Des. Codes Cryptogr. (2016) 80:165–196
DOI 10.1007/s10623-015-0075-5

Constructions and analysis of some efficient t-$(k, n)^*$-visual cryptographic schemes using linear algebraic techniques

Sabyasachi Dutta[1] · **Raghvendra Singh Rohit**[2] · **Avishek Adhikari**[1]

Received: 29 April 2014 / Revised: 3 January 2015 / Accepted: 25 March 2015 /
Published online: 8 April 2015

Abstract In this paper we put forward an efficient construction, based on linear algebraic technique, of a t-$(k, n)^*$-visual cryptographic scheme (VCS) for monochrome images in which t participants are essential in a (k, n)-VCS. The scheme is efficient in the sense that it only requires solving a system of linear equations to construct the required initial basis matrices. To make the scheme more efficient, we apply the technique of deletion of common columns from the initial basis matrices to obtain the reduced basis matrices. However finding exact number of common columns in the initial basis matrices is a challenging problem. In this paper we deal with this problem. We first provide a construction and analysis of t-$(k, n)^*$-VCS. We completely characterize the case of t-$(n-1, n)^*$-VCS, $0 \leq t \leq n-1$, by finding a closed form of the exact number of common columns in the initial basis matrices and thereby deleting the common columns to get the exact value of the reduced pixel expansion and relative contrast of the efficient and simple scheme. Our proposed closed form for reduced pixel expansion of $(n-1, n)$-VCS matches with the numerical values of the optimal pixel expansions for every possible values of n that exist in the literature. We further deal with the $(n-2, n)$-VCS and resolve an open issue by providing an efficient algorithm for grouping the system of linear equations and thereby show that our proposed algorithm works better than the existing scheme based on the linear algebraic technique. Finally we provide a bound

Communicated by C. Blundo.

✉ Avishek Adhikari
avishek.adh@gmail.com

Sabyasachi Dutta
saby.math@gmail.com

Raghvendra Singh Rohit
raghvendra11077@iiserkol.ac.in

[1] Department of Pure Mathematics, University of Calcutta, 35 Ballygunge Circular Road, Kolkata 700019, India

[2] Indian Institute of Science Education & Research Kolkata, D-313 ICVS Hostel IISER-Kolkata, PO Haringhata, Nadia 741246, West Bengal, India

for reduced pixel expansion for $(n-2, n)$-VCS and numerical evidence shows it achieves almost optimal pixel expansion.

Keywords Linear algebra · Pixel expansion · Relative contrast · System of linear equations

Mathematics Subject Classification 15A03 · 94A60

1 Introduction

A visual cryptographic scheme (VCS) for a set $\mathcal{P} = \{1, 2, \ldots, n\}$ of n participants is a method that encodes a secret image SI into n shares which are distributed among n participants 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 novelty of visual cryptography lies in the fact that the encrypted message can be decrypted directly by the human visual system, no complex computation or computer participation is required. This is the precise reason of VCS attracting a lot of attention since its inception and as a result extensive research work has been done in this area. Researchers have worked through different aspects of VCS. Definitions have been modified, changed according to the need for different applications.

The most general type of VCS deals with the situation when the "qualified" subsets of participants are just handpicked subsets of the set of participants $\mathcal{P}$. This type of visual cryptographic scheme is known as VCS for general access structure. One particular case, known as a (k, n)-threshold VCS, takes care of the scenario where any "qualified" set X of participants is a subset of $\mathcal{P}$ i.e., $X \subseteq \mathcal{P}$, such that the cardinality of X is at least k. In this case, any qualified subset of k or more participants can visually recover the secret image, whereas forbidden sets of participants consisting of $k-1$ or less number of participants have no information on the secret image.

Originally developed by Naor and Shamir [20], this concept has been extended in [1,4,7,8] to general access structures. In 1996 Droste [17] gave a brilliant algorithm and used linear program to construct basis matrices of any (k, n)-threshold VCS. In search for optimal contrast Blundo et al., [12] resorted to the LPP. They, for the first time, defined canonical form for a (k, n)-threshold VCS and analyzed the contrast for these schemes.

The idea of optimizing the pixel expansion of an VCS with the help of integer linear programming (ILP) was put forward by Blundo and De Santis [9]. However they did not implement it to get computational results. In 2011 Shyu and Chen [23] modeled the minimization of the pixel expansion of a (k, n)-threshold VCS into an ILP to acquire the optimum solution.

Adhikari et al., [4] proposed a technique to construct any (k, n)-threshold VCS using linear algebra. The technique is useful even for the case when k is large enough. However the question of optimality of pixel expansion was left open.

For other interesting and further studies in this area one may refer to [2,3,5,10,11,13,15,16,18,21,22,24,25].

Recently, a new type of VCS has been introduced [6] called a $(k, n)^*$-VCS. It addresses the scenario where one participant is "essential". Loosely speaking, in this scenario a black and white secret image is shared among n many participants in such a way that the following two conditions are satisfied while reconstructing the secret image from the shares:

- One participant is essential in the sense that his presence is necessary to retrieve the secret image. In other words the secret image cannot be retrieved in his absence.

- It is required to have the shares of at least k participants including the essential participant to recover the secret image.

Guo et al. [14] forwarded the work $(k, n)^*$-VCS of [6] by considering (k, n)-VCS with t essential participants. We denote this by the notation t-$(k, n)^*$-VCS. Note that in the paper [14], the authors denote (k, n)-VCS with t essential participants as (k, n, t)-VCS. However, to keep parity with the original paper [6], we adopt the notation t-$(k, n)^*$-VCS for $0 \leq t \leq k \leq n$. Thus for $0 \leq t \leq k \leq n$ and $\mathcal{P} = \{1, 2, 3, \ldots, n\}$, the collection of all minimal qualified sets for the t-$(k, n)^*$-VCS, denoted by Γ_0 is given by $\Gamma_0 = \{S \subseteq \mathcal{P} : 1, 2, \ldots, t \in S \wedge |S| = k\}$.

Note that the case when $t = 0$ depicts the original 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.

The scheme proposed in [14] for t-$(k, n)^*$-VCS generalizes the 1-$(k, n)^*$-VCS proposed in [6]. However, both of the schemes are based on the construction of (k, n)-VCS. In this paper we put forward an efficient but direct construction, based on linear algebraic technique, of a t-$(k, n)^*$-VCS for monochrome images. The scheme is efficient in the sense that it only requires solving a system of linear equations to construct the required initial basis matrices. To make the scheme even more efficient, we apply the technique of deletion of common columns from the initial basis matrices to obtain the reduced basis matrices. However, as mentioned in [1], finding exact number of common columns in the initial basis matrices is a challenging problem. In this paper we deal with this open issue. We first provide a construction and analysis of t-$(k, n)^*$-VCS. We completely characterize the case of t-$(n-1, n)^*$-VCS, $0 \leq t \leq n-1$, by finding a closed form of the exact number of common columns in the initial basis matrices and thereby deleting the common columns to get the exact pixel expansion and the relative contrast of the efficient and simple scheme. As a particular case of t-$(n-1, n)^*$, we derive a closed form of the reduced pixel expansion of $(n-1, n)$-VCS. We show that for odd $n \geq 3$, our scheme has exactly half the pixel expansion but achieves the same relative contrast of the canonical scheme based on LPP posed in [12]. For even $n \geq 3$, our scheme has the same relative contrast and the pixel expansion as the scheme posed in [12]. Furthermore, our closed form for the reduced pixel expansion, as the numerical evidences in [23] show, indeed provides the optimal pixel expansion for $(n-1, n)$-VCS. We further deal with the $(n-2, n)$-VCS and resolve an open issue, as posed in [1], by providing an efficient algorithm for grouping the system of linear equations and thereby show that our proposed algorithm works better in terms of pixel expansion, than the existing scheme based on the linear algebraic technique. Finally the numerical evidences shows that our scheme provides almost optimal pixel expansion for $(n-2, n)$-VCS.

1.1 Organization of the paper

The rest of the paper is organized as follows. In Sect. 2 we discuss few terms and concepts that are essential. In Sect. 3 we describe a very efficient construction based on linear algebraic tools of a t-$(k, n)^*$-VCS where t many parties are essential. In Sect. 4 we deal with the particular case when the threshold number of participants is $n-1$ and in this process we derive a closed form of the reduced pixel expansion. We present the analysis of the reduced pixel expansion of any $(n-1, n)$-VCS and give a closed form of the same. In Sect. 5 we deal with $(n-2, n)$-VCS and provide an algorithm to group minimal qualified sets such that every group contains at least three sets. We also compare our scheme with existing schemes in terms of pixel expansion and prove some bounds. Lastly we conclude with some open issues in Sect. 6.

2 The model and the prerequisites for monochrome VCS

The model that we describe here is similar to the model as described in Blundo, De Santis, and Stinson [10]. Let $\mathcal{P} = \{1, \ldots, n\}$ be a set of elements called *participants*, and let $2^{\mathcal{P}}$ denote the set of all subsets of $\mathcal{P}$. Let Γ_{Qual} and Γ_{Forb} be subsets of $2^{\mathcal{P}}$, where $\Gamma_{Qual} \cap \Gamma_{Forb} = \emptyset$. We will refer to members of Γ_{Qual} as *qualified sets* and the members of Γ_{Forb} as *forbidden sets*. The pair $(\Gamma_{Qual}, \Gamma_{Forb})$ is called the *access structure* of the scheme. In general, $\Gamma_{Qual} \cup \Gamma_{Forb}$ need not be $2^{\mathcal{P}}$.

Let $\Gamma_0 = \{A \mid A \in \Gamma_{Qual} \wedge \forall A' \subset A, A' \notin \Gamma_{Qual}\}$ be the collection of all minimal qualified sets. A participant $P \in \mathcal{P}$ is an *essential* participant if there exists a set $X \subseteq \mathcal{P}$ such that $X \cup \{P\} \in \Gamma_{Qual}$ but $X \notin \Gamma_{Qual}$. If a participant $P \in \mathcal{P}$ is not an essential participant, then we call the participant as a non-essential participant.

Let $\Gamma \subseteq 2^{\mathcal{P}} \setminus \{\emptyset\}$ ($\Gamma \subseteq 2^{\mathcal{P}}$). If $A \in \Gamma$ and $A \subseteq A' \subseteq \mathcal{P}$ ($A' \subseteq A \subseteq \mathcal{P}$) implies $A' \in \Gamma$ then Γ is said to be monotone increasing (decreasing) on $\mathcal{P}$. If Γ_{Qual} is monotone increasing, Γ_{Forb} is monotone decreasing, and $\Gamma_{Qual} \cup \Gamma_{Forb} = 2^{\mathcal{P}}$, then the access structure is called *strong* and Γ_0 is called a *basis*. A visual cryptographic scheme with a strong access structure will be termed as a *strong visual cryptography scheme*. In this paper we deal with only strong access structures. Throughout this paper, we presume that $\Gamma_{Qual} \cup \Gamma_{Forb} = 2^{\mathcal{P}}$. So any $X \subseteq \mathcal{P}$ is either a qualified set or a forbidden set of participants.

We further assume that the secret image consists of a collection of black and white pixels, each pixel being shared separately. To understand the sharing process consider the case where the secret image consists of just a single black or white pixel. On sharing, this pixel appears in the n shares distributed to the participants. However, in each share the pixel is subdivided into m *subpixels*. This m is called the pixel expansion i.e., the number of pixels, on the transparencies corresponding to the shares (each such pixel is called subpixel), needed to represent one pixel of the original image. The shares are printed on transparencies. So a "white" subpixel is actually an area where nothing is printed, and left transparent. We assume that the subpixels are sufficiently small and close enough so that the eye averages them to some shade of grey.

In order that the recovered image is clearly discernible, it is important that the grey level of a black pixel be darker than that of a white pixel. Informally, the difference in the grey levels of the two pixel types is called *contrast*. We want the contrast to be as large as possible. Three variables control the perception of black and white regions in the recovered image: a threshold value (t), a relative contrast ($\alpha(m)$), and the pixel expansion (m). The *threshold value* is a numeric value that represents a grey level that is perceived by the human eye as the color black. The value $\alpha(m) \cdot m$ is the contrast, which we want to be as large as possible. We require that $\alpha(m) \cdot m \geq 1$ to ensure that black and white areas will be distinguishable.

Notations Consider an $n \times m$ Boolean matrix M and let $X \subseteq \{1, 2, \ldots, n\}$. By $M[X]$ we will denote the $|X| \times m$ submatrix obtained from M by retaining only the rows indexed by the elements of X. M_X will denote the Boolean "or" of the rows of $M[X]$. The *Hamming weight* $w(V)$ is the number of 1's in a Boolean vector V.

2.1 Basis matrices

To construct a visual cryptographic scheme, it is sufficient to construct the basis matrices corresponding to the black and white pixel. In the following, we formally define what is meant by basis matrices.

Definition 2.1 (*adapted from* [10]) Let $(\Gamma_{Qual}, \Gamma_{Forb})$ be an access structure on a set $\mathcal{P}$ of n participants. A $(\Gamma_{Qual}, \Gamma_{Forb}, m)$-VCS with relative difference $\alpha(m)$ and a set of thresholds $\{t_X\}_{X \in \Gamma_{Qual}}$ is realized using the $n \times m$ basis matrices S^0 and S^1 if the following two conditions hold:

1. If $X = \{i_1, i_2, \ldots, i_p\} \in \Gamma_{Qual}$, then S^0_X, the "or'' of the rows $i_1, i_2, \ldots, i_p$ of S^0, satisfies $w(S^0_X) \leq t_X - \alpha(m) \cdot m$; whereas, for S^1 it results in $w(S^1_X) \geq t_X$.
2. If $X = \{i_1, i_2, \ldots, i_p\} \in \Gamma_{Forb}$, the two $p \times m$ matrices obtained by restricting S^0 and S^1 to rows $i_1, i_2, \ldots, i_p$ are equal up to a column permutation.

3 Construction and analysis of some efficient t-$(k, n)^*$-VCS

Let $\mathcal{P} = \{1, 2, 3, \ldots, n\}$ be the set of participants. Let $0 \leq t \leq k \leq n$ be three integers where t denotes the number of essential participants, k denotes the threshold number of participants that is required to recover the secret image. Without loss of generality, let us assume that the first t participants, namely, $1, 2, \ldots, t$ are the essential participants.

