Eine Einführung in die visuelle Kryptographie

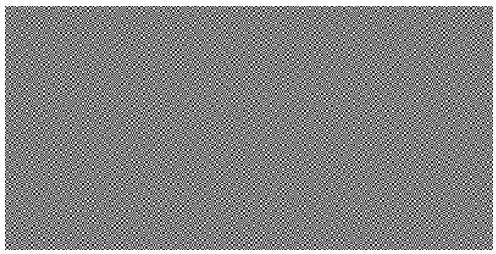
von Andreas Klein

Visuelle Kryptographie wurde 1994 von Naor und Shamir [12] *erfunden. Dabei wird ein Schwarz-Weiß-Bild so in zwei Bilder codiert, dass jedes der beiden Bilden wie ein zufälliges Punktmuster wirkt. Kopiert man jedoch diese Bilder auf Folien und legt diese übereinander, so erscheint wieder das ursprüngliche Bild. In diesem Artikel möchte ich die Methode und ihre möglichen Anwendungen kurz vorstellen.*

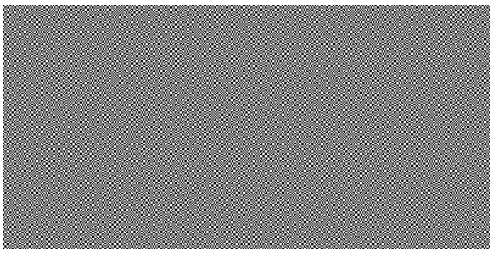
Man stelle sich die folgende Situation vor. Nach einigen Einkäufen mit der Geldkarte stellt man überrascht fest, dass mehrere Hundert Euro zu viel von der Karte abgebucht wurden. Eine genauere Überprüfung zeigt, dass der Zigarettenautomat um die Ecke statt jeweils 5 EUR immer 50 EUR für eine Schachtel verlangt haben muss. Dummerweise ist die Zahlung mit einer Geldkarte anonym und da der Automatenbetreiber schlau genug war den manipulierten Automaten auszutauschen, bevor der Betrug entdeckt wurde, kann der Betrug nicht mehr nachgewiesen werden. Der Betrogene bleibt auf seinem Schaden sitzen. Obwohl ein solcher Betrug bisher noch nicht vorgekommen ist, wäre er durchaus möglich. Das Problem liegt darin, dass die Bezahlung mit einer Geldkarte am Automaten ähnlich ist, als würde man dem Verkäufer an einer Kasse seinen Geldbeutel geben, damit er sich den fälligen Betrag selber nimmt. Die Unsicherheit dieses Vorgehens ist augenfällig. Was kann man also tun, um das Bezahlsystem sicherer zu gestalten?

Ein mögliche Lösung wäre statt anonymen Geldkarten Kreditkarten zu verwenden, bei denen alle Transaktionen protokolliert werden. Die Möglichkeiten den Kunden zu betrügen wären bei diesem Vorgehen für unseriöse Automatenhersteller stark eingeschränkt. Allerdings ist aus Datenschutzgründen ein solches Vorgehen, das einen „gläsernen Kunden“ schafft, nicht wünschenswert.

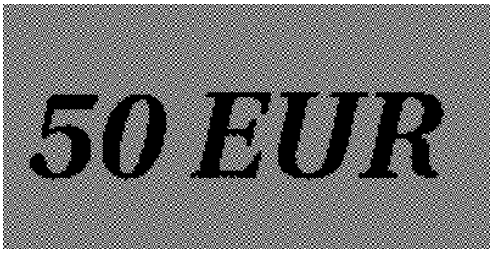
Eine andere Möglichkeit verwendet Kryptographie, um der Geldkarte eine sichere Möglichkeit zu bieten, das nicht vertrauenswürdige Display des Automaten zur Anzeige zu benutzen. Die Geldkarte erhält als Zubehör eine scheckkartengroße Folie die etwa folgendes Bild zeigt:



Der Automat sendet nun den Betrag, den er abbuchen möchte (z. B. 50 EUR) an die Karte und diese berechnet das folgende Bild, das von dem Automaten angezeigt werden soll:



Wir legen die Folie über das Display des Automaten und sehen:

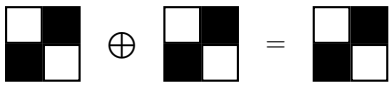


Später werden wir sehen, dass der Automat keine Möglichkeit hat das von der Karte gesendete Punktmuster gezielt zu verfälschen. Auf diese Weise können wir beim Bestätigen der Transaktion sicher sein, dass der abgebuchte Betrag 50 EUR ist.

