

Complete Codings for Visual Cryptography

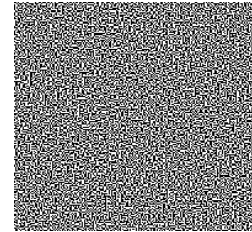


M.Sc. IT-Security Denise Doberitz
Denise.Doberitz@rub.de

Visual Cryptography - The Basic Principle

Generate Key:

Generate a key-transparency with random pixels with the size of the image to be encrypted.



Encryption:

Compute ciphertext-transparency:

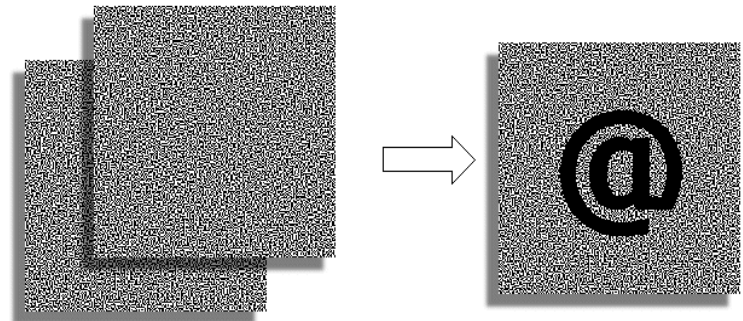
white pixel: copy pixel from the key-transparency

black pixel: compute inverse pixel of the key-transparency



Decryption:

Overlay the transparencies
(corresponds to a virtual OR-function)



Visual Cryptography - Problems

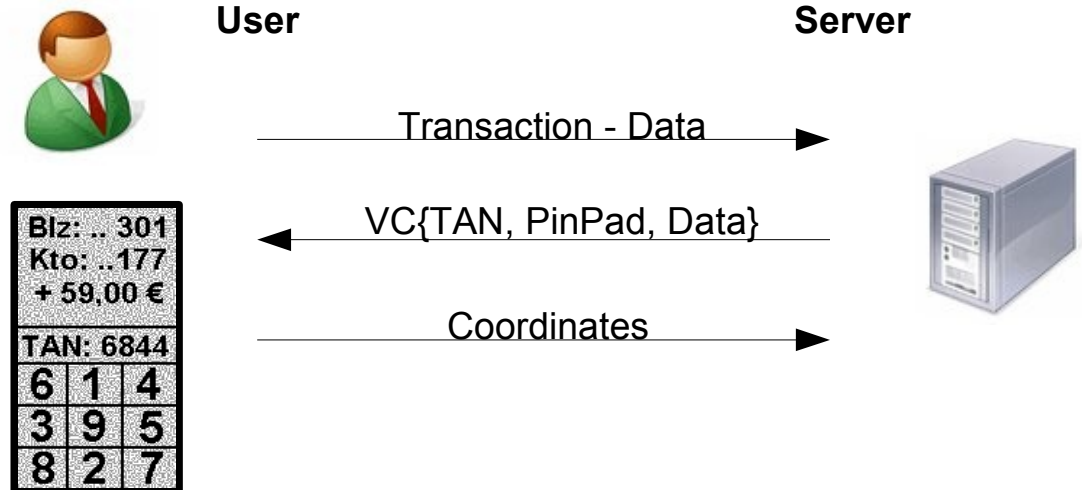
Alignment:

Must be precise to 1 pixel => difficult to handle

Reuse of key-transparencies:

Only secure as one-time pad

=> Key-transparencies can not be used more than once



Codings - Definition

Def. Coding:

Let I be the set of all information and S the set of all possible symbols $S = \{0, 1\}^n$ then a coding C has the following properties:

- $C: I \rightarrow S$

the coding maps an information $i \in I$ to a symbol $s \in S$.

- $C(i_1 \dots i_n) = C(i_1) \dots C(i_n) \forall i_j \in I \text{ and } j = \{1 \dots n\}$

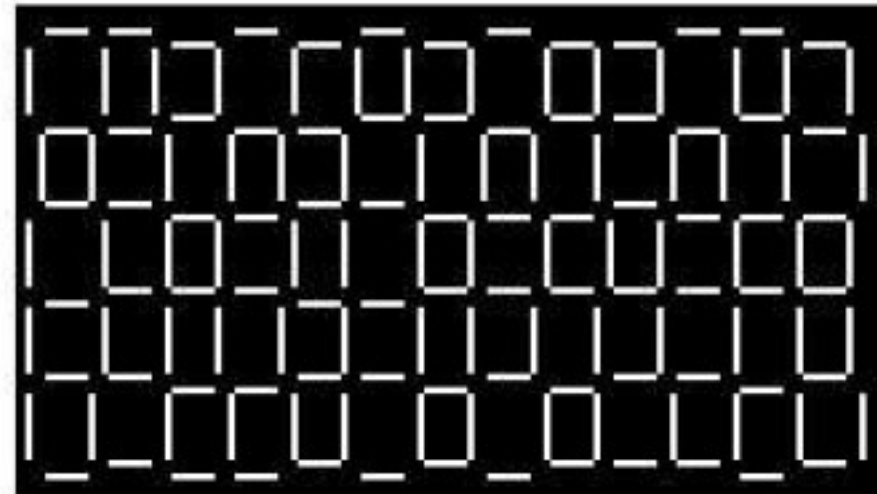
the coding must be homomorphic, in order to provide a coding for words, that are composed by letters.

