Radboud Universiteit Nijmegen

Bachelorscriptie Wiskunde

Visuele Cryptografie

Auteur:
Lean Arts
Studentnummer:
0710350

Begeleider:
Wieb Bosma

10 juli 2012

Samenvatting

Bij visuele cryptografie worden geheime afbeeldingen met behulp van een sharematrix verdeeld over de shares van de deelnemers. De shares bestaan uit zwarte en witte vakjes, afgedrukt op een transparant. Door de juiste shares te overlappen wordt een geheime afbeelding zichtbaar. In een GEVCS worden de deelnemers en geheime afbeeldingen weergegeven in een graaf G en eisen we dat de shares een herkenbare afbeelding bevatten. Het is dan mogelijk een sharematrix te maken met $\chi(5d + 1)$ kolommen, absoluut contrast 2 voor de shares en absoluut contrast 4 voor de gereconstrueerde geheime afbeeldingen. Hierbij is χ het kleurgetal van G^3.

Inhoudsopgave

Hoofdstuk 1

Inleiding

Bij visuele cryptografie worden boodschappen verborgen in afbeeldingen. Deze afbeeldingen bestaan uit zwarte en witte pixels. De geheime afbeelding wordt verdeeld over zogenoemde shares, die geen informatie geven over het geheim. Deze shares zijn zelf ook afbeeldingen die zijn afgedrukt op een transparant. Wanneer de goede shares over elkaar gelegd worden wordt de, voor het menselijk oog herkenbare, geheime afbeelding zichtbaar.

Dit idee is in 1994 ontstaan bij Moni Naor en Adi Shamir. Zij verdeelden de geheime afbeelding over n shares, die er allemaal uitzagen als een afbeelding met willekeurige witte en zwarte pixels. Wanneer k van de n shares over elkaar werden gelegd werd de geheime afbeelding zichtbaar. Maar werden er minder dan k shares gebruikt, dan kon men niets te weten komen over de geheime afbeelding. Dit wordt een k-uit-n secret sharing schema genoemd.

Het uitgangspunt van deze scriptie is het artikel *Visual Cryptography on Graphs* [1]. Hierin wordt gekeken naar het delen van een geheime afbeelding waarbij de deelnemers worden weergegeven in een graaf G. Het belangrijkste resultaat in het artikel is als volgt:

Stelling 1.1. *Laat $G = (V, E)$ een graaf zijn met maximale graad d en laat χ het kleurgetal zijn van G^3. Dan bestaat er een GEVCS voor G met pixelexpansie hoogstens $m = \chi \cdot (5d + 1)$, absoluut contrast 2 voor iedere share en absoluut contrast 4 voor iedere gereconstrueerde geheime afbeelding.*

Er wordt een expliciete constructie gegeven voor een GEVCS met pixelexpansie hoogstens $m = (d^3 + 1)(5d + 1)$.

In het volgende hoofdstuk van deze scriptie wordt meer verteld over visuele cryptografie, waarna in hoofdstuk 3 een constructie wordt gegeven waarmee bovenstaand resultaat bereikt kan worden, gevolgd door een bewijs dat deze constructie voldoet aan de genoemde pixelexpansie en contrasten en dat de constructie veilig is.

Hoofdstuk 2

Visuele Cryptografie

We bekijken een groep van n deelnemers die een geheim met elkaar willen delen. Het geheim dat ze willen delen bestaat uit een geheime afbeelding die wordt weergegeven door witte en zwarte pixels met afmeting p bij q. Er is een autoriteit die het geheim kent en dit wil opsplitsen over de deelnemers. De verzameling van deelnemers noemen we P (Participants). De autoriteit bepaalt een collectie $\Gamma_{\text{Qual}} \subseteq 2^P$ van deelnemers die het geheim mogen reconstrueren.

De autoriteit maakt voor iedere deelnemer een *share* die een deel van het geheim bevat. We noemen de autoriteit ook wel de deler. De share is een afbeelding die wordt weergegeven door witte en zwarte pixels. De afbeelding is afgedrukt op een transparant, waarbij de witte pixels volledig doorzichtig zijn en de zwarte pixels volledig donker.

Wanneer een aantal deelnemers in Γ_{Qual} hun shares over elkaar legt wordt de geheime afbeelding zichtbaar.

