Survey on Visual Cryptography for General Access Structures

Mrinaldeep Chakravorty, Sandeep Gurung

Department of Computer Science & Engineering
Sikkim Manipal Institute of technology

chakravorty.mrinaldeep@gmail.com, gurung_sandeep@yahoo.co.in

***Abstract*— Visual Cryptography Scheme (VCS) is a kind of secret sharing scheme which allows the encoding of a secret image into n shares distributed to n participants. The beauty of such a scheme is that by only using the Human Visual System (HVS), a set of qualified participants is able to recover the secret without any cryptographic knowledge or computational devices. Access structures are used in the study of security system where multiple parties need to work together to obtain a resource. Groups of parties that are granted access are called qualified. In set theoretic terms they are referred to as qualified sets. In turn, the set of all such qualified sets is called the access structure of the system. The resource is a secret shared among the participants. Only subgroups of participants contained in the access structure are able to join their shares to decrypt the secret. More generally, the resource can also be a task that a group of people can complete together, such as creating a digital signature, or decrypting an encrypted message.**

***Keywords*— Visual Cryptography, General Access Structure, Random Grids.**

I. INTRODUCTION

Secret sharing is concerned with the problem of how to distribute a secret among a group of participants, or entities, so that only a pre-designated collection of individuals are able to recreate the secret by collectively combining the parts of the secret which were allocated to them. There are numerous ways of encrypting a secret so that the secret can be distributed among participants. DES, RSA, AES are some of the encryption techniques used to encrypt and share secrets amongst participants. Visual Cryptography is an encryption technique which requires less or no computation for encrypting or decrypting information. Visual cryptography uses human visual system as the decrypting machine. Hence, for encrypting information, visual cryptography is a better technique with respect to the fore-mentioned techniques, as at times one may not be able to be near a machine to decrypt the information and also computation required to encrypt the information is less than the conventional methods of encryption. To share visual secret information, several visual sharing schemes have been developed involving complex, little or no computation in the decryption phase.

In 1995, Moni Noar and Adi Shamir [2] proposed a new technique known as Visual Cryptography, which shares information and removes the problem of computation involved in the decryption phase. This scheme is a (k, n) – threshold scheme, which encrypts a black and white secret image into n meaningless shares such that knowledge of less than k shares reveals nothing about the secret image. The reconstruction of the secret image is done by human visual system without any computation.

In 1987, Kafri and Keren [1] proposed a random grid based (2, 2) secret sharing technique in which the secret is encrypted in two cipher grids without any pixel expansion and codebook requirement. The decryption is same as the traditional VC.

Shyu [6] extended Kafri and Keren's scheme to (n, n) scheme for any n≥2. Chen also proposed (2, n) and (n, n) scheme based on random grids. Chen and Tsao proposed a random grid based (k, n) threshold scheme but this scheme is limited to threshold access structure and cannot be used for general access structures.

Visual cryptography using random grids was not able to generalize to (k, n) scheme. The quality of the output or the decrypted image degrades as the number of shares generated using random grids increases. Hence, it is feasible to use General Access Structures (GAS) for Visual Cryptography instead of random grids as GAS generalizes to (k, n) scheme and also the quality of the output generated does not degrade as much as compared to the output generated using random grids.

Access structures are used in the study of security system where multiple parties need to work together to obtain a resource. Groups of parties that are granted access are called qualified. In set theoretic terms they are referred to as qualified sets. In turn, the set of all such qualified sets is called the access structure of the system. The resource is a secret shared among the participants. Only subgroups of participants contained in the access structure are able to join their shares to

decrypt the secret. More generally, the resource can also be a task that a group of people can complete together, such as creating a digital signature, or decrypting an encrypted message. Generally, access structure is a specification of all qualified and forbidden participants, where the qualified participants are able to decrypt an information by stacking there transparencies but not forbidden participants can decrypt the secret information as they have transparencies that are meaningless and have no information about the secret.

