Segment-based Visual Cryptography

Bernd Borchert

WSI-2007-04

Universität Tübingen
Wilhelm-Schickard-Institut für Informatik
Arbeitsbereich Theoretische Informatik/Formale Sprachen
Sand 13
D-72076 Tübingen

borchert@informatik.uni-tuebingen.de

ISSN 0946-3852

Segment-based Visual Cryptography

Bernd Borchert

Universität Tübingen, Sand 13, 72076 Tübingen, Germany

borchert@informatik.uni-tuebingen.de

Abstract

A version of Visual Cryptography is presented which is not pixel-based but segment-based. It is used to encrypt messages consisting of symbols which can be represented by a segment display. For example, the decimal digits $0, \ldots, 9$ can be represented by the well-known seven-segment display. The advantage of the segment-based encryption is that it may be easier to adjust the secret images and that the symbols are potentially easier to recognize for the human eye, especially in a transparency-on-screen szenario.

1 Introduction

Visual Cryptography was introduced 1994 by Naor and Shamir [NS94]. In its basic version it represents a 2-out-of-2 secret sharing system: From a given black-and-white picture P two pictures P1 and P2 are produced. Both P1 and P2 are random, i.e. they show black and white pixels which are randomly distributed, i.e. both P1 and P2 do not show any information. But when P1 and P2 are overlayed then they show the original picture P, with a 50 percent loss of contrast, see Figure 1.

As a perfect 2-out-of-2 secret sharting system Visual Cryptography has the encryption power of the onetime-pad: given say P1, the original information P cannot be obtained without knowing P2: even large computational ressources would not help. In other words: an encryption system based on Visual Cryptography is unbreakable.

Several extension and modifications of Visual Cryptography have been introduced: in the original paper the idea is already generalized from a 2-out-of-2 secret sharing system to an m-out-of-n secret

