A new visual cryptography scheme for STS based access structures

Sucheta Chakrabarti[*]

R. K. Khanna[†]

Scientific Analysis Group

DRDO

Metcalfe House Complex

Delhi 110 054

India

Abstract

Visual Cryptography Scheme (VCS) for general access structure was developed by Ateniese, Blundo, Santis and Stinson in 1996 for black and white image and subsequently different schemes have been developed. In this paper, we propose a new model for Steiner Triple Systems (STS) based access structures by using "stacking" i.e. "superimposition" and "machine operation" which are mathematically equivalent to "*OR*" and "*XOR*" respectively. The concept of qualified set is extended. The technique to construct the VCS is developed for the model. The structure of the VCS is analysed. The contrast of the reconstructed secret image (SI) under the two operations is studied. Finally we introduce STS based $(3, n)$-Visual Threshold Scheme (VTS) and derive the ratio of its pixel expansion and the number of qualified sets.

Keywords : *Visual cryptographic scheme, visual threshold scheme, secret sharing, secret image, balanced incomplete block designs (BIBD), Steiner triple systems, access structure.*

1. Introduction

A visual cryptography scheme for black and white image was introduced by Naor and Shamir [5] in 1994 which can reconstruct the secret image by the human visual system. This can be used by anyone

[*] *E-mail*: suchetadrdo@hotmail.com

[†] *E-mail*: rkk321@hotmail.com

Journal of Discrete Mathematical Sciences & Cryptography
Vol. 9 (2006), No. 1, pp. 9–23

without any knowledge of cryptography and without performing any cryptographic computations. It is a method for a set P of n participants to encode a secret image into n images, called shares such that each participant in P receives one image. The qualified subsets of participants can "visually" recover the secret image, but forbidden sets of participants have no information about the secret image. A "visual" recovering of the secret image for a set $X \subseteq P$ has been done by "stacking" the images associated to participants in X. This physical operation "stacking" is mathematically equivalent to the operation "*OR*". In [5] (k, n)-VTS has been given in which the secret image is visible if any k images are stacked together but there will be no information gain if less than k images are stacked. The scheme is perfectly secure and easy to implement. Visual cryptographic schemes with extended capabilities have been studied in [2]. In [1] Naor and Shamir's model has been extended to general access structures with the specification of all qualified and forbidden subsets of participant set. Two techniques, one based on cumulative arrays and the other one consider the smaller schemes as building blocks for construction of VCS for the general access structures have been proposed in [1].

In this paper we introduce a new model for STS based access structures. A new concept *negative version of the image* for the black and white image is introduced by us which is used for the reconstruction of the same secret image. With this new concept the definition of qualified set in [1] is extended. The model is proposed for two different operations viz. "*OR*" i.e. "*Stacking*" and "*XOR*" i.e. "*machine operation*", which is also quite simple to compute. The technique to construct the VCS for the model is given. This is a generalization of the BIBD oriented schemes. Here the new method is given and applied first by us for the construction of the basis matrices for white pixels. This is different from the earlier used methods. We analyze the structure of the VCS and prove the improvement in the contrast by using the operation "*XOR*" compare to the operation "*OR*" with same pixel expansion. The visual cryptographic scheme is explained with the help of an example. In the Appendix we consider a secret image and illustrate the share generated by the VCS for each participant, the reconstructed image of some members of extended qualified set and forbidden set of the example. We introduce STS based $(3, n)$-VTS. It has a distinct advantage over the schemes proposed in [1]. This scheme has less ratio between pixel expansion and number of qualified sets of size 3. In other words, it gives better contrast for the qualified sets of size 3 which belong to the minimal qualified set of STS based access structures.

2. Preliminaries

In this section the basic definitions, properties and some results of combinatorial design theory [4], [7], [8] and visual cryptography [1], [3] have been given.

Definition 2.1. Let $v, k,$ and λ be positive integers such that $v > k \geq 2$. A *(v, k, λ)-balanced incomplete block design (BIBD)* is a pair $(X, \mathcal{A})$ such that the following properties are satisfied:

1. X is a set of v elements called *points*,
2. $\mathcal{A}$ is a collection of subsets of X called *blocks*,
3. each block contains exactly k *points*, and
4. every pair of distinct points is contained in exactly λ *blocks*.