Codings - Segment Based VC (Borchert)

Segment based Alphabet:

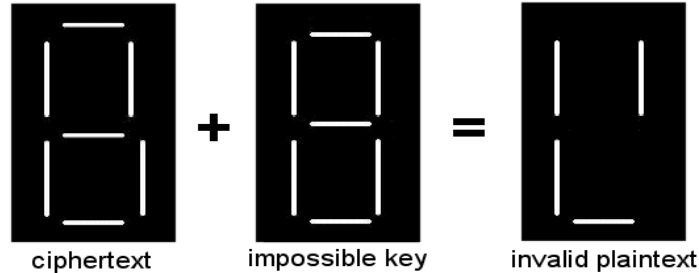


Segment based Ciphertext:



Codings - Segment Based VC (Borchert)

Attack on multiple used segments:



=> **Requirement:**

A coding, where all possible combinations of the elements of the coding can be used as valid symbols.

=> **Complete Codings**

Complete Codings - Definition

Def. Complete Coding:

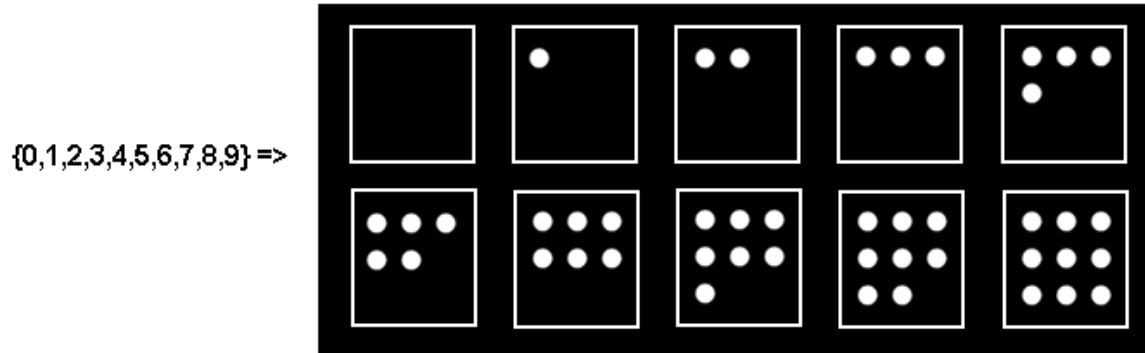
1. Let S be a set $S = \{0, 1\}^n$ of symbols.
2. A symbol $s = (s_1, \dots, s_n) \in S$ is composed of n visual elements, whereas 1 denotes, that the element is visible and 0 denotes, that the element is not visible.
3. With the help of a visualization mapping function D , that maps every possible symbol to an information, the complete set S can be used as an alphabet A .
4. The alphabet A must be sufficient to represent the required information $i \in I$ (syntactic).
5. The information is represented in a way, that can be interpreted by the user (semantic).

This includes

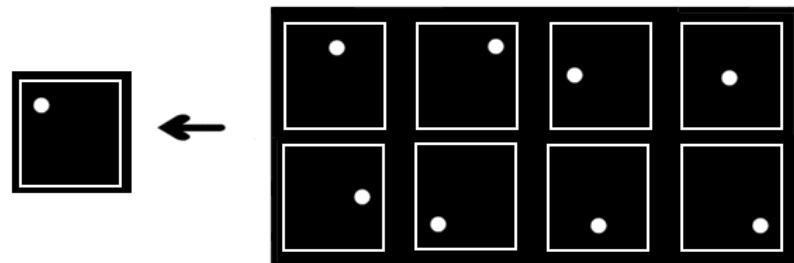
- The user has the visual ability to recognize the symbols.
- The user has the knowledge how to interpret the symbols.