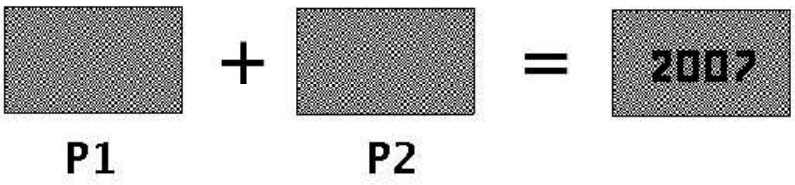


Figure 1: Visual Cryptography

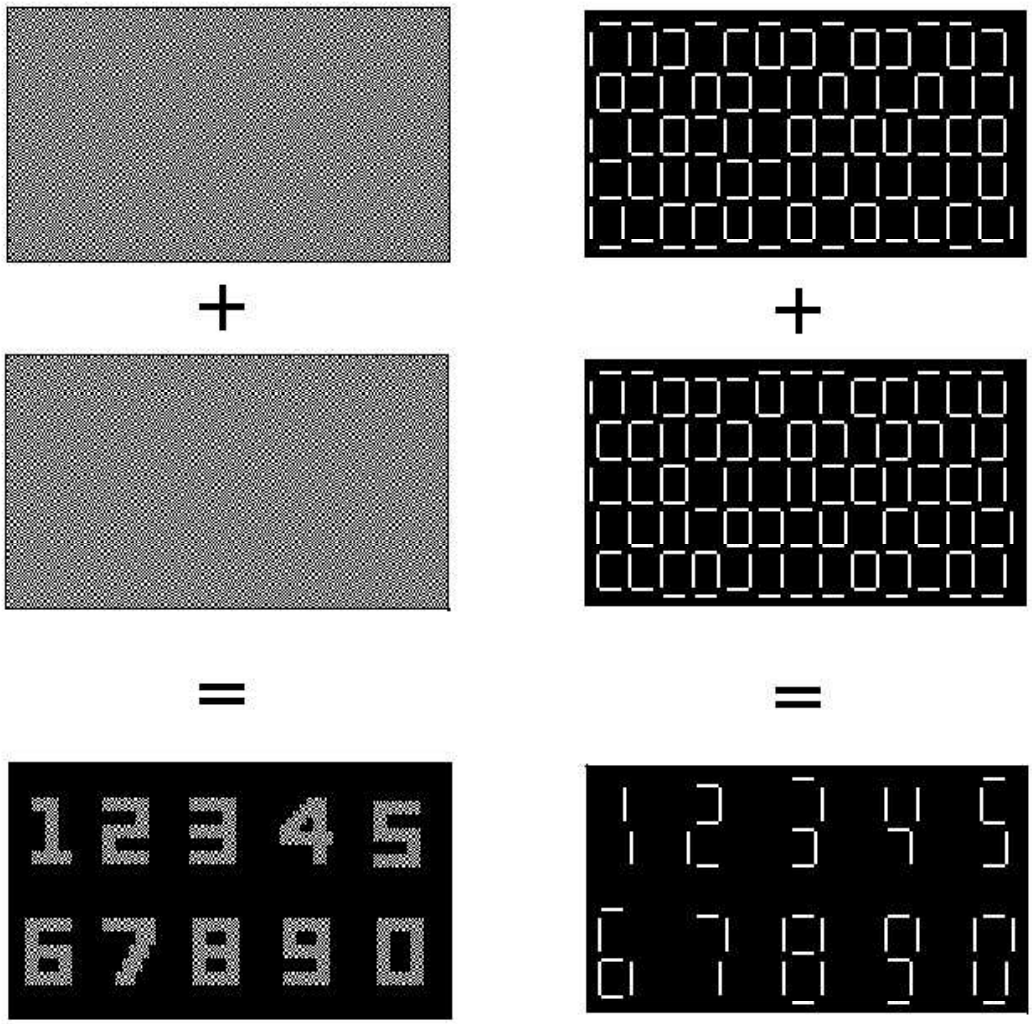


Figure 2: Pixel-based (left) versus segment-based (right) Visual Cryptography

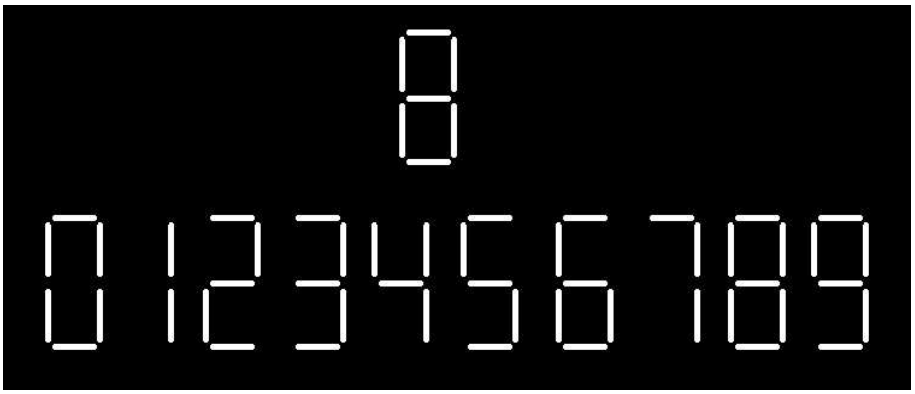


Figure 3: The seven-segment display

sharing system, for any $m \leq n$. Some modifications suggest to add the feature of steganography to Visual Cryptography, others try to go from black-and-white pictures to color pictures. See the book [Kl07] for a recent survey on Visual Cryptography and its variations.

This short note describes another variation of Visual Cryptography: instead of taking pixels as the smallest unit to be encrypted segments of a segment display are encrypted. The typical segment display is the seven-segment display, see Figure 3, it is used to represent the digits $0, 1, 2, 3, 4, 5, 6, 7, 8, 9$ (and possibly the hexadecimal digits A, b, c, d, E, F).

The suggested segment-based Visual Cryptography can be used to encode messages consisting of symbols displayable by a segment display. For example, messages consisting only of numbers can be encoded this way via segment-based Visual Cryptography using the seven segment display. An example for such a message is the information describing a money transfer (including account number, bank number and money amount) during an online banking session, see Figure 6.

