Visual Cryptography

Kristin Burke

Overview

- Background
  - Papers
  - Secret sharing
- Visual Cryptography (VC)
- VC Examples
- Extensions
  - VC & Steganography
  - Visual Threshold Schemes

2

Background - Papers

- Visual Cryptography (1995) - Moni Naor & Adi Shamir
- Constructions and Bounds for Visual Cryptography(1996) - Ateniese, Blundo, et al.
- Visual Cryptography: Threshold Schemes and Information Hiding (1999?) - Xian, Heys, Robinson
- Extended Capabilities for Visual Cryptography (1999) - Ateniese, Blundo, et al.
- Doug Stinson's Visual Cryptography Page (http://cacr.math.uwaterloo.ca/~dstinson/visual.html)
- Visual Cryptography (http://www.dia.unisa.it/VISUAL/whatis.htmL)
- Visual Cryptography Kit (www-lce.eng.cam.ac.uk/~fms27/vck)

3

Background- Secret Sharing

- Divide data D into n shares
- D can be constructed from any k shares out of n
- Complete knowledge of k-1 shares reveals no information about D
- Written (k, n): k of n shares is necessary to reveal secret data

4

Background- Secret Sharing example

- 6 thieves share a bank account
  - They don't trust one another
  - They assume there will be no collusion between more than 2 of them
- The thieves split up the password for the account in such a way that:
  - Any 3 or more thieves working together can have access to account, but NOT < 3

5

Visual Cryptography

- For a set of n participants, a secret image S is encoded into n shadow images called shares
- Each participant gets one share
- k out of n participants are needed to combine shares and see secret image

6

VC- Example (2,2)

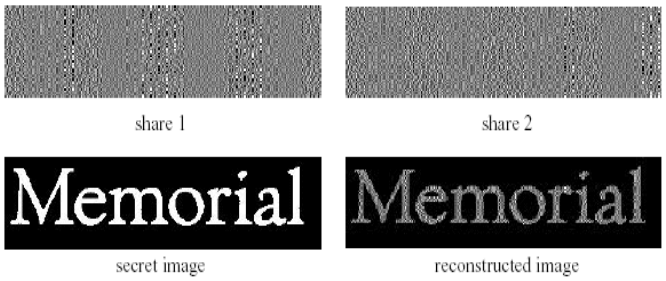


Figure 2. Implementation of a (2, 2) VTS

7

VC - Example (2,3)

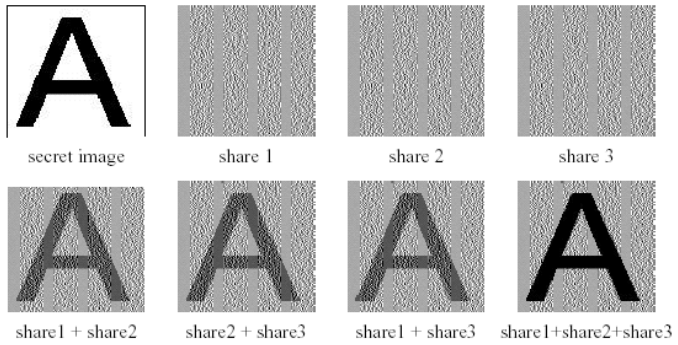
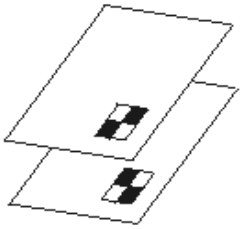


Figure 3. Implementation of a (2, 3) VTS

8

VC - How it works

- Every single pixel is split into subpixels
  - Human vision still perceives them as one pixel



The 2 out of 2 method uses: 2 foils, 1 pixel with 4 subpixels.

This overlay results in black, so the original pixel was also black.

9

http://www-fs.informatik.uni-tuebingen.de/~reinhard/krypto/Visual/Visual_Applet_e.html

VC - How it works (2)

- Information is stored in an m x n matrix S
- S[i,j] = 1 means subpixel j in foil i is black
- S[i,j] = 0 means subpixel j in foil i is white
- The overlay of the foils corresponds with the OR combinations of the m vectors in the matrix
- Grey level of the combined share is proportional to the Hamming weight H(V) of the “or”ed m-vector V

10

VC & Steganography

- Decreases probability of attacker detecting a cryptosystem
- Simple method: replace the Least Significant Bit of each pixel in an image with a bit of information from the secret
- More difficult: redefining standards of black and white and changing subpixel patterns

11

VC & S - Example

share 1 share 2 reconstructed secret

Figure 4. Conceal a secret with two innocent-looking shares

12

VC for insecure groups

- Only certain groups of members can be trusted
- Instead of having a (2,3) threshold, only certain groups of people can recover the secret message
- Groups of members are specified as qualified or forbidden

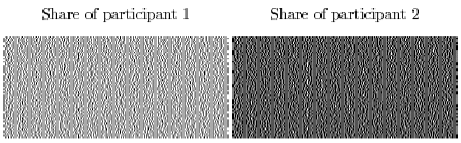
13

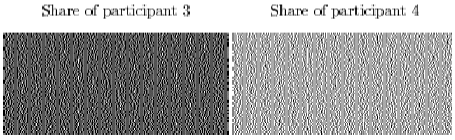
VC for Insecure groups

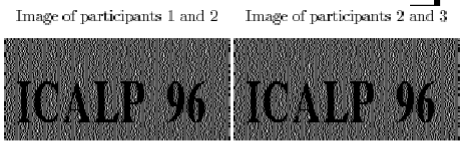
- Two properties:
  - Contrast
    - When qualified users stack their transparencies they can correctly recover the hidden message
  - Security
    - Even by inspecting all their shares, a forbidden set of participants cannot decide whether hidden image pixel should be white or black

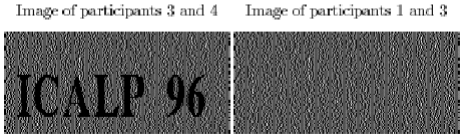
14

VC for Insecure Groups- Example





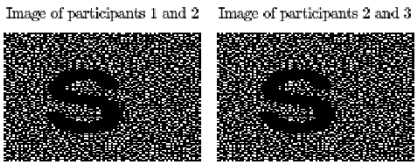


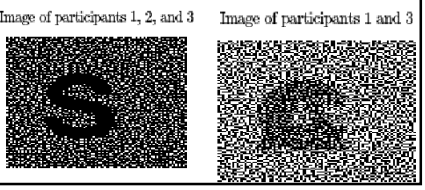


Legal groups: {{1,2}, {2,3}, {3,4}, {1,2,3}, {1,2,4}, {1,3,4}, {2,3,4}, {1,2,3,4}}

VC for Insecure Groups- Example(2)

Legal groups: {{1,2}, {2,3}, {1,2,3}}





Review

- Background
  - Papers
  - Secret sharing
- Visual Cryptography Overview
- Examples
- Extensions
  - VC and Steganography
  - VC for Insecure Groups

17

Questions?

18