Australian Journal of Basic and Applied Sciences, 2(4): 1239-1245, 2008
ISSN 1991-8178

Visual Cryptography Schemes with Veto Capabilities

[1]Massoud Hadian Dehkordi and [2]Abbas Cheraghi

[1]Department of Mathematics, Iran University of Since & Technology, Tehran, Iran.
[2]Department of Mathematics, Faculty of Khansar, University of Isfahan, Isfahan, Iran.

Abstract: Beutelspacher considered a secret sharing scheme having a veto capability. Obana and Kurosawa proved that there exist no such schemes if we do not assume that the reconstruction machine is trustworthy. Special kind of secret sharing schemes are Visual Cryptography Schemes (VCS). In this paper, we analyze visual cryptography schemes with veto capabilities in which the reconstruction of black pixels is perfect, that is, all the subpixels associated to a black pixel are black. In producing perfect black schemes we use transversal hypergraphs. Our procedure considered a method such that qualified minorities can prevent any other set of participants from reconstructing the secret.

Key words: Secret Sharing Schemes, Visual Cryptography, Hypergraphs, Transversal Sets.

INTRODUCTION

Secret Sharing Scheme is a method of distributing a secret data among a set of participants so that only qualified subsets are able to recover the data and unqualified subsets have no extra information. Shamir and Blakly independently introduced *(k, n)*-threshold schemes (Blakly, G.R., 1979; Shamir, A., 1979) in which a secret S is distributed to n participants in such a way that k or more participants can recover the original secret S and $k - 1$ or fewer participants have no information on S. (A piece of information held by a participant is called his share.) A special kind of secret sharing scheme is *visual cryptography scheme* (VCS). Visual cryptography was first introduced by Naor and Shamir (1997). A VCS is a method to secretly share an image among a given group of participants. A VCS for a set P of n participants encodes a secret image SI into n shadow images which constitute the shares given to the n participants. The shares given to participants in $X \subseteq P$ are xeroxed onto transparencies. If subset X is *qualified* then the participants in X can visually recover the secret image SI by stacking their transparencies without any cryptography knowledge and without performing any cryptographic computation. If X is *forbidden* then its participants have no information on the secret image.

Beutelspacher considered a secret sharing scheme having a veto capability such that qualified minorities can prevent any other set of participants from reconstructing the secret (Beutelspacher, A.). A *(k, h, n)*-threshold scheme with veto is defined as a *(k, n)*-threshold scheme in which h or more participants have this veto capability. Beutelspacher showed a *(k, h, n)*-threshold scheme with veto by using projective geometry. He also showed some attacks against that scheme, and to avoid such attacks he assumed that the secret reconstruction is carried out by a trustworthy machine- one that operates correctly and keeps the received shares secret from all participants. Obana and Kurosawa proved that there exist no such schemes if we do not assume that the reconstruction machine is trustworthy (Obana, S., K. Kurosawa, 1996). So throughout this paper we assume that the person who reconstructs the secret, that is called *Reconstructor* R, is trustworthy.

Blundo *et al.* showed a *(k, h, n)*-threshold scheme with veto (BDGV scheme) by using Reed Solomon codes (Blundo, C., A. De Santis, 1994), and their BDGV scheme also assume a trustworthy reconstruction machine. In this paper, we analyze visual cryptography schemes with veto capabilities in which the reconstruction of black pixels is perfect, that is, all the subpixels associated to a black pixel are black. For producing perfect black schemes we use transversal hypergraphs. This veto procedure considered a method such that qualified minorities can prevent any other set of participants from reconstructing the secret. In this method any qualified minorities can apply positive or negative transparencies until it could reconstruct the secret or veto, respectively.