The potential advantages of the segment-based Visual Cryptography as compared to pixel-based Visual Cryptography are the following:

1. It may be easier to adjust the two shares, especially in the case of a transparency-on-screen szenario,
2. it may be easier for the human eye to recognize the symbols, especially in the case of a transparency-on-screen szenario,
3. less random bits are needed, this may be an advantage if real randomness (not pseudo-randomness) is used in an encryption system,
4. it may be easier for a non-expert human user of an encryption system to understand – and therefore trust – segment-based Visual Cryptography than pixel-based Visual Cryptography.

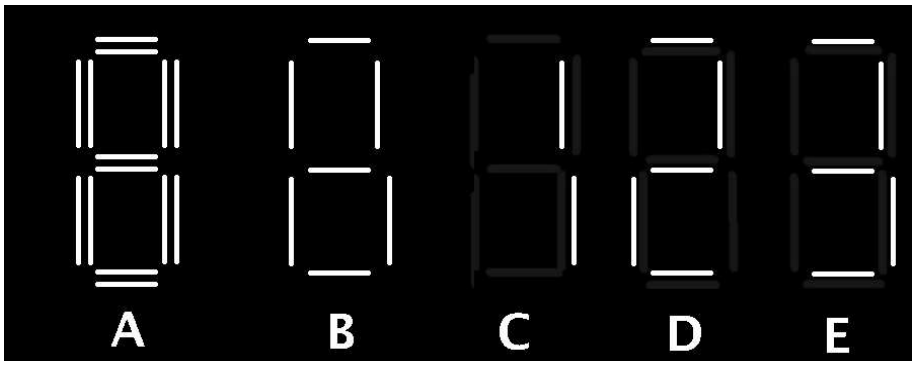


Figure 4: The principle applied to the seven-segment display

2 Segment-based Visual Cryptography

The seven-segment display was invented 1908 [Wo08]. It uses seven bars, three of them horizontal and four vertical, arranged like an 8, see top of Figure 3. By highlighting a certain selected subsets of the seven segments every digit 0,...,9 can be represented, see bottom part of Figure 3.

Let some segment display be given being able to display a certain set of symbols, for example the seven-segment display which is able to display the set of digits 0,...,9. The principle of Visual Cryptography is applied to the segment display: For every segment S draw – in white on black background – two parallel segments S1 and S2 which are close to each other but do not intersect. See for example part A of Figure 4 where this is applied to a seven-segment display.

Like in pixel-based Visual Cryptography first a random share is produced. This means in the case of segments that from every pair of parallel segments S1 and S2 one is selected randomly. This segment is kept white (=transparent), while the other parallel segement is turned black – like the backgorund of the share. Such a random selection is shown in part B of Figure 4.

Now the second share is produced. Assume that a certain symbol is to be shown. Consider the subset of segments of the segment display which are to be highlighted in order to show this symbol.

- If a segment S belongs to this subset, then in the second share the same selection S1 or S2 is made like in the random share and highlighted, and the other parallel segment is turned black. This has the effect that – in the case of overlaying – the two overlayed shares show a white (resp. transparent) segment.
- If on the other hand S does not belong to this subset, then in the second share the other segment of the two parallel segments S1 or S2 is highlighted, and the segment chosen on the random share (share 1) is turned black. This has the effect that in the case of overlaying the two shares this segment does not show a white (resp. transparent) area.

In total, exactly the segments belonging to the subset A show transparent areas when the two shares are overlayed. Therefore, after overlaying, the symbol to be shown appears to the eye of the beholder. For example, in Part C of Figure 4 the second share is chosen in that way that exactly the set of segments which are needed to show the digit 1 on the display, show transparent segments, in other

