Maximal Contrast Color Visual Secret Sharing Schemes

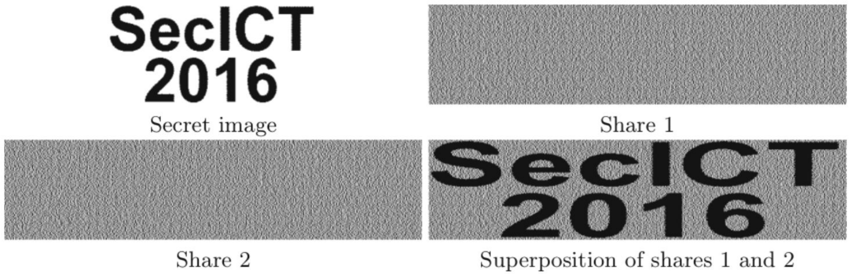
Sabyasachi Dutta, Avishek Adhikari, Sushmita Ruj

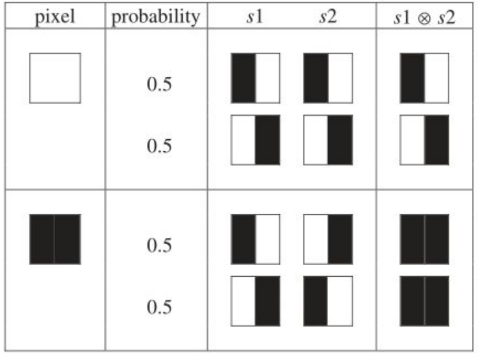
Presented by: Kyle Tilbury

Visual Cryptographic Schemes (VCS)

(k,n)-threshold visual cryptographic scheme

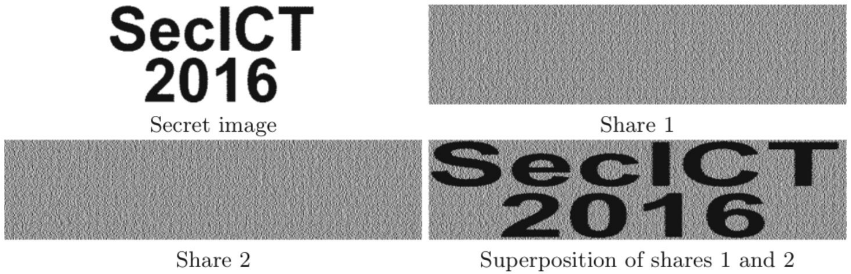
- ➔ First threshold black and white VCS was proposed by Naor and Shamir in 1994
- ➔ Sharing phase:
  - ◆ Dealer encodes the secret image into n shares and gives each participant a share
- ➔ Reconstruction phase:
  - ◆ If k or more participants come together and stack their shares they will be able to retrieve the secret image visually

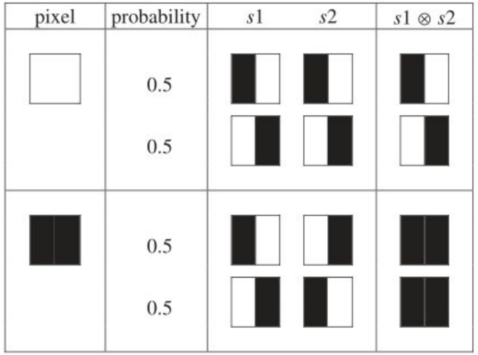




Visual Cryptographic Schemes (VCS)

- ➔ Loss of **contrast** in the reconstructed secret image
- ➔ Change in scale of shares and reconstructed secret due to **pixel expansion**
  - ◆ Pixel expansion is the number of subpixels each pixel of the original image is encoded into
  - ◆ Pixel expansion is a “goodness” measure for VCS





Colour Visual Cryptographic Schemes

- ➔ Color visual cryptography was first conceptualized by Verheul and Tilborg in 1997