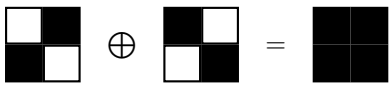
Visuelle Kryptographie

Wir wollen uns nun das Verfahren genau ansehen. Codiert werden soll ein Schwarzweiß-Bild. Dabei wird jeder Bildpunkt in vier Subpixel zerlegt. Dies geschieht so, dass sowohl auf der Folie als auch auf dem Display des Automaten jeder Bildpunkt gleichwahrscheinlich durch eine der beiden folgenden Subpixel-Kombinationen dargestellt wird.

Die Darstellung der Pixel auf der Folie und dem Display sind jedoch nicht voneinander unabhängig. Soll ein weißer Bildpunkt dargestellt werden, so wird auf beiden die gleiche Subpixel-Kombination genommen, zum Beispiel:



Für einen schwarzen Bildpunkt müssen die Subpixel-Kombinationen verschieden sein, z. B.:



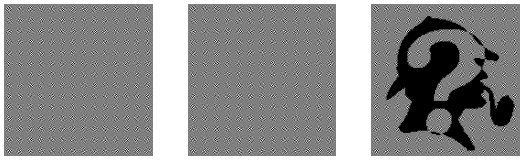
Ein Angreifer, der (wie der Automat) nur ein Teilbild kennt, sieht nur eine zufällige Verteilung von den beiden möglichen Subpixel-Kombinationen. Ein Teilbild alleine liefert daher keine Informationen über das codierte Bild. Das Verfahren ist also wie auch das bekanntere One-Time-Pad absolut sicher, und wie beim One-Time-Pad ist in diesem Fall der Schlüssel (die Folie) genauso groß wie die verschlüsselte Nachricht (das Display). Allerdings bietet das Verfahren ebenso wie das One-Time-Pad zunächst keine Nachrichten-Authentikation und keinen absoluten Schutz, wenn ein Schlüssel mehrfach verwendet wird.

Für das Beispiel in der Einleitung bedeutet das, dass die Karte nur geheime Bilder wählen darf, die der Automat nicht erraten kann. Beispielsweise könnte die Karte die 50 immer an eine zufällig gewählte Position des Displays schreiben. Außerdem sollten wir die Karte nie mehrmals hintereinander bei demselben Automaten benutzen.

Wie schnell das Verfahren unsicher wird, wenn mehr als ein Bild mit derselben Folie verschlüsselt werden soll, zeigt das folgende Beispiel.

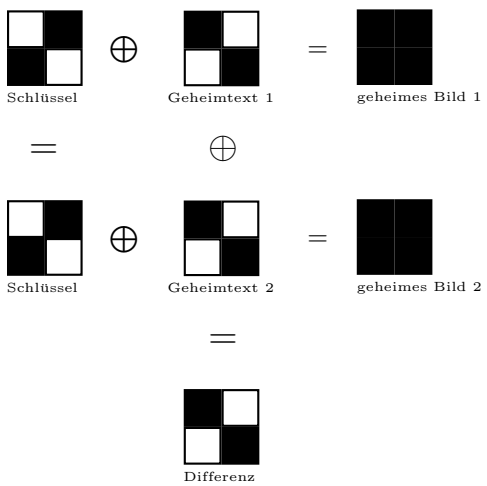
Angenommen wir wollen die beiden folgenden Bilder mit der rechts abgebildeten geheimen Folie verschlüsseln:

Wendet man das oben beschriebene Verfahren an, um die beiden Bilder zu verschlüsseln, so kann ein Angreifer aus einem geheimen Bild keine Information über das codierte Bild erhalten. Kennt der Angreifer jedoch beide geheimen Bilder (siehe unten links), so muss er sie nur auf Folien kopieren und die Folien übereinanderlegen, um den Inhalt der beiden Bilder zu erkennen (siehe unten rechts):



Man erkennt deutlich die symmetrische Differenz der beiden geheimen Bilder. Ein analoger Angriff ist übrigens auch bei Stromchiffren möglich, falls ein Initialisierungsvektor doppelt benutzt wird. (Bei diesen Verschlüsselungsalgorithmen erzeugen beide Teilnehmer eine nur ihnen bekannte Pseudozufallsfolge, die auf den zu verschlüsselnden Text addiert wird.) Trotz der Bekanntheit dieses Angriffs wird dieser Fehler jedoch immer wieder gemacht, beispielsweise verwenden einige WLAN-Produkte nach dem Einschalten immer den Initialisierungsvektor 0, was ein Eindringen in diese Netze besonders leicht macht [2].

