TECHNISCHE UNIVERSITÄT CHEMNITZ

Fakultät für Informatik

Professur Theoretische Informatik und Informationssicherheit

Bachelorarbeit

Farbige Visuelle Kryptographie

Marie Herold

Chemnitz, den 13. Dezember 2013

Gutachter: Prof. Dr. Hanno Lefmann
Dipl.-Math. Knut Odermann

Inhaltsverzeichnis

1 Einleitung

Im heutigen Computerzeitalter, wo das Internet alltäglich und kaum mehr wegzudenken ist, wird der Wunsch nach Schutz und Sicherheit in der virtuellen Welt immer größer. Im Jahr 2011 alleine nutzten 44% der deutschen Bevölkerung das Online-Banking. [ban13] Was für unsereins bequem und praktisch ist, hört sich jedoch für viele Kriminelle umso verlockender an. Glücklicherweise gibt es jedoch die Kryptographie.
Was anfänglich als Wissenschaft der Verschlüsselung von Informationen bezeichnet wurde, behandelt heutzutage in erster Linie das Thema der Informationssicherheit, also das Entwerfen und Fertigen von abwehrfähigen Informationssystemen gegenüber unbefugtem Lesen und Verändern. Ursprünglich aus der altgriechischen Sprache stammend (kryptós = verborgen/geheim & gráphein = schreiben), fand die Kryptographie bereits im dritten Jahrtausend vor Christus ihren ersten Einsatz. [kry]

Der Kern dieser Bachelorarbeit befasst sich jedoch weniger mit der Kryptographie im Allgemeinen, sondern vielmehr mit einem ihrer Teilgebiete: der *farbigen visuellen Kryptographie*.

Das Grundkonzept jedes Kryptographieverfahrens ist es, einen lesbaren Text (Klartext) mit Hilfe eines geheimen Schlüssels in einen unlesbaren/unsinnigen Zustand (Geheimtext) umzuwandeln. Nur wer den geheimen Schlüssel kennt und weiß, wie das genutzte Verfahren funktioniert, ist in der Lage, die ursprüngliche Information aus dem Geheimtext zurück zu erlangen. [kry]
Der wesentliche Unterschied bei der visuellen Kryptographie ist der, dass die zu verschlüsselnde Information nicht in Form von Zahlen oder Buchstaben vorliegt, sondern in Form von Pixeln. Einfach gesagt: visuelle Kryptographie ist die Co- und Decodierung von Bildern. [Nao94] [Kle07] Das vorangehende Wort „farbige“ bedeutet nur, dass die Codierung über Schwarz und Weiß hinaus geht. Es handelt sich also um die Verschlüsselung von Farbbildern.
Das offiziell erste visuelle Verschlüsselungsverfahren wurde 1994 von Moni Naor und Adi Shamir erfunden. [Nao94] Es handelt sich also um einen verhältnismäßig jungen Zweig der Kryptographie.

Im Rahmen dieser Arbeit werden als Einführung in die Materie zunächst einige einfache Kryptosysteme vorgestellt. Anschließend folgt der Hauptteil, in dem als erstes das Grundkonzept der visuellen Kryptographie nur mit Schwarzweißbildern (anhand eines simplen Verfahrens) erklärt wird. Dies dient der Verständlichkeit, um danach den zweiten Abschnitt des Hauptteils, welcher sich mit der farbigen visuellen Kryptographie beschäftigt und somit den Kern dieser Arbeit darstellt, besser verstehen zu können. Abschließend werden danach noch einige Anwendungen der (farbigen) visuellen Kryptographie, sowie die Übertragung auf Töne erläutert, bevor diese Arbeit mit dem Schlusswort endet.

2 Einfache Kryptosysteme

Dieser Abschnitt gibt einen kurzen ersten Einblick in die umfangreiche Welt der Kryptographie. Anhand einiger einfacher Kryptosysteme soll dem Leser zunächst die Vielfalt der Möglichkeiten, Informationen zu verschlüsseln, etwas näher gebracht werden, bevor anschließend speziell zur Codierung von Schwarzweiß- und Farbbildern übergegangen wird.

2.1 Caesar-Chiffre

Als eines der einfachsten Kryptosysteme ist die Caesar-Chiffre (auch als Caesar-Verschlüsselung oder Caesar-Algorithmus bekannt) perfekt geeignet, um das Grundprinzip der Kryptographie zu verdeutlichen. Benannt wurde sie nach dem berühmten römischen Feldherrn Gaius Julius Caesar, der diese Methode bereits im ersten Jahrhundert vor Christus zur Überbringung seiner militärischen Nachrichten nutzte. [Kle07]

Die Funktionsweise dieses Verfahrens ist leicht erklärt: der Klartext ist eine Botschaft, die aus den 26 Buchstaben des Alphabets zusammengesetzt ist. Als Schlüssel wählt man eine beliebige natürliche Zahl und um den Klartext zu verschlüsseln verschiebt man jeden Buchstaben chronologisch (also nach rechts) um die gewählte Anzahl an Stellen, wobei man nach Z stets wieder vorne bei A anfängt. Um die verschlüsselte Botschaft wieder zu entschlüsseln, verschiebt man die Buchstaben einfach wieder um die entsprechende Anzahl an Stellen zurück (also nach links). [Kle07]

Ein Beispiel:

- Die zu codierende Botschaft ist *„HALLO WELT“*.
- Als Schlüssel wählen wir *8*, also wird aus A -> I, aus B -> J, aus C -> K etc.
- Folglich ist unsere Geheimbotschaft *“PITTW EMTB“*.

In der Regel ist es jedoch so, dass die einfachsten Verfahren auch am leichtesten zu knacken sind. Die Caesar-Chiffre ist da keine Ausnahme. In fast allen Sprachen gibt es einen am häufigsten auftauchenden Buchstaben, wie zum Beispiel im Deutschen das *E*. Indem man nun in dem Geheimtext den häufigsten Buchstaben sucht, kann man so oftmals ohne Raten und Probieren den Code entschlüsseln. Und selbst wenn es keinen herausstechenden Buchstaben gibt, so ist die Anzahl an möglichen Schlüsseln doch sehr begrenzt (nur Verschiebungen um 1 bis 25 Stellen machbar). [Kle07]

2.2 Buch-Code

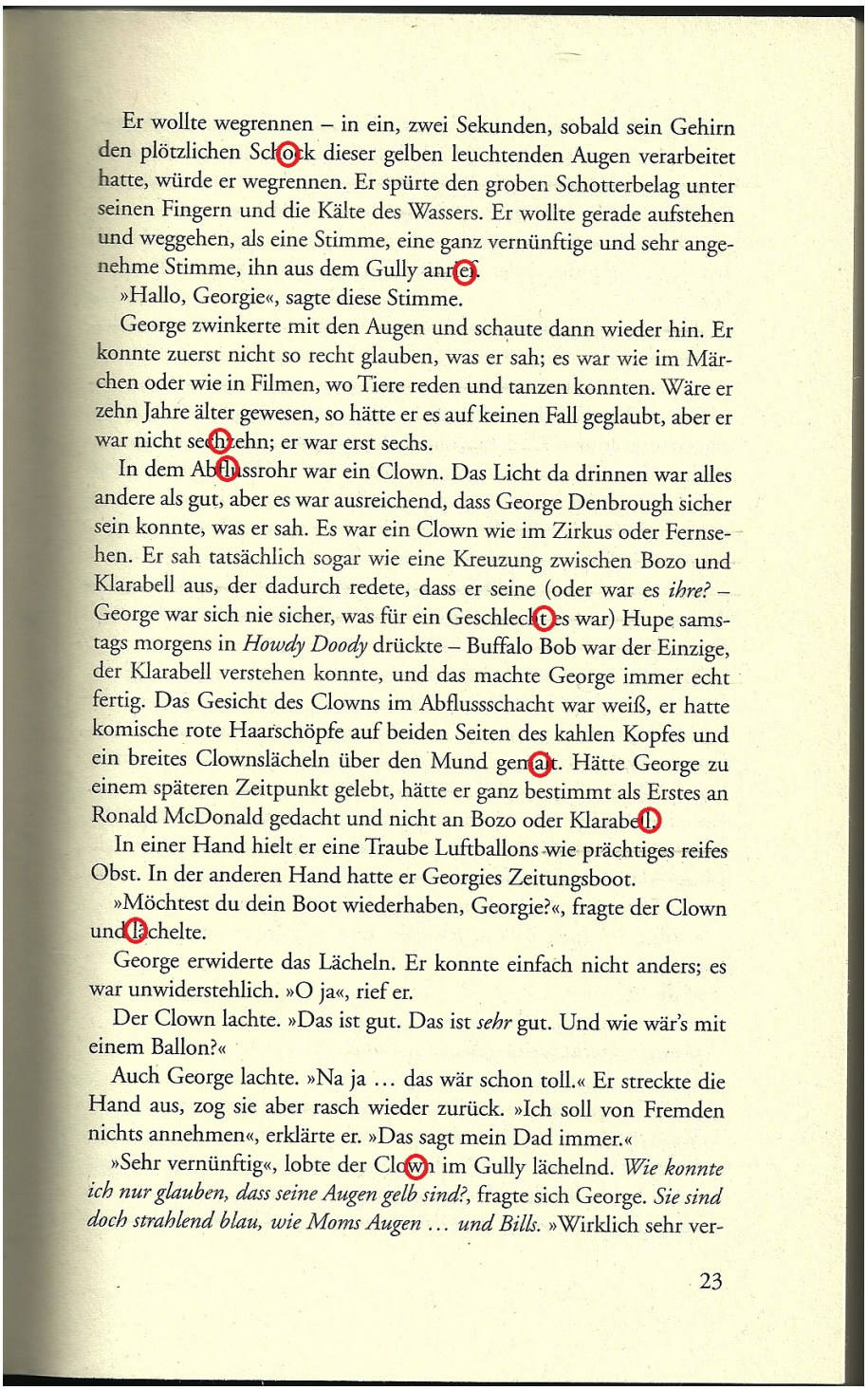
Ein weiteres relativ bekanntes Kryptosystem ist der Buch-Code (auch Buchchiffre oder Buch-Verschlüsselung genannt). Der Name kommt daher, weil man als Schlüssel ein beliebiges Buch (oder anderes Schriftstück) verwendet.

Die Botschaft, die verschlüsselt werden soll, kann hier nicht nur aus den 26 Buchstaben des Alphabets bestehen, sondern zusätzlich auch aus den Ziffern 0 bis 9. Um eine Nachricht zu codieren, sucht man jedes Zeichen von ihr der Reihe nach in dem gewählten Schlüssel-Schriftstück aus und notiert stellvertretend für das Symbol ein Tripel bestehend aus der Seitennummer, der Zeilennummer (von oben angefangen) und der Nummer des Buchstaben/der Zahl (von links beginnend; Leerzeichen, Punkte, Kommas etc. werden nicht mitgezählt). Hat man als Schlüssel ein einseitiges Dokument gewählt, so kann die Seitennummer weggelassen werden. Um die Geheimbotschaft dann wieder zu entschlüsseln, muss man das geheime Schriftstück kennen und besitzen. [buc]

Ein Beispiel:

- Die Nachricht, die wir verschlüsseln wollen, ist wieder *„HALLO WELT“*.
- Als Schlüssel nutzen wir das Buch „Es“ von Stephen King. Der Einfachheit halber nehmen wir alle Codes von der selben Seite (23), welche in Abbildung 2.1 (Seite 10) zu finden ist.
- Es gibt mehrere mögliche Geheimtexte, da jeder Buchstabe und jede Zahl in der Regel mehr als nur einmal vorkommt. Eine Möglichkeit für unser Beispiel ist *„23/12/12 23/23/38 23/13/9 23/25/48 23/2/18 23/37/26 23/6/30 23/29/4 23/18/41“*.

Im Gegensatz zur Caesar-Chiffre kann dieses Verfahren als extrem sicher bezeichnet werden, da die Anzahl an möglichen Schlüsseln fast unbegrenzt ist. Ob der Code geknackt werden kann hängt hier in erster Linie natürlich von dem gewählten Schriftstück ab. Der Angreifer muss nicht nur wissen, was als Schlüssel verwendet wurde, sondern auch noch in Besitz des entsprechenden Textes gelangen. Daher sind seltene, schwer zu beschaffende Texte für einen Buch-Code besonders geeignet. [buc]
Ein großer Nachteil der Buch-Verschlüsselung ist jedoch, dass man sich beim Abzählen der Zeilen und Symbole schnell verzählen kann. Es ist also (vor allem bei längeren Geheimbotschaften) leicht möglich, bereits beim Verschlüsseln der Botschaft Fehler zu machen, was wiederum das Entschlüsseln erschwert, wenn nicht sogar ganz unmöglich macht.



Er wollte wegrennen – in ein, zwei Sekunden, sobald sein Gehirn den plötzlichen Schock dieser gelben leuchtenden Augen verarbeitet hatte, würde er wegrennen. Er spürte den groben Schotterbelag unter seinen Fingern und die Kälte des Wassers. Er wollte gerade aufstehen und weggehen, als eine Stimme, eine ganz vernünftige und sehr angenehme Stimme, ihn aus dem Gully anrief.

»Hallo, Georgie«, sagte diese Stimme.

George zwinkerte mit den Augen und schaute dann wieder hin. Er konnte zuerst nicht so recht glauben, was er sah; es war wie im Märchen oder wie in Filmen, wo Tiere reden und tanzen konnten. Wäre er zehn Jahre älter gewesen, so hätte er es auf keinen Fall geglaubt, aber er war nicht sechzehn; er war erst sechs.

In dem Abflussrohr war ein Clown. Das Licht da drinnen war alles andere als gut, aber es war ausreichend, dass George Denbrough sicher sein konnte, was er sah. Es war ein Clown wie im Zirkus oder Fernsehen. Er sah tatsächlich sogar wie eine Kreuzung zwischen Bozo und Klarabell aus, der dadurch redete, dass er seine (oder war es *ihre?* – George war sich nie sicher, was für ein Geschlecht es war) Hupe samstags morgens in *Howdy Doody* drückte – Buffalo Bob war der Einzige, der Klarabell verstehen konnte, und das machte George immer echt fertig. Das Gesicht des Clowns im Abflussschacht war weiß, er hatte komische rote Haarschöpfe auf beiden Seiten des kahlen Kopfes und ein breites Clownslächeln über den Mund gemalt. Hätte George zu einem späteren Zeitpunkt gelebt, hätte er ganz bestimmt als Erstes an Ronald McDonald gedacht und nicht an Bozo oder Klarabell.

In einer Hand hielt er eine Traube Luftballons wie prächtiges reifes Obst. In der anderen Hand hatte er Georgies Zeitungsboot.

»Möchtest du dein Boot wiederhaben, Georgie?«, fragte der Clown und lächelte.

George erwiderte das Lächeln. Er konnte einfach nicht anders; es war unwiderstehlich. »O ja«, rief er.

