

Farbige visuelle Kryptographie

Andreas Klein

26. Februar 2001

1 Einführung

Visuelle Kryptographie ist eine noch junge Form der Kryptographie, die sichere Verfahren zu Verfügung stellt, ein Bild so zu verschlüsseln, daß es vom menschlichen Auge entschlüsselt werden kann (siehe [3]). Der Schlüssel wird dabei durch eine Folie realisiert, die über die Nachricht gelegt wird.

Die Hauptprobleme der visuellen Kryptographie sind:

1. Konstruktion von Paaren von Makropixel, die die verschiedenen Farben des Bildes repräsentieren.
2. Durch das Verschlüsseln geht immer Kontrast verloren. Dieser Kontrastverlust muß minimiert werden.

Bisher beschränkten sich Arbeiten zur visuellen Kryptographie meist auf schwarz-weiß Bilder und untersuchten die Fragen 1 und 2 im Hinblick auf die Konstruktion von k aus n Shared-Secret-Systemen (siehe z.B. [2] und [1]).

In dieser Arbeit verallgemeinern wir das Konzept der visuellen Kryptographie von dem Verschlüsseln von schwarz-weiß Bildern auf das Verschlüsseln von Farbbildern. Im Vergleich mit der visuellen Kryptographie von schwarz-weiß Bildern treten dabei zwei neue Schwierigkeiten auf.

1. Es wird nötig, sich mit Farbmischung und Farbmodellen zu beschäftigen, um zu untersuchen, wie eine bestimmte Farbe codiert werden kann.
2. Der Kontrast des Verschlüsselungssystems kann nicht mehr als die Helligkeitsdifferenz zwischen der Codierung von weiß und der Codierung von schwarz definiert werden.

Der nächste Abschnitt zeigt, wie man diese zusätzlichen Schwierigkeiten beheben kann.

In den dann folgenden Abschnitten wird jeweils ein spezielles Verfahren behandelt. Das Hauptaugenmerk wird dabei auf die Fälle mit möglichst guten Kontrastwerten gerichtet, die sich auch praktisch anwenden lassen.

2 Farbmischung und Farbmodelle

Bei der farbigen visuellen Kryptographie kommen zwei verschiedene Arten der Farbmischung zur Geltung. Legt man zwei verschiedene farbige Folien übereinander, so werden die Farben subtraktiv gemischt (CMYK-Modell).



Abbildung 1: Subtraktive Farbmischung

Wir können daher einen schwarzen Punkt durch rot auf der ersten Folie und cyan auf der zweiten Folie darstellen.

Liegen die Punkte auf den Folien nebeneinander, so erscheinen die Farben additiv gemischt (RGB-Modell).



Abbildung 2: Additive Farbmischung

Man sieht zwar immer noch die einzelnen Farben, aber ein Makropixel mit einem Drittel weiß, einem Drittel rot und einem Drittel cyan erscheint als ein sehr heller Farbton. (Im Gegensatz zu weiß bei perfekter additiver Mischung.) Bei einem Makropixel mit zwei Drittel Rot und einem Drittel cyan kann man wie folgt rechnen:

Ein Drittel rot und ein Drittel cyan heben sich auf. Das restliche Drittel rot sorgt für einen mattroten Farbton.

Bei schwarz-weißer visueller Kryptographie benutzt man den Helligkeitsunterschied zwischen dem Grauton für die Codierung von weiß und dem Grauton für die Codierung von schwarz, d.h. den Kontrast als Maßzahl für die Güte des

Systems. Im Fall von farbiger visueller Kryptographie gibt es keinen so einfachen Vergleich zwischen den verschiedenen Farben. Wir benutzen das folgende System, um die Güte des Verfahrens zu messen.

Definition 1

Für zwei Farben a und b seien der rot, grün und blau Anteil (a_1, a_2, a_3) bzw. (b_1, b_2, b_3) . (Dabei liegen a_i, b_i zwischen 0 und 1. Z.B. weiß ist $(1, 1, 1)$ und rot ist $(1, 0, 0)$.) Der Abstand der Farben a und b ist definiert durch

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

Wir werden die Güte des Systems zur visuellen Kryptographie als den Abstand, der durch additive Farbmischung entstandenen Farbe des Makropixels, zu der codierten Farbe messen. Wir nennen ein System optimal, wenn es kein anderes System gibt, das für alle codierten Farben kleinere Abstände erreicht.

