Contrast Optimal XOR Based Visual Cryptographic Schemes

Sabyasachi Dutta[1](✉) and Avishek Adhikari[2]

[1] R.C. Bose Centre for Cryptology and Security, Indian Statistical Institute,
203 B.T Road, Kolkata 700 108, India
saby.math@gmail.com
[2] Department of Pure Mathematics, Ballygunge Science College,
University of Calcutta, 35 Ballygunge Circular Road, Kolkata 700 019, India
avishek.adh@gmail.com

Abstract. OR-based Visual Cryptographic Schemes (OVCS) suffer from poor visual quality of the reconstructed image. XOR-based visual secret sharing (XVCS) can be thought of as an alternative where the relative contrast of the reconstructed image is much better. Moreover, it is possible to achieve optimum relative contrast equal to 1 in XVCS which is an impossibility in case of OVCS. Although there are examples of XVCSs where optimum relative contrast is achieved but to the best of our knowledge, this is the first theoretical work to find a necessary and sufficient condition for a XOR-based VCS to achieve optimum relative contrast equal to 1 in terms of the underlying access structure.

Keywords: Cumulative array · Relative contrast
Equivalent participants · Essential participants
Maximal forbidden sets · Visual secret sharing scheme

1 Introduction

A traditional Visual Cryptographic Scheme (VCS) for a set of n participants $\mathcal{P} = \{1, 2, \ldots, n\}$ is a variant of secret sharing, that encodes a secret image SI into n shares which are distributed by the dealer among n participants (also known as parties) in the form of transparencies on which the shares are photocopied. Such shares have the property that only "qualified" subsets of participants can visually recover the secret image by carefully stacking the transparencies. The first VCS was proposed by Naor and Shamir [20] where they considered the threshold access structure. This concept has been extended in [1,3,7,8] to general access structures.

The mathematical operation that lies beneath the physical implementation of the above mentioned schemes is the Boolean operation "OR". However the major problems for any OR-based visual cryptographic scheme are the huge share size (pixel expansion) and very poor contrast of the reconstructed image. Several

J. Shikata (Ed.): ICITS 2017, LNCS 10681, pp. 58–72, 2017.
https://doi.org/10.1007/978-3-319-72089-0_4

papers have been published to minimize the pixel expansion and to maximize contrast. One may refer to [2,4,5,9,10,12,16,21] for a detailed survey.

Arumugam et al. [6] introduced a VCS for a special type of access structure lying in between the threshold access structure and general access structure in the OR-model. They called it $(k,n)^*$-VCS, to address the scenario where one participant is "essential" and he needs the help of any $k-1$ parties other than him, to recover the secret image. Guo et al. [14] forwarded this idea to the concept of $(k,n)^*$-VCS with t essential participants who require the collaboration of $k-t$ more parties from the rest of the set of parties. Note that the case when t=0 we have the scenario of a (k,n)-VCS where no participant is essential. The case $t=1$ is the usual $(k,n)^*$-VCS while $t=n$ leads to the (n,n)-VCS.

1.1 "XOR" Based VCS: An Alternative for "OR" Based VCS

OR based visual cryptographic schemes suffer from the low quality of the reconstructed image. Tuyls et al. [22] gave a VCS based on polarization of light where the underlying mathematical operation was the Boolean "XOR" operation. The polarization of light is done by inserting a liquid crystal layer into a liquid crystal display (LCD). The advantage is two-fold. First, the liquid crystal layer can be driven in an LCD. Secondly, since the voltage applied to the liquid crystal layer makes it possible to rotate the polarization of light entering the layer over a certain angle, it facilitates a practical updating mechanism. Thus unlike OR-based schemes where a participant has to carry a number of transcripts to update the shares, in a XOR-based VCS a party has to carry just one dedicated trusted device that has a display. For recovering the secret image the shares i.e., the liquid crystal layers are to be stacked together. Moreover, due to the rapid advancement of technology these devices are getting cheaper. It is a reasonable expectation that polarization based visual cryptographic schemes will be implemented in every light-weight cryptographic situation. In [23] the authors constructed a XOR based (n,n)-VCS and proved that a XOR based $(2,n)$-VCS is equivalent to a binary code. There are also two different methods to realize the XOR operation in the field of visual cryptography. First one uses a Mach-Zehnder Interferometer [17] and the other one proposed in [24] needs a copy machine with the reversing function. One for further studies, may refer to [15,18,19,25]. All these papers have considered the common property of non-monotonicity of the access structure, i.e., super-set of the minimal qualified set may not get the secret back if all of them stack their shares. However, it does not prohibit us to define a visual cryptographic scheme. For most of the practical scenarios, the access structure is generally a public information. That is, the participants have complete knowledge of the qualified sets and forbidden sets. Therefore if a qualified set of participants come together then any minimal qualified subset of it may produce the corresponding shares to reconstruct the secret image. Thus it is sufficient to restrict ourselves to the collection of all minimal qualified sets corresponding to the access structure. The first XOR-based VCS for general access structure was proposed by Liu et al. [19]. They repeatedly used the share generation algorithm for a $(2,2)$-VCS to generate the shares of the participants for any access structure. However, their construction method is not via basis matrices. Moreover, their construction deviates from the traditional VCS in the sense that,

1. the participants may have to carry multiple share images;
2. due to the presence of multiple shares, at the time of revealing the secret, the participants have to know for which access structures they are going to submit which of their shares.

However their construction technique is novel and to the best of our knowledge there does not exist any other construction method other than [19] that constructs standard visual cryptographic scheme for the general access structure in the XOR model. So researches towards finding XOR-based VCS without these assumptions are important. Dutta et al. [11] gave an efficient technique to construct XOR-based $(k, n)^*$-VCS with t essential parties. Their linear algebraic technique can further be exploited to construct XOR-based VCS for general access structures. Yang et al. [25] provided plethora of examples of basis matrices by proving that basis matrices for OR-based (k, n)-VCS can be used as basis matrices for XOR-based (k, n)-VCS. Fu et al. [13] theoretically proved a necessary condition for the optimality of pixel expansion of any visual cryptographic scheme in both OR and XOR models. They gave an algorithm for reducing the pixel expansion of any scheme. However, their findings are based on the existence of basis matrices realizing an access structure. They have not however, given any construction method to produce the basis matrices or distribution matrices capturing the access structure in the first place. Their algorithm is novel modulo the existence of the basis matrices.

