

Visuelle Kryptographie

23. April 2009

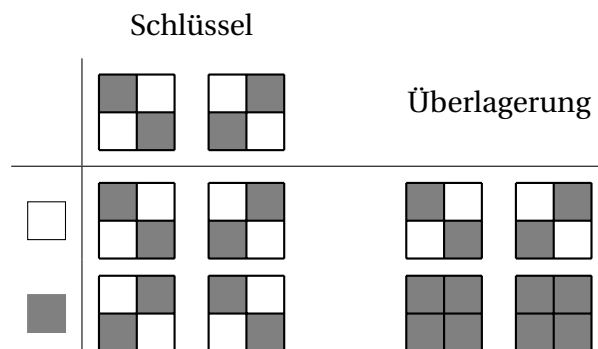
Verschlüsselung im Allgemeinen

1. Verschlüsselung: Aus *Klartext* und *Schlüssel* entsteht das *Chifftrat*.
2. Entschlüsselung: Aus *Chifftrat* und *Schlüssel* entsteht der *Klartext*.

Besonderheiten bei der visuellen Verschlüsselung

1. Klartext, Schlüssel und Chifftrat sind Bilder auf Folien. Ein Bild ist ein Pixel-raster.
2. Beim Verschlüsseln wird aus jedem Klartext-Pixel ein 2×2 -*Superpixel*. Die einzelnen Pixel eines Superpixels werden *Subpixel* genannt.
3. Das Entschlüsseln geschieht durch *Überlagerung* der beiden Folien (Chifftrat und Schlüssel). Schwarz + Schwarz = Schwarz.
4. Beim Entschlüsseln entsteht der Klartext nur mit *verringertem (halbem) Kon-
trast*, aber eindeutig erkennbar und rekonstruierbar.

Verschlüsselungstransformation für ein Pixel



Visual secret sharing schemes

Gegeben: Bild B , das so genannte *Geheimnis*, Zahlen k und n mit $k < n$

Gesucht: Bilder S_1, S_1, \dots, S_n , die so genannten *Anteile (shares)*, so dass gilt:

- Die Überlagerung von höchstens k Anteilen liefert ein Bild, das keine Information über das Geheimnis enthält.
- Die Überlagerung von mindestens $k + 1$ Anteilen bringt das Geheimnis zum Vorschein.

Vorgehensweise wie bei der visuellen Verschlüsselung (Pixel durch Superpixel ersetzen). Problem: Sehr große Anzahl von Subpixeln mitunter nötig.

Magische Überlagerungen

Die Anteile sollen vorgegebenen Bildern entsprechen. Pixel werden durch Superpixel ersetzt.

Software zum Experimentieren

Programm (Java-Archiv) unter

<http://www.ti.informatik.uni-kiel.de/wp-content/uploads/viso.jar>

Programmstart durch Klicken unter Windows (evtl. nach vorheriger Installation von Java) und durch

```
java -jar viso.jar
```

unter Linux.

Literatur

1. Lehrbuch:

Andreas Klein, *Visuelle Kryptographie*, Springer: Berlin, 2007.

2. Originalartikel:

Moni Naor, Adi Shamir, Visual Cryptography, in Alfredo de Santis, Advances in Cryptology – EUROCRYPT '94, Workshop on the Theory and Application of Cryptographic Techniques, Perugia, Italy, 1994, Lecture Notes in Computer Science, Band 950, Springer, 1995, Seiten 1 – 12.