# Visuele cryptografie met transparanten

Luc Van den Broeck

22 juli 2018

**Samenvatting**

In deze handleiding worden twee technieken beschreven voor visuele cryptografie. Bij de eerste techniek worden twee transparanten met schijnbaar willekeurige *patronen van zwarte blokjes* over elkaar geschoven om een geheime afbeelding tevoorschijn te laten komen. De tweede techniek gebruikt twee *afbeeldingen in grijstinten* die transparant over elkaar geschoven worden om een geheime afbeelding op te roepen. De enige voorkennis die nodig is om deze technieken te kunnen uitvoeren, is het gebruik van een rekenblad (hier: Excel) en van een fotobewerkingsprogramma.

## 1 Eerste techniek: geheimschrift met blokjes

### 1.1 Een geschikte zwartwitfoto zoeken

Voor het eerste deel van dit project heb je een geschikte zwartwitfoto nodig. Een foto met teveel grijswaarden bemoeilijkt de verwerking. De foto moet immers omgezet worden in een binaire tabel met de getallen 0 (voor zuiver witte pixels) en 1 (voor zuiver zwarte pixels). Voor dit doel worden best foto's gebruikt met massieve zwartpartijen bovenop een sneeuwwitte achtergrond.

Figuur 1: Twee silhouetfoto's

De makkelijkste manier om zulke foto's te verkrijgen, is door op de zoektermen *silhouet* of *silhouette* te googelen. Je vindt dan een grote collectie aan

personen, dieren en merkwaardige objecten (zie figuur 1). Creatieve leerlingen kunnen zelf een sterke tegenlichtfoto maken waarvan ze de achtergrond transparant maken via een fotobewerkingsprogramma (zie figuur 2).

Figuur 2: Een tegenlichtfoto uit Rio

De gekozen foto moet van een gebruiksvriendelijk type zijn (jpg of png) en moet verkleind worden naar een formaat waarbij zowel de breedte als de hoogte tussen de 100 en de 150 pixels bevat. Je kiest zelf met welk programma je deze herschaling doet. Je moet wel opletten dat je de lengte-breedteverhouding van de foto niet aanpast. De enige fout die je bij het herschalen kan maken, is het wijzigen van de *canvas size* in plaats van de *image size*.

## 1.2 Omzetten naar een binaire tabel


Figuur 3: Een tabel met nullen en enen

Het converteren van een afbeelding naar een binaire tabel is te moeilijk om dit zelf te programmeren. Een handige applet voor deze convertie vind je op het internet via de url: https://www.dcode.fr/binary-image. Je moet dan enkel je zwartwitafbeelding uploaden en aangeven dat je de *original size* wil behouden. Het resultaat van deze omzetting is een lijst met meer dan honderd lijnen waarop 'woorden' staan met meer dan honderd nullen en enen. In figuur 3 zie je een screenshot van een dergelijke omzetting.

De output bestaat echter *niet* uit aparte cellen met nullen en enen die je zomaar naar een rekenblad kan overhevelen. Wanneer je door deze tabel scrolt, merk je dat er al vlug meer dan 10000 nulletjes en eentjes moeten verwerkt worden. In paragraaf 1.3 leggen we uit hoe je deze massa aan nullen en enen kan omzetten naar Excel. Let op, je moet hiervoor wel een latere versie van Excel nemen. In oude versies kan je niet meer dan 256 kolommen naast elkaar zetten. Met een oudere versie kom je sowieso in de problemen als je twee stevige tekeningen (met een breedte van 150 tekens) naast elkaar wil zetten.

## 1.3 Een binary image importeren in Excel

Met knippen en plakken (met ctrl-C en ctrl-V) kan je de binaire tabel importeren in Excel. Maar het vraagt nog wel wat programmeerwerk om de originele afbeelding opnieuw in je Excelsheet te kunnen zien.

Maak de cellen in de eerste kolom van je rekenblad vooraf op als tekstvelden. Kopieer dan pas de volledige binary image in cel A2. Je ziet nu dat alle cellen in de eerste kolom vanaf A2 gevuld worden met de opeenvolgende lijnen uit de binary image. Normaal springen deze getallen (die meer dan honderd nullen en enen bevatten) automatisch over in wetenschappelijke notatie en zo kan heel wat kostbare informatie verloren gaan. Maar door de opmaak van de eerste kolom als tekstveld gebeurt dit niet en blijven de grote getallen helemaal zichtbaar.

Om de binaire getallen (die hier als tekst zijn weergegeven) op te splitsen in afzonderlijke cijfers, moet je in de eerste rij (vanaf cel B1) de hulpgetallen 1, 2, 3, ... plaatsen, tot zover het nodig is (dus tot het aantal kolommen van de binaire tabel). In cel B2 zet je een formule om het eerste cijfertje uit het eerste binaire getal te plukken. Deze formule (zie ook figuur 4) is:

$$= \text{ALS}(\text{DEEL}(\$A2; B\$1; 1) = \text{"1"}; 1; 0) \tag{1}$$

Met DEEL($A2; B$1; 1) plukken we een gedeelte van het woord in cel A2, te beginnen van de positie aangegeven in cel B1 en 1 symbool lang. Als dat ene symbool gelijk is aan de letter "1"dan noteer je het cijfer 1 in cel B2, anders noteer je het cijfer 0. Deze formule moet worden doorgesleept door het hele getallenveld. De dolartekens in de formules zorgen ervoor dat bepaalde celverwijzingen absoluut zijn en dat ze zich niet aanpassen tijdens het doorslepen.

