Visual Cryptography

Frederik Vercauteren

University of Bristol,
Merchant Venturers Building,
Woodland Road,
Bristol BS8 1UB

frederik@cs.bris.ac.uk

Overview

- Introduction
- Basic 2 out of 2 scheme
- Modelling visual cryptography schemes
- Parameters of visual cryptography schemes
- Solution for k out of k scheme
- Extensions

Introduction

Eurocrypt ’94: Naor and Shamir - Visual Cryptography

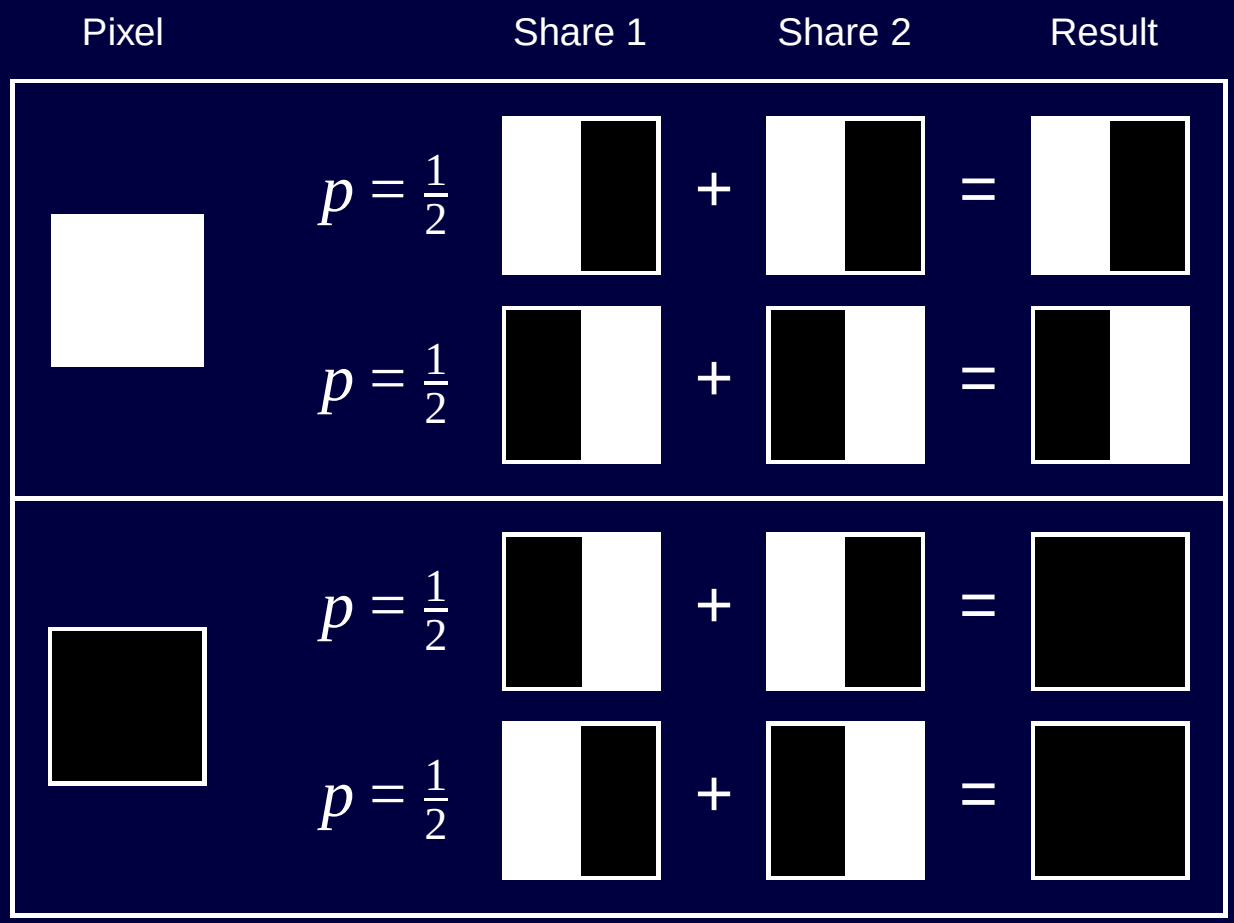
- Image split into 2 shares
- Decoding = stacking transparencies
- Perfectly secure, 1 share contains no information about image