1.2 Our Contribution

In the OR-based VCS (OVCS) the relative contrast is always less than $\frac{1}{2}$. Moreover, it follows from [20] that for any access structure if there is a minimal qualified set of size t then relative contrast can never be better than $\frac{1}{2^{t-1}}$. This is true for whatever construction method we adopt to realize OVCS, as long as it is deterministic. On the other hand, for XOR-based VCS (XVCS) there is a possibility of achieving optimal relative contrast = 1. With the help of combinatorial design *cumulative array* we show that if a given access structure is *"OPTIMAL"* then it is possible to construct XVCS with relative contrast = 1. We explicitly describe the construction method and prove the correctness of the construction. We further prove that if an access structure does not satisfy the *optimality* condition then there cannot be any construction method realizing XVCS on the access structure achieving relative contrast equal to one. There were examples of XVCS which showed optimum relative contrast is achievable but to the best of our knowledge, this is the first theoretical work to answer the question of achievability of optimum relative contrast in terms of the underlying access structure.

2 Prerequisites

2.1 The Model for Non-monotone XOR-VCS

We follow standard notations and symbols through out. Let $\mathcal{P} = \{1, 2, 3, \ldots, n\}$ denote a set of participants. Let $2^{\mathcal{P}}$ denote the set of all subsets of $\mathcal{P}$. Let $\mathcal{Q} \subseteq 2^{\mathcal{P}}$ and $\mathcal{F} \subseteq 2^{\mathcal{P}}$, where $\mathcal{Q} \cap \mathcal{F} = \emptyset$, respectively denote the set of all qualified sets and the set of all forbidden sets. The pair $(\mathcal{Q}, \mathcal{F})$ constitutes an access structure on $\mathcal{P}$. In this paper, we consider $\mathcal{Q} = \mathcal{Q}_{min} = \{X \subseteq \mathcal{P} : B \in \mathcal{F}\ \forall B \subset X\}$, the collection of all minimal qualified sets of participants.

The collection of all maximal forbidden sets is denoted by $\mathcal{F}_{max} = \{F \in \mathcal{F} : \exists B \in \mathcal{Q}_{min}\ \&\ B \subset F \cup \{i\}\ \forall i \in \mathcal{P} - F\}$. Note that in this paper, we do not care about any subset $Y \in 2^{\mathcal{P}}$ such that $X \subset Y$, for some $X \in \mathcal{Q}_{min}$. We are interested only in the fact that the minimal qualified sets of parties can recover the secret image and the forbidden sets can not. This makes the access structure non-monotone. In this paper whenever we consider an access structure, it is implicit that we are interested in $\mathcal{Q}_{min}$ and $\mathcal{F}_{max}$.

Example 1. Let $\mathcal{P} = \{1, 2, \ldots, 6\}$ and let $\mathcal{Q}_{min}$ consist of the following minimal qualified subsets of participants $B_1 = \{1, 2, 3\}$, $B_2 = \{1, 2, 5\}$, $B_3 = \{1, 3, 4\}$, $B_4 = \{1, 4, 5\}$, $B_5 = \{1, 5, 6\}$. Note that $\{1, 2, 4\}$ and $\{2, 3, 4, 5, 6\}$ are members of both $\mathcal{F}$ and $\mathcal{F}_{max}$ while $\{2, 4, 5, 6\}$ is a member of $\mathcal{F}$ but not a member of $\mathcal{F}_{max}$.

Notations: Let S be an $n \times m$ Boolean matrix and $X \subseteq \mathcal{P} = \{1, 2, \ldots, n\}$. By $S[X]$ we denote the matrix obtained by restricting the rows of S to the indices belonging to X. Further, for any $X \subseteq \mathcal{P}$ the vector obtained by applying the boolean "XOR" operation to the rows of $S[X]$ is denoted by S_X. The Hamming weight of the row vector which represents the number of ones in the vector (S_X) is denoted by $w(S_X)$, if the context is clear. Other short hand notations and abbreviations used are given below:

- VCS $\longrightarrow$ visual cryptographic scheme.
- OVCS $\longrightarrow$ OR-based visual cryptographic scheme.
- XVCS $\longrightarrow$ XOR-based visual cryptographic scheme.
- CA $\longrightarrow$ cumulative array.
- $(k, n)^*$-VCS $\longrightarrow$ (k, n)-threshold VCS with one fixed essential party who is present in every minimal qualified set along with any other $k - 1$ regular parties.
- t-$(k, n)^*$-VCS $\longrightarrow$ (k, n)-threshold VCS with t many fixed essential parties who are present in every minimal qualified set along with any other $k - t$ regular parties.
- $\mathbf{0}$ $\longrightarrow$ bold-case 0 denotes the zero-vector.
- $\mathbf{1}$ $\longrightarrow$ bold-case 1 denotes the vector with all entries equal to 1.
- Contrast-optimal XVCS $\longrightarrow$ XVCS with relative contrast equal to 1 for every minimal qualified set.

We are now in a position to give definition of a Gen-NM-XVCS. Here, "NM" stands for non-monotone while X stands for XOR.

Definition 1. *Let $\mathcal{P} = \{1, 2, 3, \dots, n\}$ be a set of participants. A Gen-NM-XVCS on $\mathcal{P}$ is a visual cryptographic scheme such that the following two conditions hold:*

1. *Any minimal qualified set of participants can recover the secret image.*
2. *Any maximal forbidden set of participants does not have any information about the secret image.*

Any visual cryptographic scheme can be implemented by means of distribution matrices. To be more specific, let n and m be two integers, where n represents the number of parties and m the pixel expansion, i.e., the parameter that specifies how many sub-pixels are needed in each share to encode a single pixel of the secret image. A scheme is usually defined by two collections of Boolean matrices.