We have not as such put any restriction on the parameters t, k and n other than $0 \leq t \leq k \leq n$. It is worth mentioning that we are interested in only those triplets (t, k, n) of parameters which admit a meaningful visual cryptographic scheme. For example, if $t = k$ then the only meaningful value that n may assume is k because if $n > k$ then the rest of the $n - k$ participants are non-essential and we can ignore them while sharing the secret. Again, if k equals n then $t = k = n$ or t equals n then all the participants are essential and the resulting scheme is again an (n, n)-VCS. The case when $t = 0$ with $n \geq k > 1$ is the original (k, n)-threshold VCS where no participant is essential and any k or more of them can recover the secret. Henceforth whenever we consider a triplet (t, k, n), it is a **meaningful triplet**. Moreover, it should be noted that once $(t - 1, k - 1, n - 1)$ is a meaningful triplet then so is (t, k, n).

We now describe a method for constructing the basis matrices realizing a t-$(k, n)^*$-VCS. The method is straightforward and efficient in the sense that it only requires solving a system of linear equations to construct the basis matrices. This method is an extension of linear algebraic method introduced by Adhikari et. al., in [4] and developed further in [1].

3.1 Construction of a t-$(k, n)^*$-VCS: linear algebraic technique

We associate to each participant i, a variable x_i for all $i = 1, 2, \ldots, n$. If X is a minimal qualified set for a t-$(k, n)^*$-VCS, then we must have each of $1, 2, \ldots, t \in X$ and $|X| = k$. Thus $\mathcal{P}$ has altogether $\binom{n-t}{k-t}$ such subsets. Based on the lexicographic ordering we arrange the subsets as follows: $B_1, B_2, \ldots, B_r$ where $r = \binom{n-t}{k-t}$. For example, if $\mathcal{P} = \{1, 2, 3, \ldots, 6\}, t = 2$ and $k = 4$ then $B_1 = \{1, 2, 3, 4\}$, $B_2 = \{1, 2, 3, 5\}$, $B_3 = \{1, 2, 3, 6\}$, $B_4 = \{1, 2, 4, 5\}$, $B_5 = \{1, 2, 4, 6\}$ and $B_6 = \{1, 2, 5, 6\}$.

Let us pair the consecutive subsets, except for the last subset B_r if r is odd, to form $\lfloor \frac{r}{2} \rfloor$ groups. For odd r, the last group will contain only one set, B_r itself. Thus, ultimately for any r, we have $\lceil \frac{r}{2} \rceil$ many groups.

The groups for 2-$(4, 6)^*$-VCS are as follows:

Group 1: (B_1, B_2); Group 2: (B_3, B_4); and Group 3: (B_5, B_6).

In general, the i-th group can be described as follows:

$$i\text{th Group} = \begin{cases} (B_{2i-1}, B_{2i}), & \text{for } 1 \le i \le \lceil \frac{r-2}{2} \rceil, \text{ and any } n > 2; \\ (B_{r-1}, B_r), & \text{for even } r > 2 \text{ and } i = \frac{r}{2}; \\ (B_r), & \text{for odd } r > 2 \text{ and } i = \lceil \frac{r}{2} \rceil. \end{cases}$$

Let us denote by $f_{B_j} = 0$, the linear equation $\sum_{k \in B_j} x_k = 0$ and by $f_{B_j} = 1$, the linear equation $\sum_{k \in B_j} x_k = 1$.

We consider the following systems of linear equations over the binary field $\mathbb{Z}_2$:
For $1 \le i \le \lceil \frac{r-2}{2} \rceil$ and for any $r \ge 3$,

$$\left.\begin{matrix} f_{B_{2i-1}} = 0 \\ f_{B_{2i}} = 0 \end{matrix}\right\} \cdots (i) \quad \text{and} \quad \left.\begin{matrix} f_{B_{2i-1}} = 1 \\ f_{B_{2i}} = 1 \end{matrix}\right\} \cdots (i')$$

For $i = \frac{r}{2}$ and for even $r > 3$,

$$\left.\begin{matrix} f_{B_{r-1}} = 0 \\ f_{B_r} = 0 \end{matrix}\right\} \cdots \left(\frac{r}{2}\right) \quad \text{and} \quad \left.\begin{matrix} f_{B_{r-1}} = 1 \\ f_{B_r} = 1 \end{matrix}\right\} \cdots \left(\frac{r'}{2}\right)$$

For $i = \lceil \frac{r}{2} \rceil$ and for odd $r \ge 3$,

$$f_{B_r} = 0 \} \cdots \left(\left\lceil \frac{r}{2} \right\rceil\right) \quad \text{and} \quad f_{B_r} = 1 \} \cdots \left(\left\lceil \frac{r'}{2} \right\rceil\right)$$

Let for any $r \ge 3$ and $1 \le i \le \lceil \frac{r-2}{2} \rceil$, S_i^0 and S_i^1 denote the Boolean matrices whose columns are all possible solutions of the equations (i) and (i') respectively. Similarly, for any even (odd) $r \ge 3$, $S_{\frac{r}{2}}^0$ $(S_{\lceil \frac{r}{2} \rceil}^0)$ and $S_{\lceil \frac{r}{2} \rceil}^1$ $(S_{\lceil \frac{r}{2} \rceil}^1)$ denote the Boolean matrices corresponding the solutions of the equations $(\frac{r}{2})((\lceil \frac{r}{2} \rceil))$ and $(\frac{r'}{2})(\lceil \frac{r'}{2} \rceil)$ respectively.

Let (S_{in}^0, S_{in}^1) denote the pair of Boolean matrices obtained by the concatenations: $S_{in}^0 = S_1^0 || S_2^0 || \cdots || S_{\lceil \frac{r}{2} \rceil}^0$ and $S_{in}^1 = S_1^1 || S_2^1 || \cdots || S_{\lceil \frac{r}{2} \rceil}^1$.

The pair of matrices S_{in}^0 and S_{in}^1, thus obtained, constitutes the basis matrices of the t-$(k, n)^*$-VCS. This result follows from a more general result viz., Theorem 2.1 in [1]. For the sake of completeness we present an easier and shorter proof of the fact. Towards proving the results we need the following facts.

Fact 1: It is a very well known fact from linear algebra that if we consider two systems of linear equations $Ax = 0$ and $Ax = b$ where $b \ne 0$, then all possible solutions of the second system can be obtained by adding (i.e, addition of solution vectors) one particular solution of the second system to each solution of the first system.

Result 1: The way we have constructed S^0 and S^1 it is now easy to see that each block S_i^1 can be obtained from S_i^0 by adding a particular solution of the system (i') to each column of S_i^0.

Theorem 3.1 *The pair of matrices* (S^0, S^1) *obtained by the above algorithm, constitute basis matrices of the* t-$(k, n)^*$-*VCS.*

Proof Let m denote the pixel expansion which is the number of columns occuring in S^0 or S^1. We need to prove the following:

1. If X is a qualified set of participants then $w(S_X^1) - w(S_X^0) \ge \alpha_X \cdot m$.
2. If $Y \subset \mathcal{P}$ is a forbidden set of participants then $S^0[Y]$ and $S^1[Y]$ are identical up to column permutation.

Let us denote $\lceil \frac{r}{2} \rceil$ by p.

First we prove the second condition viz., the security condition. Let $Y = \{i_1, i_2, \ldots, i_s\}$ be a forbidden set. We want to show that $S^0[Y]$ and $S^1[Y]$ are identical up to a column permutation. Thus it is sufficient to prove that

$$\begin{cases} S_1^0[Y] \text{ and } S_1^1[Y] \text{ are identical up to a column permutation} \\ S_2^0[Y] \text{ and } S_2^1[Y] \text{ are identical up to a column permutation} \\ \ldots \\ S_p^0[Y] \text{ and } S_p^1[Y] \text{ are identical up to a column permutation} \end{cases}$$

We will prove only for $S_1^0[Y]$ and $S_1^1[Y]$. Rest of them follow in the same manner. Recall that each column of S_1^0 and S_1^1 is a solution of the systems (1) and (1′) respectively such that the variables that are not present in any of the equations are all set equal to zero. Therefore, if we can prove that there exists a particular solution of the system (1′), say $\mathbf{c} = (c_1, c_2, \ldots, c_n)$ such that $c_j = 0$ for $j = i_1, i_2, \ldots, i_s$ then by *Result 1*, the restricted matrices $S^0[Y]$ and $S^1[Y]$ are identical up to a column permutation. Now, since Y is a forbidden set of participants therefore $B_i \nsubseteq Y$ for $i = 1, 2$ because otherwise, Y would contain a minimal qualified set and would itself become a qualified set. Suppose μ and σ be two such indices (that is, participants) such that $\mu \in B_1$ and $\sigma \in B_2$ but $\mu, \sigma \notin Y$. If $\mu = \sigma$ then $c_\mu = 1$ and $c_i = 0$ for all $i \neq \mu$, admits a particular solution to (1′). On the other hand if $\mu \neq \sigma$ then $c_\mu = c_\sigma = 1$ and $c_i = 0$ for all $i \neq \mu, \sigma$ gives rise to a particular solution to (1′). In both cases $c_j = 0$ for $j = i_1, i_2, \ldots, i_s$ and hence the proof follows.

In the same manner we can prove that $S_i^0[Y]$ and $S_i^1[Y]$ are identical up to a column permutation for all $i = 1, 2, \ldots, p$. Hence the matrices $S^0[Y]$ and $S^1[Y]$ are identical up to a column permutation. This proves the security condition.

To prove the first condition that is, the contrast condition let us consider a minimal qualified set X. Then $X = B_j$ for some $1 \leq j \leq r$, where the symbols have their usual meanings. For $S^0[X]$ let us break it up in $S_1^0[X] \| S_2^0[X] \| \cdots \| S_p^0[X]$ and for $S^1[X]$, in $S_1^1[X] \| S_2^1[X] \| \cdots \| S_p^1[X]$.

Without loss of generality, let $X = B_1 = \{1, 2, 3, \ldots, t, t+1, \ldots, k\}$. Let us now consider $S^0[X]$ and $S^1[X]$ that is, we restrict ourselves on the first k rows of the matrices. It is not hard to see that each restricted column c_X say, $(c_1, c_2, \ldots, c_k)^t$ of $S_1^0[X]$ is a solution of the homogeneous system (1) and thus there exists a all zero solution. On the other hand there does not exist an all zero solution to the non-homogeneous system (1′) and hence $w(S_{1[X]}^1) - w(S_{1[X]}^0) \geq 1$. Now since $X \neq B_j$, $j \neq 1$, therefore we argue in a similar manner as for the *security condition* to get that $S_{j, j\neq 1}^0[X]$ and $S_{j, j\neq 1}^1[X]$ are identical up to column permutation and hence $w(S_{j[X]}^0) - w(S_{j[X]}^1) = 0$ for all $j \neq 1$. Taking $\alpha_X = \frac{1}{m}$, it is easy to see that $w(S_X^1) - w(S_X^0) \geq \alpha_X \cdot m = 1$. The above technique works for any minimal qualified set X. This completes the proof of the theorem. □

Remark Notice that the construction is direct, that is, the basis matrices can be directly constructed given any meaningful triplet of parameters (t, k, n).

Example 3.1 If $\mathcal{P} = \{1, 2, 3, 4, 5, 6\}$, $t = 2$ and $k = 4$ then the minimal qualified subsets of participants are $B_1 = \{1, 2, 3, 4\}$, $B_2 = \{1, 2, 3, 5\}$, $B_3 = \{1, 2, 3, 6\}$, $B_4 = \{1, 2, 4, 5\}$, $B_5 = \{1, 2, 4, 6\}$, $B_6 = \{1, 2, 5, 6\}$.

The basis matrices for the 2-$(4, 6)^*$-VCS following the above construction rule are given by

$$S_{in}^0 = \begin{bmatrix} \leftarrow \text{Col 1 to 8} \rightarrow & \leftarrow \text{Col 9 to 24} \rightarrow & \leftarrow \text{Col 24 to 32} \rightarrow \\ 00001111 & 0000000011111111 & 00001111 \\ 00110011 & 0000111100001111 & 00110011 \\ 01010101 & 0011001100110011 & 00000000 \\ 01101001 & 0101010101010101 & 01101001 \\ 01101001 & 0101101010100101 & 01101001 \\ 00000000 & 0011110011000011 & 01010101 \end{bmatrix} \quad \textit{and}$$

$$S_{in}^1 = \begin{bmatrix} \leftarrow \text{Col 1 to 8} \rightarrow & \leftarrow \text{Col 9 to 24} \rightarrow & \leftarrow \text{Col 24 to 32} \rightarrow \\ 11110000 & 1111111100000000 & 11110000 \\ 00110011 & 0000111100001111 & 00110011 \\ 01010101 & 0011001100110011 & 00000000 \\ 01101001 & 0101010101010101 & 01101001 \\ 01101001 & 0101101010100101 & 01101001 \\ 00000000 & 0011110011000011 & 01010101 \end{bmatrix}$$

Remark The basis matrices S_{in}^0 and S_{in}^1 thus constructed may have common columns. We call these basis matrices as initial basis matrices and the corresponding pixel expansion as initial pixel expansion. In [1] the author pointed out that the common columns appearing in the initial basis matrices S_{in}^0 and S_{in}^1 may be deleted to obtain reduced basis matrices denoted by S_{red}^0 and S_{red}^1. This method reduces the pixel expansion (we call it as reduced pixel expansion) and thereby increases the relative contrast significantly. In the next section, we adopt this technique to analyze the construction technique of any t-$(k, n)^*$-VCS to get the reduced pixel expansion.

3.2 Analysis of t-$(k, n)^*$-VCS

The following discussion establishes the relationship between the pixel expansions and relative contrasts of a higher order VCS and a lower order VCS constructed by the linear algebraic method. In [14] such a discussion is given but when the difference between k and t is strictly greater than one. However, our construction method includes all the possibilities. In the following lemma we first establish the relationship between the initial pixel expansions of a higher order VCS and lower order VCS.

Lemma 1 *Suppose* $(t-1, k-1, n-1)$ *represents a meaningful triplet. Let* $m_{in}(t-1, k-1, n-1)$ *denote the initial pixel expansion of a* $(t-1)$-$(k-1, n-1)^*$*-VCS constructed by the linear algebraic method described above. Then the* t-$(k, n)^*$*-VCS constructed using linear algebra has initial pixel expansion* $2m_{in}(t-1, k-1, n-1)$.