Beispiel 2

Bei dem klassischen System zur Verschlüsselung von schwarz-weiß Bildern wird ein schwarzer Bildpunkt durch einen Makropixel aus 4 schwarzen Pixeln dargestellt. Ein weißer Bildpunkt wird jedoch durch einen Makropixel von 2 weißen und 2 schwarzen Punkten dargestellt. Die Güte des System ist demnach $(0, 0, 0)$ für die Darstellung von schwarz (d.h. schwarze Punkte werden perfekt wiedergegeben) und $(0.5, 0.5, 0.5)$ für die Darstellung von weiß. (Weiß = $(1, 1, 1)$, aber weiß wird durch einen Makropixel der zur Hälfte schwarz ist codiert. Dieser Makropixel hat den Wert $(0.5, 0.5, 0.5)$.)

Man sieht auch leicht, daß das System optimal ist, d.h. es gibt kein anderes System, das bessere Werte für weiß und schwarz liefert.

3 Reduktion auf Methoden für schwarz-weiß Bilder

Ein einfacher Ansatz zur Realisierung von farbiger Kryptographie ist das Zurückführen auf die Methoden für schwarz-weiß Bilder. Der Vorteil dieses Ansatzes ist, daß man auf bereits vorhandene Algorithmen aufbauen kann. Der Nachteil dieser Methode ist, daß sie deutlich schlechtere Kontrastwerte liefert als speziell für den farbigen Fall entwickelte Methoden. Im folgenden Satz zeigen wir wie man ausgehend von dem einfachen System aus Beispiel 2 ein System zur farbigen visuellen Kryptographie konstruieren kann. Analog läßt sich jedes andere System zur Verschlüsselung von schwarz-weiß Bildern erweitern.

Satz 3

Seien f_0, f_1, \dots, f_n beliebige Farben mit $f_0 = \text{weiß}$. Durch die folgende Vorschrift wird ein farbiges visuelles Kryptographiesystem mit den Farben f_0, f_1, \dots, f_n realisiert:

- Jeder Makropixel besteht aus $2n$ Teilen p_1, \dots, p_{2n} .

- Auf jeder Folie ist mit Wahrscheinlichkeit $p = \frac{1}{2}$ der Teil p_{2i} von der Farbe f_i und der Teil p_{2i-1} weiß bzw. umgekehrt.
- Die Teile p_{2i} und p_{2i-1} haben auf beiden Folien genau dann die gleiche Farbe, wenn die Farbe des codierten Bildpunkts verschieden von f_i ist.

Beweis

Gemäß der Konstruktion ist die Farbe weiß = f_0 durch den Makropixel P_0 mit n weißen Teilen und je einem Teil in jeder der Farben f_1, \dots, f_n codiert. Die Farbe f_i ($1 \leq i \leq n$) wird durch den Makropixel P_i mit $n-1$ weißen Teilen, 2 Teilen in der Farbe f_i und je einem Teil in den Farben f_j mit $1 \leq j \leq n$ und $j \neq i$ codiert.

P_1, \dots, P_n haben daher mehr Farbanteile als P_0 . P_0 erscheint demnach heller als P_1, \dots, P_n . Da P_i zwei Teile der Farbe f_i und nur je einen Teil der Farben f_j ($j \neq i$) enthält, liegt der Farbeindruck von P_i näher bei f_i als bei allen anderen Farben. \square

Beispiel 4

Wir benutzen Satz 3, um ein System zu konstruieren, das die Farben weiß, rot, cyan und schwarz codieren kann.

Dabei erreichen wir folgende Farbwerte bei den Codierungen

Farbe	RGB-Wert	RGB-Wert der Codierung	Güte
weiß	(1, 1, 1)	(4/6, 4/6, 4/6)	(1/3, 1/3, 1/3)
rot	(1, 0, 0)	(4/6, 3/6, 3/6)	(1/3, 1/2, 1/2)
cyan	(0, 1, 1)	(3/6, 4/6, 4/6)	(1/2, 1/3, 1/3)
schwarz	(0, 0, 0)	(3/6, 3/6, 3/6)	(1/2, 1/2, 1/2)

Man sieht, daß die Werte für die Güte der Codierung relativ schlecht sind. Im nächsten Abschnitt werden wir ein besseres Verfahren angeben.