Der Clown lachte. »Das ist gut. Das ist *sehr* gut. Und wie wär's mit einem Ballon?«

Auch George lachte. »Na ja … das wär schon toll.« Er streckte die Hand aus, zog sie aber rasch wieder zurück. »Ich soll von Fremden nichts annehmen«, erklärte er. »Das sagt mein Dad immer.«

»Sehr vernünftig«, lobte der Clown im Gully lächelnd. *Wie konnte ich nur glauben, dass seine Augen gelb sind?*, fragte sich George. *Sie sind doch strahlend blau, wie Moms Augen … und Bills.* »Wirklich sehr ver-

23

Abbildung 2.1: Stephen King „Es“, Seite 23 [Kin05]

2.3 RSA-System

Das letzte Kryptosystem, welches in diesem Kapitel vorgestellt werden soll, ist das (im Gegensatz zur Caesar-Chiffre und zum Buch-Code) etwas kompliziertere RSA-Verfahren. Seinen Name erhält es von seinen Erfindern Ronald L. Rivest, Adi Shamir und Leonard Adleman. [Bec08]

Mit diesem Verfahren lassen sich keine Buchstaben, sondern ausschließlich Zahlen codieren. Will man einen Text verschlüsseln, so müssen die einzelnen Buchstaben zuerst in Zahlen umgewandelt werden (zum Beispiel durch A = 01, B = 02, C = 03 etc.). [Bec08]
Die zu codierende Botschaft wird als $m \in \mathbb{N}$ und die Geheimbotschaft als $c \in \mathbb{N}$ bezeichnet.
Bevor jedoch ver- oder entschlüsselt werden kann, müssen erst einmal der private/geheime Schlüssel d und der öffentliche Schlüssel e ermittelt werden. Dazu benötigen wir als erstes zwei zufällig gewählte verschiedene Primzahlen p und q, mit denen wir das RSA-Modul $n = p \cdot q$ und die Eulersche φ-Funktion $\varphi(n) = (p - 1) \cdot (q - 1)$ berechnen.
Nun können die beiden Schlüssel berechnet werden. Der öffentliche Schlüssel e ist frei wählbar aus allen ganzen Zahlen, welche die beiden Gleichungen $1 < e < \varphi(n)$ und $ggT(e,\varphi(n)) = 1$ erfüllen. Der private Schlüssel d hingegen wird durch die Gleichung $d = e^{-1} \bmod \varphi(n)$ erzeugt.
Jetzt können wir den Klartext m in den Geheimtext c umwandeln: $c = m^e \bmod n$. Die hier benötigten Variablen e und n sind deshalb öffentlich bekannt.
Will man aus dem Geheimtext c den Klartext m wieder zurück erlangen, nutzt man die Formel $m = c^d \bmod n$. Damit jedoch nicht jeder die geheime Botschaft entschlüsseln kann, ist die für die Decodierung benötigte Variable d (ebenso wie die beiden Primzahlen p und q) privat. [rsa]

Ein Beispiel:

- Die Zahl, die wir codieren wollen, ist 4.
- Als Primzahlen wählen wir $p = 5$ und $q = 7$, wodurch wir $n = 5 \cdot 7 = 35$ und $\varphi(n) = (5 - 1) \cdot (7 - 1) = 4 \cdot 6 = 24$ erhalten und unsere Schlüssel $e = 11$ und $d = 11$ sind.
- Unser Geheimtext ist nun $c = 4^{11} \bmod 35 = 9$.

In der Praxis wird dieses Verfahren so jedoch nicht genutzt, da es ziemlich anfällig für Angriffe ist. Um eine höhere Widerstandsfähigkeit gegen Angriffe zu erreichen wird es in der Realität meist mit den sogenannten „Optimal Asymmetric Encryption Padding“ kombiniert. [rsa]

3 Visuelle Kryptographie

Dieses Kapitel dient dazu, einen groben Überblick darüber zu erhalten, wie visuelle Kryptographie im Allgemeinen funktioniert. Das Grundkonzept wird zudem anhand zweier einfacher visueller Kryptographieverfahren erklärt (Wie funktionieren sie? Was sind Schwachpunkte? etc.).

3.1 Das Grundprinzip

Grundlegend funktioniert die visuelle Kryptographie genau so wie jedes andere Kryptosystem: man hat einen Klartext, der mit Hilfe eines Schlüssels in einen Geheimtext umgewandelt wird. Anschließend kann man zum Klartext nur zurückgelangen, wenn man den Geheimtext besitzt und den Schlüssel kennt. Der große Unterschied bei der visuellen Kryptographie ist (wie der Name bereits verrät) der, dass hier kein Text codiert bzw. decodiert wird, sondern ein Bild. Das Ganze wird also optisch ver- und entschlüsselt.

In jedem Kryptosystem der visuellen Kryptographie gibt es eine festgelegte Menge an darstellbaren Farben, Färbungen der Subpixel eines Bildpunktes und entsprechenden Kombinationsmöglichkeiten der Subpixelfärbungen, welche die darstellbaren Farben beim Übereinanderlegen ergeben. Für eine der darstellbaren Farben kann es mehrere Kombinationen geben, es muss aber stets mindestens eine existieren.
Zunächst werden erst einmal alle Pixel in (meist vier oder neun) kleinere Subpixel zerlegt. Danach werden die zerteilten Pixel auf der Schlüsselfolie zufällig mit einer der zulässigen Subpixelfärbungen belegt. Anschließend erhält man das Geheimbild, indem man allen Pixeln die Subpixelfärbung zuordnet, die beim Übereinanderlegen mit dem Schlüssel die Farbe des Pixels im Originalbild an der entsprechenden Stelle ergibt.

Ein Teilbild alleine (also nur der Schlüssel oder nur das Geheimbild) ergibt nun beim Betrachten ein scheinbar rein zufälliges Pixelmuster, das keinerlei Informationen liefert. Nur durch das Übereinanderlegen der beiden Teilbilder ergibt sich das Originalbild, also die zuvor verschlüsselte Information.

Das zu verschlüsselnde Bild kann auch auf mehr als zwei Folien verteilt werden. Ein Beispiel hierfür kann Quelle [Kle05] entnommen werden. In dieser Arbeit werden jedoch ausschließlich Verfahren betrachtet, die ein Bild auf zwei Folien verteilen.

3.2 2-Farben-System: Schwarz und Weiß

3.2.1 Vorgehensweise

Eines der einfachsten Konzepte arbeitet mit zwei Farben (Schwarz und Weiß) und der Zerlegung in vier Subpixel.
Hierbei wird zuerst jedes Pixel der Schlüsselfolie zufällig durch eine der beiden Kombinationen aus Abbildung 3.1 ersetzt. Anschließend werden die Pixel der Geheimbildfolie ebenfalls mit einer der beiden Kombinationen belegt, jedoch hier nicht zufällig. Soll beim Übereinanderlegen der Folien an der entsprechenden Stelle ein weißes Pixel entstehen, dann muss genau das gleiche Subpixelmuster gewählt werden, welches an dieser Stelle der Schlüsselfolie steht, und wenn ein schwarzes Pixel entstehen soll, dann stets das andere Muster als jenes auf der Schlüsselfolie. [Kle05]

Abbildung 3.1: Möglichkeiten der Subpixelfärbung

3.2.2 Schwachpunkt

Das zuvor in Abschnitt 3.2.1 beschriebene System ist nicht nur besonders einfach, sondern auch ziemlich unsicher. Allein die erneute Nutzung eines Schlüssels gefährdet die Sicherheit enorm.
Legt man zwei geheime Bilder, die mit der selben Schlüsselfolie verschlüsselt wurden, übereinander, dann kann man Abdrücke der geheimen Bilder erkennen (siehe Abbildung 3.2). Schuld daran ist die symmetrische Differenz. Genauer gesagt: wenn bei den beiden Geheimbildern durch Auflegen des Schlüssels an einer Stelle gleichfarbige Pixel entstehen, dann ist das Pixel, welches durch Übereinanderlegen der beiden Geheimbilder entsteht, stets weiß, und wenn verschiedenfarbige Pixel entstehen, dann erhalten wir ein schwarzes Pixel. [Kle05] Das Ganze wird noch einmal in Abbildung 3.3 auf Seite 14 veranschaulicht.

Abbildung 3.2: Die Originalbilder (links und rechts) und die mit dem selben Schlüssel codierten Geheimbildfolien übereinander gelegt (mitte). [Kle05]

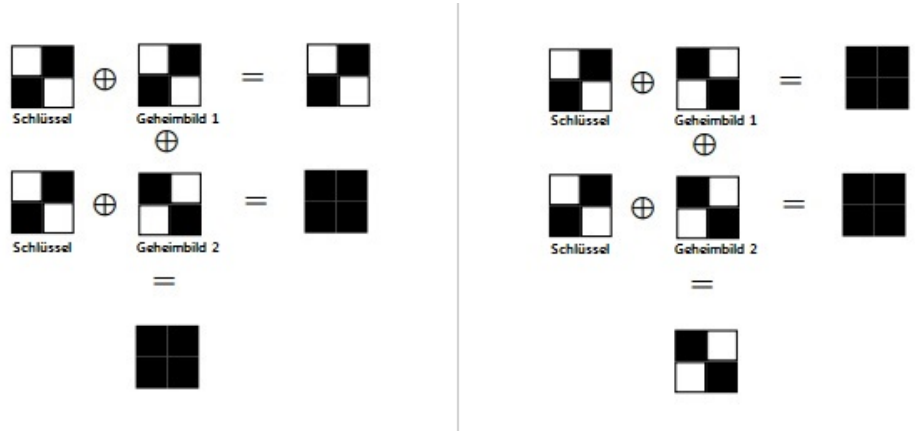


Abbildung 3.3: Die Geheimbilder codieren verschiedenfarbige Pixel (links) und gleichfarbige Pixel (rechts) mit dem selben Schlüssel.

Um dem entgegen zu wirken, könnte man das Bild zum Beispiel auf drei anstatt auf zwei Folien verteilen oder man zerlegt jedes Pixel in neun anstatt vier Subpixel. So gäbe es mehr Färbungs- beziehungsweise Kombinationsmöglichkeiten.

3.3 Verschiedene Graustufen

Außer Acht lassen sollte man auch nicht die Darstellung verschiedener Grautöne mittels der visuellen Kryptographie (als Übergang zwischen der schwarz-weißen visuellen Kryptographie und der farbigen visuellen Kryptographie).
Eine Variante ist es, durch die Zerlegung in vier Subpixel fünf verschiedene Graustufen zu codieren (0%, 25%, 50%, 75% und 100%), je nachdem wie viele Subpixel nach dem Übereinanderlegen der Folien schwarz gefärbt sind. [Kle07] Veranschaulicht wird dieses Modell in Abbildung 3.4 auf Seite 15.
So gäbe es viel mehr Möglichkeiten der Subpixelfärbung (genau $2^4 = 16$ Möglichkeiten, da jedes Subpixel entweder Schwarz oder Weiß sein kann), aber man könnte die Pixel auf der Schlüsselfolie nicht mehr ganz so zufällig einfärben, da nicht schon auf dem Schlüssel mehr Subpixel schwarz sein dürfen als für das Originalbild an der entsprechenden Stelle nötig sind. Wenn also auf dem Originalbild n Subpixel schwarz sind, dann dürfen auf dem Schlüssel an der Stelle nur $k \leq n$ Subpixel schwarz sein. Das Gegenpixel auf der Geheimbildfolie muss dann so gewählt werden, das genau $m = n - k$ Subpixel, die bei der Schlüsselfolie weiß bleiben, schwarz gefärbt werden. Es können also auch hier bis zu n Subpixel schwarz sein, je nachdem wie viele dieser Subpixel sich am Ende überlagern, und dadurch nur einmal zählen.

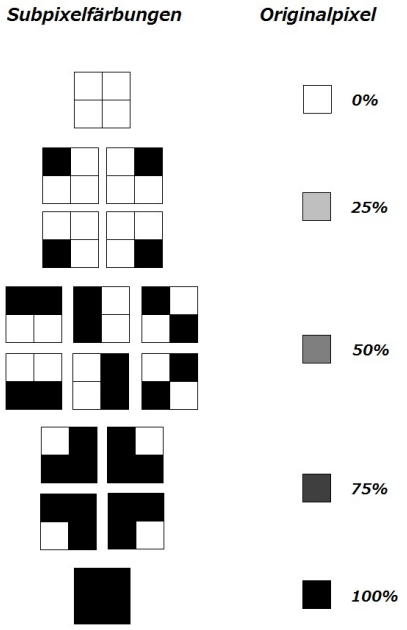


Abbildung 3.4: Darstellungsmöglichkeiten der fünf Graustufen

Zerlegt man jedes Pixel jedoch in beispielsweise neun anstatt nur vier Subpixel, könnte man sogar zehn verschiedene Grautöne darstellen (0%, 11.1%, 22.2%, 33.3%, 44.4%, 55.5%, 66.6%, 77.7%, 88.8% und 100%).
Anders gesagt: je mehr Subpixel, desto mehr Färbungsmöglichkeiten und folglich auch mehr Farben, die codiert werden können; jedenfalls mit Schwarz und Weiß.

4 Farbige Visuelle Kryptographie

4.1 Farbmodelle und Farbmischung

In der Computergraphik werden Farben anders zusammen gemischt als mit dem Farbmalkasten. Hier ergeben zum Beispiel Rot und Grün die Farbe Gelb und nicht Braun. Deshalb ist es zu Beginn wichtig, erst einmal die verschiedenen Konzepte kennen zu lernen und so zu verstehen, wie die einzelnen Farben dargestellt und gemischt werden können. Die beiden hier am häufigsten verwendeten Farbmodelle sind das RGB-Modell und das CMY-Modell. [Kle]

RGB-Modell
Das RGB-Modell baut auf den Grundfarben Rot (red), Grün (green) und Blau (blue) auf. Es ist ein additives Farbmodell, was bedeutet, dass beim Mischen der Farben Lichtstrahlen der entsprechenden Wellenlängen übereinander gelegt werden.
Addiert man Rot und Grün, ergibt das Gelb, aus Grün und Blau wird Türkis, aus Blau und Rot ergibt sich Magenta und alle drei Grundfarben zusammen ergeben Weiß. Dieses Modell wird zum Beispiel bei Computermonitoren eingesetzt. [Kle07] Die verschiedenen Kombinationsmöglichkeiten sind in Abbildung 4.1 auf Seite 17 nochmals dargestellt.

CMY-Modell
Das CMY-Modell hingegen ist ein subtraktives Farbmodell, welches aus den drei Grundfarben Türkis (cyan), Magenta (magenta) und Gelb (yellow) besteht. Subtraktive Farbmischung bedeutet, dass mit weißem Licht begonnen wird und dann nach und nach Licht der entsprechenden Wellenlängen entfernt wird.
Beim Mischen von Türkis und Magenta erhalten wir Blau, Magenta und Gelb ergeben Rot, Gelb und Türkis ergeben Grün und wenn alle drei subtrahiert werden bekommt man Schwarz. Dieses Modell ist sehr beliebt beim Mischen von Druckerfarben. [Kle07] Die Kombinationsmöglichkeiten werden auch hier in Abbildung 4.1 auf Seite 17 noch einmal veranschaulicht.

Farbdarstellung
Es gibt verschiedene Möglichkeiten wie Farben dargestellt werden können. Die hier genutzte Variante ist die, sie durch ihren Rot-, Grün- und Blauanteil zu definieren (da die meisten Computermonitore das RGB-Modell nutzen). [Hou03]

Das Ganze wird als Tripel *(r,g,b)* dargestellt, wobei alle drei Werte zwischen 0 und 1 liegen und der erste Wert r für den Rotanteil, der zweite Wert g für den Grünanteil und der dritte Wert b für den Blauanteil steht. Folglich werden die acht Farben, die hier von Bedeutung sind, so dargestellt: Rot (1,0,0), Grün (0,1,0), Blau (0,0,1), Türkis (0,1,1), Magenta (1,0,1), Gelb (1,1,0), Schwarz (0,0,0) und Weiß (1,1,1). [Kle]

Farbmischung
Bei der visuellen Kryptographie werden die Farben durch das direkte Übereinanderlegen der Folien subtraktiv gemischt und anschließend, also wenn sie (nahe) nebeneinander liegen (wobei sie aber nicht zwingend auch aneinandergrenzen müssen), additiv gemischt. [Kle]

Komplementärfarben
Es ist außerdem wichtig zu wissen, was Komplementärfarben sind. Im Farbkreis, wie man ihn aus dem Kunstunterricht kennt, sind das stets die Farben, die sich gegenüberliegen. Bei unseren Farbmodellen bedeutet das ein Farbenpaar, welches bei der additiven Mischung Weiß und bei der subtraktiven Mischung Schwarz ergibt. [Kle07]
In den beiden vorgestellten Farbmodellen sind die Komplementärfarbenpaare:
Rot-Türkis, Grün-Magenta und Blau-Gelb.