2.1 Secret sharing

Het idee om geheime informatie te verdelen over meerdere mensen biedt een zekere veiligheid. Bekijk bijvoorbeeld de toegang tot een bankkluis. Stel dat er drie personen zijn die toegang hebben tot een bankkluis. Ze vertrouwen elkaar niet volledig, dus wordt besloten dat de kluis alleen open mag worden gemaakt wanneer ten minste twee van de drie personen aanwezig zijn.

De bankbediende geeft alle drie de personen een share met ogenschijnlijk willekeurige zwarte en witte pixels. Wanneer twee van de drie shares over elkaar worden gelegd wordt de geheime toegangscode tot de kluis zichtbaar en kan de kluis geopend worden. Dit biedt op verschillende vlakken veiligheid:

- Diefstal is lastig, omdat het stelen van één share geen informatie geeft
- Intern misbruik door de deelnemers wordt bemoeilijkt, omdat er minstens twee deelnemers moeten meewerken

- Deelnemers zijn in zekere zin beschermd tegen aanvallen op hun persoon, omdat het onder druk zetten van één persoon om zijn share af te geven niets oplevert.

Een groot voordeel van visuele cryptografie is dat de deelnemers die de shares ontvangen geen kennis van cryptografie nodig hebben om de geheime boodschap te vinden. Het over elkaar leggen van transparanten is enorm eenvoudig. Daar komt bij dat er geen computer nodig is om de geheime boodschap te kunnen zien.

2.2 De shares

De moeilijkste taak is weggelegd voor de deler die de shares moet maken.

Het idee is om de pixels te verdelen in een aantal subpixels. De subpixels van de shares moeten zo gekleurd worden dat bij het overlappen van de juiste shares de geheime afbeelding zichtbaar wordt. We spreken van een *Visual Cryptography Scheme* als we een methode hebben om de subpixels te kleuren.

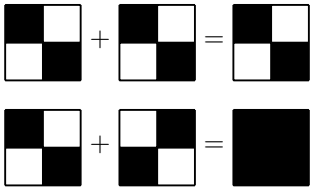
2.2.1 Voorbeeld

We bekijken een voorbeeld met twee deelnemers die samen een geheime afbeelding delen. Als we weten hoe we één geheime pixel kunnen verdelen over de twee shares dan kunnen we de hele afbeelding verdelen. We bekijken dus het verdelen van één geheime pixel. In dit voorbeeld gebruiken we 4 subpixels.

In de eerste share maken we op een willekeurige manier twee van de vier hokjes zwart. Van een afstandje zien de pixels er nu grijs uit.

Vervolgens leggen we een tweede share over de eerste share en kleuren de subpixels zo dat de kleur van de geheime pixel zichtbaar wordt. Als de geheime pixel zwart is kleuren we de twee subpixels van de tweede share zo dat de hele pixel zwart wordt. Dit is dus precies de tegenovergestelde kleuring van de eerste share. Is de geheime pixel wit dan kleuren we de tweede share zo dat de zwarte subpixels elkaar precies overlappen. Van een afstand ziet de pixel er nu grijs uit.

In de tweede share zijn ook twee van de vier subpixels zwart, dus alle pixels zien er van een afstandje grijs uit.



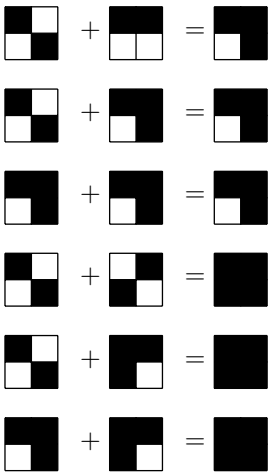
Figuur 2.1: Voorbeeld voor het kleuren van één pixel

Deze procedure herhalen we voor iedere pixel. De geheime afbeelding wordt nu zichtbaar als je de twee shares over elkaar legt. Het contrast is minder duidelijk dan in de oorspronkelijke geheime afbeelding, de afbeelding wordt immers weergegeven door grijze en zwarte pixels.

2.2.2 Uitbreiding van dit idee

De shares uit het bovenstaande schema zien er uit als willekeurige grijze pixels. Als extra eis kunnen we toevoegen dat iedere share een herkenbare afbeelding moet zijn.