Two basic properties of BIBDs are as follows:

Theorem 2.1. *In a (v, k, λ)-BIBD, every point occurs in exactly $r = \dfrac{\lambda(v-1)}{k-1}$ blocks.*

Theorem 2.2. *The number of blocks in a (v, k, λ)-BIBD is exactly $b = \dfrac{vr}{k} = \dfrac{\lambda(v^2 - v)}{k^2 - k}$.*

Definition 2.2. Let $(X, \mathcal{A})$ be a (v, k, λ)-BIBD, where $X = \{x_1, \dots, x_v\}$ and $\mathcal{A} = \{A_1, \dots, A_b\}$. The *incidence matrix* of $(X, \mathcal{A})$ is the $v \times b$ $0-1$ matrix $M = (m_{i,j})$ defined as follows:

$$m_{i,j} = \begin{cases} 1 & \text{if } x_i \in A_j \\ 0 & \text{if } x_i \notin A_j \,. \end{cases}$$

Definition 2.3. A *Steiner Triple Systems* (STS) of order v is a $(v, 3, 1)$-*BIBD*. In other words an STS on the set X is a collection $\mathcal{S}_X$ of three element subsets of X called blocks such that, any pair of distinct elements of X is contained in a unique block of $\mathcal{S}_X$.

The necessary and sufficient condition for the existence of an STS of order v is given below:

Theorem 2.3. *There exists an STS of order v if and only if $v \equiv 1, 3 \bmod 6$.*

Definition 2.4. Suppose $(X, \mathcal{A})$ and $(Y, \mathcal{B})$ are two (v, k, λ)-*BIBDs*. They are said to be isomorphic if there exists a bijection $\alpha : X \rightarrow Y$ such that

$$\{\alpha(x) : X \in A \in \mathcal{A}\} = \mathcal{B}\,.$$

In other words, if we rename every point $x \in X$ by $\alpha(x)$, then the collection of blocks $\mathcal{A}$ is transformed into $\mathcal{B}$. The bijection α is called an *isomorphism*.

Definition 2.5. Let $P = \{1, \ldots, n\}$ be a set of elements called participants. Let $\Gamma_{\text{Qual}} \subseteq 2^P$ and $\Gamma_{\text{Forb}} \subseteq 2^P$, where 2^P denote the set of all subsets of P such that $\Gamma_{\text{Qual}} \cap \Gamma_{\text{Forb}} = \emptyset$. Members of Γ_{Qual} known as qualified sets and members of Γ_{Forb} are called forbidden sets. The pair $(\Gamma_{\text{Qual}}, \Gamma_{\text{Forb}})$ is called the *access structure* of the VCS.

The set Γ_0 consists of all *minimum qualified* sets i.e.

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

The *access structure* is said to be *strong* if Γ_{Qual} is monotonically increasing, Γ_{Forb} is monotonically decreasing and $\Gamma_{\text{Qual}} \cup \Gamma_{\text{Forb}} = 2^P$. In this case Γ_0 is called a *basis*.

Definition 2.6. Let $(\Gamma_{\text{Qual}}, \Gamma_{\text{Forb}})$ be an access structure on a set of n participants. Two collections of $n \times m$ Boolean matrices $\mathcal{C}_0$ and $\mathcal{C}_1$ constitute a visual cryptographic scheme $(\Gamma_{\text{Qual}}, \Gamma_{\text{Forb}}, m)$-VCS, where m is the pixel expansion i.e. each pixel of the SI consists of m subpixels, if there exist the value $\alpha(m)$ and the set $\{(X, t_X)\}_{X \in \Gamma_{\text{Qual}}}$ satisfying:

1. Any (qualified) set $X = \{i_1, \ldots, i_p\} \in \Gamma_{\text{Qual}}$ can recover the secret image by stacking their transparencies.

   Formally, for any $\mathcal{M} \in \mathcal{C}_0$, the "or" *m-vector* V of rows $i_1, i_2, \ldots, i_p$ satisfies $wt(V) \leq t_X - \alpha(m) \cdot m$; whereas, for $\mathcal{M} \in \mathcal{C}_1$ it results that $wt(V) \geq t_X$.
2. Any (forbidden) set $X = \{i_1, \ldots, i_p\} \in \Gamma_{\text{Forb}}$ has no information on the secret image.

   Formally, the two collections of $p \times m$ matrices D_t with $t \in \{0, 1\}$ obtained by restricting each $n \times m$ matrices in $\mathcal{C}_t$ to rows $i_1, i_2, \ldots, i_p$ are indistinguishable in the sense that they contain the same matrices with the same frequencies.

Here we mention two important results about the pixel expansion m

and threshold value t_X of the qualified set X of (k, n)-VTSs which were proposed in [1].

Theorem 2.4. *Let* $(\Gamma_{\text{Qual}}, \Gamma_{\text{Forb}})$ *be a strong access structure having basis* Γ_0. *There exists a* $(\Gamma_{\text{Qual}}, \Gamma_{\text{Forb}}, m)$*-VCS where* $m = \sum_{X \in \Gamma_0} 2^{|X|-1}$.

Theorem 2.5. *Let* $(\Gamma_{\text{Qual}}, \Gamma_{\text{Forb}})$ *be a strong access structure, and let* Z_M *be the family of the maximal forbidden sets in* Γ_{Forb}. *Then there exists a* $(\Gamma_{\text{Qual}}, \Gamma_{\text{Forb}}, m)$*-VCS with* $m = 2^{|Z_M|-1}$ *and* $t_X = m$ *for any* $X \in \Gamma_{\text{Qual}}$.