Abbildung 4.1: Farbmodell CMY (links) und Farbmodell RGB (rechts) [rgb]

Ein Beispiel dafür, was das genau in der farbigen visuelle Kryptographie bedeutet: man hat alle Pixel in neun Subpixel zerlegt. Beim Zusammenfügen der Folien erhalten wir ein Drittel Grün, ein Drittel Magenta und ein Drittel Weiß. Da sich Grün und Magenta (die beide gleichgroße Anteile sind) aufheben, erscheint das Pixel als Weiß, allerdings kein reines Weiß.
Ein weiteres Beispiel: beim Zusammenfügen der Folien erhalten wir ein Drittel Gelb und zwei Drittel Blau. Je drei Subpixel von Gelb und von Blau heben sich gegenseitig auf, es bleiben allerdings drei Subpixel in Blau über, wodurch das Pixel Blau erscheint (jedoch auch hier nicht in reiner Form).

Zusätzlich sollte noch erwähnt werden, dass sich weder mit RGB noch mit CMY alle vom Menschen erfassbaren Farben darstellen lassen. Für die farbige visuelle Kryptographie spielt dies allerdings keine weitere Rolle. [Kle07]

4.2 Güte

Wenn man nach dem Verschlüsseln eines Bildes dieses wieder entschlüsselt, dann ist es meistens nicht mehr zu 100% in reiner Form. Anders gesagt: es kann sein, dass Weiß anschließend die Farbanteile (0.9, 0.9, 0.9) hat, anstatt (1, 1, 1). Es kann also eine Abweichung der dargestellten Farbe von ihrer reinen Form geben, die durch die Güte dargestellt wird. [Kle] Man nutzt diese um Vergleiche machen zu können.

Man kann die Güte d auf mehrere verschiedene Arten definieren:

- **Definition 1 - Güte der Farbanteile der einzelnen Farben:** Wenn die dargestellte Farbe a die Anteile *(r1, g1, b1)* hat und die reine Farbe b aus den Anteilen *(r2, g2, b2)* besteht, ergibt das folgende Tripel die Güte:

  $$d(a,b) = (|r1 - r2|, |g1 - g2|, |b1 - b2|)$$ [Kle].

  Auf diese Art kann gezeigt werden, wie gut/schlecht die einzelnen Farbanteile codiert werden. Ein Vergleich zwischen zwei Farben oder visuellen Kryptographiesystemen lässt sich damit aber schlecht realisieren.

- **Definition 2 - Güte der einzelnen Farben:** Die dargestellte Farbe a besteht aus den Anteilen *(r1, g1, b1)* und die reine Farbe b aus *(r2, g2, b2)*. Dann ist die Güte für diese Farbe:

  $$d(a,b) = |r1 - r2| + |g1 - g2| + |b1 - b2|$$ [Kle07].

  So kann zum Beispiel verglichen werden, welches visuelle Kryptographiesystem eine bestimmte Farbe besser codiert. Ein Vergleich, welches von mehreren Systemen das beste ist, lässt sich hier jedoch auch nicht umsetzen.

- **Definition 3 - Güte des kompletten Systems:** Es werden n verschiedene Farben codiert. Jede wird dargestellt durch die Farbanteile $(r1_n, g1_n, b1_n)$ und ihre zugehörige reine Farbe besteht aus den Anteilen $(r2_n, g2_n, b2_n)$. Somit ist die Güte:

  $$d(a,b) = \sum_{i=1}^{n} (|r1_i - r2_i| + |g1_i - g2_i| + |b1_i - b2_i|)$$ [Kle07].

  Jetzt können zwar keine einzelnen Farben mehr miteinander verglichen werden, aber dafür ist es nun möglich, zwei (oder mehr) verschiedene visuelle Kryptographiesysteme zu vergleichen.

4.3 4-Farben-System

4.3.1 Vorgehensweise

Das erste optimale Verfahren, das hier näher betrachtet werden soll, ist die Codierung von vier Farben auf zwei Folien, genauer die Verschlüsselung von Schwarz, Weiß und einem Komplementärfarbenpaar. Für die Erklärungen in diesem Abschnitt werden Blau und Gelb genutzt, das Ganze funktioniert aber ebenso mit Grün-Magenta oder Rot-Türkis. Warum dieses Verfahren optimal ist, wird in Kapitel 4.3.2 auf Seite 22 bewiesen. Hier geht es zunächst ausschließlich darum zu erläutern, wie das Verfahren funktioniert, welches der Quelle [Kle], verfasst von Andreas Klein, entnommen wurde.

Bevor verschlüsselt werden kann, müssen zuerst einmal die Möglichkeiten der Subpixelfärbung vorliegen. Hier werden die einzelnen Pixel in neun Subpixel zerlegt, von denen wiederum genau drei Weiß, drei Blau und drei Gelb gefärbt werden. Die Färbung erfolgt hier stets in den Diagonalen und die verschiedenen möglichen Subpixelfärbungen entstehen durch die Permutationen der drei Farben. Da das bildlich meist besser zu verstehen ist, sind die einzelnen Färbungsmöglichkeiten in Abbildung 4.2, Seite 19 dargestellt.

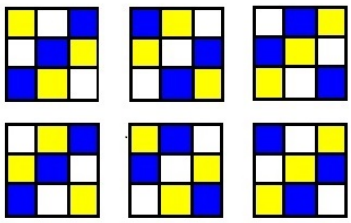


Abbildung 4.2: Möglichkeiten der Färbung der Subpixel

Wenn dann die Folien übereinander gelegt werden, werden die Farben zuerst subtraktiv gemischt, je nachdem was übereinander liegt. Bei zweimal der selben Farbe bleibt diese so zweifellos erhalten, ebenso bei der Kombination mit Weiß, und wenn die beiden Komplementärfarben übereinander liegen, erhalten wir Schwarz (siehe Definition von Komplementärfarben in Kapitel 4.1, Seite 16). Danach werden die Farben additiv gemischt, also entsprechend dem, was anschließend nebeneinander liegt. Hierbei heben sich Blau und Gelb auf, da sie komplementär sind, und es entsteht optisch Weiß in diesen Subpixeln (auch hier siehe Definition von Komplementärfarben in Kapitel 4.1, Seite 16). Liegt Blau oder Gelb neben Weiß, so dominiert diese Farbe und es erscheint als Blau beziehungsweise Gelb und liegt eine Farbe neben ihresgleichen, so bleibt diese logischerweise erhalten.

Nachdem jetzt jedes Pixel der Schlüsselfolie zufällig mit einer der sechs Kombinationen belegt wurde, müssen die Pixel des Geheimbildes mit den entsprechenden Gegenstücken belegt werden, so dass beim Übereinanderlegen der Folien die gewünschte Farbe heraus kommt.

Weiß
Soll nun ein weißes Pixel entstehen, muss einfach die gleiche Färbung der Subpixel wie auf dem Schlüssel gewählt werden. So erhalten wir nach dem Übereinanderlegen drei weiße, drei blaue und drei gelbe Subpixel. Die blauen und gelben Subpixel heben sich hier durch additive Mischung optisch auf (das heißt sie wirken weiß) und es entsteht ein weißes Pixel, jedoch kein reines Weiß, was mit Hilfe der nachfolgenden Berechnung der Farbanteile verdeutlicht wird. Alle Kombinationsmöglichkeiten für ein weißes Pixel sind noch einmal zusätzlich in Abbildung 4.3, Seite 20 zu sehen.

$$\begin{aligned}
\tfrac{1}{3} \cdot (0,0,1) &= (0,0,\tfrac{1}{3}) \rightarrow 3 \text{ blaue Subpixel} \\
\tfrac{1}{3} \cdot (1,1,0) &= (\tfrac{1}{3},\tfrac{1}{3},0) \rightarrow 3 \text{ gelbe Subpixel} \\
\tfrac{1}{3} \cdot (1,1,1) &= (\tfrac{1}{3},\tfrac{1}{3},\tfrac{1}{3}) \rightarrow 3 \text{ weiße Subpixel} \\
&\overline{(\tfrac{2}{3},\tfrac{2}{3},\tfrac{2}{3})}
\end{aligned}$$

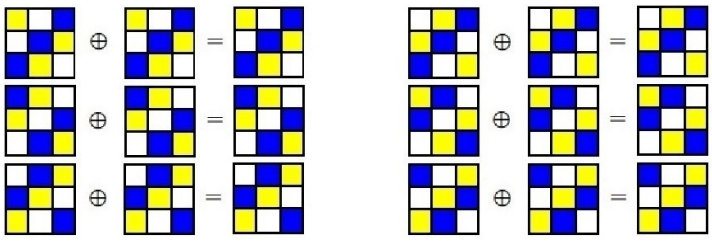


Abbildung 4.3: Kombinationsmöglichkeiten für Weiß

Blau
Will man hingegen ein blaues Pixel verschlüsseln, so muss kontinuierlich die Subpixelfärbung gewählt werden, bei der die selben Subpixel gelb sind, wie an dieser Stelle auf dem Schlüssel, und bei der die blauen und weißen Subpixel vertauscht sind (im Vergleich zu der Färbung auf der Schlüsselfolie). So erhalten wir nach dem Übereinanderlegen genau drei gelbe Subpixel und sechs blaue Subpixel, da wir sechsmal Blau auf Weiß beziehungsweise Weiß auf Blau legen, wobei durch die subtraktive Farbmischung Blau entsteht. Optisch heben sich nun drei der blauen und die drei gelben Subpixel auf, sie wirken weiß, und durch die restlichen drei blauen Subpixel erhalten wir einen schwachen Blauton (s. Rechnung). Veranschaulicht sind die entsprechenden Kombinationen noch einmal in Abbildung 4.4, Seite 21.

$$\frac{2}{3} \cdot (0,0,1) = (0,0,\frac{2}{3}) \rightarrow 6 \text{ blaue Subpixel}$$
$$\frac{1}{3} \cdot (1,1,0) = (\frac{1}{3},\frac{1}{3},0) \rightarrow 3 \text{ gelbe Subpixel}$$
$$\overline{(\frac{1}{3},\frac{1}{3},\frac{2}{3})}$$

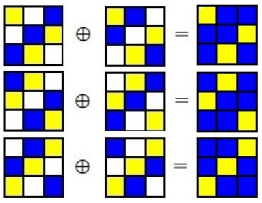


Abbildung 4.4: Kombinationsmöglichkeiten für Blau

Gelb
Um wiederum ein gelbes Pixel zu erhalten, kann man vergleichbar wie bei einem blauen Pixel vorgehen. Das bedeutet, es muss stets die Färbung für die Subpixel genommen werden, wo die selben Subpixel wie auf der Schlüsselfolie blau sind und die gelben und weißen Subpixel genau umgekehrt zur Färbung auf dem Schlüssel sind. So bekommen wir dann durch das Übereinanderlegen der beiden Folien sechs gelbe und drei blaue Subpixel. Von denen heben sich je drei optisch auf (sie erscheinen weiß) und durch die drei gelben Subpixel, die übrig bleiben, erscheint das große Pixel summa summarum in einem schwachen Gelbton (vgl. Rechnung). Die zugehörigen Kombinationsmöglichkeiten sind in Abbildung 4.5, Seite 21 dargestellt.

$$\frac{1}{3} \cdot (0,0,1) = (0,0,\frac{1}{3}) \rightarrow 3 \text{ blaue Subpixel}$$
$$\frac{2}{3} \cdot (1,1,0) = (\frac{2}{3},\frac{2}{3},0) \rightarrow 6 \text{ gelbe Subpixel}$$
$$\overline{(\frac{2}{3},\frac{2}{3},\frac{1}{3})}$$

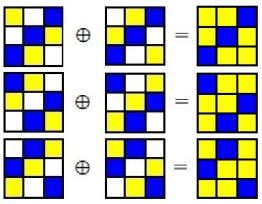


Abbildung 4.5: Kombinationsmöglichkeiten für Gelb

Schwarz
Jetzt ist nur noch offen, wie man ein schwarzes Pixel codieren kann. Das Prinzip ist dem der blauen und gelben Pixel nicht unähnlich. Der Unterschied ist hier nur der, dass die Färbung für die Subpixel so gewählt wird, das an der selben Stelle wie auf dem Schlüssel weiße Subpixel sind und die blauen und gelben Subpixel gegensätzlich sind. Auf diese Weise erhalten wir durch das Aufeinanderlegen dreimal Weiß (durch Weiß + Weiß) und sechsmal Schwarz (durch dreimal Blau + Gelb und dreimal Gelb + Blau). Das Pixel ist folglich zu $\frac{2}{3}$ schwarz, erscheint also als dunkler Grauton, der als Schwarz interpretiert werden kann. Die genauen Rot-, Grün- und Blauanteile können wieder der Rechnung entnommen werden. Alle möglichen Färbungen der Subpixel sind in Abbildung 4.6, Seite 22 nochmals abgebildet.

$$\begin{aligned} \tfrac{1}{3} \cdot (1,1,1) &= (\tfrac{1}{3},\tfrac{1}{3},\tfrac{1}{3}) \rightarrow 3 \text{ weiße Subpixel} \\ \tfrac{2}{3} \cdot (0,0,0) &= (0,0,0) \ \rightarrow 6 \text{ schwarze Subpixel} \\ &\overline{\qquad\qquad\qquad} \\ &(\tfrac{1}{3},\tfrac{1}{3},\tfrac{1}{3}) \end{aligned}$$

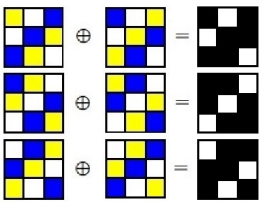


Abbildung 4.6: Kombinationsmöglichkeiten für Schwarz

4.3.2 Optimalitätsbeweis

Der hier aufgeführte Beweis, dass das in Abschnitt 4.3.1 beschriebene Verfahren optimal ist (das heißt, es gibt kein besseres zur Verschlüsselung dieser Farben), ist an den Beweis aus der Quelle [Kle] von Andreas Klein angelehnt.
Die Rot-, Grün- und Blauwerte für die optimalen Farben im Vergleich zu den hier codierten Farben und deren Differenz (die Güte) können der Tabelle 4.1 auf Seite 25 entnommen werden. Diese werden für den Beweis benötigt.

Zuerst zeigen wir, dass Lemma 1 gilt.

Lemma 1 *Es gibt kein Verfahren zur Codierung von Schwarz, Weiß und einem Komplementärfarbenpaar, welches für Weiß und Schwarz Werte liefert, die gleichzeitig näher an (1,1,1) (reines Weiß) beziehungsweise (0,0,0) (reines Schwarz) sind, als* $(\frac{2}{3},\frac{2}{3},\frac{2}{3})$ *für Weiß und* $(\frac{1}{3},\frac{1}{3},\frac{1}{3})$ *für Schwarz.*

Da wir außer Schwarz und Weiß noch zwei weitere Farben codieren wollen, dürfte klar sein, dass wir auf den einzelnen Folien nicht nur mit Schwarz und Weiß arbeiten können. Es sind also definitiv noch weitere Farben (Rot? Grün? Blau? Türkis? Magenta? Gelb?) auf den Folien vorhanden (welche genau wird später erläutert).
Die beiden Farben Schwarz und Weiß haben je gleich große Rot-, Grün- und Blauanteile. Folglich muss Hilfssatz 2 gelten.