Iedere deelnemer heeft dan een eigen bronafbeelding die bekend is bij de deler. De shares die de deler maakt moeten 'lijken' op de bronafbeelding van de deelnemer die die share krijgt. We noemen een schema dat hieraan voldoet een *Extended Visual Cryptography Scheme (EVCS)*. We zouden bijvoorbeeld kunnen eisen dat op iedere share een afbeelding staat van de eigenaar van die share. Dit biedt extra veiligheid, voor indringers is het lastiger om in het systeem in te breken.



Figuur 2.2: Voorbeeld voor het kleuren van één pixel in een EVCS

2.2.3 Verdere uitbreiding

Bij Multi-secret sharing zijn er meerdere geheimen. De deler verdeelt de shares zo dat verschillende deelverzamelingen verschillende geheimen kunnen reconstrueren. Dit biedt nieuwe mogelijkheden. Zo kan het systeem extra beveiligd worden door ook 'valse' geheimen toe te voegen. Wanneer deelnemers die geen enkel geheim mogen achterhalen hun shares overlappen zouden we dit zo kunnen organiseren dat ze een vals geheim te zien krijgen. Ze krijgen dan wel degelijk

een herkenbare afbeelding, maar deze geeft ze de verkeerde informatie.

Een *Graph-Based Extended Visual Cryptography Scheme* (GEVCS) is een schema waar de toegangsstructuur wordt weergeven in een graaf. De deelnemers worden weergegeven door punten en voor iedere zijde van de graaf hebben we een (unieke) geheime afbeelding die de aangrenzende deelnemers samen mogen reconstrueren.

Dit is een voorbeeld van Multi-secret sharing, met de beperking dat alle toegestane deelverzamelingen bestaat uit twee deelnemers.

2.3 Maken van een GEVCS

We bekijken een samenhangde graaf $G = (V, E)$ met n punten, de deelnemers. Voor iedere deelnemer $i \in V$ hebben we een bronafbeelding A_i. Voor iedere kant $(i, j) \in E$ hebben we een geheime afbeelding $B_{i,j}$. De volgorde van indices is hierbij niet van belang, dus $B_{i,j} = B_{j,i}$.

Het is voldoende om te weten hoe we één pixel kunnen delen, dus bekijken we de bronafbeeldingen en de geheime afbeeldingen per pixel. We noteren de kleur van een pixel van A_i met a_i, waarbij we 0 gebruiken voor wit en 1 voor zwart. Op dezelfde manier noteren we $b_{i,j}$ voor de kleur van de geheime pixel.

We verdelen de pixel in m subpixels, dit noemen we de *pixelexpansie*. In de praktijk zal m een kwadraat zijn, zodat de subpixels in een vierkant weergegeven kunnen worden.

Om de bronafbeeldingen zichtbaar te maken op de shares moeten we onderscheid kunnen maken tussen wit en zwart. Het *absolute contrast voor de shares* geeft aan hoe groot het verschil in het aantal zwarte subpixels moet zijn om onderscheid te kunnen maken tussen een witte en een zwarte pixel.

We zouden bijvoorbeeld kunnen afspreken dat we een pixel als zwart zien wanneer de helft of meer van de subpixels zwart zijn en dat we het anders als wit zien. In dit geval is het absolute contrast van de share 1.

Bij een groter contrast is het makkelijker om onderscheid te maken tussen wit en zwart, we zouden het absolute contrast dus zo groot mogelijk willen hebben. Merk op dat we bij een grote pixelexpansie graag een groter absoluut contrast zouden willen.

De geheime afbeelding moet ook goed zichtbaar zijn, dus willen we dat de geheime afbeelding die we reconstrueren door het overlappen van de juiste shares een zo groot mogelijk contrast heeft. We noemen dit het *absolute contrast van de gereconstrueerde geheime afbeelding.*

2.4 Noteren van een GEVCS

Om een GEVCS te maken is het noodzakelijk om voor iedere deelnemer te bepalen hoe de subpixels gekleurd moeten worden. We doen dit weer pixelsgewijs.

We gebruiken hiervoor de *sharematrix* S. Dit is een $n \times m$ matrix waarbij n het aantal deelnemers is en m de pixelexpansie. Een 0 op positie (i, j) betekent dat de j-de subpixel van de i-de deelnemer wit is en een 1 staat voor een zwarte subpixel. De i-de rij van de sharematrix is de share van deelnemer i, we noteren dit als S_i.