Extended to k out of n sharing problem

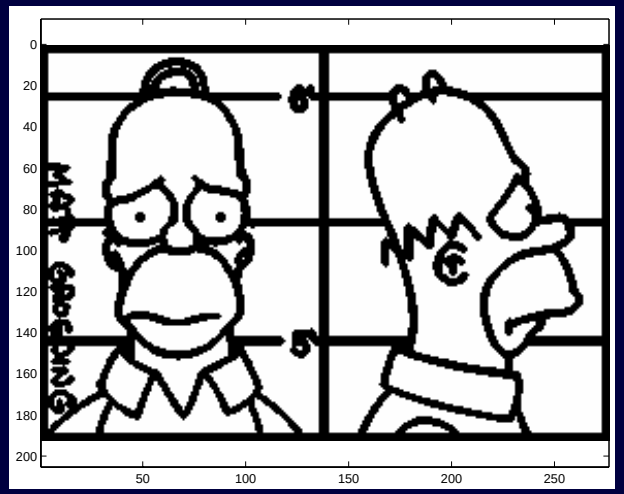
- Image split into n shares
- Any k stacked together reveal image
- Perfectly secure, any $k-1$ shares contain no information

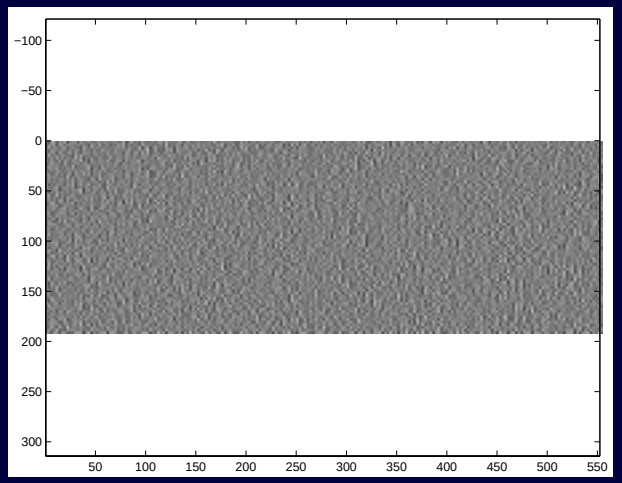
Basic Scheme: 2 out of 2

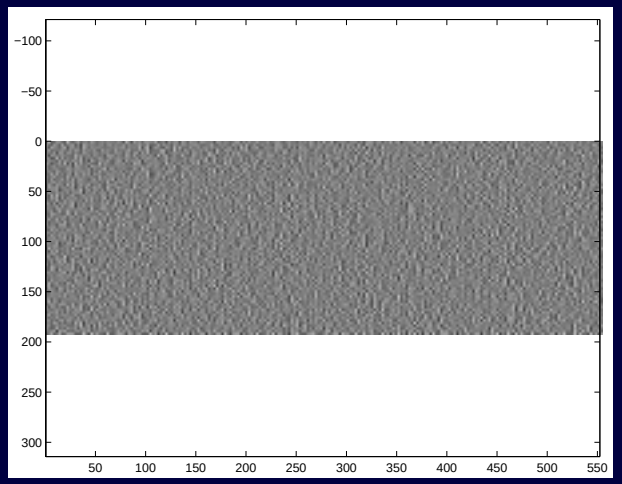
Black and white image: each pixel divided in 2 sub-pixels