Hilfssatz 2 *Bei jedem Pixel muss die Summe der einzelnen Farbanteile (Rot, Grün, Blau) der Subpixel gleich groß sein, damit Weiß und/oder Schwarz codiert werden kann/können.* $(\sum_{Rotanteile} = \sum_{Grünanteile} = \sum_{Blauanteile})$

Der Anteil eines Pixels, der mit einer der Grundfarben gefärbt ist, darf also höchstens $\frac{1}{3}$ betragen, damit Schwarz und Weiß überhaupt codiert werden können.
Optimal für die Verschlüsselung von Weiß (1,1,1) wären die Grundfarben des CMY-Farbmodells zu gleichen Teilen:

$$\begin{aligned}
\tfrac{1}{3} \cdot (1,1,1) &= (0,\tfrac{1}{3},\tfrac{1}{3}) \rightarrow \text{Türkis} \\
\tfrac{1}{3} \cdot (1,1,1) &= (\tfrac{1}{3},0,\tfrac{1}{3}) \rightarrow \text{Magenta} \\
\tfrac{1}{3} \cdot (1,1,1) &= (\tfrac{1}{3},\tfrac{1}{3},0) \rightarrow \text{Gelb} \\
&\overline{(\tfrac{2}{3},\tfrac{2}{3},\tfrac{2}{3})}
\end{aligned}$$

Für die Verschlüsselung von Schwarz (0,0,0) hingegen sind die Grundfarben des RGB-Farbmodells zu gleich großen Anteilen besser geeignet:

$$\begin{aligned}
\tfrac{1}{3} \cdot (0,0,0) &= (\tfrac{1}{3},0,0) \rightarrow \text{Rot} \\
\tfrac{1}{3} \cdot (0,0,0) &= (0,\tfrac{1}{3},0) \rightarrow \text{Grün} \\
\tfrac{1}{3} \cdot (0,0,0) &= (0,0,\tfrac{1}{3}) \rightarrow \text{Blau} \\
&\overline{(\tfrac{1}{3},\tfrac{1}{3},\tfrac{1}{3})}
\end{aligned}$$

Um nun beide Farben so gut wie möglich darstellen zu können muss also eine Kombination aus den Grundfarben des RGB- und des CMY-Farbmodells benutzt werden: ein Komplementärfarbenpaar. Dieses besteht zu gleichen Anteilen aus allen Grundfarben (das Komplement einer Grundfarbe des RGB-Farbsystems besteht immer aus den anderen beiden RGB-Grundfarben, siehe Kapitel 4.1) und mit einem solchen Farbenpaar kann man ebenso Weiß (durch additive Farbmischung) wie auch Schwarz (durch subtraktive Farbmischung) erzeugen. Logischerweise sollte das Komplementärfarbenpaar genommen werden, welches neben Schwarz und Weiß codiert werden soll, also hier Blau und Gelb, wie bei der Erklärung dieses Kryptosystems in Abschnitt 4.3.1.
Durch die Codierung nur mit Blau und Gelb (zu je 50%) könnte man perfektes Schwarz codieren (durch Übereinanderlegen von Gelb auf Blau und umgekehrt), allerdings wäre dann der Farbwert für Weiß nur $(\frac{1}{2},\frac{1}{2},\frac{1}{2})$, also ziemlich „schmutziges“ Weiß, und wie sollte man so auch Blau beziehungsweise Gelb codieren können?

Es muss also noch mindestens eine dritte Farbe auf den Folien vorhanden sein; aber welche? Schwarz oder Weiß? Diese Frage lässt sich leicht rechnerisch beantworten. Durch die Nutzung von Schwarz als dritter Farbe ließe sich kein Weiß codieren. Durch die subtraktive Mischung von Blau und Gelb, zusammen mit $\frac{1}{3}$ Schwarz, könnte man erneut perfektes Schwarz codieren. Alle drei Farben nebeneinander würden jedoch nur zu $(\frac{1}{3},\frac{1}{3},\frac{1}{3})$, also dunklem Grau führen, was eher als Schwarz anstatt Weiß gelten würde. Somit bleibt nur Weiß als dritte Farbe. Die ausführlichen Rechnungen sind im Anhang auf Seite 42, Abschnitt 8.1 zu finden.
Eine andere Farbe, außer Schwarz und Weiß, als dritte Farbe für die Folien braucht nicht in Betracht gezogen zu werden, da es zum einen nie förderlich ist eine Farbe, die nicht codiert werden soll, auf den Folien zu nutzen und zum anderen, da Schwarz und Weiß die einzigen Farben sind, die gleich große Anteile jeder Grunfarbe (Rot, Grün, Blau) besitzen, also das Verhältnis dieser zueinander nicht durcheinander bringen.
An dieser Stelle sollte noch die Überlegung erwähnt werden, den Weißanteil auf den Folien zu verkleinern oder zu vergrößern, wobei das Verhältnis des Blau- und Gelbanteils zueinander trotzdem gleich bleiben würden. Wenn der Weißanteil kleiner als $\frac{1}{3}$ wäre, dann ließe sich Schwarz besser codieren. Die Farbwerte bei der Codierung von Weiß würden aber darunter leiden. Umgekehrte Auswirkungen hätte die Vergrößerung des Weißanteils auf die codierten Werte. Folglich ist $\frac{1}{3}$ die Mitte, wo sich für beide Farben die besten Werte ergeben und es gilt Hilfssatz 3,

Hilfssatz 3 *Die bestmögliche Codierung von Schwarz und Weiß entsteht, wenn ein Pixel auf jeder Folie aus genau $\frac{1}{3}$ Blau, $\frac{1}{3}$ Gelb und $\frac{1}{3}$ Weiß besteht.*

womit auch Lemma 1 bewiesen ist.

Jetzt zeigen wir noch, dass auch Lemma 4 gilt.

Lemma 4 *Durch das Übereinanderlegen der Folien kann nie mehr als $\frac{2}{3}$ Blau beziehungsweise $\frac{2}{3}$ Gelb entstehen.*

Wir haben bereits gezeigt, dass auf jeder Folie Blau, Gelb und Weiß vorhanden seien und dass der Blau- und der Gelbanteil gleich groß seien müssen.
Um die Farbe Blau aus Blau, Gelb und Weiß herzustellen gibt es nur zwei Methoden: Blau & Blau oder Blau & Weiß subtraktiv mischen (also übereinander legen). Wenn man die Verhältnisse der Farbanteile zueinander betrachtet, kann man drei verschiedene Fälle unterscheiden: der Blauanteil ist größer als der Weißanteil, er ist kleiner als der Weißanteil oder beide Anteile sind gleich groß.

- Fall 1: Blauanteil > Weißanteil
  Man erhält das Maximum an Blau, wenn man alles Weiß von Folie 1 auf einen Teil des Blau von Folie 2 legt und umgekehrt und die restlichen blauen Stellen von Folie 1 & 2 (die folglich gleich groß seien müssen) übereinander platziert.

Der Rest besteht dann aus Gelb auf Gelb, woraus man schlussfolgern kann, das der Blauanteil nach dem Übereinanderlegen der Folien *1 - Gelbanteil* ist.
Da der Gelb- und Blauanteil gleich groß sind und der Weißanteil kleiner als die beiden ist, muss der *Gelbanteil* $> \frac{1}{3}$ sein. Also entsteht weniger als $\frac{2}{3}$ Blau.

- Fall 2: Blauanteil < Weißanteil
  Hier kann man das Maximum an Blau erzeugen, indem man alles Blau von Folie 1 auf einen Teil des Weiß von Folie 2 und umgekehrt legt. Der Rest besteht dann aus einer Kombination aus dem restlichen Weiß und Gelb.
  Der Blauanteil nach dem Übereinanderlegen der Folien ist also $2 \cdot$ *Blauanteil der einzelnen Folien.* Da wir wissen, dass der Blau- und der Gelbanteil gleich groß und kleiner als der Weißanteil sind, muss der Blauanteil einer einzelnen Folie kleiner als $\frac{1}{3}$ sein, weshalb das doppelte davon auch kleiner als $\frac{2}{3}$ ist.
- Fall 3: Blauanteil = Weißanteil
  In diesem Fall entsteht am meisten Blau, wenn man je alles Blau einer Folie auf alles Weiß der anderen Folie legt. Der Rest beider Folien muss dann Gelb sein. Es entsteht somit zweimal so viel Blau wie auf den einzelnen Folien.
  Wenn der Blau- und Weißanteil gleich groß seien sollen und (wie bereits gezeigt) der Blauanteil stets genau so groß wie der Gelbanteil ist, dann müssen alle drei Farben zu genau $\frac{1}{3}$ vorhanden sein. Demnach entstehen genau $\frac{2}{3}$ Blau.

Analog kann man die selben Schritte für Gelb durchführen, womit Lemma 4 bewiesen ist. (Dieser Beweis funktioniert ebenso mit jedem anderen Komplementärfarbenpaar.)

Infolgedessen müssen die Anteile für Blau und Gelb eines Pixels je genau $\frac{1}{3}$ sein, damit diese beiden Farben so gut wie möglich verschlüsselt werden können, was sich mit der bestmöglichen Codierung von Schwarz und Weiß deckt. Folglich gilt Satz 5.

Satz 5 *Das in Abschnitt 4.3.1 beschriebene Verfahren ist optimal für die Verschlüsselung von Schwarz, Weiß und einem Komplementärfarbenpaar.*

Farbe	RGB-Werte optimal	RGB-Werte codiert	Güte
Weiß	(1,1,1)	$(\frac{2}{3},\frac{2}{3},\frac{2}{3})$	$(\frac{1}{3},\frac{1}{3},\frac{1}{3})$
Blau	(0,0,1)	$(\frac{1}{3},\frac{1}{3},\frac{2}{3})$	$(\frac{1}{3},\frac{1}{3},\frac{1}{3})$
Gelb	(1,1,0)	$(\frac{2}{3},\frac{2}{3},\frac{1}{3})$	$(\frac{1}{3},\frac{1}{3},\frac{1}{3})$
Schwarz	(0,0,0)	$(\frac{1}{3},\frac{1}{3},\frac{1}{3})$	$(\frac{1}{3},\frac{1}{3},\frac{1}{3})$

Tabelle 4.1: Farbanteile für optimale Farbe, codierte Farbe und Güte der Farbanteile der einzelnen Farben im optimalen 4-Farben-System

4.4 7-Farben-System

4.4.1 Vorgehensweise

Das zweite Verfahren, welches hier behandelt werden soll, ist die Verschlüsselung von insgesamt sieben Farben: Rot, Grün, Blau, Türkis, Magenta, Gelb und Weiß. Dieses Verfahren wurde ebenfalls der Quelle [Kle] von Andreas Klein entnommen.

Für die Schlüssel- und Geheimbildfolie werden allerdings nur vier dieser sieben Farben genutzt. Jedes Pixel wird in vier Subpixel zerlegt, von denen je eins türkis, magenta, gelb und weiß gefärbt wird. Folglich gibt es 24 verschiedene Möglichkeiten die Subpixel zu färben. Das ergibt sich daraus, dass für das erste Subpixel vier Farben zur Auswahl stehen, für das zweite drei Farben, das dritte zwei Farben und für das letzte Subpixel nur eine Farbe, also: $4 \cdot 3 \cdot 2 \cdot 1 = 24$ verschiedene Varianten, die noch einmal in Abbildung 4.7 veranschaulicht sind.
Es handelt sich auch hier um ein optimales Verfahren. Der Beweis kann Kapitel 4.4.2 auf Seite 30 entnommen werden.

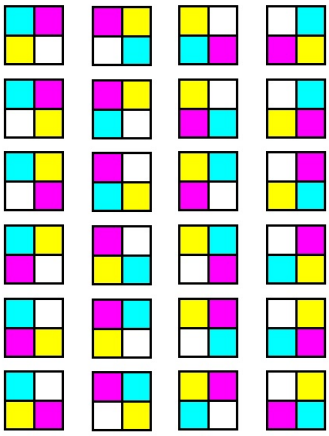


Abbildung 4.7: Alle Varianten die Subpixel einzufärben

Nun werden wieder einmal die Pixel der Schlüsselfolie zufällig mit einer dieser Kombinationen gefärbt und anschließend die zugehörigen Pixel des Geheimbildes entsprechend mit der Subpixelfärbung belegt, die beim Übereinanderlegen die gewünschte Farbe liefert. Bei 24 Möglichkeiten pro Pixel ergibt das beispielsweise für ein Foto mit 531 x 768 Pixeln Größe $24^{531 \cdot 768}$ verschiedene Schlüssel.

Wie lassen sich nun die einzelnen Farben codieren?

Weiß
Zuerst zeigen wir, wie man Weiß mischt. Das ist am einfachsten. Man muss nur die gleiche Färbung für die Subpixel nehmen, wie auf dem Schlüssel. Dadurch werden subtraktiv stets die gleichen Farben gemischt und das Pixel, was dabei heraus kommt, hat ein türkises, ein magentafarbenes, ein gelbes und ein weißes Subpixel. Wir wissen, dass sich bei der additiven Mischung von allen Grundfarben, also hier durch Türkis, Magenta und Gelb, optisch Weiß ergibt. Zusammen mit dem vierten, weißen Subpixel erscheint das komplette Pixel in einem trüben Weißton.
Das kein reines Weiß herauskommt, kann man rechnerisch durch die einzelnen Rot-, Grün- und Blauanteile der Farben zeigen.

$$\begin{aligned}
\tfrac{1}{4} \cdot (1,1,1) &= (\tfrac{1}{4},\tfrac{1}{4},\tfrac{1}{4}) \rightarrow 1 \text{ weißes Subpixel} \\
\tfrac{1}{4} \cdot (0,1,1) &= (0,\tfrac{1}{4},\tfrac{1}{4}) \rightarrow 1 \text{ türkises Subpixel} \\
\tfrac{1}{4} \cdot (1,0,1) &= (\tfrac{1}{4},0,\tfrac{1}{4}) \rightarrow 1 \text{ magentafarbenes Subpixel} \\
\tfrac{1}{4} \cdot (1,1,0) &= (\tfrac{1}{4},\tfrac{1}{4},0) \rightarrow 1 \text{ gelbes Subpixel} \\
\hline
&(\tfrac{3}{4},\tfrac{3}{4},\tfrac{3}{4})
\end{aligned}$$

Da reines Weiß die Farbanteile (1,1,1) hat, erkennt man hier gut, dass es eine Abweichung der einzelnen Farbanteile (also Güte) von $(\frac{1}{4},\frac{1}{4},\frac{1}{4})$ gibt.