- ➔ Jump from sharing a black & white secret image to a color image is not straight-forward
  - ◆ In black and white VCS, superposition of black or white pixels results in a black or a white pixel
  - ◆ With a colour image, superposition of two different coloured pixels may give rise to a third colour
  - ◆ Thus, need to define how to superimpose colours

Colour Visual Cryptographic Schemes

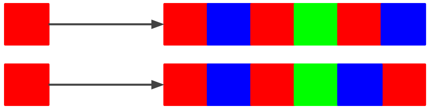
- ➔ This paper gives a generic construction method to share a colour image with maximal contrast
  - ◆ Maximal contrast means that while trying to recover a pixel of some colour no other false coloured pixel is reconstructed
- ➔ Also gives a construction of visual secret sharing for (k,n)*-access structure

Colour VCS: Colour Model

➔ A coloured image is an array of pixels which each have one of the c different colours 0, 1, …, c - 1

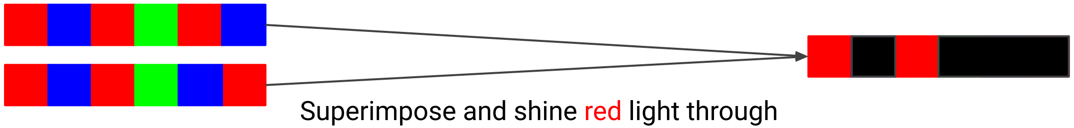
➔ Colour superposition principle:

a. Each secret pixel is divided into some number of subpixels of colour 0, 1, …, c - 1



b. If some subpixels are placed on top of one another and held to light, then a light of color i filters through the stacked subpixels if and only if all the subpixels are color i

c. Otherwise, no light (black colour) filters through the stacking



◆ The colour black is always distinguishable from the c colours and is denoted by •

Colour VCS: Colour Model

➔ The "generalized OR"(GOR) denoted by $\vee$, of the colours i $\in \{0, 1, \ldots, c-1\}$ is defined as follows:

$$(i \vee i) = i$$

and

$$(i \vee \bullet) = \bullet \text{ for all } i = 0, 1, \ldots, c-1$$

and

$$(i \vee j) = \bullet \text{ for all } i \neq j \text{ where } i, j = 0, 1, \ldots, c-1$$

Colour VCS: Colour Model

➔ For any n-dimensional vector V with entries from the set $\{0, 1, \ldots, c - 1\}$,

$z_i(V)$ denotes the number of coordinates in V equal to i where $i = 0, 1, \ldots, c - 1$

For example:

$V = (0, 1, 0, 2, 0, 1) =$ 

$z_0(V) = z$() $= 3$

$z_1(V) = z$() $= 2$

$z_2(V) = 1$

Colour VCS: Definition

- ➔ An unconditionally secure (k,n)-threshold visual cryptographic scheme with *c* colours is denoted by:

$$(k,n)_c\text{-CVCS}$$

- ➔ Let $P = \{1, 2, \ldots, n\}$ be a set of participants

- ➔ A $(k,n)_c$-CVCS on P satisfies:

1. Any subset of k participants can recover the secret image
2. Any subset of participants with size strictly less than k does not have any information about the secret image

Colour VCS: Definition

A $(k,n)_c$-CVCS with pixel expansion *m* can be implemented by means of *c* many $n \times m$ basis matrices $S^0, S^1, \ldots, S^{c-1}$, where S^b corresponds to the color $b \in \{0, 1, \ldots, c-1\}$, if there exist two non-negative numbers *h*, *l* with $l < h$ such that the following two conditions hold:

1. (Contrast condition) If $X = \{i_1, i_2, \ldots, i_k\} \subseteq P$, then for any $i = 0, 1, \ldots, c-1$ the "or" V of rows $i_1, i_2, \ldots, i_k$ of S^i satisfies $z_i(V) \geq h$ and $z_j(V) \leq l$, for $j \neq i$