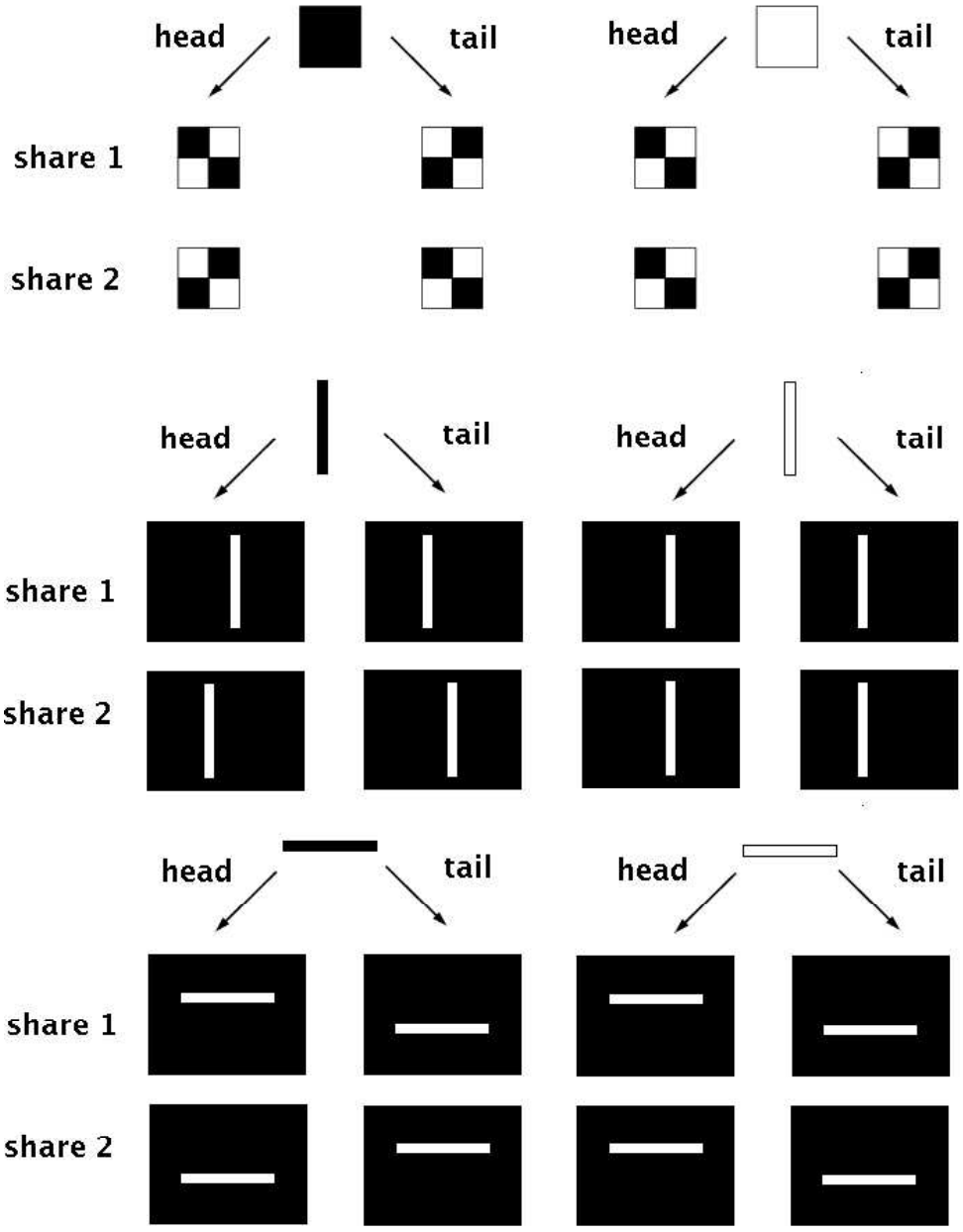


Figure 5: Pixel-based (above) vs. segment-based (center and below) Visual Cryptography

words, the beholder will see the digit 1. In Part D and E of Figure 4 the second share is chosen in that way, that the digit 2 resp. the digit 3 are shown to the beholder. Note that the first share (shown in Part B) is always the same for Part C, D, and also E.

The principle described above is also shown in Figure 5 in the center and below. You can compare this with the principle of pixel-based Visual Cryptography which is shown on top in that figure.

Of course the first share is random, i.e. does not disclosure any information, especially not any information of the coded message. With the same argumentation like for pixel-based Visual Cryptography it holds that the second share is also random: for each segment S the probability for chosing S1 is 1/2, independent of the other segments. So it is random, too.