Rot, Grün & Blau
Soll eine der Grundfarben des RGB-Farbsystems verschlüsselt werden, so muss für das Geheimbild die Färbung der Subpixel gewählt werden, wo Weiß und die Komplementärfarbe der zu verschlüsselnden Farbe auf der selben Stelle und die anderen beiden Farben vertauscht sind. Genauer gesagt: soll Rot codiert werden, dann müssen Weiß und Türkis an der selben Stelle liegen und Magenta und Gelb vertauscht werden. Soll aber Grün codiert werden, dann müssen Weiß und Magenta auf dem selben Subpixel sein und das türkise und das gelbe Subpixel umgekehrt gefärbt werden. Und wenn Blau codiert wird, dann sollten das weiße und das gelbe Subpixel bleiben und Türkis und Magenta umgedreht werden.
Wenn dann die beiden Folien übereinander gelegt werden, erhalten wir immer zwei Subpixel in der Farbe, die verschlüsselt wird, ein Subpixel in deren Komplementärfarbe und ein weißes Subpixel. Wie die beiden letzteren entstehen, bedarf keiner weiteren Erklärung, aber warum erhalten wir zwei Subpixel in der zu verschlüsselnden Farbe? Wie der Abbildung 4.1 von Seite 17 entnommen werden kann, bilden je zwei Grundfarben des CMY-Farbsystems durch subtraktive Mischung (also hier duch das übereinanderlegen der Folien) das Komplement der dritten Grundfarbe. Zusammengefasst: Magenta + Gelb = Rot (welches das Komplement von Türkis ist), Gelb + Türkis = Grün (das Komplement von Magenta) und Türkis + Magenta = Blau (das Komplement von Gelb).

Wie wir wissen, heben sich die Komplementärfarben bei additiver Farbmischung optisch auf, dass heißt sie erscheinen weiß. Neben diesen beiden „optisch weißen“ Subpixeln haben wir noch ein „echt“ weißes Subpixel und eines in der Farbe, die wir codieren. Demnach erscheint das Ganze optisch in der gewünschten Farbe. Dass diese jedoch nicht hundertprozentig getroffen wird, zeigt wieder die Summe der Rot-, Grün- und Blauanteile der einzelnen Subpixel.

Rot

$\frac{1}{4} \cdot (1,1,1) = (\frac{1}{4},\frac{1}{4},\frac{1}{4}) \rightarrow$ 1 weißes Subpixel
$\frac{1}{2} \cdot (1,0,0) = (\frac{1}{2},0,0) \rightarrow$ 2 rote Subpixel
$\frac{1}{4} \cdot (0,1,1) = (0,\frac{1}{4},\frac{1}{4}) \rightarrow$ 1 türkises Subpixel

$$\overline{(\tfrac{3}{4},\tfrac{1}{2},\tfrac{1}{2})}$$

Grün

$\frac{1}{4} \cdot (1,1,1) = (\frac{1}{4},\frac{1}{4},\frac{1}{4}) \rightarrow$ 1 weißes Subpixel
$\frac{1}{2} \cdot (0,1,0) = (0,\frac{1}{2},0) \rightarrow$ 2 grüne Subpixel
$\frac{1}{4} \cdot (1,0,1) = (\frac{1}{4},0,\frac{1}{4}) \rightarrow$ 1 magentafarbenes Subpixel

$$\overline{(\tfrac{1}{2},\tfrac{3}{4},\tfrac{1}{2})}$$

Blau

$\frac{1}{4} \cdot (1,1,1) = (\frac{1}{4},\frac{1}{4},\frac{1}{4}) \rightarrow$ 1 weißes Subpixel
$\frac{1}{2} \cdot (0,0,1) = (0,0,\frac{1}{2}) \rightarrow$ 2 blaue Subpixel
$\frac{1}{4} \cdot (1,1,0) = (\frac{1}{4},\frac{1}{4},0) \rightarrow$ 1 gelbes Subpixel

$$\overline{(\tfrac{1}{2},\tfrac{1}{2},\tfrac{3}{4})}$$

Man erkennt auch hier den Unterschied zu reinem Rot (1,0,0), Grün (0,1,0) und Blau (0,0,1).

Türkis, Magenta & Gelb

Will man jedoch eine Grundfarbe des CMY-Systems codieren, dann sollte man die Subpixel auf der Geheimbildfolie so wählen, dass (im Vergleich zur Färbung der Schlüsselfolie) stets Weiß und die Farbe, die codiert werden soll, vertauscht sind und die anderen beiden auf ihren Plätzen bleiben. Für die CMY-Grundfarben bedeutet das im Einzelnen: wenn Türkis verschlüsselt werden soll, dann müssen Magenta und Gelb an ihren Stellen bleiben und Weiß mit Türkis den Platz tauschen. Bei Magenta als zu codierender Farbe tauschen Weiß und Magenta ihre Positionen und Türkis und Gelb bleiben. Und wenn Gelb verschlüsselt werden soll, dann müssen die Positionen von Weiß und Gelb umgedreht werden und Türkis und Magenta behalten ihre bei.

Werden dann der Schlüssel und das Geheimbild übereinander gelegt, bekommen wir zwei Subpixel mit der Farbe, die verschlüsselt werden soll, und je ein Subpixel mit den anderen beiden Grundfarben des CMY-Farbmodells. Warum gerade diese Farben herauskommen, dürfte offensichtlich sein: subtraktives Mischen von zweimal der selben Farbe ergibt wieder diese und wenn eine Farbe mit Weiß gemischt wird (egal ob additiv oder subtraktiv), so bleibt sie immer erhalten.
Wenn die Farben anschließend additiv gemischt werden, haben wir folglich ein Subpixel in jeder Grundfarbe (also türkis, magentafarben und gelb) und ein zusätzliches in der Farbe, die codiert wird. Da die additive Mischung alle Grundfarben optisch Weiß ergibt, erhalten wir eine blasse Form der Farbe, die das vierte Subpixel hat, also genau die, die auch entstehen soll.

Türkis

$\frac{1}{2} \cdot (0,1,1) = (0,\frac{1}{2},\frac{1}{2}) \rightarrow$ 2 türkise Subpixel
$\frac{1}{4} \cdot (1,0,1) = (\frac{1}{4},0,\frac{1}{4}) \rightarrow$ 1 magentafarbenes Subpixel
$\frac{1}{4} \cdot (1,1,0) = (\frac{1}{4},\frac{1}{4},0) \rightarrow$ 1 gelbes Subpixel

$\overline{(\frac{1}{2},\frac{3}{4},\frac{3}{4})}$

Magenta

$\frac{1}{4} \cdot (0,1,1) = (0,\frac{1}{4},\frac{1}{4}) \rightarrow$ 1 türkises Subpixel
$\frac{1}{2} \cdot (1,0,1) = (\frac{1}{2},0,\frac{1}{2}) \rightarrow$ 2 magentafarbene Subpixel
$\frac{1}{4} \cdot (1,1,0) = (\frac{1}{4},\frac{1}{4},0) \rightarrow$ 1 gelbes Subpixel

$\overline{(\frac{3}{4},\frac{1}{2},\frac{3}{4})}$

Gelb

$\frac{1}{4} \cdot (0,1,1) = (0,\frac{1}{4},\frac{1}{4}) \rightarrow$ 1 türkises Subpixel
$\frac{1}{4} \cdot (1,0,1) = (\frac{1}{4},0,\frac{1}{4}) \rightarrow$ 1 magentafarbenes Subpixel
$\frac{1}{2} \cdot (1,1,0) = (\frac{1}{2},\frac{1}{2},0) \rightarrow$ 2 gelbe Subpixel

$\overline{(\frac{3}{4},\frac{3}{4},\frac{1}{2})}$

Die genauen Abweichungen von reinem Türkis (0,1,1), Magenta (1,0,1) beziehungsweise Gelb (1,1,0) können erneut anhand der Summierung der Rot-, Grün- und Blauanteile verdeutlicht werden.

In der folgenden Abbildung 4.8 wird gezeigt, wie man mit einer beliebigen Subpixelfärbung alle sieben Farben codieren kann.
Die komplette Auflistung aller Kombinationsmöglichkeiten für alle Farben in diesem System ist im Anhang auf den Abbildungen 8.1 (Seite 43, Kombinationen für Weiß), 8.2 (Seite 44, Kombinationen für Rot), 8.3 (Seite 44, Kombinationen für Grün), 8.4 (Seite 45, Kombinationen für Blau), 8.5 (Seite 45, Kombinationen für Türkis), 8.6 (Seite 46, Kombinationen für Magenta) und 8.7 (Seite 46, Kombinationen für Gelb) zu finden.

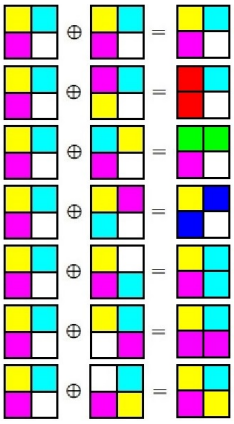


Abbildung 4.8: Codierung aller sieben Farben mit der gleichen Subpixelfärbung (von oben nach unten: Weiß, Rot, Grün, Blau, Türkis, Magenta, Gelb)

4.4.2 Optimalitätsbeweis

Auch dieser Beweis (für die Optimalität des in Abschnitt 4.4.1 vorgestellten Verfahrens) ist auf die von Andreas Klein verfasste Quelle [Kle] zurückzuführen. Alle dafür benötigten (Farb-)Werte sind in Tabelle 4.2 auf Seite 36 zu finden.

Wir beginnen, indem wir zeigen, dass Lemma 6 gilt.

Lemma 6 *Die Anzahl der Subpixel (bei jeder zulässigen Färbung), welche in den einzelnen Grundfarben eines Farbsystems gefärbt sind, ist gleich groß. Das bedeutet es sind immer genau gleich viele rote, grüne und blaue Subpixel beziehungsweise genau gleich viele türkise, magentafarbene und gelbe Subpixel vorhanden.*

Während des Optimalitätsbeweises des 4-Farben-Systems (Abschnitt 4.3.2) haben wir bereits gezeigt, dass die Summen der einzelnen Farbanteile aller Subpixel auf den Folien immer gleich groß seien müssen, wenn man Weiß beziehungsweise Schwarz codieren möchte ($\sum_{Rotanteile} = \sum_{Grünanteile} = \sum_{Blauanteile}$, siehe Hilfssatz 2).

Dies schließt allerdings nicht mit ein, dass auch die Anzahl der Subpixel, die in den einzelnen Grundfarben gefärbt sind, gleich sein muss (bei dem 4-Farben-System hatte es ausgereicht, Gelb (1,1,0) stellvertretend für Rot (1,0,0) und Grün (0,1,0) zu benutzen). Hier wollen wir neben Weiß aber noch Rot, Grün, Blau, Türkis, Magenta und Gelb verschlüsseln.
Es gibt fünf verschiedene Varianten, mit welchen Farben man die Subpixel färben kann, mit denen ein gleiches Verhältnis der einzelnen Farbanteile zueinander realisierbar ist:
(Durch das gleiche Verhältnis der Farbanteile zueinander wissen wir, dass sich auf jeden Fall Weiß codieren lässt. Außerdem kann Weiß als weitere Farbe hinzugenommen werden, da diese das Verhältnis der einzelnen Farbanteile zueinander nicht beeinflusst. Es geht hier in erster Linie darum zu zeigen, mit welchen Farbkombinationen die sieben Farben (Rot, Grün, Blau, Türkis, Magenta, Gelb und Weiß) überhaupt dargestellt werden können (wie gut/schlecht spielt in diesem Moment noch keine Rolle).)

1. **1 Komplementärfarbenpaar:** Durch ein Komplementärfarbenpaar lassen sich nicht alle sieben Farben darstellen.
   Gegenbeispiel: wir nutzen Rot (1,0,0) und Türkis (0,1,1). Man kann nie einen Blauwert erreichen, der ungleich dem Grünwert ist, da diese beiden Farbanteile bei allen Farben gleich groß sind. Es lassen sich also weder Blau noch Grün noch Gelb oder Magenta darstellen.
   Analog lässt sich der Gegenbeweis auch für die anderen beiden Paare anwenden.
2. **2 Komplementärfarbenpaare:** Auch mit Hilfe von zwei Komplementärfarbenpaaren lassen sich nicht alle sieben Farben darstellen.
   Gegenbeispiel: wir nutzen Grün, Magenta, Blau und Gelb. Die dritte Grundfarbe des CMY-Farbmodells, also hier Türkis, lässt sich so nicht codieren. Subtraktiv kann Türkis nicht gemischt werden, es kann jedoch durch additive Farbmischung aus Grün und Blau gewonnen werden. Würde man aber zwei identische Folien aufeinander legen, so würden sich Blau und Grün nicht additiv miteinander mischen, sondern mit ihren Komplementärfarben zu Weiß werden. Das kann auch anhand der Addition der einzelnen Farbanteile gezeigt werden. (Diese würden hier stets gleich groß bleiben und somit Weiß darstellen.)
   Analog funktioniert dieser Gegenbeweis auch bei Rot-Türkis-Blau-Gelb und Rot-Türkis-Grün-Magenta.
3. **3 Komplementärfarbenpaare:** Drei Komplementärfarbenpaare bedeutet, wir haben Rot, Grün, Blau, Türkis, Magenta, Gelb und zusätzlich noch Weiß auf jeder Folie. Damit lassen sich alle sieben Farben realisieren.
   Egal ob wir Rot, Grün, Blau, Türkis, Magenta oder Gelb codieren wollen, wir müssen die Folien einfach nur so aufeinander platzieren, dass soviel der zu codierenden Farbe wie möglich auf Weiß und umgekehrt liegt und die restlichen

Farben auf sich selbst.

4. **Grundfarben des RGB-Farbsystems:** Mit Rot, Grün, Blau und zusätzlich Weiß können wir alle sieben Farben darstellen.
   Rot, Grün und Blau lassen sich dadurch realisieren, indem man einfach so viel wie möglich von der zu codierenden Farbe auf Weiß und umgekehrt legt und die anderen beiden Farben mit sich selbst subtraktiv mischt.
   Türkis, Magenta oder Gelb könnte man dadurch erhalten, indem man das Weiß der beiden Folien je zur Hälfte auf die beiden Farben legt, aus denen sich die zu codierende Farbe additiv mischen lässt. Bei der restlichen Folie legt man einfach jede Farbe auf sich selbst.
5. **Grundfarben des CMY-Farbsystems:** Mit Türkis, Magenta, Gelb und zusätzlich Weiß lassen sich ebenfalls alle sieben Farben darstellen.
   Um Türkis, Magenta oder Gelb zu codieren reicht es aus, die Folien so übereinander zu platzieren, dass soviel der zu codierenden Farbe wie möglich auf Weiß und umgekehrt liegt und die restlichen Farben auf sich selbst.
   Rot, Grün und Blau kann man darstellen, indem man die beiden Farben, aus denen sich die zu codierende Farbe subtraktiv mischen lässt, übereinander und die anderen Farben wieder auf sich selbst platziert.

Folglich bleiben nur drei Möglichkeiten: die Grundfarben des RGB-Farbsystems & Weiß, die Grundfarben des CMY-Farbsystems & Weiß und die Grundfarben beider Farbsysteme & Weiß. Welche dieser drei Varianten am Ende am besten zur Codierung von Rot, Grün, Blau, Türkis, Magenta, Gelb und Weiß geeignet ist, wird in den nachfolgenden Abschnitten geklärt. Aber egal welche Variante genommen wird, bei allen dreien muss das Verhältnis von Rot zu Grün zu Blau beziehungsweise von Türkis zu Magenta zu Gelb (also je die Anzahl der Subpixel) gleich sein, damit auch das Verhältnis der einzelnen Farbanteile zueinander im gesamten Pixel gleich bleibt. Somit ist Lemma 6 belegt.

