International Journal of Mathematical Archive-2(10), 2011, Page: 1882-1884
Available online through www.ijma.info ISSN 2229 – 5046

A METHOD FOR THE CONSTRUCTION OF VISUAL CRYPTOGRAPHIC SECRET SHARING SCHEME

[1]M. Varaprasad Rao* and [2]N. Ch. Bhatra Charyulu

[1]Department of Computer Science, Matrusri Institute of PG Studies, Hyd-59, India
E-mail: vpr_m@yahoo.com

[2]Department of Statistics, University College of Science, O.U. Hyd-7, India
E-mail: dwarakbhat@osmania.ac.in

(Received on: 12-09-11; Accepted on: 05-10-11)

ABSTRACT

Naor and Shamir (1994) and Blakely (1995) independently introduced a Visual Cryptography Scheme. Ateniese, Blundo, Santis and Stinson (1996, 1999) developed Visual Cryptography Scheme (VCS) for general access structure for black and white images and subsequently different schemes have been developed. Adhikari A, Bose M and Bimal Roy (2004, 2005) also made an attempt on the construction of visual cryptographic schemes.In this paper, we made an attempt to propose a new method for the construction of (k, n) visual cryptographic threshold secret sharing scheme using combinatorial methods.

Keywords: *Visual Cryptography Scheme, Combinatorial method*

---

1. INTRODUCTION:

Secret sharing scheme is a method for distributing a secret among a group of participants. Each Participant is given a share of the secret. The secret can only be reconstructed when the shares are combined together. Any individual participant cannot recover the secret on his/her own. In secret sharing scheme, let there are '**n'** participants. Each participant gets a share in such a way that any group of '**t'** or more participants can together reconstruct the secret but no group of less than 't' participants can recover the secret. Such a system is called a (**t**, **n**) – threshold scheme. Here't' is the threshold.

In (**t**, **n**) visual cryptographic schemes, a secret image (text or picture) is encrypted into '**n**' shares, which are distributed among '**n**' participants. The image cannot be decoded from any **(t–1)** or fewer shares but any 't' or more participants can together decode it visually, without using any complex decoding mechanism. Naor and Shamir first proposed this concept of visual cryptography in the open literature in 1994. In this proposal, an image consisting of text, drawings etc. are encrypted and the resultant into two images. These images are given to two different parties as shares. Decryption is not possible without having both of them together. These shares are stored on transparencies and the process of decryption begins with stacking these two transparencies together on the overhead projector. Decryption is done by the human visual system. Blakely in 1995 also independently introduced the same concept of Visual Cryptography Schemes (VCS) by considering each share is a plane and the secret is the point at which three shares intersect. Two shares are insufficient to determine the secret. This scheme is less efficient than Shamir's scheme because the shares are '**t'** times larger where '**t'** is threshold.

Suppose that six thieves have deposited their loot in a numbered Swiss bank account. Being thieves, they do not trust each other not to withdraw the money and take the next plane to Brazil. However, being sentimental, they do not assume a conspiracy of two or more thieves that will try to take out the money without "authorization" and they want any two of them to able to withdraw the money. They therefore want to divide the secret number into shares so that from each share you cannot learn anything about the secret number, but from any two shares you can reconstruct the secret number. This problem is the by now classical secret sharing problem.

Definition: A solution to the 'k' out of 'n' visual secret scheme consists of two collections of n x m Boolean matrices C_0 and C_1. To share a white pixel, the dealer randomly chooses one of the matrices in C_0, and to share a black pixel, the dealer randomly chooses one of the matrices in C_1. The chosen matrix defines the color of the m sub pixels in each of the n transparencies. The solution is considered as valid, if the following three conditions are satisfied:

**Corresponding author: [1]M. Varaprasad Rao*, *E-mail: vpr_m@yahoo.com*

1. For any S in C_0, the "or" V of any 'k' of the rows satisfies H (V) ≤ d - α.m

2. For any S in C_1, the "or" V of any 'k' of the rows satisfies H(V) ≥ d

3. For any subset $\{i_1, i_2, \ldots i_q\}$ of {1,2, … n} with q<k, the two collections of q x m matrices $\mathbf{D}_t$ for t {0,1} obtained by restricting each n x m matrix in Ct (where t=0,1) to rows $i_1, i_2, .. i_q$ are indistinguishable in the sense that they contain the same matrices with same frequencies.