4 Folien in 4 Farben

Als erstes Beispiel eines optimalen Systems zur farbigen visuellen Kryptographie betrachten wir ein System mit zwei Folien, das außer weiß und schwarz noch eine Farbe und ihre Komplementärfarbe zuläßt. Als Beispiel wählen wir rot und cyan. Das Verfahren funktioniert jedoch mit beliebigen Paaren von komplementären Farben.

Die Makropixel der einzelnen Folien müssen dazu zu je einem Drittel die Farben weiß, rot und cyan enthalten. Diese Farben können nicht durch subtraktive Farbmischung gewonnen werden. Im Gegensatz dazu erzeugen wir schwarz nur durch subtraktive Farbmischung aus rot und cyan. Wir wählen als Makropixel die sechs verschiedenen 3×3 Raster, die durch Permutation der Farben in Abbildung 3 entstehen.

Die vier verschiedenen Farben werden durch die folgenden Kombinationen dargestellt (Abbildung 4):

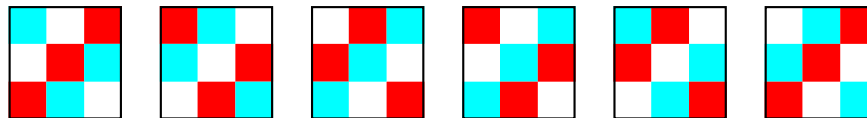


Abbildung 3: Die sechs verschiedenen Makropixel

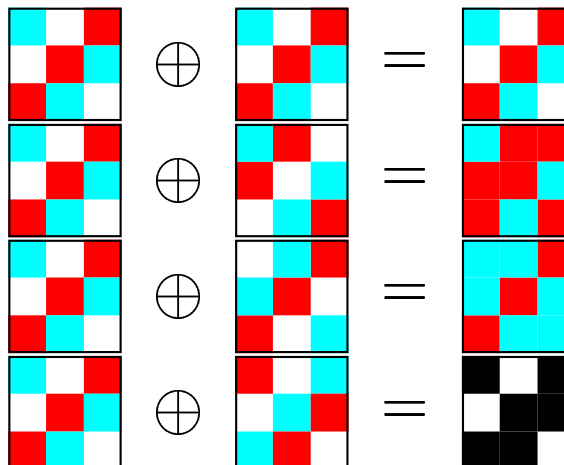


Abbildung 4: Kombination der Makropixel

Bei der ersten Kombination erhält man weiß als Farbeindruck, da sich die beiden Komplementärfarben „optisch“ aufheben. Im zweiten und dritten Fall bleibt nach dem Aufheben der Komplementärfarben jeweils noch ein Drittel rot bzw. cyan über. Es ergibt sich also ein schwach roter bzw. cyan Farbton. Im vierten Fall erhält man ein Makropixel mit zwei Drittel schwarz und einem Drittel weiß, d.h. es entsteht ein dunkelgrauer Farbton.

Man wählt nun für die erste Folie einen der sechs Makropixel mit der Wahrscheinlichkeit $\frac{1}{6}$ aus. Der Makropixel für die zweite Folie wird entsprechend der Zielfarbe gewählt. Man sieht sofort, daß unabhängig von der codierten Farbe jeder der sechs Makropixel mit Wahrscheinlichkeit $\frac{1}{6}$ auftritt, d.h. keine Folie allein liefert Information über das codierte Bild.

Satz 5

Es gibt kein Verfahren, das alle vier Farben (weiß, rot, cyan, schwarz) besser codiert als das oben beschriebene, d.h. das oben angegebene Verfahren ist optimal.