Of course, segment-based Visual Cryptography can also be applied to sets of symbols being representable by another kind of segment display, for example there is a well-known fourteen-segement display which is able to represent all letters and digits.

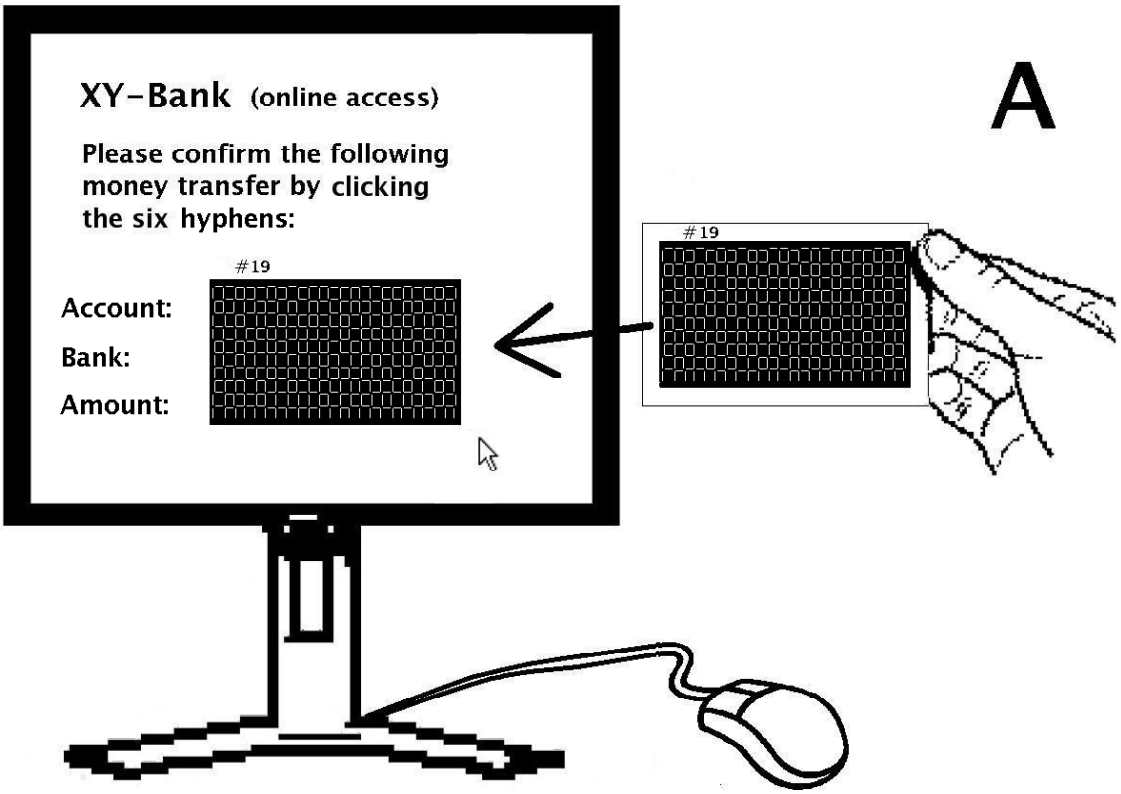
Potential advantages of segment-based Visual Cryptography as compared to pixel-based Visual Cryptography are listed at the end of the Introduction.

3 An Application to Online Banking Security

Figure 6 shows an application of Visual Cryptography: it improves the security of online banking. Instead of a list of Transaction Numbers (TAN's or iTAN's) the bank customer gets from his bank a block a transparencies on which randomly produced shares (share 1) are printed. When the bank customer wants to confirm a money transfer in an online banking session the bank server asks for a confirmation: the customer is asked to mouseclick certain areas on the screen. The bank customer has to put the transparency with the number asked for on top of the share (share 2) shown on the screen. After overlaying the shares he can see the information about the money transfer and also the areas to click on. If the information shown about the money transfer is ok he will do the mouse clicks, and this will be considered by the bank server as a confirmation of the money transfer. This encryption prevents a Man-in-the-Middle attack. The encryption system was suggested in [BR07] and [Gr07], using pixel-based Visual Cryptography. The segment-based version shown in Figure 6 has the four potential advantages listed at the end of the Introduction, as compared to the pixel-based version. Moreover, as Ulrich Greveler pointed out, the segment-based version may have the advantage that the analysis and potential mathematical proof of its security may be easier than in the case of the original pixel-based version because the model is more discrete.

