Visual Cryptography

Christopher Grob

Übersicht

- Einleitung und Ziel
- Modell
- Effiziente Lösungen für kleine k und n
- (k,k) visual secret sharing problem
- (k,n) visual secret sharing problem (Idee)
- Erweiterungen des Modells

Einleitung und Ziel

- Geheimnis unter n Personen aufteilen
- Je k Personen können das Geheimnis entschlüsseln
- Weniger als k Personen können nichts über das Geheimnis erfahren
- Entschlüsselung erfolgt allein durch das menschliche Auge
- Technik anwendbar ohne Kenntnisse der Verschlüsselungstechnik

Modell

- Annahme: Nachricht besteht nur aus schwarzen und weißen Pixeln
- Jedes Pixel kommt in n modifizierten Versionen vor („shares“)
- Besteht aus m schwarzen und weißen Subpixeln
- n x m Boolean Matrix $S=[s_{ij}]$
- $S_{ij} = 1 \Rightarrow$ j-tes Subpixel im i-ten Transparenz ist schwarz
- Schwarze Subpixel werden von einem Boolean „oder“ der Zeilen dargestellt

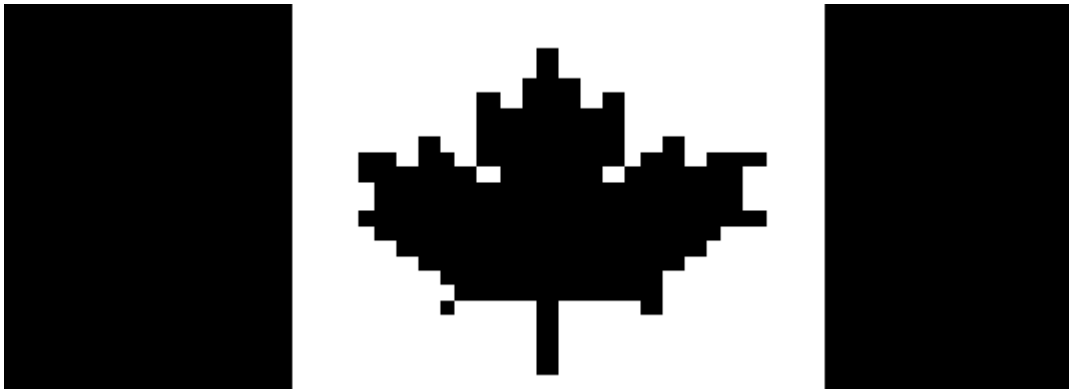
Modell

- Problem
  - Visueller Effekt eines schwarzen Subpixels kann von anderen Subpixeln nicht rückgängig gemacht werden
- Graue und schwarze Pixel
- Graustufe proportional zum „Hamming weight“ H(V), wobei V der „oder“ Vektor der Subpixel ist

Hamming weight H(V)
Anzahl der Symbole einer Zeichenkette V, die ungleich des Null-Symbols des benutzten Alphabets sind.
Alphabet: 0,1 Zeichenkette: 11101 Hamming weight: 4

