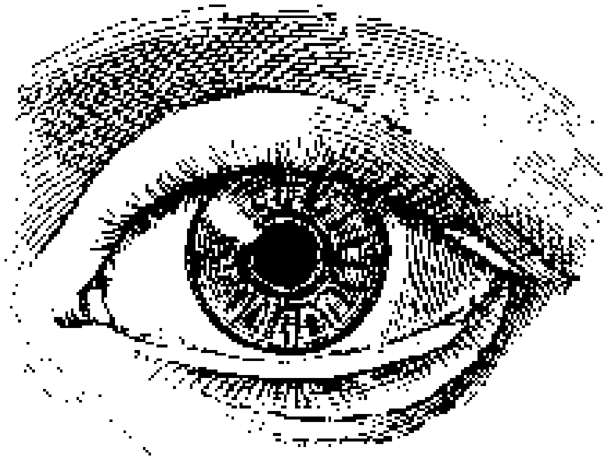


Visual Cryptography,

or

Seeing is Believing

Douglas R. Stinson

School of Computer Science

University of Waterloo

http://cacr.math.uwaterloo.ca/~dstinson/index.html

Secret Sharing

- let $\mathbf{k} = k_1 k_2 \cdots k_n$ be a binary string of length n, called the $\boxed{\text{secret}}$
- for $1 \leq i \leq n$, let $x_i \in \mathbb{Z}_2$ be chosen at random
- for $1 \leq i \leq n$, let $y_i = x_i + k_i \bmod 2$
- then $\mathbf{x} = x_1 x_2 \cdots x_n$ and $\mathbf{y} = y_1 y_2 \cdots y_n$ are two $\boxed{\text{shares}}$ corresponding to the secret $\mathbf{k}$
- neither $\mathbf{x}$ nor $\mathbf{y}$ provide any information as to the secret
- however, $\mathbf{x}$ and $\mathbf{y}$ together allow the secret to be computed as $\mathbf{k} = \mathbf{x} + \mathbf{y} \bmod 2$

Threshold Schemes

- a $\boxed{(t, w) \text{ threshold scheme}}$ allows a secret $\mathbf{k}$ to be split into w shares
- any t of the w shares can be used to reconstruct the secret
- no $t-1$ shares reveal any information as to the value of the secret
- the scheme described above is a $(2, 2)$ threshold scheme
- in 1979, Shamir showed how to construct a (t, w) threshold scheme based on polynomial interpolation over a finite field $\mathbb{F}_q$, provided that $q \geq w + 1$

Shamir Threshold Scheme

- let $x_1, x_2, \ldots, x_w$ be w distinct non-zero elements of $\mathbb{F}_q$
- given a secret $\mathbf{k} \in \mathbb{F}_q$, w shares are generated as follows:
  1. let $a_1, \ldots, a_{t-1}$ be chosen independently at random from $\mathbb{F}_q$
  2. let
  $$a(x) = \mathbf{k} + \sum_{j=1}^{t-1} a_j\, x^j$$
  3. for $1 \leq i \leq w$, let the share $s_i = (x_i, y_i)$ where $y_i = a(x_i)$
- given t shares, $\mathbf{k}$ can be computed by using an interpolation formula:

$$\mathbf{k} = \sum_{j=1}^{t} \left(\prod_{1 \leq k \leq t, k \neq j} \frac{x_{i_k}}{x_{i_k} - x_{i_j}} \right) y_{i_j}$$

Visual Secret Sharing

- in a "regular" threshold scheme, the reconstruction of the secret typically involves computations in a finite field
- in a visual threshold scheme, the secret is reconstructed visually
- the secret and the shares are images represented on transparencies consisting of black and white (transparent, actually) pixels
- to reconstruct the secret, t of the w shares (transparencies) are superimposed