Voor een kant $e = (i, j)$ van de graaf moeten deelnemer i en j hun share over elkaar leggen om de geheime afbeelding $B_{i,j}$ te zien. Dit komt neer op het 'overlappen' van de i-de en j-de rij van de sharematrix. Alleen wanneer beide deelnemers een witte subpixel hebben zal de subpixel in de geheime pixel een wit resultaat gegeven. In alle andere gevallen is het resultaat zwart. Overlappen betekent dus plaatsgewijs het maximum nemen van S_i en S_j.

Het is niet van belang hoe de subpixels geplaatst worden in de pixel, mits dit in iedere share op dezelfde manier gebeurt. De deler mag de kolommen van S dus permuteren, dit is zeker aan te raden om de veiligheid te vergroten. De collectie $\mathcal{S}$ bevat alle permutaties van de kolommen van S.

De deler maakt nu de share van deelnemer i door rij i van een matrix uit $\mathcal{S}$ te nemen en deze 'in te vullen' op een transparant.

De deler herhaalt deze procedure voor iedere pixel en maakt zo de share voor de hele afbeelding.

Het algoritme van de deler om een bronafbeelding te coderen is *perfectly secret* als je, wanneer je een pixel van één van de twee benodigde shares te zien krijgt, je met kans 1/2 goed gokt wat de kleur van de pixel van de geheime afbeelding is.

Hoofdstuk 3

Constructie

In dit hoofdstuk wordt een constructie gegeven waar met de inputs a_i en $b_{i,j}$ shares worden gemaakt voor de n deelnemers. Het idee voor de constructie is om gebruik te maken van steroverdekkingen van de graaf G. Voor sterren is het eenvoudig een share te maken, met behulp van de kleuring van G^3 maken we een steroverdekking voor $G = (V, E)$ en vervolgens kunnen we de shares van ieder onderdeel van de overdekking samenvoegen tot we een GEVCS hebben voor de hele graaf.

3.1 GEVCS voor een ster, de constructie

Een *ster* is een samenhangende graaf waar hoogstens 1 punt, het *centrum*, graad groter dan 1 heeft.

Bekijk een ster G met $d+1$ punten. Het centrum van de ster is het punt 0, de andere punten zijn genummerd van 1 t/m d. We maken een sharematrix voor het verdelen van één pixel. Merk op dat de eerste rij van S de share van deelnemer 0 is en dat S_i op rij $i+1$ van S staat.

Om de sharematrix te krijgen maken we eerst de volgende matrices:

$$U = \begin{bmatrix} a_0 & 1 & 1 & \cdots & 1 \\ 1 & a_1 & 1 & \cdots & 1 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & 1 & \cdots & a_d \end{bmatrix}$$

$$T_0 = \begin{bmatrix} 0 & 0 & \cdots & 0 & 1 & 1 & \cdots & 1 \\ b_{0,1} & 0 & \cdots & 0 & 1-b_{0,1} & 0 & \cdots & 0 \\ 0 & b_{0,2} & \cdots & 0 & 0 & 1-b_{0,2} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & b_{0,d} & 0 & 0 & \cdots & 1-b_{0,d} \end{bmatrix}$$

Voor $i \neq 0$ maken we T_i als volgt:

$$T_i = \begin{bmatrix} b_{i,0} & 1 - b_{i,0} \\ 0 & 0 \\ \vdots & \vdots \\ 0 & 1 \\ \vdots & \vdots \\ 0 & 0 \end{bmatrix}$$

De sharematrix S krijgen we nu door de bovenstaande matrices achter elkaar te plakken: $S = U|T_0| \cdots |T_d$

3.2 Waarom de constructie werkt

Met bovenstaande constructie krijgen we een sharematrix, we willen nu laten zien dat dit een goede sharematrix is.

Stelling 3.1. *Voor een ster $G = (V, E)$ van graad d kunnen we een GEVCS maken met pixelexpansie $m = 5d + 1$, absoluut contrast 1 voor de shares en absoluut contrast 2 voor de gereconstrueerde geheime afbeeldingen. Deze GEVCS voldoet aan de gladheidseigenschap.*

Bewijs. We controleren de verschillende claims.

