Institut für Theoretische Informatik
Fakultät für Elektrotechnik und Informatik
Universität Hannover

Visuelle Kryptographie

Studienarbeit in Informatik

Verfasst von:
Lennart Suhr

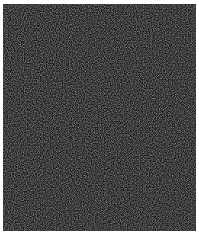
Sommersemester 2011 Betreuer: Dr. Olaf Beyersdorff

Inhaltsverzeichnis

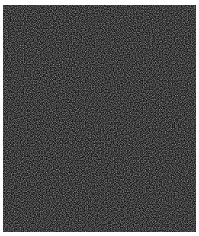
1 Einleitung

Die visuelle Kryptographie ist ein von Moni Naor und Adi Shamir entworfenes Konzept des *secret sharings* und beruht auf der Verschlüsselung von Bildern mit Hilfe von Pixelsubstitutionen. Es wurde erstmals 1994 in einem Artikel im Rahmen der EUROCRYPT veröffentlicht. Bis zum heutigen Tage gibt es zu diesem Thema viele vertiefende Ausarbeitungen und auch einige Erweiterungen.
Die Besonderheit des Verfahrens liegt im einfachen Verständnis und der leichten Anwendung. Um das Prinzip zu verstehen bedarf es keiner tief gehenden mathematischen Kenntnisse und die Entschlüsselung ist im Gegensatz zu anderen gängigen Verfahren ohne die Hilfe eines Computers in wenigen Augenblicken durchführbar.
Die Idee ist ganz einfach: Ein Bild wird in 2 bis n Folien zerlegt, die aus scheinbar zufällig zusammengewürfelten schwarzen und weißen Pixeln bestehen. Doch legt man diese Folien exakt übereinander erscheint wieder das Originalbild.

Folie 1:



Folie 2:



Folie 1 und 2:

2. Das Modell

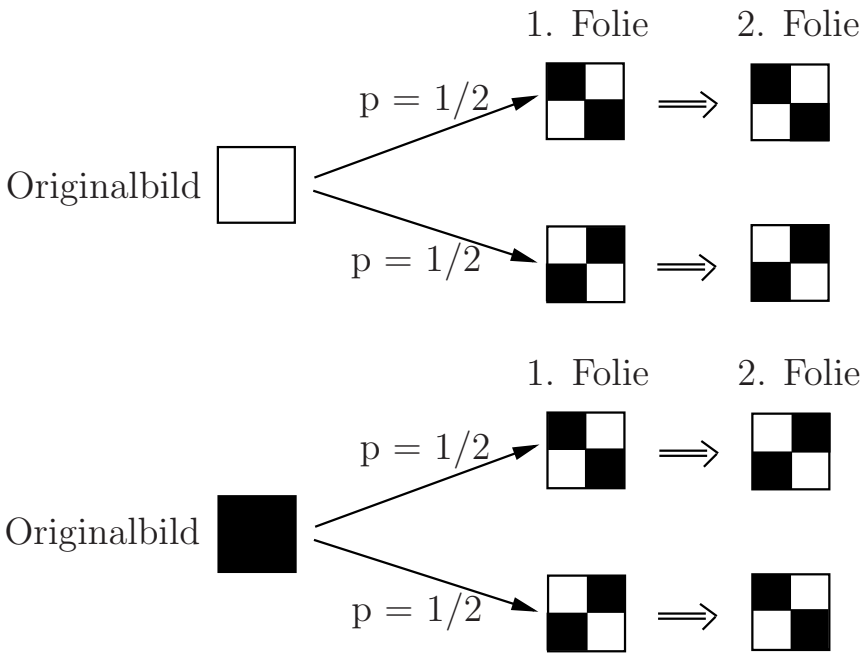
In dem folgenden Kapitel wird ein noch übersichtliches “2 aus 2” secret sharing -Verfahren der visuellen Kryptographie mit vier Unterpixeln beschrieben, um anschaulich einige Beispiele anbringen zu können und die Grundlagen zu setzen. In den darauf folgenden Abschnitten wird anschließend noch auf allgemeine “k aus k” und “k aus n” -Verfahren eingegangen.

2.1 “2 aus 2” secret sharing -Verfahren

Bei einem “2 aus 2” secret sharing -Verfahren geht es darum, ein Geheimnis in zwei Teile zu teilen, wobei keines für sich Rückschlüsse auf das Original liefern darf. Erst wenn beide Teile wieder zusammengefügt werden, ergibt sich die ursprüngliche Nachricht. In der visuellen Kryptographie muss die geheime Nachricht als schwarzweißes Bild vorliegen, da hier mit einer pixelweisen Substitution gearbeitet wird. Mittlerweile existieren aber auch erweiterte Verfahren für die Verschlüsselung von Grau- und Farbbildern (siehe Kapitel 3.3 und 3.4).

Jeder Pixel des Originalbildes wird einzeln für jede der zwei benötigten Folien (auch shares genannt) nach einem unterschiedlichen Muster in vier Unterpixel unterteilt, wobei die Anordnung der Unterpixel in der 2. Folie von der durch Zufall (mit Wahrscheinlichkeit p) entschiedenen Form der ersten abhängt. Um das ursprüngliche Bild erkennen zu können, müssen beide Folien präzise übereinander gelegt werden, sodass sich die Unterpixel ergänzen.
Die Zuweisung der Unterpixel eines schwarzen oder weißen Originalpixels lässt sich mit Hilfe einer boolschen n x m-Matrix $S^t = [s_{i,j}]$ mit $t \in \{0, 1\}$ darstellen, wobei die i-te Zeile der i-ten Folie und die j-te Spalte dem j-ten Unterpixel entspricht. n ist also gleich der Anzahl der Folien und m entspricht der Anzahl der Unterpixel. Das t steht für die Zuordnung zu weißen ($t = 0$) bzw. schwarzen Pixeln ($t = 1$).
Es gilt: $[s_{i,j}] = 1$, wenn der j-te Subpixel in der i-ten Folie schwarz ist und umgekehrt $[s_{i,j}] = 0$, wenn er weiß ist. Die Nummerierung der Pixel erfolgt hierbei zeilenweise, von oben links nach unten rechts.

Beispiel:



Dies entspricht folgenden 2 x 4-Matrizen:

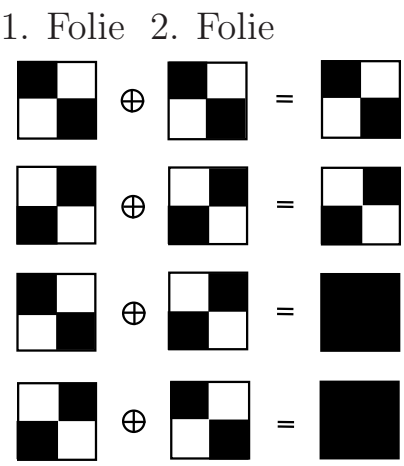
$S^0 = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \end{pmatrix}$ oder $S^0 = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \end{pmatrix}$ für einen weißen Pixel

und $S^1 = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}$ oder $S^1 = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}$ für einen schwarzen.

Jede Folie erhält mit diesem Schema sowohl für schwarze als auch für weiße Originalpixel eine zufällige der zwei möglichen Substitutionen und es ist somit für beide Folienbesitzer alleine unmöglich mit bloßem Auge oder Erraten auf das Originalbild zu schließen. Wenn nun aber beide Folien übereinandergelegt werden, ergänzen sich die entsprechenden Unterpixel entweder zu einem vollen Schwarz, falls die Unterpixel der Folien komplementär waren, oder zu einem Grauwert, sofern die Unterpixel übereinstimmen.

Die folgende Grafik visualisiert die Möglichkeiten die Unterpixel zu kombinieren:

Kombinierte Pixel:



Wichtig hierbei ist zu beobachten, dass ein schwarzer Unterpixel nicht durch einen weißen wieder ausgelöscht bzw. “aufgehellt” werden kann. Sobald in einer der Folien ein Bereich durch einen schwarzen Unterpixel ausgefüllt ist, wird dieser Teil auch beim Übereinanderlegen schwarz bleiben. Die zugrunde liegende algebraische Struktur ist vergleichbar mit der einer Halbgruppe, in welcher es keine inversen Elemente gibt.