Corresponding Author: Abbas Cheraghi, Department of Mathematics, Faculty of Khansar, University of Isfahan, Isfahan, Iran.
E-mail: cheraghi@sci.ui.ac.ir

Preliminaries:

2.1. Transversal Sets:

Let $X=\{x_1, x_2, \ldots, x_n\}$ be a finite set. A *hypergraph* on X is a family $H= (E_1, E_2, \ldots, E_m)$ of subsets X such that

$E_i \neq \varnothing \quad (i = 1, 2, \ldots, m)$,

$$\bigcup_{i=1}^{m} E_i = X$$

A set $T \subset X$ is a transversal of H if it meets all the edges, i.e., $T \cap E_i \neq \varnothing$ for $1 \leq i \leq m$. The family of minimal transversals of H constitutes a simple hypergraph on X called the *transversal hypergraph* of H, and is denoted by $T(H)$.

2.2. Visual Cryptography Scheme:

A visual cryptography scheme (VCS) is a method to share an image secretly among a given group of participants. If X is qualified then the participants in X can visually recover the secret image SI by stacking their transparencies without any cryptography knowledge and without performing any cryptographic computation. If X is forbidden then its participants have no information on SI.

A visual cryptography scheme is based on the fact that each pixel of an image is divided into a certain number of m subpixels. This number m is called the *pixel expansion* of the image. Let $P= \{1, 2, \ldots, n\}$ be a set of elements called participants and let 2^P denote the set of all subsets of P. Let $Q \subset 2^P$ and $F \subset 2^P$, where $Q \cap F = \varnothing$. Q is monotonically increasing if $X \in Q$ implies that for all $X \subseteq Y$, $Y \in Q$. We refer to members of Q as *qualified sets* and members of F as *forbidden sets*. We call $\Gamma= (P, Q, F)$ the *access structure* of the scheme. Define Γ_0 to consist of all minimal qualified sets,

$\Gamma_0= \{A | A \in Q \ \& \ B \notin Q, \text{ for all } B \subset A, B \neq A\}$.

In the case where Q is monotone increasing, and $Q \cup F=2^P$, the access structure is said to be *strong*, and Γ_0 is termed a basis. Throughout of this paper we will consider access structures to be strong.

We assume that the message consists of a collection of black and white pixels. Each pixel appears in n versions called shares, one for each transparency. Each share is a collection of m black and white subpixel. The resulting structure can be described by an $n \times m$ Boolean matrix $S = [s_{ij}]$ where $s_{ij} = 1$ if and only if j-th subpixel in the i-th transparency is black.

Let B be a Boolean matrix and B_i be the i-th row vector of B. Let B_i+B_j be the bit-wise OR of vectors B_i and B_j. Let X be a subset $\{i_1, i_2, \ldots, i_q\}$ of a participant set P. We define $OR(B, X) = B_{i_1} + B_{i_2} + \cdots + B_{i_q}$. Let $\omega(v)$ be the Hamming weight of row vector v. For briefly, we let $\omega(B, X) = \omega(OR(B, X))$.

Definition 2.1:

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

1. Any qualified set $X= \{i_1, i_2, \ldots, i_q\} \in Q$ can recover the shared image by stacking their transparencies. Formally, for any "or" V of rows $i_1, i_2, \ldots, i_q$ of S_0 satisfies $\omega(S_0, X) \leq t_X - \alpha(m) \cdot m$; whereas, $\omega(S_1, X) \geq t_X$.
2. Any forbidden set $X = \{i_1, i_2, \ldots, i_q\} \in F$ has no information on the shared image. Formally, the two $q' \times m$ matrices obtained by restricting S_0 and S_1 to rows $i_1, i_2, \ldots, i_{q'}$ are equal up to a column permutation.

The value m is called *pixel expansion*, the value $\alpha(m)$ is called *contrast*. We want the number $\alpha(m) \cdot m$ to be as large as possible and at least one, that is, $\alpha(m) \geq 1/m$. Also, two conditions are called *contrast* and *security*, respectively. Matrices S_0 and S_1 are called *basis matrices*.

The best way to understand visual cryptography is by restoring to an example.