Tot slot voegen we een likje verf aan de tabel toe. Met de optie 'voorwaardelijke opmaak' kan je alle velden met inhoud 0 een witte achtergrond- en letterkleur geven en die met inhoud 1 een zwarte achtergrond- en letterkleur. Als je geen fouten hebt gemaakt, verschijnt na de voorwaardelijke opmaak de originele figuur terug, zij het met een getrapte omtrekslijn (zie figuur 5).

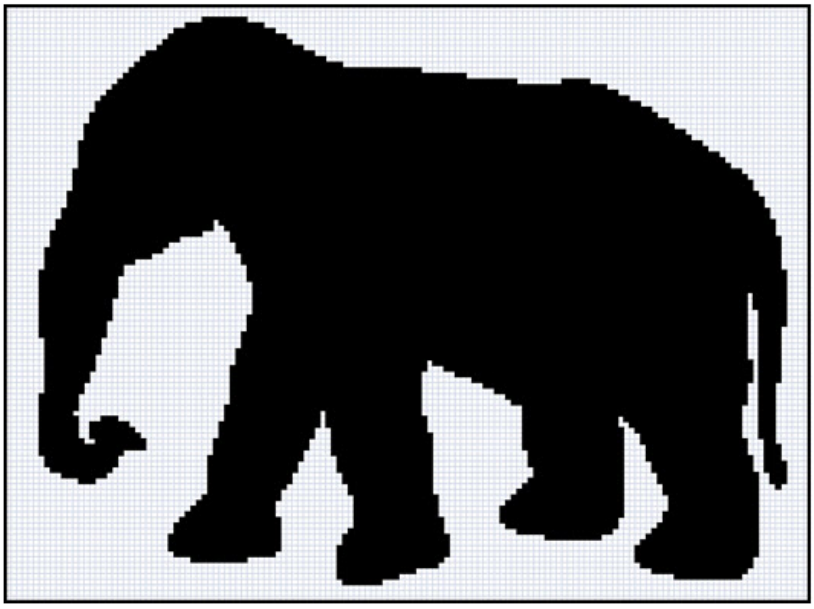
Als de afbeelding teveel uitgerekt is in de ene of de andere richting moet je de breedte van de kolommen en de hoogte van de rijen in het Excelbestand aanpassen. Een goed formaat voor de cellen is 6 pixels bij 6 pixels. Kleinere

B2 | =ALS(DEEL($A2;B$1;1)="1";0;1)

| | A | B | C | D | E | F | G | H |
|---|---|---|---|---|---|---|---|---|
| 1 | | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 2 | 11100000( | 0 | 0 | 0 | 1 | 1 | 1 | 1 |
| 3 | 111100000 | 0 | 0 | 0 | 0 | 1 | 1 | 1 |
| 4 | 111110001 | 0 | 0 | 0 | 0 | 0 | 1 | 1 |
| 5 | 000011111 | 1 | 1 | 1 | 1 | 0 | 0 | 0 |
| 6 | 001111111 | 1 | 1 | 0 | 0 | 0 | 0 | 0 |
| 7 | 001111111 | 1 | 1 | 0 | 0 | 0 | 0 | 0 |
| 8 | 001111001 | 1 | 1 | 0 | 0 | 0 | 0 | 1 |

Figuur 4: Binaire getallen uitsplitsen in cijfers

cellen geven een mooier beeld. Maar ze maken het nadien ook moeilijker om de twee transparanten correct over elkaar te schuiven.



Figuur 5: Een olifant in blokjes

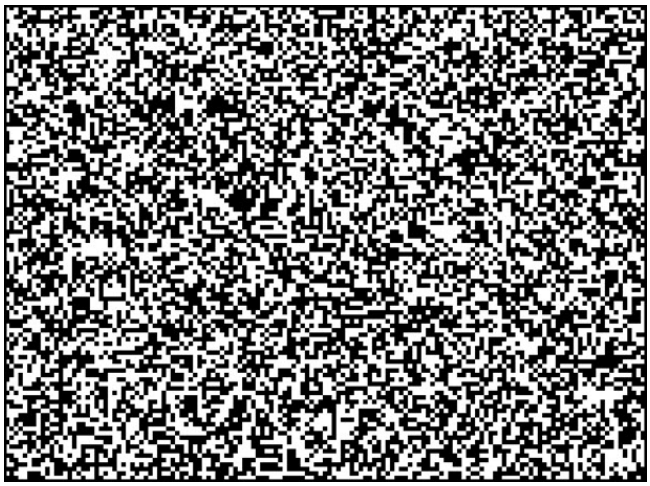
## 1.4 Een geheime sleutel maken

Om de blokjesfoto te coderen hebben we een geheime sleutel nodig. Met een sleutel bedoelen we een tabel die even groot is als de originele afbeelding en waarvan elke cel een toevallige keuze van nullen en enen bevat. De makkelijkste manier om op een toevallige wijze een 0 of 1 te genereren, is een randomgetal in het interval [0, 1] te nemen en dit getal naar boven of beneden af te ronden tot 0 of 1. In Excel kunnen we de instructie ASELECT() gebruiken om een willekeurig getal tussen 0 en 1 te kiezen. Met een ALS-commando ronden we het aselect gekozen getal af. De volledige Excel-formule voor de cellen van de

geheime sleutel is:

$$= \text{ALS}(\text{ASELECT}() < 0,5; 0; 1).$$

Deze formule moet ook weer doorgesleept worden door het hele getallenveld. Je kunt deze sleutel die zo ontstaat op dezelfde manier voorwaardelijk inkleuren als de originele afbeelding. Het resultaat kan er uitzien zoals figuur 6. Als alles goed gaat, zie je geen regelmaat in deze ruis aan zwarte hokjes.



