible that each share shows a different image initially and a different combination of shares shows a different secret image. Kim et al. [9] discussed negative images for access structures.

2. Model and Notation

Access Structure. We consider arbitrary access structures. Let $P = \{1, 2, \ldots, n\}$ be a set of participants. $\Gamma = (P, Q, F)$ is an access structure if both Q and F are subsets of 2^P and $Q \cap F = \emptyset$. Each $X \in Q$ is a qualified set of participants and each $Y \in F$ is a forbidden (non-qualified) set of participants. We call (P, Q, F) *complete* if $F = 2^P - Q$, which is denoted by (P, Q) in short. (P, Q) is a (k, n)-*threshold* access structure if all k- or more-element subsets of P are in Q. Q is monotonically increasing if $X \in Q$ implies that for all $X' \supseteq X$, $X' \in Q$. F is monotonically decreasing if $X \in F$ implies that for all $X' \subseteq X$, $X' \in F$. We say that $\Gamma = (P, Q, F)$ is *monotonic* if Q is monotonically increasing and F is monotonically decreasing. We remark that Q is not necessarily monotonically increasing and F is not necessarily monotonically decreasing for an arbitrary access structure (P, Q, F).

Notation. Let B be a Boolean matrix and B_i be the ith row vector of B. Let $B_i + B_j$ be the bit-wise OR of vectors B_i and B_j. Let X be a subset $\{i_1, i_2, \ldots, i_q)$ of a participant set P. We define $OR(B, X)$ to be the vector of "OR" of rows $i_1, i_2, \ldots, i_q$ of B, that is, $OR(B, X) = B_{i_1} + B_{i_2} + \cdots + B_{i_q}$. Let $w(v)$ be the Hamming weight of row vector v. For brevity, we let $w(B, X) = w(OR(B, X))$. Let $A \| B$ denote the concatenation of two matrices A and B of the same number of rows. Let $|X|$ be the number of elements in set X.

In visual cryptography, a secret image consists of a collection of black and white pixels. We use 0 to denote the white pixel and 1 to denote the black pixel. Each pixel in the image is considered separately. A pixel is divided into pixel shares. Each pixel share consists of m subpixels and is given to a participant such that a qualified set of participants can recover the pixel by stacking their pixel shares and a set of forbidden participants cannot get any information about the pixel, that is, the subpixel patterns of the pixel shares of the black pixel are the same as those of the white pixel. An *image share* (or share) of an image consists of all the pixel shares of its pixels.

To construct n shares of an image for n participants, we prepare two collections C_0 and C_1, which consist of $n \times m$ Boolean matrices. A row in a matrix in C_0 and C_1 corresponds to m subpixels such that 0 denotes the transparent point and 1 denotes the dark point. For a white (black) pixel in the image, we randomly choose a matrix M from C_0 (C_1, respectively) and assign row i of M to the corresponding position of share i. The resultant shares need satisfy the properties of visual cryptography. The conventional definition for *VCS* is as follows.

Definition 2.1. [2] Let $\Gamma = (P, Q, F)$ be an access structure. Two collections (multisets) C_0 and C_1 of $n \times m$ Boolean matrices constitute a visual cryptography scheme (Γ, m)-VCS if there exist a value $\alpha(m) > 0$ and a set $\{(X, t_X)\}_{X \in Q}$ satisfying:

1. Any qualified set $X = \{i_1, i_2, \ldots, i_q\} \in Q$ can recover the shared image by stacking their transparencies. Formally, for any $M \in C_0$, $w(M, X) \leq t_X - \alpha(m) \cdot m$; whereas, for any $M' \in C_1$, $w(M', X) \geq t_X$.
2. Any forbidden set $X = \{i_1, i_2, \ldots, i_q\} \in F$ has no information on the shared image. Formally, the two collections $D_t, t \in \{0, 1\}$, of $q \times m$ matrices obtained by restricting each $n \times m$ matrix in $M \in C_t$ to rows $i_1, i_2, \ldots, i_q$, are indistinguishable in the sense that they contain the same matrices with the same frequencies.

The first property, called *contrast,* ensures that the image revealed by the stacked shares of a qualified set of participants in Q shows enough difference between the white pixels and the black pixels. The value m is called *pixel expansion* and the value $\alpha(m)$ is called *contrast,* which should be as large as possible. The larger the contrast is, the sharper the image revealed by the stacked shares is. We call $\{(X, t_X)\}_{X \in Q}$ *the set of thresholds,* where t_X is the threshold associated with X. The second property, called *security,* ensures that nothing about the image can be recovered from the shares of a forbidden set of participants. We do not care about what image is revealed by the shares of a participant set $X \notin Q \cup F$.

We observe that by the definition only monotonic access structures have visual cryptography schemes. Assume that a forbidden set $X \in F$ contains a qualified set $Y \in Q$. Then, X's corresponding D_0 and D_1 are distinguishable by observing the matrices of D_0 and D_1 restricted to the rows of Y.

We consider general access structures. An access structure is non-monotonic if some forbidden set contains a qualified set. Non-monotonic access structures have some applications. For example, it may be that a participant x has the right to veto the decision of a qualified set X, such that $X \cup \{x\}$ is a forbidden set. We point out that the participants may not know Q and F. When some participants come together, all they do is to stack their shares and get the image revealed by their stacked shares. Therefore, non-monotonic access structures have some physical meaning.

We can see that by Definition 2.1, recovered images are always darker than backgrounds. As explained above, we give a new definition for visual cryptography that stresses "contrast." That is, some recovered images are darker than backgrounds and some are lighter than backgrounds.

Definition 2.2. Let $\Gamma = (P, Q, F)$ be an access structure. Two collections (multisets) C_0 and C_1 of $n \times m$ Boolean matrices constitute a visual cryptography scheme (Γ, m)-VCS if there exist value $\alpha(m) > 0$ and the set $\{(X, t_X)\}_{X \in Q}$ satisfying:

1. Any qualified set $X = \{i_1, i_2, \ldots, i_q\} \in Q$ can recover the shared image by stacking their shares. Formally, for any $M \in C_0$, $w(M, X) = t_X$; whereas, for any $M' \in C_1$, $w(M', X) \geq t_X + \alpha(m) \cdot m$ or for any $M' \in C_1$, $w(M', X) \leq t_X - \alpha(m) \cdot m$.
2. Any forbidden set $X = \{i_1, i_2, \ldots, i_q\} \in F$ has no information on the shared image. Formally, let $D_t, t \in \{0, 1\}$, be two collections of $q \times m$ matrices obtained by restricting each $n \times m$ matrix in $M \in C_t$ to rows $i_1, i_2, \ldots, i_q$, such that
   (a) If X does not contain any qualified set in Q, D_0 and D_1 are indistinguishable in the sense that they contain the same matrices with the same frequencies.
   (b) If X contains a qualified set in Q, the two collections $V_t, t \in \{0, 1\}$, of $1 \times m$ vectors obtained by *OR*-ing all rows of each $q \times m$ matrix in D_t are indistinguishable in the sense that they contains the same vectors with the same frequencies.

Our definition changes the property of contrast, in which the revealed images may be darker or lighter than backgrounds. We fix the threshold associated to $M \in C_0$ and adjust the threshold associated to $M \in C_1$. In defining security, 2(b) deals with the case of non-monotonic access structures. We require that the "stacked shares" (the *OR* vector of the corresponding rows) reveal no information about the image.

We shall use VCS_1 for a VCS based on Definition 2.1 and VCS_2 for a VCS based on Definition 2.2.

We give an example in Appendix to show that this definition may reduce the pixel expansion rate. We can see that the secret image "CRYPTOLOGY" is either darker or lighter than the background. The basis matrices (to be defined in the next section) of our VCS_2 construction have $m = 4$ and $\alpha(m) = 1/4$. However, by the previous definition, any VCS_1 for the access structure needs at least $m = 12$ and $\alpha(m) = 1/12$.