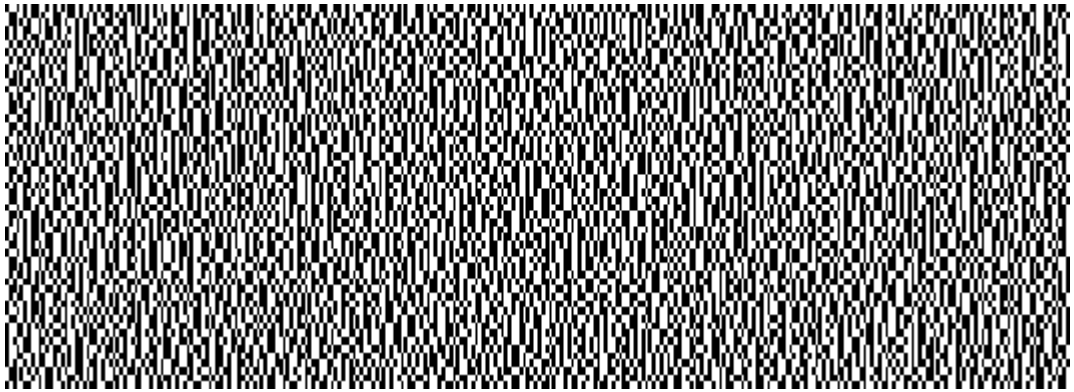
Modell

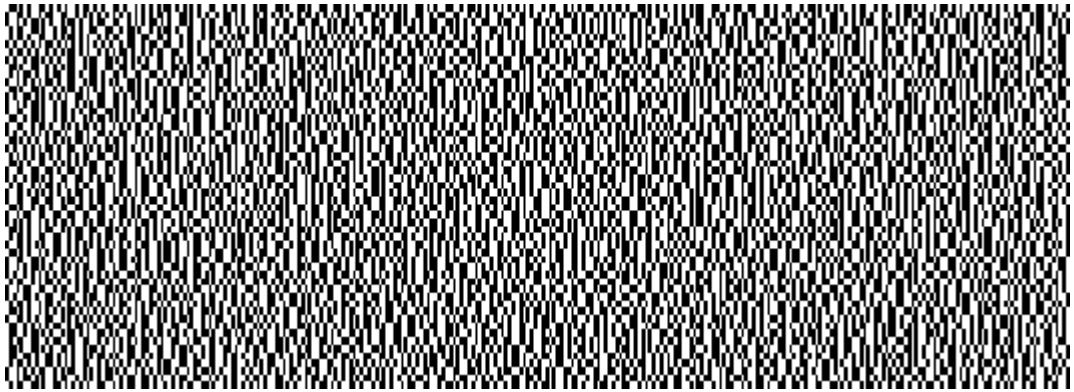
- Beispiel (von Doug Stinson)
  - Ursprüngliches Bild:



Modell

- Shares:





Modell

- Beide Shares übereinandergelegt:

Modell

- Wahrnehmung des menschlichen Auges
  - $H(V) \geq d$: schwarz
  - $H(V) \leq d - \alpha m$: weiß bzw. grau
    - Schwellenwert $1 \leq d \leq m$
    - Kontrastfaktor: $\alpha > 0$
    - Subpixelzahl m

Modell

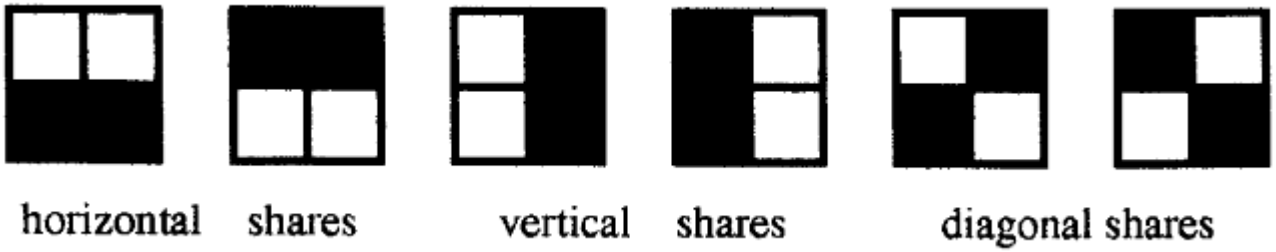
- Vorgehensweise bei der Verschlüsselung
  - Zwei Collections von n x m Boolean Matrizen C_0 und C_1
  - Weißes Pixel: Auswahl einer zufälligen Matrix aus C_0
  - Schwarzes Pixel: Auswahl einer zufällige Matrix aus C_1
  - Die gewählte Matrix definiert die Farbe der m Subpixel in jeder der n shares

Modell

- **Bedingungen**
- Kontrast:
  1. Für jede Matrix S aus C_0 erfüllen k von n Reihen die Bedingung: $H(V) \leq d - \alpha m$
  2. Für jede Matrix S aus C_1 erfüllen k von n Reihen die Bedingung: $H(V) \geq d$
- Sicherheit:
  3. Für jede Teilmenge $\{i_1, i_2, \ldots, i_q\}$ von $\{1,2,\ldots,n\}$ mit $q < k$ sind die beiden Collections von q x m Matrizen D_0 und D_1, die man erhält, wenn man jede n x m Matrix in C_0 und C_1 entsprechend kürzt ununterscheidbar.

Effiziente Lösungen für kleines k und n

- **(2,2) visual secret sharing problem**
- Ein weißes Pixel erhält man, indem man zwei identische Pixel übereinanderlegt
- Ein schwarzes Pixel, indem man zwei Komplementäre übereinanderlegt



Effiziente Lösungen für kleines k und n

- **(2,n) visual secret sharing problem**
  - $C_0 =$ { Alle Matrizen, die man durch Permutation folgender Reihen erhält } $\begin{bmatrix} 100\ldots0 \\ 100\ldots0 \\ \ldots \\ 100\ldots0 \end{bmatrix}$
  - $C_1 =$ { Alle Matrizen, die man durch Permutation folgender Reihen erhält } $\begin{bmatrix} 100\ldots0 \\ 010\ldots0 \\ \ldots \\ 000\ldots1 \end{bmatrix}$