Figuur 6: Een sleutel met blokjes

De originele boodschap (hier: de olifant) en de geheime sleutel plaats je netjes naast elkaar op je rekenblad. Dat kan je precies doen want beide getallenvelden zijn even groot. Vervolgens ontwerp je nog een derde getallenveld met dezelfde afmetingen. Dit getallenveld is de versleutelde boodschap van de originele afbeelding.

## 1.5 Een versleutelde boodschap maken

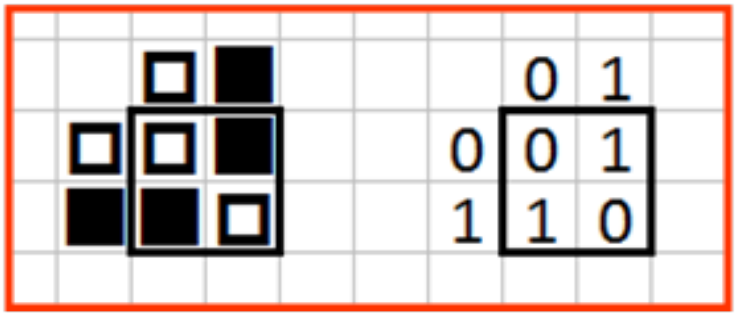
Met welke techniek kan je de originele boodschap (hier: een olifant) versleutelen? Wel, de regel is dat een cel van de gecodeerde boodschap enkel zwart gekleurd wordt als

- ofwel op de originele foto een zwart vakje staat maar niet op de sleutel
- ofwel op de sleutel een zwart vakje staat maar niet op de originele foto.

In de andere gevallen moet het vakje wit (of transparant) gekleurd worden. Op deze manier zal de originele boodschap terug te vinden zijn door de sleutel en de gecodeerde boodschap transparant over elkaar te leggen. Ga zelf na dat dit klopt.

We vertalen dit algoritme in een wiskundige formule. Stel dat $x$ een celwaarde is van de originele figuur en dat $y$ de overeenkomstige celwaarde is van de geheime sleutel. Dan gaan we op zoek naar een formule $f(x, y)$ voor de overeenkomstige celwaarde van de versleutelde boodschap. Deze functiewaarden

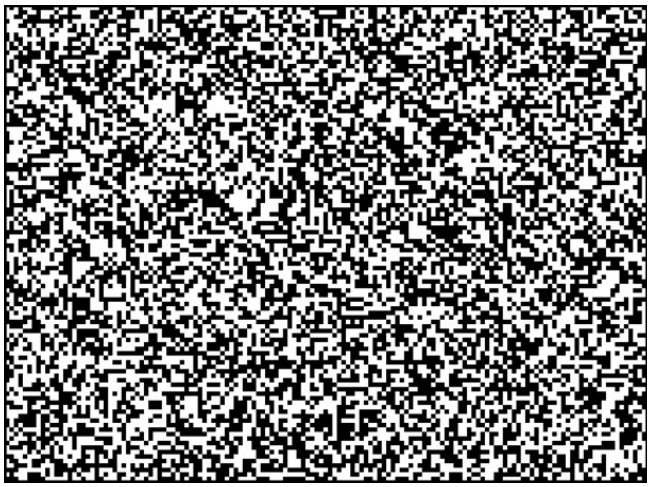
kunnen we aflezen uit de volgende functietabel (zie figuur 7). In de linkerrand lees je de waarde van $x$ af en in de bovenrand de waarde van $y$. In het hart van de tabel vind je $f(x, y)$.




Figuur 7: De functietabel voor de versleuteling

Met de formule $f(x, y) = \text{REST}(x + y, 2)$ lukt het om de bovenstaande bewerking in Excel te programmeren. De functie $\text{REST}(x+y, 2)$ staat hier voor de rest van de deling van $x + y$ door 2. Ga na dat $f(0, 0) = 1$, $f(0, 1) = 0$, $f(1, 0) = 0$ en $f(1, 1) = 1$.

Op deze manier is het mogelijk om in Excel een versleuteld bericht te maken vanuit een originele afbeelding en een sleutel. Ook in de ruis van dit versleutelde bericht lijkt er geen patroon te zitten. Mocht je toch een afbeelding menen te herkennen dan zal het vast geen olifant zijn. De enige regelmaat die we kunnen opmerken is de vaststelling dat ongeveer de helft van de blokjes zwart is ingekleurd (zie figuur 8).



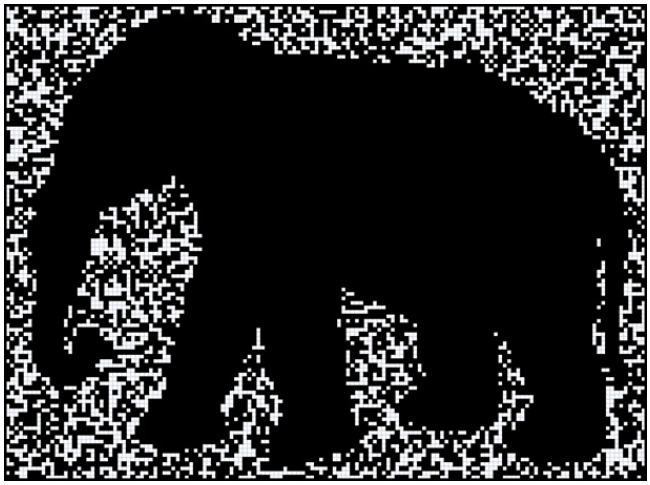
Figuur 8: Het gecodeerde bericht

## 1.6 De ontknoping

De tijd voor de ontknoping is aangebroken. Kopieer de afbeeldingen van figuur 6 en figuur 8 op een transparant, leg de transparanten precies over elkaar en

bekijk het gedecodeerde bericht (zie figuur 9).