2.1. Basis Matrix

We usually don't construct C_0 and C_1 directly. Instead, we construct two $n \times m$ basis matrices S_0 and S_1 and then let C_t be the set of all matrices obtained by permuting columns of S_t, $t \in \{0, 1\}$. The VCS_2 definition based on basis matrices is as follows.

Definition 2.3. Let $\Gamma = (P, Q, F)$ be an access structure. Two $n \times m$ Boolean matrices S_0 and S_1 constitute a basis for a visual cryptography scheme (Γ, m)-VCS if there exist value $\alpha(m) > 0$ and the set $\{(X, t_X)\}_{X \in Q}$ satisfying:

1. Any qualified set $X = \{i_1, i_2, \ldots, i_q\} \in Q$ can recover the shared image by stacking their shares. Formally, $w(S_0, X) = t_X$; whereas $w(S_1, X) \geq t_X + \alpha(m) \cdot m$ or $w(S_1, X) \leq t_X - \alpha(m) \cdot m$.
2. Any forbidden set $X = \{i_1, i_2, \ldots, i_q\} \in F$ has no information on the shared image. Formally, let D_t, $t \in \{0, 1\}$, be two $q \times m$ matrices obtained by restricting S_t to rows $i_1, i_2, \ldots, i_q$ such that
   (a) If X does not contain any qualified set in Q, D_0 and D_1 are equal up to column permutation.
   (b) If X contains a qualified set in Q, the Hamming weight of the vector of *OR*-ing all rows of D_0 is equal to that of *OR*-ing all rows of D_1, that is, $w(D_0, X) = w(D_1, X)$.

We call VCS in Definition 2.2 as VCS_2 *with collections* and that in Definition 2.3 as VCS_2 *with bases*.

3. Properties of VCS_2

In this section, we study properties about VCS_2 and show how to construct a VCS_2 from smaller VCS_2.

Since VCS_2 is a generalization of VCS_1, any VCS_1 is a VCS_2.

THEOREM 3.1. *Let* $\Gamma = (P, Q, F)$ *be an access structure. Any* (Γ, m)-VCS_1 *is a* (Γ, m)-VCS_2.

Proof. This is trivial since VCS_1 is a special case of VCS_2. ■

If basis matrices S_0 and S_1 have a common column, we can delete it from S_0 and S_1 to reduce pixel expansion.

THEOREM 3.2 (Deletion). *Let $\Gamma = (P, Q, F)$ be an access structure. If S_0 and S_1 are basis matrices for a (Γ, m)-VCS_2, S'_0 and S'_1 are basis matrices for a $(\Gamma, m-k)$-VCS_2, where S'_0 and S'_1 are obtained from S_0 and S_1 by deleting the same k columns.*

Proof. Assume that $b_1, b_2, \ldots, b_k$ are the columns deleted from S_0 and S_1. Let $B = b_1 \| b_2 \| \cdots \| b_k$. For $X \in Q$, $w(S'_0, X) = w(S_0, X) - w(B, X) = t_X - w(B, X)$ and $w(S'_1, X) = w(S_1, X) - w(B, X) \geq t_X + m \cdot \alpha(m) - w(B, X)$ or $w(S'_1, X) = w(S_1, X) - w(B, X) \leq t_X - m \cdot \alpha(m) - w(B, X)$. Let $t'_X = t_X - w(B, X)$, $m' = m - k$ and $\alpha(m') = m \cdot \alpha(m)/m'$. Then, S'_0 and S'_1 meets the contrast requirement of VCS_2.

For $X \in F$, after deleting the same columns, S'_0 and S'_1 still meet the security requirements of VCS_2. Therefore, S'_0 and S'_1 are basis matrices for a (Γ, m')-VCS_2. ■

We can exchange the roles of S_0 and S_1 in a VCS_2. Therefore, if we find a VCS_2 for an access structure, we have another one immediately.

THEOREM 3.3 (Inverse). *Let $\Gamma = (P, Q, F)$ be an access structure. If S_0 and S_1 are basis matrices for a (Γ, m)-VCS_2, S'_0 and S'_1 are basis matrices for a (Γ, m)-VCS_2, where $S'_0 = S_1$ and $S'_1 = S_0$.*

Proof. For each $X \in Q$, we set t'_X to be $t_X + m \cdot \alpha(m)$ if $w(S_1, X) \geq t_X + m \cdot \alpha(m)$ and to be $t_X - m \cdot \alpha(m)$ if $w(S_1, X) \leq t_X - m \cdot \alpha(m)$. Then, for each $X \in Q$, $w(S'_1, X) = w(S_0, X) \leq t'_X - m \cdot \alpha(m)$ or $w(S'_1, X) = w(S_0, X) \geq t'_X - m \cdot \alpha(m)$.

The security requirements are not affected by exchanging S_0 and S_1. ■

We can add a participant such that Q is augmented.

THEOREM 3.4. *Let $\Gamma = (P, Q, F)$ be an access structure and $x \notin P$. If there exists a (Γ, m)-VCS_2 with bases, there exists a (Γ', m)-VCS_2 with bases, where $\Gamma' = (P \cup \{x\}, Q \cup \{\{x\}\}, F)$.*

Proof. Without loss of generality, let x be the $(n+1)$th element in $P \cup \{x\}$. Let S_0 and S_1 be the basis matrices for a (Γ, m)-VCS_2. It is easy to see that

$$S'_0 = \begin{bmatrix} S_0 \\ 0 \cdots 0 \end{bmatrix} \quad \text{and} \quad S'_1 = \begin{bmatrix} S_1 \\ 1 \cdots 1 \end{bmatrix}$$

are basis matrices for a (Γ', m)-VCS_2. ■

THEOREM 3.5. *Let $\Gamma = (P, Q)$ be a complete access structure and $x \notin P$. If there exists a (Γ, m)-VCS_2 with bases, there exists a (Γ', m)-VCS_2 with bases, where $\Gamma' = (P \cup \{x\}, Q \cup \{X \cup \{x\} | X \in Q\})$.*

Proof. Without loss of generality, let x be the $(n+1)$th participant in $P \cup \{x\}$. Let S_0 and S_1 be the basis matrices for a (Γ, m)-VCS_2. It is easy to see that

$$S_0' = \begin{bmatrix} S_0 \\ 0 \cdots 0 \end{bmatrix} \quad \text{and} \quad S_1' = \begin{bmatrix} S_1 \\ 0 \cdots 0 \end{bmatrix}$$

are basis matrices for a (Γ', m)-VCS_2. ∎

THEOREM 3.6. *Let $\Gamma = (P, Q, F)$ be an access structure and $x \notin P$. If there exists a (Γ, m)-VCS_2 with bases, there exists a $(\Gamma', m+1)$-VCS_2 with bases, where $\Gamma' = (P \cup \{x\}, Q \cup \{X \cup \{x\} | X \subseteq P\}, F)$.*

Proof. Without loss of generality, let x be the $(n+1)$th element in $P \cup \{x\}$. Let S_0 and S_1 be the basis matrices for a (Γ, m)-VCS_2. Let

$$S_0' = \begin{bmatrix} & & & 0 \\ & S_0 & & \vdots \\ & & & 0 \\ 1 & \cdots & 1 & 0 \end{bmatrix}, \quad S_1' = \begin{bmatrix} & & & 0 \\ & S_1 & & \vdots \\ & & & 0 \\ 1 & \cdots & 1 & 1 \end{bmatrix} \quad \text{and} \quad \alpha(m+1) = 1/(m+1).$$

For every $X \in Q' = Q \cup \{X \cup \{x\} | X \subseteq P\}$, if $X \in Q$, we have $w(S_0', X) = w(S_0, X)$ and $w(S_1', X) = w(S_1, X)$. If $x \in X$, we have $w(S_0', X) = m$ and $w(S_1', X) = m+1$, where $t_X = m$. Thus, S_0' and S_1' meet the contrast property. Since all forbidden sets are in F, S_0' and S_1' meet the security requirement. Therefore, S_0' and S_1' are basis matrices for a $(\Gamma', m+1)$-VCS_2. ∎

We can construct a VCS_2 for Γ' from a VCS_2 for Γ when Γ' is obtained by adding an additional participant x to Γ such that some sets containing x are forbidden.