2. (Security condition) If $X = \{i_1, i_2, \ldots, i_p\} \subseteq P$, with $p < k$, then the $p \times m$ matrices obtained by restricting $S^0, S^1, \ldots, S^{c-1}$ to rows $i_1, i_2, \ldots, i_p$ are equal up to a column permutation

Colour VCS: Definition

More simply:

➔ (Contrast condition) A pixel will be seen as a pixel of colour *i* if and only if:

Sufficiently many subpixels (at least *h*) are of colour *i*

and

For any $j \neq i$, not too many subpixels (at most *l*) are of colour *j*

Schemes having $l = 0$ are maximal-contrast schemes

➔ (Security condition) With less than the threshold of k participants, the matrices are indistinguishable in the sense that they contain the same matrices with the same frequencies

Colour VCS: Example

When k = 2, n = 4, and c = 5, the five basis matrices of a $(2, 4)_5$-CVCS are:

$$S^0 = \begin{bmatrix} 01234 \\ 02341 \\ 03412 \\ 04123 \end{bmatrix} \quad S^1 = \begin{bmatrix} 10234 \\ 12340 \\ 13402 \\ 14023 \end{bmatrix} \quad S^2 = \begin{bmatrix} 21034 \\ 20341 \\ 23410 \\ 24103 \end{bmatrix}$$

$$S^3 = \begin{bmatrix} 31204 \\ 32041 \\ 30412 \\ 34120 \end{bmatrix} \quad S^4 = \begin{bmatrix} 41230 \\ 42301 \\ 43012 \\ 40123 \end{bmatrix}.$$

In this scheme we have m = pixel expansion = 5, l = 0, and h = 1

Colour VCS: Example

Share generation:

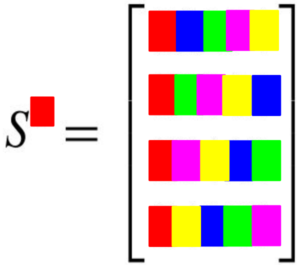
1. During share generation phase the dealer chooses the matrix S^b if the secret pixel is colour $b \in \{0,1,\ldots,c-1\}$
2. Then he applies a random column permutation on the matrix S^b and gives the participant P_i the i^{th} row of the resulting matrix as the participant's share for all i
3. When the dealer wants to share a *c*-coloured image then for each constituent pixel he repeatedly performs the above process till all the pixels are shared

Colour VCS: Example

Share generation:

1. During share generation phase the dealer chooses the matrix S^b if the secret pixel is colour $b \in \{0,1,\ldots,c-1\}$

$$S^0 = \begin{bmatrix} 01234 \\ 02341 \\ 03412 \\ 04123 \end{bmatrix} =$$

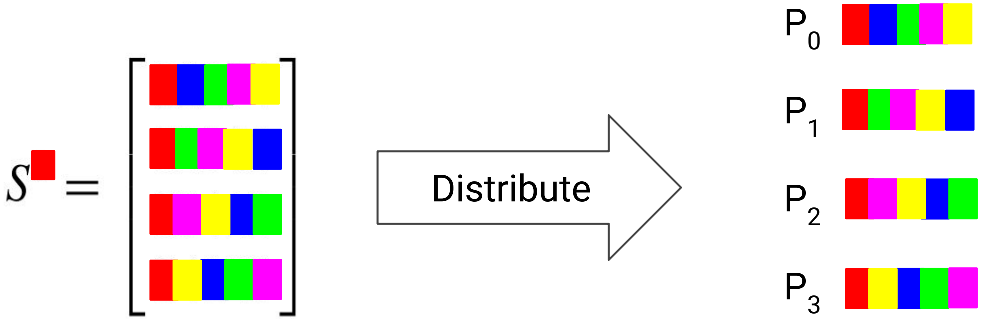


Suppose our secret pixel colour b = 0 = red

Colour VCS: Example

2. Then he applies a random column permutation on the matrix S^b and gives the participant P_i the i^{th} row of the resulting matrix as the participant's share for all *i*