Definition 2. ***(via Collection of Matrices)***
Let $\mathcal{P} = \{1, 2, 3, \dots, n\}$ be a set of participants. Let $(\mathcal{Q}_{min}, \mathcal{F}_{max})$ be the access structure defined on $\mathcal{P}$. Let m and $\{h_X\}_{X \in \mathcal{Q}_{min}}$ be non-negative integers satisfying $1 \leq h_X \leq m$. Two collections of $n \times m$ binary matrices $\mathcal{C}_0$ and $\mathcal{C}_1$ realize a $(\mathcal{Q}_{min}, \mathcal{F}_{max})$-NM-XVCS, if there exists $\{\alpha_X > 0 : X \in \mathcal{Q}_{min}\}$ such that

1. *For any $S \in \mathcal{C}_0$, the XOR operation of the rows of $S[X]$ for any minimal qualified set X results in a vector v_0 satisfying $w(v_0) \leq h_X - \alpha_X \cdot m$.*
2. *For any $T \in \mathcal{C}_1$, the XOR operation of the rows of $T[X]$ for any minimal qualified set X results in a vector v_1 satisfying $w(v_1) \geq h_X$.*
3. *Any forbidden set $Y \in \mathcal{F}_{max}$ has no information on the shared image. Formally, the two collections of $|Y| \times m$ matrices $\mathcal{D}_t$, with $t \in \{0, 1\}$, obtained by restricting each $n \times m$ matrix in $\mathcal{C}_t$ to rows indexed by Y are indistinguishable in the sense that they contain the same matrices with the same frequencies.*

The symbols α_X and $\alpha_X \cdot m$ respectively denote the relative contrast and contrast of the recovered image reconstructed by the minimal qualified set X. We are considering only "Black and White" images in this paper. A white pixel is identified as 0 while a black pixel is identified as 1.

During share generation phase the dealer chooses randomly a matrix from $\mathcal{C}_b$, if the secret pixel is $b \in \{0, 1\}$, and gives the participant P_i the i-th row as the participant's share for all i. When the dealer wants to share a black and white secret image then for each constituent pixel he repeatedly performs the above process till all the pixels are shared. Note that the dealer has to store huge collections of matrices $\mathcal{C}_0$ and $\mathcal{C}_1$ to share an image. To reduce the storage space, a Gen-NM-XVCS may also be modelled by introducing the concept of basis matrices. The formal definition is as follows:

Definition 3 ***(via Basis Matrices).*** *A $(\mathcal{Q}_{min}, \mathcal{F}_{max})$-NM-XVCS is realized using two $n \times m$ binary matrices S^0 and S^1 called basis matrices, if there exist two sets of non-negative real numbers $\{\alpha_X\}_{X \in \mathcal{Q}_{min}}$ and $\{t_X\}_{X \in \mathcal{Q}_{min}}$ such that the following two conditions hold:*

1. (*contrast condition*) *If* $X \in \mathcal{Q}_{min}$*, then* S^0_X*, the "XOR" of the rows indexed by* X *of* S^0*, satisfies* $w(S^0_X) \leq t_X - \alpha_X \cdot m$*; whereas, for* S^1 *it results in* $w(S^1_X) \geq t_X$*.*
2. (*security condition*) *If* $Y = \{i_1, i_2, \ldots, i_s\} \in \mathcal{F}$ *then the two* $s \times m$ *matrices* $S^0[Y]$ *and* $S^1[Y]$ *obtained by restricting* S^0 *and* S^1 *respectively to rows* $i_1, i_2, \ldots, i_s$ *are identical up to a column permutation.*

For any minimal qualified set $X \in \mathcal{Q}_{min}$, the relative contrast of the reconstructed image is given by $\alpha_X = \frac{w(S^1_X) - w(S^0_X)}{m}$, where m is the pixel expansion of the scheme. If the secret pixel is $b \in \{0, 1\}$ then the dealer gives a random permutation to the columns of S^b and distributes the rows of the resulting matrix as shares to the parties. Similarly if the secret pixel is black then the dealer repeats the same process with the matrix S^1. The collections of matrices $\mathcal{C}_0$ and $\mathcal{C}_1$, that one requires to realize a VCS may be thought of as the collection of all possible matrices obtained by giving all possible column permutations to the basis matrices S^0 and S^1 respectively. As a result, the dealer has to store only the two matrices S^0 and S^1, making the scheme efficient space-wise.

2.2 Equivalent Parties and Simplification of Access Structures

We now discuss a technique which simplifies and reduces a class of more complex access structures into a simpler one. For that we need to first define the notion of *equivalent participants*. In words, equivalent parties are the parties who enjoy the same rights and hence they can be given identical shares without hampering the access structure of a secret sharing scheme. Hence given an access structure if we can identify the equivalent parties then they can be given the same shares and the access structure reduces to a much simpler one. One can treat the reduced access structure (which is simpler than the original one) as the given access structure and build schemes keeping in mind that ultimately while distributing the shares the equivalent parties receive the same shares. We start with the formal definition of equivalent participants.

Definition 4 *(adapted from [19]). Let* $\mathcal{Q}_{min}$ *and* $\mathcal{F}_{max}$ *denote the collections of minimal qualified sets and maximal forbidden sets respectively on a set of parties* $\mathcal{P} = \{1, 2, \ldots, n\}$*. If parties* i *and* j *satisfy that, for all* $F \in \mathcal{F}_{max}$*,* $i \in F$ *if and only if* $j \in F$*, then the parties* i *and* j *are called equivalent participants for the access structure.*

Example 2. Let us consider 3-$(4, 6)^*$-XVCS on the set of participants $\mathcal{P} = \{1, 2, \ldots, 6\}$, where the first three parties are essential in the sense that they are present in each of the minimal qualified sets. However, they need the share of one more party to reconstruct the secret image. Here, $\mathcal{Q}_{min} = \{\{1, 2, 3, 4\}, \{1, 2, 3, 5\}, \{1, 2, 3, 6\}\}$ and $\mathcal{F}_{max} = \{\{1, 2, 3\}, \{1, 2, 4, 5, 6\}, \{1, 3, 4, 5, 6\}, \{2, 3, 4, 5, 6\}\}$. In this access structure 4, 5, 6 are equivalent parties.

It is easy to see that the relation ‘ $\sim$’ defined on $\mathcal{P}$ by $i \sim j$ if and only if i and j are equivalent parties, is an equivalence relation on $\mathcal{P}$. Thus, the set $\mathcal{P}$ is partitioned into equivalence classes. An equivalence class of $i \in \mathcal{P}$ is the set $[i] = \{j \in \mathcal{P} : i \sim j\}$. For the sake of better representation we will denote the equivalence class $[p]$ by $\tilde{p}$. We now give the definition of the simplified access structure $\tilde{\mathcal{Q}}_{min}$ derived from $\mathcal{Q}_{min}$.