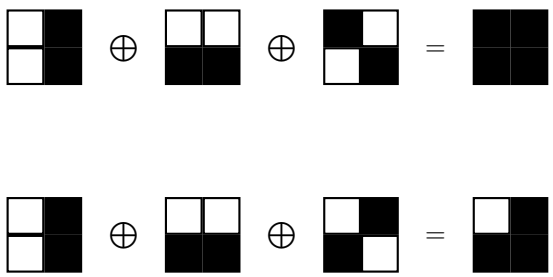
Die nachfolgende Abbildung demonstriert das Problem am Beispiel eines Pixels, der in beiden geheimen Bildern schwarz ist.



Diese Überlegungen zeigen, dass man eine gewisse Vorsicht walten lassen muss, wenn man visuelle Kryptographie als eine Authentikationmethode verwenden will. Eine ausführliche Diskussion findet man in [11].

Geteilte Geheimnisse

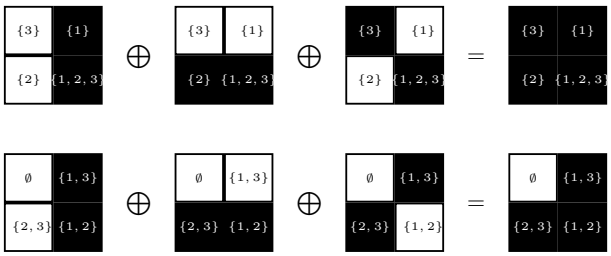
Richtig spannend wird visuelle Kryptographie erst, wenn man das geheime Bild auf mehr als zwei Folien verteilt. Das unten stehende Beispiel zeigt eine Variante mit drei Folien.



Auf der ersten Folie sind jeweils zwei vertikal übereinander liegende Subpixel schwarz, auf der zweiten Folie liegen die beiden schwarzen Subpixel horizontal nebeneinanderer und auf der dritten Folie liegen sie einander diagonal gegenüber. Die Verteilung der Subpixel ist so gewählt, dass beim Übereinanderlegen der drei Folien entweder alle vier Subpixel schwarz werden oder ein Subpixel frei bleibt, je nachdem ob ein schwarzer oder weißer Bildpunkt codiert werden soll. Dabei garantiert die Anordnung der Subpixel, dass ein Angreifer der nur zwei der drei Folien kennt, keine Information über das codierte Bild erhält.

Allgemein kann man zu jedem n und jedem $k \leq n$ eine Menge von n Folien konstruieren, so dass aus je k Folien das geheime Bild rekonstruiert werden kann. Dieses führt auf einige reizvolle kombinatorische Probleme von denen noch längst nicht alle gelöst sind (siehe z. B. [1, 5, 8]).

Um einen Eindruck von der Art der Konstruktionen zu geben, beschreibe ich hier kurz einen Verfahren, bei dem man alle n Folien übereinanderlegen muss, um das geheime Bild zu rekonstruieren. Dazu wird jeder Pixel in 2^{n-1} Subpixel unterteilt. Will man einen dunklen Punkt darstellen, werden die Subpixel in einer zufälligen Reihenfolge mit den Teilmengen ungerader Mächtigkeit von $\{1, \ldots, n\}$ beschriftet. Für einen hellen Punkt nimmt man die Teilmengen gerader Mächtigkeit. Nun werden auf der Folie Nummer i alle Subpixel, in deren Beschriftung i enthalten ist, gefärbt. Das Beispiel mit den drei Folien wurde folgendermaßen konstruiert:



Dieses Vorgehen garantiert, dass man beim Übereinanderlegen aller Folien entweder genau ein oder kein helles Subpixel sieht, d. h. das Bild ist zu erkennen. Legt man jedoch nur k Folien übereinander, z. B. die Folien mit den Nummern 1 bis k, so bleiben alle Subpixel frei, die mit einer Teilmenge von $\{k+1, \ldots, n\}$ beschriftet sind. Wegen

$$\sum_{i \equiv 1 \ (2)} \binom{n-k}{i} = \sum_{i \equiv 0 \ (2)} \binom{n-k}{i} \quad \text{für } n-k \geq 1$$

sind dies in jedem Fall 2^{n-k-1} Subpixel, d.h. die Sicherheit bleibt gewahrt. Dieses Verfahren ist auch optimal in dem Sinn, dass kein anderes Verfahren mit weniger Teilpixeln existiert [12]. Dies folgt aus dem folgenden kombinatorischen Satz [10]:

Sind $A_1, \ldots, A_n$ und $B_1, \ldots, B_n$ Teilmengen der Grundmenge G und gilt für jede echte Teilmenge $U \subsetneq \{1, \ldots, n\}$ die Gleichung

$$\left|\bigcap_{i \in U} A_i\right| = \left|\bigcap_{i \in U} B_i\right|,$$

so gilt

$$\left|\bigcup_{i=1}^{n} A_i\right| \leq \frac{1}{2^{n-1}}|G| + \left|\bigcup_{i=1}^{n} B_i\right|,$$

d. h. sind die Schnitte der A_i's und B_i's jeweils gleich groß, müssen auch ihre Vereinigungen ungefähr die gleiche Größe haben.

Eine andere Variante der visuellen Kryptographie, die mir besonders gut gefällt, ist die folgende: Es ist möglich n Folien so zu konstruieren, dass man für jede der $2^n - 1$ nichtleeren Teilmengen der Folien beim Übereinanderlegen der entsprechenden Folien ein anderes vorgegebenes Bild erhält. Auch bei diesem System bleibt die Sicherheit gewahrt, d. h. man kann durch Untersuchen eines Teils der Bilder keine Rückschlüsse auf die anderen Bilder ziehen. Die folgende Abbildung zeigt das Prinzip mit zwei Folien.

In dieser Allgemeinheit wurde die Aussage zuerst in [4] bewiesen. In einer neueren Arbeit habe ich zusammen mit M. Wessler dieses System untersucht. Wir haben Sätze über den optimalen Kontrast (das Verhältnis von hell zu dunkel) der codierten Bilder gezeigt [7].

Ausblick

Die hier präsentierten Resultate sind noch nicht alle Möglichkeiten, die in der visuellen Kryptographie stecken. Man kann die Ideen auch auf Graustufen [9] oder farbige Bilder [13], [6] ausdehnen. Sogar eine Übertragung auf Töne [3] ist möglich. Wer die Beispiele dieses Artikels selber mit Folien ausprobieren möchte, kann sich auf meiner Homepage (`www.mathematik.uni-kassel.de/~klein/vis-crypt/index.html`) die nötigen Bilddateien besorgen.

Literaturverzeichnis

[1] G. Ateniese, C. Blundo, A. D. Santis und D. R. Stinson: *Constructions and bounds for visual cryptography.* In: *ICALP*, Band 1099 von *Lect. Notes Comput. Sci.*, S. 416–428. Springer, Berlin, 1996.

[2] N. Borisov, I. Goldberg und D. Wagner: *Intercepting Mobile Communications: The Insecurity of 802.11.* In: 7th Annual International Conference on Mobile Computing and Networking `http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html`.

[3] Y. Desmedt, S. Hou und J.-J. Quisquater: *Audio and optical cryptography.* In: *Advances in cryptology – ASIACRYPT '98*, Band 1514 von *Lect. Notes Comput Sci.*, S. 392–404. Springer, Berlin, 1998.

[4] S. Droste: *New results in visual cryptography.* In: *Advances in cryptology – CRYPTO '96*, Band 1109 von *Lect. Notes Comput. Sci.*, S. 401–415. Springer, Berlin, 1996.

[5] T. Hofmeister, M. Krause und H. Simon: *Contrast-optimal k out of n secret sharing schemes in visual cryptography.* Theor. Comput. Sci. 240(2): 471–485, 2000.

[6] A. Klein: *Farbige visuelle Kryptographie.* Technischer Bericht 05/01, Mathematische Schriften Kassel, 2001. `http://www.mathematik.uni-kassel.de/sites/downloads/prep0105.pdf`.

[7] A. Klein und M. Wessler: *Extended visual cryptography schemes.* Information and Computation to appear.

[8] C. Kuhlmann und H. Simon: *Construction of visual secret sharing schemes with almost optimal contrast.* In: *Proceedings of the 11th annual ACM-SIAM symposium on Discrete algorithms*, S. 263–272. 2000.