Dadurch, dass ein weißer Originalpixel zur Hälfte schwarz wird, entsteht immer ein gewisser Kontrastverlust zwischen Schwarz und Weiß gegenüber dem Originalbild, welchen man natürlich möglichst klein halten möchte (vergleiche Kapitel 2.2).
Der so entstehende Grauwert eines Pixels lässt sich anhand des Hamming-Gewichts H des Vektors V ablesen, der durch das boolesche “oder” der Zeilen der zugehörigen Matrix entsteht. Je größer der Wert, desto mehr Unterpixel des kombinierten Pixels sind schwarz.

Beispiel:

$$A = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

$$\underline{\quad or: \quad}$$

$$V = \begin{pmatrix} 1 & 0 & 1 & 1 \end{pmatrix} \Rightarrow H(V) = 3$$

Gilt $H(V) \geq d$, für einen festgelegten Wert d, $d \leq m$, so wird der Pixel als schwarz interpretiert. Gilt $H(V) \leq d - \alpha \cdot m$, wobei m der Unterpixelanzahl entspricht und α $(0 < \alpha \leq 1)$ für den relativen Unterschied zwischen schwarzen und weißen Pixeln steht, dann wird der Pixel als weiß interpretiert. Der maximale Kontrastverlust berechnet sich folglich durch: $v_{max} = \frac{100}{m} * (d - \alpha \cdot m)$

Definition: Angelehnt an die Variable "d" bezeichen wir die durch den Ausdruck "$d - \alpha \cdot m$" beschriebene maximale Unterpixelzahl eines kombinierten weißen Pixels mit w.

In unserem Beispiel ist $d = 4$, $m = 4$ und $\alpha = 1/2$. Für das Hamming-Gewicht des "oder"-Vektors der Matrizen für einen schwarzen Pixel gilt jeweils
$H(V) = 4 \geq d$, für die Matrizen eines weißen Pixels gilt in beiden Fällen $H(V) = 2 \leq w$ $(w = 4 - 1/2 \cdot 4)$. Das Hamming-Gewicht $H(V)$ ist stets entweder kleiner als w oder größer als d.
Es liegt folglich also ein Kontrastverlust von 50% gegenüber einem weißen Originalpixel vor (ein weißer Originalpixel wird zur Hälfte schwarz). Je kleiner α bei einer Konstruktion ist, desto dunkler erscheinen am Ende die weißen Originalpixel. Es ist in der visuellen Kryptographie nicht möglich, dass diese Pixel auf dem Bild der zusammengefügten Folien wieder ein reines Weiß ergeben. Um das zu erreichen, dürfte man weiße Pixel erst gar nicht verschlüsseln.
Der Wert von m steht für den Verlust an Auflösung zwischen dem zusammengesetzten Bild und dem Originalbild. Aus diesem Grund möchte man stets mit der geringsten Zahl an Unterpixeln arbeiten. Ebenfalls wäre es optimal, wenn dieser Wert das Quadrat einer natürlichen Zahl a $(a \geq 2)$ darstellt, damit die Unterpixel quadratisch angeordnet werden können und es zu keiner Verzerrung des Originalbildes kommt. Im Allgemeinen ist dies aber nur selten realisierbar, da die dafür in Frage kommenden Unterpixelzahlen sehr begrenzt sind und nicht immer alle nötigen Bedingungen für das aktuelle Schema erfüllen.

Natürlich gibt es auch noch andere Möglichkeiten für die Matrizen eines "2 aus 2" -Verfahrens der visuellen Kryptographie mit vier Unterpixeln, sodass sich beim Übereinanderlegen der Folien wieder das Originalbild ergibt. Der Einfachheit wegen wurden anfangs nur jeweils zwei Matrizen verwendet.

Definition:

- Die Menge aller möglichen Matrizen für einen weißen Pixel wird mit C_0 bezeichnet.
- Die Menge aller möglichen Matrizen für einen schwarzen Pixel wird mit C_1 bezeichnet.

Es gilt für unser Beispiel:

$$C_0 = \{A \in \{0,1\}^{2x4} \mid A \text{ ist Spaltenpermutation von } \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{pmatrix}\}$$

$$C_1 = \{A \in \{0,1\}^{2x4} \mid A \text{ ist Spaltenpermutation von} \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}\}$$

Die Matrizen, aus welchen durch Permutation der Spalten die Kollektionen C_0 und C_1 entstehen bezeichnen wir fortan als *Basismatrizen*. Es ist leicht zu sehen, dass in diesem Fall jede Kollektion sechs Matrizen enthält und somit für *jeden einzelnen* weißen Originalpixel zufällig ($p = 1/6$) eine Matrix aus C_0 und für *jeden einzelnen* schwarzen Originalpixel zufällig ($p = 1/6$) eine Matrix aus C_1 gewählt wird, anhand derer die substituierten Pixel auf den Folien erstellt werden. Entsprechend bezeichnen wir die Anzahl der Elemente der Mengen C_0 und C_1 mit r.
Es gilt hier also $r = 6$. Generell müssen die beiden Mengen nicht gleich groß sein, aber in den meisten Konstruktionen sind sie es.

2.2 Verallgemeinerung zu “k aus k” -Verfahren

Natürlich lässt sich das Verfahren auch auf Systeme erweitern, die mit mehr als zwei Folien arbeiten. Übersichtliche, mit dem menschlichen Auge erkennbare Lösungen lassen sich aber meist nur für geringe Werte von k finden, da mit steigender Folienzahl auch die Anzahl der benötigten Unterpixel m wächst und der Kontrastverlust sehr groß wird.

Schon bei fünf Teilnehmern ist es unmöglich ein Schema mit nur vier Unterpixeln zu erstellen, welches erst bei Zusammenführung sämtlicher Folien das Originalbild preisgibt. So entwickelten Moni Naor und Adi Shamir (siehe [1]) für generelle k-Werte eine Unterpixelzahl von $m = 2^{k-1}$ mit $\alpha = \frac{1}{2^{k-1}}$ und zeigten, dass dies die optimalen Werte sind für ein "k aus k"-Schema.
Optimal bedeutet in diesem Sinne, dass die Pixelzahl so gering wie möglich und die Sicherheit so groß wie möglich gehalten wurden. Leider hat dies aber immer einen sehr hohen Kontrastverlust zur Folge.

Definition: Ein "k aus k"-Verfahren ist genau dann am sichersten, wenn für jede Teilmenge $\{i_1, ..., i_q\}$ der Folien $\{1, 2, ..., k\}$ mit $q < k$, die daraus entstehenden reduzierten Kollektionen dieselben Matrizen mit derselben Häufigkeit enthalten. Mit anderen Worten, wenn es selbst für den stärksten Kryptoanalytiker unmöglich ist darauf zu schließen, ob ein spezifischer Pixel schwarz oder weiß wird.

Es darf beim Übereinander legen von nur einer bis zu $k - 1$ Folien auch mit größter Genauigkeit und selbst mit technischen Mitteln nicht möglich sein festzustellen, ob ein spezifischer Pixel schwarz oder weiß wird. Wenn nun aber bei $k - 1$ Folien schon deutlich erkennbar ist, welche Pixel vermutlich schwarz werden und welche nicht und somit die Struktur des Originalbildes erraten werden könnte, dann ist das System nicht 100%ig sicher und für praktische Zwecke nicht wirklich brauchbar.

Satz: *Je größer α, desto besser der Kontrast, aber desto unsicherer das Verfahren.*

Beweis: Seien k, d und m sinnvoll gewählt, $d \leq m$. Für das Hamming-Gewicht $H(V)$ des "oder"-Vektors einer Matrix, die für einen schwarzen Pixel steht, muss bekanntlich gelten: $H(V) \geq d$. Für weiße entsprechend $H(V) \leq w$ (Erinnerung: $w = d - \alpha \cdot m$). Je größer α, desto größer ist also die Differenz dieser Werte und desto weniger schwarze Unterpixel enthält ein kombinierter weißer Originalpixel. Dies bedeutet es gibt einen höheren Kontrast zwischen weißen und schwarzen Pixeln.

Die höchste Sicherheit bietet nach Definition ein System, in welchem für jede Teilmenge $\{i_1, ..., i_q\}$ der Folien $\{1, 2, ..., k\}$ mit $q < k$ nicht ersichtlich ist, ob ein spezifischer Pixel schwarz oder weiß wird. Bei gewünschtem hohen Kontrast muss die maximale schwarze Unterpixelzahl eines kombinierten weißen Pixels w so klein wie möglich gewählt werden, was aber in Widerspruch zu der Unmöglichkeit der vorzeitigen Rekonstruktion des Originalbildes steht. Je weniger schwarze Unterpixel ein kombinierter weißer Pixel besitzen darf, desto nahe liegender ist der Gedanke bei steigender kombinierter Folienzahl q, dass es sich bei entsprechenden Pixeln um weiße handelt und sämtliche andere schwarz sein müssen.