Beweis

Das beschriebene Verfahren hat folgende Werte für die Darstellung der einzelnen Farben:

Farbe	RGB-Wert	RGB-Wert der Codierung	Güte
weiß	(1, 1, 1)	(2/3, 2/3, 2/3)	(1/3, 1/3, 1/3)
rot	(1, 0, 0)	(2/3, 1/3, 1/3)	(1/3, 1/3, 1/3)
cyan	(0, 1, 1)	(1/3, 2/3, 2/3)	(1/3, 1/3, 1/3)
schwarz	(0, 0, 0)	(1/3, 1/3, 1/3)	(1/3, 1/3, 1/3)

Wir zeigen zunächst, daß es kein Verfahren gibt, das sowohl für weiß als auch für schwarz bessere Werte erreicht. Angenommen ein Verfahren erreicht mindestens die Güte $(1/3, 1/3, 1/3)$ für weiß, dann darf jede Folie höchstens ein Drittel von jeder der drei Grundfarben enthalten.

Legen wir die beiden Folien übereinander, kann maximal zwei Drittel der Fläche von rot bedeckt sein, das restliche Drittel hat ein Farbwert von $(?, 1, 1)$. Entsprechende Überlegungen für cyan ergeben, daß beim Übereinanderlegen der beiden Folien immer ein Farbwert (x, y, z) mit $x, y, z \geq \frac{2}{3}$ entsteht.

Falls schwarz durch den Wert $(1/3, 1/3, 1/3)$ codiert wird, folgt, daß jede Folie genau $1/3$ rot und $1/3$ cyan Anteil hat. Es folgt weiter, daß die Werte für rot bzw. cyan im besten Fall $(2/3, 1/3, 1/3)$ bzw. $(1/3, 2/3, 2/3)$ sind. \square

5 Ein allgemeines 2 aus n System

Die praktische Umsetzung von farbigen k aus n Shared-Secret-System scheitert bereits bei kleinen Werten von k und n an der notwendigen Größe der Makropixel und dem mangelhaften Kontrast. Insbesondere die Fälle mit $k > 2$ haben ausgesprochen schlechte Kontrastwerte. Für den einfachen Fall eines drei Farbensystems (weiß, schwarz und eine weitere Farbe) kann man jedoch ein effizientes 2 aus n Shared-Secret-System konstruieren.

Die Makropixel bestehen aus $(n + 1) \times (n + 1)$ -Subpixeln. Jeder Makropixel besteht aus einer schwarzen und einer Spalte mit der Farbe f . Es gibt demnach $(n + 1)n$ verschiedene Makropixel.

Einen weißen Punkt codieren wir, indem wir für jede Folie denselben Makropixel wählen. Bei einem Punkt der Farbe f färben wir auf jeder Folie dieselbe Spalte schwarz (z.B. Spalte $n + 1$). Die Spalten mit Farbe f wechseln auf jeder Folie (z.B. Spalte i auf Folie i wird mit f gefärbt). Bei schwarzen Punkten werden die Rollen von f bzw. schwarz vertauscht.

Satz 6

Das oben beschriebene Verfahren realisiert ein 2 aus n Shared-Secret-System.

Beweis

Gemäß Konstruktion treffen beim Übereinanderlegen der Folien entweder zwei Subpixel mit der gleichen Farbe aufeinander oder eine farbige Stelle trifft auf eine durchsichtige Stelle. Es tritt also nie der Fall einer subtraktiven Farbmischung ein.

Die dritte Farbe f habe den RGB-Wert (x, y, z) . Ein weißer Makropixel wird durch $n - 1$ weiße Subpixel, einen Subpixel der Farbe f und einen schwarzen Subpixel codiert. Daher hat ein weißer Makropixel den Farbwert

$(\frac{n-1+x}{n+1}, \frac{n-1+y}{n+1}, \frac{n-1+z}{n+1})$. Entsprechend haben die Makropixel von der Farbe f den Farbwert $(\frac{n-2+2x}{n+1}, \frac{n-2+2y}{n+1}, \frac{n-2+2z}{n+1})$ und die schwarzen Makropixel den Wert $(\frac{n-2+x}{n+1}, \frac{n-2+y}{n+1}, \frac{n-2+z}{n+1})$.