Proof Suppose the set of participants for $(t-1)$-$(k-1, n-1)^*$-VCS is $\mathcal{P} = \{2, 3, \ldots, n\}$, where the participants $2, 3, \ldots, t$ are the essential participants. To construct a t-$(k, n)^*$-VCS, we add another essential participant 1 to the set of participants. The new set of participants becomes $\bar{\mathcal{P}} = \{1, 2, 3, \ldots, n\}$ and the basis matrices for t-$(k, n)^*$-VCS are constructed by solving the set of linear equations same as those for the $(t-1)$-$(k-1, n-1)^*$-VCS with the modification that the new variable x_1 is added to the left hand side of each of the linear equations. Since x_1 appears in each of the equations and that x_1 can have two distinct values 0 and 1, therefore the initial pixel expansion of the t-$(k, n)^*$-VCS is exactly twice the initial pixel expansion of $(t-1)$-$(k-1, n-1)^*$-VCS. □

In the following lemma we show a relationship between the number of common columns appearing in the initial basis matrices of a lower order VCS and a higher order VCS. Deleting those common columns will reduce the pixel expansion of the schemes and we establish a relation between the reduced pixel expansions.

Lemma 2 *Let* $(t-1, k-1, n-1)$ *represent a meaningful triplet. Let* $m_{red}(t-1, k-1, n-1)$ *denote the reduced pixel expansion of a* $(t-1)$-$(k-1, n-1)^*$*-VCS constructed by the linear algebraic method. Then the* t-$(k, n)^*$*-VCS constructed using linear algebra has reduced pixel expansion* $2m_{red}(t-1, k-1, n-1)$.

Proof It suffices to show that the number of common columns occurring in the initial basis matrices of t-$(k, n)^*$-VCS is exactly twice to that of $(t-1)$-$(k-1, n-1)^*$-VCS. Suppose c is a common column occurring in the initial basis matrices of $(t-1)$-$(k-1, n-1)^*$-VCS. Corresponding to this c, by Lemma 1, two columns appear in each of the basis matrices of t-$(k, n)^*$-VCS, namely the columns $(0, c)$ and $(1, c)$. Since c is a common column that occurs in the basis matrices of the $(t-1)$-$(k-1, n-1)^*$-VCS, c must satisfy both the systems, for some i and j with $i \neq j$, as given below:

$$\left.\begin{aligned} f_{B_{2i-1}} &= 0 \\ f_{B_{2i}} &= 0 \end{aligned}\right\} \quad \text{and} \quad \left.\begin{aligned} f_{B_{2j-1}} &= 1 \\ f_{B_{2j}} &= 1 \end{aligned}\right\}$$

Then it is easy to see that $(0, c)$ is solution to both the systems

$$\left.\begin{aligned} x_1 + f_{B_{2i-1}} &= 0 \\ x_1 + f_{B_{2i}} &= 0 \end{aligned}\right\} \quad \text{and} \quad \left.\begin{aligned} x_1 + f_{B_{2j-1}} &= 1 \\ x_1 + f_{B_{2j}} &= 1 \end{aligned}\right\}$$

corresponding to the access structure of t-$(k, n)^*$-VCS. Similarly $(1, c)$ is also a common column. Now the proof follows. □

The following theorem is immediate.

Theorem 3.2 *Let* (t, k, n) *be a meaningful triplet such that* $(0, k-t, n-t)$ *is also meaningful. Let the pixel expansion and relative contrast of the* 0-$(k-t, n-t)^*$*-VCS be* m *and* α *respectively. Then the pixel expansion and relative contrast of the* t-$(k, n)^*$*-VCS will be* $2^t m$ *and* $\frac{\alpha}{2^t}$ *respectively.*

Corollary *It is immediate that if* m^* *be the optimal pixel expansion and* α^* *be the optimal relative contrast of a* t-$(k, n)^*$*-VCS then* $m^* \leq 2^t m$ *and* $\alpha^* \geq \frac{\alpha}{2^t}$ *where* m *is pixel expansion and* α *is relative contrast of the* 0-$(k-t, n-t)^*$*-VCS.*

Remark A version of Theorem 4 in [14] can be derived from Theorem 3.2. So in particular, a version of Theorem 2.3 in [6] may also be derived by setting $t = 1$.

The following section deals with the scenario when $k - t = 1$. In this process we are able to address the following issues. The method of construction adopted in [14] constructs the basis matrices of a higher order t-$(k, n)^*$-VCS out of the basis matrices of a $(k-t, n-t)$-VCS and basis matrices of an optimal (t, t)-VCS. Hence, as the authors pointed out, Corollary 1 and Corollary 2 to Theorem 4 in [14] hold true if $k - t \geq 2$. Our construction method is direct and this enables to circumvent this obstacle when the difference between k and t is equal to 1. On the other hand we generalize the $(2, n)^*$-VCS in [6] to the case when there are t many essential parties. Moreover, in [1], the author pointed out an interesting question whether or not collecting three or more equations at a time gives better result in terms of pixel expansion while constructing a VCS for general access structure. We resolve the issue for $(k-1)$-$(k, n)^*$-VCS by considering three or more equations at a time to obtain better results in terms of pixel expansion and relative contrast.

3.2.1 On construction of $(k-1)$-$(k,n)^*$-VCS

Let us consider a restricted (k,n)-VCS having $k-1$ essential participants. In this case the minimal qualified sets are $\{1,\ldots,k-1,k\}, \{1,\ldots,k-1,k+1\}, \{1,\ldots,k-1,k+2\},\ldots,\{1,\ldots,k-1,n-1\}, \{1,\ldots,k-1,n\}$. Observe that taking any number of equations at a time does not affect the security and contrast conditions of a visual cryptography scheme. We need not take two equations at a time to form groups of linear equations. We may take all the equations at a time forming only one group and the values of the variables $x_1, x_2, \ldots, x_{k-1}$ determine the values of the rest of the variables. In this scenario the pixel expansion thus becomes 2^{k-1}. We start with an example for better understanding.

Example 3.2 Consider 3-$(4,7)^*$-VCS. Here, $\Gamma_0 = \{\{1,2,3,4\},\{1,2,3,5\},\{1,2,3,6\},\{1,2,3,7\}\}$. To construct the 3-$(4,7)^*$-VCS, we consider the following system of linear equations over the binary field $\mathbb{Z}_2$. The first system is a homogeneous system of equations and the latter one is a non-homogeneous system of equations.

$$\begin{cases} x_1+x_2+x_3+x_4=0 \\ x_1+x_2+x_3+x_5=0 \\ x_1+x_2+x_3+x_6=0 \\ x_1+x_2+x_3+x_7=0 \end{cases} \tag{1}$$

$$\begin{cases} x_1+x_2+x_3+x_4=1 \\ x_1+x_2+x_3+x_5=1 \\ x_1+x_2+x_3+x_6=1 \\ x_1+x_2+x_3+x_7=1 \end{cases} \tag{2}$$

The solution of the above systems admits the following basis matrices:

$$S^0 = \begin{bmatrix} 00001111 \\ 00110011 \\ 01010101 \\ 01101001 \\ 01101001 \\ 01101001 \\ 01101001 \end{bmatrix} \quad and \quad S^1 = \begin{bmatrix} 11110000 \\ 00110011 \\ 01010101 \\ 01101001 \\ 01101001 \\ 01101001 \\ 01101001 \end{bmatrix}.$$

The pixel expansion is 8 and the relative contrast is $\frac{1}{8}$.

Looking at the above example we now prove the following theorem.

Theorem 3.3 *For a meaningful triplet (t,k,n) with $t=k-1$, there exists a $(k-1)$-$(k,n)^*$-VCS having pixel expansion 2^{k-1} and relative contrast $\frac{1}{2^{k-1}}$.*

Proof Let m denote the number of columns of the matrices S^0 and S^1 (i.e, m denotes the pixel expansion). Note that in this theorem $m=2^{k-1}$. We need to prove the following:

1. If X is a qualified set then $w(S^1_X) - w(S^0_X) \geq \frac{1}{2^{k-1}} \cdot m$.
2. If $Y \subset \mathcal{P}$ is a forbidden set of participants then $S^0[Y]$ and $S^1[Y]$ are identical up to column permutation.

First we prove the second condition viz., the security condition. Let $Y = \{i_1, i_2, \ldots, i_s\}$ be a forbidden set. We want to show that $S^0[Y]$ and $S^1[Y]$ are identical up to a column permutation. Recall that each column of S^0 is a solution of the homogeneous system of equations and each column of S^1 is a solution of the non-homogeneous system of equations. If we can prove that there exists a particular solution of the non-homogeneous system, say $\mathbf{c} = (c_1, c_2, \ldots, c_n)$ such that $c_j = 0$ for $j = i_1, i_2, \ldots, i_s$ then by *Result 1*, the restricted matrices $S^0[Y]$ and $S^1[Y]$ will be identical up to a column permutation. Since Y is a forbidden set of participants, Y does not contain any B_i for all i because otherwise, Y would contain a minimal qualified set and would itself become a qualified set. In a $(k-1)$-$(k, n)^*$-VCS there are two types of maximal forbidden sets:

1. Type 1: $\{1, 2, 3, \ldots, k-2, k-1\}$ that is all the essential parties are present but a regular party is unavailable.
2. Type 2: $\{2, 3, \ldots, k-2, k-1, k, k+1, \ldots, n-1, n\}$ that is all regular parties along with $k-2$ essential parties are present but one essential party namely, 1 is missing.

If we can prove that neither type 1 nor type 2 subsets can have any information about the secret then we are done. Let us first consider type 1 i.e. $Y = \{1, 2, 3, \ldots, k-2, k-1\}$. In this case we see that $c_1 = c_2 = c_3 y = \cdots = c_{k-1} = 0$ and $c_k = c_{k+1} = \cdots = c_n = 1$ is particular solution to the non-homogeneous system. Again, if $Y = \{2, 3, \ldots, k-2, k-1, k, k+1, \ldots, n\}$ is of type 2 then also $c_1 = 1$ and $c_2 = c_3 = \cdots = c_n = 0$ is a particular solution to the non-homogeneous system. Hence the proof follows.

For the proof of the contrast condition let X be a minimal qualified set of participants. Corresponding to this X an all zero solution vector occurs in $S^0[X]$ but there is no such vector in $S^1[X]$. Hence, $w(S^0_X) - w(S^1_X) \geq 1$ which proves the contrast condition. □

Remark Theorem 3.3 reveals that for the $(k-1)$-$(k, n)^*$-VCS, constructed using above construction, the pixel expansion and hence relative contrast depend only on k and surprisingly not on n.

4 On construction of t-$(n-1, n)^*$-VCS

In this section we deal with the particular case of the restricted access structure t-$(k, n)^*$-VCS with $k = n-1$. For the construction and analysis of t-$(n-1, n)^*$-VCS, $(n-1, n)$-VCS plays an important role. In this section we first revisit the technique as given in Adhikari [1] to obtain an $(n-1, n)$-threshold VCS. In that paper [1], the author pointed out that by deleting common columns from the initial basis matrices S^0_{in} and S^1_{in}, one may construct better VCS in terms of less pixel expansion and better relative contrast. However, the author failed to provide the exact number of common columns in S^0_{in} and S^1_{in} for any $(n-1, n)$-VCS. In the next section, we provide the exact count of the common columns and thereby provide a closed form formula for the exact pixel expansion of an efficient $(n-1, n)$-VCS.

4.1 On $(n-1, n)$-VCS

The construction of an $(n-1, n)$-VCS essentially follows from the construction of a general t-$(k, n)^*$-VCS (as described in Sect. 3) by considering $t = 0$. For the sake of completeness we sketch the construction method.

Consider a set of participants $\mathcal{P} = \{1, 2, \ldots, n\}$ and let $X \subseteq \mathcal{P}$ having $n-1$ elements. Then $\mathcal{P}$ has altogether $\binom{n}{n-1} = n$ such subsets. Based on the increasing lexicographic

arrangement we arrange the subsets as follows: $B_1, B_2, \ldots, B_n$. We now collect the subsets to form $\lceil \frac{n}{2} \rceil$ many groups. In general, the ith group G_i can be described as follows:

$$i\text{th Group}(G_i) = \begin{cases} (B_{2i-1}, B_{2i}), & \text{for } 1 \leq i \leq \left\lceil \frac{n-2}{2} \right\rceil, \text{ and any } n > 2; \\ (B_{n-1}, B_n), & \text{for even } n > 2 \text{ and } i = \frac{n}{2}; \\ (B_n), & \text{for odd } n > 2 \text{ and } i = \left\lceil \frac{n}{2} \right\rceil, \end{cases}$$

where

$$B_j = \begin{cases} \{1, 2, \ldots, n-2i, n-2i+1, n-2i+3, n-2i+4, \ldots\}, \ j = 2i-1 \text{ and } i \leq \left\lceil \frac{n-2}{2} \right\rceil; \\ \quad \leftarrow \quad n-1 \text{ many elements} \quad \rightarrow \\ \{1, 2, \ldots, n-2i, n-2i+2, n-2i+3, n-2i+4, \ldots\}, \ j = 2i \text{ and } i \leq \left\lceil \frac{n-2}{2} \right\rceil; \\ \quad \leftarrow \quad n-1 \text{ many elements} \quad \rightarrow \\ \qquad \{1, 3, 4, 5, \ldots, n\}, \qquad \text{for } j = n-1; \\ \qquad \{2, 3, 4, 5, \ldots, n\}, \qquad \text{for } j = n. \end{cases}$$

Now we consider the following systems of linear equations:
For $1 \leq j \leq \lceil \frac{n-2}{2} \rceil$ and for any $n > 2$,

$$\left.\begin{matrix} f_{B_{2j-1}} = 0 \\ f_{B_{2j}} = 0 \end{matrix}\right\} \cdots (j) \quad \text{and} \quad \left.\begin{matrix} f_{B_{2j-1}} = 1 \\ f_{B_{2j}} = 1 \end{matrix}\right\} \cdots (j')$$

For $i = \frac{n}{2}$ and for even $n > 2$,

$$\left.\begin{matrix} f_{B_{n-1}} = 0 \\ f_{B_n} = 0 \end{matrix}\right\} \cdots \left(\frac{n}{2}\right) \quad \text{and} \quad \left.\begin{matrix} f_{B_{n-1}} = 1 \\ f_{B_n} = 1 \end{matrix}\right\} \cdots \left(\frac{n'}{2}\right)$$

For $i = \lceil \frac{n}{2} \rceil$ and for odd $n > 2$,

$$\left.\begin{matrix} f_{B_n} = 0 \\ x_1 = 0 \end{matrix}\right\} \cdots \left(\left\lceil \frac{n}{2} \right\rceil\right) \quad \text{and} \quad \left.\begin{matrix} f_{B_n} = 1 \\ x_1 = 0 \end{matrix}\right\} \cdots \left(\left\lceil \frac{n'}{2} \right\rceil\right)$$

For any $n > 2$ and $1 \leq j \leq \lceil \frac{n-2}{2} \rceil$, let S_j^0 and S_j^1 denote the Boolean matrices whose columns are all possible solutions of the systems (j) and (j') respectively over the binary field. Similarly, for any even (resp. odd) $n > 2$, let $S_{\frac{n}{2}}^0$ (resp. $S_{\lceil \frac{n}{2} \rceil}^0$) and $S_{\lceil \frac{n}{2} \rceil}^1$ (resp. $S_{\lceil \frac{n}{2} \rceil}^1$) denote the Boolean matrices corresponding to the solutions of the equations $(\frac{n}{2})(resp.(\lceil \frac{n}{2} \rceil))$ and $(\frac{n'}{2})(resp.\lceil \frac{n'}{2} \rceil)$.
Then the matrices $S_{in}^0 = S_1^0 || S_2^0 || \cdots || S_{\lceil \frac{n}{2} \rceil}^0$ and $S_{in}^1 = S_1^1 || S_2^1 || \cdots || S_{\lceil \frac{n}{2} \rceil}^1$ formed by the concatenation constitute the initial basis matrices of an $(n-1, n)$-VCS. The proof of this fact can be found in [1]. For the rest of our discussion we will call the matrices S_j^0 and S_j^1 for all j as the jth blocks of the initial basis matrices.