Example 2.1:

Suppose $P=\{1, 2, 3\}$ and consider the strong access structure with basis $\Gamma_0=\{\{i, j\}|i, j \in P \text{ and } i\neq j\}$. This access structure is based on the complete graph with *3* vertices and it is equivalent to a *2* out of *3* threshold structure. The following basis matrices represent a VCS for the strong access structure on the set of participants P with basis Γ_0.

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

In this scheme any pixel of the original image is encoded into four subpixels. Any single share in either S_0 or S_1 is a random choice of two black and two white subpixeles. Any two shares of a white pixel have a combined Hamming weight of *2*, whereas any two shares of a black pixel have a combined Hamming weight of *3*, which looks darker. The visual difference between the two cases becomes clearer as we stack additional transparencies. Then it is straightforward to verify that S_0 and S_1 are basis matrices of a VCS for the basis access structure Γ_0. To do not distort the aspect ratio of the original image it is convenient to arrange the subpixels in a 2×2 array where each share has the form depicted in Figure 1.

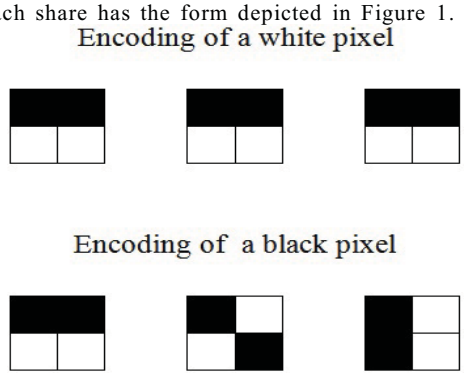

Fig. 1: Shares of the 2 out of 3 Threshold VCS

These shares correspond to the rows of the basis matrices S_0 and S_1, respectively. The subpixels are disposed in a clockwise fashion starting from the upper-left corner of the 2×2 array. Clearly, to any permutation of the columns of S_0 and S_1 will correspond a new rearrangement of the subpixels into the 2×2 array. In this scheme we have, $m=4$ and $\alpha(m)=1/4$.

Visual cryptography schemes for which $t_X= m$, are referred to as visual cryptography schemes with perfect reconstruction of black pixels. Such schemes have been proposed in (Blundo, C., A. De Bonis, 2001; Blundo, C., A. De Santis, 1998). In section 3 we propose visual cryptography schemes with perfect reconstruction of black pixels for strong access structure. It presents a more straight technique with respect to the one proposed in (Ateniese, G., C. Blundo, 1996; Simmons, G.J., W. Jackson, 1991), and it is simpler. Also it has this property that for any qualified set, t_X will remain fixed.

2.3 (k, h, n)-threshold Schemes with Veto:

In a *(k, h, n)*-threshold scheme with veto, there is a dealer D, reconstruction machine R and n participants $p_1, p_2, \ldots, p_n$. Let s denote a secret. In the distribution phase, D randomly produces shares $v_i=(v^P_i, v^N_i)$ for $i = 1, 2, \ldots, n$ on input s, and each p_i gets v_i as his share. v^P_i is called a *positive share* and v^N_i is a *negative share*. In the reconstruction phase, a subset of participants sends v^P_i or v^N_i to R. Assume that R is trustworthy (i.e., that R keeps all inputs secret and operates correctly.) If R receives $k-1$ or fewer shares, R has no information on s, but if R receives h or more negative shares, R cannot reconstruct s. Otherwise, that is, if R receives k or more positive shares and $h-1$ or fewer negative shares, R can determine s uniquely. Beutelspacher showed a *(k, h, n)*-threshold scheme with veto by using projective geometry. His basic *(2, 2, n)*-threshold scheme is described as follows:

Beutelspacher's Scheme:(Beutelspacher, A):