3. Model for STS based access structures

Let $P = \{1, \ldots, n\}$ be the set of *participants* where $n \equiv 1, 3 \bmod 6$, having the STS $\mathcal{S}_P$. Let $\mathcal{S}'_P$ be the isomorphic to $\mathcal{S}_P$ such that $\mathcal{S}_P \cap \mathcal{S}'_P = \emptyset$ and $\Gamma^{\text{op}}_{\text{EQual}} = \Gamma_{\text{EQual}} = \Gamma_{+\text{iveQual}} \cup \Gamma_{-\text{iveQual}} \subset 2^P$ with op $\in \{\text{"}OR\text{"}, \text{"}XOR\text{"}\}$, where 2^P is the set of all subsets of P.

Here Γ_{EQual} – denotes *extended qualified set* consisting of members which are *qualified sets* in the sense that they will be able to reconstruct secret image either as it is or the negative version by the operation "*OR*" (stacking) and by "*XOR*" (machine operation).

$\Gamma_{+\text{iveQual}}$ – denotes *positive qualified set* of members called *positive qualified* sets which recover the secret image as it is (positive version)by the above mentioned operations.

$\Gamma_{-\text{iveQual}}$ – denotes *negative qualified set* of members called *negative qualified* sets which recover negative version of the secret image by the same operations.

Unless otherwise stated the qualified sets include both. The positive and the negative qualified set are specified as follows:

$$\begin{aligned}
\Gamma_{+\text{iveQual}} &= \{X \subset P : |X| \geq 3 \text{ and } |Y_X \cap \mathcal{S}_P| > |Y_X \cap \mathcal{S}'_P|\}, \\
\Gamma_{-\text{iveQual}} &= \{X \subset P : |X| \geq 3 \text{ and } |Y_X \cap \mathcal{S}'_P| > |Y_X \cap \mathcal{S}_P|\},
\end{aligned}$$

where

$$Y_X = \{U \subset X : |U| = 3\}. \tag{3.1}$$

Let $\Gamma_{\text{Forb}} \subseteq 2^P$ where $\Gamma_{\text{EQual}} \cap \Gamma_{\text{Forb}} = \emptyset$.

Γ_{Forb} – denotes the *forbidden set* consists of members which are *forbidden sets* i.e. they will be unable to retrieve any information under the specific operations.

Here, $\Gamma_{\text{Forb}} = \{X \subseteq P : Y_X \cap (\mathcal{S}_P \cup \mathcal{S}'_P) = \emptyset\}$; where Y_X is as defined in (3.1). Note that all single element sets and two elements sets are obviously forbidden sets since in both cases $Y_X = \emptyset$.

The pair $(\Gamma_{\text{EQual}}, \Gamma_{\text{Forb}})$ is called *the STS access structure*.

The set Γ_0 consists of all *minimal qualified sets* i.e.

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

So for this structure $\Gamma_0 = \mathcal{S}_P \cup \mathcal{S}'_P$, $|A| = 3$ and $|\Gamma_0| = n(n-1)/3$.

The *STS access structure* is not *strong* since qualified sets are not monotonically increasing. It is also noted that if a set of participants X is a superset of a qualified set X', then they can retrieve the secret image by considering only the shares of the set X'. This does not in itself rule out the probability that all shares of the participants in X under the operations do not reveal any information about the secret image. In this accesses structure the forbidden sets are monotonically decreasing.

Here we assume that the image consists of a collection of black and white pixels. Each pixel of the original image will be encoded into n pixels, each of which consists of m subpixels. We therefore define two collections of Boolean matrices $\mathcal{C}_0, \mathcal{C}_1$ of $n \times m$ such that $\mathcal{C}_0 \cap \mathcal{C}_1 = \emptyset$. To encode a white (black, resp.) pixel we choose a random $M \in \mathcal{C}_0$, ($\mathcal{C}_1$, resp.) and on share i we place m subpixels listed in row i of M. The chosen matrix defines the m subpixels in each of the n shares. The realization of the scheme lies in the way $\mathcal{C}_0$ *and* $\mathcal{C}_1$ are chosen.

We formalize the requirements of a VCS for the model in the following definition, which is an extension that given in [1], [5].

Definition 3.1. Let $(\Gamma_{\text{EQual}}, \Gamma_{\text{Forb}})$ be an STS access structure on a set of n-participants. Two collections of $n \times m$ Boolean matrices $\mathcal{C}_0$ and $\mathcal{C}_1$ constitute a visual cryptographic scheme $(\Gamma_{\text{EQual}}, \Gamma_{\text{Forb}}, m)$-VCS under the operation *"OR"* and *"XOR"* if there exist the value $\alpha_{\text{op}}(m)$ and the set $\{(X, t_X^{\text{op}})\}_{X \in \Gamma_{\text{EQual}}}$ with op $\in$ {*"OR"*, *"XOR"*} satisfying:

1. Any (extended qualified) set $X = \{i_1, i_2, \ldots, i_p\} \in \Gamma_{\text{EQual}}$ can recover the positive or negative version of the shared secret image by *"stacking"* (*super imposition*) and by using *"machine operation"* of their shares.