Korollar: *Je größer w, desto sicherer das Verfahren.*

Beispiel: $m = 9$, $d = 8$ und $k = 4$.

Folgende Tabelle zeigt den Zusammenhang zwischen α, der maximalen schwarzen Unterpixelzahl w eines kombinierten weißen Pixels und dem entsprechenden maximalen Kontrastverlust v_{max} in Prozent:

$\boldsymbol{\alpha}$	1/9	2/9	3/9	4/9	5/9	6/9	7/9	8/9	1
w	7	6	5	4	3	2	1	0	-
$\mathbf{v_{max}}$ **in %**	77,8	66,7	55,6	44,4	33,3	22,2	11,1	0	-

Da die Substitution eines weißen Originalpixels für jede der vier Folien mindestens *einen* schwarzen Unterpixel enthalten muss (das Originalbild wäre andernfalls sofort ersichtlich), gilt notwendigerweise im minimalsten Fall: $w \geq 1$. Es existiert somit in diesem Beispiel ein Kontrastverlust von mindestens 11,1%.
Am sichersten aber wäre dieses nun Beispiel bei $w = 7$, woraufhin $\alpha = 1/9$ gilt und es einen Kontrastverlust von 77,8% beinhaltet. So wäre es selbst bei $k-1$ übereinanderliegenden Folien unmöglich herauszufinden, wie das Originalbild ausieht, da jeder Pixel bei $k - 1$ Folien bis zu sieben schwarze Unterpixel enthalten kann und erst die $k - te$ Folie Klarheit verschafft.

Nach den Formeln von Moni Naor und Adi Shamir ([1]) würden sich für ein optimales "4 aus 4" -Verfahren die Werte $m = 2^{4-1} = 8$ und $\alpha = \frac{1}{2^{4-1}} = 1/8$ ergeben. Somit gilt: $d = 8$, $w = 8 - 1/8 \cdot 8 = 7$ und $v = 87,5\%$. Verglichen mit unserem Beispiel stimmt dies fast überein, nur dass dort mit einer Unterpixelzahl von $m = 9$ gearbeitet wurde. Acht Unterpixel würden in praktischen Zwecken, wie schon erwähnt, eine Verzerrung des Originalbildes bewirken (siehe nächstes Beispiel).

Wie sehen nun aber konkret die Kollektionen für ein (optimales) "k aus k"-Verfahren aus? Hierfür gibt es viele grundsätzlich verschiedene Varianten. Eine davon wurde direkt von Moni Naor und Adi Shamir ([1]) beschrieben, welche im Folgenden auch direkt erläutert wird. Zur anschaulichen Herleitung wird eine Unterpixelzahl von $m = 2^k$ verwendet, auch wenn die oben erwähnten $2^k - 1$ sogar noch ein wenig effizienter wären.

Wir definieren uns zwei Listen von Vektoren $J_1^0, J_2^0, \ldots, J_k^0$ und $J_1^1, J_2^1, \ldots, J_k^1$ mit der Eigenschaft, dass $J_1^0, J_2^0, \ldots, J_k^0$ Vektoren der Länge k über dem Körper F_2 sind, bei denen $k-1$ linear unabhängig und alle k linear abhängig sind. Ein Beispiel für eine solche Konstruktion liefert $J_i^0 = 0^{i-1}10^{k-i}$ für $1 \leq i \leq k$ und $J_k^0 = 1^{k-1}0$. Für die Liste $J_1^1, J_2^1, \ldots, J_k^1$ gilt ebenso, dass dies Vektoren der Länge k über F_2 sein müssen und zusätzlich aber die lineare Unabhängigkeit sämtlicher Vektoren. Eine einfache Konstruktion ist $J_i^1 = 0^{i-1}10^{k-i}$.
Jeder dieser Liste definiert nun auf folgende Weise eine k x 2^k-Matrix S^t für $t \in \{0, 1\}$:

$S^t[i, c] :=< J_i^t, x_c >$ für $1 \leq i \leq k$ und für *jeden* möglichen Vektor x_c der Länge k über F_2. Es ist schnell ersichtlich, dass für c gelten muss: $c \in \{1, \ldots, 2^k\}$. $<,>$ bezeichnet hierbei das Skalarprodukt über F_2.

Beispiel: $k = 3$

Damit gilt nach obigen Konstruktionen:

$J_i^0 = 0^{i-1}10^{3-i}$ für $1 \leq i < 3$, $\quad J_3^0 = 1^{3-1}0$ und $J_i^1 = 0^{i-1}10^{3-i}$.

Ausgeschrieben bedeutet dies:

$$J_1^0 = \begin{pmatrix} 1 & 0 & 0 \end{pmatrix} \qquad J_2^0 = \begin{pmatrix} 0 & 1 & 0 \end{pmatrix} \qquad J_3^0 = \begin{pmatrix} 1 & 1 & 0 \end{pmatrix}$$

$$J_1^1 = \begin{pmatrix} 1 & 0 & 0 \end{pmatrix} \qquad J_2^1 = \begin{pmatrix} 0 & 1 & 0 \end{pmatrix} \qquad J_3^1 = \begin{pmatrix} 0 & 0 & 1 \end{pmatrix}$$

Für c gilt nun: $c = 2^3 = 8$
Es ergeben sich somit folgende 8 Vektoren (Reihenfolge frei gewählt):

$$x_1 = \begin{pmatrix} 0 & 0 & 0 \end{pmatrix} \qquad x_2 = \begin{pmatrix} 0 & 0 & 1 \end{pmatrix} \qquad x_3 = \begin{pmatrix} 0 & 1 & 0 \end{pmatrix}$$

$$x_4 = \begin{pmatrix} 0 & 1 & 1 \end{pmatrix} \qquad x_5 = \begin{pmatrix} 1 & 0 & 0 \end{pmatrix} \qquad x_6 = \begin{pmatrix} 1 & 0 & 1 \end{pmatrix}$$

$$x_7 = \begin{pmatrix} 1 & 1 & 0 \end{pmatrix} \qquad x_8 = \begin{pmatrix} 1 & 1 & 1 \end{pmatrix}$$

Es folgt für die Matrizen S^0 und S^1:

$S^0[1, c] =< J_1^0, x_c >$

$S^0[2, c] =< J_2^0, x_c > \qquad \longrightarrow S^0 = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \end{pmatrix}$

$S^0[3, c] =< J_3^0, x_c >$

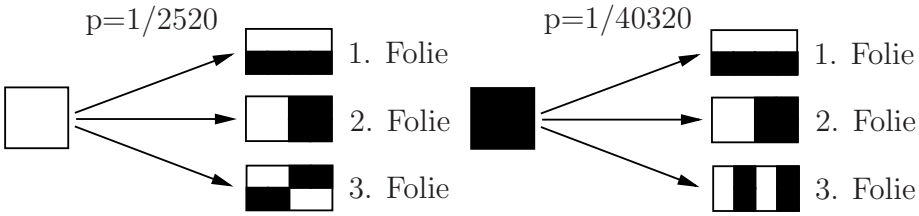
$S^1[1, c] =< J_1^1, x_c >$

$S^1[2, c] =< J_2^1, x_c > \qquad \longrightarrow S^1 = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$

$S^1[3, c] =< J_3^1, x_c >$

Die Kollektionen C_0 und C_1 lassen sich nun aus sämtlichen möglichen Permutationen der Spalten dieser Matrizen erstellen. Für die Größe der Menge C_0 gilt demnach: $r = \frac{8!}{(2!)^4} = 2520$ (Anzahl Permutationen mit Gruppen nicht unterscheidbarer Elemente), wohingegen für C_1 gilt: $r = 8! = 40320$. Tatsächlich können diese Mengen also sehr wohl unterschiedlich groß sein.
Für das Hamming-Gewicht des "oder"-Vektors jeglicher Permutation von S^0 gilt stets $H(V) = 6$, für S^1 hingegen $H(V) = 7$.