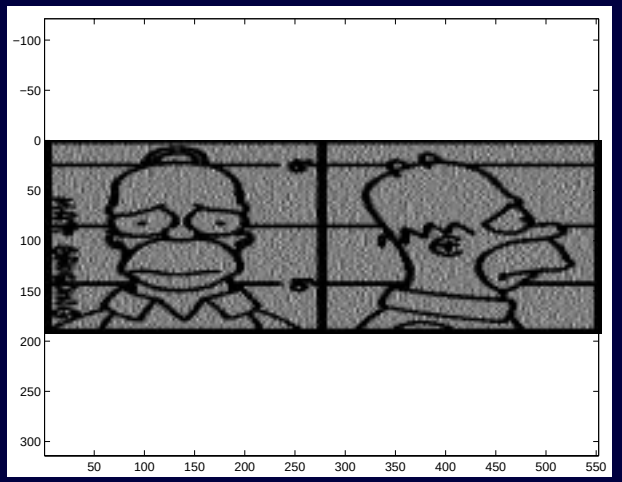


Basic Scheme: Example









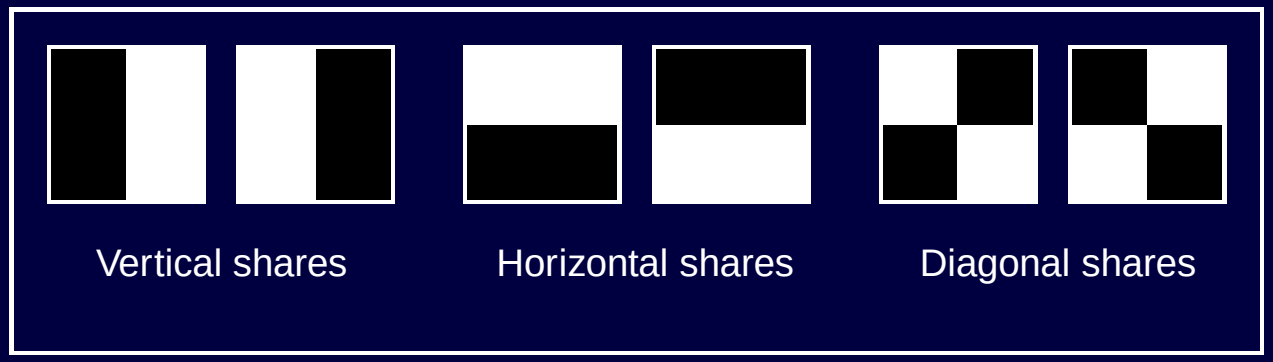
Basic Scheme - No Distortion

Black and white image: each pixel divided in 4 sub-pixels

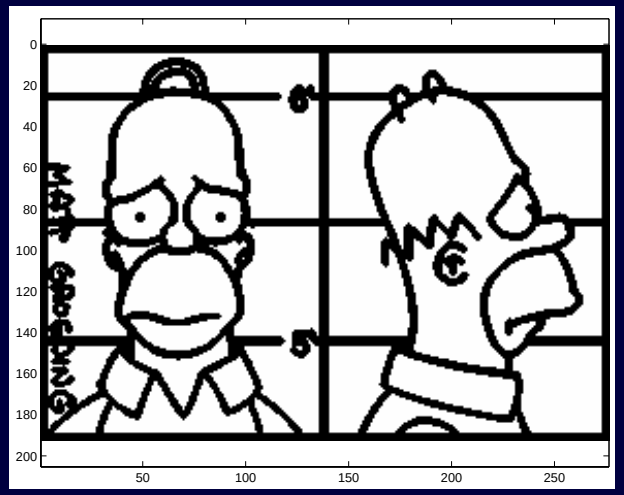
- White pixel: shared into two identical sub-pixel layouts
- Black pixel: shared into two complementary sub-pixel layouts

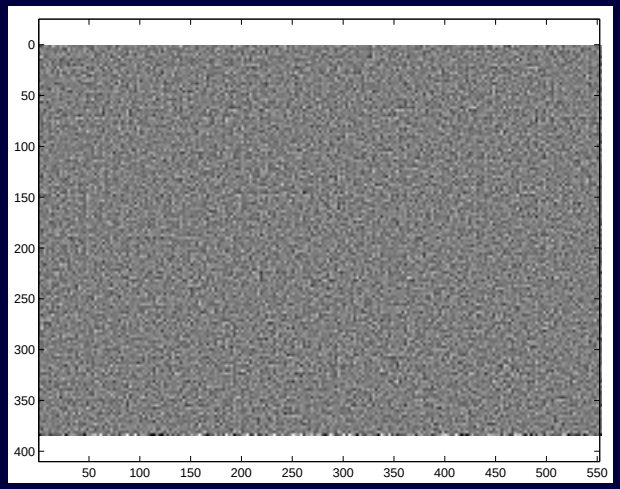
$\Rightarrow$ Perfect security:

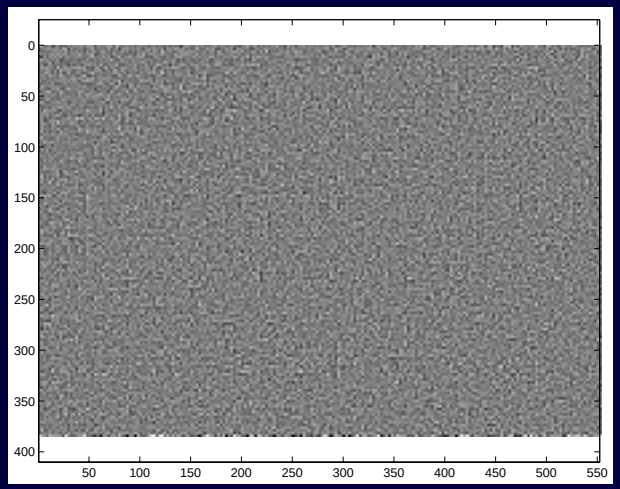
- Layout was randomly chosen
- Each pixel has 2 black and 2 white sub-pixels

