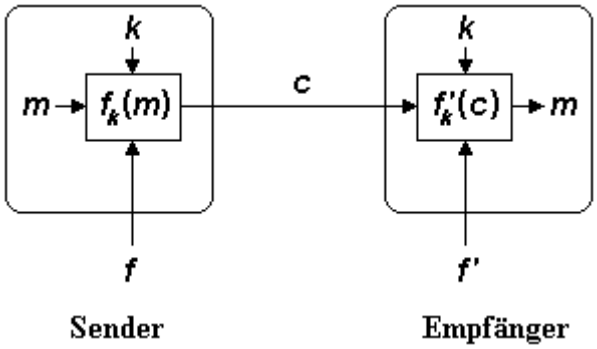
Visuelle Kryptografie

Was ist Kryptografie ?

Eine Nachricht wird so verschlüsselt, dass sie nur mit dem richtigen Schlüssel erkannt werden kann. So kann zum Beispiel ein Sender eine geheime Nachricht sicher zu einem Empfänger senden, ohne dass ein möglicher Angreifer sie unterwegs erkennen kann.
Im folgenden Beispiel haben wir eine Nachricht *m,* einen Schlüssel *k* und eine Verschlüsselungsfunktion *f* und eine Entschlüsselungsfunktion *f '.*

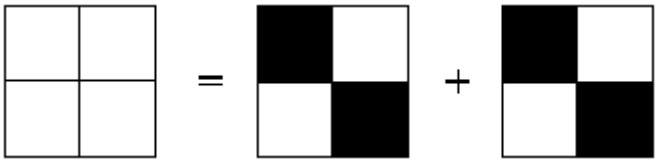


Das erste visuelle Verschlüsselungsverfahren wurde 1994 von Moni Naor und Adi Shamir entwickelt. Bei visueller Kryptografie wird ein Bild in mehrere Teilbilder codiert, so dass jedes einzelne Teilbild wie ein zufälliges Punktmuster wirkt. Legt man die Teilbilder dann übereinander, so erkennt man erst das ursprüngliche Bild.

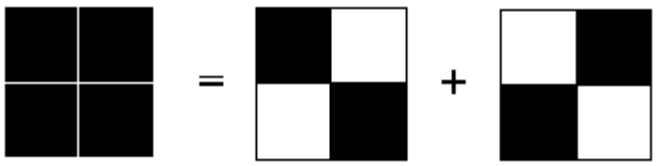
Verfahren bei Visueller Kryptografie

Jeder Bildpunkt wird in 4 Subpixel zerlegt. Bei 2 Teilbildern geht man wie folgt vor: Jeder Bildpunkt wird auf jedem Teilbild mit gleicher Wahrscheinlichkeit durch eine der folgenden Subpixel-Kombinationen dargestellt:

Für einen weißen Punkt wählen wir zwei gleiche Kombinationen:



Für einen schwarzen Punkt wählen wir zwei verschiedene Kombinationen:



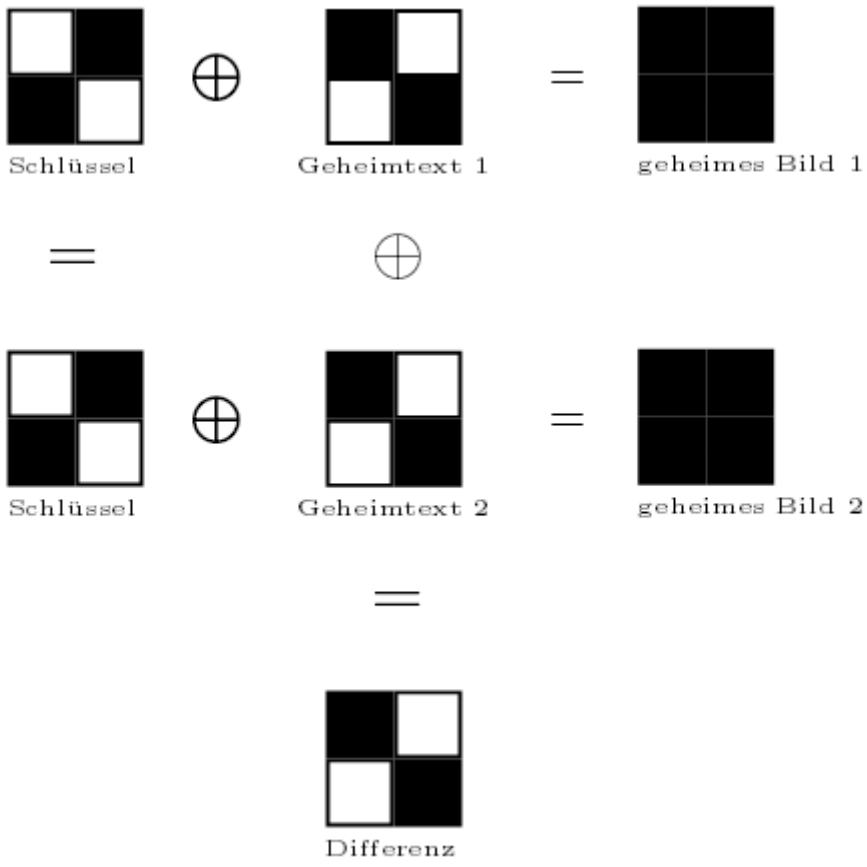
Ein Teilbild zeigt uns eine zufällige Verteilung der beiden Subpixel-Kombinationen und liefert daher einem möglichen Angreifer keine Information über das ursprüngliche Bild. Der Schlüssel ist genauso groß wie die verschlüsselte Nachricht.