Da $0 \leq x, y, z \leq 1$ gilt, sind die weißen Makropixel am hellsten (und werden daher als weiß wahrgenommen). Die schwarzen Makropixel sind am dunkelsten. Da in den Makropixel der Farbe f die Werte x, y, z mit doppeltem Gewicht eingehen, wird er als entsprechend heller Ton der Farbe f wahrgenommen. \square

Um die Optimalität des Verfahrens zu beweisen, benötigen wir noch eine zusätzliche Voraussetzung an die dritte Farbe. Wir können jedoch den folgenden Satz beweisen:

Satz 7

Das oben beschriebene Shared-Sercet-System mit den Farben weiß, rot (bzw. grün, blau, cyan, magenta oder gelb) und schwarz ist optimal.

Beweis

Um die Formulierungen möglichst einfach zu halten, führen wir den Beweis nur für den Fall, daß die dritte Farbe rot ist, durch. Die anderen fünf Farben lassen sich mit denselben Argumenten behandeln.

Ein weißer Makropixel wird durch die Farbe $(\frac{n}{n+1}, \frac{n-1}{n+1}, \frac{n-1}{n+1})$ codiert, daher kann kein Makropixel zu mehr als $\frac{1}{n+1}$ schwarz gefärbt sein.

Da ein schwarzer Makropixel durch die Farbe $(\frac{n-1}{n+1}, \frac{n-2}{n+1}, \frac{n-2}{n+1})$ codiert wird, muß jeder Makropixel genau $\frac{1}{n+1}$ Teile schwarz enthalten.

Nun folgt aus dem Farbwert der Codierung für weiß, daß kein Makropixel mehr als $\frac{1}{n+1}$ Teil rot enthält. Aus den Werten für rot folgt, daß jeder Makropixel genau zu $\frac{1}{n+1}$ Teilen rot ist.

D.h. die einzelnen Makropixel müssen die Form, wie im obigen Verfahren beschrieben, haben. Aus den Werten für die einzelnen Farben folgt nun direkt, daß auch die Codierung der Farben auf beiden Folien dem oben beschriebenen Verfahren entsprechen muß. \square

6 Folien in 7 Farben

Das folgende Schema zur farbigen visuellen Kryptographie benutzt auf jeder Folie die drei Grundfarben des CMYK-Modells (cyan, magenta, gelb). Es können die folgenden sieben Farben codiert werden: weiß, cyan, magenta, gelb, rot, grün und blau).

Jeder Punkt wird durch einen Makropixel, der aus vier Teilen besteht, codiert. Dabei hat jeweils ein Teil die Farbe cyan, magenta bzw. gelb. Der letzte Teil ist durchsichtig (weiß). Es gibt also $4! = 24$ verschiedene Makropixel. Jeder dieser Makropixel wird mit gleicher Wahrscheinlichkeit verwendet.

Wir müssen nun für alle sieben Farben angeben, wie sie durch Übereinanderlegen der Folien erzeugt werden.

Dieses Verfahren erreicht folgende Werte bei der Approximation der einzelnen Farben:

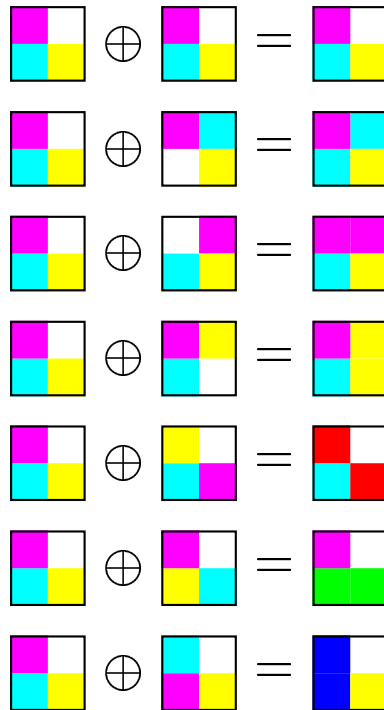


Abbildung 5: Visuelle Kryptographie mit sieben Farben

Farbe	RGB-Wert	RGB-Wert der Codierung	Güte
weiß	(1, 1, 1)	(3/4, 3/4, 3/4)	(1/4, 1/4, 1/4)
cyan	(0, 1, 1)	(1/2, 3/4, 3/4)	(1/2, 1/4, 1/4)
magenta	(1, 0, 1)	(3/4, 1/2, 3/4)	(1/4, 1/2, 1/4)
gelb	(1, 1, 0)	(3/4, 3/4, 1/2)	(1/4, 1/4, 1/2)
rot	(1, 0, 0)	(3/4, 1/2, 1/2)	(1/4, 1/2, 1/2)
grün	(0, 1, 0)	(1/2, 3/4, 1/2)	(1/2, 1/4, 1/2)
blau	(0, 0, 1)	(1/2, 1/2, 3/4)	(1/2, 1/2, 1/4)

Satz 8

Das oben beschriebene Verfahren ist optimal.