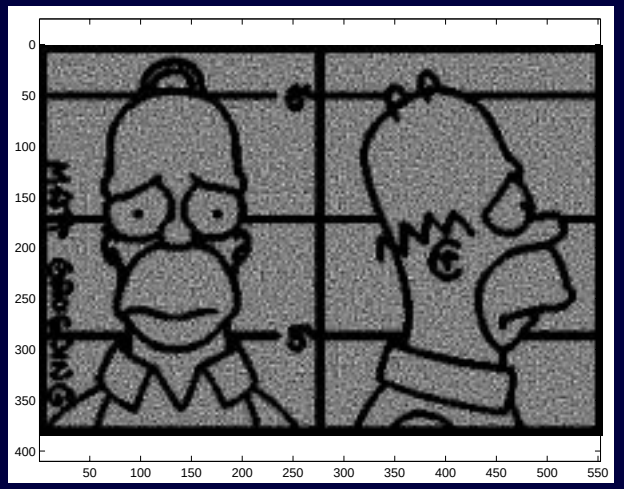


Basic Scheme - No Distortion: Example









Visual Cryptography Schemes: Model

Each pixel (black or white):

- appears in n shares
- divided into m sub-pixels

$\Rightarrow$ 1 pixel represented by $n \times m$ Boolean matrix $S = [s_{ij}]$

$s_{ij} = 1$ iff jth sub-pixel in the ith transparency is black

Example: 2 out of 2 scheme with 2 sub-pixels

- White pixel: $\begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}$ or $\begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}$
- Black pixel: $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ or $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

Visual Cryptography Schemes: Model

Combining shares $i_1, \ldots, i_r$ gives Boolean or V of rows $i_1, \ldots, i_r$ of S

Grey level proportional to Hamming weight $H(V)$

- Interpreted as black if $H(V) \geq d$ for threshold d
- Interpreted as white if $H(V) \leq d - \alpha \cdot m$ for relative difference $\alpha > 0$

Example: 2 out of 2 scheme with 4 sub-pixels gives $d = 4$ and $\alpha = 1/2$

Resemblance of construction:

- linear codes based on groups
- VCS based on semi-groups, black sub-pixel cannot be undone

Visual Sharing Scheme: k out of n

Solution consists of 2 collections of $n \times m$ Boolean matrices C_0 and C_1

- Share white pixel: randomly choose one matrix in C_0
- Share black pixel: randomly choose one matrix in C_1

Solution is valid iff 3 conditions are met:

1. For any $S \in C_0$, the or of any k rows V satisfies $H(V) \leq d - \alpha \cdot m$
2. For any $S \in C_1$, the or of any k rows V satisfies $H(V) \geq d$
3. For any subset $\{i_1, \ldots, i_q\}$ of $\{1, \ldots, n\}$ with $q < k$, the two collections D_t for $t \in \{0, 1\}$ obtained by restricting each matrix in C_t to rows $\{i_1, \ldots, i_q\}$ are indistinguishable.

Visual Sharing Scheme: Parameters

Number of pixels m in share:

- Loss in resolution
- m as small as possible

Relative difference α:

- Loss in contrast
- α as large as possible

Size r of collections C_0 and C_1:

- $\log r$ is number of random bits needed to generate share
- Does not affect quality of the picture

General k out of k Scheme

Theorem: For all k there exists a general k out of k scheme with

$$m = 2^{k-1} \qquad \alpha = \frac{1}{2^{k-1}} \qquad r = 2^{k-1}!$$

Construct $k \times 2^{k-1}$ matrices S^0 (white pixels) and S^1 (black pixels) as:

- S^0 contains the 2^{k-1} vectors with even number of 1's
- S^1 contains the 2^{k-1} vectors with odd number of 1's

C_0 and C_1 consist of all permutations of columns in S^0 and S^1

Naor and Shamir: any k out of k scheme $\alpha \leq \frac{1}{2^{k-1}}$ and $m \geq 2^{k-1}$

General k out of k Scheme: Examples

$k = 3$, therefore $m = 4$, $\alpha = 1/4$ and $r = 24$

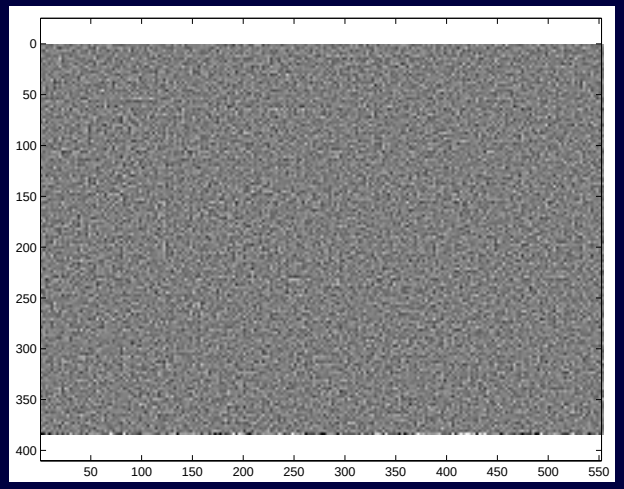
$$S^0 = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix} \qquad S^1 = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \end{bmatrix}$$