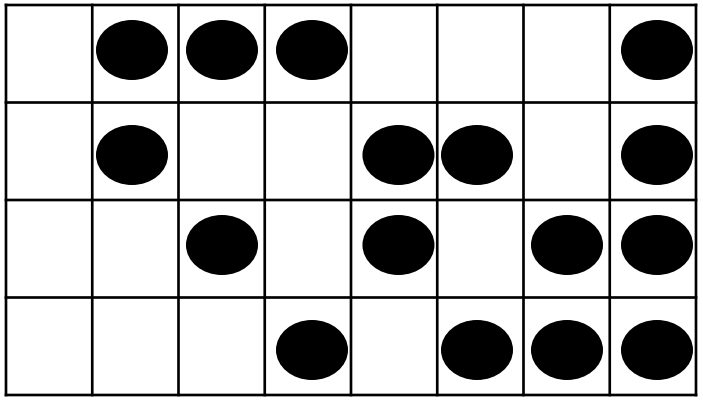
Effiziente Lösungen für kleines k und n

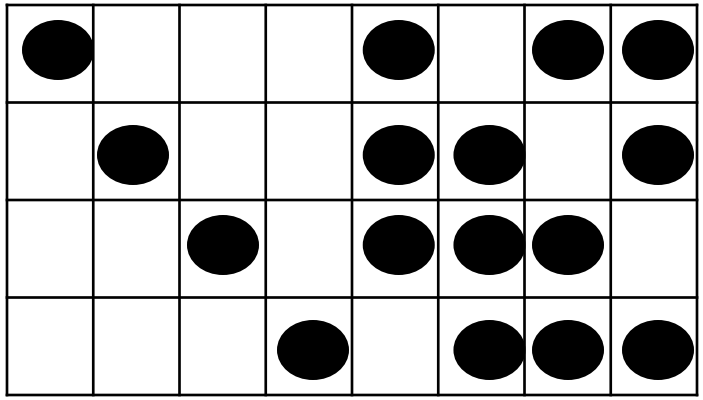
- **(3,3) visual secret sharing problem**
  - $C_0 = \left\{ \begin{bmatrix} 0011 \\ 0101 \\ 0110 \end{bmatrix} \right.$

  - $C_1 = \left\{ \begin{bmatrix} 1100 \\ 1010 \\ 1001 \end{bmatrix} \right.$

(k,k) visual secret sharing problem

- Konstruktion
  - Matrizen sind aus allen möglichen k-zeiligen Spaltenvektoren zusammengesetzt
  - Spalten, bei denen H(V) gerade oder null ist -> C_0
  - Spalten, bei denen H(V) ungerade ist -> C_1
  - $d = m = 2^{k-1}$, $\alpha = 2^{-(k-1)}$





Und alle Permutationen der Spalten!

(k,k) visual secret sharing problem

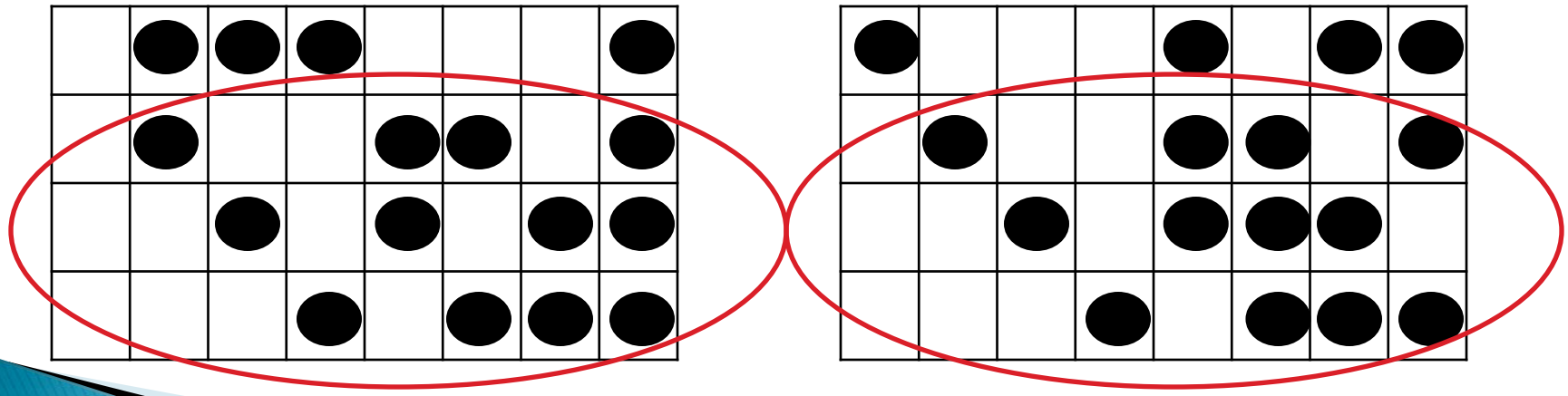
- Überprüfen der Bedingungen
  - Kontrast
    - Für jede Matrix S aus C_0 erfüllen k von n Reihen die Bedingung: $H(V) \leq d - \alpha m$
    - Für jede Matrix S aus C_1 erfüllen k von n Reihen die Bedingung: $H(V) \geq d$