THEOREM 3.7. *Let $\Gamma = (P, Q, F)$ be an access structure and $x \notin P$. If there exists a (Γ, m)-VCS_2 with bases, there exists a (Γ', m)-VCS_2 with bases, where $\Gamma' = (P \cup \{x\}, Q, F \cup \{X \cup \{x\} | X \in F\})$.*

Proof. Without loss of generality, let x be the $(n+1)$th element in $P \cup \{x\}$. Let S_0 and S_1 be the basis matrices for a (Γ, m)-VCS_2. It is easy to see that

$$S_0' = \begin{bmatrix} S_0 \\ 1 \cdots 1 \end{bmatrix} \quad \text{and} \quad S_1' = \begin{bmatrix} S_1 \\ 1 \cdots 1 \end{bmatrix}$$

are basis matrices for a (Γ', m)-VCS_2. ∎

COROLLARY 3.8. *Let $\Gamma = (P, Q, F)$ be an access structure and $x \notin P$. If there exists a (Γ, m)-VCS_2 with bases, there exist a (Γ', m)-VCS_2 with bases and a (Γ'', m)-VCS_2 with bases, where $\Gamma' = (P \cup \{x\}, Q, F \cup \{\{x\}\})$, and $\Gamma'' = (P \cup \{x\}, Q, F)$.*

We can concatenate the basis matrices of two VCS_2's if their access structures satisfy some conditions.

THEOREM 3.9 (Composition). *Let* $\Gamma_1 = (P, Q_1, F_1)$ *and* $\Gamma_2 = (P, Q_2, F_2)$ *be two access structures. Assume that* $Q_1 \cap Q_2 = \emptyset$. *If there exist a* (Γ_1, m_1)-VCS_2 *with bases and a* (Γ_2, m_2)-VCS_2 *with bases, there exists a* $(\Gamma, m_1 + m_2)$-VCS_2 *with bases, where* $\Gamma = (P, Q_1 \cup Q_2, F_1 \cap F_2)$.

Proof. Let S_0^1 and S_1^1 be basis matrices for a (Γ_1, m_1)-VCS_2 and S_0^2 and S_1^2 be basis matrices for a (Γ_2, m_2)-VCS_2. We show that $S_0 = S_0^1 \| S_0^2$ and $S_1 = S_1^1 \| S_1^2$ with $m = m_1 + m_2$ and $\alpha(m) = \min\{m_1 \cdot \alpha(m_1), m_2 \cdot \alpha(m_2)\}/(m_1 + m_2)$ are basis matrices for a (Γ, m)-VCS_2.

Let $Q = Q_1 \cup Q_2$ and $F = F_1 \cap F_2$. For $X \in Q$, if $X \in Q_1 \cap F_2$, we have

$$\begin{aligned} |w(S_0, X) - w(S_1, X)| &= \left|w\left(S_0^1, X\right) + w\left(S_0^2, X\right) - w\left(S_1^1, X\right) - w\left(S_1^2, X\right)\right| \\ &\geq \left|w\left(S_0^1, X\right) - w\left(S_1^1, X\right)\right| \\ &\geq m \cdot \alpha(m); \end{aligned}$$

if $X \in F_1 \cap Q_2$, we have

$$\begin{aligned} |w(S_0, X) - w(S_1, X)| &= \left|w\left(S_0^1, X\right) + w\left(S_0^2, X\right) - w\left(S_1^1, X\right) - w\left(S_1^2, X\right)\right| \\ &\geq \left|w\left(S_0^2, X\right) - w\left(S_1^2, X\right)\right| \\ &\geq m \cdot \alpha(m). \end{aligned}$$

Thus, S_0 and S_1 meet the contrast requirement.

For $X \in F$, since $X \in F_1 \cap F_2$, the matrix obtained by restricting S_t to rows of X is that obtained by restricting S_t^1 and S_t^2 to rows of X, $t \in \{0, 1\}$. Since S_0^1 and S_1^1 (S_0^2 and S_1^2) meet the security requirement, S_0 and S_1 meet the security requirement. ■

Even if the participant sets are not the same, we can modify the basis matrices a bit and concatenate them.

COROLLARY 3.10. *Let* $\Gamma_1 = (P_1, Q_1, F_1)$ *and* $\Gamma_2 = (P_2, Q_2, F_2)$ *be two access structures. Assume that* $Q_1 \cap Q_2 = \emptyset$. *If there exist a* (Γ_1, m_1)-VCS_2 *with bases and a* (Γ_2, m_2)-VCS_2 *with bases, there exists a* $(\Gamma, m_1 + m_2)$-VCS_2 *with bases, where* $\Gamma = (P_1 \cup P_2, Q_1 \cup Q_2, F_1 \cap F_2)$.

Proof. By Theorem 3.7, we can construct basis matrices for (Γ_1', m_1)-VCS_2 and (Γ_2', m_2)-VCS_2, where $\Gamma_1' = (P_1 \cup P_2, Q_1, F_1)$ and $\Gamma_2' = (P_1 \cup P_2, Q_2, F_2)$. Then, by Theorem 3.9, we concatenate the basis matrices of (Γ_1', m_1)-VCS_2 and (Γ_2', m_2)-VCS_2. ■

4. Some Results

We now present some results that are useful for constructing VCS_2 for general access structures.

4.1. *Optimal VCS_2 for (n, n)-Threshold Access Structure*

Let S_0 be the $n \times 2^{n-1}$ matrix whose columns are those that have exactly an even number of $1's$ and S_1 be the $n \times 2^{n-1}$ matrix whose columns are those that have exactly an odd number of $1's$. Then, S_0 and S_1 are the optimal basis matrices for a VCS_1 for the (n, n)-threshold access structure. This construction is optimal for VCS_2, too, that is, any VCS_2 with bases must have $n \times m$ basis matrices with $m \geq 2^{n-1}$ and $\alpha(m) \leq 1/2^{n-1}$.

THEOREM 4.1. *[13] Any VCS_2 with bases for the (n, n)-threshold access structure must have $m \geq 2^{n-1}$ and $\alpha(m) \leq 1/2^{n-1}$.*

4.2. *Q with a Single Qualified Set*

Let $\Gamma = (P, Q)$ be a complete access structure such that Q contains a single set $X = \{i_1, i_2, \ldots, i_q\}$ only. We construct $n \times 2^{q-1}$ matrices S_0 and S_1 for a $(\Gamma, 2^{q-1})$-VCS_2 from a VCS_2 for the (q, q)-threshold access structure.