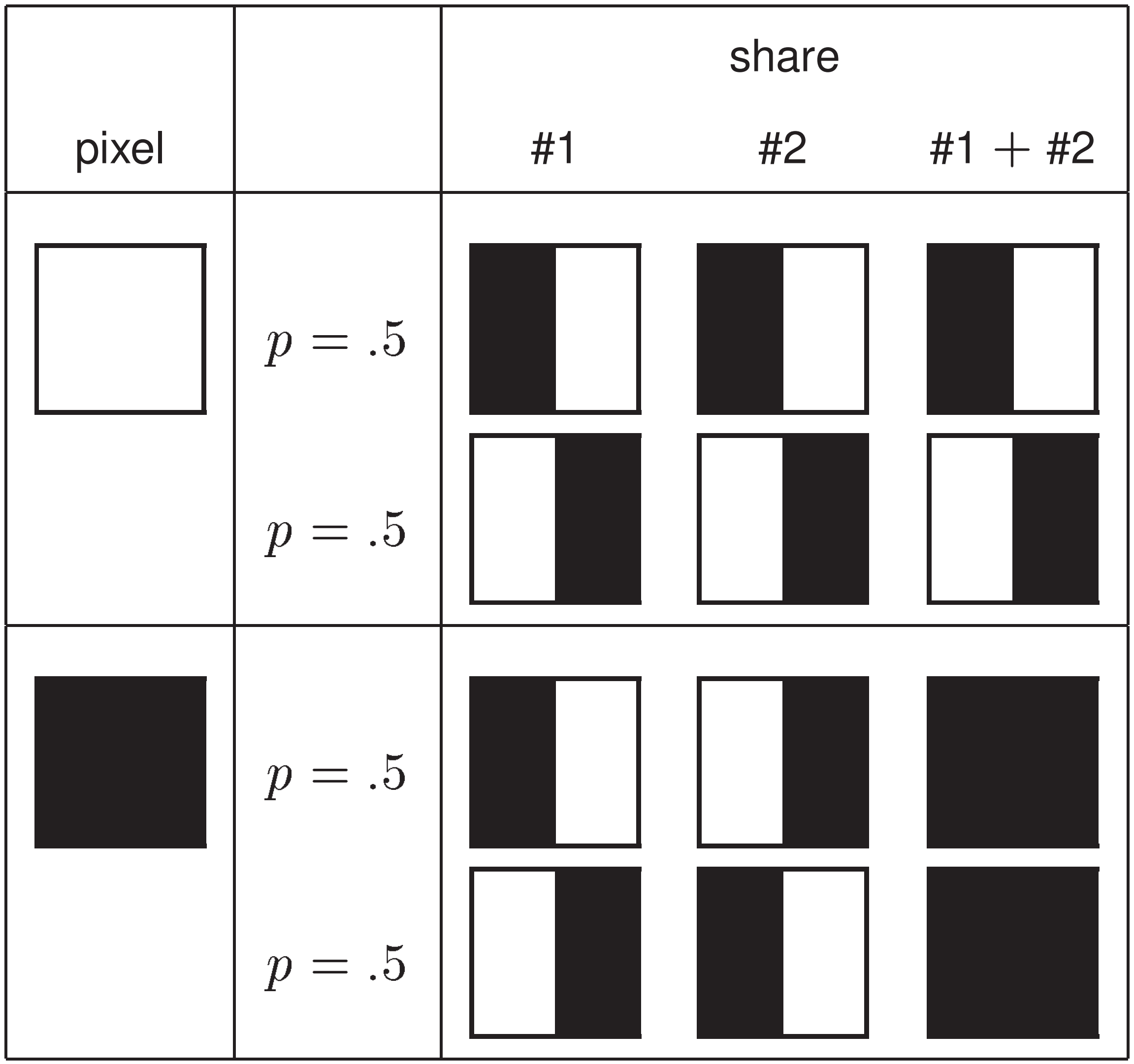
Visual Secret Sharing (cont.)

- let's consider a $(2, 2)$ threshold scheme, where $0 + 0 = 0$, $0 + 1 = 1$, $1 + 0 = 1$ and $1 + 1 = 0$
- suppose we let "black" correspond to 1 and "white" correspond to "0"
- if we superimpose "white" and "white" we get "white" ($0 + 0 = 0$, GOOD!)
- if we superimpose "white" and "black" we get "black" ($0 + 1 = 1$, GOOD!)
- if we superimpose "black" and "black" we get "black" ($1 + 1 = 1$, OOPS!)
- our visual system performs a boolean "or", when what we want is a boolean "xor"

Visual Secret Sharing (cont.)

- Naor and Shamir (1994) had the idea of replacing each pixel in the image by some number, m, of subpixels in each share
- if the $\boxed{\text{gray level}}$ of a black pixel (in t superimposed shares) is darker than the gray level of a white pixel, then the image should be recognizable
- it is also required that no information about a pixel can be obtained by examining $t-1$ or fewer shares
- this cannot be accomplished if $m = 1$, because a black pixel in any share implies that the corresponding pixel in the image is black

A $(2,2)$ Visual Threshold Scheme



Basis Matrices

- let S^0 and S^1 be two w by m $\quad 0-1$ matrices
- S^0 and S^1 are defined to be $\boxed{\text{basis matrices}}$ for a $\boxed{(t,w)\text{-visual threshold scheme}}$ (VTS) with $\boxed{\text{pixel expansion}}$ m and $\boxed{\text{relative contrast}}$ γ, provided that they satisfy the following properties for every set $X \subseteq \{1,\ldots,w\}$ of cardinality at most t:
  1. if $X = \{i_1,\ldots,i_t\}$, then the difference of the weight of the "or" of rows $i_1,\ldots,i_t$ of S^1 and the weight of the "or" of rows $i_1,\ldots,i_t$ of S^0 is at least γm
  2. if $X = \{i_1,\ldots,i_p\}$, with $p \le t-1$, then the two p by m matrices obtained by restricting S^0 and S^1 to rows $i_1,\ldots,i_p$ are identical up to a column permutation.