Als nächstes ermitteln wir die optimalen Anteile des Pixels, die in den einzelnen Farben gefärbt sind.
Betrachten wir Magenta: (1,0,1). Damit der Rotanteil den Wert $\frac{3}{4}$ (siehe Tabelle 4.2, Seite 36) erreichen kann, darf höchstens $\frac{1}{4}$ des kompletten Pixels Türkis, Grün und Blau sein, denn dies sind die einzigen Farben, deren Rotwert gleich 0 ist (auch bei Schwarz ist der Rotwert 0, aber diese Farbe spielt in diesem System keine Rolle). Analog kann für den Blauanteil gesagt werden, dass es zusammen maximal $\frac{1}{4}$ Gelb, Grün und Rot (die Farben mit einem Blauanteil von 0) im Pixel geben darf, damit auch dieser Wert $\frac{3}{4}$ erreichen kann (siehe Tabelle 4.2, Seite 36). Da außerdem bei Magenta ein Grünanteil von 0 codiert werden soll, muss der Anteil des Pixels, der in Magenta, Rot und Blau gefärbt ist (den Farben mit einem Grünwert von 0), mindestens $\frac{1}{4}$ sein, damit überhaupt die Möglichkeit besteht, dass dieser Farbwert kleiner als die anderen beiden Farbwerte (Rot und Blau) werden kann.

Führt man nun analoge Rechnungen für Türkis und Gelb aus (diese sind ausführlich im Anhang auf Seite 47, Abschnitt 8.3 zu finden), ergibt sich Hilfssatz 7 (dabei sind stets die Anteile des Pixels in den entsprechenden Farben gemeint):

Hilfssatz 7 *Türkis + Magenta + Gelb + 2 · (Rot + Grün + Blau) = $\frac{3}{4}$*

Mit Hilfe von Lemma 6 und Hilfssatz 7 lassen sich nun die Größe des Rot-, Grün- beziehungsweise Blauanteils (hier bezeichnet als x) und des Türkis-, Magenta- bezeihungsweise Gelbanteils (hier bezeichnet als y) berechnen (Hilfssatz 8):

$\Rightarrow$ Türkis + Magenta + Gelb + 2 · (Rot + Grün + Blau) = $\frac{3}{4}$ | Rot=Grün=Blau=x
$\Rightarrow$ Türkis + Magenta + Gelb + 2 · 3x = $\frac{3}{4}$ | Türkis=Magenta=Gelb=y
$\Rightarrow$ 3y + 6x = $\frac{3}{4}$ | -6x
$\Rightarrow$ 3y = $\frac{3}{4}$ - 6x | ÷3
$\Rightarrow$ y = $\frac{1}{4}$ - 2x

Zusätzlich haben wir auch noch eine siebte Farbe, deren Anteil des Pixels (also wie viel des Pixels in dieser Farbe gefärbt wird) nun noch zu bestimmen ist: Weiß. Da am Ende ein ganzes Pixel entstehen muss, müssen die Anteile des Pixels, die in einer der sieben Farben gefärbt sind, zusammen *1* ergeben. Der Weißanteil (hier bezeichnet als z) ist (Hilfssatz 8):

$\Rightarrow$ 3x + 3y + z = 1 | y = $\frac{1}{4}$ - 2x
$\Rightarrow$ 3x + $\frac{3}{4}$ - 6x + z = 1 | - $\frac{3}{4}$
$\Rightarrow$ -3x + z = $\frac{1}{4}$ | + 3x
$\Rightarrow$ z = $\frac{1}{4}$ + 3x

Folglich sind die Anteile:

Hilfssatz 8 *Der Anteil des Pixels in Rot/Grün/Blau: x.*
Der Anteil des Pixels in Türkis/Magenta/Gelb: y = $\frac{1}{4}$ - 2x.
Der Anteil des Pixels in Weiß: z = $\frac{1}{4}$ + 3x.

Nun kann gezeigt werden, dass die Farbwerte dieses Verfahrens optimal sind. Wenn Weiß, also (1,1,1), codiert werden soll, dann müssen nach dem Übereinanderlegen der Folien weiße Subpixel und/oder gleich viele Subpixel von jeder Grundfarbe (Rot-Grün-Blau und/oder Türkis-Magenta-Gelb) entstehen, da sich diese additiv gemischt aufheben. Allerdings sind für die Verschlüsselung von Weiß nur die Grundfarben des RGB-Farbsystems allein nicht förderlich. Bei gleich großen Anteilen von Rot (1,0,0), Grün (0,1,0) und Blau (0,0,1), die je höchstens $\frac{1}{3}$ seien können, könnte maximal ($\frac{1}{3}$,$\frac{1}{3}$,$\frac{1}{3}$) entstehen, was eher als Schwarz anstatt Weiß interpretiert wird. Da wir außer Weiß noch andere Farben verschlüsseln wollen, dürfte klar sein, dass wir nie ein komplett weißes Pixel auf einer Folie haben werden. Folglich müssen nach dem Aufeinanderlegen der Folien Türkis, Magenta und Gelb zu gleichen Teilen da sein. Da diese drei Farben nicht subtraktiv gemischt werden können (außer man legt eine der Farben auf sich selbst oder Weiß) können wir Hilfssatz 9 ableiten:

Hilfssatz 9 *Ein Teil jedes Pixels muss in Türkis, in Magenta und in Gelb (im gleichen Verhältnis zueinander) gefärbt sein.*

Zudem wird mindestens ein weißes Subpixel gebraucht, um auch die anderen Farben codieren zu können (sonst würden wir es nie schaffen, dass ein Farbwert höher oder niedriger als die anderen wird). Wenn wir nun versuchen, die Anteile an Türkis, Magenta und Gelb zu maximieren, müssen wir das x aus Hilfssatz 8 auf 0 setzen, denn nur so kann y aus Hilfssatz 8 den maximalen Wert von $\frac{1}{4}$ erlangen. Die Konsequenz davon wäre ein Weißanteil z von ebenfalls $\frac{1}{4}$ (siehe Hilfssatz 8).
Also muss Lemma 10 gelten:

Lemma 10 *Der bestmögliche Wert, der für Weiß erlangt werden kann, ist* $(\frac{3}{4},\frac{3}{4},\frac{3}{4})$.

Dieser Wert (aus Lemma 10) kann nur durch das Übereinanderlegen zweier identischer Subpixelfärbungen mit je $\frac{1}{4}$ Türkis, Magenta, Gelb und Weiß erreicht werden. An dieser Stelle kann zudem bereits gesagt werden, dass es nicht nötig ist, Rot, Grün oder Blau auf einer der Folien zu haben, da diese zum einen nicht für das Mischen von Weiß, Türkis, Magenta oder Gelb nötig sind und zum anderen da sie aus Türkis, Magenta und Gelb (die auf jeden Fall auf den Folien vorkommen) subtraktiv gemischt werden können.
Es gilt Hilfssatz 11.

Hilfssatz 11 *Auf keiner Folie muss Rot, Grün oder Blau vorkommen.*

Es reicht also aus, wenn jedes Pixel zu je $\frac{1}{4}$ aus Weiß, Türkis, Magenta und Gelb besteht, um alle sieben Farben codieren zu können und das Maximum für Weiß rauszuholen.

Als nächstes zeigen wir, dass dann Lemma 12 gilt:

Lemma 12 *Die optimalen Werte* $(\frac{1}{2},\frac{3}{4},\frac{3}{4})$ *für Türkis,* $(\frac{3}{4},\frac{1}{2},\frac{3}{4})$ *für Magenta und* $(\frac{3}{4},\frac{3}{4},\frac{1}{2})$ *für Gelb werden nur dann erlangt, wenn jedes Pixel zu genau* $\frac{1}{4}$ *aus den Farben Weiß, Türkis, Magenta und Gelb besteht.*

Damit auch die Codierung von Türkis optimal wird, müssen die Folien so übereinander platziert werden, dass Rot auf Rot, Grün auf Grün, Blau auf Blau, Magenta auf Magenta und Gelb auf Gelb liegt. Warum gerade diese Farben? Türkis hat die Farbwerte (0,1,1), also wird ein möglichst hoher Grün- und Blauanteil benötigt, und Rot (1,0,0), Blau (0,0,1) und Magenta (1,0,1) sind die drei Farben mit einem Grünanteil von 0 beziehungsweise Rot (1,0,0), Grün (0,1,0) und Gelb (1,1,0) die Farben mit einem Blauanteil von 0. Für die bestmögliche Codierung von Weiß benötigen wir Pixel, die aus Türkis, Magenta, Gelb und Weiß zu je $\frac{1}{4}$ bestehen, auf den einzelnen Folien. In diesem Fall müssten dann für die bestmögliche Codierung von Türkis Magenta auf Magenta und Gelb auf Gelb liegen.

Und die anderen beiden Farben? Abgesehen von den hohen Grün- und Blauanteilen ist noch ein möglichst geringer Rotanteil nötig. Da Weiß einen Rotanteil von 1 besitzt, ist es nicht von Vorteil, wenn Weiß auf Weiß liegen würde. Also bleibt nur die Variante, Weiß auf Türkis und umgekehrt zu legen. So würde subtraktiv Türkis dominieren, welches hier codiert werden soll und dementsprechend ideale Rot-, Grün- und Blauanteile hat.
Durch zusätzliches Rot, Grün und Blau auf den Folien würden die einzelnen Farbanteile des gesamten Pixels um den selben Subtrahend (dessen Größe davon abhängig ist, wie viel des Pixels man Rot, Grün und Blau färben würde) verringert werden, was für den Rotanteil von Vorteil wäre, da dieser so nah wie möglich an 0 sein soll, sich aber auf den Grün- und Blauanteil nachteilig auswirkt, da diese kleiner werden würden, obwohl sie eigentlich so nah wie möglich an 1 sein sollten.
Folglich kann Türkis nicht besser codiert werden, als mit Pixeln, die zu je $\frac{1}{4}$ aus Weiß, Türkis, Magenta und Gelb bestehen, was zu den Farbwerten $(\frac{1}{2},\frac{3}{4},\frac{3}{4})$ führt.
Durch analoge Überlegungen für Magenta und Gelb, wobei die Farben nur zyklisch vertauscht werden müssen, gelangt man zu dem Ergebnis, dass Lemma 12 gelten muss.

Zum Schluss zeigen wir noch, dass auch Lemma 13 gilt:

Lemma 13 *Wenn jedes Pixel zu genau $\frac{1}{4}$ aus den Farben Weiß, Türkis, Magenta und Gelb besteht, dann sind die bestmöglichen Farbwerte, die für Rot, Grün und Blau erlangt werden können: $(\frac{3}{4},\frac{1}{2},\frac{1}{2})$ für Rot, $(\frac{1}{2},\frac{3}{4},\frac{1}{2})$ für Grün und $(\frac{1}{2},\frac{1}{2},\frac{3}{4})$ für Blau.*

Wir wissen bereits, dass wir die bestmöglichen Werte für Weiß, Türkis, Magenta und Gelb nur dann erhalten können, wenn jedes Pixel zu je $\frac{1}{4}$ aus eben diesen Farben besteht. Folglich ist es an dieser Stelle nur logisch, diese Färbung des Pixels beizubehalten, wenn die Codierung von Rot, Grün und Blau betrachtet wird.
Wenn man zum Beispiel Rot verschlüsseln will, dann sollte man stets versuchen, den Rotanteil zu maximieren und die Grün- und Blauanteile zu minimieren. Rot lässt sich subtraktiv aus Magenta und Gelb mischen, also ist es nur logisch, diese beiden Farben übereinander zu positionieren. Somit erhalten wir bereits einen Rotanteil von $\frac{1}{2}$, während der Grün- und der Blauanteil bei 0 bleiben. Nun sind noch Türkis und Weiß auf den Folien übrig. Da Türkis das Komplement von Rot ist und demzufolge einen Rotanteil von 0 und einen Grün- und Blauanteil von 1 hat, ist es am besten, so wenig wie möglich türkise Subpixel zu haben. Es bleibt also nur die eine Möglichkeit, Türkis auf Türkis und Weiß auf Weiß zu platzieren. Somit gibt es keine besseren Farbwerte für die Codierung von Rot als $(\frac{3}{4},\frac{1}{2},\frac{1}{2})$.
Auch hier können wieder analoge Überlegungen für Grün und Blau angestellt werden, wodurch gezeigt wird, dass es für Rot, Grün und Blau keine bessere Verschlüsselung als diese gibt, ohne die optimale Codierung für Weiß, Türkis, Magenta und Gelb wieder zu zerstören. Es gilt also Lemma 13.

Ergo kann aus den Lemmas 10, 12 und 13 der folgende Satz 14 abgeleitet werden.

Satz 14 *Das in Abschnitt 4.4.1 beschriebene Verfahren ist optimal für die Verschlüsselung der sieben Farben Rot, Grün, Blau, Türkis, Magenta, Gelb und Weiß.*

Farbe	RGB-Werte optimal	RGB-Werte codiert	Güte
Weiß	(1,1,1)	$(\frac{3}{4},\frac{3}{4},\frac{3}{4})$	$(\frac{1}{4},\frac{1}{4},\frac{1}{4})$
Rot	(1,0,0)	$(\frac{3}{4},\frac{1}{2},\frac{1}{2})$	$(\frac{1}{4},\frac{1}{2},\frac{1}{2})$
Grün	(0,1,0)	$(\frac{1}{2},\frac{3}{4},\frac{1}{2})$	$(\frac{1}{2},\frac{1}{4},\frac{1}{2})$
Blau	(0,0,1)	$(\frac{1}{2},\frac{1}{2},\frac{3}{4})$	$(\frac{1}{2},\frac{1}{2},\frac{1}{4})$
Türkis	(0,1,1)	$(\frac{1}{2},\frac{3}{4},\frac{3}{4})$	$(\frac{1}{2},\frac{1}{4},\frac{1}{4})$
Magenta	(1,0,1)	$(\frac{3}{4},\frac{1}{2},\frac{3}{4})$	$(\frac{1}{4},\frac{1}{2},\frac{1}{4})$
Gelb	(1,1,0)	$(\frac{3}{4},\frac{3}{4},\frac{1}{2})$	$(\frac{1}{4},\frac{1}{4},\frac{1}{2})$

Tabelle 4.2: Farbanteile für optimale Farbe, codierte Farbe und Güte der Farbanteile der einzelnen Farben im optimalen 7-Farben-System

5 Anwendungen

Beim Lesen dieser Bachelorarbeit oder anderer Texte über die (farbige) visuelle Kryptographie hat sich sicherlich jeder schon einmal die Frage gestellt, wozu man das Ganze eigentlich braucht. Wo wird visuelle Kryptographie im realen Leben genutzt?

Zum jetzigen Zeitpunkt findet die visuelle Kryptographie kaum praktische Anwendung. Nur in sehr seltenen und extremen Situationen wird sie ab und zu genutzt, zum Beispiel wenn man die Sicherheit eines modernen Kryptographieverfahrens nutzen möchte, aber kein Computer zur Verfügung steht um die Codierung zu berechnen. In einem solchen Fall kann es sinnvoller sein ein unkonventionelleres Verschlüsselungsverfahren zu nutzten, wie zum Beispiel die visuelle Kryptographie. [Kle07]

Einige konkretere Beispiele für Anwendungsmöglichkeiten wären:

1. Das Versenden eines verschlüsselten Faxes, wenn nur ein Faxgerät mit E-Mail-Anschluss, aber kein Rechner zur Verfügung steht.
2. Die Vermeidung von Betrug bei der Geldabbuchung von Geldkarten. (Wenn man mit einer Geldkarte bezahlt, dann ist es so, als würde man dem Verkäufer einfach sein Portemonnaie geben und ihm sagen, er soll sich den fälligen Betrag selbst heraus nehmen, ohne aber dabei zu kontrollieren, ob er auch wirklich nur so viel Geld raus nimmt wie man zahlen muss. Eine sehr einfache Lösung dieses Problemes wäre es, einfach alle Transaktionen zu protokollieren, aber dann würde auch jeder Geldkartennutzer zu einer Art „gläsernem Menschen“ werden, was nicht sonderlich viel Zuspruch finden würde. Wie die Lösungsmöglichkeit mittels der visuellen Kryptographie im Einzelnen aussieht kann der entsprechenden Quelle [Kle07] entnommen werden)

Die visuelle Kryptographie ist allerdings auch ein typisches Beispiel eines Secret-Sharing-Systems. Mit Secret-Sharing werden Techniken bezeichnet, die genutzt werden, um ein Geheimnis auf mehrere Komponenten aufzuteilen (wie bei der visuellen Kryptographie auf die einzelnen Folien). [Sta96] [Nao94]

In Zukunft wird die visuelle Kryptographie möglicherweise eine größere Rolle spielen, sie ist ja immerhin noch eine verhältnismäßig junge Wissenschaft und ihr Potential sicherlich noch nicht komplett ausgeschöpft. Momentan kann man jedoch nur sagen, dass die visuelle Kryptographie keine Schlüsselrolle bei der Sicherheit unserer Daten in der virtuellen Welt spielt.