$k = 4$, therefore $m = 8$, $\alpha = 1/8$ and $r = 40320$

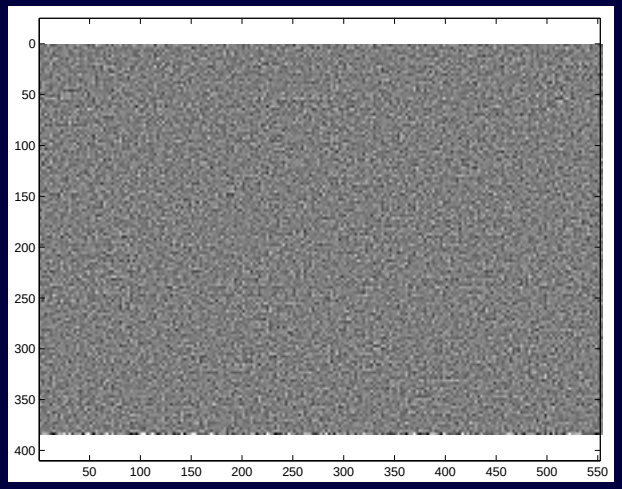
$$S^0 = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix} \qquad S^1 = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0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

General k out of k Scheme: Example

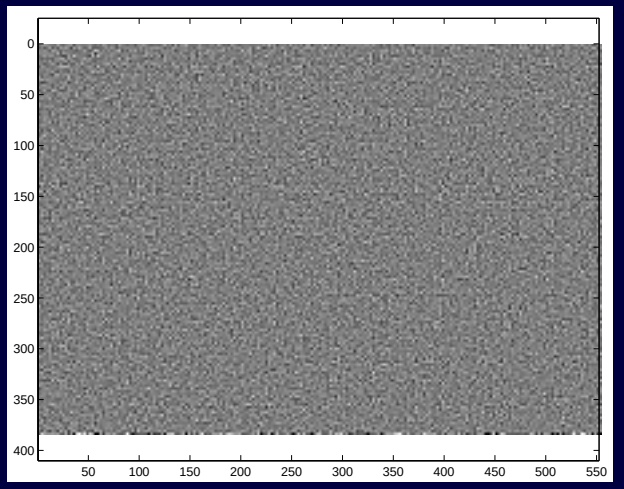
Share 1