Claim 3.2. *De pixelexpansie is $m = 5d + 1$.*

Bewijs. De matrix U heeft in de constructie $d + 1$ kolommen, T_0 heeft $2d$ kolommen en de overige T_i hebben allen 2 kolommen. Het aantal kolommen van S is dus $(d + 1) + 2d + d \cdot 2 = 5d + 1$ en dit is de pixelexpansie. □

Claim 3.3. *Het absolute contrast van de bronafbeeldingen is 1.*

Bewijs. We bekijken S_i in de sharematrix. Het absolute contrast wordt bepaald door a_i, deze komt alleen voor in de matrix U. Als $a_i = 0$ dan hebben we 1 één minder in U dan wanneer $a_i = 1$. We zien dus dat het absolute contrast 1 is. □

Claim 3.4. *Het absolute contrast van de gereconstrueerde geheime afbeeldingen is 2.*

Bewijs. We zijn geïnteresseerd in het aantal enen dat het overlappen van twee rijen oplevert. We bekijken het overlappen van S_0 met S_i waar $i \neq 0$. Omdat $(0, i)$ een kant is van de ster hebben we een geheime pixel $b_{0,i}$. De a_0 en a_i zijn niet van belang, omdat in U alles buiten de diagonaal 1 is.

Stel $b_{0,i} = 0$.
Overlappen van twee rijen geeft in U altijd $d+1$ enen. In T_0 staan op de eerste rij eerst d nullen en vervolgens d enen. Omdat $b_{0,i} = 0$ staan er op de eerste d plekken van de $i+1$-de rij nullen, dus overlappen van de twee rijen geeft d enen.

Vervolgens bekijken we T_i. Op rij 1 staat eerst $b_{0,i} = 0$ en dan $1 - b_{0,i} = 1$. Op de $i+1$-de rij staat eerst 1 nul en dan 1 één, dus het overlappen van de twee rijen levert 1 één.

Als laatste bekijken we T_j waar $j \neq 0, i$. Op rij $i+1$ staan alleen nullen. Op de eerste rij staan $b_{j,0}$ en $1 - b_{j,0}$ dus overlappen geeft 1 één.

We tellen nu het totale aantal enen. We hebben er $d+1$ in U, dan d in T_0, vervolgens 1 in T_i en dan 1 in iedere andere T_j. In totaal zijn dat dus $(d+1) + d + 1 + (d-1) \cdot 1 = 3d + 1$.

Stel $b_{0,i} = 1$.
Overlappen van twee rijen geeft in U weer $d+1$ enen.

In T_0 staan op de eerste rij eerst d nullen en vervolgens d enen. Omdat $b_{0,i} = 1$ in de eerste helft van de $i+1$-de rij levert overlappen van de twee rijen $d+1$ enen.

Vervolgens bekijken we T_i. Op de eerste rij staat eerst $b_{0,i} = 1$ en dan $1 - b_{0,i} = 0$. In rij $i+1$ staat eerst 1 nul een dan 1 één, dus overlappen levert 2 enen.

Als laatste bekijken we T_j waar $j \neq 0, i$. Op rij $i+1$ staan alleen nullen en op de eerste rij staan $b_{j,0}$ en $1 - b_{j,0}$ dus overlappen geeft 1 één.

We tellen nu het totale aantal enen. We hebben er $d+1$ in U, dan $d+1$ in T_0, vervolgens 2 in T_i en dan 1 in iedere andere T_j. In totaal zijn dat dus $(d+1) + (d+1) + 2 + (d-1) = 3d + 3$.

Het absolute contrast is het verschil tussen een witte en een zwarte geheime pixel. We zien dus dat het absolute contrast van de gereconstrueerde geheime afbeeldingen 2 is. □

Claim 3.5. *Het GEVCS heeft de gladheidseigenschap. D.w.z. dat het overlappen van shares die geen geheim mogen delen altijd evenveel enen levert.*

Bewijs. We bekijken het overlappen van twee rijen S_i en S_j buiten het centrum van de ster. Dat betekent dat er geen kant is tussen i en j. (Een graaf met twee punten en één kant zien we als ster, waar één van de punten als centrum wordt gekozen.)

Overlappen van twee rijen geeft in U altijd $(d+1)$ enen. In T_0 komen $b_{0,i}$, $b_{0,j}$, $1 - b_{0,i}$ en $1 - b_{0,j}$ in verschillende kolommen voor en twee van deze leveren één, dus overlappen levert altijd twee enen. In T_i staat op rij $i+1$ eerst een 0 en dan een 1 en is rij $j+1$ nul, bij T_j is dat net andersom. Beide leveren dus 1 één. De T_k voor $k \neq 0, i, j$ hebben op rij $i+1$ en $j+1$ alleen nullen en leveren dus geen bijdrage. Het totale aantal enen van S_i overlapt met S_j is dus altijd $(d+1) + 2 + 1 + 1 = d + 5$ onafhankelijk van de kleuren van de bronpixels en de geheime pixels. □

We hebben nu alle uitspraken bewezen. □

3.3 GEVCS voor een willekeurige graaf

We beginnen met een aantal definities.