   Formally, for any $M \in \mathcal{C}_0$ ($M \in \mathcal{C}_1$ *respectively*) the Hamming weight $wt_{\text{op}}(V)$ of the m-vector V which is equal to "op" of rows $i_1, i_2, \ldots, i_p$ satisfies $wt_{\text{op}}(V) \leq t_X^{\text{op}} - \alpha_{\text{op}}(m) \cdot m$; whereas, for any

$M \in \mathcal{C}_1$ ($M \in \mathcal{C}_0$ *respectively*) it results that $wt_{\text{op}}(V) \geq t_X^{\text{op}}$ for positive (negative respectively) qualified sets.

2. Any (forbidden) set $X = \{i_1, \ldots, i_p\} \in \Gamma_{\text{Forb}}$ has no information on the secret image.

   Formally, the two collections of $p \times m$ matrices D_t with $t \in \{0, 1\}$ obtained by restricting each $n \times m$ matrices in $\mathcal{C}_t$ to rows $i_1, i_2, \ldots, i_p$ are indistinguishable in the sense that they contain the same matrices with the same frequencies.

The 1st property is related to the contrast of the image. The value $\alpha_{\text{op}}(m)$ is called *relative difference* or *relative contrast* for the operation "op", the number $\alpha_{\text{op}}(m) \cdot m$ is referred to as the contrast of the image, the set $\{(X, t_X^{\text{op}})\}_{X \in \Gamma_{\text{EQual}}}$ is called the set of thresholds, and t_X^{op} is the threshold associated to $X \in \Gamma_{\text{EQual}}$ for the operation "op". The 2nd property is called the security condition.

3.1 *Basic matrices for STS based access structures*

The VCS for STS access structure in this paper is constructed by using $n \times m$ matrices $\mathcal{S}^0$ *and* $\mathcal{S}^1$, called *STS basis matrices*. The families $\mathcal{C}_0$ and $\mathcal{C}_1$ can be constructed by taking every column permutation of the $\mathcal{S}^0$ and $\mathcal{S}^1$ respectively. The *STS basis matrices* $\mathcal{S}^0$ *and* $\mathcal{S}^1$ must satisfy properties very similar to the Definition 3.1 which are given below:

Definition 3.2. Let $(\Gamma_{\text{EQual}}, \Gamma_{\text{Forb}})$ be an *STS access structure* on a set of n-participants. A $(\Gamma_{\text{EQual}}, \Gamma_{\text{Forb}}, m)$-VCS under the operation *"OR"* and *"XOR "* with relative difference $\alpha_{\text{op}}(m)$ and set of thresholds $\{(X, t_X^{\text{op}})\}_{X \in \Gamma_{\text{EQual}}}$ for op $\in$ {*"OR"*, *"XOR"*} is realized using the two $n \times m$ STS basis matrices $\mathcal{S}^0$ and $\mathcal{S}^1$ if the following conditions hold:

1. If $X = \{i_1, \ldots, i_p\} \in \Gamma_{\text{EQual}}$, then the "op" *m-vector* V of rows $i_1, i_2, \ldots, i_p$ of $\mathcal{S}^0$ ($\mathcal{S}^1$ respectively) satisfies $wt_{\text{op}}(V) \leq t_X^{\text{op}} - \alpha_{\text{op}}(m) \cdot m$; whereas, for $\mathcal{S}^1$ ($\mathcal{S}^0$ respectively) it results that $wt_{\text{op}}(V) \geq t_X^{\text{op}}$ for $X \in \Gamma_{+\text{iveQual}}$ ($X \in \Gamma_{-\text{iveQual}}$ respectively).
2. If $X = \{i_1, \ldots, i_p\} \in \Gamma_{\text{Forb}}$ then the two $p \times m$ matrices obtained by restricting $\mathcal{S}^0$ and $\mathcal{S}^1$ to rows $\{i_1, \ldots, i_p\}$ are equal up to column permutation.

Example 3.1. Let $n = 7$ be the number of participants i.e. the set of participants $P = \{1, 2, 3, 4, 5, 6, 7\}$.

Let $\mathcal{S}_P = \{\{1,2,4\},\{2,3,5\},\{3,4,6\},\{4,5,7\},\{1,5,6\},\{2,6,7\},\{1,3,7\}\}$.

Let $\alpha : P \to P$ be a bijective mapping as follows:

$1 \to 4, 2 \to 6, 3 \to 5, 4 \to 7, 5 \to 3, 6 \to 1, 7 \to 2$.

