Design of visual cryptography scheme using 3-way trades

Saeedeh Rashidi[1]

Department of Applied Mathematics, Faculty of Mathematics and Computer, Shahid Bahonar University of Kerman, Kerman, Iran.

Nasrin Soltankhah

Department of Mathematics, Faculty of Mathematical Sciences, Alzahra University Tehran, Iran.

Abstract

A visual cryptography scheme (VCS) is a type of secret sharing scheme in which the secret is an image. The qualified subsets of participants can recover the image. Here, we introduce a new visual cryptography scheme method. In this method we apply one combinatorial object that is a 3-way $(v, k, 2)$ trade.

MSC: 05B30; 05B05

KEYWORDS: visual cryptography scheme; 3-way trade; 3-way Steiner trade

1 Introduction

The VCS was first introduced by Naor and Shamir in 1994 [5]. For more study, see [1, 4], and [6]. We recall some notations for defintion of VCS from [2]. Let $\mathcal{P} = \{1, \cdots, n\}$ be a set of participants, and Let $\Gamma_{Qual} \subseteq 2^{\mathcal{P}}$ and $\Gamma_{Forb} \subseteq 2^{\mathcal{P}}$, where $\Gamma_{Qual} \cap \Gamma_{Forb} = \phi$. Γ_{Qual} contains qualified sets, Γ_{Forb} contains forbidden sets and pairs $(\Gamma_{Qual}, \Gamma_{Forb})$ are called the access structure of the scheme. Let $S = [s_{ij}]$ be an $n \times m$ Boolean matrix. $s_{ij} = 1$ iff jth sub-pixel in the ith transparency is black. In fact each pixel expands to m sub-pixel. The parameter m is named pixel expansion of the scheme. The value $\omega(V)$ is the Hamming weight of the vector $V = OR(r_{i_1}, \cdots, r_{i_s})$, where $\{r_{i_1}, \cdots, r_{i_s}\}$ are the rows of S.

Definition 1.1. [1] Let $(\Gamma_{Qual}, \Gamma_{Forb})$ be an access structure on a set of n participants. A $(\Gamma_{Qual}, \Gamma_{Forb}, m)$ -VCS with relative difference $\alpha(m)$ and 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 $X = \{i_1, i_2, \cdots, i_p\} \in \Gamma_{Qual}$ (i.e., if X is a qualified set), then the "or" V^0 of rows $i_1, i_2, \cdots, i_p$ of S^0 satisfies $\omega(V^0) \leq t_X - \alpha(m).m$; whereas for S^1 it results that $\omega(V^1) \geq t_X$.
2. If $X = \{i_1, i_2, \cdots, i_p\} \in \Gamma_{Qual}$ (i.e., if X is a forbidden set), then the two $p \times m$ matrices obtained by restricting S^0 and S^1 to rows $i_1, i_2, \cdots, i_p$ are equal up to a column permutation.

[1] speaker

The VCSs with optimal contrast were constructed in [1] and the following theorem is obtained by using the balanced incomplete block designs (BIBDs) about the optimal contrast. We observed (2,n)-VCS which are made based on BIBDs [1]. In fact, the property of balanced incomplete block design plays a major role in creating these (2,n)-VCSs. Based on some other combinatorial objects, new (2,n)-VCS can be obtained. These objects must somehow have the characteristic of being balanced. The combinatorial object that we use in the new proposed method and has the mentioned property is trade.

Theorem 1.2. *[1] Let $n \geq 2$. In any $(2, n)$-VCS with pixel expansion m, it holds that $\alpha(m) \leq \alpha^*(n)$.*

Notice that:

$$\alpha^*(n) = \begin{cases} \frac{n}{4n-4} & \text{if n is even} \\ \\ \frac{n+1}{4n} & \text{if n is odd} \end{cases} \tag{1}$$

Definition 1.3. [6] A (v, k, λ)-BIBD (balanced incomplete block design) is a pair (X, B), where X is a set of v elements (called points) and B is a collection of subsets of X (called blocks), such that each block contains exactly k points and each pair of points is a subset of exactly λ blocks.

Definition 1.4. [6] A μ-way (v, k, t) *trade* of volume m consists of μ disjoint collections T_1, $T_2, \ldots, T_\mu$ each of m blocks, such that for every t-subset of v-set V, the number of blocks containing this t-subset is the same in each T_i $(1 \leq i \leq \mu)$. In the other words any pair of $(T_i, T_j),\ i \neq j$ is a (v, k, t) trade of volume m.

We use special types of trades for our construction that mention it below.

Definition 1.5. [5] A μ-way (v, k, t) trade is called μ-way (v, k, t) *Steiner trade* if any t-subset of $found(T)$ occurs at most once in T_1 $(T_j,\ j \geq 2)$.

Definition 1.6. The trade is called d-homogeneous if each point occurs in exactly d blocks of each T_i.

The following example is a 3-way 3-homogeneous Steiner trade.

T_1	T_2	T_3
123	124	127
147	138	135
158	157	148
248	237	246
267	268	238
357	467	367
368	458	457
456	356	568

2 Main construction for $(2, n)$-VCS

Golalizadeh and Soltankhah studied the existence of d-Homogeneous μ -way (v, 3, 2) Steiner trades [3]. Rashidi and Soltankhah studied μ-way trades [6], and later they proposed a new idea for constructing new $(2, n)$-VCS by trades [7]. Now, we explain this new method for constructing the $(2, n)$-VCS from homogeneous trade. In this example, we construct three different $(2, n)$-VCSs with the same parameters. These $(2, n)$-VCS schemes have a relative difference that has slightly different from the value of $\alpha^*(n)$ Then we generalize this method to the general structure.