Bei Benutzung der Beispielmatrizen (die Wahrscheinlichkeit dafür ist angegeben) sieht die Zuweisung der Unterpixel eines einzelnen schwarzen/weißen Originalpixels wie folgt aus:



Bedingt durch die nicht quadratische Unterpixelzahl wird das Originalbild, wie deutlich ersichtlich, etwas verzerrt dargestellt.
Zusammengefasst ergeben sich für das Beispiel nun folgende Werte:
$k = 3$, $m = 8$, $d = 7$, $w = 6$, $\alpha = 1/8$ und $v = 75\%$.

Satz: Das oben beschriebene Schema für die Erstellung der Kollektionen liefert ein sicheres "k aus k"-Verfahren mit Parametern $m = 2^k$ und $\alpha = 1/2^k$.

Beweis: Die entsprechenden Parameter ergeben sich direkt aus den Formeln (siehe Beispiel). Wichtig ist der Punkt der Sicherheit:
In der Matrix S^0 befinden sich immer zwei Spalten, die nur aus Nullen bestehen. Ausgehend von den Beispielkonstruktionen $J_i^0 = 0^{i-1}10^{k-i}$ für $1 \leq i \leq k$ und $J_k^0 = 1^{k-1}0$ werden diese aus dem Skalarprodukt mit $x_c = 0^k$ bzw. $x_c = 0^{k-1}1$ gebildet. In S^1 befindet sich immer eine Spalte die nur aus Nullen besteht, welche ausgehend von $J_i^1 = 0^{i-1}10^{k-i}$ durch das Skalarprodukt mit $x_c = 0^k$ gebildet wird.

Aus diesem Grund beinhaltet der "oder"-Vektor jeglicher Permutation von S^0 lediglich $2^k - 2$ Einsen, aber der von S^1 stets $2^k - 1$.
Die Vektoren J_i^t, welche für jegliche möglichen $k-1$ Zeilen in S^0 und S^1 stehen, sind stets linear unabhängig. Betrachtet man daher nun die 2^k Spalten in S^0 und S^1, welche sich aus den gewählten $k-1$ Zeilen ergeben, so kommt jede Zuordnung der $k-1$ Einträge der Spalten exakt zweimal vor. Daraus folgt, dass eine zufällige Permutation der Zeilen, wie es zur Erstellung von C_0 und C_1 verwendet wird, stets dieselbe Verteilung ergibt, unabhängig davon, welche $k-1$ Zeilen ausgewählt wurden.

2.3 "k aus n" -Verfahren

Bei einem "k aus n"- secret sharing Verfahren geht es darum ein Geheimnis in n Teile zu teilen, sodass keines für sich Rückschlüsse auf das Original liefern darf. Sobald *mindestens* k beliebige Teile wieder zusammengefügt werden, lässt sich die ursprüngliche Nachricht wieder rekonstruieren, $k-1$ Teile hingegen ergeben nicht den geringsten Anhaltspunkt. Entsprechend den "k aus k" -Verfahren kann diese Variante mit Hilfe der visuellen Kryptographie realisiert werden. Im Gegensatz zu einem "k aus k" -Verfahren der visuellen Kryptographie müssen die Kollektionen C_0 und C_1 aber die folgenden spezielleren Bedingungen erfüllen:

1. Für jede Matrix S^0 in C_0 muss der "oder" -Vektor V von *beliebigen* n der k Zeilen $H(V) \leq d - \alpha \cdot m = w$ genügen.

2. Für jede Matrix S^1 in C_1 muss der "oder" -Vektor V von *beliebigen* n der k Zeilen $H(V) \geq d$ genügen.

3. Ein "k aus n" -Verfahren ist genau dann am sichersten, wenn für jede Teilmenge $\{i_1, ..., i_q\}$ der Folien $\{1, 2, ..., k\}$ mit $q < k$, die daraus entstehenden reduzierten Kollektionen dieselben Matrizen mit derselben Häufigkeit enthalten.

Das nun präsentierte Schema gibt ein Beispiel für ein Verfahren, bei welchem mindestens zwei Teilnehmer notwendig sind um das Geheimnis wieder rekonstruieren zu können:

Beispiel: *"2 aus n "*

Folgende mögliche n x n -Kollektionen erfüllen die Bedingungen:

$$C_0 = \{A \in \{0,1\}^{nxn} \mid A \text{ ist Spaltenpermutation von } \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 1 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 0 & \cdots & 0 \end{pmatrix}\}$$

$$C_1 = \{A \in \{0,1\}^{nxn} \mid A \text{ ist Spaltenpermutation von } \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & & 0 \\ \vdots & \vdots & & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix}\}$$

Es ist schnell ersichtlich, dass jegliche zwei Zeilen einer Matrix aus C_0, welche genau zwei Folien entsprechen, ein Hamming-Gewicht von 1 haben und jegliche zwei Zeilen einer Matrix aus C_1 ein Hamming-Gewicht von 2. Sobald also zwei Folien übereinandergelegt werden, erscheinen ursprüngliche schwarze Pixel dunkler als ursprüngliche weiße Pixel. Je mehr der n Folien wieder zusammengetragen werden, desto deutlicher wird dieser Unterschied und desto klarer das Ergebnis.

"k aus n" -Verfahren benötigen im Allgemeinen eine geringere Unterpixelzahl als "k aus k" -Verfahren. Dies kann man sich leicht überlegen, da es natürlich komplizierter wird das Originalbild zu verbergen, je mehr Folien übereinander gelegt werden *dürfen*. Die gesamten bisher ausführlich beschriebenen Parameter der visuellen Kryptographie sind übertragbar auf "k aus n" -Verfahren. Es existieren bereits zu beiden Formen jede Menge ausführlicher Ausarbeitungen. Neben den sogenannten *klassischen* Verfahren der visuellen Kryptographie ("k aus k" und "k aus n"), entwickelten sich mit der Zeit einige speziellere Varianten. Der folgende Teil liefert einen Einblick in die Erweiterungen der visuellen Kryptographie.

3. Erweiterungen des Konzeptes

Nachdem das allgemeine Konzept der visuellen Kryptographie nun abschließend erläutert wurde, werden in diesem Kapitel einige Erweiterungen des Verfahrens beschrieben. Angefangen mit Teilmengen-Verfahren, über die Verknüpfung zur Steganographie bis hin zu Graustufen und Farbbildern. Die einzelnen Themen werden dabei grundlegend und beispielhaft betrachtet. Auf eine tiefer gehenden Behandlung wird an dieser Stelle bewusst verzichtet, da diese eigenständige Arbeiten füllen könnte.

3.1 Teilmengen-Verfahren

Teilmengenverfahren in der visuellen Kryptographie gestalten sich als sehr interessant, da hier im Gegensatz zu einer festen Schranke bei einem "k aus n" -Verfahren verschiedene und sogar unterschiedlich große Teilmengen der n Folien das Originalbild wiederherstellen können (Stichpunkt "General Access Structures", [3], [4] und [6]). Die Teilnehmer eines Schemas wurden bis jetzt immer als gleichbedeutend behandelt, wohingegen es ja auch sein kann, dass einige Individuen eine höhere Bedeutung haben sollen. Für den Nutzen dahinter kann man sich zum Beispiel vorstellen, dass eine Räuberbande einen Schatz vergräbt, den geheimen Ort auf einer Schatzkarte verzeichnet und diese nun in 4 Teile teilen möchte, damit nicht ein einzelner den Schatz heimlich wieder ausgräbt. Der Räuberboss beschließt, dass entweder er und ein weiterer Räuber oder drei Räuber gemeinsam die Schatzkarte wieder zusammensetzen können. Es würde sich also ein "Räuberboss + 1 oder 3 aus 4" -Verfahren ergeben.
Mit Hilfe der visuellen Kryptographie ließe sich dies nun folgendermaßen bewerkstelligen (vergleiche [9], S.21 ff.):

Angenommen die Räubergruppe setzt sich aus dem Räuberboss Gorlan und den drei anderen Schlitzohren Charles, Henry und Joe zusammen. Zuallererst muss nun überlegt werden, welche der Räuber eine qualifizerte Teilmenge aller Möglichkeiten für die Rekonstruktion des Bildes sind und welche nicht.