Hence, $\alpha(\mathcal{S}_P) = \mathcal{S}'_P = \{\{4,6,7\},\{6,5,3\},\{5,7,1\},\{7,3,2\},\{4,3,1\},\{6,1,2\},\{4,5,2\}\}$.

Therefore, $\mathcal{S}'_P$ is isomorphic to $\mathcal{S}_P$. Here, $\mathcal{S}_P \cap \mathcal{S}'_P = \emptyset$.

In this case the incidence matrices of $\mathcal{S}_P$ and $\mathcal{S}'_P$ are actually the basis matrices $\mathcal{S}^1$ and $\mathcal{S}^0$ respectively. It is easy to see that these two incidence matrices satisfy the conditions of basis matrices.

Here $n = 7$ *and* $m = b-$ *number of blocks in STS* $= 7$.

Then the two 7×7 STS basis matrices are as follows:

$$\mathbf{S^0} = \begin{bmatrix} 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 \end{bmatrix}, \quad \mathbf{S^1} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}.$$

Here the relative difference for the STS basis matrices is

$$\alpha_{\text{op}}(7) = \begin{cases} 1/7 & \text{if “op” = “}OR\text{”} \\ 4/7 & \text{if “op” = “}XOR\text{”}. \end{cases}$$

3.2 *Construction for VCS using STS basis matrices*

Let $(\Gamma_{\text{EQual}}, \Gamma_{\text{Forb}})$ be an STS access structure on the set P having the STS $\mathcal{S}_P$. Let Γ_0 denote the collection of all minimal qualified sets of Γ_{EQual} i.e. $\Gamma_0 = \{X \in \Gamma_{\text{EQual}} : X \setminus i \in \Gamma_{\text{Forb}} \text{ for all } i \in X\}$. A set $\mathcal{S}'_P$ is isomorphic to $\mathcal{S}_P$ for the given structure if there exists a bijective mapping $\alpha : P \to P$ with $\mathcal{S}'_P = \{\alpha(B) : B \in \mathcal{S}_P\}$ such that $i \in B \Leftrightarrow \alpha(i) \in \alpha(B)$ for $i \in P$ and $\mathcal{S}_P \cap \mathcal{S}'_P = \emptyset$. Hence, $\Gamma_0 = \mathcal{S}_P \cup \mathcal{S}'_p$. Then the *incidence matrices* $\mathcal{S}_P$ and $\mathcal{S}'_P$ play the role of $\mathcal{S}^1$ and $\mathcal{S}^0$ respectively for $(\Gamma_{\text{EQual}}, \Gamma_{\text{Forb}}, m)$-VCS where $m = |\Gamma_0|/2$.

From the properties of STS ([4], [7], [8]) the following result follows for STS access structures:

Theorem 3.1. *If* $X \in \Gamma_0$ *then* t_X^{op} *is constant with* op $\in$ {*“OR”, “XOR”*} *and* $t_X^{\text{op}} = 3r - 2$ *where r is the number of* 1*’s in a row of an STS basis matrices.*

Proof. From the property of STS we know that any two members belong to a unique block and each member belongs to r number of blocks. Now $X \in \Gamma_0$ implies that the three participants in X which belong to a single block of the STS. So it follows immediately that $t_X^{\text{op}} = 3r - 2$. □

Theorem 3.2. *If the number of participants is n then the maximum number of members in a qualified set is* $n - 3$.

Proof. It follows immediately from the properties of STS that for $|X| > n - 3$, $wt_{\text{op}}(V)$ of X for STS basis matrices $\mathcal{S}^0$ *and* $\mathcal{S}^1$ are equal. □

Note that this never rule out the existence of neither forbidden nor qualified set of size $n - 3$. Now we will prove the result about the the contrast of the VCS for STS access structure by using STS basis matrices under the two operations.

Theorem 3.3. *For* $(\Gamma_{\text{EQual}}, \Gamma_{\text{Forb}})$*-STS access structure on the participant set* $P = \{1, 2, \ldots, n\}$*, the* $(\Gamma_{\text{EQual}}, \Gamma_{\text{Forb}}, m)$*-VCS gives the relative contrast* $\alpha_{OR}(m) = (1/m)$ *and* $\alpha_{XOR}(m) = 4/m$ *for* $X \in \Gamma_{\text{EQual}}$ *and* $|\,|Y_X \cap \mathcal{S}_P| - |Y_X \cap \mathcal{S}'_P|\,| = 1$ *where* Y_X *is as defined in (3.1).*