[9] C.-C. Lin und W.-H. Tsai: *Visual cryptography for gray-level images by dithering techniques.* Pattern Recognit. Lett. 24(1-3): 349–358, 2003.

[10] N. Linial und N. Nisan: *Approximate inclusion-exclusion.* Combinatorica 10: 349–365, 1990.

[11] M. Naor und B. Pinkas: *Visual authentication and identification.* In: *Advances in Cryptology – CRYPTO '97*, Band 1294 von *Lect. Notes Comput. Sci.*, S. 322–336. 1997.

[12] M. Naor und A. Shamir: *Visual cryptography.* In: *Advances in Cryptology – EUROCRYPT '94* (Herausgegeben von A. D. Santis), Band 950 von *Lect. Notes Comput. Sci.*, S. 1–12. Springer, Berlin, 1994.

[13] C.-N. Yang und C.-S. Laih: *New colored visual secret sharing schemes.* Des. Codes Cryptography 20(3): 325–336, 2000.

Adresse des Autors
Dr. Andreas Klein
Fachbereich für Mathematik und Informatik
Universität Kassel
Heinrich-Plett-Straße 40 (AVZ)
34132 Kassel
`klein@mathematik.uni-kassel.de`

Andreas Klein hat in Gießen Mathematik und Informatik studiert und arbeitet seit Dezember 2000 als wissenschaftlicher Mitarbeiter in der Arbeitsgruppe „Computational Mathematics“ der Universität Kassel. In der Forschung beschäftigt er sich mit verschieden Anwendungen der Kombinatorik in der endlichen Geometrie, Codierungstheorie, Kryptographie etc. Im Februar dieses Jahres hat er seine Habilitation über Faltungscodes erfolgreich abgeschlossen.

Zentralblatt MATH-Konsortium der DMV

Nach Verhandlungen der Herren Bierstedt (für die DMV) und Wegner (Editor-in-Chief, Zentralblatt MATH) mit dem Springer-Verlag und dem Fachinformationszentrum (FIZ) Karlsruhe wurde mit Zustimmung des Präsidiums der DMV beschlossen, das bisherige Zentralblatt MATH-Konsortium der DMV zu analogen Bedingungen für weitere fünf Jahre fortzuführen. Das Konsortium hatte sich in der ersten Phase (1999–2004) bewährt.

Die Teilnehmer an der zweiten Phase des Zentralblatt MATH-Konsortiums (mathematische Institute oder deren Bibliotheken) verpflichten sich wieder, ihre Abonnements des Zbl. MATH für die nächsten fünf Jahre 2005–2009 nicht zu kündigen, und beziehen das Zbl. MATH über die DMV (was erfordert, dass das Institut bzw. seine Bibliothek Mitglied der DMV ist). Im Gegenzug wird für die fünf Jahre 2005–2009 der jährlich zu zahlende Preis für das Zbl. MATH festgeschrieben.

Der jährliche Nettopreis beträgt für Paket 1 (Online mit Backup-CD) EUR 4.400 und für Paket 2 (Print plus Online mit Backup-CD) EUR 5.200; das Bestellen der Printversion allein kostet genauso viel wie Paket 2. Dies ist bereits ein durchschnittlicher Rabatt von ca. 20 % auf die regulären Preise für 2005. Der Rabatt erhöht sich in den Folgejahren durch die Festschreibung dieses Preises, sofern der reguläre Preis steigt. – Für mathematische Institute in Nordrhein-Westfalen gelten über die Digitale Bibliothek NRW andere Preise.

Die Preissteigerung für Paket 1 betrug in den vergangenen fünf Jahren insgesamt moderate 11 %. Dies ist z. T. auf den Einfluss der beiden Unterzeichner im Coordinating Committee für das Zentralblatt MATH zurückzuführen, obwohl nach wie vor der Preis vertragsgemäß allein von FIZ Karlsruhe und Springer-Verlag festgelegt wird. Natürlich war es nicht möglich, den Preis von 1999 für die Teilnehmer des Konsortiums auch über 2004 hinaus zu erhalten, aber wir denken, dass das neue Konsortium den mathematischen Instituten in Deutschland hilft, in den nächsten Jahren etwas zur Konsolidierung der Bibliotheksetats beizutragen.

gez. Klaus D. Bierstedt und Bernd Wegner