Definition:

- $\Gamma := \{1, \ldots, n\}$, die Menge der Teilnehmer
- $\Gamma_{Qual} := \{X \subseteq \mathcal{P}(\Gamma) |$ X soll das Geheimnis rekonstruieren können$\}$
- $\Gamma_{Forb} := \{X \subseteq \mathcal{P}(\Gamma) |$ X darf das Geheimnis nicht rekonstruieren können$\}$

$\mathcal{P}(\Gamma)$ bezeichnet hierbei die Potenzmenge von Γ. Es ist schnell ersichtlich, dass gelten muss: $\Gamma_{Qual} \cap \Gamma_{Forb} = \emptyset$ und $\Gamma_{Qual} \cup \Gamma_{Forb} = \mathcal{P}(\Gamma)$.

Ausgehend von dem oben genannten Beschluss des Räuberbosses ergeben sich unter Festlegung der Nummerierung {Gorlan, Charles, Henry, Joe} := {1, 2, 3, 4} folgende Mengen:

$$\Gamma_{Qual} = \{\{\text{Gorlan, Charles}\}, \{\text{Gorlan, Henry}\}, \{\text{Gorlan, Joe}\}, \{\text{Gorlan, Charles, Henry}\}, \{\text{Gorlan, Charles, Joe}\}, \{\text{Gorlan, Henry, Joe}\}, \{\text{Charles, Henry, Joe}\}, \{\text{Gorlan, Charles, Henry, Joe}\}\}.$$

$$\Gamma_{Forb} = \{\{\text{Gorlan}\}, \{\text{Charles}\}, \{\text{Henry}\}, \{\text{Joe}\}, \{\text{Charles, Henry}\}, \{\text{Charles, Joe}\}, \{\text{Henry, Joe}\}, \{\emptyset\}\}.$$

Die leere Menge ist nur der Vollständigkeit wegen aufgelistet, wird aber im Folgenden nicht weiter beachtet.
Einige dieser Mengen können nun gestrichen werden, da sich ihre Bedeutung wiederholt. Wenn {Gorlan, Charles} eine qualifizierte Teilmenge ist, so ist es {Gorlan, Charles, Joe} erst recht. Genauso für {Charles} und {Charles, Henry}. Wenn Charles und Henry zusammen das Geheimnis nicht rekonstruieren können, dann kann es Charles alleine erst recht nicht.

Die zusammengefassten *minimalen* bzw. *maximalen* Mengen sehen nun so aus:

$$\Gamma_{Qual^{min}} = \{\{\text{Gorlan, Charles}\}, \{\text{Gorlan, Henry}\}, \{\text{Gorlan, Joe}\}, \{\text{Charles, Henry, Joe}\}\}.$$

$$\Gamma_{Forb^{max}} = \{\{\text{Gorlan}\}, \{\text{Charles, Henry}\}, \{\text{Charles, Joe}\}, \{\text{Henry, Joe}\}\}.$$

Übersetzt in die oben genannte Zuordnung:

$$\Gamma_{Qual^{min}} = \{\{1, 2\}, \{1, 3\}, \{1, 4\}, \{2, 3, 4\}\}.$$

$$\Gamma_{Forb^{max}} = \{\{1\}, \{2, 3\}, \{2, 4\}, \{3, 4\}\}.$$

Für den weiteren Verlauf ist es nötig *cumulative arrays* zu betrachten, welche in [3], S.8 ff., ausgiebiger beschrieben werden (Herleitung über die *cumulative map*). Es wird sich an diesem Punkt auf die Definition und die Bedeutung für das Teilmengenverfahren beschränkt, da hier nur die grundlegende Vorgehensweise des Schemas erläutert werden soll. Es existieren aber weiterhin auch andere mögliche Wege zur Realisierung des Verfahrens.

Definition: Sei $\Gamma_{Forb^{max}} = \{X_1, \ldots, X_t\}$ wie oben beschrieben die Menge der maximal verbotenen Teilmengen. Ein *cumulative array* ist eine $|\Gamma|$ x t Matrix, genannt CA, mit der Eigenschaft, dass $CA(i, j) = 1 \Leftrightarrow i \notin X_j$.

Mit $\Gamma_{Forb^{max}} = \{\{1\}, \{2, 3\}, \{2, 4\}, \{3, 4\}\}$ ergibt sich also:

$$CA = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \end{pmatrix}$$

Des Weiteren benötigen wir nun zwei Basismatrizen S^0 und S^1 eines “t aus t” -Verfahrens, welche dann mit Hilfe der Matrix CA zu den benötigten Basismatrizen $\hat{S}^0$ und $\hat{S}^1$ dieses Teilmengenverfahrens angepasst werden.

In unserem Beispiel ist $t = 4$ und unter Verwendung des in Kapitel 2.2 beschriebenen Schemas zur Herstellung der Kollektionen C_0 und C_1 lassen sich damit folgende 4 x 16 Basismatrizen konstruieren:

$$S^0 = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}$$

$$S^1 = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

Die angepassten Matrizen ergeben sich nun auf folgende Weise: Für jede vorkommende 1 in jeder der i Zeilen der Matrix $CA(i, j)$, merke dir die Nummer der Spalte. Die i-te Zeile der Matrizen $\hat{S}^0$ und $\hat{S}^1$ ist dann gleich dem "oder" -Vektor der Zeilen $\{1, \ldots, k\}$ der Matrizen S^0 und S^1, deren Nummern den Spalten j_k der i-ten Zeile von CA entsprechen, in welchen eine 1 gestanden hat.

Das Ganze sieht dann so aus:

$$\hat{S}^0 = \begin{pmatrix} 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

$$\hat{S}^1 = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

Mit Hilfe dieser Basismatrizen und sämtlichen Permutationen lassen sich nun die Kollektionen C_0 und C_1 für das Teilmengenverfahren erstellen. Die Folien {1} ,{2, 3}, {2, 4} und {3, 4} reichen nicht aus das ursprüngliche Bild wiederherzustellen, wohingegen {1, 2}, {1, 3}, {1, 4} und {1, 2 ,3} zusammengefügt das Geheimnis lüften können.

Der Trick, welcher dies möglich macht ist, dass durch die Verwendung des *cumulative arrays* jeder maximal verbotenen Teilmenge eine "Folie" eines "k aus k" -Verfahrens zugeordnet wird und jeder Teilnehmer genau die Kombination an Folien der maximal verbotenen Teilmengen bekommt, in welchen er nicht enthalten ist. Auf diese Weise können nur die speziellen zugelassenen Teilmengen die Rekonstruktion des Originalbildes durchführen.

3.2 Steganographie und visuelle Kryptographie

Die Steganographie bezeichnet die Kunst der Verbergung der bloßen Existenz von geheimen Nachrichten, welche sich meist versteckt hinter einem offensichtlichen Medium befinden. Ein Dritter sieht zwar, dass unscheinbare Information übertragen wird, aber erkennt bei einem sicheren steganographischen Verfahren nicht, ob sich noch eine relevante geheime Nachricht dahinter verbirgt. Selbst wenn dieser weiß, dass sich dort noch geheime Informationen befinden, darf er nicht in der Lage sein, diese zu offenbaren.
Ein einfaches Beispiel hierfür ist eine Nachricht hinter der Konkatenation jedes ersten Buchstaben der Wörter eines Satzes zu verstecken:

Tristam **r**echnet **e**inigermaßen **f**leißig **f**ür **e**ine **n**otwendige **U**eberpruefung **m**athematischer **F**aehigkeiten **u**nd **e**rhaelt **n**eues **F**achwissen.

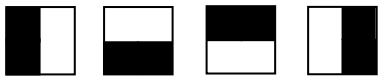
Die geheime Nachricht lautet: **T r e f f e n U m F u e n F**

Dies ist aber ein eher simples, wenn auch aufwendiges, steganographisches Verfahren und es bedarf nicht viel Technik dieses zu lösen, sofern die Existenz der zusätzlichen Information entdeckt wurde. Weitaus komplexer ist zum Beispiel eine unterschwellige Tonspur in Audiodateien oder die Verbergung eines geheimen Bildes hinter den Bildpunkten eines offensichtlichen.

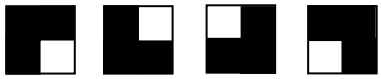
Nach dieser Idee kann auch in der visuellen Kryptographie mit der Steganographie gearbeitet werden und jeder Folie und sogar beliebigen Teilmengen von Folien jeweils ein unterschiedliches Bild gegeben werden, welches nicht im Geringsten etwas mit dem Originalbild zu tun haben.