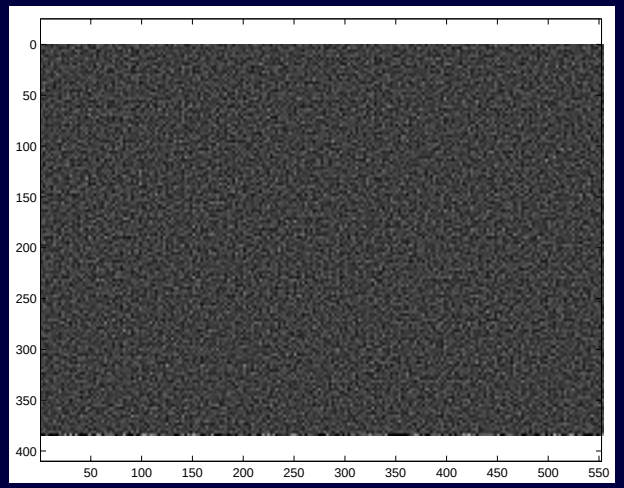


Share 2

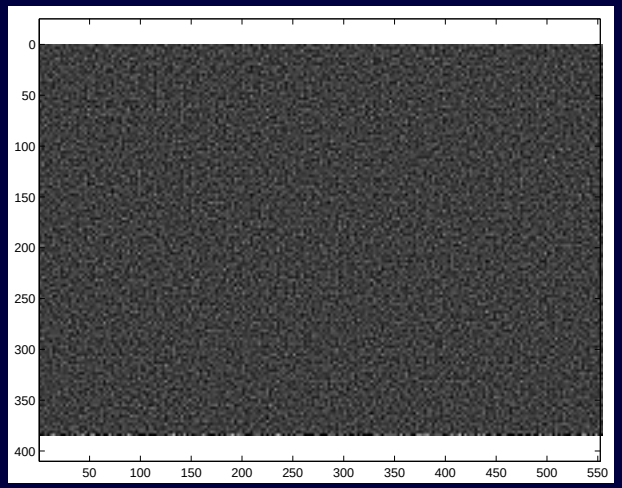


Share 3

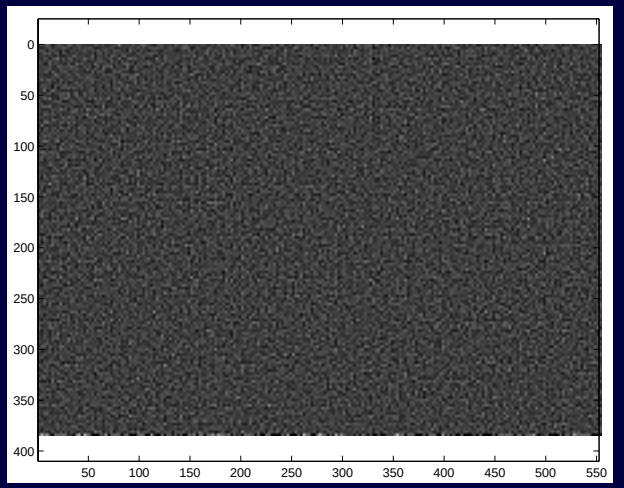




Share 1 + 2

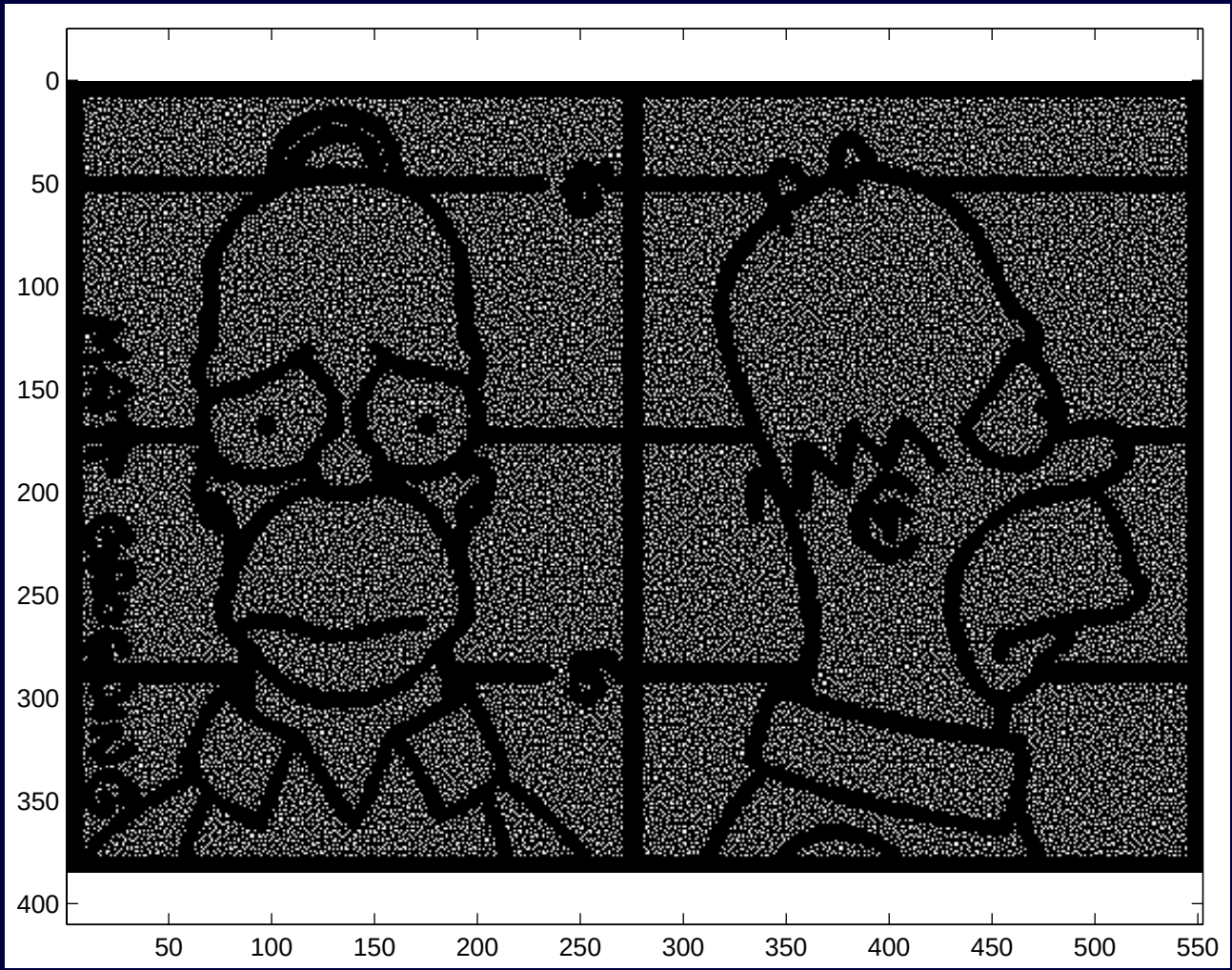


Share 1 + 3



Share 2 + 3

General k out of k Scheme: Example



Extensions of VCS

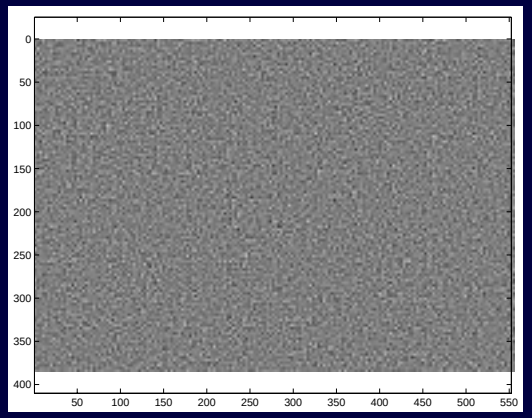
Visual cryptography for general access structures

- Set of participants $P = \{1, \ldots, n\}$
- Qualified set $G_{\text{Qual}} \subset 2^P$, forbidden set $G_{\text{Forb}} \subset 2^P$
- If $G_{\text{Qual}} \cap G_{\text{Forb}} = \emptyset$ then $(G_{\text{Qual}}, G_{\text{Forb}})$ is general access structure

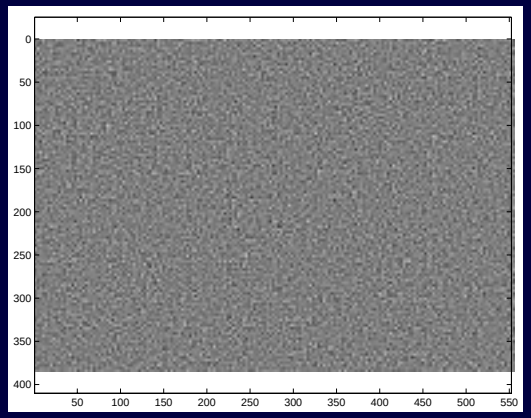
Example: $P = \{1, 2, 3, 4\}$ and G_{Qual} generated by $\{\{1, 4\}, \{1, 2, 3\}\}$ then