Share Distribution Algorithm

For each pixel P, do the following:

1. Generate a random permutation π of the set $\{1, \ldots, m\}$
2. If P is a black pixel, then apply π to the columns of S^1, else apply π to the columns of S^0. Call the resulting matrix T.
3. For $1 \leq i \leq w$, row i of T comprises the m sub-pixels of pixel P in the ith share.

Examples of Basis Matrices

A $(2,2)$-VTS with $m = 2$ and $\gamma = 1/2$:

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

A $(2,3)$-VTS with $m = 3$ and $\gamma = 1/3$:

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

Another Example of Basis Matrices

A $(2,4)$-VTS with $m = 6$ and $\gamma = 1/3$:

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

Yet Another Example of Basis Matrices

- a $(3,3)$-VTS with $m = 4$ and $\gamma = 1/4$:

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

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

(w, w)-Visual Threshold Schemes

Theorem 1 (Naor and Shamir)
For any integer $w \geq 2$, there exists a (w, w)-VTS with $m = 2^{w-1}$ and $\gamma = 1/2^{w-1}$.

Proof. Define the columns of S^0 to consist of all binary w-tuples containing an even number of 1's, and define the columns of S^1 to consist of all binary w-tuples containing an odd number of 1's.

A Structure Theorem For (w, w)-VTS

Theorem 2 (Blundo, De Santis and Stinson)
Suppose S^0 and S^1 are basis matrices for a (w, w)-VTS such that there is no column that appears in both S^0 and S^1. Then there is an integer h such that every binary w-tuple containing an even number of 1's occurs exactly h times as a column of S_0, and every binary w-tuple containing an odd number of 1's occurs exactly h times as a column of S_1.

Idea. Suppose **c** and **d** are (column) binary w-tuples that differ only in the ith entry. If **c** appears as a column of S^i with multiplicity h, then **d** appears as a column of S^{1-i} with multiplicity h.

$(2, w)$-VTS

- we restate the conditions on basis matrices for $(2, w)$-VTS
- let S^0 and S^1 be two w by m $0-1$ matrices
- S^0 and S^1 are basis matrices for a (t, w)-VTS with pixel expansion m and relative contrast γ provided that they satisfy the following properties of cardinality at most t:
  1. for all $1 \leq i < j \leq w$, the difference of the weight of the "or" of rows i and j of S^1 and the weight of the "or" of rows i and j of S^0 is at least γm
  2. for all $1 \leq i \leq w$, the weight row i of S^1 is the same as the weight of row i of S^0.

An Upper Bound on the Contrast of $(2, w)$-VTS

Theorem 3 (Blundo, De Santis and Stinson)

In any perfect $(2, w)$-VTS, it holds that

$$\gamma \leq \gamma^*(w) = \frac{\lceil \frac{w}{2} \rceil \lfloor \frac{w}{2} \rfloor}{w(w-1)}.$$

Idea. Define

$$T = \{(i, j, c) : S^1(i, c) = 1, S^1(j, c) = 0\}.$$

On one hand,

$$|T| \geq w(w-1)\gamma m.$$

On the other hand,

$$|T| \leq m \left\lceil \frac{w}{2} \right\rceil \left\lfloor \frac{w}{2} \right\rfloor .$$

Balanced Incomplete Block Designs

- let v, k and λ be positive integers such that $v > k \geq 2$.
- a $\boxed{(v, k, \lambda)\text{-balanced incomplete block design}}$ (BIBD) is a pair $(X, \mathcal{A})$ such that the following properties are satisfied:
  1. X is a set of v elements called $\boxed{\text{points}}$,
  2. $\mathcal{A}$ is a collection of subsets of X called $\boxed{\text{blocks}}$,
  3. each block contains exactly k points, and
  4. every pair of distinct points is contained in exactly λ blocks.

BIBDs (cont.)