We merken op dat de decodering met transparanten een zekere tol heeft geëist. In plaats van een zwarte olifant op een witte achtergrond zien we een zwarte olifant op een 50% grijsgestippelde achtergrond. Een decodering met een zwarte afbeelding op een sneeuwwitte achtergrond is enkel mogelijk door te programmeren in het rekenblad. We laten dit hier achterwege.



Figuur 9: De visuele decodering van het bericht

Bij de visuele decodering met transparanten kunnen verschillende problemen optreden. Eerst en vooral is het nodig dat de hokjes op beide transparanten precies even groot zijn. De screenshots neem je dus met een uiterste precisie. Geen enkele prent mag door een manuele uitrekking vergroot of verkleind worden.

Verder is het duidelijk dat het eindresultaat zich beter aftekent tegen de achtergrond wanneer de zwarte hokjes kleiner zijn. Als je de hokjes echter te klein neemt, zal het motorisch niet meer haalbaar zijn om de transparanten secuur op elkaar te leggen.

Indien je geen transparanten bij de hand hebt, kan je het gebruik van transparanten ook digitaal simuleren. Je importeert de versleutelde figuur en de sleutel dan in een fotoprogramma of in Word en je vervangt alle *witte* vierkantjes door *transparante* vierkantjes. Daarna leg je de twee bewerkte foto's in het gebruikte programma slordig over elkaar en verschuif je ze langzaam totdat ze precies boven elkaar liggen. Bij een precieze overdekking zie je onverwacht de geheime figuur op het computerscherm verschijnen.

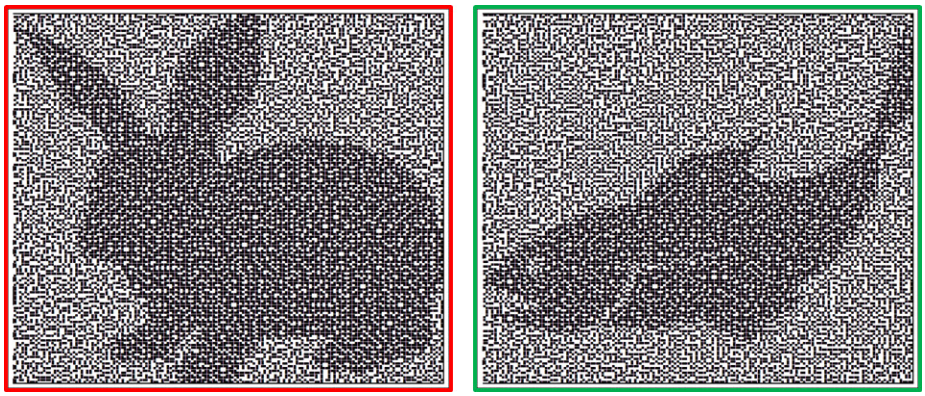
# 2 Tweede techniek: geheimschrift met twee afbeeldingen in grijswaarden

Volgens cryptografen bestaat er bij de visuele cryptografie een reëel gevaar dat de sleutel ontvreemd wordt, vooral wanneer hij meermaals hergebruikt wordt. Cryptografen raden aan om te werken met een verzameling van verschillende sleutels, die afwisselend gebruikt worden.

Sleutels voor visuele cryptografie hebben het nadeel herkenbaar te zijn. Een transparant met chaotische pixels in zwart en wit kan je immers niet voor veel andere doeleinden gebruiken dan voor cryptografische versleuteling. Daarom werd er een techniek ontwikkeld om de sleutels (en de versleutelde boodschap) te camoufleren met een afleidingsfiguur in grijstinten. Een voorbeeld maakt duidelijk hoe dit werkt.

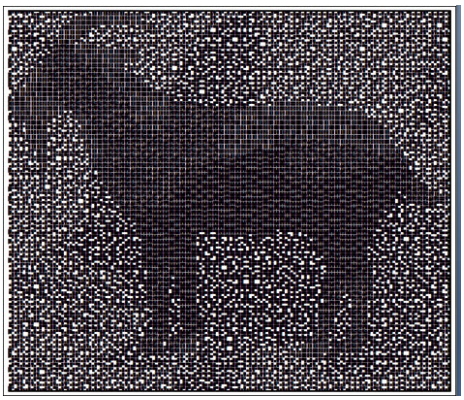
## 2.1 Voorbeeld

Als voorbeeld van deze camouflage laten we in figuur 10 een afbeelding zien van een sleutel (een konijn) en van een gecodeerd bericht (een vis). Beide dieren zijn afleiders. Ze hebben niets met de geheime boodschap te maken. Als je deze transparanten met precisie over elkaar legt, verschijnt de geheime boodschap (een bok), zie figuur 11.



Figuur 10: De sleutel en het gecodeerde bericht

Het gebruik van de afleidingsfiguren in grijstinten vraagt een bijkomende tol. De drie afbeeldingen zijn nu iets minder scherp afgelijnd, er is minder contrast van de figuur met de achtergrond. Bovendien is er een verschil tussen de afbeeldingen in figuur 10 en die in figuur 11. De eerste twee afbeeldingen zijn 75% grijs tegen een achtergrond die 50% grijs is. De laatste afbeelding is 100% grijs (zwart) tegen een achtergrond die 75% grijs is. Dit verschil is essentieel voor het ontwerpen van dit type van visuele cryptografie. We leggen verderop uit hoe het vermengen van verschillende grijswaarden kan benut worden in de visuele cryptografie.