In this paper the various ways of generating a visual cryptography scheme for general access structures is discussed. The paper is organized as follows. Section 2 reviews Visual Cryptography scheme. Section 3 reviews the backgrounds of general access structures and describes in brief the various techniques of generating the general access structures. Section 4 gives a comparative conclusion between Visual Cryptography Scheme and schemes used to construct VCS for general access structures. Section 5 gives potential applications where these schemes may be used.

II. VISUAL CRYPTOGRAPHY SCHEME

In this scheme a solution to the k out of n visual secret sharing technique is provided where n users are provided with n transparencies and a minimum of k transparencies is required to reveal the secret information; but any k-1 transparencies cannot reveal the secret information.

A solution to the k out of n visual secret sharing 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 subpixels in each of the n transparencies. The solution is considered to be valid if and only if the following three conditions are met [2]:

- For any S in C_0, the "or" V of any k of the n rows satisfies $H(V) \leq d-(\alpha.m)$.
- For any S in C_1, the "or" V of any k of the n rows satisfies $H(V) \geq d$.
- For any subset $\{i_1, i_2, \ldots, i_q\}$ of $\{1,2,\ldots,n\}$ with $q<k$, the two collections of q x m matrices D_t for $t \in \{0,1\}$ obtained by restricting each n x m matrix in C_t (where t = 0,1) to rows $i_1, i_2, \ldots, i_q$ are indistinguishable in the sense that they contain the same matrices with the same frequencies.

Condition 3 implies that by inspecting fewer than k shares, even an infinitely powerful cryptanalyst cannot gain any advantage in deciding whether the shared pixel was white or black.

The first two conditions are called contrast and the third condition is called security. The important parameters of a scheme are:

- m, the number of pixels in a share. This represents the loss in resolution from the original picture to the shared one.
- α, the relative difference in weight between combined shares that come from a white pixel and a black pixel in the original picture. This represents the loss in contrast.
- r, the size of the collections C_0 and C_1. log r represents the number of random bits needed to generate the shares and does not affect the quality of the picture.

The scheme has contrast ¼; any two shares of C_0 cover 2 out of 4 of the pixels, while any pair of shares from C_1 covers at least 3 out of 4 pixels (some cover all four). The security of the scheme follows from the fact that in both C_0 and C_1 each share is a random subset of 2 black pixels out of 4. One possible generalization of this scheme to a 2 out of n scheme is to fix m so that $(m|(m/2)) \geq n$ and consider all subsets of size m/2 of some ground set of size m. The contrast achieved this way is 1/m.

CONSTRUCTION OF MATRICES C_0 and C_1:

Let B be the black n x (n-2) matrix which contains only 1's and let I be the identity n x n matrix which contains 1's on the diagonal and 0's elsewhere. Let BI denote the n x (2n-2) matrix obtained by concatenating B and I, and let c(BI) be the Boolean compliment of the matrix BI. Then

C_0 = {all the matrices obtained by permuting the columns of c(BI)}

C_1 = {all the matrices obtained by permuting the columns of BI}

The matrices C_0 and C_1 has the following properties: Any single share contains an arbitrary collection of n-1 black and n-1 white subpixels; any pair of shares have n-2 common black and two individual black subpixels; any stacked triplet of shares from C_0 has n black subpixels, whereas any stacked triplet of shares from C_1 has n+1 black subpixels.

III. GENERAL ACCESS STRUCTURES

Access structures are used in the study of security system where multiple parties need to work together to obtain a resource. Groups of parties that are granted access are called qualified. In set theoretic terms they are referred to as qualified sets. In turn, the set of all such qualified sets is called the access structure of the system. The resource is a secret shared among the participants. Only subgroups of participants contained in the access structure are able to join their shares to decrypt the secret. More generally, the resource can also be a task that a group of people can complete together,

such as creating a digital signature, or decrypting an encrypted message. Generally, access structure is a specification of all qualified and forbidden participants, where the qualified participants are able to decrypt an information by stacking there transparencies but not forbidden participants can decrypt the secret information as they have transparencies that are meaningless and have no information about the secret.