Beweis

Im ersten Schritt zeigen wir, daß die Anteile von rot, grün und blau bzw. cyan, magenta und gelb in jedem Makropixel gleich sind.

Betrachten wir die Werte für die Farbe cyan, so sehen wir, daß die Anteile von gelb, rot und grün in jedem Makropixel zusammen höchstens 1/4 sein können, denn anderenfalls wäre der blau Anteil von jeder möglichen Farbe kleiner als

$3/4$. Analog folgt, daß auch der magenta, rot und blau Anteil kleiner als $1/4$ ist.

Da der rot Anteil bei der Codierung von cyan kleiner als $1/2$ ist, muß auf jeder Folie der Anteil der Farben cyan, grün und blau mindestens $1/4$ sein, denn man kann nur dann einen Punkt ohne rot Anteil erhalten, wenn auf mindestens einer Folie eine dieser Farben vorkommt.

Aus analoger Betrachtung für die Farben magenta und gelb ergeben sich entsprechende Abschätzungen, wobei cyan, magenta und gelb bzw. rot, grün und blau zyklisch vertauscht werden. Addition dieser Abschätzungen liefert, daß der Anteil von cyan, magenta und gelb plus dem doppelten Anteil von rot, grün und blau genau $3/4$ sein muß. Daher gilt in allen Abschätzungen die Gleichheit.

Durch die Abschätzungen bei der Codierung von magenta folgt, daß der blau Anteil gleich dem grün Anteil sein muß. Zyklisches vertauschen der Farben liefert: Auf jeder Folie sind genau x Teile rot, grün bzw. blau. Die Anteile von cyan, magenta und gelb betragen jeweils $1/4 - 2x$. Demnach sind die restlichen $1/4 + 3x$ Teile jedes Makropixels weiß.

Nun können wir direkt nachrechnen, daß die Farbwerte des oben angegebenen Verfahrens optimal sind.

Die bestmögliche Darstellung von weiß wird erreicht, wenn auf beiden Folien der gleiche Makropixel verwendet wird. In diesem Fall ist der Farbwert $(3/4, 3/4, 3/4)$, d.h. kein System erreicht eine bessere Codierung von weiß als das oben angegebene.

Damit die Codierung von cyan mindestens $3/4$ Anteile grün enthält, müssen in den beiden Makropixeln die Farben rot, blau und magenta übereinander liegen. Entsprechend müssen auch rot, grün und gelb übereinander liegen, damit der Anteil von $3/4$ blau erreicht wird. Es folgt, daß auf beiden Folien rot übereinander liegt. Außerdem folgt, daß der grün und der blau Anteil nicht höher als $3/4$ sein kann.

Damit der Anteil von der Farbe rot möglichst gering ist, muß der cyan Anteil einer Folie auf den weiß Anteil der anderen Folie treffen. Der rot Anteil ist demnach mindestens $x + 5x + 2 * (1/4 - 3x) = 1/2$. (Bei x Teilen sind beide Folien rot. Wenn die beiden cyan Anteile der Folien sich nicht überlappen, so haben die Folien genau $1/4 + 3x - (1/4 - 2x) = 5x$ Teile weiß gemeinsam. In jedem anderen Fall sind es mehr. Um möglichst viel rot Anteil von magenta auszublenden, muß man die x Teile blau auf der einen Folie mit dem magenta der anderen Folie mischen. Es bleiben trotzdem noch mindestens $1/4 - 3x$ Teile magenta übrig. Analog liefert auch der gelbe Teil beider Folien $1/4 - 3x$ rot Anteile.) Daher kann kein System eine bessere Approximation als $(1/2, 3/4, 3/4)$ für cyan erreichen. Aus Symmetriegründen folgt, daß auch magenta und gelb nicht besser als in dem oben angegebenen Verfahren dargestellt werden können.