6 Aussicht: Übertragung auf Töne

Geheime Botschaften lassen sich nicht nur in Texten und Bildern, sondern ebenso in Tönen verstecken. Die sogenannte Audio-Kryptographie nutzt Musikstücke, um darin Nachrichten einzubetten. Die verschlüsselte Nachricht erhalten wir nur dann, wenn wir alle Kanäle gleichzeitig abspielen. Ein einziger abgespielter Musikkanal liefert keinerlei Informationen über das Geheimnis, ebenso wie bei der visuellen Kryptographie einer einzelnen Folie keinerlei Information entnommen werden kann.

Grundlagen
Das System baut auf zwei Dingen auf: der Interferenzeigenschaft von Schallwellen (also des Klanges) und der Eigenschaft des menschlichen Hörsystems Phasenunterschiede wahrzunehmen.
Interferenz: Ein Klang ist eine Druckwelle, die sich durch Luft, Wasser oder ein anderes Medium bewegt, wobei die Welle durch eine Abfolge von hohem und niedrigem Druck entsteht. Wenn nun zwei dieser Wellen aufeinander treffen spricht man von Interferenz. Treffen dabei zwei Teile mit hohem beziehungsweise zwei Teile mit niedrigem Druck aufeinander, dann verstärken sie sich und wenn dabei zwei Teile unterschiedlichen Druckes aufeinander treffen, so heben sie sich gegenseitig auf und es gibt keinen Ton mehr (siehe Abbildung 6.1). Man könnte auch sagen, das Interferenz-Prinzip verhält sich wie eine XNOR-Verknüpfung (00→1, 01→0, 10→0, 11→1).
Phasenunterscheidung: Anhand der Ankunftszeit einer Klangwelle am linken und am rechten Ohr (den Phasenunterschied) können wir die Richtung und Entfernung der Audioquelle lokalisieren.

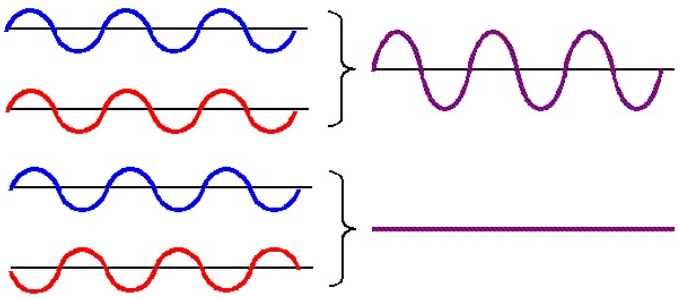


Abbildung 6.1: Verstärkung (oben) und Auslöschung (unten) von Wellen [int]

Grundidee
Das Ziel ist es, die Botschaft in einer Hülle (einem Musikstück) zu verstecken. Dazu beginnen wir mit dem entsprechenden Musikstück, welches wir so in zwei Teile aufteilen, dass diese einzeln abgespielt ganz normal wirken, zusammen abgespielt jedoch die geheime Botschaft freigeben.
Der erste Musikteil *S1* wird durch einen zufälligen Münzwurf b (also zu 50% 1 und zu 50% 0) erzeugt und der zweite Musikteil *S2* durch b *XNOR* S, wobei S das zu codierende Bit der geheimen Nachricht ist.

Ablauf: Codierung
Für die Codierung benötigen wir folgende Parameter:

- S: Klartext in Form einer Reihe von Bits (Binärzahlen)
- L: Länge (Anzahl der Bits) des Klartextes S
- T: Anzahl der Sekunden die für 1 Bit der geheimen Nachricht S nötig sind

$\Rightarrow$ wir benötigen $T \cdot L$ Sekunden um eine Botschaft der Länge L zu verschlüsseln

- B: Verhüllungsmusikstück, welches mindestens $T \cdot L$ Sekunden lang ist

Anschließend erfolgt die Codierung wie folgt:

- *S1* wird mit B initialisiert. Aller T Sekunden von *S1* gibt es einen Münzwurf b. Ist $b = 0$, geschieht nichts, ansonsten wird das entsprechende Bit von *S1* zu diesem Zeitpunkt mit *-1* multipliziert (180° Phasenverschiebung).
- *S2* wird mit B initialisiert. Aller T Sekunden von *S2* errechnen wir mit dem Wert b des Münzwurfes zum selben Zeitpunkt bei *S1* $b' = b$ *XNOR* S (dabei ist S zum Zeitpunkt $1 \cdot T$ das 1. Bit von S, zum Zeitpunkt $2 \cdot T$ das 2. Bit von S etc.). Ist $b' = 0$, geschieht auch hier nichts, ansonsten wird ebenfalls das entsprechende Bit von *S2* zu diesem Zeitpunkt mit *-1* multipliziert.

Zusammengefasst: ist das n-te Bit des Klartextes eine 1, dann sind *S1* und *S2* zum Zeitpunkt $n \cdot T$ gleich, und ist das Bit 0, so sind sie ungleich.

Ablauf: Decodierung
Es gibt zwei Wege die geheime Botschaft zu entschlüsseln, die eine nutzt die Interferenz und die andere die Phasenwahrnehmungseigenschaft des menschlichen Hörsystems.
Methode 1 - Interferenz: Zunächst werden zwei Lautsprecher sehr nah beieinander und sich zugewandt aufgestellt. Dann senden wir *S1* zu dem einen und *S2* zu dem anderen Lautsprecher.
Beim gleichzeitigen Abspielen der beiden Musikteile kann man nun Lautstärkeänderungen feststellen. Wird es lauter, dann haben wir ein geheimes Bit mit 1 und wenn es leiser wird, dann haben wir eine 0 als geheimes Bit.
Diese Methode kann jedoch sehr leicht gestört werden, zum Beispiel durch die Reflektion des Klanges von einer Wand.

Methode 2 - Phasenunterschied: Ein Lautsprecher wird zur Linken und einer zur Rechten des Hörers aufgestellt (erneut sich zugewandt). Dann senden wir *S1* zu dem einen und *S2* zu dem anderen Lautsprecher.
Beim Hören der Musikteile kann man nun bemerken, dass sich die Klangquelle von den Seiten zur Mitte (und umgekehrt) bewegt (das kommt durch einen Phasenunterschied). Ist das geheime Bit eine 0, dann befinden sich die Kanäle in verschiedenen Phasen und dem Hörer erscheint es so, als komme eine Quelle von rechts und eine von links. Ist das geheime Bit jedoch eine 1, dann müssen sich die Signale der beiden Kanäle in der selben Phase befinden, was dem Hörer das Gefühl vermittelt, dass nur eine Quelle aus der Mitte kommt und die andere von rechts beziehungsweise links.
Diese Methode kann alternativ auch mit Kopfhörern realisiert werden.

Wie die visuelle Kryptographie zählt die Audio-Kryptographie zu den Secret-Sharing-Systemen. Das Geheimnis wird auf mehrere Komponenten verteilt, wobei der Hörer einer einzelnen Komponente (Musikteil) nicht in der Lage ist zu unterscheiden, ob diese eine geheimte Botschaft enthalten könnte oder nicht. Der Geheimhaltungsgrad ist also ziemlich hoch.
Das in diesem Kapitel vorgestellte Verfahren, sowie alles Dazugehörende, entstammen Quelle [Des98], verfasst von Yvo Desmedt, Shuang Hou & Jean-Jacques Quisquater.

7 Zusammenfassung

Wir wissen jetzt, dass die (farbige) visuelle Kryptographie die Co- und Decodierung von Bildern ist. Zudem haben wir zwei Verfahren der farbigen visuellen Kryptographie ausführlicher kennen gelernt und deren Optimalität bewiesen. Und wir haben gelernt, dass die (farbige) visuelle Kryptographie eher theoretisch ist und in der Praxis bisher kaum Anwendung findet. Sie hat jedoch auch einen sehr großen Vorteil gegenüber vielen anderen Kryptosystemen, weshalb es trotzdem sinnvoll ist sich weiterhin mit ihr zu beschäftigen. Die meisten traditionellen Kryptographieverfahren haben den Nachteil, dass man, sobald ihre Methode bekannt ist, relativ leicht an die geheime Nachricht gelangen kann. Nicht so jedoch die visuelle Kryptographie. Sie ist in diesem Punkt ein vollkommen sicheres Verfahren. [Des98]

An dieser Stelle sollte zudem noch erwähnt werden, dass die in dieser Bachelorarbeit genannte Menge an Verfahren der visuellen Kryptographie nicht komplett ist. Es gibt noch zahlreiche weitere Verfahren, auf die hier nicht näher eingegangen wurde. Man könnte etwa das Bild auf mehr als zwei Folien verteilen, die Pixel anders als in vier oder neun Subpixel zerteilen oder noch mehr als sieben Farben codieren. Einige Beispiele lassen sich in den Quellen [Kle05], [Kle07] und [Hou03] finden.

Abschließend möchte ich noch auf die Kernprobleme bei der (farbigen) visuellen Kryptographie hinweisen, denen wir nicht nur innerhalb dieser Bachelorarbeit mehrfach begegnet sind, sondern die sich auch darüber hinaus in eigentlich jedem Schriftstück über diese Thematik wiederfinden lassen:

1. Sich zulässigen Färbungen der Subpixel ausdenken und das Konstruieren von Paaren aus diesen, um die verschiedenen Farben des Bildes repräsentieren zu können.
2. Minimierung des Kontrastverlustes, der sich hierbei nicht vermeiden lässt.

Durch die Erweiterung von Schwarzweiß- auf Farbbilder ergeben sich zwei zusätzliche Erschwernisse:

3. Die verschiedenen Farbmodelle und Farbmischungen müssen verstanden und umgesetzt werden, um bestimmte Farben codieren zu können.
4. Der Kontrast des Systems kann nicht größer als die Differenz zwischen der Codierung von Weiß und der Codierung von Schwarz sein.

Diese vier Punkte sind an die Hauptprobleme der visuellen Kryptographie aus Quelle [Kle] von Andreas Klein angelehnt.

8 Anhang

8.1 Nebenrechnung für den Beweis der Optimalität des 4-Farben-Systems

Schwarz als dritte Farbe neben Blau und Gelb:

Um Schwarz zu codieren werden die Folien so übereinander platziert, dass Blau auf Gelb liegt und Gelb auf Blau. Die dritte Farbe (Schwarz) bleibt an der selben Stelle.

$$\begin{array}{l} \frac{2}{3} \cdot (0,0,0) = (0,0,0) \rightarrow \text{Schwarz} \\ \frac{1}{3} \cdot (0,0,0) = \underline{(0,0,0)} \rightarrow \text{Schwarz} \\ \qquad\qquad\quad (0,0,0) \end{array}$$

Um Weiß zu codieren werden die Folien so übereinander platziert, dass stets die selben Farben auf einander liegen.

$$\begin{array}{l} \frac{1}{3} \cdot (0,0,1) = (0,0,\frac{1}{3}) \rightarrow \text{Blau} \\ \frac{1}{3} \cdot (1,1,0) = (\frac{1}{3},\frac{1}{3},0) \rightarrow \text{Gelb} \\ \frac{1}{3} \cdot (0,0,0) = \underline{(0,0,0)} \rightarrow \text{Schwarz} \\ \qquad\qquad\quad (\frac{1}{3},\frac{1}{3},\frac{1}{3}) \end{array}$$

Weiß als dritte Farbe neben Blau und Gelb:

Um Schwarz zu codieren werden die Folien so übereinander platziert, dass Blau auf Gelb liegt und Gelb auf Blau. Die dritte Farbe (Weiß) bleibt an der selben Stelle.

$$\begin{array}{l} \frac{2}{3} \cdot (0,0,0) = (0,0,0) \rightarrow \text{Schwarz} \\ \frac{1}{3} \cdot (1,1,1) = \underline{(\frac{1}{3},\frac{1}{3},\frac{1}{3})} \rightarrow \text{Weiß} \\ \qquad\qquad\quad (\frac{1}{3},\frac{1}{3},\frac{1}{3}) \end{array}$$

Um Weiß zu codieren werden die Folien so übereinander platziert, dass stets die selben Farben auf einander liegen.

$$\begin{array}{l} \frac{1}{3} \cdot (0,0,1) = (0,0,\frac{1}{3}) \rightarrow \text{Blau} \\ \frac{1}{3} \cdot (1,1,0) = (\frac{1}{3},\frac{1}{3},0) \rightarrow \text{Gelb} \\ \frac{1}{3} \cdot (1,1,1) = \underline{(\frac{1}{3},\frac{1}{3},\frac{1}{3})} \rightarrow \text{Weiß} \\ \qquad\qquad\quad (\frac{2}{3},\frac{2}{3},\frac{2}{3}) \end{array}$$