Consider a three-dimensional geometry. We shall restrict ourselves to the three-dimensional projective space $PS=p(3, q)$ of order q. Let U be a nonempty subset of a PS. Then the *span* of U in PS is the set of all possible finite linear combinations of the vectors in U. We use the notation $<U>$ to denote the span of U in PS (for geometric background, see (Beutelspacher, A., 1982; Simmons, G.J., W. Jackson, 1991). Fix a line l_0 and let it be publicly open. Choose a secret point X on the line l_0. Furthermore, choose a line l through X. Let $P=\{v_1^P, v_2^P, \ldots, v_n^P\}$, $N = \{v_1^N, v_2^N, \ldots, v_n^N\}$. Now we define (see Figure 2):

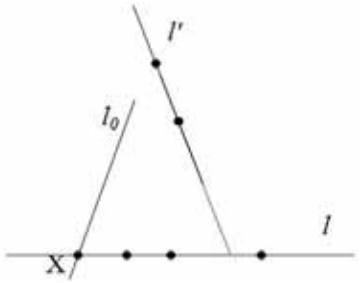

Fig. 2: *(2, 2, n)*-threshold scheme

- a set P of points on the line l intersecting l_0 at X and
- a set N of points distinct from $l' \cap <l, l_0>$ on a line l' skew to l.

Protocol:

If a set U of (positive and negative) points is active (i.e., that R receives a set U of points), then R compute $<U>$ and intersects it with l_0. If $<U> \cap l_0$ is a point, R takes it as the secret.

Analysis:

- If at least two points of P are active, but no point of N is, then R computes l and $l \cap l_0 = X$.
- If at least two points of P and exactly one point Y of N is active, then R computes the plane $E=<l, Y>$: since $Y \notin <l,l_0>$, we have $E \neq <l, l_0>$ so E intersects l_0 only at X.
- If at least two points of P and at least two points of N are active, then R computes $<l, l'>=PS$ intersects it with l_0 and gets l_0. The probability of choosing the correct secret point is only $1/(1 + q)$. So the secret cannot be retrieved.
- If at most one point of P and at least two points of N are active, then R gets a point different from X.

Beutelspacher showed an attack against his own scheme. In his basic *(2, 2, n)* scheme, suppose that R gets $(v_1^P, v_2^P, v_3^N, v_4^N)$ that is, two positive shares and two negatives shares. Then R forms all element subsets of this set and tries each possibility. Now R can get the secret X from (v_1^P, v_2^P).

The Model:

In this section we propose visual cryptography schemes with perfect reconstruction of black pixels for the strong access structure using transversal hypergraphs. It presented a more straight technique in comparison with (Ateniese, G., C. Blundo, 196; Blundo, C., A. De Santis, 1998) to construct perfect black VCS for strong access structure. Thereafter apply it to offer a visual cryptography scheme with veto capability such that qualified minorities can prevent any other set of participants from reconstructing the secret.

Perfect Black Schemes for Strong Access Structure:

Let $P=\{p_1, p_2, \ldots, p_n\}$ be a finite sets of participants. A hypergraph access structure on P is a family $H = (E_1, E_2, \ldots, E_m)$ of minimal qualified subsets of P such that

$E_i \neq \varnothing \quad (i = 1, 2, \ldots, m)$,

$$\bigcup_{i=1}^{m} E_i = P$$

Let $T(H)=(C_1, C_2, \ldots, C_k)$ where C_i are the minimal transversals of H $(1 \le i \le k)$ and k is the number of minimal transversal sets of the hypergraph H and S'_0 and S'_1 be the optimal $k \times 2^{k-1}$ basis matrices for a VCS of the *(k, k)*-threshold access structure mentioned in (Beutelspacher, A.) The dealer gives the *i*-th transparency of this structure to all the members of C_i, and every participant must be stacks his transparencies to obtain his original share.

Theorem 1:

The above construction is a perfect black VCS for any strong access structure $\Gamma = (P, Q, F)$ with pixel expansion 2^{k-1}.