THEOREM 4.2. *Let $\Gamma = (P, \{X\})$ be a complete access structure with $X = \{i_1, i_2, \ldots, i_q\}$. There exist basis matrices for a $(\Gamma, 2^{q-1})$-VCS_2.*

Proof. Let P_X be the set of participants in X. $\Gamma' = (P_X, \{X\})$ is a (q, q)-threshold access structure. Let S'_0 and S'_1 be the optimal basis matrices for a $(\Gamma', 2^{q-1})$-VCS_2, as shown in Section 4.1. By Theorem 3.7, we add the participants of $P - P_X$ to the participant set one by one and get $n \times 2^{q-1}$ basis matrices S_0 and S_1 for a $(\Gamma, 2^{q-1})$-VCS_2, where the i_jth row of S_t is the jth row of S'_t, $1 \leq j \leq q$, and all other rows are 1's, $t \in \{0, 1\}$. ■

4.3. *The Cumulative Array Method*

We review the cumulative array method that constructs a VCS_1 for a complete monotonic access structure $\Gamma = (P, Q)$ [2,16]. Assume that $P = \{1, 2, \ldots, n\}$. We define Z_{MF} to be the collection of the maximal forbidden sets in $F = 2^P - Q$, i.e.,

$$Z_{MF} = \{B \in F \mid B \cup \{i\} \in Q \text{ for all } i \in P \setminus B\}.$$

Assume that $Z_{MF} = \{z_1, z_2, \ldots, z_m\}$. We define the $n \times m$ Boolean matrix

$$CA_{Z_{MF}} = [a_{i,j}]_{n \times m},$$

where $a_{i,j} = 0$ if and only if participant $i \in z_j$.

Let $A_i = \{j \mid a_{i,j} = 1, 1 \leq j \leq m\}, 1 \leq i \leq n$. Let S'_0 and S'_1 be the optimal $m \times 2^{m-1}$ basis matrices for a VCS_1 of the (m, m)-threshold access structure. Then, S_0 and S_1 constitute basis matrices for a VCS_1 for Γ, where the ith row of S_t is $OR(S'_t, A_i)$, for $1 \leq i \leq n$ and $t \in \{0, 1\}$.

4.4. An Upper Bound for 2-out-n Access Structure

We now give an upper bound for pixel expansion of any VCS_2 for the special 2-out-n access structures. $\Gamma = (P, Q)$ is the 2-out-n access structure if $|P| = n$ and $Q = \{X \subseteq P : |X| = 2\}$. We present a VCS_2 with bases for the 2-out-n access structure.

THEOREM 4.3. *There is a VCS_2 with pixel expansion $m(n)$ and contrast $1/m(n)$ for the 2-out-n access structure such that*

$$m(n) = \begin{cases} \frac{(n-1)(n+3)}{4} & \text{if } n \text{ is odd} \\ \frac{n(n+2)}{4} & \text{if } n \text{ is even} \end{cases}$$

Proof. Let $b_{i,j}$ be the n-dimensional column vector whose ith and jth entries are 0 and all other entries are 1, $1 \le i < j \le n$. Let c_i be the n-dimensional column vector whose ith entry is 0 and all other entries are 1. Let $\vec{1}$ be the n-dimensional vector of all entries being 1.

For the case $n = 2m + 1$, we let S_0 contain all $b_{i,j}$'s with $i + j =$ odd and S_1 contains all $b_{i,j}$'s with $i + j =$ even. Furthermore, we add 2 copies of c_i to S_1 for even i, $1 \le i \le n$, and m copies of $\vec{1}$ to S_0. For example, the following are basis matrices of a VCS_2 for the 2-out-5 access structure:

$$S_0 = \begin{bmatrix} 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}, \quad S_1 = \begin{bmatrix} 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

There are $m^2 + 2m$, which is $(n-1)(n+3)/4$, columns in S_0 and S_1.

We now consider the contrast and security properties of this construction. Since there is only one $b_{i,j}$ column in either S_0 or S_1, for any two participants i and j, we have $|w(S_0, \{i, j\}) - w(S_1, \{i, j\})| = 1$. For any X containing 3 or more participants $i_1, i_2, \ldots, i_k$, $k \ge 3$, we have $w(S_0, \{i_1, i_2, \ldots, i_k\}) = w(S_1, \{i_1, i_2, \ldots, i_k\}) = m(n)$ since each column has at most two 0's. For any X containing only one participant i, row i of S_0 contains m 0's if i is odd and $m + 1$ 0's if i is even. This holds for S_1 also. Therefore, any single participant computes absolutely no information about the secret from his share.

For the case $n = 2m$, we let S_0 contains all $b_{i,j}$'s with $i + j =$ odd and S_1 contains all $b_{i,j}$'s with $i + j =$ even. Furthermore, we add a copy of c_i to S_1, $1 \le i \le n$, and m copies of $\vec{1}$ to S_0. For example, the following are basis matrices of a VCS_2 for the 2-out-4 access structure:

$$S_0 = \begin{bmatrix} 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}, \quad S_1 = \begin{bmatrix} 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 & 0 \end{bmatrix}$$

There are $m^2 + m$, which is $n(n+2)/4$, columns in S_0 and S_1.

We can discuss the contrast and security properties for this construction similarly. This completes the proof. ∎

Droste's VCS_1 construction for the 2-out-n access structure has the pixel expansion $m = C_2^n \cdot \sum_{i=1}^{n} (2^i \cdot C_i^n)$ [6]. By the cumulative array method, the VCS_1 construction for the 2-out-n access structure has pixel expansion $m = 2 \cdot C_2^n$. We are aware that there are $(2, n)$-threshold VCS_1 that have pixel expansion $m = 2\lceil \log n \rceil$ [2]. However, the 2-out-n access structure is different from the $(2, n)$-threshold access structure. The later one allows more than two participants to reveal the secret, while the former one does not.

5. Partition of Access Structures

For a given access structure $\Gamma = (P, Q, F)$, we can decompose it into smaller access structures $\Gamma_1 = (P, Q_1, F_1)$, $\Gamma_2 = (P, Q_2, F_2)$, $\ldots$, $\Gamma_k = (P, Q_k, F_k)$ such that

1. $Q_1 \cup Q_2 \cup \cdots \cup Q_k = Q$;
2. $Q_i \cap Q_j = \emptyset$ for $1 \leq i \neq j \leq k$;
3. $F_1 \cap F_2 \cap \cdots \cap F_k = F$.

We call such decomposition as a *partition* of Γ. By generalizing Theorem 3.9, we can concatenate the smaller basis matrices for (Γ_i, m_i)-VCS_2's to form basis matrices for a (Γ, m)-VCS_2.

THEOREM 5.1 (Partition). *Let $\Gamma_1, \Gamma_2, \ldots, \Gamma_k$ be a partition of the access structure Γ. Assume that S_0^i and S_1^i are basis matrices for a (Γ_i, m_i)-VCS_2. Then, $S_0^1 \| S_0^2 \| \cdots \| S_0^k$ and $S_1^1 \| S_1^2 \| \cdots \| S_1^k$ are basis matrices for a $(\Gamma, \sum_{i=1}^{k} m_i)$-$VCS_2$.*

Proof. This is proved by induction on k, $k \geq 2$. The induction basis holds by Theorem 3.9. The induction step follows easily. ■

5.1. An Upper Bound for General Access Structures

By the results in Theorems 4.2 and 5.1, we give an upper bound on pixel expansion for any access structure.

THEOREM 5.2. *Let $\Gamma = (P, Q, F)$ be an access structure. There exists a (Γ, m)-VCS_2 with bases, where $m = \sum_{X \in Q} 2^{|X|-1}$.*

Proof. Let Q be $\{X_1, X_2, \ldots, X_k\}$ and $\Gamma' = (P, Q)$. Since any (Γ, m)-VCS_2 is a (Γ', m)-VCS_2, we consider only $\Gamma' = (P, Q)$. We partition $\Gamma' = (P, Q)$ into $(P, \{X_1\})$, $(P, \{X_2\})$, $\ldots$, $(P, \{X_k\})$. For each $\Gamma_i = (P, \{X_i\})$, we construct $n \times 2^{|X_i|-1}$ basis matrices for a VCS_2 of Γ_i. Since $2^P - Q = \bigcap_{i=1}^{k} 2^P - \{X_i\}$, by Theorem 5.1 we concatenate these basis matrices to get basis matrices for a (Γ', m)-VCS_2, where $m = \sum_{i=1}^{k} 2^{|X_i|-1}$. ■

6. VCS_2 Construction for General Access Structure

We present two methods of constructing basis matrices for a VCS_2 of an arbitrary access structure. Without loss of generality, we consider a complete access structure $\Gamma = (P, Q)$, where $P = \{1, 2, \ldots, n\}$ is the set of participants. In case that the input access structure is not complete, we add the "don't care" participant sets into F and form a complete access structure.