Definition 5 *(adopted from [19]). Let $(\mathcal{Q}_{min}, \mathcal{F}_{max})$ be a given access structure on a set $\mathcal{P}$ of parties. Let $\tilde{\mathcal{P}} = \{\tilde{p} : p \in \mathcal{P}\}$. We choose one single representative from an equivalence class that is, one party represents an equivalence class. We say $\tilde{\mathcal{Q}}_{min} = \{\{\tilde{p} \in \tilde{\mathcal{P}} : p \in B\} : B \in \mathcal{Q}_{min}\}$ as the simplified access structure of the given access structure. If $\tilde{\mathcal{Q}}_{min} = \mathcal{Q}_{min}$ then the access structure is called the most simplified access structure.*

Remark 1. For $2 \leq k \leq n$, the threshold access structure corresponding to (k, n)-XVCS are already in the most simplified form. In other words, no two parties are equivalent.

Example 3. Continuing from Example 2, we see that $\tilde{\mathcal{P}} = \{1, 2, 3, \tilde{4}\}$ and $\tilde{\mathcal{Q}}_{min} = \{\{1, 2, 3, \tilde{4}\}\}$, where $\tilde{4} = [4] = \{4, 5, 6\}$. This $\tilde{\mathcal{Q}}_{min}$ is the most simplified form of the given access structure.

2.3 Cumulative Array for an Access Structure

So far we have seen a way to simplify certain access structures via the concept of equivalent parties. Let $(\mathcal{Q}_{min}, \mathcal{F}_{max})$ be the given access structure and suppose that the access structure be already in its *most simplified form*. Let $\mathcal{F}_{max} = \{F_1, F_2, \ldots, F_t\}$. Let us now recall the idea of cumulative array (see [7]) for $\mathcal{Q}_{min}$. The cumulative array (CA) is an $n \times t$ Boolean matrix such that $CA(i, j) = 1$ if and only if $i \notin F_j$ where n is the number of participants.

Example 4. The cumulative array for 3-$(4, 6)^*$-access structure from Example 2 is given by

Parties	$F_1 = \{123\}$	$F_2 = \{12456\}$	$F_3 = \{13456\}$	$F_4 = \{23456\}$
1	0	0	0	1
2	0	0	1	0
3	0	1	0	0
4	1	0	0	0
5	1	0	0	0
6	1	0	0	0

where $\{123\}$ means the set $\{1, 2, 3\}$, $\{12456\}$ means the set $\{1, 2, 4, 5, 6\}$ etc. We will sometimes denote a set in this form for brevity, when there is no scope for confusion.

It is not very hard to see the following necessary and sufficient condition for checking whether two participants i and j are equivalent or not using cumulative array.

Proposition 1. *Two parties i and j are equivalent if and only if ith row and jth row of the corresponding cumulative array are identical.*

Thus once an access structure is reduced, via equivalent parties, to its most simplified form then the associated cumulative array does not contain two identical rows.

Observation. An access structure is in its "most simplified form" if the corresponding CA has no identical rows. For example, the CA for a (k, n)-threshold VCS with $1 < k \leq n$ has no identical rows and hence is in most simplified form.

Observation. Every row of an CA contains at least one 1, otherwise the party (indexing the row) belongs to every maximal forbidden set and hence in no minimal qualified set. So the party can be deleted from the access structure. Moreover, if $B \in \mathcal{Q}_{min}$ then $CA[B]$ contains at least one 1 in every column, otherwise B becomes a subset of some maximal forbidden set and hence not qualified to recover the secret image.

3 Main Results

Definition 6. *A cumulative array for $\mathcal{Q}_{min}$ (which is in its most simplified form) is called* **OPTIMAL** *if it satisfies the following property:*
for each minimal qualified set $\{i_1, i_2, \ldots, i_k\}$, every column of the restricted array $CA[\{i_1, i_2, \ldots, i_k\}]$ contains only odd many 1's.

For example, the cumulative array for an (n, n)-threshold VCS is *OPTIMAL* whereas for a (k, n)-threshold VCS with $k < n$, it is not OPTIMAL.

We now present an easy lemma to show the existence of a XOR-based VCS which achieves optimal relative contrast 1.

Lemma 1. *Let (S^0, S^1) be the basis matrices constructed by the method of Naor-Shamir as in [20] to realize an (n, n)-OVCS. Then (S^0, S^1) also realizes (n, n)-XVCS having pixel expansion 2^{n-1} and optimal relative contrast 1.*

Proof. : We recall that S^0 consists of all possible even columns of length n while S^1 consists of all possible odd columns of same length, as given in [20]. It is easy to see that S^0 and S^1 can be used to distribute shares to the participants in the XOR model. The only qualified set of parties is $\mathcal{P}$ itself. Also, $w(XOR(S^1_{\mathcal{P}})) = 2^{n-1}$ and $w(XOR(S^0_{\mathcal{P}})) = 0$. It follows that the "contrast condition" of Definition 3 is satisfied. The "security condition" for both OR based and XOR based models is the same. Hence we have the result. We further observe that the Naor-Shamir construction admits pixel expansion equal to 2^{n-1} and the relative contrast is 1 which is maximum in XOR-based VCS.

Construction 1. *Let us consider an access structure, in its most simplified form, $(\mathcal{Q}_{min}, \mathcal{F}_{max})$ on a set of n parties $\mathcal{P}$. Let the corresponding CA be OPTIMAL. Let $\mathcal{F}_{max} = \{F_1, F_2, \ldots, F_k\}$ i.e. we have k many maximal forbidden sets.*

Let $W_{(k,k)}$ and $B_{(k,k)}$ respectively denote the Naor-Shamir [20] white basis matrix and black basis matrix corresponding to a (k,k)-threshold access structure. Each of $W_{(k,k)}$ and $B_{(k,k)}$ is of size $k \times 2^{k-1}$, where the rows are indexed by the maximal forbidden sets $\{F_1, F_2, \ldots, F_k\}$ with respect to which the CA is constructed. Let us write $W_{(k,k)} = \begin{bmatrix} .. \; R_1^0 \; .. \\ .. \; R_2^0 \; .. \\ .. \; .. \; .. \\ .. \; R_k^0 \; .. \end{bmatrix}$ and $B_{(k,k)} = \begin{bmatrix} .. \; R_1^1 \; .. \\ .. \; R_2^1 \; .. \\ .. \; .. \; .. \\ .. \; R_k^1 \; .. \end{bmatrix}$, where R_i^0 denotes the ith row of $W_{(k,k)}$ and R_i^1 denotes the ith row of $B_{(k,k)}$. Notice that the rows are the shares of the participants.