8.2 Codierungsmöglichkeiten für das 7-Farben-System

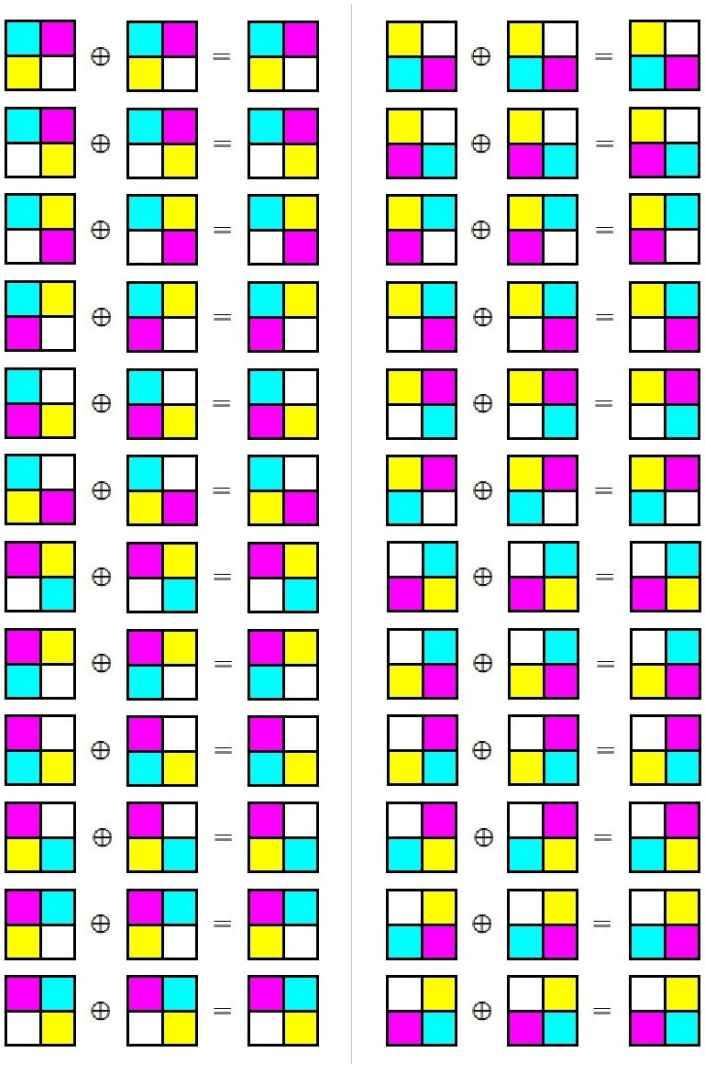


Abbildung 8.1: Alle Codierungsmöglichkeiten für Weiß im 7-Farben-System

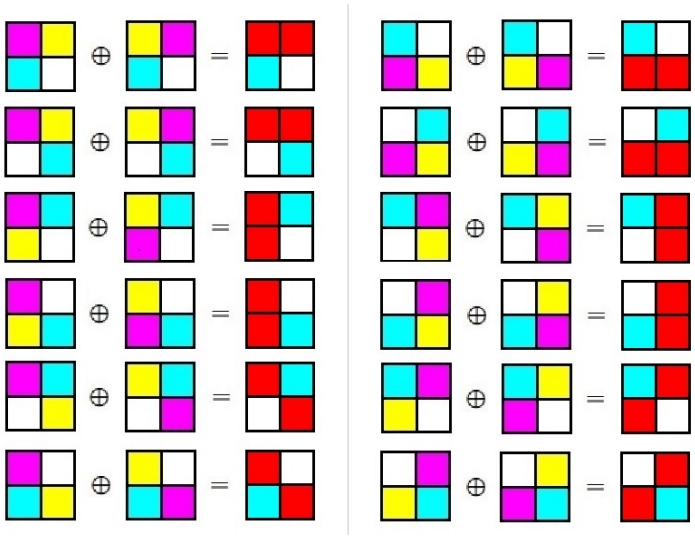


Abbildung 8.2: Alle Codierungsmöglichkeiten für Rot im 7-Farben-System

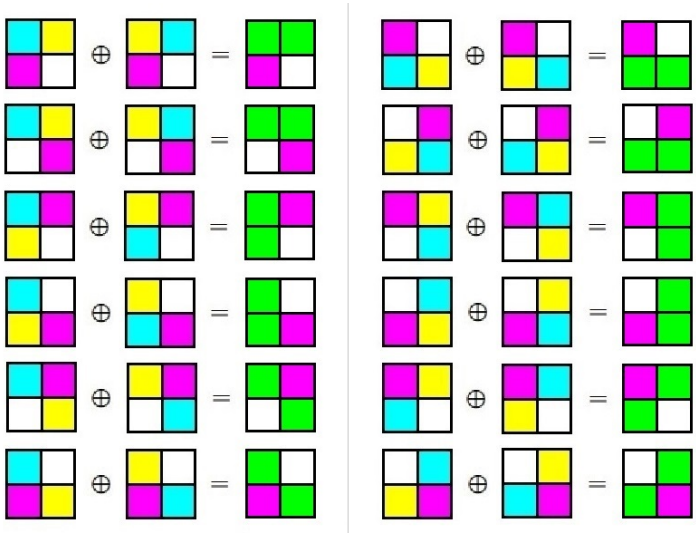


Abbildung 8.3: Alle Codierungsmöglichkeiten für Grün im 7-Farben-System

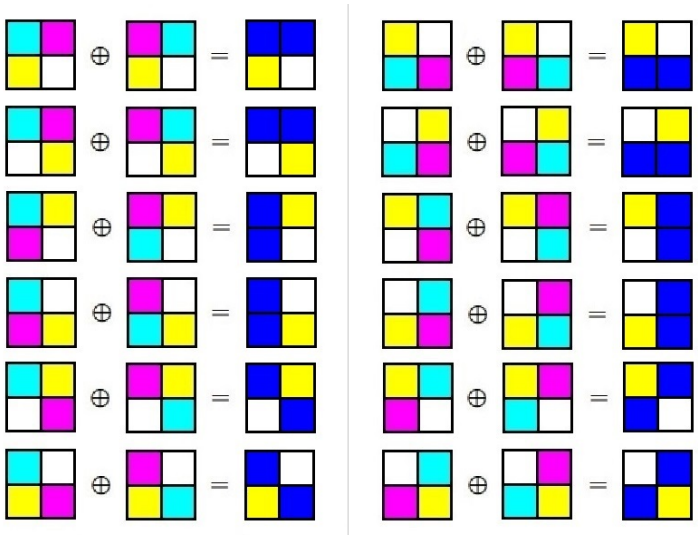


Abbildung 8.4: Alle Codierungsmöglichkeiten für Blau im 7-Farben-System

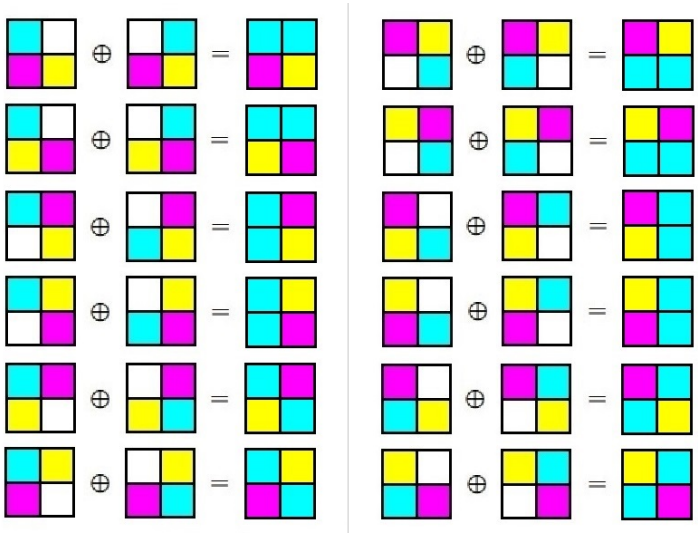


Abbildung 8.5: Alle Codierungsmöglichkeiten für Türkis im 7-Farben-System

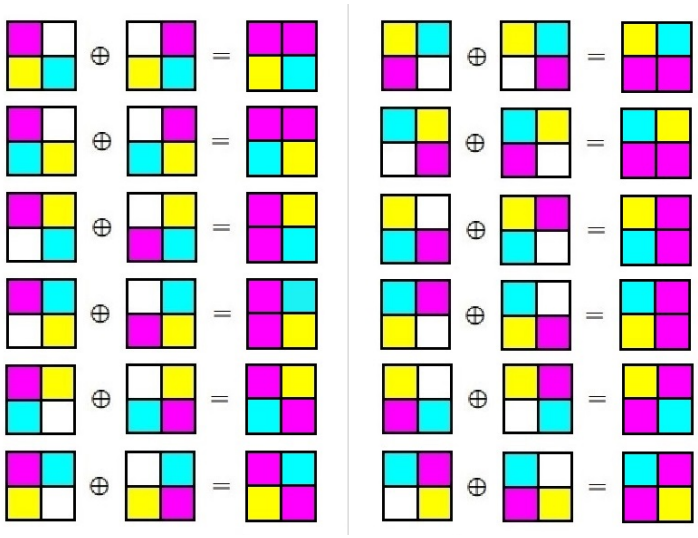


Abbildung 8.6: Alle Codierungsmöglichkeiten für Magenta im 7-Farben-System

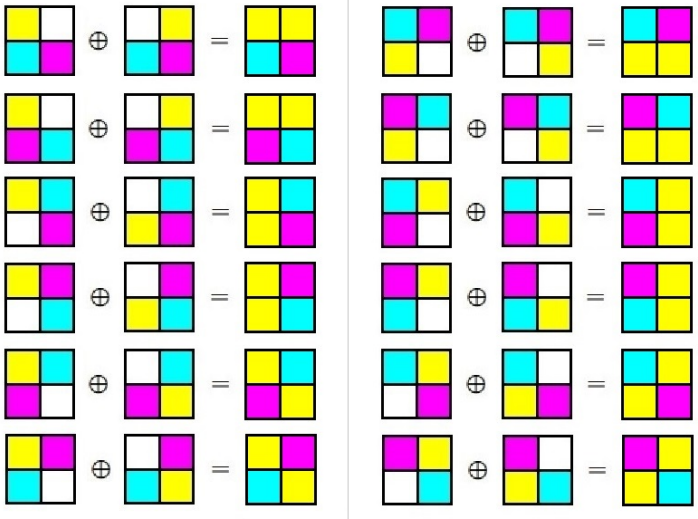


Abbildung 8.7: Alle Codierungsmöglichkeiten für Gelb im 7-Farben-System

8.3 Nebenrechnung für den Beweis der Optimalität des 7-Farben-Systems

Türkis: rein (0,1,1), codiert $(\frac{1}{2},\frac{3}{4},\frac{3}{4})$
- Rotanteil: Türkis + Grün + Blau $\geq \frac{1}{4}$
- Grünanteil: Magenta + Blau + Rot $\leq \frac{1}{4}$
- Blauanteil: Gelb + Rot + Grün $\leq \frac{1}{4}$

Magenta: rein (1,0,1), codiert $(\frac{3}{4},\frac{1}{2},\frac{3}{4})$
- Rotanteil: Türkis + Grün + Blau $\leq \frac{1}{4}$
- Grünanteil: Magenta + Blau + Rot $\geq \frac{1}{4}$
- Blauanteil: Gelb + Rot + Grün $\leq \frac{1}{4}$

Gelb: rein (1,1,0), codiert $(\frac{3}{4},\frac{3}{4},\frac{1}{2})$
- Rotanteil: Türkis + Grün + Blau $\leq \frac{1}{4}$
- Grünanteil: Magenta + Blau + Rot $\leq \frac{1}{4}$
- Blauanteil: Gelb + Rot + Grün $\geq \frac{1}{4}$

$\Longrightarrow$ Türkis + Grün + Blau $= \frac{1}{4}$
Magenta + Blau + Rot $= \frac{1}{4}$
Gelb + Rot + Grün $= \frac{1}{4}$

$\Longrightarrow$ Türkis+Grün+Blau + Magenta+Blau+Rot + Gelb+Rot+Grün $= \frac{1}{4}+\frac{1}{4}+\frac{1}{4}$

$\Longrightarrow$ Türkis + Magenta + Gelb + $2 \cdot$ (Rot + Grün + Blau) $= \frac{3}{4}$

Abbildungsverzeichnis

Tabellenverzeichnis

Literaturverzeichnis

[ban13] Zahlen, Daten, Fakten der Kreditwirtschaft, Bundesverband deutscher Banken e. V., 2013, online verfügbar auf https://bankenverband.de/publikationen/ods/bb-weitere-statistiken-ueber-banken-in-deutschland/?searchterm=fakten%20und%20zahlen; zuletzt abgerufen am 11.12.2013.

[Bec08] Becker, Johannes: RSA-Verschlüsselung, Techn. Ber., 2006/2008, online verfügbar auf http://www.uni-giessen.de/~g013/code/rsa6.pdf; zuletzt abgerufen am 11.12.2013.

[buc] Buch-Verschlüsselung, www.wikipedia.de, online verfügbar auf http://de.wikipedia.org/wiki/Buchcode; zuletzt abgerufen am 15.11.2013.

[Des98] Desmedt, Yvo & Hou, Shuang & Quisquater, Jean-Jacques: Advances in cryptology – ASIACRYPT '98, Vol. 1514, Kap. Audio and Optical Cryptography, Springer, 1998, online verfügbar auf http://link.springer.com/content/pdf/10.1007%2F3-540-49649-1_31.pdf; zuletzt abgerufen am 20.11.2013.

[Hou03] Hou, Young-Chang: Pattern Recognition 36, Kap. Visual cryptography for color images, Elsevier Science Ltd., 2003, online verfügbar auf http://csis.bits-pilani.ac.in/faculty/murali/netsec-10/seminar/refs/muralikrishna3.pdf; zuletzt abgerufen am 15.10.2013.

[int] Interferenz und Beugung, www.uni-kiel.de, online verfügbar auf http://www.tf.uni-kiel.de/matwis/amat/mw1_ge/kap_2/basics/b2_1_6.html; zuletzt abgerufen am 24.11.2013.

[Kin05] King, Stephen: Es, Weltbild, 2005.

[Kle] Klein, Andreas: Farbige visuelle Kryptographie, Techn. Ber., online verfügbar auf http://www.mathematik.uni-kassel.de/sites/downloads/prep0105.pdf; zuletzt abgerufen am 14.11.2013.

[Kle05] Klein, Andreas: Eine Einführung in die visuelle Kryptographie, DMV-Mitteilungen, 2005, online verfügbar auf http://www.mathematik.de/ger/presse/ausdenmitteilungen/artikel/mdmv13-1-054-klein.pdf; zuletzt abgerufen am 10.10.2013.

[Kle07] Klein, Andreas: Visuelle Kryptographie, Springer, 2007.

[kry] Kryptographie, www.wikipedia.de, online verfügbar auf http://de.wikipedia.org/wiki/Kryptographie; zuletzt abgerufen am 05.11.2013.

[Nao94] Naor, Moni & Shamir, Adi: Visual cryptography, Advances in cryptology – EUROCRYPT '94, 1994, online verfügbar auf http://books.google.de/books?id=gytHgadVA5sC&pg=PA1&lpg=PA1&dq=visual+cryptography+eurocrypt&source=bl&ots=Ns3zYnuFjs&sig=BdDMy-3VwHeDwskQOVc8i6JoJok&hl=de&sa=X&ei=A-qqUtyDEcKWtQbmxoCIAQ&ved=0CF0Q6AEwBA#v=onepage&q=visual%20cryptography%20eurocrypt&f=false; zuletzt abgerufen am 11.12.2013.

[rgb] RGB und CMYK, www.lez.ch, online verfügbar auf http://www.lez.ch/con/cms/front_content.php?idcat=3&artid=7&ridcat=3; zuletzt abgerufen am 19.08.2013.

[rsa] RSA-Kryptosystem, www.wikipedia.de, online verfügbar auf http://de.wikipedia.org/wiki/RSA-Kryptosystem; zuletzt abgerufen am 15.11.2013.

[Sta96] Stadler, Markus: Publicly Verifiable Secret Sharing, Advances in cryptology – EUROCRYPT '96, 1996, online verfügbar auf http://download.springer.com/static/pdf/687/chp%253A10.1007%252F3-540-68339-9_17.pdf?auth66=1387107281_d999cbbff90a89779eb28ecb1d38c0b4&ext=.pdf; zuletzt abgerufen am 11.12.2013.

TECHNISCHE UNIVERSITÄT CHEMNITZ

Zentrales Prüfungsamt
(Anschrift: TU Chemnitz, 09107 Chemnitz)

Selbstständigkeitserklärung*

Name: Vorname: geb. am: Matr.-Nr.:	**Bitte Ausfüllhinweise beachten:** 1. Nur Block- oder Maschinenschrift verwenden.

Ich erkläre gegenüber der Technischen Universität Chemnitz, dass ich die vorliegende selbstständig und ohne Benutzung anderer als der angegebenen Quellen und Hilfsmittel angefertigt habe.

Die vorliegende Arbeit ist frei von Plagiaten. Alle Ausführungen, die wörtlich oder inhaltlich aus anderen Schriften entnommen sind, habe ich als solche kenntlich gemacht.

Diese Arbeit wurde in gleicher oder ähnlicher Form noch bei keinem anderen Prüfer als Prüfungsleistung eingereicht und ist auch noch nicht veröffentlicht.

Datum: ..... Unterschrift: .....

* Diese Erklärung ist der eigenständig erstellten Arbeit als Anhang beizufügen.