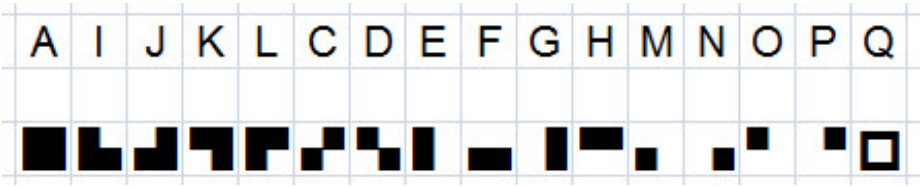


Figuur 11: Het gedecodeerde bericht

## 2.2 Een lettertype met 16 tekens

Als je in Excel pixel per pixel onderscheid wil maken tussen verschillende grijswaarden, heb je een zelfgemaakt lettertype nodig waarbij elke letter bestaat uit vier blokjes die wit of zwart kunnen zijn. In totaal heb je 16 verschillende letters in dit lettertype. Je ziet ze in figuur 12. Uiterst links staat de letter A die 100% zwart is. De letters I, J, K en L zijn 75%grijs. Dan volgen de letters C, D, E, F, G en H die 50% grijs zijn. De letters M, N, O en P staan voor letters die 25% grijs zijn. En uiterst rechts vind je een symbool voor het volledig transparante hokje. De laatste vijf symbolen zullen we niet nodig hebben bij de visuele cryptografie. Ze worden enkel voor de volledigheid vermeld.

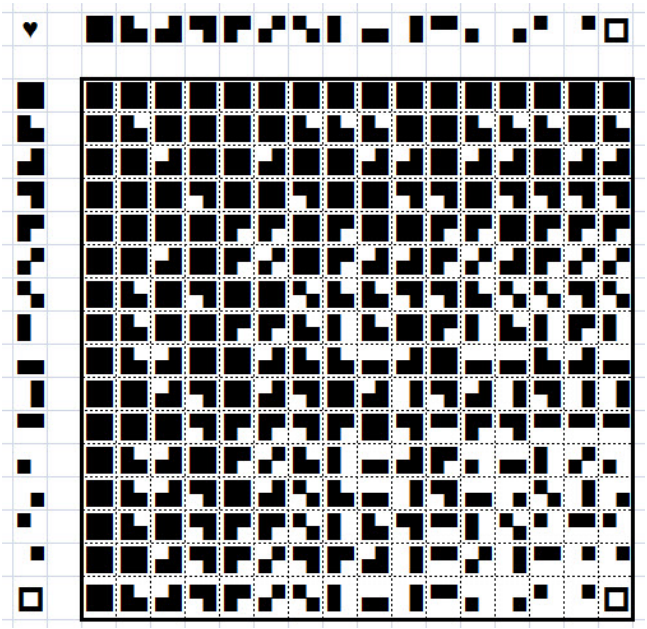
Als je een geschikte app zoekt dan kan je zelf een font ontwerpen voor dit geblokte lettertype. In bijlage vind je een *.ttf-bestand met de naam *kwadranten* dat je eventueel kan gebruiken voor deze techniek van visuele cryptografie. Bewaar het op je computer in de map waarin je alle fonts bewaart.




Figuur 12: Lettertype met 16 letters

Als je twee willekeurige 'lettertekens' transparant op elkaar legt, zie je een letterteken dat je als de som van de twee afzonderlijke lettertekens zou kunnen beschouwen. Deze som is een bewerking die we in het vervolg met een ♡ zullen aanduiden. De bewerking ♡ kan schematisch vastgelegd worden in de Cayley-tabel uit figuur 13.

De bewerking ♡ heeft enkele merkwaardige eigenschappen die je wellicht zelf kan ontdekken. Is er een neutraal element voor de bewerking ♡ in de verzameling van deze 16 letters? Hoe zie je dit aan de Cayley-tabel? Is de bewerking ♡ commutatief in deze letterverzameling? Hoe lees je dit af uit de Cayley-tabel? Maak een redenering om aan te tonen dat de bewerking ♡ associatief is in de

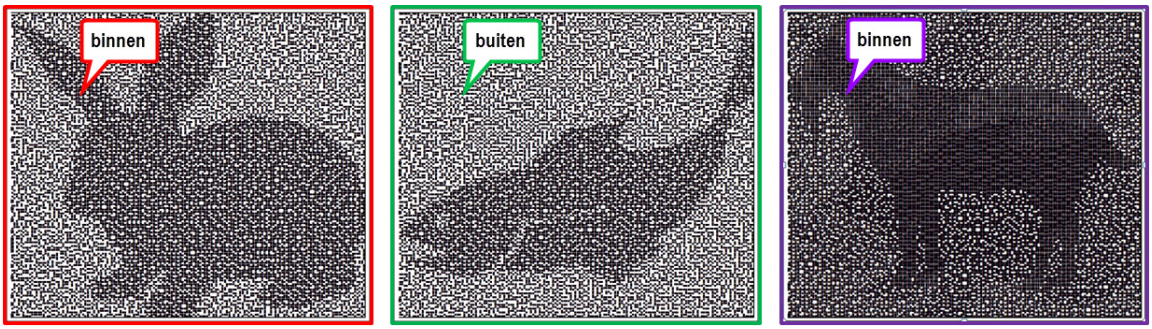


Figuur 13: Cayleytabel van de bewerking ♡

verzameling met de 16 letters. Is er voor elke letter een inverse letter voor de bewerking ♡? Toon dit aan. Is de verzameling van deze 16 lettertekens uitgerust met de bewerking ♡ een commutatieve groep?