6.1. Top-Down Approach

The idea of our first construction is to partition Q into maximal monotonic subsets Q_i, $1 \le i \le k$, and use the methods in Sections 4.2 and 4.3 to construct the basis matrices for these access structures (P, Q_i). Then, by Theorem 5.1, we concatenate these basis matrices for a (Γ, m)-VCS_2.

Our algorithm A1 is in Figure 1. We first pick a qualified set X with a maximum number of participants and incorporate as many qualified sets under X as possible. That is, for each picked X, we find the maximum monotonic collection Z_{MMQ} of qualified sets under X:

$$Z_{MMQ}(X, Q) = \{X' \mid X' \in Q, \text{ there is no } Y \in 2^{P_X} - Q \text{ such that } X' \subset Y \subset X\}.$$

Let $\Gamma_1 = (P_X, Z_{MMQ}(X, Q))$. Note that by our definition, Γ_1 is monotonic. We then subtract $Z_{MMQ}(X, Q)$ from Q and continue to find Γ_2, and so on. This process does not stop until Q becomes empty.

We give an example to illustrate this partition. Let $P = \{1, 2, 3, 4, 5\}$, $Q = \{\{1, 3\}, \{2, 3\}, \{3, 4\}, \{4, 5\}, \{1, 2, 3\}, \{1, 3, 4, 5\}, \{2, 3, 4, 5\}, \{1, 2, 3, 4, 5\}\}$ and $F = 2^P - Q$. First, we choose the maximum set $X_1 = \{1, 2, 3, 4, 5\}$ and set $Z_1 = Z_{MMQ}(X_1, Q) = \{\{1, 3, 4, 5\}, \{2, 3, 4, 5\}, \{1, 2, 3, 4, 5\}\}$. Therefore, $\Gamma_1 = (P_{X_1}, Z_1)$. Then, we subtract Z_1 from Q. Q becomes $\{\{1, 3\}, \{2, 3\}, \{3, 4\}, \{4, 5\}, \{1, 2, 3\}\}$. We select $X_2 = \{1, 2, 3\}$ and set $Z_2 = Z_{MMQ}(X_2, Q) = \{\{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$. Therefore, $\Gamma_2 = (P_{X_2}, Z_2)$. This process continues and we get $\Gamma_3 = (P_{X_3}, Z_3)$ and $\Gamma_4 = (P_{X_4}, Z_4)$, where $X_3 = \{3, 4\}$, $X_4 = \{4, 5\}$, $Z_3 = \{\{3, 4\}\}$ and $Z_4 = \{\{4, 5\}\}$.

Input: $\Gamma = (P, Q)$, where $F = 2^P - Q$.
1. if $Q = \emptyset$, return $S_0 = \mathbf{0}_{n\times 1}$ and $S_1 = \mathbf{0}_{n\times 1}$;
2. $A \leftarrow Q$; $i \leftarrow 0$;
3. while $A \neq \emptyset$ do
4. $\quad i \leftarrow i + 1$;
5. $\quad$ let X_i be the maximum set in A; (break tie randomly)
6. $\quad Z_i \leftarrow Z_{MMQ}(X_i, A)$;
7. $\quad A \leftarrow A - Z_i$;
8. $k \leftarrow i$;
9. construct basis matrices S_0^i and S_1^i for $\Gamma_i = (P_{X_i}, Z_i)$ and extend them to T_0^i and T_1^i for $\Gamma_i' = (P, Z_i)$, $1 \le i \le k$;
10. return $S_0 = T_0^1 \| T_0^2 \| \cdots \| T_0^k$ and $S_1 = T_1^1 \| T_1^2 \| \cdots \| T_1^k$.

Figure 1. A1: Partition Q and find basis matrices.

After finding a partition Γ_i, $1 \le i \le k$, of Γ, we construct a VCS_2 for each $\Gamma_i = (P_{X_i}, Z_i)$. If Z_i contains only a single qualified set X_i, we use the method in Section 4.2 to construct basis matrices S_0^i and S_1^i for a (Γ_i, m_i)-VCS_2, where $m_i = 2^{|X_i|-1}$. If Z_i contains two or more qualified sets, we use the cumulative method in Section 4.3 to construct S_0^i and S_1^i for a (Γ_i, m_i)-VCS_2, where m_i is the parameter implied by the cumulative method. By Theorem 3.7, we extend S_0^i and S_1^i to basis matrices T_0^i and T_1^i for a (Γ_i', m_i)-VCS_2, where $\Gamma_i' = (P, Z_i)$. Note that Γ_i and Γ_i' differ on the participant set.

We continue the example and compute

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

$$T_0^2 = \begin{bmatrix} 1&0 \\ 1&0 \\ 1&0 \\ 1&1 \\ 1&1 \end{bmatrix}, \quad T_1^2 = \begin{bmatrix} 1&0 \\ 1&0 \\ 0&1 \\ 1&1 \\ 1&1 \end{bmatrix},$$

$$T_0^3 = \begin{bmatrix} 1&1 \\ 1&1 \\ 1&0 \\ 1&0 \\ 1&1 \end{bmatrix}, \quad T_1^3 = \begin{bmatrix} 1&1 \\ 1&1 \\ 1&0 \\ 0&1 \\ 1&1 \end{bmatrix}, \quad T_0^4 = \begin{bmatrix} 1&1 \\ 1&1 \\ 1&1 \\ 1&0 \\ 1&0 \end{bmatrix}, \quad \text{and} \quad T_1^4 = \begin{bmatrix} 1&1 \\ 1&1 \\ 1&1 \\ 1&0 \\ 0&1 \end{bmatrix}.$$

By concatenating these basis matrices, we get basis matrices S_0 and S_1 for a (Γ, m)-VCS_2 with $m = 14$, $\alpha(m) = 1/14$,

$$S_0 = \begin{bmatrix} 0&0&0&1&0&1&1&1&1&0&1&1&1&1 \\ 0&0&0&1&0&1&1&1&1&0&1&1&1&1 \\ 0&0&1&0&1&0&1&1&1&0&1&0&1&1 \\ 0&1&0&0&1&1&0&1&1&1&1&0&1&0 \\ 0&1&1&1&0&0&0&1&1&1&1&1&1&0 \end{bmatrix}$$

and

$$S_1 = \begin{bmatrix} 0&0&0&1&0&1&1&1&1&0&1&1&1&1 \\ 0&0&0&1&0&1&1&1&1&0&1&1&1&1 \\ 0&0&1&0&1&0&1&1&0&1&1&0&1&1 \\ 0&1&0&0&1&1&0&1&1&1&0&1&1&0 \\ 1&0&0&0&1&1&1&0&1&1&1&1&0&1 \end{bmatrix}.$$

If we use Droste's method [6] directly to construct basis matrices for a (Γ, m)-VCS_1, we get $m = 44$ and $\alpha(m) = 1/44$. In the next section, we apply the techniques implied in Theorems 3.2 and 3.3 to improve this m and $\alpha(m)$ to 6 and $1/6$, respectively.

We now show correctness of our construction.

THEOREM 6.1. *The algorithm A1 in Figure 1 outputs basis matrices for a* (Γ, m)*-VCS*$_2$.