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

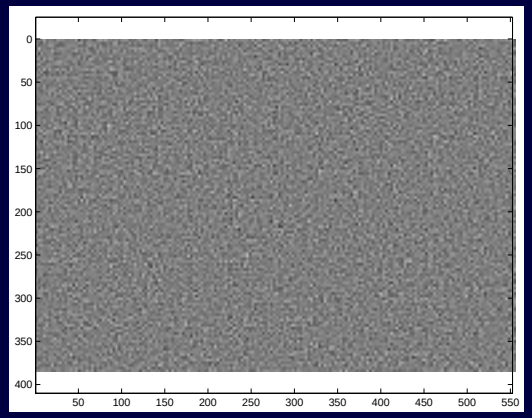
Extensions of VCS: Example



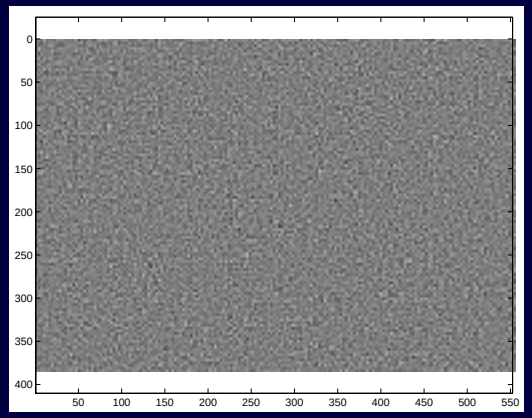
Share 1



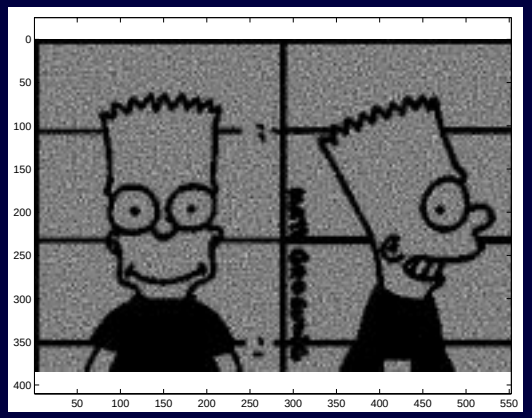
Share 2



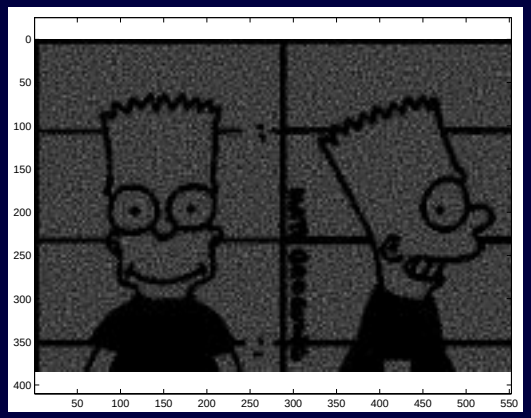
Share 3



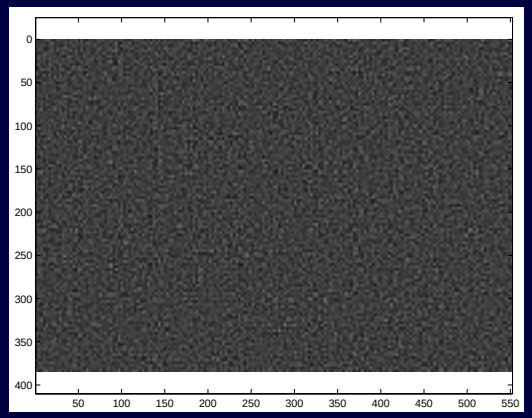
Share 4



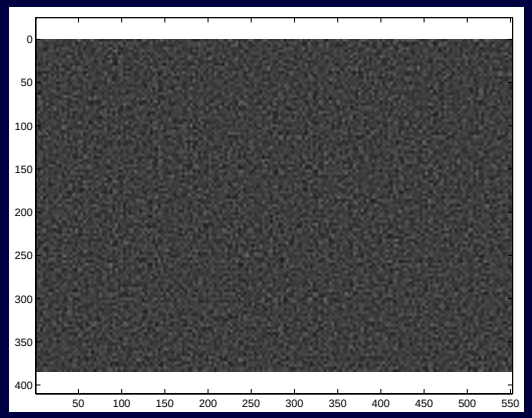
Share 1 + 4



Share 1 + 2 + 3



Share 1 + 2



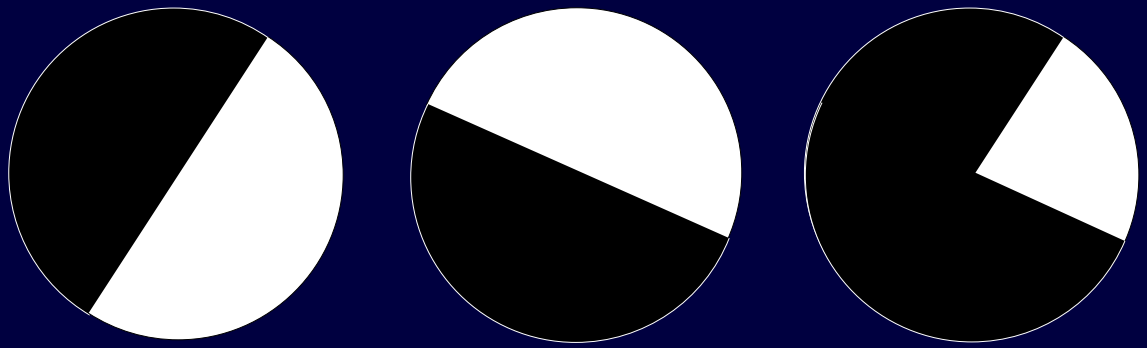
Share 2 + 3 + 4

Extensions of VCS

Grey scale images: pixels range from 0 (white) to 256 (black)

Encoding using rotated half-circles:

- Angle of first half-circle is random
- Angle of second half-circle is chosen $\sim$ grey level



Share 1 Share 2 Result

Extensions of VCS

- Different schemes for colour images
- Schemes for visual authentication and identification
- Concealment of existence of secret message:
  - Each share contains innocent looking image
  - Stacking shares reveals secret image
  - No sign of innocent images remains