Let P = {1,2,….,n} be a set of n participants and 2P denote the set of all subsets of P. Let $\Gamma_{Qual} \subseteq 2P$ and $\Gamma_{Forb} \subseteq 2P$, where $\Gamma_{Qual} \cap \Gamma_{Forb} = \Phi$. The members of Γ_{Qual} are referred as qualified sets, while the members of Γ_{Forb} are referred as forbidden sets. The pair (Γ_{Qual}, Γ_{Forb}) is known as access structure.

Γ_0 is a set consisting of the minimal qualified sets, i.e., $\Gamma_0 = \{Q \in \Gamma_{Qual} : Q' \notin \Gamma_{Qual}, \forall Q' \subset Q\}$. A monotone increasing access structure Γ on P is a subset $\Gamma \subseteq 2P$ such that if $Q \in \Gamma$ and $Q \subseteq Q' \subseteq P$, the $Q' \in \Gamma$. If Γ_{Qual} is monotone increasing, Γ_{Forb} is monotone decreasing, and $\Gamma_{Qual} \cup \Gamma_{Forb} = 2^P$ then the access structure is called strong access structure and $\Gamma 0$ is called the basis of the access structure [4] [7] [8].

There are various techniques to realize visual cryptography schemes for any access structure. In this paper two construction techniques for realizing visual cryptography schemes for access structure has been discussed.

IV. Construction Of Vcs Using Cumulative Arrays

Cumulative arrays are array generated using the forbidden sets. The column index *i* of the cumulative array is assigned value zero if *i* is present in the forbidden set. Cumulative array is a combination of a cumulative map (β, T) and the participant set P. a cumulative map (β, T) for Γ_{Qual} is a finite set T along with a mapping β: $P \rightarrow 2^T$. We can construct a cumulative map (β, T) for any Γ_{Qual} by using the collection of the maximal forbidden sets $Z_M = \{F_1, F_2 \ldots F_t\}$ as:

$$B(i) = \{T_j \mid i \notin F_j, 1 \leq j \leq t\}$$

From this mapping one can obtain the Cumulative array for Γ_{Qual}.

The reason that the cumulative map is of interest is as follows. Let (α, S) be the cumulative map for F. Take an (|S|, |S|)-threshold scheme X, defined on set S, and then use the cumulative map to distribute sets of shares of X to each participant in *P*. In other words, give the shares of X corresponding to p^{α} to participant p. If we then operate X in the normal way, only participants belonging to sets in F will be able to accumulate all the shares of X and hence reconstruct the secret in X. The disadvantages of the above system is that each participant in P tends to get many shares of scheme X and consequently the information rates of schemes formed in this way are low. However, the cumulative array is in fact a very significant structure in the theory of geometric secret sharing schemes. However, rather than being used as a scheme itself, the cumulative array for F would appear to contain useful information when it comes to considering constructing other geometric schemes. The significance of this is that it may lead to more systematic methods for constructing geometric schemes as opposed to the somewhat ad hoc methods currently being used.

Let (Γ_{Qual}, Γ_{Forb}) be a strong access structure on the set of participants $P = \{1, 2 \ldots n\}$. Let Z_M denote the collection of the maximal forbidden sets of Γ [3]:

$$Z_M = \{B \in \Gamma_{Forb} : B \cup \{i\} \in \Gamma_{Qual} \text{ for all } i \in P \backslash B\}.$$

A cumulative array is a |*P*| x |T| Boolean matrix, denoted by CA, such that CA (i, j) = 1 if and only if $i \notin F_j$, where F_j is a forbidden set.