Proof. Let $\mathcal{S}^0$ and $\mathcal{S}^1$ be the $n \times m$ STS basis matrices for the STS access structure. Let $|Y_X \cap \mathcal{S}_P| = q$ and $|Y_X \cap \mathcal{S}'_P| = q - 1$ and vice versa for $X \in \Gamma_{+\text{iveQual}}$ and $X \in \Gamma_{-\text{iveQual}}$ respectively. By the properties of STS we get that if $X = \{i_1, i_2, \ldots, i_p\} \in \Gamma_{\text{EQual}}$ then $wt(V)$ of m vector $V = OR$ (rows$\{i_1, \ldots, i_p\}$) $= pr - {}^pC_2 + q = \beta$ associated with $\mathcal{S}^1$ and $wt(V) = pr - {}^pC_2 + (q-1) = \gamma$ associated with $\mathcal{S}^0$ and vice versa for $X \in \Gamma_{+\text{iveQual}}$ and $X \in \Gamma_{-\text{iveQual}}$ where p is the number of the participants in the set X, r is the number of 1's in a row of $\mathcal{S}^i$, $i \in \{0, 1\}$ and ${}^pC_2$ is the total number of combinations of 2 participants out of p participants. So the relative contrast $\alpha_{OR}(m) = |\beta - \gamma| = 1/m$.

Now $wt(V)$ of *m-vector* $V = XOR(\text{rows}\{i_1, \ldots, i_p\}) = pr - 2({}^pC_2) + 4q = \beta'$ associated with $\mathcal{S}^1$ and $wt(V) = pr - 2({}^pC_2) + 4(q-1) = \gamma'$ associated with $\mathcal{S}^0$ and vice versa for $X \in \Gamma_{+\text{iveQual}}$ and $X \in \Gamma_{-\text{iveQual}}$. So the relative contrast $\alpha_{XOR}(m) = |\beta' - \gamma'| = 4/m$. □

Corollary 3.1. *If* $|X| \geq 3$ *then X is a forbidden set if and only if* $|Y_X \cap \mathcal{S}_P| = |Y_X \cap \mathcal{S}'_P| = 0$ *where* Y_X *is as in* (3.1).

Corollary 3.2. *Let* $X \in \Gamma_{\text{EQual}}$ *then* t_X^{op} *is constant for all X of same cardinality.*

Corollary 3.3. *If* $|X| > 3$ *then it is neither forbidden nor qualified set if and only if* $|Y_X \cap \mathcal{S}_P| = |Y_X| \cap \mathcal{S}'_P| \neq 0$.

We give the following example to illustrate all results:

Example 3.2. Let the set of $n = 7$ *participants* $P = \{1, 2, 3, 4, 5, 6, 7\}$.

Let $\mathcal{S}_P = \{\{1, 2, 4\}, \{2, 3, 5\}, \{3, 4, 6\}, \{4, 5, 7\}, \{1, 5, 6\}, \{2, 6, 7\}, \{1, 3, 7\}\}$ and α be a bijective mapping as defined in Example 3.1.

So $\mathcal{S}'_P = \{\{4, 6, 7\}, \{6, 5, 3\}, \{5, 7, 1\}, \{7, 3, 2\}, \{4, 3, 1\}, \{6, 1, 2\}, \{4, 5, 2\}\}$.

The $\Gamma_{\text{EQual}} = \Gamma_{\text{+iveQual}} \cup \Gamma_{\text{−iveQual}}$ is as follows:

$$\left\{\begin{array}{c} \{1,2,4\}, \{2,3,5\}, \{3,4,6\} \\ \{4,5,7\}, \{1,5,6\}, \{2,6,7\}, \\ \{1,3,7\}, \{1,2,3,5\}, \{1,2,4,7\} \\ \{1,3,6,7\}, \{1,4,5,6\}, \{2,3,4,6\}, \\ \{2,5,6,7\}, \{3,4,5,7\} \end{array}\right\} \cup \left\{\begin{array}{c} \{4,6,7\}, \{6,5,3\}, \{5,7,1\} \\ \{7,3,2\}, \{4,3,1\}, \{6,1,2\}, \\ \{4,5,2\}, \{1,2,3,6\}, \{1,2,5,7\} \\ \{1,3,4,5\}, \{1,4,6,7\}, \{2,3,4,7\} \\ \{2,4,5,6\}, \{3,5,6,7\} \end{array}\right\}$$

Here, $\Gamma_{\text{Forb}} = \{\{x\}, \{x, y\}$ where $x, y \in P$ and $Y_P \setminus \Gamma_0\}$.