Das macht es für Dritte schwieriger herauszufinden, ob eine sich im Besitz befindene Folie Teil eines secret sharing -Verfahren ist, welches der sich ergebenden Bilder aus mehreren Folien denn das Originalbild sein soll bzw. ob überhaupt eine geheime Information "eingebettet" ist.
Um dieses Vorgehen verständlich zu verdeutlichen, betrachten wir beispielhaft ein einfaches "2 aus 2" -Verfahren mit vier Unterpixeln, bei der auf jeder der beiden Folien ein anderes Bild zu sehen sein soll und mit den zusammengefügten Folien das Originalbild. Folgende Konstruktionsregeln müssen beachtet werden (vergleiche [7], S.89/90):

- Soll auf einer Folie (!) ein Pixel als weiß interpretiert werden, so kann er durch eine der folgenden vier möglichen Unterpixelkombinationen ersetzt werden:



- Ebenso für die gewünschte Interpretation eines schwarzen Pixels eine dieser vier möglichen Unterpixelkombinationen:



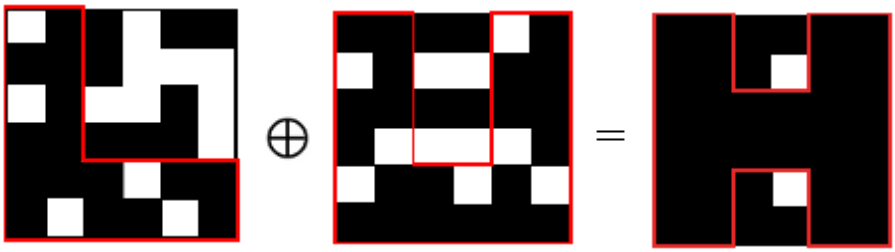
- Ist das Originalbild an der Stelle des betrachteten Pixels schwarz, so muss die gewählte Kombination der Folien beim Zusammenfügen vier schwarze Unterpixel ergeben. Bei einem weißen Originalpixel müssen es drei schwarze und ein weißer Unterpixel sein.

Die möglichen zulässigen Kombinationen hierfür lassen sich schnell herausfinden, weswegen an dieser Stelle auf eine komplette Auflistung verzichtet wird. Das folgende Beispiel sollte das Schema aber verdeutlichen.

Angenommen es soll das aus neun (sehr großen) Pixeln bestehende Bild "**H**" kodiert werden:

Auf der ersten Folie soll nun ein “**L**” gelesen werden, auf der zweiten ein “**U**” und auf der kombinierten wieder das “**H**” zu erkennen sein. Nach der oben stehenden Konstruktion wird für jeden Pixel und für jede Folie, entsprechend den gewünschten zu erkennenden Pixeln auf den einzelnen Folien, zufällig eine der vier Möglichkeiten für die Unterpixel auf der ersten Folie gewählt und dazu passend die Unterpixel für die zweite Folie. Drei schwarze Unterpixel und ein weißer auf den *einzelnen Folien* werden als schwarz interpretiert und zwei weiße und zwei schwarze als weiß. Auf der zusammengefügten Folie sind es hingegen vier schwarze Unterpixel für schwarz und drei für weiß.

Das Ganze könnte dann zum Beispiel so aussehen (die rote Umrandung verdeutlicht die Einzelbilder):



Die Pixel des “**L**” und des “**U**” erscheinen hier dunkler als die Umgebung. Bei normal üblichen, weitaus größeren Pixelzahlen für Bilder, würden die Teilbilder entsprechend besser zu erkennen sein. Hier wurde aber Wert auf den Bezug zur anschaulichen Pixelsubstitution gelegt.
Eine Verwendung von Teilbildern kann in der visuellen Kryptographie auch auf weitaus mehr als zwei Folien bzw. n Folien ausgedehnt werden, bei denen beliebige Teilmengen der Folien unterschiedliche Bilder zeigen.

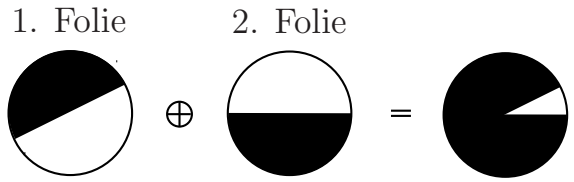
S. Droste führte dies bereits 1998 in seiner Arbeit "New Results on Visual Cryptography" genauer aus und erweiterte das klassische Verfahren unter Benutzung speziellerer Algorithmen, die sich vom oben genannten Beispielschema für $k = 2$ von A. Klein entsprechend unterscheiden.

3.3 Graustufen

Als Graustufen bezeichnet man die Stufenintervalle zwischen reinem Weiß und reinem Schwarz. Sämtliche bisher beschriebene Verfahren der visuellen Kryptographie basieren auf einem schwarzweißen Originalbild, bei welchem nur rein schwarze und rein weiße Pixel substituiert werden können. Diese Erweiterung bietet die Möglichkeit der Verschlüsselung von komplizierteren Bildern, die sich aus mehreren Graustufen zusammensetzen.
Es existieren einige unterschiedliche Varianten dies zu realisieren. So wurde von Moni Naor und Adi Shamir ([1]) bereits 1994 ein Verfahren beschrieben, welches statt mit rechteckig angeordneten Pixeln mit rotierenden Halbkreisen arbeitet. Unterschiedlich gedreht und übereinandergelegt lassen sich auf diese Weise, bestimmt durch den entstehenden Winkel :=Θ, beliebige Grauwerte zwischen 50% und 100% Schwärze realisieren. Folgende Tabelle verdeutlicht dies:

Θ	0°	18°	36°	54°	72°	90°	108°	126°	144°	162°	180°
%	100	95	90	85	80	75	70	65	60	55	50

Beispiel:



Hier ergibt sich ein Winkel von ca. 36°. Dies entspricht einer Schwärze des Kreises von ungefähr 90% und steht daher für einen relativ dunklen Grauwert.

Wenn nun für jeden Pixel zufällig eine Rotation des Halbkreises für die erste Folie gewählt wird und man die zweite Folie entsprechend dem gewünschten Grauwert angleicht, dann enthalten die einzelnen Folien keinerlei Informationen über das Originalbild. Aber zusammengefügt entsteht wieder das verschlüsselte Graustufenbild.
Es ist natürlich möglich, diese Idee mit einer beliebigen Anzahl an Folien durchzuführen. Praktisch gesehen ist dieses Verfahren aber viel zu aufwendig zu realisieren, da durch die nötige Kreisform der Substitutionen verhältnismäßig viel mehr Unterpixel überhaupt zur Darstellung des Kreises benötigt werden als bei anderen Lösungen.
Eine andere Möglichkeit von A. Klein [7] für Graustufenbilder liefert eine relativ simple Methode, bei der aber nur von maximal fünf möglichen Graustufen (0%, 25%, 50%, 75% und 100% Schwärze) ausgegangen wird. Jeder Pixel wird, bereits vor der eigentlichen Verschlüsselung auf den Folien, entsprechend seines Grauwertes in vier quadratisch angeordnete Unterpixel aufgeteilt:

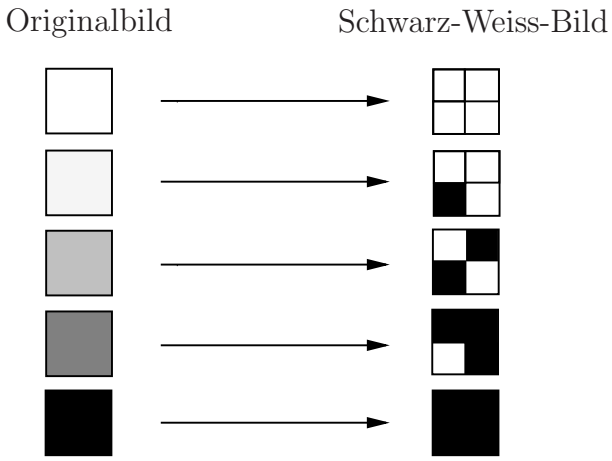


Bild nach [7], Seite 111.

Die links stehenden Graustufen symbolisieren die einzelnen, oben angegebenen 25%-Intervalle. Mit dem so entstehenden Schwarz-Weiß-Bild kann dann, wie mit allen bisherigen Bildern, gearbeitet werden. Die einzelnen schwarzen und weißen (Unter-)Pixel werden gemäß der Basimatrix eines beliebigen Verfahrens der visuellen Kryptographie auf den einzelnen Folien erneut in weitere Unterpixel unterteilt.