Proof:

Let $\Gamma = (P, Q, F)$ be a strong access structure with the minimal qualified set $Q = \{E_1, E_2, \ldots, E_m\}$, thus we can suppose that Q is a hypergraph with transversal hypergraph $T(Q) = (C_1, C_2, \ldots, C_k)$. Define the sets $U_i = \{j | p_i \in C_j\}$ for $1 \le i \le n$. Then, S_0 and S_1 constitute a basis matrices for Q, in which the i-th row of S_t is $OR(S'_i, U_i)$, for $1 \le i \le n$ and $t \in \{0, 1\}$. If X is an access set there exist at least one E_j such that $E_j \subseteq X$. Hence $X \cap C_i \neq \varnothing$ for every $1 \le i \le k$, so the participants in X have all the k distinct transparencies of the *(k, k)*-threshold access structure and they can recover the secret image *SI*. But if X' is not an access set it means that $E_j \not\subseteq X'$ for every $1 \le j \le m$, therefore the transversal set $C = \{p_j \mid p_j \in E_j \setminus X' : 1 \le j \le n\}$ include a minimal transversal set $C_i \subseteq C$ hence $X' \cap C_i = \varnothing$, for some $1 \le i \le k$. Since the participants in X' don't have all of the k distinct transparencies of the *(k, k)*-threshold access structure, they can't recover the secret image *SI*.

(k, h, n)-threshold Visual Cryptography Schemes with Veto:

In many practical situations, especially in visual cryptography scheme (VCS), it is desirable that a qualified minority should also be able to "block" the secret image *SI*. Think for example of the serious problem of deactivating, a master key after a certain time. Here one would like to have a visual cryptography schemes which allows a qualified set, veto the *SI*. The aim of this section is to introduce such a scheme. These will be "ordinary threshold schemes" with an additional negative feature. We will generalize this method in section 3.4.

In a *(k, h, n)*-threshold visual cryptography scheme with veto capability, there is a dealer D, n participants $p_1, p_2, \ldots, p_n$ and the reconstructor R. Typically, every participant will get a "positive" and a "negative" transparency. Let *SI* denote a secret image. In the distribution phase, Dealer produces positive and negative shares as follows:

- To produce positive shares $v_1^P, v_2^P, \ldots, v_n^P$, dealer "$D$" employs the perfect black *(k, n)*-threshold visual cryptography scheme with the pixel expansion m and the basis matrices S_0 and S_1 proposed in the section 3.1. D applies S_0 and S_1 on the white and black pixels of *SI*, respectively.
- To produce negative shares $v_1^N, v_2^N, \ldots, v_n^N$, "$D$" employs the perfect black *(h, n)*-threshold visual cryptography scheme with the pixel expansion m' and the basis matrices S'_0 and S'_1 proposed in the section 3.1. D only applies S'_1 on all of the "subpixels" of *SI*. It means that on producing negative shares, D considers the subpixels *SI* instead of the pixels of the secret image, following the Figure 3.

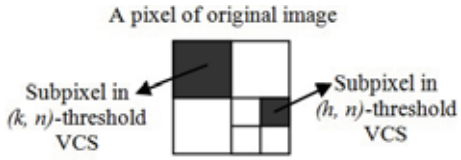

Fig. 3: subpixel in *(k, n)*-threshold VCS and *(h, n)*-threshold VCS

By using the technique based on transversal hypergraphs we obtain a *(k, n)*-threshold VCS (*(h, n)*-threshold VCS, resp.), in which $m = 2^{C(n,k-1)-1}$ and $t_X = m$ ($m' = 2^{C(n,h-1)-1}$ and $t_X = m'$, resp.). Utilization of transversal hypergraphs method causes to k or more positive shares reconstruct the pixels of *SI* uniquely. Furthermore when D is using S'_1 on all of the subpixels of *SI*, it cause h or more negative share cannot reconstruct *SI*, because they get a perfect black sheet. It is straightforward to check that when R receives k or more positive shares and $h-1$ or fewer negative shares, R can reconstruct *SI* with the contrast at least $1/(m \cdot m')$.