Where m, α and r are the parameters indicating the number of pixels in a share, relative difference in weight between combined shares that come from white and black pixel in the original picture and the size of the collections of basis matrices C_0 and C_1 respectively.

The first two conditions are called contrast and the third condition is called security and it inspecting fewer than 'k' shares. The combined shares from q < k transparencies consists of all the V's with H (V) = f (q) with uniform probability distribution, regardless of whether the matrices were taken from C_0 and C_1. Such a scheme is called Uniform.

2. METHODS FOR CONSTRUCTION OF VCS SCHEME:

Naor and Shamir in 1994 and Blakely in 1995 independently introduced a Visual Cryptography scheme. Blakely in 1995 also independently introduced the same concept of Visual Cryptography schemes by considering each share is a plane and the secret is the point at which three shares intersect. Two shares are insufficient to determine the secret. This scheme is less efficient than Shamir's scheme because the shares are **t** times larger where **t** is threshold. Ateniese, Blundo, Santis and Stinson (1996, 1999) developed Visual Cryptography Scheme (VCS) for general access structure for black and white image and subsequently different schemes have been developed. In such schemes, shares of a secret are distributed among the users, in such a way that only authorized subsets (those in the access structure) can recover the secret from their shares. Adhikari A, Bose M and Bimal Roy (2004, 2005) also made an attempt on visual cryptographic schemes.

The heart of any VCS depends on the construction of basis matrices as defined satisfying those conditions. The basis matrices (incidence matrices) that are taken for a (2, n) – VCS were vague. Rather they were chosen on a trial basis to start with. Even Stinson method for constructing such a scheme was rather vague to start with. Stinson converted this scheme to a general scheme by using one technique known as cumulative array (CU) technique which gives more optimization in terms VCS parameters.

In this paper an attempt is made to propose a new method for the construction of visual cryptographic secret sharing scheme.

3. NEW METHOD FOR THE CONSTRUCTION OF VCS:

In this section, a method for the construction of (2, n) VCS scheme using some combinatorial method is proposed and presented below.

Method: Let P= {1, 2… n} be a set of elements called participants. Let C_0 and C_1 are the two collections of matrices. The matrix C_0 can be constructed by using a list of vectors $J_1, J_2, \ldots J_k, O_{k+1}, \ldots O_n$ where J_i be the column vector consisting of elements 1's for 1<i<k and O be the column vector consisting of elements 0's. The matrix C_1 can be constructed by using a list of vectors $u_1, u_2, \ldots, u_n$ each of length n+k; where u_i $O^{i-1}1^kO^{n-i}$.

Example 3.1: When n=5, k=2 the basis matrices are

$$C_1 = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \end{bmatrix}$$

$$C_2 = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix}$$

REFERENCES:

[1] Adhikari A, Bose M, 2004, "A new visual cryptographic scheme using Latin squares", IEICE Trans Fund E, Vol.87, pp.1998-2002.

[2] Adhikari A, Bose M, Kumar D, Roy B, 2005, "Applications of PBIBD's in developing visual cryptographic schemes", ISI Technical report No: ASD/2005/11.

[3] Atenson G, Blundo C, de Santis, Stinson D, 1996, "Visual cryptography for general access structures", Information and Computation, Vol.129 (2), pp.86-106

[4] Atenson G, Blundo C, de Santis, Stinson D, 1999, "Construction and bounds for Visual cryptography", Theoretical Computer science, Vol.250, pp.143-161

[5] Noar M, Shamir A, 1994, "Visual cryptography", Eurocrypt'94, Springer-Verlog, Berlin, pp.1-12.

****