Beispiel k=4
$m = d = 2^3 = 8$
$\alpha = 1/8$
C_0: $H(V) = 7$
C_1: $H(V) = 8$

- In C_0 ex. genau eine Spalte ohne schwarze Einträge!

(k,k) visual secret sharing problem

- Überprüfen der Bedingungen
  - Sicherheit
    - Für jede Teilmenge $\{i_1, i_2, \ldots, i_q\}$ von $\{1,2,\ldots,n\}$ mit $q < k$ sind die beiden Collections von q x m Matrizen D_0 und D_1, die man erhält, wenn man jede n x m Matrix in C_0 und C_1 entsprechend kürzt ununterscheidbar.
      - Jede Spalte tritt 2^{k-q} mal gleichverteilt in beiden auf

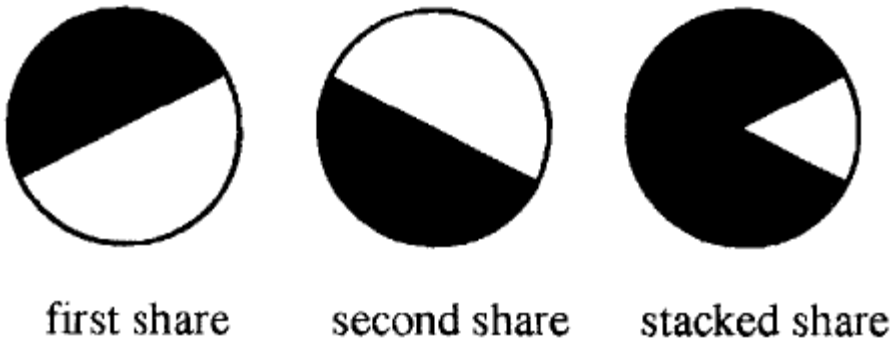


(k,n) visual secret sharing problem

- Idee
  - Grundlage: (k,k) Modell
  - Matrizen auf n Zeilen erweitern durch Hashfunktionen H_i
  - Die neuen Matrizen entstehen aus allen möglichen Kombinationen der alten Matrizen

Erweiterungen

- Nachrichten in Bildern verstecken
  - Verschleiern, dass überhaupt eine geheime Nachricht existiert
- Graustufen durch kreisförmige Pixel



Erweiterungen

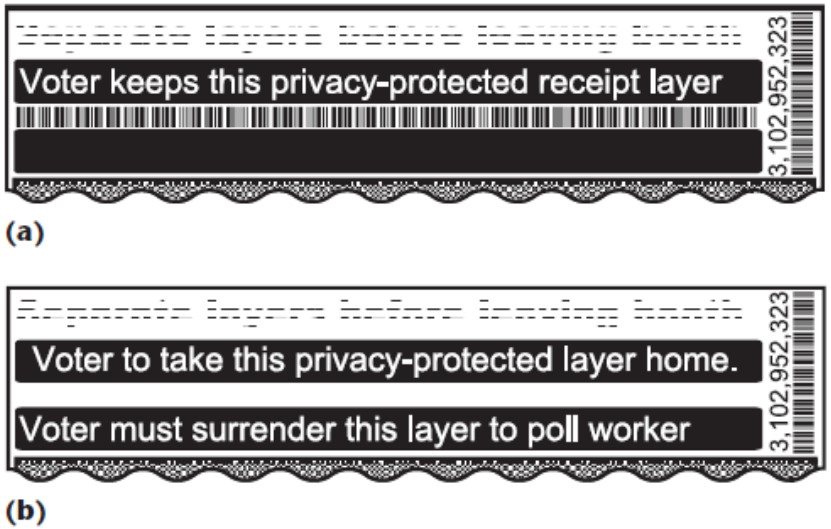
- Farbige Folien
- Verbesserung von Kontrast/Minimierung der Größe der Shares
- Anwendung zum Thema E-voting: David Chaum

