Visual Cryptography

Matthias Baumgart
matthias.baumgart@informatik.tu-chemnitz.de

Chemnitz, January 19, 2003

Structure

1. Introduction

2. The Model

3. How to Encrypt

4. Secret Sharing Schemes

   - 2 out of 2 Secret Sharing Scheme
   - 2 out of n Secret Sharing Scheme
   - 3 out of 3 Secret Sharing Scheme

Introduction

- Visual Cryptography solves the problem of encrypting written material (e.g. printed text, handwritten notes, pictures...)
- It is perfectly secure
- It can be decoded directly by the human visual system
- Examples...

The Model

Given n users and a secret information

Task: Encrypt the secret information into n transparencies (for each of the n users one transparency) so that

- k or more users can see the secret information by stacking their transparencies

- $k-1$ or less users gain no information

$\Longrightarrow$ k out of n Secret Sharing Scheme

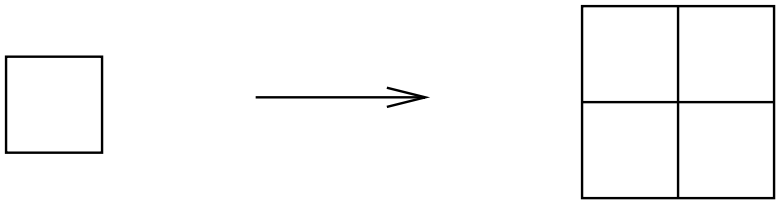
Assume that the message consists of a collection of black and white pixels

The Model

Each original pixel appears in n modified versions (called shares)
- one for each transparency

Each share is a collection of m black and white subpixels

For example: one pixel is divided into four subpixel

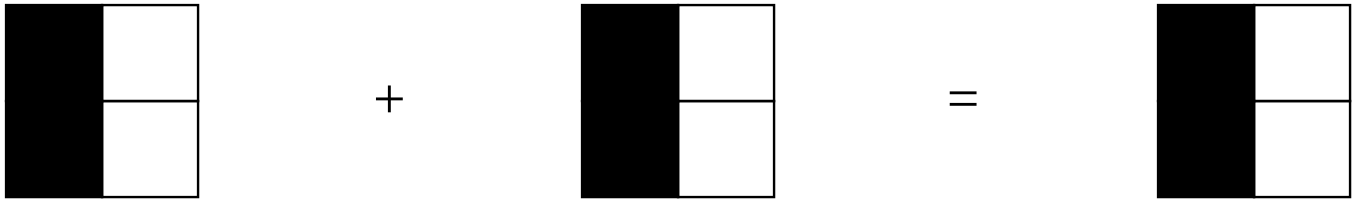


Obviously, m must be greater than one

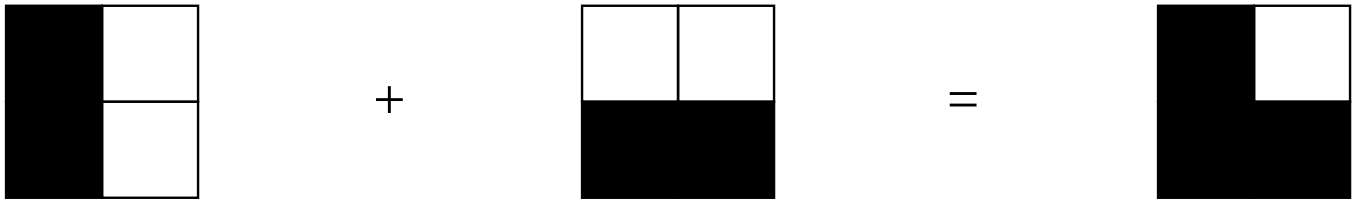
The Model

Stacking two pixels (each consists of four subpixels) can occur for example the following two cases:

1.



2.



The Model

- In the following we replace white with 0 and black with 1

- The resulting structure is a Boolean $n \times m$ matrix $M = [m_{ij}]$
  $m_{ij} = 1$ iff the jth subpixel in the ith transparency is black

- When transparencies are stacked together a combined share can be seen

- Black subpixels are represented by the Boolean OR of rows

- The grey level of this combined share is proportional to the Hamming weight $H(V)$ of the OR-ed vector V

- This grey level is interpreted by the visual system of the users
  as black if $H(V) \geq d$
  as white if $H(V) \leq d - \alpha m$
  for some fixed threshold $1 \leq d \leq m$ and relative contrast α

The Model

Definition 1 *A k out of n visual secret sharing scheme consists of two collections of Boolean $n \times m$ matrices C_0 and C_1. This scheme has threshold d and relative contrast α if the following three conditions are met*

(i) For any M in C_0 the Boolean OR V of any k of the n rows satisfies $H(V) \leq d - \alpha \cdot m$

(ii) For any M in C_1 the Boolean OR V of any k of the n rows satisfies $H(V) \geq d$

(iii) For any $j < k$ choosen rows the submatrices of the matrices from C_0 and C_1 occur with the same frequencies

How to Encrypt

For each pixel of the original do:

Choose randomly one of the matrices in

- C_0 if you want to share a white pixel
- C_1 if you want to share a black pixel

The choosen matrix defines the color of the m subpixels in each of the n transparencies

2 out of 2 Secret Sharing Scheme

The original is encrypted into 2 transparencies

You need both transparencies to decode the message

The 2 out of 2 Secret Sharing Scheme is given by

$$C_0 := \left[\text{all permutations of columns of } \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}\right]$$

$$C_1 := \left[\text{all permutations of columns of } \begin{pmatrix} 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \end{pmatrix}\right]$$

and the parameters $m = 4$, $\alpha = 1/2$ and $d = 4$

2 out of n Secret Sharing Scheme

The original is encrypted into n transparencies

You need any 2 (or more) of them to decode the message

The 2 out of n Secret Sharing Scheme is given by

$$C_0 := \left[\text{all permutations of columns of } \begin{pmatrix} 1 & 0 & 0 & \dots & 0 \\ 1 & 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 1 & 0 & 0 & \dots & 0 \end{pmatrix} \right]$$

$$C_1 := \left[\text{all permutations of columns of } \begin{pmatrix} 1 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix} \right]$$

and the parameters $m = n$, $\alpha = 1/n$ and $d = 2$

3 out of 3 Secret Sharing Scheme

The original is encrypted into 3 transparencies

You need all of them to decode the message

The 3 out of 3 Secret Sharing Scheme is given by

$$C_0 := \left[\text{all permutations of columns of } \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix} \right]$$

$$C_1 := \left[\text{all permutations of columns of } \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \end{pmatrix} \right]$$

and the parameters $m = 4$, $\alpha = 1/4$ and $d = 4$