The following lemma is immediate from the construction.

Lemma 3 *The $(n-1, n)$-VCS, constructed using the linear algebraic technique as described above, has initial pixel expansion $m_{in} = \lceil \frac{n}{2} \rceil 2^{n-2}$.*

Example 4.1 For the $(4, 5)$-VCS, the five subsets can be grouped as follows: $G_1 = \{\{1, 2, 3, 4\}, \{1, 2, 3, 5\}\}$, $G_2 = \{\{1, 2, 4, 5\}, \{1, 3, 4, 5\}\}$, $G_3 = \{\{2, 3, 4, 5\}\}$.

The initial basis matrices obtained by solving the set of linear equations corresponding to the above groups, are given by

$$S_{in}^0 = \begin{bmatrix} \leftarrow \text{Col 1 to 8} \rightarrow & \leftarrow \text{Col 9 to 16} \rightarrow & \leftarrow \text{Col 17 to 24} \rightarrow \\ 01010101 & 01010101 & 00000000 \\ 00110011 & 01101001 & 01010101 \\ 00001111 & 01101001 & 00110011 \\ 01101001 & 00110011 & 00001111 \\ 01101001 & 00001111 & 01101001 \end{bmatrix} \textit{and}$$

$$S_{in}^1 = \begin{bmatrix} \leftarrow \text{Col 1 to 8} \rightarrow & \leftarrow \text{Col 9 to 16} \rightarrow & \leftarrow \text{Col 17 to 24} \rightarrow \\ 01010101 & 01010101 & 00000000 \\ 00110011 & 10010110 & 01010101 \\ 00001111 & 10010110 & 00110011 \\ 10010110 & 00110011 & 00001111 \\ 10010110 & 00001111 & 10010110 \end{bmatrix}.$$

The initial pixel expansion is 24.

Now observe that the following columns are common to both S_{in}^0 and S_{in}^1.

S_{in}^0	2	3	5	7	10	11	13	15	24
S_{in}^1	16	22	23	9	8	24	20	1	7

As described in [1], these common columns can be deleted to form the reduced matrices S_{red}^0 and S_{red}^1 which still remain basis matrices of the (4, 5)-VCS. Moreover the pixel expansion of the reduced scheme is reduced to 15.

In general, the above technique can be applied to the initial basis matrices of any $(n-1, n)$-VCS to obtain the reduced basis matrices with less pixel expansion. We are now going to determine, case by case the exact number of common columns occurring in the initial basis matrices S_{in}^0 and S_{in}^1 of an $(n-1, n)$-VCS constructed by the linear algebraic method and find the exact value of the reduced pixel expansion of the scheme. Towards finding the results the following lemmas play an important role.

Lemma 4 *Let S_{in}^0 and S_{in}^1 be the basis matrices of an $(n-1, n)$-VCS, $n \geq 3$, constructed using linear algebraic technique. Then,*

- *For even n, the columns with hamming weights* 0, 1, $(n-1)$ *and n cannot be deleted from S_{in}^0 and S_{in}^1.*
- *For odd n, the columns with hamming weights* 0, 1 *and n cannot be deleted from S_{in}^0 and S_{in}^1.*

Proof Let us first consider the case when n is even. Then for any group G_j for $1 \leq j \leq \frac{n}{2}$, there are $n-2$ independent variables common in both the systems (j) and (j'). The values of these variables determine the values of the remaining two variables. Moreover for every fixed $(n-2)$-tuple of values of the independent variables, the values of the two dependent

variables are equal. Further a column c with hamming weight $w(c) = 0$ can appear only as a solution of the equation (j) and not of the equation (j'). So, if $w(c) = 0$ then $c \in S^0_{in}$ only. Again if $w(c) = 1$ then $c \in S^1_{in}$ only. If $w(c) = n - 1$ then the only possibility is that among $(n - 2)$ independent variables, $(n - 3)$ assume the value 1 and the two dependent variables must be 1. So, if $w(c) = n - 1$ then $c \in S^0_{in}$ only. Lastly, when $w(c) = n$, then all the variables assume the value 1 and the n-tuple $(1, 1, \ldots, 1)$ can only be a solution of the equation (j'). Hence, if $w(c) = n$ then $c \in S^1_{in}$ only.
Using the same arguments we can see that for odd n,

- if $w(c) = 0$ then $c \in S^0_{in}$ only,
- if $w(c) = 1$ then $c \in S^1_{in}$ only and
- if $w(c) = n$ then $c \in S^0_{in}$ only.

This completes the proof. □

Remark For an $(n - 1, n)$-VCS and $n \geq 3$

- For even n, the possible common columns occurring in S^0_{in} and S^1_{in} are the columns with hamming weights $2, 3, \ldots, n - 4, n - 3, n - 2$.
- For odd n, the possible common columns for S^0_{in} and S^1_{in} are the columns with hamming weights $2, 3, \ldots, n - 3, n - 2, n - 1$.

Now that we understand the distribution of possible common columns of an $(n-1, n)$-VCS constructed by linear algebraic method, we proceed to calculate exact number of common columns. In the following we will denote the number of **common columns** with hamming weight j by d_j. For example, by Lemma 4, $d_0 = d_1 = d_n = 0$.

Towards finding the exact number of common columns for any $(n - 1, n)$-VCS we divide the proof technique into two parts. Sect. 4.2 deals when n is even while Sect. 4.3 deals when n is odd.

4.2 Number of common columns when *n* is even

Throughout this subsection, n is assumed to be even. To find the closed form of the number of common columns, the following lemmas play an important role.

The following lemma enables us to look only at the weights that lie between 1 and $\frac{n}{2}$ while calculating the exact number of common columns occurring in the initial basis matrices.

Lemma 5 *For even $n \geq 4$, the $(n - 1, n)$-VCS constructed using linear algebraic method has the property that $d_j = d_{n-j}$ for all $j = 1, 2, \ldots, \frac{n}{2}$.*

Proof Recall that S^0_{in} is constructed by concatenating the blocks $S^0_1, S^0_2, \ldots, S^0_{\frac{n}{2}}$ which are obtained respectively by solving the systems of equations $(1), (2), \ldots, (\frac{n}{2})$. Now $S^1_1, S^1_2, \ldots, S^1_{\frac{n}{2}}$ can be obtained by adding (modulo 2) a particular solution to each of the columns of $S^0_1, S^0_2, \ldots, S^0_{\frac{n}{2}}$ respectively. In this case, observe that $(1, 1, 1, \ldots, 1)$ is a particular solution to each of the system of equations $(1'), (2'), \ldots, (\frac{n'}{2})$. Thus if a column $c \in S^0_{in}$ then its complement $\bar{c} \in S^1_{in}$ and vice versa. Therefore if c is a common column to both S^0_{in} and S^1_{in} then so is $\bar{c}$. Lastly, if weight of c is j then weight of $\bar{c}$ is $(n - j)$. Hence, $d_j = d_{n-j}$ for all $j = 1, 2, 3, \ldots, \frac{n}{2}$. □

Lemmas 6 and 7 give a closed form formula for the number of common columns of weight $j, 2 \leq j \leq \frac{n}{2}$ when j is even and odd respectively.

Lemma 6 *For even $n \geq 4$, the $(n-1, n)$-VCS obtained using linear algebraic technique has the property that if j is even and $2 \leq j \leq \frac{n}{2}$ then $d_j = \frac{n}{2}\binom{n-2}{n-j}$.*

Proof Let us first consider the first block S_1^0 of S_{in}^0. Suppose c is a column of weight j, where j is even, occurring in S_1^0. Therefore c is a solution to the system

$$\begin{aligned} x_1 + x_2 + \cdots + x_{n-2} + x_{n-1} &= 0 \\ x_1 + x_2 + \cdots + x_{n-2} + x_n &= 0 \end{aligned} \tag{3}$$

It is not hard to see that since j is even, $x_{n-1} = x_n = 0$, that is, the last two entries of the column c, corresponding to x_{n-1} and x_n are both 0. Since $w(c) = j$, therefore among the variables $x_1, x_2, \ldots, x_{n-2}$ only j many variables assume the value 1 and the rest of them are all 0. Thus there are in total $\binom{n-2}{j}$ possible choices which implies that there are $\binom{n-2}{j}$ many columns of weight j occurring in S_1^0. Following similar argument it is easy to see that each of the rest of $(\frac{n}{2} - 1)$ blocks have the same number of weight j columns. Therefore, there are altogether $\frac{n}{2}\binom{n-2}{j}$ many columns of weight j occurring in S_{in}^0.

Now let us consider the first block S_1^1 of S_{in}^1. Suppose c is a column of weight j, where j is even, occurring in S_1^1. Therefore c is a solution to the system

$$\begin{aligned} x_1 + x_2 + \cdots + x_{n-2} + x_{n-1} &= 1 \\ x_1 + x_2 + \cdots + x_{n-2} + x_n &= 1 \end{aligned} \tag{4}$$

Again, it is not hard to see that since j is even, $x_{n-1} = x_n = 1$, that is, the last two entries of column c, corresponding to x_{n-1} and x_n, are both 1. Following a similar argument as above we see that there are $\binom{n-2}{j-2}$ many columns of weight j occurring in S_1^1. Hence there are $\frac{n}{2}\binom{n-2}{j-2}$ many columns of weight j occurring in S_{in}^1.

Observe that, $\frac{n}{2}\binom{n-2}{j-2} \leq \frac{n}{2}\binom{n-2}{j}$ for $2 \leq j \leq \frac{n}{2}$.

Now we shall show that if there exists a column c of weight j, where j is even, in S_{in}^1 then that c must also occur in S_{in}^0.

Towards this let c be any column of weight j such that $c \in S_{in}^1$. Then c must belong to some block, say the block constructed by solving the system of equations,

$$\begin{aligned} x_1 + x_2 + \cdots + x_{2k-2} + x_{2k-1} + x_{2k+1} + \cdots + x_n &= 1 \\ x_1 + x_2 + \cdots + x_{2k-2} + x_{2k} + x_{2k+1} + \cdots + x_n &= 1 \end{aligned} \tag{5}$$

It is easy to see $x_{2k-1} = x_{2k} = 1$ and among the $(n-2)$ remaining variables only $(j-2)$ assume the value 1. The rest of the variables assume 0. Let us write $c = (c_1, c_2, \ldots, c_{2k-1}, c_{2k}, \ldots, c_n)$. Now observe that since n is even therefore there are exactly $\frac{n}{2}$ many pairs of the form (c_{2i-1}, c_{2i}), namely, $(c_1, c_2), (c_3, c_4), \ldots, (c_{n-1}, c_n)$. Among these pairs we have already seen that $(c_{2k-1}, c_{2k}) = (1, 1)$. Since $j - 2 \leq \frac{n}{2} - 2$, by Pigeon Hole principle there exists at least one pair say, $(c_{2r-1}, c_{2r}) = (0, 0)$. It is now easy to observe that c is also a solution to the system

$$\begin{aligned} x_1 + x_2 + \cdots + x_{2r-2} + x_{2r-1} + x_{2r+1} + \cdots + x_n &= 0 \\ x_1 + x_2 + \cdots + x_{2r-2} + x_{2r} + x_{2r+1} + \cdots + x_n &= 0 \end{aligned} \tag{6}$$

Thus $c \in S^0_{in}$. Again it is not hard to see that if a column c of weight j, where j is even, occurs multiple times in S^1_{in} then c also occurs at least that many times in S^0_{in}. Hence the proof follows. □

Lemma 7 *For even $n \geq 4$, the $(n-1, n)$-VCS constructed using the linear algebraic method has the property that if j is odd and $3 \leq j \leq \frac{n}{2}$ then $d_j = \frac{n}{2}\binom{n-2}{j-2}$.*

Proof Proof is similar to that of Lemma 6.

Now we are in a position to calculate the exact value of reduced pixel expansion m_{red}. The following theorem provides the exact value of pixel expansion of an efficient $(n-1, n)$-VCS with basis matrices S^0_{red} and S^1_{red} having no common columns.