- each point in a (v, k, λ)-BIBD occurs in exactly $r = \frac{\lambda(v-1)}{k-1}$ blocks
- the number of blocks in a (v, k, λ)-BIBD is exactly $b = \frac{vr}{k} = \frac{\lambda(v^2-v)}{k^2-k}$
- $(X, \mathcal{A})$ is said to be a (v, b, r, k, λ)-BIBD
- the $\boxed{\text{incidence matrix}}$ of $(X, \mathcal{A})$ is the v by b $0-1$ matrix $M = (m_{i,j})$ defined by the rule

$$m_{i,j} = \begin{cases} 1 & \text{if } x_i \in A_j \\ 0 & \text{if } x_i \notin A_j, \end{cases}$$

where $X = \{x_i : 1 \leq i \leq v\}$ and $\mathcal{A} = \{A_j : 1 \leq j \leq b\}$

A $(7,7,3,3,1)$-BIBD

- $X = \{1,2,3,4,5,6,7\}$
- $\mathcal{A} = \left\{ \begin{array}{l} \{1,2,4\},\{2,3,5\},\{3,4,6\},\{4,5,7\}, \\ \{1,5,6\},\{2,6,7\},\{1,3,7\} \end{array} \right\}$
- the incidence matrix is:

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$$

Constructing $(2, w)$-VTS From BIBDs

- let S^1 be the incidence matrix of a (w, b, r, k, λ)-BIBD
- define S^0 to be the w by b matrix in which every row consists of r 1s followed by $b - r$ 0s
- the pixel expansion is $m = b$
- every row of S^0 or S^1 has weight r.
- the weight of the "or" of two rows of S^0 has weight r

$(2, w)$-VTS From BIBDs (cont.)

- for any two rows of S^1, there are λ columns in which there is a "1" in both rows
- the weight of the "or" of two rows of S^1 has weight $2r - \lambda$
- the contrast is thus

$$\gamma = \frac{2r - \lambda - r}{b} = \frac{r - \lambda}{b}$$

$(2, w)$-VTS From BIBDs (cont.)

Theorem 4 (Blundo, De Santis and Stinson)
Suppose there exists a (w, b, r, k, λ)-BIBD. Then there exists a $(2, w)$-VTS with pixel expansion $m = b$ and relative contrast $\gamma = (r - \lambda)/b$.

Corollary 5
Suppose there exists a $(4s - 1, 2s - 1, s - 1)$-BIBD. Then there exists a $(2, 4s - 1)$-VTS with pixel expansion $m = 4s - 1$ and (optimal) relative contrast $\gamma^*(4s - 1) = s/(4s - 1)$.

An Example

A $(2,7)$-VTS with $m = 2$ and $\gamma = 2/7$:

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

Hadamard Matrices and Designs

- an n by n matrix H with entries ± 1, such that $HH^T = nI_n$, is called a $\boxed{\text{Hadamard matrix}}$ of order n
- a Hadamard matrix of order n exists only if $n = 1$, $n = 2$ or $n \equiv 0 \bmod 4$
- a Hadamard matrix of order $4s$ is equivalent to a $(4s-1, 4s-1, 2s-1, 2s-1, s-1)$-BIBD
- the famous **Hadamard Matrix Conjecture** (1893) states that a of order $4s$ exists for all positive integers s
- the conjecture is proved for all $s \le 107$

Examples of Hadamard Matrices

- a Hadamard matrix of order 2:

$$\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

- a Hadamard matrix of order 4:

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

Examples of Hadamard Matrices (cont.)

- a Hadamard matrix of order 8:

$$\begin{pmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & -1 & -1 & -1 & 1 & -1 & 1 \\
1 & 1 & 1 & -1 & -1 & -1 & 1 & -1 \\
1 & -1 & 1 & 1 & -1 & -1 & -1 & 1 \\
1 & 1 & -1 & 1 & 1 & -1 & -1 & -1 \\
1 & -1 & 1 & -1 & 1 & 1 & -1 & -1 \\
1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \\
1 & -1 & -1 & -1 & 1 & -1 & 1 & 1
\end{pmatrix}$$

A Construction for Hadamard BIBDs

- suppose $p \equiv 3 \bmod 4$ is prime
- let $A_0 = \{x^2 \bmod p : 1 \leq x \leq (p-1)/2\}$
- for $1 \leq i \leq p-1$, let $A_i = A_0 + i \bmod p$
- let $\mathcal{A} = \{A_i : 0 \leq i \leq p-1\}$
- then $(\mathbb{Z}_p, \mathcal{A})$ is a $\left(p, \frac{p-1}{2}, \frac{p-3}{4}\right)$-BIBD