Protocol:

If a set of positive and negative shares is active, then *R* stacks them, so *R* visually recovers *SI* or recovers a perfect black sheet.

Reconstruction Phase:

In the reconstruction phase, a subset of participants sends v_i^P or v_i^N transparencies to *R*.

- If *R* receives $k-1$ or fewer shares, *R* has no information on *SI*.
- If *R* receives *h* or more negative shares, *R* recovers a perfect black sheet and cannot reconstruct *SI*.
- Otherwise, that is, if *R* receives *k* or more positive shares and $h - 1$ or fewer negative shares, *R* can reconstruct *SI* with the contrast at least $1/(m \cdot m')$.

Experimental Result of VCS with Veto Capability:

To demonstrate the feasibility of veto, we conduct several experiments. For a *(2, 2, 4)*-threshold visual cryptography scheme, the four shares are described as follows:

The secret image *IF* shown in Figure 4(a) is employed as the original secret image, Figure 4(b)-(c) are the corresponding positive shares v_1^P and v_2^P and Figure 4(d)-(e) are the corresponding negative shares v_3^N and v_1^N. The results of superimposing two of shares v_1^P and v_2^P are shown in Figure 4(f) and The results of superimposing two of shares v_1^P , v_2^P and v_3^N are shown in Figure 4(g). The result of superimposing negative shares v_3^N and v_4^N (shown in Figure 4(h)) clearly reveals the vetoing secret Image.

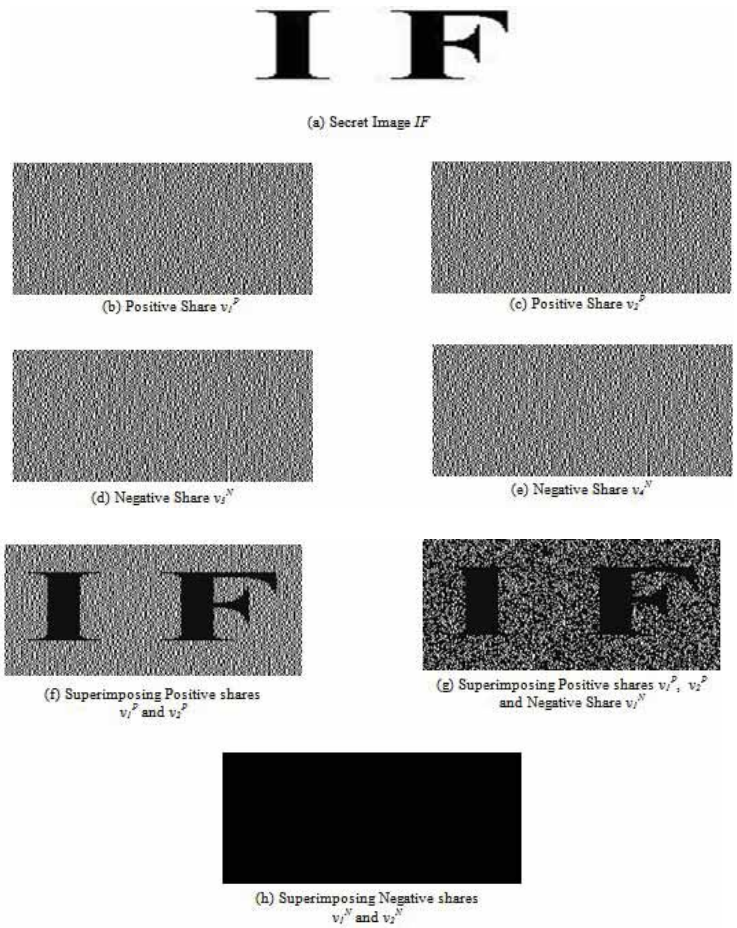

Fig. 4: (2, 2, 4)-threshold visual cryptography scheme

Attacks:

Similar to Beutelspacher models, there is an obvious attack against our model of *(k, h, n)*-threshold visual cryptography schemes with veto. Somebody who knows a set $P \cup N$ of active positive and negative shares with $|P| \geq k$ has a good chance to forge the system. If he knows P, he can directly determine the secret. On the other hand, if he knows only $P \cup N$ then he can form all k-element subsets of this set and try each possibility; so trustworthy operation in the secret reconstruction phase is essential.