$$S^0 = \begin{bmatrix} 01234 \\ 02341 \\ 03412 \\ 04123 \end{bmatrix} =$$



Suppose this is the random column permutation result

Colour VCS: Example

3. When the dealer wants to share a *c*-coloured image then for each constituent pixel he repeatedly performs the above process till all the pixels are shared

$$S^0 = \begin{bmatrix} 01234 \\ 02341 \\ 03412 \\ 04123 \end{bmatrix} \qquad S^1 = \begin{bmatrix} 10234 \\ 12340 \\ 13402 \\ 14023 \end{bmatrix} \qquad S^2 = \begin{bmatrix} 21034 \\ 20341 \\ 23410 \\ 24103 \end{bmatrix}$$

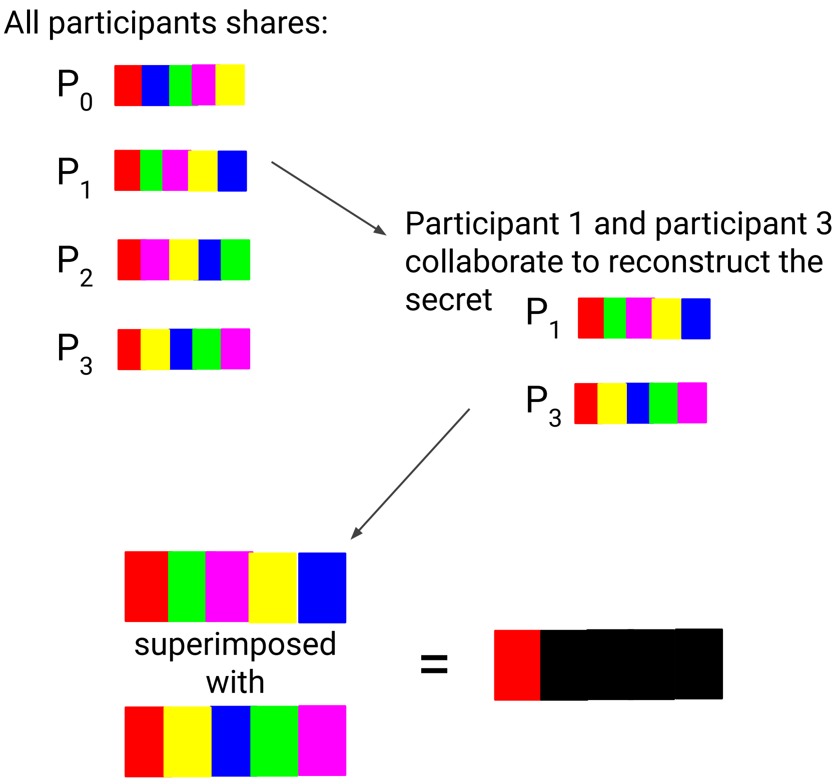
$$S^3 = \begin{bmatrix} 31204 \\ 32041 \\ 30412 \\ 34120 \end{bmatrix} \qquad S^4 = \begin{bmatrix} 41230 \\ 42301 \\ 43012 \\ 40123 \end{bmatrix}.$$

Colour VCS: Example

Reconstruction

Recall:

1. We have a $(2, 4)_5$-CVCS
2. The superposition principle for the colours $i \in \{0, 1, \ldots, c - 1\}$ is:
   a. $(i \vee i) = i$ and
   b. $(i \vee \bullet) = \bullet$ for all $i = 0, 1, \ldots, c - 1$ and
   c. $(i \vee j) = \bullet$ for all $i \neq j$ where $i, j = 0, 1, \ldots, c - 1$
3. A pixel will be seen as a pixel of colour i if and only if: Sufficiently many subpixels (at least *h*) are of colour *i* and for any $j \neq i$, not too many subpixels (at most *l*) are of colour *j*
   a. We have l=0 and h=1