## 2.3 Konijn + vis = bok

In een eerdere paragraaf zagen we dat het mogelijk is om een afbeelding van een konijn te vermengen met een afbeelding van een vis om een bokje te bekomen. Om het mechanisme hierachter te begrijpen, moeten we pixel per pixel bekijken wat er gebeurt.




Figuur 14: Overeenkomstige pixels in drie afbeeldingen

In figuur 14 zijn drie overeenkomstige pixels aangeduid in de twee bronafbeeldingen (konijn en vis) en in het gedecodeerde bericht (bok). Deze pixels kunnen binnen of buiten de figuur liggen en worden respectievelijk licht of don-

ker ingekleurd. In totaal heb je acht verschillende situaties. De situatie die hieronder aangeduid is vatten we samen als 'binnen + buiten = binnen' of als 'donker + licht = donker' (korter: dld).

Hoe kunnen we er met het zelfgemaakte lettertype voor zorgen dat donker (75%) plus licht (50%) gelijk is aan donker (100%)? Wel, dat kan op 12 manieren. Ze zijn samengevat in de tabel van figuur 15. Het zou ideaal zijn als er in de drie figuren voldoende kan afgewisseld worden tussen deze 12 mogelijkheden om donker en licht om te kunnen zetten in donker maar het is geen must.

Er zijn veel minder mogelijkheden om licht en licht om te zetten in donker (lld). Kan je ze opsommen? En er zijn nog minder mogelijkheden om donker en donker om te zetten in licht (ddl). Kan je hier een overzicht van geven?

Voor je verder gaat zou je voor jezelf een overzicht moeten maken van de acht mogelijkheden bij de pixelverwerking. Zoek dus minstens één oplossing voor het probleem van 'licht plus licht is licht' (lll), 'licht plus licht is donker' (lld), 'licht plus donker is licht'(ldl), 'licht plus donker is donker' (ldd), 'donker plus licht is licht' (dll), 'donker plus licht is donker' (dld), 'donker plus donker is licht' (ddl) en 'donker plus donker is donker' (ddd). Dit overzicht is nodig voor de verwerking in Excel.

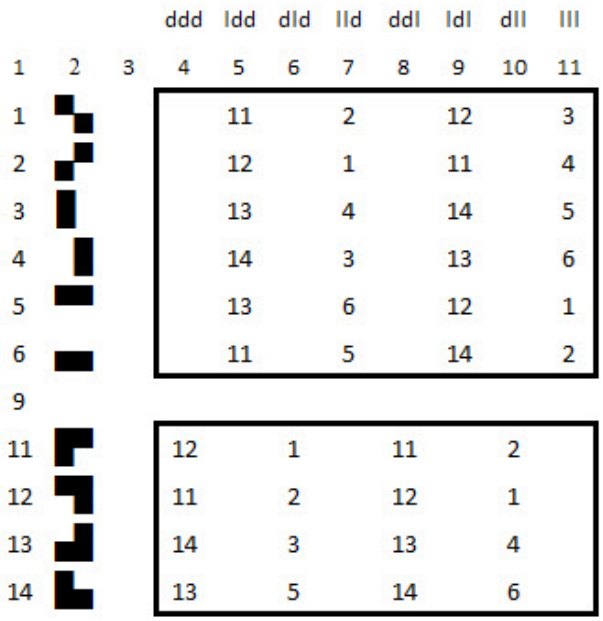
Figuur 15: Donker ♡ licht = donker

## 2.4 Overzicht van keuze van letters in Excel

Cruciaal in de verwerking met Excel is het gebruikte algoritme om de geschikte pixels te kiezen. Dit bestaat uit een overzicht van de acht gevallen, die je hierboven opsomde.

Begin bovenaan je Excelsheet met een overzicht waarbij voor elk van deze acht gevallen (ddd, ldd, dld, ...) een keuze wordt gemaakt tussen de pixels die boven elkaar kunnen gelegd worden. Dit overzicht kan er uit zien als in de figuur 16. We leggen uit hoe dit overzicht moet geïnterpreteerd worden.

In de linkse kolom staan cijfers die geassocieerd worden met de tien letters uit het lettertype *kwadranten*. De cijfers van 1 tot 6 komen overeen met de letters met een grijswaarde van 50%. De cijfers van 11 tot 14 komen overeen met letters met een grijswaarde van 75%.



| | | | ddd | ldd | dld | lld | ddl | ldl | dll | lll |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
| 1 | | | | 11 | | 2 | | 12 | | 3 |
| 2 | | | | 12 | | 1 | | 11 | | 4 |
| 3 | | | | 13 | | 4 | | 14 | | 5 |
| 4 | | | | 14 | | 3 | | 13 | | 6 |
| 5 | | | | 13 | | 6 | | 12 | | 1 |
| 6 | | | | 11 | | 5 | | 14 | | 2 |
| 9 | | | | | | | | | | |
| 11 | | | 12 | | 1 | | 11 | | 2 | |
| 12 | | | 11 | | 2 | | 12 | | 1 | |
| 13 | | | 14 | | 3 | | 13 | | 4 | |
| 14 | | | 13 | | 5 | | 14 | | 6 | |

Figuur 16: Schema voor de overlapping van pixels

In de kolom *ddd* staan de combinaties van de letters die je overeen kan leggen om twee donkere letters te combineren tot een donkere letter. Zo kan je letter 11 op letter 12 leggen. Of letter 12 op letter 11. Of 13 op 14. Of 14 op 13. In de zeven andere kolommen zijn gelijkaardige keuzes geïnventariseerd voor *ldd*, voor *dld* enz ...