So, here $(\Gamma_{\text{EQual}}, \Gamma_{\text{Forb}})$ is the STS access structure. The $(\Gamma_{\text{EQual}}, \Gamma_{\text{Forb}}, 7)$-VCS for the STS access structures is constructed by using the following STS basis matrices $\mathcal{S}^0$ and $\mathcal{S}^1$:

$$\mathbf{S^0} = \begin{bmatrix} 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 \end{bmatrix}, \quad \mathbf{S^1} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}.$$

If $X = \{i_1, i_2, i_3\} \subset P$ and $X \notin \mathcal{S}_P \cup \mathcal{S}'_P$ then op(rows $\{i_1, i_2, i_3\}$) of $\mathcal{S}^0$ and $\mathcal{S}^1$ are equal for op $\in \{$*"OR"*, *"XOR"*$\}$ i.e. they are forbidden sets. viz. the set $X = \{1, 2, 3\}$. So, $\Gamma_0 = \{\mathcal{S}_P \cup \mathcal{S}'_P\}$. In the scheme each pixel of original image is encoded into $n = 7$ pixels, each of which consists of $m = n(n - 1)/6 = 7$ subpixels. The threshold value of X is $t_X^{\text{op}} = 3 \cdot 3 - 2 = 7$ with op $\in \{$*"OR"*, *"XOR"*$\}$ for all $X \subset P \in \Gamma_0$. Maximum size of qualified set is $7 - 3 = 4$. But there exist neither forbidden nor qualified sets of size 4, viz. the set $X = \{1, 2, 3, 4\}$. The relative difference for the extended qualified set is $1/7$ and $4/7$ under the operation *"OR"* and *"XOR"* respectively. The property 2 of the Definition 3.2 is easily verified for the forbidden set. This is not a strong access structure since not all superset of $X \in \Gamma_0$ are qualified, viz. the set $\{2, 3, 5, 6\}$. Also all subsets of a forbidden set is forbidden, viz.

$\{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\} \subset \{1,2,3\}$ which are forbidden sets.

4. STS based $(3,n)$-VTS

The VCS for STS access structure on a participant set $n \equiv 1,3 \bmod 6$ constructed above also equivalent to $(3,n)$-VTS where the qualified sets of 3 participants belong to the minimal extended qualified set Γ_0, called STS based $(3,n)$-VTS. The following result holds from the properties of the VCS for STS access structures.

Theorem 4.1. *For the STS based $(3,n)$-VTS on a participant set $\{1,2,\ldots,n\}$ the expansion of the pixel is $m = n(n-1)/6$ and the number of qualified sets is $n(n-1)/3 = 2m$.*

Proof. In STS based $(3,n)$-VTS the pixel expansion m is equal to the number of blocks in STS. So $m = n(n-1)/6$ and the number of qualified sets is equal to $|\Gamma_0| = 2(n(n-1)/6) = 2m$. □

We can verify this result in the Example 3.2.

The ratio between the expansion of the pixel and the number of qualified sets of the two constructions based on the techniques described in (4.1 and 4.2 of [1]) for $(3,n)$-VTS are as follows:

(i) $2^{\binom{n}{2}-1} : \binom{n}{3}$;

(ii) $4\binom{n}{3} : \binom{n}{3}$ i.e. $4:1$

In our construction the ratio is

(iii) $\frac{1}{n-2}\binom{n}{3} : \frac{2}{n-2}\binom{n}{3}$ i.e. $1:2$

which clearly depicts the advantage in the relative contrast for the qualified sets of size 3.

For $n = 7$ the three ratios are $2^{140} : 35$; $4:1$ and $1:2$, respectively.

5. Conclusion

The model proposed is online workable and gives better visual performance under "machine operation". Also proposed $(3,n)$-VTS gives better relative contrast compare to the schemes in [1]. The VCS for STS access structures can be applied in the scenario where we need restricted qualified set. It increases the secrecy in a sense that any three members can't read the secret message but only some particular combinations of three members can read the secret message. The method may be generalized for Steiner systems, other BIBDs and also for colour images.

6. Appendix

6.1 *Pictorial presentation of VCS for STS based access structure*

Here pictorial presentation of the secret image, the share corresponding to participants and few members of extended qualified set and forbidden set of the Example 3.2 are given below:

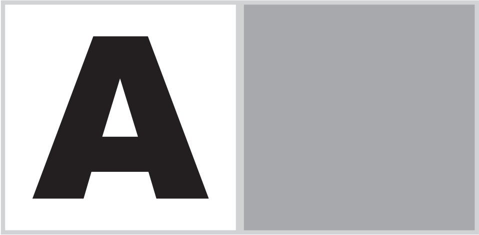

Figure 1
(left) Secret image, (right) Share of single participant

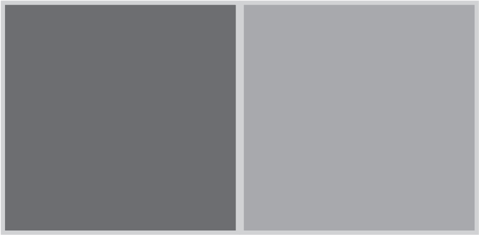

Figure 2
Image of participants 1 and 2 (left) Under OR (right) Under XOR

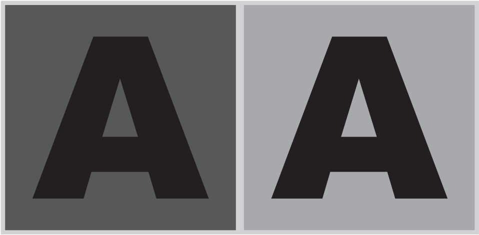

Figure 3
Image of participants 1, 2 and 4 (left) Under OR (right) Under XOR

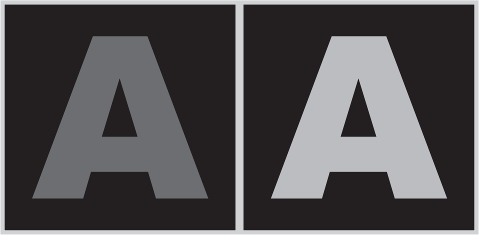

Figure 4
Image of participants 4, 6 and 7 (left) Under OR (right) Under XOR

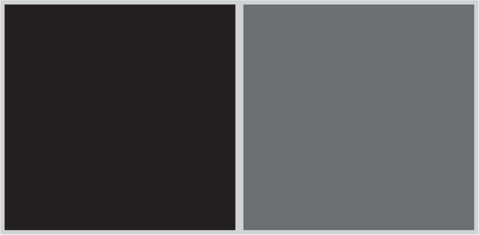

Figure 5
Image of participants 1, 2 and 3 (left) Under OR (right) Under XOR

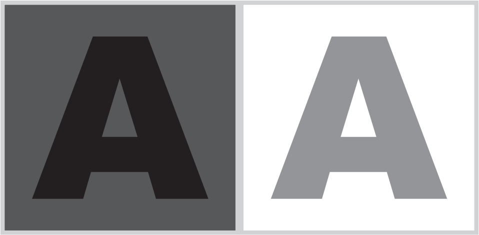

Figure 6
Image of participants 1, 2, 4 and 7 (left) Under OR (right) Under XOR

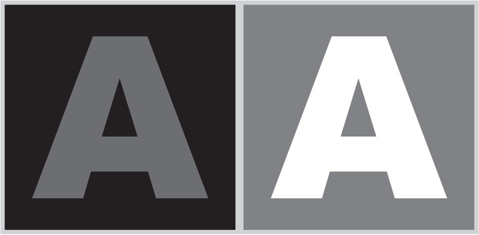

Figure 7
Image of participants 1, 3, 4 and 5 (left) Under OR (right) Under XOR

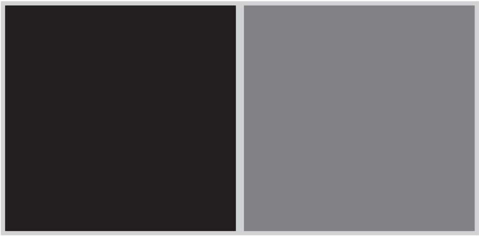

Figure 8
Image of participants 2, 3, 4 and 5 (left) Under OR (right) Under XOR

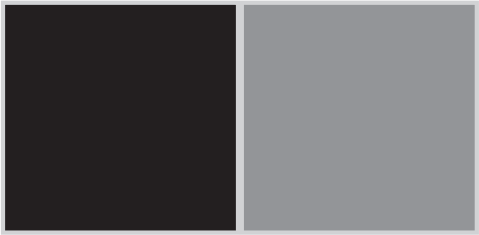

Figure 9
Image of participants 2, 3, 5, 6 and 7 (left) Under OR (right) Under XOR

Acknowledgements. Authors are grateful to Dr. P. K. Saxena, Director, SAG, DRDO for his permission and constant encouragement for the research. Our heartiest thanks to Professor Bimol Roy, ISI, Kolkata; S. K. Pal, SAG, Delhi for valuable discussions and comments for the improvements of the paper.

References

[1] G. Ateniese, C. Blundo, A. De Santis and D. R. Stinson, Visual cryptography for general access structures, *Information and Computation*, Vol. 129 (1996), pp. 86–106.

[2] G. Ateniese, C. Blundo, A. De Santis and D. R. Stinson, Extended capabilities for visual cryptography, *Theoretical Computer Science*, Vol. 250 (2001), pp. 143–161.

[3] P. A. Eisen and D. R. Stinson, Threshold visual cryptography schemes with specified whiteness levels of reconstructed pixels, *Designs, Codes and Cryptography*, Vol. 25 (1) (2002), pp. 15–61.

[4] M. Hall, Jr., *Combinatorial Theory,* Wiley-Interscience Publication, 1986.

[5] M. Naor and A. Shamir, Visual Cryptography, Advances in Cryptology – Eurocrypt'94, *Lecture Notes in Computer Science*, Vol. 950 (1995), pp. 1–12.

[6] D. R. Stinson, Visual cryptography or seeing is believing, *Lecture Note*, 2002.

[7] D. R. Stinson, Combinatorial designs with selected applications, *Lecture Note*, 1996.

[8] W. D. Wallis, *Combinatorial Designs*, Marcel Dekker, Inc., 1988.

Received June, 2005