Da kein Makropixel mehr als $3/4$ Anteile rot enthält, kann der rot Anteil nie größer als $3/4$ werden. Um möglichst viele Anteile von blau und grün auszulöschen, muß beim Übereinanderlegen rot immer auf weiß und magenta immer auf gelb treffen. Außerdem können x Teile grün bzw. blau ausgelöscht werden, wenn man den blauen bzw. grünen Teil einer Folie über den cyan, weiß

oder grün bzw. blau Teil der anderen Folie legt. Es bleiben daher mindestens $3/4 + 2x + 3/4 - 2x + x - x = 1/2$ Teile blau bzw. grün übrig. (Dieser Wert ergibt sich als: $3/4 + 2x$ Teile weiß, $3/4 - 2x$ Teile cyan, x Teile blau. x Teile blau können durch subtraktive Farbmischung mit den x Teilen grün der anderen Folie ausgelöscht werden). Daher kann die Codierung von rot nie besser als $(3/4, 1/2, 1/2)$ sein. Aus der Symmetrie des Systems folgt, daß auch grün und blau nicht besser als in dem oben beschriebenen Verfahren codiert werden können.

Damit ist gezeigt, daß kein System bessere Werte bei der Codierung der Farben erreicht als das oben beschriebene. Dies ergibt sich, wenn man $x = 0$ wählt. \square

7 Beispiel

Da ein Beispiel oft mehr sagt als 1000 Worte, bringen wir am Ende noch ein Beispiel zweier Folien, die nach dem Verfahren aus Abschnitt 4 konstruiert wurden.

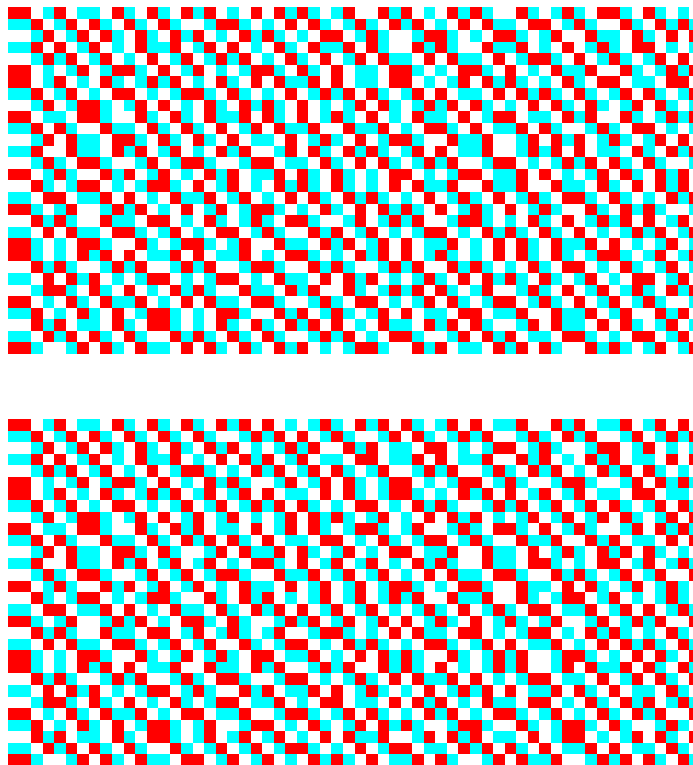


Abbildung 6: Ein Beispiel

Literatur

- [1] Carlo Blundo, Alfredo De Santis, and Douglas R. Stinson. On the contrast in visual cryptography schemes. *J. Cryptology*, 12(4):261–289, 1999.
- [2] Thomas Hofmeister, Matthias Krause, and Hans U. Simon. Contrast-optimal k out of n secret sharing schemes in visual cryptography. *Theor. Comput. Sci.*, 240(2):471–485, 2000.
- [3] Moni Naor and Adi Shamir. Visual cryptography. In Alfredo De Santis, editor, *Advances in cryptology - EUROCRYPT '94*, volume 950 of *Lect. Notes Comput. Sci.*, pages 1–12. Springer-Verlag, 1995.