Proof. We only have to show that $\Gamma'_1, \Gamma'_2, \ldots, \Gamma'_k$ form a partition of $\Gamma = (P, Q)$ and T_0^i and T_1^i are the basis matrices for a (Γ'_i, m)-*VCS*$_2$. The later one holds by the constructions in Sections 4.2 and 4.3. For the former one, by the definition of $Z_{MMQ}(X, Q)$, $\Gamma_i = (P_X, Z_{MMQ}(X, Q)$ is a complete access structure over P_X. By the algorithm, the next Γ_{i+1} is computed from Q', where $Q' = Q - Z_{MMQ}(X, Q)$. Therefore, Γ'_i, $1 \le i \le k$, form a partition for Γ. ∎

6.2. *Further Improvement*

By Theorem 3.3, if S_0 and S_1 are basis matrices for a (Γ, m)-*VCS*$_2$, S'_0 and S'_1 are also basis matrices for a (Γ, m)-*VCS*$_2$, where $S'_0 = S_1$ and $S'_1 = S_0$. In Step 9 of A1 in Figure 1, for each Γ'_i, we actually have two *VCS*$_2$'s with bases: one is (T_0^i, T_1^i) and the other is $(T_0'^i, T_1'^i)$, where $T_0'^i = T_1^i$ and $T_1'^i = T_0^i$. Therefore, we have 2^k (Γ, m)-*VCS*$_2$'s in total. By searching among these schemes and removing redundant columns, we can find a *VCS*$_2$ with better contrast. For example, continuing the example of the previous section, we let

$$S_0 = T_1^1 \| T_0^2 \| T_1^3 \| T_0^4 = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \end{bmatrix}$$

and

$$S_1 = T_0^1 \| T_1^2 \| T_0^3 \| T_1^4 = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 \end{bmatrix}.$$

By Theorem 3.2, we delete equal columns from S_0 and S_1 and get

$$S'_0 = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 \end{bmatrix} \quad \text{and} \quad S'_1 = \begin{bmatrix} 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix},$$

which have $m = 6$ and $\alpha(m) = 1/6$.

LEMMA 6.2. *Any* $S_0 = T_{t_1}^1 \| T_{t_2}^2 \| \cdots \| T_{t_k}^k$ *and* $S_1 = T_{\bar{t}_1}^1 \| T_{\bar{t}_2}^2 \| \cdots \| T_{\bar{t}_k}^k$ *are basis matrices for a* (Γ, m)*-VCS*$_2$*, where* $t_i \in \{0, 1\}$ *and* $\bar{t}_i$ *is the complement of* t_i, $1 \le i \le k$.

Proof. By Theorem 3.3, (T_0^i, T_1^i) and (T_1^i, T_0^i) are both basis matrix pair for a (Γ'_i, m_i)-*VCS*$_2$, $1 \le i \le k$. By Theorem 5.1 for composition of a partition, this lemma holds. ∎

Though to find S_0 and S_1 with minimal pixel expansion among the 2^k VCS_2's is NP-complete, we provide a dynamic programming-type heuristic method to find a reasonable one.

We assume a canonical order $b_1, b_2, \ldots, b_{2^n}$ for n-dimensional Boolean vectors. Let $f_t^i = (i_1, i_2, \ldots, i_{2^n})$ be the *column spectrum* of T_t^i, $t \in \{0, 1\}$, $1 \le i \le k$, such that i_j is the number of b_j in columns of T_t^i. For example, if

$$T_0^i = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix},$$

then $f_0^i = (3, 1, 0, 0, 0, 0, 1, 1)$ is its column spectrum, where $b_1 = [0\,0\,0]^T$, $b_2 = [1\,0\,0]^T$, etc. For a spectrum $f = (i_1, i_2, \ldots, i_{2^n})$, let $|f| = \sum_{j=1}^{2^n} |i_j|$. Let $m(i, j)$ denote the differential column spectrum between

$$S_0^{i,j} = T_{t_i}^i \| T_{t_{i+1}}^{i+1} \| \cdots \| T_{t_j}^j \quad \text{and} \quad S_1^{i,j} = T_{\bar{t}_i}^i \| T_{\bar{t}_{i+1}}^{i+1} \| \cdots \| T_{\bar{t}_j}^j$$

for some $t_l \in \{0, 1\}$, $i \le l \le j$, where $m(i, j)$ is defined recursively as follows:

$$m(i, j) = \begin{cases} f_0^i - f_1^i & \text{if } i = j \\ \min_{i \le l \le j} \{m(i, l) + m(l+1, j) m(i, l) - m(l+1, j)\} & \text{if } i > j, \end{cases}$$

where $\min\{v_1, v_2, \ldots, v_r\} = v_i$ if $|v_i| \le |v_j|$ for all j, $1 \le j \le r$ (we break tie randomly). That is, $m(i, j)$ is the difference of the column spectrums of $S_0^{i,j}$ and $S_1^{i,j}$. We can see that the smaller $|m(i, j)|$ is, the smaller the pixel expansion $S_0^{i,j}$ and $S_1^{i,j}$ have after deleting equal columns. Our goal is to find smaller $|m(1, k)|$. The search algorithm is shown in Figure 2. During computing $m(i, i+z)$, we keep track the choice of t_l, $i \le l \le i+z$, in order to compute the indices for $m(1, k)$.

6.3. *Bottom-Up Approach*

Our second method uses the bottom-up approach. For a qualified set $X \in Q$, we define the collection of the qualified sets Y that contain X such that all sets between X and Y are qualified:

$$M(X, Q) = \{Y \mid X \subseteq Y, \text{ for all } X' \subseteq Y - X, X \cup X' \in Q\}.$$

Input: T_0^i, T_1^i, $1 \le i \le k$;
1. compute f_0^i and f_1^i, $1 \le i \le k$;
2. for $z = 0$ to $k-1$ do
3. for $i = 1$ to $k - z$ do
4. compute $m(i, i+z)$ and record t_l, $i \le l \le i+z$;
5. let t_l, $1 \le l \le k$, be the indices by which $m(1, k)$ is computed;
6. return $S_0 = T_{t_1}^1 \| T_{t_2}^2 \| \cdots \| T_{t_k}^k$ and $S_1 = T_{\bar{t}_1}^1 \| T_{\bar{t}_2}^2 \| \cdots \| T_{\bar{t}_k}^k$.

Figure 2. Search a VCS_2 with better pixel expansion.

Input: $\Gamma = (P, Q)$, where $F = 2^P - Q$.
1. if $Q = \emptyset$, return $S_0 = \mathbf{0}_{n\times 1}$ and $S_1 = \mathbf{0}_{n\times 1}$;
2. $A \leftarrow Q$; $i \leftarrow 0$;
3. while $A \neq \emptyset$ do
4. $\quad i \leftarrow i + 1$;
5. $\quad$ let X_i be the minimum set in A; (break tie randomly)
6. $\quad$ let Y_i be the maximum set in $M(X_i, A)$; (break tie randomly)
7. $\quad A \leftarrow A - Q(X_i, Y_i)$;
8. $k \leftarrow i$;
9. construct basis matrices S_0^i and S_1^i for $\Gamma_i = (P, Q(X_i, Y_i))$,
10. $\quad$ as shown in Lemma 6.3;
11. return $S_0 = S_0^1 \| S_0^2 \| \cdots \| S_0^k$ and $S_1 = S_1^1 \| S_1^2 \| \cdots \| S_1^k$.

Figure 3. A2: Bottom-up partition Q and find basis matrices.

$M(X, Q)$ is not empty since $X \in M(X, Q)$. For any $Y \in M(X, Q)$, let $B(X, Y) = \{X' | X \subseteq X' \subseteq Y\}$.

