Visuelle Kryptographie

Moderne Schatzkarten-Zerteiler

In Märchen und Legenden sowie unter Piraten und ähnlichem Volk ist es oftmals Gang und Gebe, Schatzkarten in mehrere Stücke zu zerteilen und diese dann an getrennten Orten aufzuheben. Dies soll verhindern, dass eine einzelne Person, die in Besitz einer dieser Schatzkartenteile kommt, sofort in der Lage ist, den Schatz zu finden.

Die visuelle Kryptographie hat ein ganz ähnliches Ziel, das allerdings noch etwas schwieriger zu erreichen ist: Die Schatzkarte soll so in mehrere Karten „aufgeteilt“ werden, dass sich aus den Einzelkarten *überhaupt keine* Informationen über die Lage des Schatzes herleiten lässt (im Gegensatz hierzu hat der Schatzsucher aus dem Märchen auch dann eventuell eine gewisse Chance, den Schatz zu finden, wenn sich nur *ein* Kartenteil in seinem Besitz befindet). Außerdem sollen sich die Teilkarten natürlich wiederum derart zusammenfügen lassen, dass sich die volle Information der ursprünglichen Schatzkarte zurück gewinnen lässt.

Statt sich auf Schatzkarten zu beschränken, behandelt die visuelle Kryptographie natürlich beliebige visuelle Informationen, die sich in Form digitaler Bilder darstellen lassen. Wir wollen uns hier zunächst nur auf den Fall von Schwarz-Weiß-Bildern beschränken; diese bestehen aus einem Raster von Pixeln, die entweder schwarz oder weiß sein können.

Wie funktioniert’s?

Die Informationen des zu verschlüsselnden Bildes werden auf mehrere transparente Folien verteilt, die durch Übereinanderlegen wieder die ursprünglichen Informationen zurückliefern. Sobald allerdings eine der Folien fehlt, soll keinerlei Information über das Bild herauszufinden sein.

Jedes einzelne Pixel wird dabei in Unterpixel zerlegt, die so dicht beisammen liegen, dass das menschliche Auge sie als einzelnes Pixel mit einem gewissen Grauwert (entsprechend der Anzahl der schwarzen und weißen Unterpixel) wahrnimmt. Diese Unterpixel werden durch Matrizen dargestellt, deren Einträge aus Nullen und Einsen bestehen (je nachdem, ob die Pixel schwarz oder weiß sind). Die Matrix für ein einzelnes schwarzes oder weißes Pixel wird bei der Verschlüsselung zufällig aus einer zuvor festgelegten Menge für weiße Pixel bzw. für schwarze Pixel gewählt.

Werden nun mehrere Folien übereinander gelegt, so entsteht im Gesamtbild überall dort ein schwarzes Pixel, wo in mindestens einer der Folien ein schwarzes Pixel gesetzt ist. In der Fachsprache sagt man, dass die Überlagerung der Folien der bitweisen Oder-Verknüpfung der Codierungsmatrizen entspricht. Die Festlegung der Matrizen für weiße Pixel muss so geschehen, dass ihre Oder-Verknüpfung (Überlagerung) immer einen Grauwert liefert, den das Auge noch deutlich von Schwarz unterscheiden kann. Die Matrizen für schwarze Pixel hingegen werden so gewählt, dass die Oder-Verknüpfung aller Folien den Wert Schwarz ergibt. Ferner muss die Verknüpfung von *nicht* allen Folien einen Grauwert ergeben, der sich nicht von der Verknüpfung der weißen Pixel unterscheidet. Somit wird im letzten Fall keine Information sichtbar.

Erweiterungen

k aus n Folien

Es sind beliebige Varianten mit k aus n Folien möglich, d.h. es werden k der insgesamt n verschlüsselten Folien benötigt, um die Information zurückzuerhalten. Sobald man weniger als k Folien übereinanderlegt, entsteht ein zufälliges Muster, aus dem sich keinerlei Informationen herleiten lassen. Legt man jedoch k beliebige der n Folien übereinander, so gewinnt man die volle Information zurück.

Farbige visuelle Kryptographie

Durch Ausnutzen von subtraktiver und additiver Farbmischung kann man visuelle Kryptographie auch mit farbigen Folien (für farbige Bilder) erreichen.

Facts'n'Features

- Visuelle Kryptographie wurde zum ersten Mal 1994 von Naor und Shamir vorgestellt (EUROCRYPT-Konferenz).
- Visuelle Kryptographie wird zur verschlüsselten Übertragung von geschriebenem/gedrucktem Material (gedruckter Text, handgeschriebene Notizen, Bilder usw.) eingesetzt.
- Die Verschlüsselung ist *verlustfrei* (d.h. die zu verschlüsselnde Information lässt sich fehlerfrei rekonstruieren).
- Visuelle Kryptographie ist absolut sicher (ein Angreifer kann keine Information gewinnen, wenn er nicht die erforderliche Anzahl von Folien besitzt).
- einfache Dekodierung (etwa durch das Auge des Betrachters; kein Computer erforderlich, sondern lediglich transparente Folien)
- einfache Handhabung (verschlüsselte Information kann etwa per Fax oder per Post verschickt werden)
- einfaches Verschlüsselungsverfahren (sind die Verschlüsselungs-Matrizen einmal generiert, so ist die Verschlüsselung sehr einfach)