Now *construct* S^0 (white basis matrix) and S^1 (black basis matrix) realizing the given access structure $(\mathcal{Q}_{min}, \mathcal{F}_{max})$ as follows:
The i-th row of S^0 = XOR of those rows in $W_{(k,k)}$ for which $i \notin F_j = R_{j_1}^0 \oplus R_{j_2}^0 \oplus \cdots \oplus R_{j_s}^0$,
where $R_{j_\alpha}^0$s are those rows of $W_{(k,k)}$ such that $i \notin F_{j_1} \cup F_{j_2} \cup \cdots \cup F_{j_s}$.
The i-th row of S^1 = XOR of those rows in $B_{(k,k)}$ for which $i \notin F_j = R_{j_1}^1 \oplus R_{j_2}^1 \oplus \cdots \oplus R_{j_s}^1$,
where $R_{j_\alpha}^1$s are those rows of $B_{(k,k)}$ such that $i \notin F_{j_1} \cup F_{j_2} \cup \cdots \cup F_{j_s}$.

Proposition 2. *Let $(\mathcal{Q}_{min}, \mathcal{F}_{max})$ be a non-monotone access structure (in its most simplified form) with OPTIMAL CA. The matrices (S^0, S^1) constructed in the above manner are indeed the basis matrices realizing XVCS on the given access structure. Moreover, maximum relative contrast equal to 1 is attained through this construction.*

Remark 2. Before proving the proposition, we point out that if the CA of an access structure (after reducing it to its most simplified form) is not Optimal then the above construction method does not admit basis matrices for XVCS. For example, let us consider the $(2,3)$-threshold access structure. The CA for the access structure is constructed with the help of $\mathcal{F}_{max} = \{\{1\}, \{2\}, \{3\}\}$ and is given by

Parties	$F_1 = \{1\}$	$F_2 = \{2\}$	$F_3 = \{3\}$
1	0	1	1
2	1	0	1
3	1	1	0

From the CA it is clear that the access structure is already in its most simplified form. Moreover, the CA is not Optimal as $CA[\{1,2\}] = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}$, which is the restriction of the CA to rows indexed by the minimal qualified set $\{1,2\}$ contains an even column. The last column of this restricted CA is indexed by the maximal forbidden set $\{3\}$. Since the number of maximal forbidden sets is 3, we consider the Naor-Shamir basis matrices for $(3,3)$-VCS,
$W_{(3,3)} = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}$ and $B_{(3,3)} = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \end{bmatrix}$. So by the above construction method we compute
$\boldsymbol{S}^0 = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}$ and $\boldsymbol{S}^1 = \begin{bmatrix} 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix}$. Now it is easy to see that the contrast condition is not holding for any minimal qualified set.

Proof of Proposition 2: Let $|\mathcal{F}_{max}| = t$, i.e. the access structure in its most simplified form has t many maximal forbidden sets and also it is given that the corresponding CA is optimal. We observe that if X is a minimal qualified set and since the CA is OPTIMAL then every column of the restricted CA, viz. $CA[X]$ contains odd number of 1s. The contrast condition holds because XOR of the shares of the participants in X satisfy the following:
XOR of the rows (in S^1) corresp. to the parties in X = XOR of *all* the rows in $B_{(t,t)} = (1, 1, \ldots, 1) = 2^{t-1}$ tuple with all entries equal to 1

and

XOR of the rows (in S^0) corresp. to the parties in X = XOR of *all* the rows in $W_{(t,t)} = (0, 0, \ldots, 0) = 2^{t-1}$ tuple with all entries equal to 0.

Hence,

wt.(XOR of the rows (in S^1) corresp. to the parties in X) − wt.(XOR of the rows (in S^0) corresp. to the parties in X) $= 2^{t-1} - 0 = 2^{t-1}$, which gives optimal relative contrast 1.

To prove the security condition we need to show that if F is any maximal forbidden set then the restricted matrices $S^0[F]$ and $S^1[F]$ are equal, upto a column permutation. So let F be a maximal forbidden set. The restricted matrix $CA[F]$ contains an all zero column, say the rth column. Here we notice that F is the rth maximal forbidden set indexing the rth column of the CA. Now, by our construction method, the shares of the participants in F do not contain any information about the rth row of $W_{(t,t)}$ and $B_{(t,t)}$. Now from the security condition (see Lemma 1) of (t, t)-threshold scheme, $W_{(t,t)}$ minus the rth row is equal (upto a column permutation) to $B_{(t,t)}$ minus the rth row. Without loss of generality we can assume that the matrices are equal. If two matrices M and N are equal then so are the matrices M' and N' obtained by giving same row operations on M and N respectively. This result follows from the fact that giving a row operation on a matrix is equivalent to multiplying the matrix by an elementary matrix from the left. Hence, the result follows.

Example 5. Consider the access structure $\mathcal{Q}_{min} = \{123, 14\}$ on the set of four parties $\mathcal{P} = \{1, 2, 3, 4\}$. Thus, $\mathcal{F}_{max} = \{12, 13, 234\}$ and the corresponding CA is

Parties	$F_1 = \{12\}$	$F_2 = \{13\}$	$F_3 = \{234\}$
1	0	0	1
2	0	1	0
3	1	0	0
4	1	1	0

which shows that access structure is already in its most simplified form. Thus, $CA[\{123\}] = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}$ and $CA[\{14\}] = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}$ which show that the CA is OPTIMAL.

Since $|\mathcal{F}_{max}| = 3$, we consider the Naor-Shamir basis matrices for $(3, 3)$-VCS, $W_{(3,3)} = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}$ and $B_{(3,3)} = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \end{bmatrix}$.

We can now construct the basis matrices using the method of Construction 1

$S^0 = \begin{bmatrix} 0&1&1&0 \\ 0&1&0&1 \\ 0&0&1&1 \\ 0&1&1&0 \end{bmatrix}$ and $S^1 = \begin{bmatrix} 1&1&0&0 \\ 1&0&1&0 \\ 1&0&0&1 \\ 0&0&1&1 \end{bmatrix}$ which give optimal relative contrast XVCS on the given access structure.