An Example

- suppose $p = 11$
- the blocks of the $(11, 5, 2)$-BIBD are as follows:

$$\begin{array}{ll}
A_0 = \{1, 3, 4, 5, 9\} & A_1 = \{2, 4, 5, 6, 10\} \\
A_2 = \{0, 3, 5, 6, 7\} & A_3 = \{1, 4, 6, 7, 8\} \\
A_4 = \{2, 5, 7, 8, 9\} & A_5 = \{3, 6, 8, 9, 10\} \\
A_6 = \{0, 4, 7, 9, 10\} & A_7 = \{0, 1, 5, 8, 10\} \\
A_8 = \{0, 1, 2, 6, 9\} & A_9 = \{1, 2, 3, 7, 10\} \\
A_{10} = \{0, 2, 3, 4, 8\} &
\end{array}$$

Optimal Contrast $(2, w)$-VTS

Theorem 6 (Blundo, De Santis and Stinson)

Suppose the Hadamard Matrix Conjecture is true. Then, for every integer $w \geq 2$, then there exists a $(2, w)$-VTS with (optimal) relative contrast $\gamma^*(w)$, having pixel expansion

$$m = \begin{cases} 2w - 2 & \text{if } w \text{ is even} \\ w & \text{if } w \equiv 3 \bmod 4 \\ 2w & \text{if } w \equiv 1 \bmod 4 \end{cases}$$

- the $(2, w)$-VTS are all constructed from BIBDs obtained from Hadamard matrices
- the resulting pixel expansions are optimal among all $(2, w)$-VTS having optimal relative contrast

Minimal Pixel Expansion in $(2, w)$-VTS

Theorem 7

There exists a $(2, w)$-VTS with pixel expansion m and relative contrast $\gamma \geq 1/m$ if and only if there exists a Sperner family of size w over a ground set of cardinality m.

- for example, $\{1, 2, 3\}$, $\{1, 4\}$, $\{2, 4\}$, $\{3, 4\}$ is a Sperner family over the ground set $\{1, 2, 3, 4\}$
- this gives rise to the following basis matrices for a $(2, 4)$ threshold VCS with $m = 4$:

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

Sperner's Theorem

Theorem 8 (Sperner, 1928)

Suppose $\mathcal{A}$ is a Sperner family over the ground set $\{1, \ldots, m\}$. Then

$$|\mathcal{A}| \leq \binom{m}{\lceil \frac{m}{2} \rceil}.$$

Further, equality occurs if and only if $\mathcal{A}$ consists of all the subsets of $\{1, \ldots, m\}$ of cardinality $\lceil \frac{m}{2} \rceil$, or all the subsets of $\{1, \ldots, m\}$ of cardinality $\lfloor \frac{m}{2} \rfloor$.

- hence, there exists a $(2, w)$ VTS with pixel expansion m and relative contrast $\gamma \geq 1/m$ if and only if $w \leq \binom{m}{\lceil \frac{m}{2} \rceil}$
- we can take $m = O(\log w + \log \log w)$

Visual Cryptographic Schemes for Graph Access Structures

- suppose $G = (V, E)$ is a graph with vertex set $V = \{1, \ldots, w\}$
- a $\boxed{G\text{-visual cryptographic scheme}}$ (or G-VCS) satisfies the following properties:
  1. the image is revealed by superimposing two shares i and j if $\{i, j\} \in E$
  2. no information about the image can be obtained from any one share, or from two shares i and j if $\{i, j\} \notin E$

A VCS for the Path of Length Three

- suppose $w = 4$ and P_3 is the following graph:

- here are the basis matrices for a P_3-VCS with $m = 3$ and $\gamma = 1/3$:

$$S^0 = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \quad S^1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Some References

- M. Naor and A. Shamir. Visual Cryptography, *EUROCRYPT '94 Proceedings*.
- G. Ateniese, C. Blundo, A. De Santis and D.R. Stinson. Visual Cryptography for General Access Structures, *Information and Computation*, 1996.
- C. Blundo, A. De Santis and D.R. Stinson. On the Contrast in Visual Cryptography Schemes, *Journal of Cryptology*, 1999.
- T. Hofmeister, M. Krause and H.U. Simon. Contrast-optimal k out of n secret sharing schemes in visual cryptography. *Theoretical Computer Science*, 2000.
- G. Ateniese, C. Blundo, A. De Santis and D.R. Stinson. Extended capabilities for visual cryptography. *Theoretical Computer Science*, 2001.
- P.A. Eisen and D.R. Stinson. Threshold visual cryptography schemes with specified whiteness levels of reconstructed pixels, *Designs, Codes and Cryptography*, 2002.