E-Voting

- Wahlmaschinen geben keinen Beleg
- proprietäre „Black Box“ Technologie
- Open-source Anwendung für jeden Standard PC
- Ausdruck:

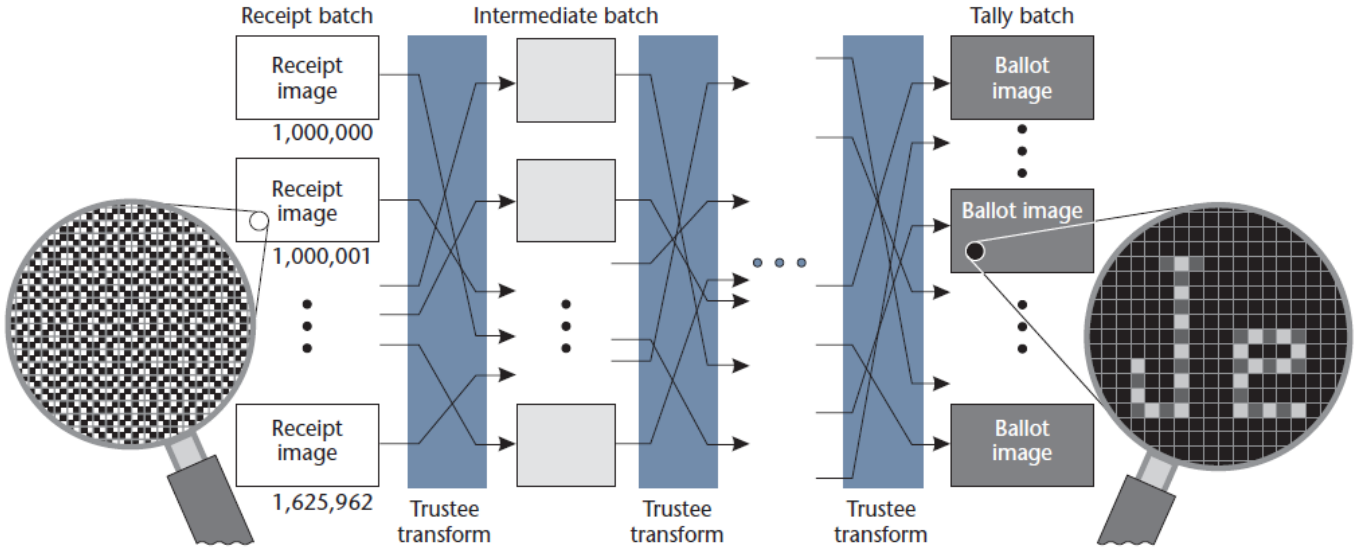
E-Voting

- Besteht aus zwei Folien
- Wähler entscheidet ob er obere oder untere Folie behält



E-Voting

- Nicht gewählte Folie wird vernichtet
- Public-key encryption
- Entschlüsselung durch mehrere vertrauenswürdige Institutionen



E-Voting

- Annahme: Alle Wahlcomputer sind kompromittiert
- Mögliche Betrugsmöglichkeiten:
  - Eine Folie fehlerhaft drucken und darauf hoffen, dass der Wähler die Andere wählt
  - Selbe Seriennummer für zwei Belege wählen und hoffen, dass beide Wähler die selbe Folie nehmen
  - Den Zählprozess nicht korrekt ausführen
- Wahrscheinlichkeit, dass der Betrugsversuch entdeckt wird ist jeweils 50%
- Nicht alle Wähler überprüfen ihre Belege
  - 100 Stimmen wurden geändert
  - Nur 5 % überprüfen ihre Belege
  - Chance, das der Betrugsversuch nicht entdeckt wird: 1: 1000

Quellen

- M. Naor and A. Shamir: Visual Cryptography
- Nicolai Hähnle: Visuelles Secret Sharing
  - http://homepages.uni-paderborn.de/prefect/cs/vss-vortrag.pdf
- Matthias Baumgart: Visual Cryptography
  - http://www14.informatik.tu-muenchen.de/personen/baumgart/download/public/vc.pdf
- Doug Stinson's Visual Cryptography Page
  - http://www.cacr.math.uwaterloo.ca/~dstinson/visual.html
- Secret-Ballot Receipts: True Voter-Verifiable Elections
  - http://courses.csail.mit.edu/6.897/spring04/Chaum-SecretBallotReceiptsTrueVoterVerifiableElections.pdf