This example shows that there exist optimal contrast XVCS without being of the (n, n)-threshold type. Other examples of access structures that can have optimal contrast XVCS include *star-graph access structures, any access structure with just two minimal qualified sets,* $(k-1)$-$(k, n)^*$ *type access structures, complete bipartite graph access structure.*

From Proposition 2 we see that if the cumulative array of an access structure (in its most simplified form) is OPTIMAL then there exists a contrast optimal XVCS realizing that access structure. We now ask the converse question, namely if we somehow know that there is an access structure on which it is possible to have contrast optimal XVCS then is it necessarily true that the corresponding cumulative array of the access structure (in its most simplified form) OPTIMAL? Notice that we are not restricting ourselves to one particular way of constructing basis matrices so that contrast optimality is achieved. We seek for the result for any arbitrary method of construction.

To rephrase, we are finding the truth value of the following statement: If an access structure (in its most simplified form) has non-Optimal CA then there is no construction technique which will give contrast-optimal XVCS realizing the access structure.

Let us first consider two examples to gain insight into the problem.

Example 6. Let us consider a $(2, 3)$-XVCS on the set of parties $\mathcal{P} = \{1, 2, 3\}$. Thus $\mathcal{Q}_{min} = \{12, 13, 23\}$ and $\mathcal{F}_{max} = \{1, 2, 3\}$. The cumulative array for this access structure is given in Remark 2 which shows that the access structure is already in its most simplified form. Consider the restriction of the CA to the rows indexed by the minimal qualified set 12, $CA[\{12\}] = \begin{bmatrix} 0&1&1 \\ 1&0&1 \end{bmatrix}$ and thus it is non-Optimal.

Suppose it is possible to construct basis matrices S^0 and S^1 which give contrast optimal XVCS.

Let $S^0 = \begin{bmatrix} \cdot\cdot & R_1^0 & \cdot\cdot \\ \cdot\cdot & R_2^0 & \cdot\cdot \\ \cdot\cdot & R_3^0 & \cdot\cdot \end{bmatrix}$ and $S^1 = \begin{bmatrix} \cdot\cdot & R_1^1 & \cdot\cdot \\ \cdot\cdot & R_2^1 & \cdot\cdot \\ \cdot\cdot & R_3^1 & \cdot\cdot \end{bmatrix}$. From the definition of relative contrast it follows that for contrast to be 1

$$\left.\begin{array}{l} R_1^0 \oplus R_2^0 = \mathbf{0} \\ R_1^0 \oplus R_3^0 = \mathbf{0} \\ R_2^0 \oplus R_3^0 = \mathbf{0} \end{array}\right\} \qquad \text{and} \qquad \left.\begin{array}{l} R_1^1 \oplus R_2^1 = \mathbf{1} \\ R_1^1 \oplus R_3^1 = \mathbf{1} \\ R_1^1 \oplus R_2^1 = \mathbf{1} \end{array}\right\}$$

where $\mathbf{0}$ denotes the tuple with all-zero entries and $\mathbf{1}$ denotes the tuple with all-one entries. Now, the last three equations

$$\left.\begin{array}{l} R_1^1 \oplus R_2^1 = \mathbf{1} \\ R_1^1 \oplus R_3^1 = \mathbf{1} \\ R_1^1 \oplus R_2^1 = \mathbf{1} \end{array}\right\}$$

are inconsistent.

Hence, there can not be any construction method whatsoever that will give contrast-optimal XVCS on $(2,3)$-threshold access structure.

Another type of situation may occur which we explain in the next example.

Example 7. Let us consider a $(3,4)$-threshold access structure on the set of parties $\mathcal{P} = \{1,2,3,4\}$.
Thus $\mathcal{Q}_{min} = \{123, 124, 134, 234\}$ and $\mathcal{F}_{max} = \{12, 13, 14, 23, 24, 34\}$. The CA for this access structure is given by

Parties	$F_1 = \{12\}$	$F_2 = \{13\}$	$F_3 = \{14\}$	$F_4 = \{23\}$	$F_5 = \{24\}$	$F_6 = \{34\}$
1	0	0	0	1	1	1
2	0	1	1	0	0	1
3	1	0	1	0	1	0
4	1	1	0	1	0	0

From the CA it is clear that the access structure is already in its most simplified form. Moreover, the CA is non-Optimal as $CA[\{1,2,3\}] = \begin{bmatrix} 0&0&0&1&1&1 \\ 0&1&1&0&0&1 \\ 1&0&1&0&1&0 \end{bmatrix}$, which is the restriction of the CA to rows indexed by the minimal qualified set $\{1,2,3\}$. It contains three columns with weight 2. Let us consider this minimal qualified set $\{123\}$ and take F_6 which has made the CA non-Optimal.

Suppose it is possible to construct basis matrices S^0 and S^1 which give contrast optimal $(3,4)$-XVCS.

Let $S^0 = \begin{bmatrix} ..\ R_1^0\ .. \\ ..\ R_2^0\ .. \\ ..\ R_3^0\ .. \\ ..\ R_4^0\ .. \end{bmatrix}$ and $S^1 = \begin{bmatrix} ..\ R_1^1\ .. \\ ..\ R_2^1\ .. \\ ..\ R_3^1\ .. \\ ..\ R_4^1\ .. \end{bmatrix}$.

Now $\{1\} \cup F_6 = \{134\}$ and $\{2\} \cup F_6 = \{234\}$ are minimal qualified sets and hence

$$\left.\begin{array}{l} R_1^0 \oplus R_3^0 \oplus R_4^0 = \mathbf{0} \\ R_2^0 \oplus R_3^0 \oplus R_4^0 = \mathbf{0} \end{array}\right\} \quad \text{and} \quad \left.\begin{array}{l} R_1^1 \oplus R_3^1 \oplus R_4^1 = \mathbf{1} \\ R_2^1 \oplus R_3^1 \oplus R_4^1 = \mathbf{1} \end{array}\right\}$$

Moreover, we started with the minimal qualified set $\{123\}$ and therefore we have

$$R_1^0 \oplus R_2^0 \oplus R_3^0 = \mathbf{0}\,\} \qquad \text{and} \qquad R_1^1 \oplus R_2^1 \oplus R_3^1 = \mathbf{1}\,\}$$

Now, from the equations related to white pixel we get $R_3^0 = \mathbf{0}$ and from the equations related to black pixel we have $R_3^1 = \mathbf{1}$. Thus the third participant alone is able to recover the secret although he belongs to the forbidden set F_6. This contradiction shows that there can not be a contrast-optimal $(3,4)$-XVCS.