LEMMA 6.3. *$\Gamma' = (P, B(X, Y))$ have a VCS_2 with $n \times 2^{|X|-1}$ basis matrices S_0 and S_1, where the rows of $S_0(S_1)$ for X is the $S_0'(S_1')$ of the optimal $(|X|, |X|)$-VCS_1, the rows of $S_0(S_1)$ for $Y - X$ are all 0 and the rows of $S_0(S_1)$ for $P - Y$ are all 1.*

Proof. By Theorem 3.5, we extend $\Gamma' = (P_X, \{X\})$ to $\Gamma'' = (P_Y, B(X, Y))$ and by Theorem 3.7, we extend $\Gamma'' = (P_Y, B(X, Y))$ to $\Gamma = (P, B(X, Y))$. The basis matrices S_0 and S_1 are constructed accordingly. ■

For example, for $\Gamma = (\{1, 2, 3, 4\}, \{\{2, 3\}, \{1, 2, 3\}, \{2, 4\}\})$ and $X = \{2, 3\}$, $M(X) = \{\{1, 2, 3\}\}$ and $\Gamma' = (\{1, 2, 3, 4\}, \{\{2, 3\}, \{1, 2, 3\}\})$ has a VCS_2 with

$$S_0 = \begin{bmatrix} 0 & 0 \\ 0 & 1 \\ 0 & 1 \\ 1 & 1 \end{bmatrix} \quad \text{and} \quad S_1 = \begin{bmatrix} 0 & 0 \\ 1 & 0 \\ 0 & 1 \\ 1 & 1 \end{bmatrix}.$$

The algorithm A2 based on bottom-up partition is shown in Figure 3. We reduce the pixel expansion by applying the algorithm in Figure 2.

7. Experiments and Comparison

We compare the results of our two methods on random access structures with those of the Droste's method, which is the most efficient method of constructing VCS_1 for arbitrary access structures. The experimental results show that our VCS_2's indeed have better pixel expansion (contrast) in average.

We implement A1, A2 and the Droste's method for arbitrary access structures. The columns of the basis matrices produced by A1 and A2 are reduced by the search algorithm in Figure 2. We also remove redundant columns in basis matrices produced by the Droste's

Table 1. Comparison of three methods with $|Q| \approx 2^{n-1}$.

The Number n of Participants	The Number of Random Γ	Average Pixel Expansion m		
		A1	A2	Droste's
3	50	2.1	2.0	2.8
4	100	3.9	4.2	6.6
5	150	8.2	8.8	15.9
6	200	17.2	18.5	38.8
7	300	39.0	41.1	93.9
8	400	87.6	92.1	224.4

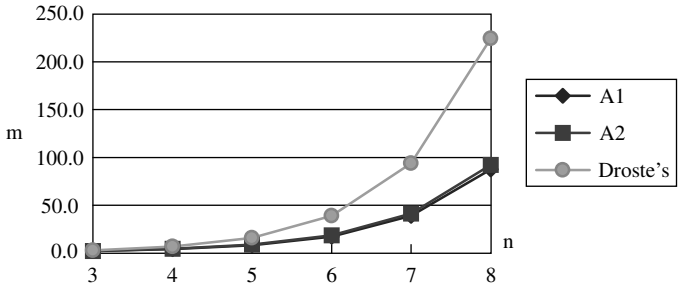


Table 2. Comparison of three methods with $|Q| \approx 2^n/3$.

The Number n of Participants	The Number of Random Γ	Average Pixel Expansion m		
		A1	A2	Droste's
3	50	1.9	2.0	2.6
4	100	3.8	4.0	6.1
5	150	8.2	8.7	15.7
6	200	17.2	18.9	38.5
7	300	38.5	41.9	93.3
8	400	88.2	101.9	230.1

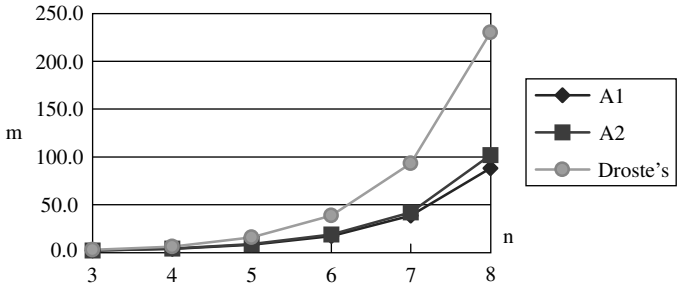


Table 3. Comparison of three methods with monotonic Γ.

The Number n of Participants	The Number of Random Γ	Average Pixel Expansion m		
		A1	A2	Droste's
3	50	2.0	2.0	2.0
4	100	4.1	3.9	4.1
5	150	10.0	7.8	10.0
6	200	25.1	15.5	25.1
7	300	64.4	31.7	64.4
8	400	187.3	73.5	187.3

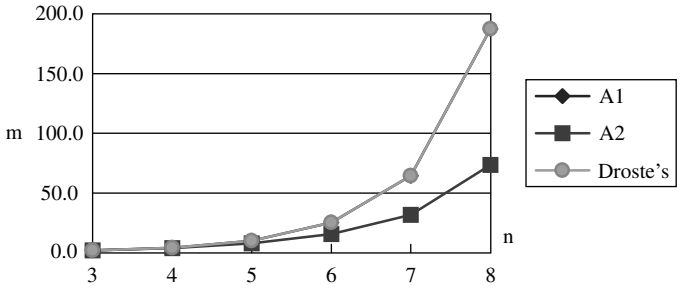


Table 4. Two examples of comparing our methods with Droste's.

	$P = \{1, 2, 3\}$, $Q = (\{1\}, \{2, 3\}, \{1, 2, 3\})$, $F = 2^P - Q$
Our VCS_2	$S_0 = \begin{bmatrix} 0 & 1 \\ 0 & 1 \\ 0 & 1 \end{bmatrix}$, $S_1 = \begin{bmatrix} 0 & 0 \\ 1 & 0 \\ 0 & 1 \end{bmatrix}$
Droste's VCS	$S_0 = \begin{bmatrix} 0 & 0 & 0 \\ 1 & 0 & 1 \\ 1 & 0 & 1 \end{bmatrix}$, $S_1 = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}$
	$P = \{1, 2, 3, 4\}$, $F = 2^P - Q$ $Q = (\{1, 2\}, \{1, 3\}, \{2, 3\}, \{2, 4\}, \{1, 3, 4\}, \{1, 2, 3, 4\})$
Our VCS_2	$S_0 = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}$, $S_1 = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix}$
Droste's VCS	$S_0 = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \end{bmatrix}$, $S_1 = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$

method. For a particular number of participants, we run these algorithms on a number of randomly chosen access structures. The results are shown in Tables 1, 2 and 3. In Table 1, we randomly choose access structures with $|Q| \approx 2^{n-1}$. In Table 2, we randomly choose access structures with $|Q| \approx 2^n/3$. For both cases, the average pixel expansion of our VCS_2 for a random access structure is only one half of that of the VCS produced by the Droste's method. In Table 3 for monotonic access structures, the A1 algorithm takes the whole Q as a partition and produces the same result as that of the Droste's method. But, the A2 algorithm produces VCS_2 with much better pixel expansion. Table 4 shows two access structures that have better pixel expansion based on our definition.

8. Conclusion

We have proposed a new definition for visual cryptography, in which the revealed images may be lighter or darker than backgrounds. We run experiments on random access structures. The results show that our VCS_2 indeed has better pixel expansion (contrast). We have studied properties about our new definition. We also show upper bounds for pixel expansion of VCS_2 for general and some special access structures.