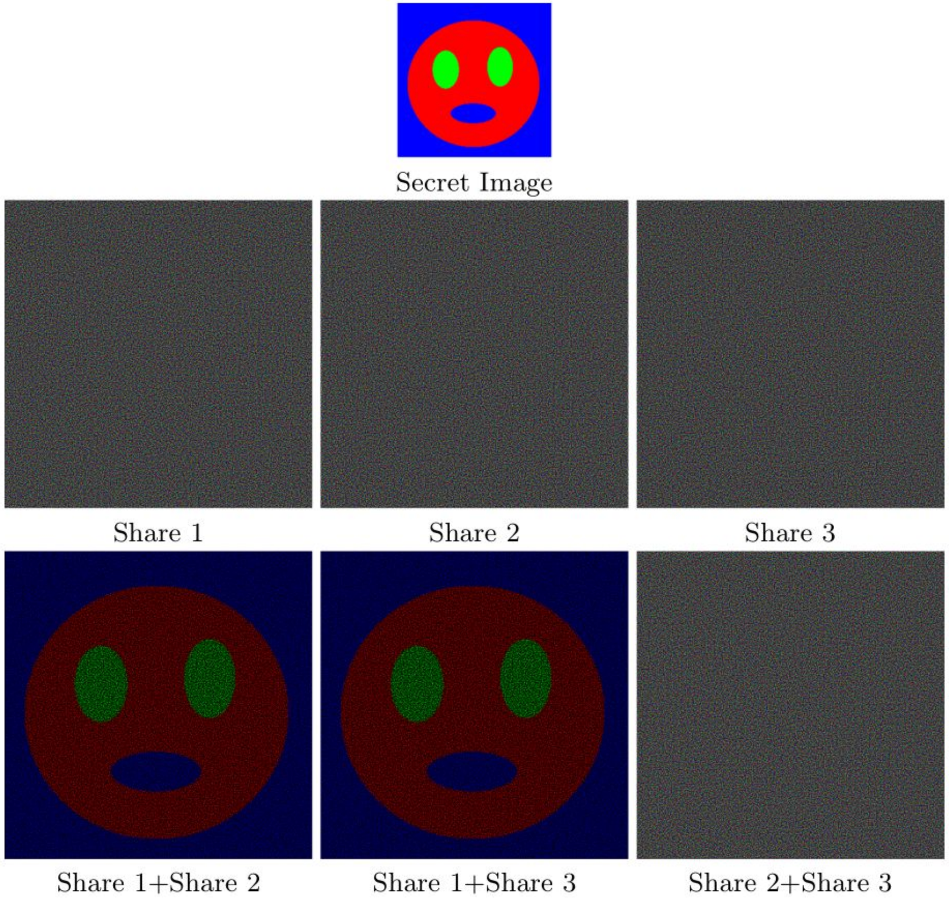


Colour VCS on (k,n)*-access structure

- (k,n)*-access structure
  - Address the scenario where one participant is “essential”
  - The essential participant needs the help of k-1 participants, other than himself, to recover the secret image
- Specific construction details can be found in the paper

Colour VCS: Example

- ➔ Example of a $(2, 3)_3$*-CVCS
- ➔ “Essential” participant is the participant with Share 1



Conclusion and Discussion

Conclusion:

- ➔ Provided some overview of background for VCS
- ➔ Went through a specific construction for a CVCS
- ➔ Showed example of CVCS on (k,n)*-access structure

Discussion:

- ➔ Is there any applications for this? Is this just a fun “toy” problem to solve?

References

- Dutta, S., Adhikari, A., & Ruj, S. (2018). Maximal contrast color visual secret sharing schemes. *Designs, Codes and Cryptography*, 1-13.

- Blundo, C., De Bonis, A., & De Santis, A. (2001). Improved schemes for visual cryptography. *Designs, Codes and Cryptography*, *24*(3), 255-278.