Keeping the above examples in mind we now proceed to prove the following proposition.

Proposition 3. *If the cumulative array for a most simplified access structure* $(\mathcal{Q}_{min}, \mathcal{F}_{max})$ *is non-Optimal then there cannot be a contrast-optimal XVCS realizing the access structure.*

Proof: Suppose there exists a construction method by which it is possible to have relative contrast 1.

Let the basis matrices be $S^0 = \begin{bmatrix} .. & R^0_1 & .. \\ .. & R^0_2 & .. \\ .. & .. & .. \\ .. & R^0_n & .. \end{bmatrix}$ and $S^1 = \begin{bmatrix} .. & R^1_1 & .. \\ .. & R^1_2 & .. \\ .. & .. & .. \\ .. & R^1_n & .. \end{bmatrix}$, where n is number of participants.

Now we know that the corresponding CA is not Optimal and therefore there exists at least one minimal qualified set say, B such that $CA[B]$ contains at least one non-zero even column. Let $F \in \mathcal{F}_{max}$ be that maximal forbidden set for which the column is of non-zero even weight. Let the weight be $2k$ where $k \neq 0$. Suppose $i_1, i_2, \ldots, i_{2k}$ be the corresponding parties in B but not in F. Let $B = \{i_1, i_2, \ldots, i_{2k}, j_1, j_2, \ldots, j_s\}$ such that the first $2k$ many parties are in $B \setminus F$. We have used different symbols $j_1, j_2, \ldots, j_s$ to denote the other parties in B, because it is possible that $B = \{i_1, i_2, \ldots, i_{2k}\}$ and there is no more parties in B (e.g. see Example 6).

Since F is maximal forbidden set and $i_1, i_2, \ldots, i_{2k} \notin F$ therefore $F \cup \{i_1\}$ contains at least one minimal qualified set, $F \cup \{i_2\}$ contains at least one minimal qualified set, ..., $F \cup \{i_{2k}\}$ contains at least one minimal qualified set. We note that these minimal qualified sets respectively contain $i_1, i_2, \ldots, i_{2k}$. Let the minimal qualified sets be respectively,

$\{f^1_1, f^1_2, \ldots, f^1_{\alpha(1)}, i_1\}, \ \{f^2_1, f^2_2, \ldots, f^2_{\alpha(2)}, i_2\}, \ \ldots, \ \{f^{2k}_1, f^{2k}_2, \ldots, f^{2k}_{\alpha(2k)}, i_{2k}\}$.

Thus we must have the following sets of equations (and using the fact of optimal relative contrast)

$$\left.\begin{array}{ll} R^0_{f^1_1} \oplus R^0_{f^1_2} \oplus \ldots \oplus R^0_{f^1_{\alpha(1)}} \oplus R^0_{i_1} & = \mathbf{0} \\ R^0_{f^2_1} \oplus R^0_{f^2_2} \oplus \ldots \oplus R^0_{f^2_{\alpha(2)}} \oplus R^0_{i_2} & = \mathbf{0} \\ \ldots\ldots & \\ R^0_{f^{2k}_1} \oplus R^0_{f^{2k}_2} \oplus \ldots \oplus R^0_{f^{2k}_{\alpha(2k)}} \oplus R^0_{i_{2k}} & = \mathbf{0} \end{array}\right\}$$

and

$$\left.\begin{array}{ll} R^1_{f^1_1} \oplus R^1_{f^1_2} \oplus \ldots \oplus R^1_{f^1_{\alpha(1)}} \oplus R^1_{i_1} & = \mathbf{1} \\ R^1_{f^2_1} \oplus R^1_{f^2_2} \oplus \ldots \oplus R^1_{f^2_{\alpha(2)}} \oplus R^1_{i_2} & = \mathbf{1} \\ \ldots\ldots & \\ R^1_{f^{2k}_1} \oplus R^1_{f^{2k}_2} \oplus \ldots \oplus R^1_{f^{2k}_{\alpha(2k)}} \oplus R^1_{i_{2k}} & = \mathbf{1} \end{array}\right\}$$

Notice that there are $2k$ many equations in each set and the rows $R^0_{i_1}, R^0_{i_2}, \ldots, R^0_{i_{2k}}$ corresponding to $i_1, i_2, \ldots, i_{2k}$ occur exactly once in each set. Rows other than these are shares corresponding to the parties in F.

Last we have two more sets of equations corresponding to the parties B,

$$R^0_{i_1} \oplus \ldots \oplus R^0_{i_{2k}} \oplus R^0_{j_1} \oplus \ldots \oplus R^0_{j_s} = \mathbf{0} \ , \ R^1_{i_1} \oplus \ldots \oplus R^1_{i_{2k}} \oplus R^1_{j_1} \oplus \ldots \oplus R^1_{j_s} = \mathbf{1}$$

We observe that $j_1, j_2, \ldots, j_s \in F$ and there are $(2k+1)$ (odd) many equations for each set. Adding modulo 2 i.e. taking XOR of all the equations corresponding to white pixel 0 we observe that the rows indexed by $i_1, i_2, \ldots, i_{2k}$ are deleted. Same thing happens with the equations corresponding to black pixel 1. Whatever rows we are left with, all are indexed by the parties in F. There are only two possibilities. Either the equations have inconsistency (as in Example 6) or a forbidden set of parties are able to retrieve the secret image (as in Example 7). These contradictions show that we cannot have such basis matrices which give optimal contrast for an access structure whose CA is not Optimal. This completes the proof of the proposition.

By Construction 1, Propositions 2 and 3 we now conclude that

Theorem 1. *A necessary and sufficient condition for* $(\mathcal{Q}_{min}, \mathcal{F}_{max})$*-XVCS to achieve optimum relative contrast* 1 *is that the corresponding cumulative array of* $\mathcal{Q}_{min}$ *is* **OPTIMAL***, where the access structure* $(\mathcal{Q}_{min}, \mathcal{F}_{max})$ *is in its* **most simplified form***.*

From the first *Observation* following Proposition 1 and from Theorem 1 we now have the following corollary.