Example 1: Let $P = \{1, 2, 3, 4\}$, $\Gamma_0 = \{\{1, 2\}, \{2, 3\}, \{3, 4\}\}$, $Z_M = \{\{1, 4\}, \{1, 3\}, \{2, 4\}\}$, then $F_1 = \{1, 4\}$, $F_2 = \{1, 3\}$, and $F_3 = \{2, 4\}$. Therefore, |T| = 3. The cumulative array for Γ_{Qual} is given by:

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

Let B^0 and B^1 be the basis matrix generated using the (n, n) threshold scheme. B^0 and B^1 is given as

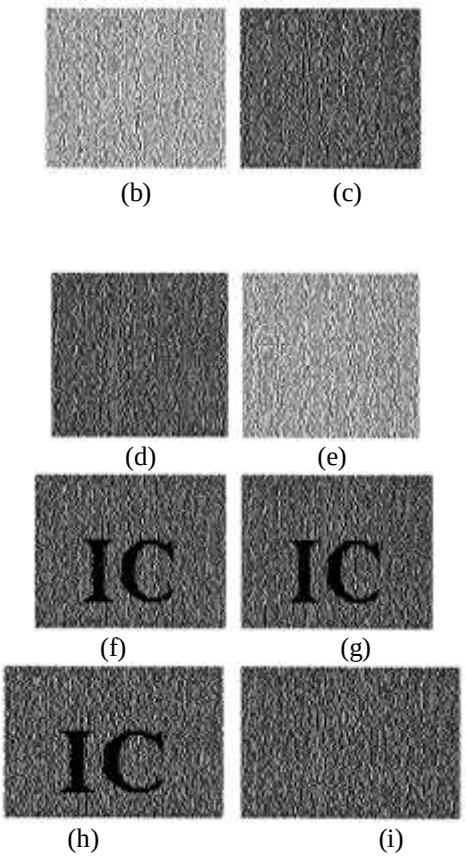
$$B^0 = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix} B^1 = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix}$$

The basis matrices S^0 and S^1 in a VCS realizing the strong access structure with the basis Γ_0 are

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

The second row of S^0 is the *or* of rows 1 and 2 of B^0 and the third row of S^0 is the *or* of rows 1 and 3 of B^0. The first and fourth rows of S^0 are equal to rows 3 and 2 of B^0, respectively, and similarly for S^1.

(a)



(b) (c) (d) (e) (f) (g) (h) (i)

Figure 1: The experimental results [3] for Example 1: (a) Binary secret image; (b) R_1; (c) R_2; (d) R_3; (e) R_4; (f) $R_1 \oplus R_2$; (g)$R_2 \oplus R_3$; (h) $R_3 \oplus R_4$; (i) $R_1 \oplus R_3$;

1.1 CONSTRUCTION OF VCS FROM SMALLER SCHEMES

In this section, construction for VCS using smaller schemes as building blocks in the construction of larger schemes is discussed. In this scheme the basis qualified set Γ_0 is divided into smaller basis sets and then the basis matrices are generated for the smaller basis sets. Finally the basis matrices S^0 and S^1 is generated by concatenating the basis matrices generated from the smaller basis sets.

Let $(\Gamma'_{Qual}, \Gamma'_{Forb})$ and $(\Gamma''_{Qual}, \Gamma''_{Forb})$ be two access structures on a set of *n* participants *P* [3]. Suppose there exist a $(\Gamma'_{Qual}, \Gamma'_{Forb}, m')$ - VCS and a $(\Gamma''_{Qual}, \Gamma''_{Forb}, m'')$ – VCS with basis matrices R^0, R^1 and T^0, T^1, respectively. From the matrices R^0, R^1, T^0 and T^1 two pairs of matrices, (X^0, X^1) and (Y^0, Y^1), can be constructed each consisting of *n* rows. For i = 1… *n*, the i^{th} row of X^0 has all zeroes as entries if the participant i is not an essential participant of $(\Gamma'_{Qual}, \Gamma'_{Forb})$; otherwise, it is the row of X^0 corresponding to participant i. The matrices X^1, Y^0, and Y^1 are constructed similarly. Finally the basis matrices S^0 and S^1 for $(\Gamma_{Qual}, \Gamma_{Forb})$ can be realized by concatenating the matrices X^0 and Y^0 for S^0 and X^1 and Y^1 for S^1.