Theorem 4.1 *Let $n \geq 4$ be even. Then there exists an $(n-1, n)$-VCS obtained by linear algebraic technique having pixel expansion $m_{red} = \frac{n}{4}\binom{n}{\frac{n}{2}}$ and relative contrast $\frac{1}{m_{red}}$.*

Proof Let $\mathcal{K} = \{k : 2 < k \leq \frac{n}{2} \text{ and } k \text{ is odd}\}$ and $\mathcal{L} = \{k : 2 \leq k \leq \frac{n}{2} \text{ and } k \text{ is even}\}$. Then the reduced pixel expansion is given by

$$\begin{aligned} m_{red} &= m_{in} - \sum_{2 \leq k \leq n-2} d_k \\ &= m_{in} - \left[\sum_{2 \leq k \leq \frac{n}{2}} d_k + \sum_{\frac{n}{2} < k \leq n-2} d_k \right] \\ &= m_{in} - \left[\sum_{2 \leq k \leq \frac{n}{2}} d_k + \sum_{2 \leq k < \frac{n}{2}} d_{n-k} \right]. \end{aligned}$$

Therefore by Lemma 5,

$$\begin{aligned} m_{red} &= m_{in} - 2 \sum_{2 \leq k \leq \frac{n}{2}} d_k \\ &= m_{in} - 2 \left[\sum_{k \in \mathcal{K}} d_k + \sum_{k \in \mathcal{L}} d_k \right] \\ &= m_{in} - 2\frac{n}{2} \left[\sum_{k \in \mathcal{K}} \binom{n-2}{k-2} + \sum_{k \in \mathcal{L}} \binom{n-2}{k-2} \right] + d_{\frac{n}{2}} \\ &= m_{in} - \frac{n}{2} \left[2 \sum_{k \in \mathcal{K}} \binom{n-2}{k-2} + 2 \sum_{k \in \mathcal{L}} \binom{n-2}{k-2} \right] + d_{\frac{n}{2}} \\ &= m_{in} - \frac{n}{2} \sum_{0 \leq k \leq n-2} \binom{n-2}{k} + \frac{n}{2} \binom{n-2}{\frac{n}{2}-1} + d_{\frac{n}{2}} \end{aligned}$$

$$= m_{in} - \frac{n}{2}\sum_{0\le k\le n-2}\binom{n-2}{k} + \frac{n}{2}\binom{n-2}{\frac{n}{2}-1} + d_{\frac{n}{2}}$$

$$= m_{in} - \frac{n}{2}2^{n-2} + \frac{n}{2}\binom{n-2}{\frac{n}{2}-1} + d_{\frac{n}{2}}.$$

By Lemma 3, $m_{in} = \frac{n}{2}2^{n-2}$ and therefore,

$$m_{red} = \frac{n}{2}\binom{n-2}{\frac{n}{2}-1} + \frac{n}{2}\binom{n-2}{\frac{n}{2}-2}.$$

Using the identities on binomial coefficients the above expression reduces to $m_{red} = \frac{n}{4}\binom{n}{\frac{n}{2}}$. This completes the proof of the theorem. □

We have found the exact value of the pixel expansion of an $(n-1, n)$-VCS constructed by using the linear algebraic technique for the case when n is even. In the next subsection we find the same for odd $n \geq 3$. For this we take a similar approach as described in Lemma 1.

4.3 Number of common columns when n is odd

Throughout this subsection we assume that n is odd. To start with, we consider the set of participants to be the set $\mathcal{P} = \{2, 3, \ldots, n+1\}$ consisting of n many participants where $n \geq 3$ is odd. The minimal qualified sets arranged in the lexicographic order are given by $B_1 = \{2, 3, \ldots, n\}$, $B_2 = \{2, 3, \ldots, n-1, n+1\}, \ldots, B_n = \{3, 4, \ldots, n+1\}$. As described in Sect. 4.1, the above collection of minimal qualified sets can be grouped as follows: $G_1 = (B_1, B_2), G_2 = (B_3, B_4), \ldots, G_{\lceil \frac{n}{2} \rceil} = (B_n)$. The initial basis matrices can be found by solving the appropriate systems of linear equations corresponding to the above grouping.

We now transform the access structure of the $(n-1, n)$-VCS to the access structure of an $(n, n+1)$-VCS in the following manner:

We incorporate another participant 1 to the set of participants and define $\mathcal{P}^* = \{1\} \bigcup \mathcal{P} = \{1, 2, 3, \ldots, n+1\}$ and $\mathcal{B}_1^* = \{1\} \bigcup B_1, \mathcal{B}_2^* = \{1\} \bigcup B_2, \ldots, \mathcal{B}_n^* = \{1\} \bigcup B_n$ and introduce $\mathcal{B}_{n+1}^* = \{2\} \bigcup B_n$. Now these $(n+1)$ many subsets $\mathcal{B}_1^*, \mathcal{B}_2^*, \ldots, \mathcal{B}_{n+1}^*$ are precisely the minimal qualified sets of an $(n, n+1)$-VCS on the set of participants $\mathcal{P}^*$, where $n+1$ is even. As already described these sets can now be grouped into $\frac{n+1}{2}$ many groups namely, $\mathcal{G}_1^*, \mathcal{G}_2^*, \ldots, \mathcal{G}_{\frac{n+1}{2}}^*$ and then solving the corresponding linear equations, the basis matrices for the $(n, n+1)$-VCS are obtained. By Theorem 4.1, the reduced pixel expansion of the transformed scheme becomes $\frac{n+1}{4}\binom{n+1}{\frac{n+1}{2}}$. Using this we calculate the exact value of the reduced pixel expansion for the $(n-1, n)$-VCS, when $n \geq 3$ is odd.

Note: We will use the following notations and symbols for the rest of this section. All the constructions of basis matrices are done using the linear algebraic technique. We will denote by $S_{in}^0(k, r)$ and $S_{in}^1(k, r)$ the initial basis matrices of the (k, r)-VCS. $S_{red}^0(k, r)$ and $S_{red}^1(k, r)$ will denote the reduced basis matrices of the (k, r)-VCS. To distinguish between the linear equations corresponding to the $(n-1, n)$-VCS and $(n, n+1)$-VCS we will use the variables $x_2, x_3, \ldots, x_{n+1}$ corresponding to the participants in $\mathcal{P}$ and the variables $y_1, y_2, \ldots, y_{n+1}$ corresponding to the participants in $\mathcal{P}^*$.

Now we proceed to find the exact pixel expansion of the reduced basis matrices when n is odd. We first give the overview of the steps. First, in Lemma 8 we find the relationship

between the initial pixel expansions of $(n-1, n)$-VCS and $(n, n+1)$-VCS. From Lemmas 9 to 15 we calculate the number of common columns that can be deleted from the initial basis matrices for both cases and find the relationship between the number of common columns. Lastly, Theorem 4.2 gives the closed form of the reduced pixel expansion.

Lemma 8 *Let m_{in} be the initial pixel expansion of the $(n-1, n)$-VCS obtained by the linear algebraic technique, where $n \geq 3$ is odd. If m^*_{in} denotes the initial pixel expansion of the $(n, n+1)$-VCS then $m^*_{in} = 2m_{in}$.*

Proof The proof is immediate.

In the following two lemmas we show that for every column in the initial basis matrices of the $(n-1, n)$-VCS, where $n \geq 3$ is odd, which does not appear in the last block $S^0_{\lceil \frac{n}{2} \rceil}$ of $S^0_{in}(n-1, n)$ or $S^1_{\lceil \frac{n}{2} \rceil}$ of $S^1_{in}(n-1, n)$, there exist exactly two columns viz. $(0, c)$ and $(1, c)$ that occur in the initial basis matrices of the $(n, n+1)$-VCS.

Lemma 9 *Let c be a column such that $c \in S^0_{in}(n-1, n)$, where $n \geq 3$ is odd. Further assume that c appears as a solution to any system of equations (as described earlier) except the following system of equations*

$$\begin{cases} x_3 + x_4 + \cdots + x_{n+1} = 0 \\ x_2 = 0 \end{cases} \tag{7}$$

Then the columns $(0, c)$ and $(1, c)$ occur respectively in the initial basis matrices $S^0_{in}(n, n+1)$ and $S^1_{in}(n, n+1)$ of the $(n, n+1)$-VCS.

Proof Let $c = (b_2, b_3, \ldots, b_{n+1})$, where each $b_i \in \{0, 1\}$. By the given conditions c is a solution to some system, say

$$\begin{cases} x_2 + \cdots + x_{2k-2} + x_{2k-1} + x_{2k+1} + \cdots + x_{n+1} = 0 \\ x_2 + \cdots + x_{2k-2} + \ \ x_{2k} \ + x_{2k+1} + \cdots + x_{n+1} = 0 \end{cases} \tag{8}$$

Then it is easy to see that $(0, b_2, b_3, \ldots, b_{n+1})$ is a solution to the system

$$\begin{cases} y_1 + y_2 + \cdots + y_{2k-2} + y_{2k-1} + y_{2k+1} + \cdots + y_{n+1} = 0 \\ y_1 + y_2 + \cdots + y_{2k-2} + \ \ y_{2k} \ + y_{2k+1} + \cdots + y_{n+1} = 0 \end{cases} \tag{9}$$

corresponding to the $(n, n+1)$-VCS and $(1, b_2, b_3, \ldots, b_{n+1})$ is a solution to the system

$$\begin{cases} y_1 + y_2 + \cdots + y_{2k-2} + y_{2k-1} + y_{2k+1} + \cdots + y_{n+1} = 1 \\ y_1 + y_2 + \cdots + y_{2k-2} + \ \ y_{2k} \ + y_{2k+1} + \cdots + y_{n+1} = 1 \end{cases} \tag{10}$$

corresponding to the $(n, n+1)$-VCS. Hence the proof. □

Lemma 10 *Let c be a column such that $c \in S^1_{in}(n-1, n)$, where $n \geq 3$ is odd. Further assume that c appears as a solution to any system of equations except the following system of equations*

$$\begin{aligned} x_3 + x_4 + \cdots + x_{n+1} &= 1 \\ x_2 &= 0 \end{aligned} \tag{11}$$

Then the columns $(0, c)$ and $(1, c)$ occur respectively in the initial basis matrices $S^1_{in}(n, n+1)$ and $S^0_{in}(n, n+1)$ of the $(n, n+1)$-VCS.

Proof Same as the proof of the Lemma 9. □

At this point it is not clear what happens if a column occurs in the block $S^0_{\lceil \frac{n}{2} \rceil}$ of $S^0_{in}(n-1, n)$ or occurs in the block $S^1_{\lceil \frac{n}{2} \rceil}$ of $S^1_{in}(n-1, n)$.

Let us recall that the system of linear equations corresponding to the last block $S^0_{\lceil \frac{n}{2} \rceil}$ of $S^0_{in}(n-1, n)$ is

$$\begin{cases} x_3 + x_4 + \cdots + x_{n+1} = 0 \\ x_2 = 0 \end{cases} \tag{12}$$

and the system corresponding to $S^1_{\lceil \frac{n}{2} \rceil}$ of $S^1_{in}(n-1, n)$ is

$$\begin{cases} x_3 + x_4 + \cdots + x_{n+1} = 1 \\ x_2 = 0 \end{cases} \tag{13}$$

A typical solution of these particular systems can be written as $(0, b_3, \ldots, b_{n+1})$, where each $b_i \in \{0, 1\}$.

Let us consider the system of linear equations given by (12). Observe that by our construction method, this system of linear equations corresponding to the $(n-1, n)$-VCS is somewhat transformed into the system of linear equations

$$\begin{cases} y_1 + y_3 + \cdots + y_{n-1} + y_n + y_{n+1} = 0 \\ y_2 + y_3 + \cdots + y_{n-1} + y_n + y_{n+1} = 0 \end{cases} \tag{14}$$

corresponding to the $(n, n+1)$-VCS. Moreover the set of all solutions to the system (14) constitutes the columns of the $\frac{n+1}{2}$-th block of $S^0_{in}(n, n+1)$. In (14) the variables $y_3, y_4, \ldots, y_{n+1}$ are independent and for each of the 2^{n-1} many possible tuples of values of them the dependent variables y_1 and y_2 assume the same value. A similar transformation also holds for the system of linear equations given by (13). The corresponding system of linear equations becomes

$$\begin{cases} y_1 + y_3 + \cdots + y_{n-1} + y_n + y_{n+1} = 1 \\ y_2 + y_3 + \cdots + y_{n-1} + y_n + y_{n+1} = 1 \end{cases} \tag{15}$$

Now we have the following lemmas.

Lemma 11 *Suppose $n \geq 3$ is odd. Let the column $(0, b_3, \ldots, b_{n+1}) \in S^0_{\lceil \frac{n}{2} \rceil}$ corresponding to the $(n-1, n)$-VCS where each $b_i \in \{0, 1\}$. Then the column $(0, 0, b_3, \ldots, b_{n+1})$ occurs in the $\frac{n+1}{2}$-th block of $S^0_{in}(n, n+1)$ and $(1, 1, b_3, \ldots, b_{n+1})$ occurs in the $\frac{n+1}{2}$-th block of $S^1_{in}(n, n+1)$.*

Proof Given that $(0, b_3, \ldots, b_{n+1})$ is a solution to

$$\begin{cases} x_3 + x_4 + \cdots + x_{n+1} = 0 \\ x_2 = 0 \end{cases} \tag{16}$$

It immediately follows that $(0, 0, b_3, \ldots, b_{n+1})$ is a solution to the system

$$\begin{cases} y_1 + y_3 + \cdots + y_{n-1} + y_n + y_{n+1} = 0 \\ y_2 + y_3 + \cdots + y_{n-1} + y_n + y_{n+1} = 0 \end{cases} \tag{17}$$

Again it is not hard to see that $(1, 1, b_3, \ldots, b_{n+1})$ is a solution to the system

$$\begin{cases} y_1 + y_3 + \cdots + y_{n-1} + y_n + y_{n+1} = 1 \\ y_2 + y_3 + \cdots + y_{n-1} + y_n + y_{n+1} = 1 \end{cases} \tag{18}$$

Hence the proof follows. □

Lemma 12 *Suppose $n \geq 3$ is odd. Let the column $(0, b_3, \ldots, b_{n+1}) \in S^1_{\lceil \frac{n}{2} \rceil}$ corresponding to the $(n-1, n)$-VCS where each $b_i \in \{0, 1\}$. Then the column $(0, 0, b_3, \ldots, b_{n+1})$ occurs in the $\frac{n+1}{2}$-th block of $S^1_{in}(n, n+1)$ and $(1, 1, b_3, \ldots, b_{n+1})$ occurs in the $\frac{n+1}{2}$-th block of $S^0_{in}(n, n+1)$.*

Proof Same as the proof of Lemma 11. □

Now that the redistribution of the columns is well understood, we proceed to find the relationship between the number of deleted columns in both cases.