Example: Dice Coding

Numbers in Dice Coding:

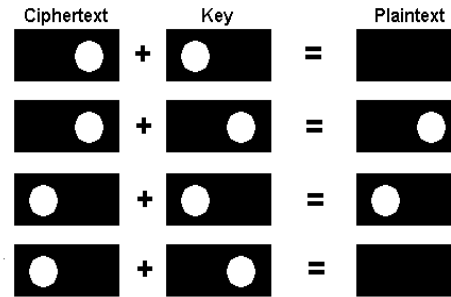


Mapping function:

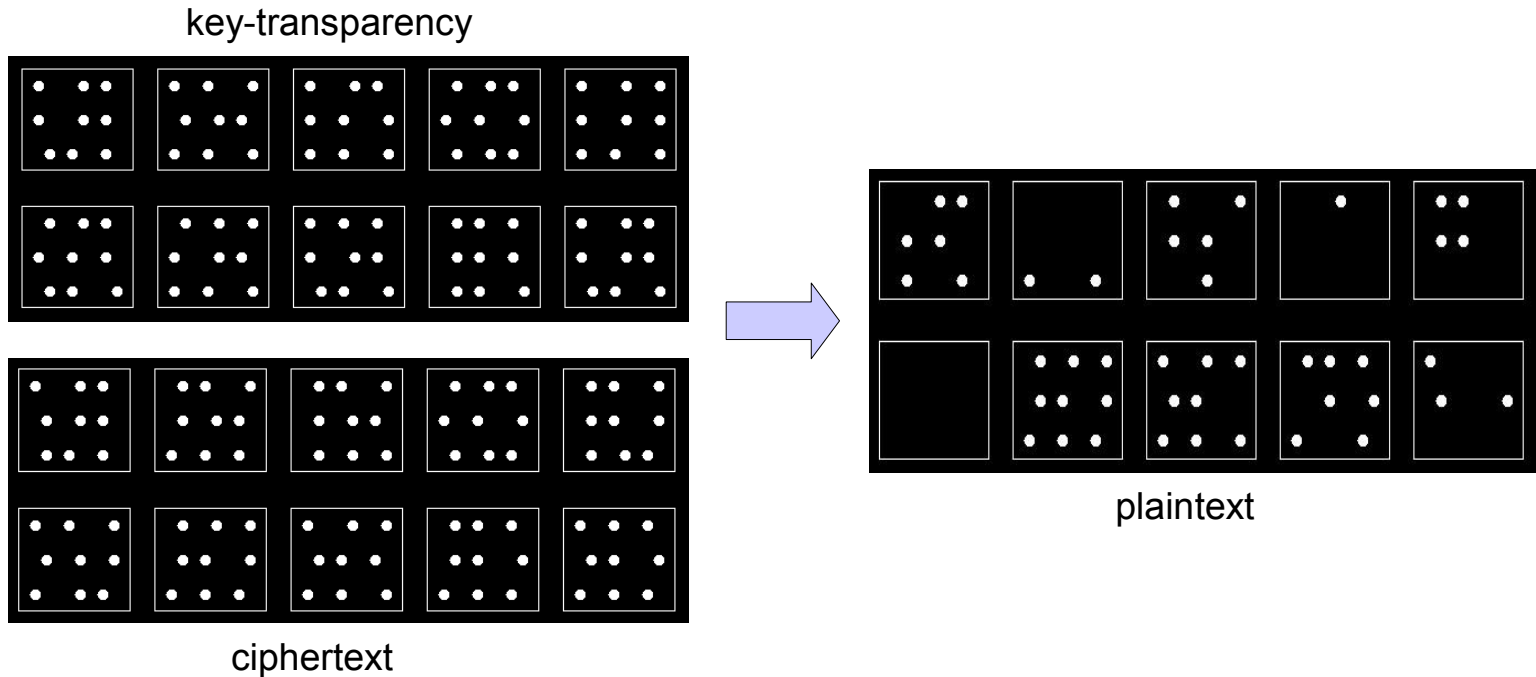


Example: Visual Cryptography with Dice Coding

Encryption of a point:



Decryption:



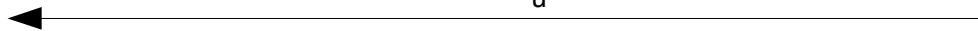
Example: TAN submission with Dice Coding

Client
(K_u , TAN)

Server
(K_u , TAN)

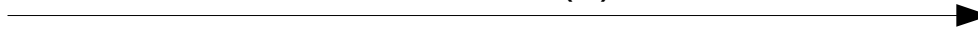
$\sigma \in R \Sigma$
 $\sigma_u \leftarrow \text{Encrypt}(\sigma, K_u)$

σ_u



$\sigma \leftarrow \text{Decrypt}(\sigma_u, K_u)$
TAN = c
 $\text{select}(c) \leftarrow \text{Select}(c, \sigma)$

$\text{select}(c)$



$c' \leftarrow \text{Extract}(\text{select}(c), \sigma)$
verify: $c = \text{TAN} ?$

Thank you for your attention!



M.Sc. IT-Security Denise Doberitz
Denise.Doberitz@rub.de

References

[1] Naor M. and Shamir A., *Visual Cryptography*, Eurocrypt '94, Springer-Verlag LNCS Vol. 950, Springer-Verlag, 1995, 1-12.

[2] Denise Doberitz and Sebastian Gajek. *Visual Cryptography - an approach to secure online banking*. 7. Kryptotag, November 2007.

[3] B. Borchert. *Segment-based visual cryptography*. WSI, April 2007.