Example 2: Let $P = \{1, 2, 3, 4, 5\}$, $\Gamma_0 = \{\{1, 2\}, \{2, 3\}, \{3, 4\}, \{4, 5\}, \{1, 5\}, \{2, 5\}\}$. Let $\Gamma'_0 = \{\{1, 2\}, \{1, 5\}\}$ and $\Gamma''_0 = \{\{2, 3\}, \{3, 4\}, \{4, 5\}, \{2, 5\}\}$, respectively:

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

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

From the above matrices one can obtain the matrices for X^0, X^1, Y^0, and Y^1:

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

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

Concatenating the matrices X^0 and Y^0 gives the basis matrix S^0 as

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

Similarly S^1 is constructed by concatenating X^1 and Y^1 as

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

V. CONCLUSION

Based on the survey a comparative conclusion can be derived.

- Pixel Expansion: The best results are obtained when the pixel expansion *m* is a square. The conventional visual cryptographic scheme has a pixel expansion of *n* whereas, the schemes for constructing visual cryptography for general access structures has a pixel expansion of log *n*.
- Contrast: The quality of the decrypted image degrades in conventional visual cryptography as the number of

shares increases, i.e., the contrast of the image increases and the relative difference decreases, whereas in schemes for constructing visual cryptography for general access structure the contrast decreases and relative difference increases as the number of shares increases. The best solution is obtained for 2 out of *n* scheme.

TABLE 1: PROS AND CONS OF THE SCHEMES.

Proposed Scheme	Pros	Cons
Visual Cryptography Scheme (VCS).	• Pioneered a general solution for *k* out of *n* visual secret sharing scheme theoretically. • Maximum contrast is achieved with three participants. • HVS – the scheme uses human visual system (HVS) for decrypting the secret	• Pixel expansion – the size of each share is not same as that of the original image. Scheme has a pixel expansion of *n*. • The technique could not be generalized for (*k*, *n*) scheme because the creation of the basis matrices is dependent on the values of *k* and *n*. • This scheme was tested only for black and white pixels. • Multiple secrets cannot by encrypted.
Construction of VCS using General Access Structures	• Generalized – these schemes generalizes the scheme proposed by M. Noar and A. Shamir to (*k*, *n*) scheme. • Wide image format – it can be used for encrypting both binary as well as color images. • This scheme can give more mapping by permuting the basis matrices columns. • Pixel expansion – construction scheme has pixel expansion of only log *n*. • No leakage of information - as the information cannot be recreated using the forbidden sets.	• Best results are acquired when there are 4 participants. • Greater the number of participants greater the noise present in the decrypted image. • Multiple secrets cannot by encrypted. • The scheme cannot be used for general visual cryptography.

VI. POTENTIAL APPLICATIONS FOR VCS FOR GENERAL ACCESS STRUCTURES

The potential applications where these schemes may be used are:

- Image sharing
- Visual authentication
- Digital watermarking
- Image hiding

REFERENCES

[1] O. Kafri and E. Keren. Encryption of pictures and shapes by random grids. Optics Letters, 12(6):377–379, 1987.

[2] M. Naor and A. Shamir. Visual cryptography. In Proceedings of Advances in Cryptology (EUROCRYPT 94), volume 950, pages 1–12. LNCS,Springer-Verlag, 1995.

[3] G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson. Visual cryptography for general access structures. Information and Computation, 129:86–106, 1996.

[4] A. Adhikari, T. K. Dutta, and B. Roy. A new black and white visual cryptographic scheme for general access structures. In Indocrypt'04, volume 3348, pages 399–413. LNCS, Springer-Verlag, 2004.

[5] K. Martin, Siaw – Lynn Ng. The combinatorics of generalised cumulative arrays, JMC, volume 13-32, 2007. DOI 10.1515/JMC.2007.002.

[6] S. J. Shyu. Image encryption by multiple random grids. Pattern Recognition, 42:1582–1596, 2009.

[7] C. Guo, C. C. Chang. A construction for Secret Sharing Scheme with General Access Structure, Journal of Information Hiding and Multimedia Signal Processing, volume 4, number 1, January, 2013, ISSN 2073-4212.

[8] S. Kumar, R. K. Sharma. Secret Image Sharing for General Access Structures using random grids, IJCA (0975 8887), volume 83- No. 7, December 2013.