## 2.5 Drie afbeeldingen digitaliseren met blokjespatronen

De volgend stap van dit project is het digitaliseren van drie silhouetfiguen. Dit gaat ongeveer zoals bij het *geheimschrift met blokjes*: maak de drie figuren even groot, zet ze om in een binary image, zet de drie figuren met nullen en enen naast elkaar je Excelsheet. Tot hier is het enkel een herhaling van wat je al eerder deed.

Vervolgens bewerk je de drie binaire tabellen in Excel. Je zorgt ervoor dat alle enen (die staan voor een lichte kleur) vervangen worden door een willekeurig geheel getal van 1 tot 6 en dat alle nullen (die staan voor een donkere kleur) vervangen worden door een willekeurig geheel getal van 11 tot 14. Een willekeurig getal kiezen van 1 tot 6 in Excel doe je met de instructie AFRONDEN.BOVEN(ASELECT()*6;1). Een willekeurig getal kiezen van 11 tot 14 doe je met de formule AFRONDEN.BOVEN(ASELECT()*4;1)+10. De formule (analoog aan formule (1)) om de woorden uit de binary image uit te splitsen in afzonderlijke symbolen wordt nu:

$$
\begin{aligned}
= \mathrm{ALS}(\mathrm{DEEL}(\$A2; B\$1; 1) = \text{"1"};& \\
\mathrm{AFRONDEN.BOVEN}(\mathrm{ASELECT}() * 4; 1) + 10;& \qquad (2)\\
\mathrm{AFRONDEN.BOVEN}(\mathrm{ASELECT}() * 6; 1))&
\end{aligned}
$$

Indien deze formule doorgesleept wordt, verschijnt er een getallenveld zoals op figuur 17. De getallen onder de 10 stellen de lichte vakjes voor en de getallen boven de 10 de donkere.

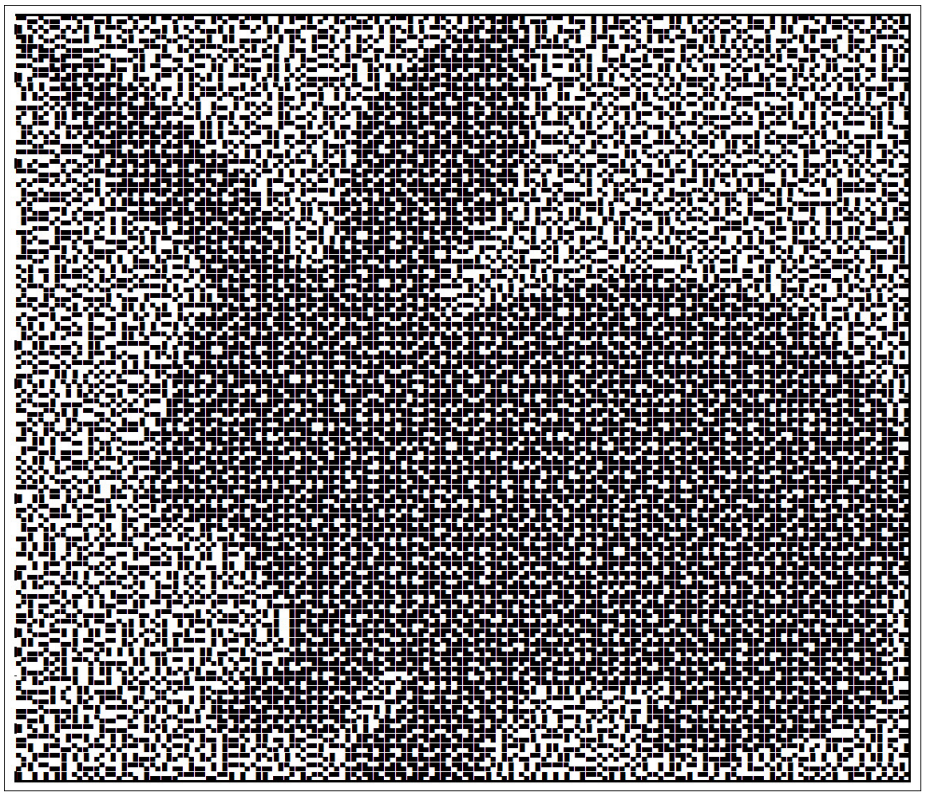
Figuur 17: Gedigitaliseerde afbeelding van een konijn met getallen

Als je wil controleren of de drie figuren correct zijn weergegeven dan maak je drie nieuwe afbeeldingen. Je vervangt de randomgetallen door de tekens uit de tweede kolom van het schema uit figuur 16. In Excel doe je dit met de instructie VERT.ZOEKEN. Als je bijvoorbeeld het equivalent wil zoeken van het getal in cel D9 in de tweede kolom van de tabel met linkerbovenhoek A4 en rechteronderhoek B14 dan gebruik je hiervoor de formule:

$$= \mathrm{VERT.ZOEKEN}(D9; \$A\$4 : \$B\$14; 2).$$

Na het doorslepen van deze formule vind je drie controlefiguren met blokjesletters uit het lettertype *kwadranten* zoals in figuur 18.

Als de drie figuren in blokjesmotief er goed uit zien, ben je klaar voor de volgende stap. De eerste figuur (hier: het konijn) mag afgeprint worden. Dit is de sleutel die je gebruikt voor de visuele cryptografie. De twee andere figuren



Figuur 18: Gedigitaliseerde afbeelding van een konijn met letters uit *kwadranten*

hoef je nog niet af te printen. Ze dienen enkel voor de crytografische versleuteling in de volgende stap.