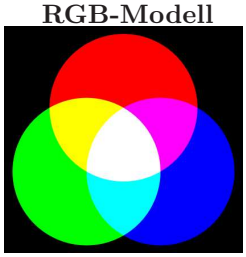
Der Nachteil zum vorherigen Verfahren ist, dass nicht einfach beliebige Grauwerte verarbeitet können, sondern immer nur bestimmte Prozentteile. Bei mehr als vier Unterpixeln wäre aber auch hier eine feinere Einteilung möglich. Des Weiteren muss man das Originalbild erst bearbeiten bevor man es mit Hilfe eines Verfahrens der visuellen Kryptographie verschlüsseln kann.

Einige der weiteren Verfahren, welche mit der Zeit entwickelt wurden (vergleiche [5]), arbeiten mit einer eigenen, separaten Basismatrix für jede einzelne Graustufe. Die Komplexität der Verarbeitung steigt aber auch hier mit der Zahl der gewünschten Stufen. Generell ist es weitaus effizienter nur Schwarz-Weiß-Bilder zu betrachten, da der mögliche erhöhte Informationsgehalt des Originalbildes durch das Hinzufügen von Graustufen sowieso nur sehr gering ist. Etwas Anderes ist es wenn es um Farben geht.

3.4 Farbbilder

Um Farbbilder in der visuellen Kryptographie zu realisieren, benötigt man etwas Verständnis über die additive und die subtraktiven Farbmischung. Additive Farbmischung beschreibt die Veränderung der Wahrnehmung einer Farbe bei sukzessiver Hinzunahme (Addition) von Spektralbereichen verschiedener Farben. Die Primärfarben sind hierbei Rot, Grün und Blau:

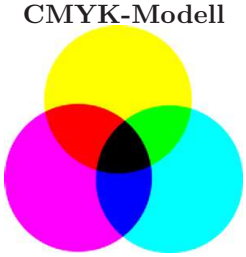
RGB-Modell



Dieses Modell kommt unter anderem bei Bildschirmen, der Digitalfotografie oder im menschlichen Auge zur Anwendung. Bei der Addition sämtlicher drei Primärfarben ergibt sich weiß, während die Addition von immer nur zwei Primärfarben die Mischfarben Cyan, Magenta und Gelb sichtbar werden lässt, welche die Grundfarben für das CMYK-Modell der subtraktiven Farbmischung liefern (vergleiche nächstes Bild).

Im Gebiet der subtraktiven Farbmischung werden Spektralbereiche einzelner Farben ausgeblendet (Subtrahiert) und dadurch eine andere Farbwahrnehmung erreicht.

CMYK-Modell



Die drei verwendeten Primärfarben Cyan, Magenta und Gelb können sich wie Farbfilter vorgestellt werden, welche den entsprechenden Spektralbereich, ausgehend von Weiß, ausblenden. So entsteht durch Subtraktion sämtlicher Primärfarben, beziehungsweise dem Übereinanderlegen der Farbfilter, Schwarz und bei nur jeweils zwei der Primärfarben die Grundfarben Rot, Grün und Blau der Additiven Farbmischung. Das CMYK-Modell lässt sich unter anderem bei Druckern wiederfinden.

Beide dieser Verfahren finden nun in der farbigen visuellen Kryptographie ihren Einsatz. Werden zwei Folien mit unterschiedlich farbigen Unterpixeln übereinander gelegt, dann ist dies eine subtraktive Farbmischung. Liegen auf einer Folie mehrere unterschiedlich farbige Unterpixel nebeneinander, so entsteht aus der Entfernung betrachtet ein Farbgemisch beziehungsweise eine andere Farbe. Dies beruht auf der additiven Farbmischung.
Die grundlegende Idee hinter der farbigen visuellen Kryptographie sollte damit schon klar werden. Ähnlich, wie die in Kapitel 3.3 erläuterten Kreise von Moni Naor und Adi Shamir ([1]), gibt es auch hier die Variante, welche bereits 1997 von Verheul und Tilborg aufgefasst wurde ([10]), Kreise in gleich große Segmente zu unterteilen und die einzelnen Kreisausschnitte mit (unterschiedlichen) Farben zu belegen. Sämtliche Farbbereiche die beim Übereinanderlegen der Folien nicht für die gewünschte, zu erkennende Farbe an dieser Stelle nötig sind, werden durch schwarze Segmente überlagert, wohingegen die richtige Farbe überall erhalten bleibt.

Der Nachteil besteht hierbei, genauso wie bei den Graustufen, in der Schwierigkeit der genügenden Darstellung der Kreise durch wenige Pixel.
Es existieren auch unter der Berücksichtigung von Farben wieder mehrere Möglichkeiten die Verschlüsselung umzusetzen. Eine anschauliche Variante von A. Klein, [7] und [8], arbeitet mit den oben beschriebenen Farbmodellen und der bekannten rechteckigen Anordnung von Unterpixeln. Da eine Farbe des Originalbildes nach diesem Schema, ähnlich wie der Kontrastverlust bei dem Weiß eines Schwarz-Weiß-Bildes nicht 100%ig rekonstruiert werden kann, benutzt er das folgende System zur Feststellung der Güte eines Verfahrens:

Definition: Für zwei Farben a und b seien der rote, grüne und blaue Anteil (a_1, a_2, a_3) bzw. (b_1, b_2, b_3), wobei gilt: a_i, $b_i \in$ [0,1] (Weiß ist z.B. daher gleich (1, 1, 1) und Rot gleich (1, 0, 0)). Der Abstand der Farben a und b ist definiert durch:

$$d(a, b) = (|a_1 - b_1|, |a_2 - b_2|, |a_3 - b_3|).$$

Die Güte des Systems ist gleich den Abständen, der durch die additive Farbmischung entstehenden Farben und der Originalfarbe. Seien nun a^{F_c} die Originalfarben und b^{F_c} die Darstellungen dieser Farben in einem Schema, dann bezeichnet

$$A = \sum_{c=1}^{k} |a_1^{F_c} - b_1^{F_c}| + |a_2^{F_c} - b_2^{F_c}| + |a_3^{F_c} - b_3^{F_c}|$$

die Abweichung des Schemas vom Sollwert. Ein System heißt optimal, wenn kein anderes System existiert, das eine geringere Abweichung hat.

Ein Verfahren, in welchem sich alle acht Primärfarben der Farbmodelle (Rot, Grün, Blau, Cyan, Magenta, Gelb, Schwarz und Weiß) wiederfinden lassen, mit denen nahezu sämtliche Farben realisiert werden können, benötigt mindestens 8 Unterpixel, für jede Farbe einen. Folgendermaßen *könnte* dies mit zwei Folien realisiert werden:

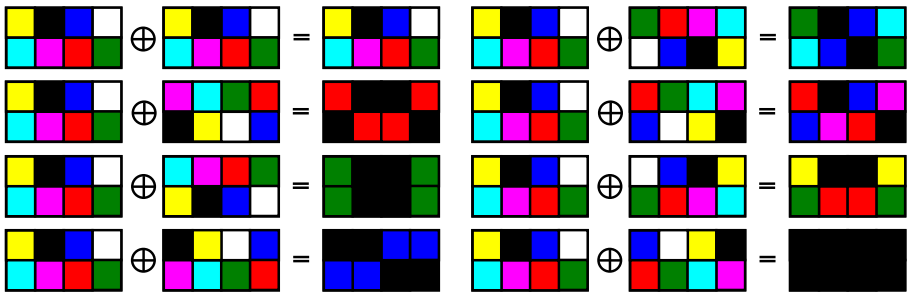


Bild nach [7], S.123

Die entsprechenden RGB-Anteile der codierten Farben können der folgenden Tabelle entnommen werden (die Reihenfolge der Farben ist hierbei beibehalten):

Farbe	Weiß	Rot	Grün	Blau	Cyan	Mag.	Gelb	Schw.
Soll	(1,1,1)	(1,0,0)	(0,1,0)	(0,0,1)	(0,1,1)	(1,0,1)	(1,1,0)	(0,0,0)
Ist	$(\frac{1}{2},\frac{1}{2},\frac{1}{2})$	$(\frac{1}{2},0,0)$	$(0,\frac{1}{2},0)$	$(0,0,\frac{1}{2})$	$(0,\frac{1}{2},\frac{1}{2})$	$(\frac{1}{2},0,\frac{1}{2})$	$(\frac{1}{2},\frac{1}{2},0)$	(0,0,0)
Abst.	$3 \cdot \frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	1	1	1	0

Es lässt sich also eine Abweichung von $A = 3 \cdot \frac{1}{2} + \frac{1}{2} + \frac{1}{2} + \frac{1}{2} + 1 + 1 + 1 = 6$ errechnen. Dieses Schema ist damit optimal. Der Beweis hierzu geht über ein Optimierungsverfahren (vergleiche [7], S.120-122) mit einer größeren Menge an Variablen und kann hier daher nicht weiter ausgeführt werden. Die allgemeine Funktionsweise für farbige visuelle Kryptographie sollte dennoch anschaulich nachvollziehbar sein.
Die Konstruktionen für farbige Originalbilder hängen immer stark von den notwendigen Farben ab und können daher sehr unterschiedlich ausfallen. Angelehnt an die oben stehende Definition wird es aber immer eine optimale Lösung hinsichtlich der minimalen Farbabweichung geben. Ob diese nun anschließend praktikabel und effizient umsetztbar sein kann, ist eine andere Sache.