4 Acknowledgements

Thanks to Ulrich Greveler and Klaus Reinhardt for comments on the idea.



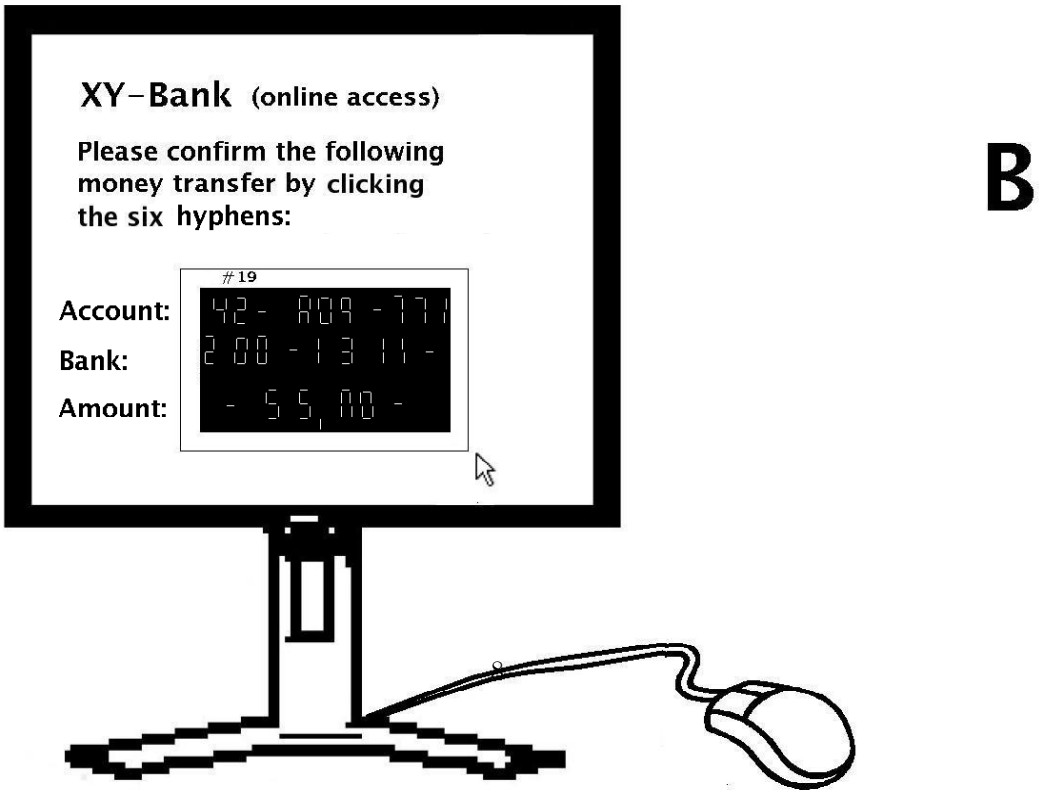


Figure 6: Visual TAN (vTAN)

References

[BR07] Bernd Borchert, Klaus Reinhardt: Abhör- und manipulationssichere Verschlüsselung für Online Accounts. Patent application DE-10-2007-018802.3, 2007

[Gr07] Ulrich Greveler: VTANs - Eine Anwendung visueller Kryptographie in der Online-Sicherheit. Kryptologie in Theorie und Praxis, 2007, to appear

[Kl07] Andreas Klein: Visuelle Kryptographie. Springer Verlag, 2007.

[NS94] Moni Naor, Adi Shamir: Visual Cryptography. EUROCRYPT 1994: 1-12.

[Wo08] F.W.Wood: Illuminated Announcement and Display Signal. US Patent 974943, 1908