Lemma 13 *Suppose $n \geq 3$ is odd. Let us for the time being, restrict our view within the first $\frac{n-1}{2}$ many blocks of the initial basis matrices $S^0_{in}(n-1, n)$ and $S^1_{in}(n-1, n)$. Further assume that c is a common column occurring in these restricted portions of the basis matrices. Then both the columns $(0, c)$ and $(1, c)$ are common columns occurring in the basis matrices $S^0_{in}(n, n+1)$ and $S^1_{in}(n, n+1)$ of the $(n, n+1)$-VCS.*

Proof Let c occur as solution to the systems

$$\begin{cases} x_2 + \cdots + x_{2k-2} + x_{2k-1} + x_{2k+1} + \cdots + x_{n+1} = 0 \\ x_2 + \cdots + x_{2k-2} + \ x_{2k} \ + x_{2k+1} + \cdots + x_{n+1} = 0 \end{cases} \tag{19}$$

and

$$\begin{cases} x_2 + \cdots + x_{2r-2} + x_{2r-1} + x_{2r+1} + \cdots + x_{n+1} = 1 \\ x_2 + \cdots + x_{2r-2} + \ x_{2r} \ + x_{2r+1} + \cdots + x_{n+1} = 1 \end{cases} \tag{20}$$

corresponding to the $(n-1, n)$-VCS, where $k \neq r$. That is, c occurs in $S^0_{in}(n-1, n)$ and also in $S^1_{in}(n-1, n)$. Since c is a solution to 19, by Lemma 9, $(0, c)$ is a solution to the system

$$\begin{cases} y_1 + y_2 + \cdots + y_{2k-2} + y_{2k-1} + y_{2k+1} + \cdots + y_{n+1} = 0 \\ y_1 + y_2 + \cdots + y_{2k-2} + \ y_{2k} \ + y_{2k+1} + \cdots + y_{n+1} = 0 \end{cases} \tag{21}$$

and $(1, c)$ is a solution to the system

$$\begin{cases} y_1 + y_2 + \cdots + y_{2r-2} + y_{2r-1} + y_{2r+1} + \cdots + y_{n+1} = 1 \\ y_1 + y_2 + \cdots + y_{2r-2} + \ y_{2r} \ + y_{2r+1} + \cdots + y_{n+1} = 1 \end{cases} \tag{22}$$

corresponding to the $(n, n+1)$-VCS. In other words, $(0, c) \in S^0_{in}(n, n+1)$ and $(1, c) \in S^1_{in}(n, n+1)$. Similarly by Lemma 10, $(0, c)$ and $(1, c)$ occur as columns in $S^1_{in}(n, n+1)$ and $S^0_{in}(n, n+1)$ respectively. The proof follows. □

Therefore if d is the number of columns deleted from the initial basis matrices of the $(n-1, n)$-VCS where the columns satisfy the conditions of Lemma 13, then $2d$ many corresponding columns will be deleted from the initial basis matrices of the $(n, n+1)$-VCS. After deleting those common columns we are now left with $(m_{in} - d)$ many columns in the

partly reduced basis matrices of the $(n-1, n)$-VCS and $(m^*_{in} - 2d)$ many columns in the partly reduced basis matrices of the $(n, n+1)$-VCS. At this stage if c be any column that is common to both the partly reduced basis matrices of the $(n-1, n)$-VCS then it must hold that either c occurs in the block $S^0_{\lceil \frac{n}{2} \rceil}$ of $S^0_{in}(n-1, n)$ or in the block $S^1_{\lceil \frac{n}{2} \rceil}$ of $S^1_{in}(n-1, n)$ but not both.

Lemma 14 *Let $n \geq 3$ be odd. Further let c be a common column occurring in the partly reduced basis matrices of the $(n-1, n)$-VCS such that $c \in S^0_{\lceil \frac{n}{2} \rceil}$. Then corresponding to this c there are two columns namely, $(0, c)$ and $\overline{(0, c)}$, the complement of $(0, c)$, that are common columns occurring in the partly reduced basis matrices of the $(n, n+1)$-VCS.*

Proof As $c \in S^0_{\lceil \frac{n}{2} \rceil}$ and c is a common column appearing in the partly reduced basis matrix $S^0_{in}(n-1, n)$, c must belong to some i-th block of the partly reduced $S^1_{in}(n-1, n)$ where $i \neq \lceil \frac{n}{2} \rceil$. By Lemma 10, $(0, c)$ appears as a column in the i-th block of partly reduced $S^1_{in}(n, n+1)$ corresponding to the $(n, n+1)$-VCS. Again since $c \in S^0_{\lceil \frac{n}{2} \rceil}$ corresponding to the $(n-1, n)$-VCS, by Lemma 11, $(0, c)$ appears as a column in the $\frac{n+1}{2}$-th block of $S^0_{in}(n, n+1)$ corresponding to the $(n, n+1)$-VCS. Thus $(0, c)$ is a common column in the partly reduced basis matrices of the $(n, n+1)$-VCS.
Now as $(0, c)$ appears as a column in the $\frac{n+1}{2}$-th block of $S^0_{in}(n, n+1)$ therefore it must be a solution to the system

$$\begin{cases} y_1 + y_3 + \cdots + y_{n+1} = 0 \\ y_2 + y_3 + \cdots + y_{n+1} = 0 \end{cases} \tag{23}$$

Hence its complement $\overline{(0, c)}$ is a solution to the system

$$\begin{cases} y_1 + y_3 + \cdots + y_{n+1} = 1 \\ y_2 + y_3 + \cdots + y_{n+1} = 1 \end{cases} \tag{24}$$

This follows from the fact that $y_1 = 1, y_2 = 1, \ldots, y_{n+1} = 1$ is a particular solution to the system (24) as n is odd. Similarly as $(0, c)$ occurs in the i-th block of the partly reduced matrix $S^1_{in}(n, n+1)$ therefore $\overline{(0, c)}$ occurs in i-th block of $S^0_{in}(n, n+1)$ corresponding to the $(n, n+1)$-VCS.
The proof follows. □

By an essentially same line of argument we can prove the following lemma.

Lemma 15 *Let $n \geq 3$ be odd. Further let c be a common column occurring in the partly reduced basis matrices of the $(n-1, n)$-VCS such that $c \in S^1_{\lceil \frac{n}{2} \rceil}$. Then corresponding to this c there are two columns namely, $(0, c)$ and $\overline{(0, c)}$, the complement of $(0, c)$, that are common columns occurring in the partly reduced basis matrices of the $(n, n+1)$-VCS.*

If d' be the number of such common columns occurring in the partly reduced basis matrices of the $(n-1, n)$-VCS then there are $2d'$ many common columns occurring in the partly reduced basis matrices of the $(n, n+1)$-VCS. Thus we have shown that to each common column appearing in the initial basis matrices of the $(n-1, n)$-VCS there are two corresponding columns that are common to the initial basis matrices of the $(n, n+1)$-VCS. Moreover, it is easy to see that the common columns occurring in the basis matrices of the $(n, n+1)$-VCS arise only in this manner. There are no more common columns. Hence the

exact pixel expansions (after reduction) of an $(n-1, n)$-VCS and the $(n, n+1)$-VCS are related via,

$$\begin{aligned} m^*_{red} &= m^*_{in} - 2(d + d') \\ &= 2m_{in} - 2(d + d') \\ &= 2(m_{in} - d - d') \\ &= 2m_{red}. \end{aligned}$$

Thus we have the following theorem.

Theorem 4.2 *Let m_{red} be the reduced pixel expansion of an $(n-1, n)$-VCS where $n \geq 3$ is odd. Then*

$$m_{red} = \frac{n}{2}\binom{n-1}{\frac{n-1}{2}}.$$

Proof The reduced pixel expansion m_{red} is given as follows

$$m_{red} = \frac{1}{2}\frac{n+1}{4}\binom{n+1}{\frac{n+1}{2}} = \frac{n}{2}\binom{n-1}{\frac{n-1}{2}}.$$

□

Remark Thus we have given a closed form formula regarding the pixel expansion and relative contrast of an $(n-1, n)$-VCS constructed using the linear algebraic technique. It is to be noted that for odd $n \geq 3$, our closed form formula for pixel expansion is exactly half that of given in Lemma 4.4 in [12] and (ii) of Sect. 3.2 of [19]. However, the expression that we have found for m_{red} is exactly the same as the formulas that appear in [12,19], for even n. Further Table 1 shows that our proposed closed form for reduced pixel expansion of $(n-1, n)$-VCS for every possible value of n matches with the numerical values of the optimal pixel expansions as shown in [23].

We are now in a position to calculate the exact pixel expansion of any t-$(n-1, n)^*$-VCS for a meaningful triplet $(t, n-1, n)$ such that $(0, n-1-t, n-t)$ is also a meaningful one. Using Theorem 3.2, we have the following theorem.

Table 1 Comparison of pixel expansions for different $(n-1, n)$-VCSs of various values of n

$(n-1, n)$-VCS	m_{red}	m_{CA}	m_A	m_{BDSS}	m_K	m_S	m_D
(2,3)-VCS	3	4	4	3	3	3	3
(3,4)-VCS	6	2^5	8	6	6	6	6
(4,5)-VCS	15	2^9	24	15	15	15	15
(5,6)-VCS	30	2^{14}	48	30	30	30	30
(6,7)-VCS	70	2^{20}	128	70	70	70	70
(7,8)-VCS	140	2^{27}	256	140	140	140	140
(8,9)-VCS	315	2^{35}	640	315	315	315	315

In the following table, m_{red} stands for the reduced pixel expansion of our scheme, m_{CA} denotes the pixel expansion obtained by cumulative array method [7], m_A denotes the pixel expansion obtained by Theorem 2.5 of [1], m_{BDSS} denotes the pixel expansion as given in Appendix B of [12], m_K denotes the pixel expansion as given in Table 1 of [19], m_S denotes the optimal pixel expansion as obtained in Table II, Sect. IV of [23] and m_D denotes the pixel expansion of as shown in Table 1 of [17]

Theorem 4.3 *For any meaningful triplet $(t, n-1, n)$ such that $(0, n-1-t, n-t)$ is also meaningful, there exists a t-$(n-1, n)^*$-VCS having reduced pixel expansion*

$$m_{red} = \begin{cases} 2^t \frac{n-t}{4} \binom{n-t}{\frac{n-t}{2}}, \text{ if } n-t \text{ is even} \\ 2^t \frac{n-t}{2} \binom{n-t}{\frac{n-t-1}{2}}, \text{ if } n-t \text{ is odd} \end{cases}$$

and relative contrast $\frac{1}{m_{red}}$.

4.4 Some features of the basis matrices of $(n-1, n)$-VCS with even n

We analyze the structures of the basis matrices S^0 and S^1 for $(n-1, n)$-VCS, with even n, obtained by the process described so far. In this case $(n-1)$ becomes odd and we have already observed in Lemma 4 that the n-tuple $(1, 1, 1, \ldots, 1)$ is a particular solution to each of the system of equations (as in Sect. 4.1)

$$\left.\begin{aligned} f_{B_{2j-1}} &= 1 \\ f_{B_{2j}} &= 1 \end{aligned}\right\}$$

for all j such that $1 \leq j \leq \frac{n}{2}$.

Now let us consider the initial basis matrix S^0_{in}. We observe that once the first block S^0_1 is constructed the rest of the blocks S^0_2, S^0_3,..., $S^0_{n/2}$ can be constructed by suitable permutations of rows. More explicitly, recall that the block S^0_1 contains, as its columns, the solution vectors of the system

$$\begin{cases} x_1 + x_2 + \cdots + x_{n-2} + x_{n-1} = 0 \\ x_1 + x_2 + \cdots + x_{n-2} + \quad x_n = 0 \end{cases} \tag{25}$$

In the above system of equations observe that the variables x_{n-1} and x_n are dependent on the rest of the variables. Thus all possible 2^{n-2} binary column vectors occur in the $(n-2) \times n$ submatrix and the last two rows (which represent the values of x_{n-1} and x_n) are obtained from them. For constructing the second block S^0_2 we solve the following system:

$$\begin{cases} x_1 + x_2 + \cdots + x_{n-4} + x_{n-3} + x_{n-1} + x_n = 0 \\ x_1 + x_2 + \cdots + x_{n-4} + x_{n-2} + x_{n-1} + x_n = 0 \end{cases} \tag{26}$$

In this system x_{n-3} and x_{n-2} are dependent on the rest of the variables. Thus S^0_2 can be easily obtained from S^0_1 by interchanging $(n-1)$-th row with $(n-3)$-th row and row n with row $n-2$ and keeping all other rows fixed. In the similar manner we can construct $S^0_3, S^0_4, \ldots, S^0_{n/2}$.

Following the exact same steps we can construct the matrix S^1_{in} from its first block S^1_1. As we have noted that the n-tuple $(1, 1, \ldots, 1)$ is a particular solution of the system

$$\begin{cases} x_1 + x_2 + \cdots + x_{n-2} + x_{n-1} = 1 \\ x_1 + x_2 + \cdots + x_{n-2} + \quad x_n = 1 \end{cases} \tag{27}$$

therefore the solutions of this system can be obtained by adding (modulo 2) the particular solution $(1, 1, \ldots, 1)$ to each of the solutions of the system (25). Hence, $\overline{S^0_i} = S^1_i$ for all i such that $1 \leq i \leq \frac{n}{2}$. Thus $\overline{S^0_{in}} = S^1_{in}$. It is immediate that if c is a column appearing in

S^0_{in} then it must belong to S^0_i, for some i and thus S^1_i contains $\bar{c}$ as one of its columns. The following lemma summarizes the above discussion.

Lemma 16 *Suppose S^0_{in} and S^1_{in} denote the basis matrices of an $(n-1, n)$-VCS constructed by the linear algebraic method where $n \geq 4$ is even. Then the frequency with which a column c appears in S^b_{in} equals the frequency with which $\bar{c}$ occurs in S^{1-b}_{in} for $b \in \{0, 1\}$.*

Recall that we delete the common columns from S^0_{in} and S^1_{in} to construct the reduced basis matrices S^0_{red} and S^1_{red}. In this process, suppose that a column v gets deleted. Thus v occurs as a column in both S^0_{in} and S^1_{in}. Therefore v occurs in some block S^0_r for some r and also occurs in some block S^1_t for some t where $r \neq t$. Now

- $v \in S^0_r \Rightarrow \bar{v} \in S^1_r$ and
- $v \in S^1_t \Rightarrow \bar{v} \in S^0_t$

Hence $\bar{v}$ also is a common column and hence gets deleted. We now have the following theorem.