Die farbige visuelle Kryptographie war das Letzte der in dieser Arbeit behandelten Erweiterungen der visuellen Kryptographie. Die beschriebenen Verfahren zählen zu den grundlegenden Ergänzungen des klassischen Verfahrens.

4. Ausblick

Dieses Kapitel soll abschließend ein Verständnis dafür schaffen, wie es mit der Anwendung der visuellen Kryptographie in der Realität aussieht. Unter diesem Gesichtspunkt wird auf die Vor- und Nachteile eingegangen, wobei ein wichtiger Aspekt, der Betrug, noch etwas genauer behandelt wird. Zu guter Letzt wird zusammenfassend ein Ausblick auf die mögliche weitere Entwicklung gegeben.

4.1 Verwendbarkeit

Die visuelle Kryptographie ist eine Spezialisierung der schon etwas länger existierenden Thematik des *secret sharings* und generell nur ein sehr theoretisches Konzept. Zu heutiger Zeit findet es praktisch gesehen keine wirkliche Verwendung und könnte höchstens in sehr extremen Momenten als Einsatz zur Verschlüsselung von Daten in Erwägung gezogen werden. Sofern ein Computer vorhanden ist, wie zum Beispiel ein PC, Laptop oder Handy, sollte die Realisierung immer mit Hilfe standardmäßiger, moderner und komplizierter kryptographischer Verfahren geschehen.
Eine theoretische Möglichkeit wäre es aber die Folien bzw. Protokolle zum Beispiel für die Authentifizierung und Identifizierung von Nutzern zu verwenden (siehe *Visual Authentication and Identification*, [10]). Auch A. Klein ([7]) beschreibt häufig eine Anwendung bei Warenautomaten, die mit EC-Kartenbezahlung arbeiten. Hier könnte zur Bestätigung einer Abbuchung für den Kunden stets eine Übereinstimmung der Kaufsumme mit dem Bild von zusammengefügten Folien durchgeführt werden, wobei eine Folie vom Display des Automaten angezeigt und die andere vom Nutzer bei sich getragen wird. Dies könnte dem Betrug einer manipulierten höheren Abbuchung entgegen wirken, hat aber auch seine Schwächen (vergleiche [7], S. 3-5).
Neben der Sicherheit gegen vorzeitige Rekonstruktionen von verschlüsselten Geheimbildern, hohem Kontrast und niedrigen Pixelexpansionen gibt es noch einen weiteren Punkt, um den man sich einige Gedanken machen muss:

4.2 Cheating

Cheating bezeichnet das Betrügen eines oder mehrerer Teilnehmer eines Verfahrens der visuellen Kryptographie. Dabei werden entsprechende, sich im Besitz befindene Folien der cheatenden Teilnehmer dahingegend manipuliert, dass das Originalbild selbst mit sämtlichen Folien aller Teilnehmer nicht mehr rekonstruierbar ist oder ein ganz anderes Bild erscheint. Bisher wurde immer davon ausgegangen, dass alle Teilnehmer eines Verfahrens ehrlich sind, aber das lässt sich natürlich nicht verallgemeinern.

Ein durchgeführter Betrugsversuch gilt als erfolgreich, wenn er erst gar nicht entdeckt wird oder aber der entsprechende Verursacher selbst mit allen Mitteln nicht identifiziert werden kann.
Als Beispiel könnte man sich ein "$k-1$ aus k" -Verfahren vorstellen, bei welchem $k-1$ Teilnehmer das Geheimnis rekonstruieren und anschließend die fehlende k-te Folie algorithmisch bestimmen. Nun könnten sie ihre Folien anpassen und ein vollkommen anderes Bild bei Hinzunahme des k-ten Teilnehmers erzeugen.

Cheating ist ein allgemeines Problem des *secret sharings* und somit auch der visuellen Kryptographie. Eine gewollte Manipulation ist dabei auf einige Konstruktionen besser und auf andere schlechter anwendbar. Entscheidend ist deswegen zusätzlich die Cheating-Resistenz eines Verfahrens gegen eventuelle Manipulierversuche. Mit der Zeit wurden dabei dahingehend viele verschiedene Verfahren entwickelt, welche teils sogar komplett geschützt gegen erfolgreiche Cheating-Angriffe sind. Es hat sich heraus gestellt, dass, ähnlich der Sicherheit eines Verfahrens (vergleiche Kapitel 2.2), ein hoher Kontrast zwischen schwarzen und weißen Pixeln bzw. eine geringe Anzahl Unterpixel anfälliger für Cheating sind als Entwürfe, in denen die Werte entsprechend anders sind. Dies sind aber genau die Punkte, auf den viele Verfahren hin optimiert wurden. Für eine praktische Anwendung sollte daher stets die höchste mögliche Sicherheit und Cheating-Resistenz gewährleistet sein.

4.3 Fazit

Die Idee der visuellen Kryptographie ist zwar in einigen Bereichen nur sehr theoretisch, dafür im Allgemeinen wirklich anschaulich und greifbar. Das Grundkonzept lässt sich schnell nachvollziehen und wirklich jeder ist in der Lage zwei transparente Pixelfolien übereinander zu legen und über das Ergebnis zu staunen. Sobald es aber in den Bereich der Optimierung von Konstruktionen bezüglich der Unterpixelzahl, dem maximalen Kontrast und ähnlichem, verbesserten Algorithmen für bestimmte n und k Werte oder erweiterte Verfahren geht, konnten diese Punkte viele Wissenschaftler des Forschungsgebiets über Jahre beschäftigen und werden dies auch weiterhin tun. Das Potential ist noch lange nicht ausgeschöpft.

5. Literaturverzeichnis

[1] Moni Naor and Adi Shamir. Visual Cryptography. *Advances in Cryptology - Eurocrypt '94*, Vol. 950 of Lecture Notes in Computer Science: 1-12, 1995

[2] Stefan Droste. New Results on Visual Cryptography. *Lecture Notes on Computer Science*, Vol. 1109:401-415, 1996.

[3] Giuseppe Ateniese, Carlo Blundo, Alfredo De Santis, Douglas R. Stinson. Visual Cryptography for General Access Structures. *Information and Computation*, Vol. 129, No. 2:86-106, 1996.

[4] Giuseppe Ateniese, Carlo Blundo, Alfredo De Santis, Douglas R. Stinson. Extended Schemes for Visual Cryptography. *Theoretical Computer Science*. 1996.

[5] Alfredo de Santis Carlo Blundo and Moni Naor. Visual cryptography for grey level images. *Information Processing Letters 75*, pages 255-259, 2000.

[6] Jim Cai. A Short Survey on Visual Cryptography Schemes, 2004 *http://www.cs.toronto.edu/∼jcai/paper.pdf* : 28.08.2011

[7] Andreas Klein. *Visuelle Kryptographie*. Springer, 2007.

[8] Andreas Klein. Farbige visuelle Kryptographie. *Mathematisch Schriften Kassel*, 2001.

[9] Martin Apel. Visuelle Kryptographie, 2007. *http://www.informatik.hu-berlin .de/forschung/gebiete/algorithmenII/Lehre/abschlussarbeiten/visuellekryptografie.pdf* : 28.08.2011

[10] E. R. Verheul and H. C. A. Van Tilborg. Constructions and Properties of k out of n Visual Secret Sharing Schemes. *Designs, Codes and Cryptography*, 11:179-196, 1997.

[11] Moni Naor und Benny Pinkas. Visual Authentication and Identification. *Advances in Cryptology - Crypto '97 Proceedings*, 1294:322-336, 1997.