Frage: Ist das Verfahren sicher?

Ein Verschlüsselungs-Verfahren gilt als sicher, wenn, wenn der Schlüssel nur durch Ausprobieren von sehr vielen Möglichkeiten gefunden werden kann. Wir haben es bei einem Bild jeweils mit endlich vielen Pixeln zu tun. Deswegen gibt es auch nur endlich viele Möglichkeiten, Verschlüsselungsfolien zu erstellen.
Im oben beschriebenen Fall gibt es für ein Bild mit n Pixeln jeweils 2^n mögliche Folien. Bei einer für heutige Verhältnisse relativ geringen Bildschirmauflösung von 1024 x 768 Pixeln gibt es somit $2^{786'432}$ mögliche visuelle Verschlüsselungen. Der WEB 2.0 Rechner gibt diese Zahl schon als unendlich aus.
(Vergleich: 2^{400} ist schon eine 113-stellige Zahl.)
Also ja, das Verfahren ist laut Definition sicher.

Frage: Unter welchen Umständen ist das Verfahren sicher?

Wenn jede Folie nur einmal verwendet wird. Sobald man dieselbe Folie für zwei Bilder verwendet, kann man mit jeweils einer Teilfolie der zwei Bilder den Inhalt beider Bilder erkennen. Ein Pixel, der in beiden geheimen Bildern schwarz ist, wird dann weiß:



Frage: Was passiert mit einem Pixel, der in beiden Bildern weiß ist?

Er wird auch weiß.

<u>Frage:</u> Was passiert mit einem Pixel, der in beiden Bildern unterschiedlich ist?

Ein Punkt, der in einem Bild schwarz und im anderen Bild weiß ist, wird dann schwarz.

Also sieht man beim Aufeinanderlegen von zwei Teilfolien unterschiedlicher Bilder, die mit derselben Verschlüsselungsfolie erstellt wurden deren Differenz.

Visuelle Kryptografie wird umso spannender, je mehr Teilfolien man von einem Bild erstellt. Das folgende Beispiel zeigt eine Variante für Pixel-Zerlegungen um drei Teilbilder zu erstellen.

<u>Aufgabe:</u> Suchen Sie nach weiteren Varianten von Pixel-Zerlegungen für drei Folien.

Auch Farbbilder kann man nach dem gleichen Prinzip verschlüsseln. Das Verfahren wird mit 4 Farben noch interessanter. Unten ist eine Tabelle mit Pixelzerlegungen für zwei Teilbilder in 4 Farben (Weiss, Gelb, Magenta und Cyan). Die erste Reihe steht für Folie 1, die zweite Reihe für Folie zwei und die dritte für das ursprüngliche Bild.

<u>Frage:</u> Wie kann man das Verfahren sicherer machen, wenn das verschlüsselte Bild auf dem Display eines Bankautomaten ist und in unserer Bankkarte eine Schlüsselfolie gespeichert ist?

Indem man die Position der Information auf dem Display immer wieder ändert.

Das waren die einfachsten Beispiele für Visuelle Kryptografie. Je mehr Folien und je mehr Farben man für die Verschlüsselung verwendet, desto komplexer und sicherer wird das Verfahren. Visuelle Kryptografie findet zum Beispiel Anwendung in der „Secure Iris Authentication“, bei Gesichts-Erkennung und bei der Verschlüsselung von Finanz-Dokumenten.