Theorem 4.4 *Let $n \geq 4$ be even. Then for an $(n-1, n)$-VCS constructed using linear algebraic method number of times a column c appears in S^b_{red} is equal to the number of times the column $\bar{c}$ occurs in S^{1-b}_{red} for $b \in \{0, 1\}$.*

5 On $(n-2, n)$-VCS

In this section we focus our attention on the construction of an $(n-2, n)$-VCS. The motivation of this section is two-fold. First, we resolve an open issue posed in [1] where the author pointed out [Remark 4, Sect. 3] that for some specific access structures one may take three equations at a time to reduce pixel expansion. In this section we first show by providing concrete examples that taking three equations at a time works better than taking two equations at a time. Then we go on providing an algorithm, for an $(n-2, n)$-VCS, that takes three equations at a time to construct the systems of linear equations. We further show that using this simple algorithm we can always have less initial pixel expansion than the initial pixel expansion while taking two equations at a time. The second motivation is to provide a closed form formula of the pixel expansion for any $(n-2, n)$-VCS and thereby provide a closed form of any t-$(n-2, n)^*$-VCS, with meaningful triplet $(t, n-2, n)$. The closed form of the pixel expansion of any $(n-2, n)$-VCS as provided in Theorem 5.3 gives much better pixel expansion than the closed forms of the schemes as posed in [1,7]. We further show that further reduction in pixel expansion may be possible by deleting the common columns of the basis matrices. More precisely, in Sect. 5.1 we first discuss the difficulties of taking three equations at a time and then give algorithms overcoming the difficulties, separately for odd and even n, to collect three minimal qualified subsets at a time to form groups. In Sect. 5.2 we provide upper bounds iteratively, for initial and reduced pixel expansions of any $(n-2, n)$-VCS constructed by the algorithm in Sect. 5.1. Lastly, in Sect. 5.3 we give the exact form of the initial pixel expansion of any $(n-2, n)$-VCS and prove that taking three equations together always works better than taking two equations at a time. Numerical evidence shows that our algorithm provides almost optimal pixel expansion. Further numerical evidence shows that for $(n-2, n)$-VCS, the reduced pixel expansion obtained using our proposed algorithm provides much less pixel expansion compared to the reduced pixel expansion obtained by taking two equations at a time.

Before starting the formal discussion, let us first fix up certain notations that will be used throughout this section.

Notation Let $m_{in}^{(2)}(k,n)(m_{in}^{(3)}(k,n))$ and $m_{red}^{(2)}(k,n)(m_{red}^{(3)}(k,n))$ denote respectively the initial pixel expansion and the reduced pixel expansion of the (k, n)-VCS obtained by considering two (three) equations at a time.

Remark From Theorem 2.5 of [1], it follows that

$$m_{in}^{(2)}(n-2,n) = \begin{cases} n(n-1)2^{n-5}, & \text{if } n \equiv 0,1 \pmod 4 \\ (n(n-1)+2)2^{n-5}, & \text{if } n \equiv 2,3 \pmod 4 \end{cases} \tag{28}$$

Hence we can now find the pixel expansion of t-$(n-2, n)^*$-VCS using Theorem 3.2.

To get the motivation why three equations taken at a time may provide better pixel expansion than two equations taken at a time, let us first consider the following example where we first consider two equations at a time.

Example 5.1 Consider a $(3, 5)$-VCS where the groups are $G_1 = \{\{1, 2, 3\}, \{1, 2, 4\}\}, G_2 = \{\{1, 2, 5\}, \{1, 4, 5\}\}, G_3 = \{\{1, 3, 4\}, \{1, 3, 5\}\}, G_4 = \{\{2, 3, 4\}, \{2, 3, 5\}\}, G_5 = \{\{2, 4, 5\}, \{3, 4, 5\}\}$. Then the initial basis matrices are given by

$$S_{in}^0 = \begin{bmatrix} 0011 & 0011 & 0011 & 0000 & 0000 \\ 0101 & 0110 & 0000 & 0011 & 0110 \\ 0110 & 0000 & 0101 & 0101 & 0110 \\ 0110 & 0110 & 0110 & 0110 & 0011 \\ 0000 & 0101 & 0110 & 0110 & 0101 \end{bmatrix} \quad \textit{and}$$

$$S_{in}^1 = \begin{bmatrix} 0011 & 0011 & 0011 & 0000 & 0000 \\ 0101 & 1001 & 0000 & 0011 & 1001 \\ 1001 & 0000 & 0101 & 0101 & 1001 \\ 1001 & 1001 & 1001 & 1001 & 0011 \\ 0000 & 0101 & 1001 & 1001 & 0101 \end{bmatrix}.$$

Here, $m_{in}^{(2)}(3, 5) = 20$. However, we may further reduce the pixel expansion by deleting the following common columns:

- 16th column of S_{in}^0 and 17th column of S_{in}^1.
- 20th column of S_{in}^0 and 13th column of S_{in}^1.

Thus $m_{red}^{(2)}(3, 5) = 20 - 2 = 18$.

5.1 Reducing the pixel expansion: taking three equations at a time

By considering the Example 5.1, we shall illustrate further that if we can choose the equations suitably by taking three equations at a time, then the pixel expansion may be reduced significantly.

Example 5.2 Let us regroup the minimal qualified sets for $(3, 5)$-VCS as follows: $G_1 = \{\{1, 2, 3\}, \{1, 2, 4\}, \{2, 4, 5\}, \{2, 3, 5\}\}$, $G_2 = \{\{1, 2, 5\}, \{1, 3, 5\}, \{1, 4, 5\}\}, G_3 = \{\{1, 3, 4\}, \{2, 3, 4\}, \{3, 4, 5\}\}$.

Note that for G_1, the first three equations, corresponding to the first three minimal qualified subsets of G_1, give rise (addition modulo 2) to the last equation corresponding to the last minimal qualified subset $\{2, 3, 5\}$, i.e.,

$$\begin{array}{r} x_1 + x_2 + x_3 = b \\ x_1 + x_2 + x_4 = b \\ x_2 + x_4 + x_5 = b \\ \hline x_2 + x_3 + x_5 = b \end{array} \tag{29}$$

where $b \in \{0, 1\}$.
Thus considering the three groups we have the following initial basis matrices:

$$S^0_{in} = \begin{bmatrix} 0011 & 0011 & 0110 \\ 0101 & 0110 & 0110 \\ 0110 & 0110 & 0011 \\ 0110 & 0110 & 0101 \\ 0011 & 0101 & 0110 \end{bmatrix} \quad and \quad S^1_{in} = \begin{bmatrix} 0011 & 0011 & 1001 \\ 0101 & 1001 & 1001 \\ 1001 & 1001 & 0011 \\ 1001 & 1001 & 0101 \\ 0011 & 0101 & 1001 \end{bmatrix}.$$

After deleting the common columns, we have the reduced basis matrices as follows:

$$S^0_{red} = \begin{bmatrix} 00 & 001 & 011 \\ 01 & 011 & 011 \\ 01 & 011 & 001 \\ 01 & 011 & 010 \\ 01 & 010 & 011 \end{bmatrix} \quad and \quad S^1_{red} = \begin{bmatrix} 01 & 011 & 001 \\ 11 & 001 & 001 \\ 01 & 001 & 011 \\ 01 & 001 & 101 \\ 01 & 101 & 001 \end{bmatrix}.$$

Thus by choosing suitably three equations at a time, we have $m^{(3)}_{red}(3, 5) = 8$, a significant reduction in pixel expansion from 18 to 8.

Example 5.2 shows that if we carefully collect three equations at a time then the pixel expansion is reduced drastically. We now describe an algorithm for constructing the groups such that each group contains at least three equations. In other words, we try to collect three minimal qualified subsets of participants such that all minimal qualified subsets are exhausted and solving the corresponding simultaneous linear equations we construct the basis matrices corresponding to any $(n - 2, n)$-VCS. While developing the algorithm we must take care of the fact that collecting three minimal qualified sets (three equations at a time) together admits, in each group, a fourth subset of participants which may be a forbidden subset of participants and in this process this forbidden subset becomes a qualified one. For example, while constructing $(3, 5)$-VCS, if we take the following three equations at a time corresponding to the minimal qualified sets $\{1, 2, 3\}$, $\{1, 2, 4\}$ and $\{2, 3, 4\}$:

$$\begin{array}{r} x_1 + x_2 + x_3 = b \\ x_1 + x_2 + x_4 = b \\ x_2 + x_3 + x_4 = b \\ \hline x_2 \qquad\quad = b \end{array}$$

where $b \in \{0, 1\}$, the set $\{2\}$ becomes qualified. We do not want that. So we should take care of the fact that the fourth subset of participants, obtained as above, must be a qualified set.

The algorithm we are now going to discuss makes sure that the fourth subset is a qualified one. Two things may happen in this process. Firstly, if three equations are added modulo 2 then the resulting equation may contain all the n variables (which obviously corresponds to a qualified set $\{1, 2, \ldots, n\}$). Secondly, the resulting equation may contain exactly $(n - 2)$ variables which corresponds to a minimal qualified set of $(n - 2, n)$-VCS. To describe the algorithm, we define these two different types of groups.

Definition 5.1 When three minimal qualified sets are collected to form a group and the resulting fourth qualified set is the full set of participants then the group is called a X-type group.

Definition 5.2 When three minimal qualified sets are collected to form a group and the resulting fourth qualified set is another distinct minimal qualified set then the group is called a Y-type group.

Example 5.3 If we consider the $(3, 5)$-VCS as described in Example 5.2, the group G_1 is a Y-type group while G_2 and G_3 are X-type groups.

We are now in a position to describe an algorithm for making the groups of minimal qualified subsets of the $(n-2, n)$-VCS, taking three equations at a time. We divide the algorithm for two case, namely n even and odd. First let us describe the algorithm for odd $n \geq 5$.

Grouping algorithm when $n(\geq 5)$ **is odd:** In this case, $n-2$ is also odd and there are $\binom{n}{n-2}$ many minimal qualified sets, $\mathcal{B}_1, \mathcal{B}_2, \ldots, \mathcal{B}_{\binom{n}{n-2}}$, arranged in a lexicographic order. We then form $\lceil \frac{n-2}{2} \rceil$ that is, $\frac{n-1}{2}$ many X-type groups say, $X_1, X_2, \ldots, X_{\frac{n-1}{2}}$. Corresponding to each X_m, except the last one, we form m many Y-type groups say, $Y_{m,1}, Y_{m,2}, \ldots, Y_{m,m}$. Thus there are in all $\frac{(n-1)(n-3)}{8}$ many Y-type groups.
The grouping algorithm is as follows:

for $m = 1$ **to** $\frac{n-1}{2}$
  $X_m \leftarrow \{\mathcal{B}_{m(2m-1)}, \mathcal{B}_{(m+1)(2m-1)}, \mathcal{B}_{m(2m+1)}\}$
for $m = 1$ **to** $\frac{n-1}{2} - 1$
  for $j = 1$ **to** m
    $Y_{m,j} \leftarrow \{\mathcal{B}_{m(2m+1)+2j-1}, \mathcal{B}_{(m+1)(2m+1)+2j}, \mathcal{B}_{m(2m+1)+2m+2j}, \mathcal{B}_{m(2m+1)+2m+2j+1}\}$

Remark Observe that the linear equation corresponding to the last element of $Y_{m,j}$ arises from the first three. Now, as usual we construct the linear equations for each X_m and each $Y_{m,j}$ and solving them we get the initial basis matrices of the $(n-2, n)$-VCS.

Let us now illustrate the above algorithm through the following example.

Example 5.4 Let us consider a $(7, 9)$-VCS. Let $\Gamma_0 = \{\mathcal{B}_i : i = 1, 2, \ldots, 36\}$ be the set of all minimal qualified sets arranged in the lexicographic order. Then

$$\begin{aligned}
X_1 &= \{\mathcal{B}_1, \mathcal{B}_2, \mathcal{B}_3\},\\
Y_{1,1} &= \{\mathcal{B}_4, \mathcal{B}_5, \mathcal{B}_7, \mathcal{B}_8\},\\
X_2 &= \{\mathcal{B}_6, \mathcal{B}_9, \mathcal{B}_{10}\},\\
Y_{2,1} &= \{\mathcal{B}_{11}, \mathcal{B}_{12}, \mathcal{B}_{16}, \mathcal{B}_{17}\},\\
Y_{2,2} &= \{\mathcal{B}_{13}, \mathcal{B}_{14}, \mathcal{B}_{18}, \mathcal{B}_{19}\},\\
X_3 &= \{\mathcal{B}_{15}, \mathcal{B}_{20}, \mathcal{B}_{21}\},\\
Y_{3,1} &= \{\mathcal{B}_{22}, \mathcal{B}_{23}, \mathcal{B}_{29}, \mathcal{B}_{30}\},\\
Y_{3,2} &= \{\mathcal{B}_{24}, \mathcal{B}_{25}, \mathcal{B}_{31}, \mathcal{B}_{32}\},\\
Y_{3,3} &= \{\mathcal{B}_{26}, \mathcal{B}_{27}, \mathcal{B}_{33}, \mathcal{B}_{34}\},\\
X_4 &= \{\mathcal{B}_{28}, \mathcal{B}_{35}, \mathcal{B}_{36}\}.
\end{aligned}$$

Solving the corresponding simultaneous linear equations we get the basis matrices of the $(7, 9)$-VCS. In this case, $m_{in}^{(3)}(7, 9) = 640$ and $m_{red}^{(3)}(7, 9) = 256$.

Grouping algorithm for the case when $n(>4)$ is even: In this case the list (L) of all minimal qualified sets, arranged in the lexicographic order, is divided into 2 separate sublists, L_1, L_2, where:

$$L_1 = \{\mathcal{B} \in L : 1 \in \mathcal{B}\} \text{ and}$$
$$L_2 = \{\mathcal{B} \in L : \mathcal{B} \notin L_1\}$$

It is easy to see that $|L_1| = \binom{n-1}{n-3}$ and $|L_2| = \binom{n-1}{n-2}$.
Now observe that in the list L_1 if we ignore the participant 1 then the list is essentially the list of all minimal qualified sets of an $(n-3, n-1)$-VCS on the participant set $\mathcal{P} = \{2, 3, \ldots, n\}$. Since $(n-1)$ is odd, we may use the grouping algorithm for odd n (as described above) to exhaust the sublist for L_1. Now for the sublist L_2 it is nothing but the list of all minimal qualified sets of an $(n-2, n-1)$-VCS on the participant set $\mathcal{P} = \{2, 3, \ldots, n\}$. We can collect two minimal qualified sets at a time as described in Sect. 4.1 to form the groups.
Let us illustrate the above algorithm through an example.