Corollary 1. *For* $2 \leq k \leq n-1$*, there does not exist* (k, n)*-XVCS that can achieve optimal relative contrast* 1*.*

Acknowledgement. Research of the second author is partially supported by National Board for Higher Mathematics, Department of Atomic Energy, Government of India, Grant No. 2/48(10)/2013/NBHM(R.P.)/R&D II/695.

References

1. Adhikari, A.: Linear algebraic techniques to construct monochrome visual cryptographic schemes for general access structure and its applications to color images. Des. Codes Crypt. **73**(3), 865–895 (2014)
2. Adhikari, A., Bose, M.: A new visual cryptographic scheme using latin squares. IEICE Trans. Fundam. Electron. Commun. Comput. Sci. **87**(5), 1198–1202 (2004)
3. Adhikari, A., Dutta, T.K., Roy, B.: A new black and white visual cryptographic scheme for general access structures. In: Canteaut, A., Viswanathan, K. (eds.) INDOCRYPT 2004. LNCS, vol. 3348, pp. 399–413. Springer, Heidelberg (2004). https://doi.org/10.1007/978-3-540-30556-9_31
4. Adhikari, A., Bose, M., Kumar, D., Roy, B.K.: Applications of partially balanced incomplete block designs in developing (2, n) visual cryptographic schemes. IEICE Trans. **90-A**(5), 949–951 (2007)
5. Adhikari, A., Roy, B.: On some constructions of monochrome visual cryptographic schemes. In: 1st International Conference on Information Technology, IT 2008, pp. 1–6. IEEE (2008)
6. Arumugam, S., Lakshmanan, R., Nagar, A.K.: On (k, n)*-visual cryptography scheme. Des. Codes Crypt. **71**(1), 153–162 (2014)
7. Ateniese, G., Blundo, C., Santis, A.D., Stinson, D.R.: Visual cryptography for general access structures. Inf. Comput. **129**, 86–106 (1996)

8. Ateniese, G., Blundo, C., De Santis, A., Stinson, D.R.: Constructions and bounds for visual cryptography. In: Meyer, F., Monien, B. (eds.) ICALP 1996. LNCS, vol. 1099, pp. 416–428. Springer, Heidelberg (1996). https://doi.org/10.1007/3-540-61440-0_147
9. Blundo, C., D'arco, P., De Santis, A., Stinson, D.R.: Contrast optimal threshold visual cryptography. SIAM J. Discrete Math. **16**(2), 224–261 (2003)
10. Droste, S.: New results on visual cryptography. In: Koblitz, N. (ed.) CRYPTO 1996. LNCS, vol. 1109, pp. 401–415. Springer, Heidelberg (1996). https://doi.org/10.1007/3-540-68697-5_30
11. Dutta, S., Adhikari, A.: XOR based non-monotone t-$(k, n)^*$-visual cryptographic schemes using linear algebra. In: Hui, L.C.K., Qing, S.H., Shi, E., Yiu, S.M. (eds.) ICICS 2014. LNCS, vol. 8958, pp. 230–242. Springer, Cham (2015). https://doi.org/10.1007/978-3-319-21966-0_17
12. Dutta, S., Singh Rohit, R., Adhikari, A.: Constructions and analysis of some efficient t-$(k, n)^*$-visual cryptographic schemes using linear algebraic techniques. Des. Codes Crypt. **80**(1), 165–196 (2016). Springer
13. Fu, Z., Yu, B.: Optimal pixel expansion of deterministic visual cryptography scheme. Multimedia Tools Appl. **73**(3), 1177–1193 (2014)
14. Guo, T., Liu, F., Wu, C.K., Ren, Y.W., Wang, W.: On (k, n) visual cryptography scheme with t essential parties. In: Padró, C. (ed.) ICITS 2013. LNCS, vol. 8317, pp. 56–68. Springer, Cham (2014). https://doi.org/10.1007/978-3-319-04268-8_4
15. Hao, H., Shen, G., Zhengxin, F., Bin, Y., Wang, J.: General construction for XOR-based visual cryptography and its extended capability. Multimedia Tools Appl. **75**(21), 13883–13911 (2016)
16. Kafri, O., Keren, E.: Encryption of pictures and shapes by random grids. Opt. Lett. **12**(6), 377–379 (1987)
17. Lee, S.S., Na, J.C., Sohn, S.W., Park, C., Seo, D.H., Kim, S.J.: Visual cryptography based on an interferometric encryption technique. ETRI J. **24**(5), 373–380 (2002)
18. Liu, F., Wu, C.K., Lin, X.J.: Some extensions on threshold visual cryptography schemes. Comput. J. **53**, 107–119 (2010)
19. Liu, F., Wu, C., Lin, X.: Step construction of visual cryptography schemes. IEEE Trans. Inf. Forensics Secur. **5**, 27–38 (2010)
20. Naor, M., Shamir, A.: Visual cryptography. In: De Santis, A. (ed.) EUROCRYPT 1994. LNCS, vol. 950, pp. 1–12. Springer, Heidelberg (1995). https://doi.org/10.1007/BFb0053419
21. Shyu, S.J., Chen, M.C.: Optimum pixel expansions for threshold visual secret sharing schemes. IEEE Trans. Inf. Forensics Secur. **6**(3), pt. 2, 960–969 (2011)
22. Tuyls, P., Hollmann, H.D.L., Lint, H.H., Tolhuizen, L.: A polarisation based visual crypto system and its secret sharing schemes (2002), http://eprint.iacr.org
23. Tuyls, P., Hollmann, H., Lint, J., Tolhuizen, L.: Xor-based visual cryptography schemes. Des. Codes Crypt. **37**, 169–186 (2005)
24. Viet, D.Q., Kurosawa, K.: Almost ideal contrast visual cryptography with reversing. In: Okamoto, T. (ed.) CT-RSA 2004. LNCS, vol. 2964, pp. 353–365. Springer, Heidelberg (2004). https://doi.org/10.1007/978-3-540-24660-2_27
25. Yang, C.-N., Wang, D.-S.: Property analysis of XOR-based visual cryptography. IEEE Trans. Circ. Syst. Video Technol. **24**(2), 189–197 (2014)