A Primer on Visual Cryptography

Sergio A. Figueroa, Suela Kodra & César Pereida G.

Printed perfect secrecy

★ **Perfect secrecy** is an essential concept in cryptography: given an encrypted message, but not the key, every plaintext is possible.
- It is **not practical**: the key must be **as long as the message** and **cannot be reused**.

sendmoremoney
zeokjomsxzpmh
cashnotneeded

One Time Pad: each letter is rotated a different amount of times (the key). Different keys can produce totally oposite results with equal likelihood.

Key for "sendmoremoney": (9; 0; 7; 23; 15; 21; 14; 11; 11; 2; 8; 9)

Key for "cashnotneeded": (22; 4; 4; 1; 4; 0; 7; 21; 19; 21; 12; 8; 4)

Extended Visual Cryptography Scheme (EVCS)

★ **Access structure (Γ_{Qual} ,Γ_{Forb})** Given a set of *n* participants only a set $X \in \Gamma_{Qual}$ is able to retrieve the secret message. Any set $Y \in \Gamma_{Forb}$ does not have any information about the secret.
- No **cryptographic knowledge** nor **computation** is needed to recover the secret by Γ_{Qual} .
- EVCS achieves **unconditional security.** Any forbidden set cannot gain information even with infinite computational power.
- Original messages are **meaningful,** users can identify their share

Share of participant 1 | Share of participant 2 | Share of participant 3

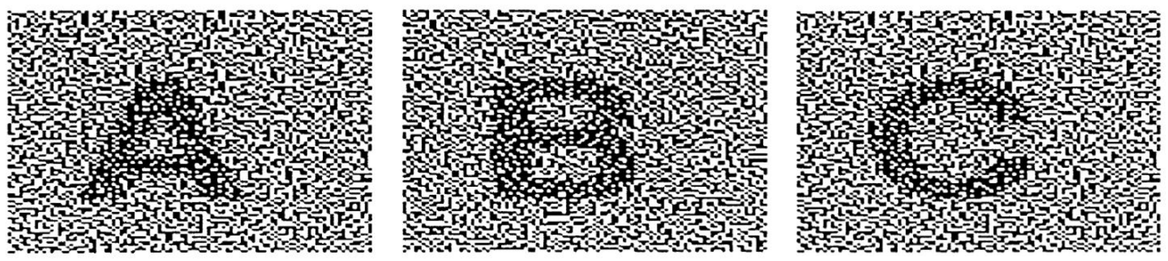
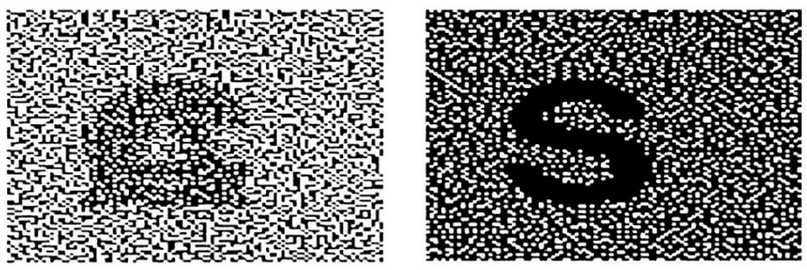


Image of participants 1 and 3 | Image of participants 1, 2, and 3



Some applications

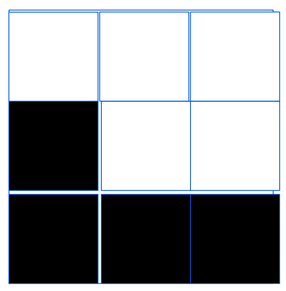
★ **Internet Voting**
- The **secret image** is divided into 2 shares.
- The administrator (*Election authority*) sends **share 1** to the e-mail of the voter before the election. **Share 2** will be available in the voting system for his login during election.
- The voter logs in and casts his vote by entering the correct password revealed by **overlapping the shares**.

Visual Cryptography

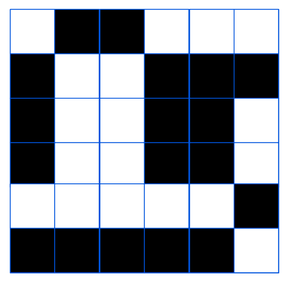
★ In 1994, Adi Shamir proposed a way to achieve **perfect secrecy for printed documents** in a practical way.
- It relies on the skills of the human brain for detecting patterns, but is subject to practical usability limitations.
- **Pixel expansion** - number of sub-pixels each pixel is encoded.
- **Contrast** is the difference of pixels in the reconstructed image.

Naor and Shamir VCS (Two Halves Version)

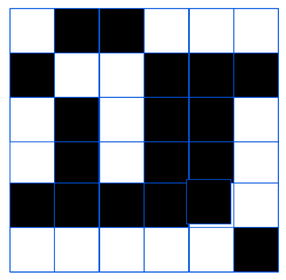
Step 1: take a black and white bitmap. That is the **message.**



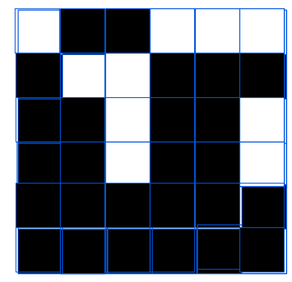
Step 2: create a grid twice as long and twice as high as the message. For each 2x2 square, mark two of the squares as black *randomly*. That is the **key.**



Step 3: create a second grid of the size of the key. If a pixel in the message is *white*, color the same pattern as in the key. If it is *black*, color the complementary pattern. That is the **ciphertext**.



Step 4: overlap the key and the ciphertext (note that, for one of them, white pixels must be transparent). The message loses quality, but is readable.



★ **Online Payment System**
- The **password** of the customer is hidden inside a cover text through a steganographic process and the account number is placed above this text.
- A snapshot is taken and the **shares** are produced. One of these shares is taken by the customer and the other is saved in the database of the certification.
- During the payment process, the shopper sends his own share and the merchant submits his own account details to CA, which combines his share with the one of the customer, to get the **original image** which contains the password and other details.
- The information is sent to the bank to validate the transaction.

★ **Anti-Phishing Framework**
- The client can ensure if the web site is genuine or not, by typing his user name. The server **sends a share** from its database. The client will **superimpose** his own share with the one sent by the site to ensure this is not a phishing page and type his information.

[1] *Naor, M. and A. Shamir.* **Visual cryptography, Advances in cryptology.** Eurocrypt '94 Proceeding LNCS, 950:1–12, 1995.
[2] *Giuseppe Ateniese, Carlo Blundo, Alfredo De Santis, Douglas R. Stinson*. **Extended capabilities for visual cryptography**, Theoretical Computer Science, Volume 250, Issues 1–2, 6 January 2001.
[3] *Mr. K. A. Aravind1, Mr. R .Muthu Venkata Krishnan*, **Anti-Phishing Framework for Banking Based on Visual Cryptography**, International Journal of Computer Science and Mobile Applications, Vol.2 Issue. 1, January-2014.
[4] *Souvik Roy, P.Venkateswaran*, **Online Payment System using Steganography and Visual Cryptography**, 'Proceedings of IEEE Students' Conference on Electrical, Electronics and Computer Science,2014.
[5] *Rajendra A B and Sheshadri H S*, **Visual Cryptography in Internet Voting system**, IEEE, 2013.

TARTU ÜLIKOOL · UNIVERSITAS TARTUENSIS · 1632

NordSecMob
Master's Programme in Security and Mobile Computing