VCS with Veto Capabilities for Strong Access Structure:

In this section we will present a construction technique to realize visual cryptography schemes with veto capabilities for any strong access structure. The construction we have considered is based on the transversal hypergraphs introduced in section 3.1. Let $P=\{p_1, p_2, \ldots, p_n\}$ be a sets of participants, $Q \subseteq 2^P$ and $Q' \subseteq 2^P$. We refer to members of Q as qualified sets which are eligible to reconstruct secret image and members of Q' as qualified sets which are eligible to veto secret image. Let the transversal hypergraphs of Q and Q' be denoted by $T(Q) = (C_1, C_2, \ldots, C_k)$ and $T(Q') = (D_1, D_2, \ldots, D_{k'})$ respectively. By using Theorem 1 and apply the same method in section 3.2, we can employ transversal hypergraphs to produce a perfect black VCS for strong access structure $\Gamma = (P, Q, 2^P \setminus Q)$ ($\Gamma' = (P, Q', 2^P \setminus Q)$, resp.) with the pixel expansion 2^{k-1}, ($2^{k'-1}$, resp.), to produce positive (negative resp.) shares.

In the reconstruction phase, a subset of participants sends v_i^P or v_i^N transparencies to R.

- If R receives a set of positive shares $X \in 2^P \setminus Q$, R has no information on *SI*.
- If R receives a set of negative shares $Y \in Q'$, R recovers a perfect black sheet and cannot reconstruct *SI*.
- Otherwise, that is, if R receives a set of positive shares $X \in Q$ and a set of negative shares $Y \in 2^P \setminus Q$, R can reconstruct *SI* with the contrast at least $1/2^{k+k'-2}$.

REFRENCES

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

Beutelspacher, A., 1982. Einführung in die Endiliche Geometrie I. Block Pläne, (B.I, Wissenschaftsverlag, Mannheim).

Beutelspacher, A. How to Say "No", Advances in Cryptology- EUROCRYPT' 89, Lecture Note in Computer Science, 434 Springer, Berlin, 491-496.

Blakly, G.R., 1979. Safeguarding Cryptographic Keys, Proc. AFIPS 1979 Nat. Computer Conf. 313-317.

Blundo, C., A. De Bonis, A. De Santis, 2001. Improved Schemes for Visual Cryptography, Des. Codes and Cryptography, 24: 255-278.

Blundo, C., A. De Santis, 1998. Visual Cryptography Schemes with Perfect Reconstruction of Black Pixels, J. Comput. Graphics, 22(4): 449-455.

Blundo, C., A. De Santis, A. Gaggia and U. Vaccaro, 1994. Secret Sharing Schemes with Veto Capabilities, G. Cohen, S. Litsyn, A. Lobstein and G. Zemmor eds. Proc. French- Israeli Workshop in Algebraic Coding, Lecture Notes in Computer Science, 781: Springer, Berlin, 82-89.

Beutelspacher, A. Visual Cryptography, in: Advances in Cryptology-EUROCRYPT'94, Lecture Notes in Computer Science, 1189, Springer, Berlin, 197-202.

Dembowski, P., 1968. Finite Geometries, Springer, Berlin.

Obana, S., K. Kurosawa, 1996. Veto is Impossible in Secret Sharing Schemes, Information Processing Letters, 58: 293-295.

Shamir, A., 1979. How to Share a Secret, Comm. ACM., 22: 612-613.

Simmons, G.J., W. Jackson and K. Martin, 1991. The Geometry of Shared Secret Schemes, Bulletin of the ICA., 1: 71-88.