Example 5.5 Let us now consider the $(8, 10)$-VCS. Let Let $\{\mathcal{C}_i : i = 1, 2, \ldots, 45\}$ be the all minimal qualified sets arranged in the lexicographic order. Then the first 36 subsets $\mathcal{C}_1$ through $\mathcal{C}_{36}$ are grouped as the $(7, 9)$-VCS, that is, just replace $\mathcal{C}_i$ in place of $\mathcal{B}_i$ for all i= 1, 2, ..., 36. For the 9 subsets, $\mathcal{C}_{37}$ to $\mathcal{C}_{45}$, group as follows:
G_1= $\{\mathcal{C}_{37}, \mathcal{C}_{38}\}$, G_2= $\{\mathcal{C}_{39}, \mathcal{C}_{40}\}$, G_3= $\{\mathcal{C}_{41}, \mathcal{C}_{42}\}$, G_4= $\{\mathcal{C}_{43}, \mathcal{C}_{44}\}$ and G_5= $\{\mathcal{C}_{45}\}$.

Remark The above algorithms hold when $n \geq 5$. For the $(2, 4)$-VCS we directly construct the basis matrices by considering the following groups: $G_1 = \{\{1, 2\}, \{1, 3\}, \{1, 4\}\}$, $G_2 = \{\{2, 3\}, \{2, 4\}\}$ and $G_3 = \{\{3, 4\}\}$ and then solving the corresponding systems of linear equations.

5.2 Bounds and numerical evidence of betterment of pixel expansion

It is immediate from the Example 5.5 that if $m_{red}^{(l)}(k, n)$ denotes the reduced pixel expansion of a (k, n)-VCS constructed by considering l equations at a time, then

$$m_{red}^{(3)}(8, 10) \leq 2m_{red}^{(3)}(7, 9) + m_{red}^{(2)}(8, 9).$$

This can be very easily generalized to the following theorem.

Theorem 5.1 *Let $m_{red}^{(l)}(k, n)$ denote the reduced pixel expansion of a (k, n)-VCS after deleting the common columns. Then for all even $n > 4$*

$$m_{red}^{(3)}(n-2, n) \leq 2m_{red}^{(3)}(n-3, n-1) + m_{red}^{(2)}(n-2, n-1).$$

In a similar way we can give (in a recursive manner) an upper bound for the case when $n \geq 5$ is odd. For this we break the list of all minimal qualified sets of an $(n-2, n)$-VCS into two parts namely, L_1 which contains all those subsets containing 1 and L_2 which contains all other minimal qualified subsets that are not in L_1. Now it is easy to see that L_1 can be identified as the minimal qualified sets for a 1-$(n-2, n)^*$-VCS with 1 as the essential participant. Again, L_2 can be identified as the minimal qualified sets of an $(n-2, n-1)$-VCS on the participant set $\{2, 3, \ldots, n-1\}$. Hence we have the following theorem.

Table 2 Comparison of pixel expansions for different $(n-2, n)$-VCSs of various values of n

$(n-2, n)$-VCS	$m_{red}^{(3)}$	m_{BDSS}	m_K	m_S	m_D
(2,4)-VCS	4	6	6	4	4
(3,5)-VCS	8	8	8	8	8
(4,6)-VCS	24	36	36	23	24
(5,7)-VCS	48	48	48	48	48
(6,8)-VCS	128	198	198	120	128
(7,9)-VCS	256	252	252	252	256
(8,10)-VCS	640	1020	590	590	640

In the following table, $m_{red}^{(3)}$ stands for the reduced pixel expansion of our scheme obtained by considering three equations at a time, m_{BDSS} denotes the pixel expansion as shown in Appendix B of [12], m_K denotes the pixel expansion as shown in Table 1, Sect. 3.2 of [19], m_S denotes the optimal pixel expansion as obtained in Table 2, Sect. IV of [23] and m_D denotes the pixel expansion of as shown in Table 1 of [17]. The value of m_K for (8,10)-VCS is collected from [23]

Theorem 5.2 *Let $m_{red}^{(l)}(k, n)$ denote the reduced pixel expansion of a (k, n)-VCS after deleting the common columns. Then for all odd $n \geq 5$*

$$m_{red}^{(3)}(n-2, n) \leq m_{red}^{(2)}(1-(n-2, n)^*) + m_{red}^{(2)}(n-2, n-1)$$

that is,

$$m_{red}^{(3)}(n-2, n) \leq 2m_{red}^{(2)}(n-3, n-1) + m_{red}^{(2)}(n-2, n-1).$$

Actually the above upper bound of the pixel expansion is far from being tight. The exact pixel expansion comes out to be much less than the upper bound. It is an interesting problem to find the exact reduced pixel expansion of an $(n-2, n)$-VCS. Numerical evidence, as shown in Table 2, shows that our algorithm provides almost optimal pixel expansion compared with the optimal pixel expansion as obtained in [23].

5.3 Comparison of pixel expansions while taking two and three equations at a time

We further deal with the $(n-2, n)$-VCS and resolve an open issue, as posed in [1]. In [1] the author pointed out [Remark 4, Sect. 3] that for some specific access structure one may take three equations at a time to reduce pixel expansion. In this section we resolve this issue by showing that our grouping algorithm for taking three equations at a time always provides less initial pixel expansion than the initial pixel expansion while taking two equations at a time.

We have already observed in Eq. (28) the exact value of initial pixel expansion of an $(n-2, n)$-VCS constructed using linear algebraic technique when two equations are taken at a time. Our bound in this matter (when taking three equations at a time) is a recursive one, viz. Theorems 5.1 and 5.2. We now find the exact value of the initial pixel expansion when the grouping of the minimal qualified sets are done using the grouping algorithm described in the last section.

Let us first consider the case when $n \geq 5$ is odd. Our algorithm for constructing the groups, taking at least three minimal qualified sets at a time, guarantees the following: there are $\frac{n-1}{2}$ many X-type groups and $\frac{1}{8}(n-1)(n-3)$ many Y-type groups. In any system of linear equations corresponding to a X-type group there are $(n-3)$ many independent variables.

Table 3 Numerical evidence of getting significantly less pixel expansion for $(n-2, n)$-VCS different values of n

$(n-2, n)$-VCS	(2, 4)	(3, 5)	(4, 6)	(5, 7)	(6, 8)	(7, 9)	(8, 10)
$m_{red}^{(2)}$	6	18	48	126	312	754	1766
$m_{red}^{(3)}$	4	8	24	48	128	256	640

Therefore, the total pixel expansion contributed by all X-type groups is $\frac{n-1}{2}2^{n-3}$, that is, $(n-1)2^{n-4}$. Similarly in any system of linear equations corresponding to a Y-type group there are $(n-3)$ many independent variables and hence the total pixel expansion contributed by all Y-type groups is $(n-1)(n-3)2^{n-6}$.
Therefore initial pixel expansion

$$m_{in}^{(3)}(n-2, n) = (n^2-1)2^{n-6} \; \forall \; odd \; n \geq 5.$$

Now it not hard to see that $m_{in}^{(2)}(n-2, n) > m_{in}^{(3)}(n-2, n)$ for all odd $n \geq 5$.
If n is even then as per our algorithm the initial pixel expansion becomes

$$m_{in}^{(3)}(n-2, n) = 2m_{in}^{(3)}(n-3, n-1) + m_{in}^{(2)}(n-2, n-1) \; \forall \; even \; n > 4.$$

Observe that $(n-1)$ is odd and therefore the right hand side becomes $2^{n-6}(n^2+2n)$ after some algebra. Now for $n > 4$ with n even it is not hard to see that $m_{in}^{(2)}(n-2, n) > m_{in}^{(3)}(n-2, n)$. Thus we have calculated the initial pixel expansion $m_{in}^{(3)}(n-2, n)$ for even $n > 4$, in terms of the pixel expansions of the $(n-3, n-1)$-VCS and $(n-2, n-1)$-VCS. However, for the $(2, 4)$-VCS, constructed directly [See Remark following Example 5.5] using the linear algebraic technique, the initial pixel expansion equals $2^{n-6}(n^2+2n)$ with $n = 4$. In this case $m_{in}^{(2)}(2, 4) = m_{in}^{(3)}(2, 4)$. Thus we have the following theorem.

Theorem 5.3 *Let $m_{in}^{(l)}(k, n)$ denote the initial pixel expansion of a (k, n)-VCS taking l equations at a time. Then $m_{in}^{(2)}(n-2, n) \geq m_{in}^{(3)}(n-2, n)$, where*

$$m_{in}^{(3)}(n-2, n) = \begin{cases} (n^2-1)2^{n-6}, & for\ all\ \ odd\ n \geq 5 \\ 2^{n-6}(n^2+2n), & for\ all\ \ even\ n \geq 4. \end{cases}$$

Moreover the equality $m_{in}^{(2)}(n-2, n) = m_{in}^{(3)}(n-2, n)$ holds if and only if $n = 4$.

Further numerical evidence, as shown in Table 3, shows that for $(n-2, n)$-VCS, the reduced pixel expansion obtained using our proposed algorithm provides much less pixel expansion compared to the reduced pixel expansion obtained by taking two equations at a time.

6 Conclusion and open issues

In this paper we have put forward a construction and analysis, based on linear algebraic technique, of a t-$(k, n)^*$-VCS for monochrome images in which t participants are essential in a (k, n)-VCS. We grouped the minimal qualified sets, taken two at a time, to form systems of linear equations solving which we constructed the initial basis matrices. We then, applied

the technique of deleting the common columns occurring in the initial basis matrices to reduce the pixel expansion. We completely characterize the case of t-$(n-1, n)^*$-VCS by deriving a closed form of the reduced pixel expansion and hence a closed form for the relative contrast too. We further investigated the case of an $(n-2, n)$-VCS and provided an algorithm to collect at least three minimal qualified sets at a time for grouping in such a way that the resulting basis matrices, in their reduced forms, have almost optimal pixel expansions. An interesting open issue would be to compute exact values of the reduced pixel expansions of any t-$(n-2, n)^*$-VCS and more generally of any t-$(k, n)^*$-VCS and derive a closed form for it.

Acknowledgments We would like to thank the anonymous reviewers for their important and helpful comments. Research of the first author is supported by CSIR PhD Fellowship, Government of India, Grant no.-09/028(0808)/2010-EMR-I. Research of the third author is partially supported by National Board for Higher Mathematics, Department of Atomic Energy, Government of India (No 2/48(10)/2013/NBHM(R.P.)/R&D II/695). The third author is also thankful to the Centre of Excellence in Cryptology of Indian Statistical Institute.

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 Cryptogr. **73**(3), 865–895 (2014).
2. Adhikari A., Bose M.: A new visual cryptographic scheme using latin squares. IEICE Trans. Fundam. **E87-A**(5), 1998–2002 (2004).
3. Adhikari A., Sikdar S.: A new (2, n)-color visual threshold scheme for color images. In: INDOCRYPT'03, Lecture Notes in Computer Science, vol. 2904, pp. 148–161. Springer, Berlin (2003).
4. Adhikari A., Dutta T.K., Roy B.: A new black and white visual cryptographic scheme for general access structures. In: INDOCRYPT'04, Lecture Notes in Computer Science, vol. 3348, pp. 399–413. Springer, Berlin (2004).
5. Adhikari A., Kumar D, Bose M., Roy B.: Applications of partially balanced and balanced incomplete block designs in developing visual cryptographic schemes. IEICE Trans. Fundam. Jpn. **E-90A**(5), 949–951 (2007).
6. Arumugam S., Lakshmanan R., Nagar A.K.: On (k, n)*-visual cryptography scheme. Des. Codes Cryptogr. **71**(1), 153–162 (2014).
7. Ateniese G., Blundo C., De Santis A., Stinson D.R.: Visual cryptography for general access structures. Inf. Comput. **129**, 86–106 (1996).
8. Ateniese G., Blundo C., De Santis A., and Stinson D.R.: Constructions and bounds for visual cryptography. In: 23rd International Colloquium on Automata, Languages and Programming (ICALP '96). Lecture Notes in Computer Science, vol. 1099, pp. 416–428. Springer, Berlin (1996).
9. Blundo C., De Santis A.: Visual cryptography schemes with perfect reconstruction of black pixels. Comput. Graph. **22**, 449–455 (1998).
10. Blundo C., De Santis A., Stinson D.R.: On the contrast in visual cryptography schemes. J. Cryptol. **12**(4), 261–289 (1999).
11. Blundo C., Bonis A.D., Santis A.D.: Improved schemes for visual cryptography. Des. Codes Cryptogr. **24**, 255–278 (2001).
12. Blundo C., D'arco P., De Santis A., Stinson D.R.: Contrast optimal threshold visual cryptography. SIAM J. Discret. Math. **16**(2), 224–261 (2003).
13. Bose M., Mukerjee R.: Optimal (k, n) visual cryptographic schemes for general k. Des. Codes Cryptogr. **55**(1), 19–35 (2010).
14. Guo T., Liu F., Wu C., Ren Y.W., Wang W.: On (k, n) visual cryptography scheme with t essential parties. In: ICITS 2013. Lecture Notes in Computer Science, pp. 56–68. Springer, Berlin (2013).
15. Cimato S., Prisco R.D., Santis A.D.: Optimal colored threshold cisual cryptography schemes. Des. Codes Cryptogr. **35**, 311–335 (2005).
16. Cimato S., De Prisco R., De Santis A.: Colored visual cryptography without color darkening. Theor. Comput. Sci. **374**(1–3), 261–276 (2007).
17. Droste S.: New results on visual cryptography, advance in cryptography. In: CRYPTO'96. Lecture Notes in Computer Science, vol. 1109, pp. 401–415. Springer, Berlin (1996).

18. Ishihara T., Koga H.: New constructions of the lattice-based visual secret sharing using mixture of colors. IEICE Trans. Fundam. **E85-A**(1), 158–166 (2002).
19. Koga H.: A general formula of the (t, n)-threshold visual secret sharing scheme. In: ASIACRYPT 2002. Lecture Notes in Computer Science, vol. 2501, pp. 328–345. Springer, Berlin (2002).
20. Naor M., Shamir A.: Visual cryptography, advance in cryptography. In: EUROCRYPT'94. Lecture Notes in Computer Science, vol. 950, pp. 1–12. Springer, Berlin (1994).
21. Shyu S.J.: Image encryption by random grids. Pattern Recognit. **40**(3), 1014–1031 (2007).
22. Shyu S.J.: Image encryption by multiple random grids. Pattern Recognit. **42**(7), 1582–1596 (2009).
23. 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).
24. Verheul E.R., Tilborg V.H.C.A.: Constructions and properties of k out of n visual secret sharing schemes. Des. Codes Cryptogr. **11**, 179–196 (1997).
25. Wang D.S., Yi F., Li X.: On general construction for extended visual cryptography schemes. Pattern Recognit. **42**(11), 3071–3082 (2009).