Appendix

Let $\Gamma = (P, Q, F)$, where $P = \{1, 2, 3, 4\}$, $Q = \{(1, 2), (1, 4), (2, 3), (2, 4), (1, 3, 4), (1, 2, 3, 4)\}$ and $F = \{(1, 3), (3, 4), (1, 2, 3), (1, 2, 4), (2, 3, 4)\}$. Any (Γ, m)-VCS_1 has $m = 12$ at least. The basis matrices are:

$$S_0 = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \end{bmatrix}$$

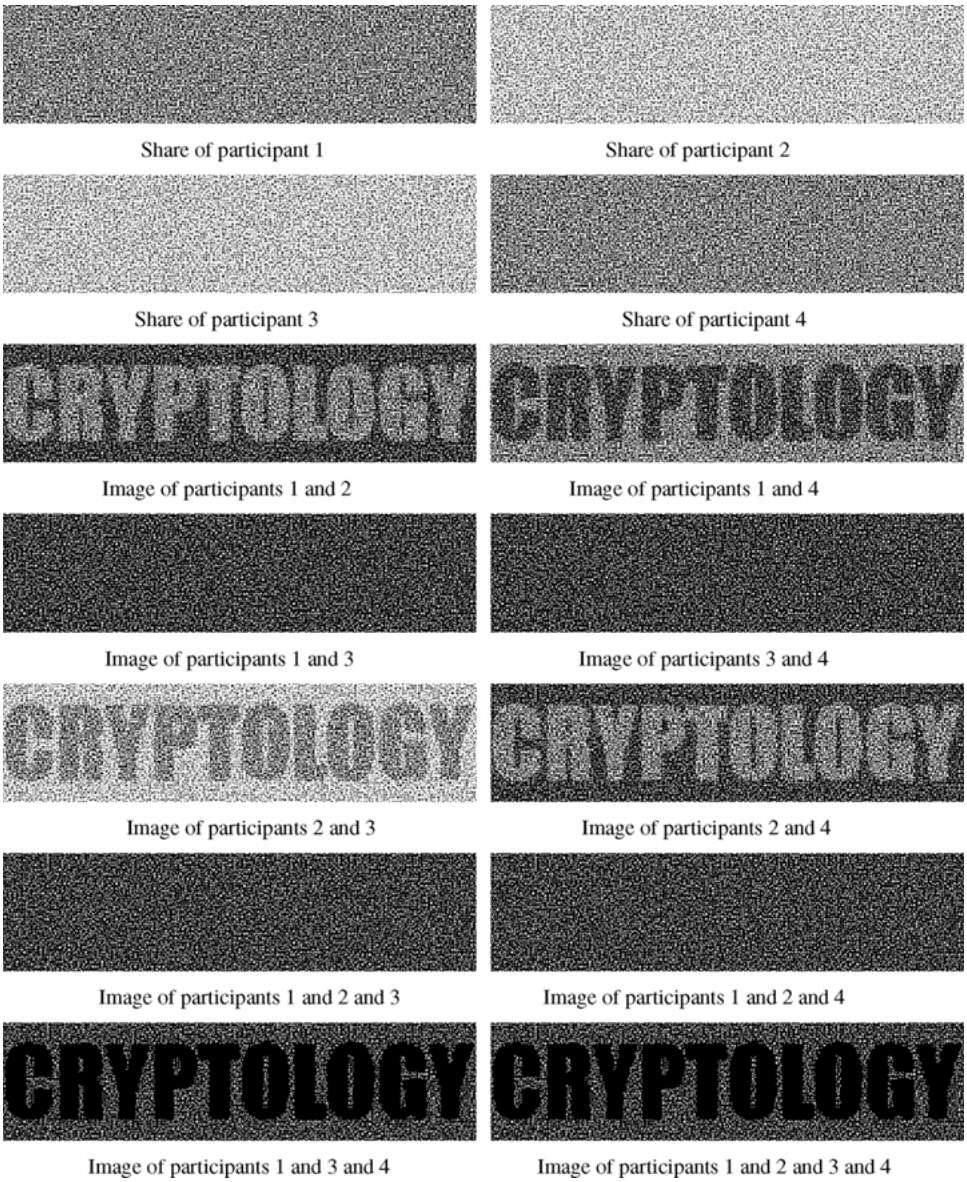
and

$$S_1 = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}$$

Our (Γ, m)-VCS_2 has $m = 4$ and $\alpha(m) = 1/4$. The basis matrices are

$$S_0 = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix} \quad \text{and} \quad S_1 = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix}.$$

The following shows the shares of all participants and images of the stacked shares of participants of qualified and forbidden sets.



Share of participant 1

Share of participant 2

Share of participant 3

Share of participant 4

Image of participants 1 and 2

Image of participants 1 and 4

Image of participants 1 and 3

Image of participants 3 and 4

Image of participants 2 and 3

Image of participants 2 and 4

Image of participants 1 and 2 and 3

Image of participants 1 and 2 and 4

Image of participants 1 and 3 and 4

Image of participants 1 and 2 and 3 and 4

References

1. G. Ateniese, C. Blundo, A. De Santis and D. R. Stinson, Constructions and bounds for visual cryptography, In *Proceedings of the 23rd International Colloquium on Automata, Languages, and Programming (ICALP 96),* LNCS, Vol. 1099, Springer-Verlag (1996).
2. G. Ateniese, C. Blundo, A. De Santis and D. R. Stinson, Visual cryptography for general access structures, *Information and Computation,* Vol. 129, No. 2 (1996) pp. 86–106.

3. G. Ateniese, C. Blundo, A. De Santis and D. R. Stinson, Extended capabilities for visual cryptography, *Theoretical Computer Science,* Vol. 250, No. 1–2 (2001) pp. 143–161.
4. C. Blundo, A. De Santis and D. R. Stinson, On the contrast in visual cryptography schemes, *Journal of Cryptology,* to appear.
5. C. Blundo, P. D'Arco, A. De Santis and D. R. Stinson, Contrast optimal threshold visual cryptography Schemes, manuscript.
6. S. Droste, New results on visual cryptography, In *Proceedings of Advances in Cryptology-CRYPTO 96,* LNCS, Vol. 1109, Springer-Verlag (1996) pp. 401–415.
7. T. Hofmeister, M. Krause and H. U. Simon, Contrast-optimal k-out-of-*n* secret sharing schemes in visual cryptography, *COCOON 97,* LNCS, Vol. 1276, Springer-Verlag (1997).
8. T. Katoh and H. Imai, Some visual secret sharing schemes and their share size, In *Proceedings of International Conferences on Cryptology and Information Security* (1996) pp. 41–47.
9. K. Kim, J. Park and Y. Zheng, Human-machine identification using visual cryptography, In *Proceedings of the 6th IEEE International Workshop on Intelligent Signal Processing and Communication Systems* (1998) pp. 178–182.
10. K. Kobara and H. Imai, Limiting the visible space visual secret sharing schemes and their application to human identification, In *Proceedings of Advances in Cryptology—ASIACRYPT 96,* LNCS, Vol. 1163, Springer-Verlag (1996) pp. 185–195.
11. D. Naccache, Colorful cryptography—a purely physical secret-sharing scheme based on chromatic filters, In Coding and Information Integrity, French-Israeli Workshop (1994).
12. M. Naor and B. Pinkas, Visual authentication, In *Proceedings of Advances in Cryptology—CRYPTO 97,* LNCS, Vol. 1294 (1997) pp. 322–336.
13. M. Naor and A. Shamir, Visual cryptography, In *Proceedings of Advances in Cryptology—EUROCRYPT 94,* LNCS, Vol. 950, Springer-Verlag (1995) pp. 1–12.
14. M. Naor and A. Shamir, Visual cryptography II: improving the contrast via the cover base, Cambridge Workshop on Cryptographic Protocols (1996). A full version is available at ftp://theory.lcs.mit.edu/pub/tcrypto/96-07.ps.
15. V. Rijmen and B. Preneel, Efficient colour visual encryption or shared colors of Benetton, presented at EUROCRYPT 96 Rump Session.
16. G. J. Simmons, W. Jackson and K. Martin, *The geometry of shared secret schemes,* Bulletin of the ICA, Vol. 1 (1991) pp. 71–88.
17. D. R. Stinson, Visual cryptography and threshold schemes, Dr. Dobb's Journal (1998).
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, Vol. 11, No. 2 (1997) pp. 179–196.