## 2.6 Cryptografische versleuteling

Dit is de moeilijkste fase in het proces. De opdracht is een figuur te ontwerpen met het uitzicht heeft van figuur 2 (de vis) en die bovenop figuur 1 (het konijn) kan gelegd worden om bij de proef met de transparanten figuur 3 (de bok) te genereren. We leggen in deze paragraaf m.a.w. uit hoe je een nieuw blokjespatroon ontwerpt voor figuur 2 (de vis) zodanig dat de figuren 1 en 2 geschikt zijn voor een visuele cryptografie met figuur 3 als geheime boodschap.

Neem een welbepaalde pixel in gedachte, bijvoorbeeld de pixel linksboven in de drie afbeeldingen. Stel dat deze pixel achtereenvolgens in de cellen AA4 en FA4 en KA4 zit. Kijk na of deze pixel in elk van de drie afbeelding donker is (ddd). Dit kan je zien aan het randomgetal dat in deze cel staat: kleiner dan 10 betekent licht en groter dan 10 betekent donker. Je stelt in Excel dus de vraag:

$$\mathrm{EN}(\mathrm{AA4} > 10; \mathrm{FA4} > 10; \mathrm{KA4} > 10).$$

Indien het antwoord op deze vraag 'ja' is dan zoek je in de vierde kolom van de tabel 16 op welke keuze je moet maken voor de pixel linksboven in de cryptografische versleuteling van het symbool uit cel AA4. Je zoek het symbool uit AA4

dus op in de eerste kolom van de tabel (met bijvoorbeeld linkerbovenhoek A4 en rechteronderhoek K14) en je plukt het equivalent uit kolom 4. Deze instructie vertaal je als:

$$\begin{aligned}&\text{ALS}(\text{EN}(\text{AA4} > 10; \text{FA4} > 10; \text{K4} > 10);\\&\quad\text{VERT.ZOEKEN}(\text{AA4}; \$\text{A}\$4 : \$\text{K}\$14; 4);\\&\quad\ldots)\end{aligned}$$

Vervolgens stel je je de vraag of deze pixel in de drie afbeeldingen licht, donker en donker is (ldd). In dit geval kies je het equivalent van A44 uit de vijfde kolom van de tabel 16. De bovenstaande instructie kan op de stippeltjes aangevuld worden met een ALS-instructie die in de vorige ALS-instructie genesteld is:

$$\begin{aligned}&\text{ALS}(\text{EN}(\text{AA4} > 10; \text{FA4} > 10; \text{KA4} > 10);\\&\quad\text{VERT.ZOEKEN}(\text{AA4}; \$\text{A}\$4 : \$\text{K}\$14; 4);\\&\quad\text{ALS}(\text{EN}(\text{AA4} < 10; \text{FA4} > 10; \text{KA4} > 10);\\&\qquad\text{VERT.ZOEKEN}(\text{AA4}; \$\text{A}\$4 : \$\text{K}\$14; 5);\\&\qquad\ldots))\end{aligned}$$

In totaal moet je 8 ALS-instructies in elkaar stoppen. Het is een hele klus om deze programmaregel foutloos in te voeren. Achteraan beëindig je deze regel met 8 afsluithaakjes. Het staat vast dat het ontwerpen van de cryptografische versleuteling alleen weggelegd is voor onverschrokken programmeurs.

Helemaal tot slot sleep je de formule met de 8 ALS-instructies weer door tot je een nieuwe afbeelding krijgt (een nieuwe vis), die geschikt is voor de cryptografische versleuteling. Deze afbeelding druk je af voor de ultieme proef: je legt de cryptografische versleuteling (hier: de vis) op de sleutel (hier: het konijn) en je ziet de geheime boodschap (hier: de bok).

## 2.7 Een animatiefilmpje

Ben je niet zo handig in het zorgvuldig over elkaar schuiven van transparanten dan hoef je dit ook niet te doen. Je kan een filmpje maken van over elkaar schuivende transparanten.

Bewerk de sleutel (het konijn) en de cryptografische versleuteling (de vis) zo dat de witte hokjes transparant gemaakt worden. Dit kan met bijna om het even welk fotobewerkingsprogramma maar het kan ook in Word. Leg de twee digitale transparanten daarna naast elkaar op een leeg blad in een tekstverwerker. Met een muisgestuurd handje kan je de ene afbeelding dan over de andere slepen. Als je alles goed gedaan hebt, zie je de derde afbeelding (de bok) verschijnen en kan je een filmpje proberen te maken van je cryptografisch hoogstandje. Achtergrondmuziek en ingesproken commentaar kunnen een meerwaarde zijn.


Figuur 19: Animatiefilm: konijn + vis = bok

# Inhoudsopgave



# Referenties

[1] G. Hautekiet en M. Roelens. *Wiskunde achter beeldverwerking.* Uitwiskeling 22/4, 21-24. Acco, Leuven, ISSN 0774-6814, 2016.

[2] J. P. Delahaye. *Spelen met rekenkunde en geometrie: wiskundige uitvindingen*, 138-147. Veen Media, Amsterdam, ISBN 9789085715016, 2015.

[3] F. Kern, B. Burgereth en D. Eichhorn. *Algoritmen zur Bildbearbeitung.* Mathematik Lehren 188, Friedricht Verlach, Seelze, 2015.

[4] J. P. Delahaye. *La Cryptographie visuelle.* http://www.lifl.fr/ jdelahay/pls/223.pdf