Example 2.1. Let T be a 3-way $(8,3,2)$ homogeneous Steiner trade of the previous example. Now, we construct two matrices S^0 and S^1 that have the properties of Definition 1.1. let $S^1 = [s^1_{ij}]_{8\times 8}$ where $j \in \{1, \cdots, 8\}$, $i \in$ found(T) and

$$s^1_{ij} = \begin{cases} 1 & i \in B_j \\ 0 & i \notin B_j \end{cases} \tag{2}$$

.

$$S^1 = \begin{array}{|c cccccccc|}
 & B_1 & B_2 & B_3 & B_4 & B_5 & B_6 & B_7 & B_8 \\
\hline
1: & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\
2: & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\
3: & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\
4: & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\
5: & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\
6: & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\
7: & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\
8: & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0
\end{array}$$

$$S^0 = \begin{bmatrix}
1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\
1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\
1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\
1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\
1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\
1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\
1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\
1 & 1 & 1 & 0 & 0 & 0 & 0 & 0
\end{bmatrix}$$

Now, check the property one of the definition 1.1. Let $t_X = 5$ and $\alpha(m) = \frac{2}{8}$. Notice that $m = 8$.

$$\begin{cases} 3 = \omega(V) \leq t_X - \alpha(m).m \rightarrow 3 \leq 5 - 8 \times \frac{2}{8} & for\ S^0 \\ t_X \leq \omega(V) \rightarrow 5 \leq 5 \text{ or } 6 & for\ S^1 \end{cases} \tag{3}$$

Both rows of matrix S^1 have at most one column in common with entry ‘1‘. Since this trade is Steiner. If two rows of S^1 have one same column with entry ‘1‘ then $\omega(V) = 5$ otherwise $\omega(V) = 6$. In this scheme $m = 8$ and $\alpha = \frac{1}{4} = 0.25$
Notice that $\alpha^*(n) = \frac{n}{4n-4} = \frac{8}{32-4} = 0.285$ (optimal value).
The second property of Definition 1.1 is obviously held. Also, we can construct two new schemes with the same parameters and different structures by using T_2 and T_3.

We perform the following simulations using MATLAB and PYTHON and known programs for VCSs for this example. The pixel expansion of VCS corresponds to two rows of matrix S^0 and matrix S^1. In this image, we insert the original image, shares, recovered image, and their histograms. In the previous example, we propose the main structure and idea for constructing the (2,n)-VCS. We obtain the following

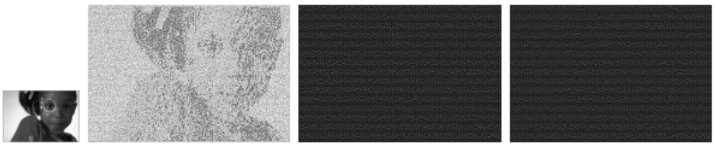

Figure 1: girl image, retrieved image and shares

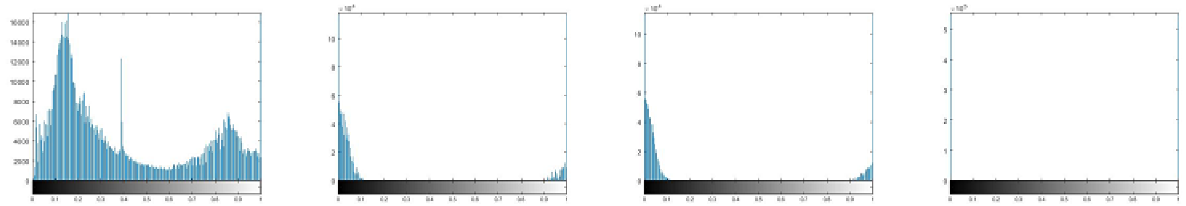

Figure 2: Histogram of girl image, shares and retrieved image, respectively

theorems:

Theorem 2.2. *For any $k \geq 3$ there exists three $(2, 3k)$-VCSs, with pixel expansion $m = k + 3$ and $\alpha(m) = \frac{k-1}{k+3}$.*

Theorem 2.3. *For any $k \leq 3$ there exists a $(2, 9k)$-VCS, with pixel expansion $m = k + 3$ and $\alpha(m) = \frac{k-2}{k+3}$.*

References

[1] Ateniese, G., Blundo, C., De Santis, A., and Stinson, D. R. (1996). Visual cryptography for general access structures. Information and computation, 129(2), 86-106.

[2] Blundo, C., De Santis, A., and Stinson, D. R. (1999). On the contrast in visual cryptography schemes. Journal of Cryptology, 12(4), 261-289.

[3] Golalizadeh, S., and Soltankhah, N. (2019). On the Existence of d-Homogeneous μ -Way (v, 3, 2) Steiner Trades. Graphs and Combinatorics, 35(2), 471-478.

[4] Hajiabolhassan, H., and Cheraghi, A. (2010). Bounds for visual cryptography schemes. Discrete Applied Mathematics, 158(6), 659-665.

[5] M. Naor and A. Shamir, Visual Cryptography, in ”Advances in Cryptology Eurocrypt ’94”, A. De Santis Ed., Vol. 950 of Lecture Notes in Computer Science, Springer-Verlag, Berlin, pp. 1-12, 1995.

[6] Rashidi, S., and Soltankhah, N. (2014). On the possible volume of μ-(v, k, t) trades. Bulletin of the Iranian Mathematical Society, 40(6), 1387-1401.

[7] Rashidi, S., and Soltankhah, N. A Novel Visual Cryptography Scheme Based on Steiner Trades. Advanced Defence Sci. & Technol., 4, 345-357.

e-mail: `s.rashidi@uk.ac.ir`
e-mail: `soltan@alzahra.ac.ir`