Definitie 3.6. *De omgeving $N(v)$ van v bestaat uit het punt v, alle buren van V en de kanten die het punt v met zijn buren verbindt. Merk op dat $N(v)$ een ster is, met v als centrum.*

Definitie 3.7. *Een sterrenbos is een graaf waar iedere samenhangscomponent een ster is.*

Definitie 3.8. *Gegeven een graaf $G = (V, E)$. Een collectie van deelgrafen $H_1, \ldots, H_k$ van G is een graafoverdekking van G als iedere kant in E bevat is in ten minste één H_i.*

Definitie 3.9. *Gegeven een graaf $G = (V, E)$. De derdemacht van G is een nieuwe graaf $G^3 = (V, E')$, waar $(v, w) \in E'$ als v en w zijn verbonden door een pad in G van lengte hoogstens 3. Merk op dat de puntverzameling van G^3 hetzelfde is als die van G, maar dat de kantenverzameling verschilt.*

Definitie 3.10. *Bij een kleuring van een graaf G krijgen alle punten van de graaf een kleur, waarbij er geen kant mag zijn tussen punten met dezelfde kleur. Het chromatisch getal χ is het minimale aantal kleuren dat nodig is om de graaf te kleuren.*

Om de sharematrix van een willekeurige graaf te maken gebruiken we een graafoverdekking. Omdat we voor sterren weten hoe we een GEVCS kunnen maken willen we een overdekking maken met sterren. We maken daarvoor gebruik van de kleuring van G^3.

3.3.1 Maken van de graafoverdekking

Stel we hebben een kleuring van G^3 met kleuren $1, \ldots, \ell$. We kunnen deze kleuring doorgeven aan G, omdat de puntverzamelingen van G^3 en G gelijk zijn. Vervolgens bekijken we punten v van G met kleur i, laat $K_i = \bigcup_{v \text{ met kleur } i} N(v)$.

Claim 3.11. *Iedere K_i is een sterrenbos.*

Bewijs. Iedere $N(v)$ is een ster en de centra van alle sterren hebben dezelfde kleur. Sterren kunnen niet aan elkaar zitten, want dan zou er een pad van lengte 2 zijn in G tussen twee punten met dezelfde kleur. □

Claim 3.12. *Er zijn geen kanten in G tussen twee punten van K_i die niet in dezelfde ster zitten.*

Bewijs. Bekijken twee sterren van K_i, dan hebben de centra van deze sterren dezelfde kleur. Stel dat er een kant zit tussen deze twee sterren, dan is er een pad van lengte 3 tussen de centra van beide sterren via deze kant. Maar dan hebben we een pad van lengte 3 in G tussen twee punten met dezelfde kleur en dat mag niet. □

Claim 3.13. *De collectie $K_1, \ldots, K_\ell$ vormt een graafoverdekking van G.*

Bewijs. We moeten laten zien dat iedere kant van G in ten minste één K_i zit. Een kant is aan twee uiteinden gekleurd, dus iedere kant zit in precies twee van de K_i. □

3.3.2 De constructie

De constructie gaat in twee stappen.

Stap 1: GEVCS voor K_i
Maak een sharematrix voor iedere ster $N(v)$ volgens de gegeven constructie. Laat m de maximale pixelexpansie zijn van alle sterren in K_i. Ieder punt van K_i zit in precies één ster, dus we kunnen een sharematrix voor K_i maken door voor ieder punt de bijhorende rij van de sharematrix van die unieke ster te nemen. Door de rijen eventueel aan te vullen met nullen krijgen alle rijen lengte m.

Stelling 3.14. *Voor K_i kunnen we een GEVCS maken met pixelexpansie $m = 5d + 1$ (waar d de maximale graad in G is), absoluut constrast 1 voor de shares en absoluut contrast 2 voor de gereconstrueerde geheime afbeeldingen.*

Bewijs.

- De pixelexpansie is duidelijk.
- Het absolute contrast blijft 1 omdat dat in de ster ook al zo is.
- We bekijken een geheime afbeelding in K_i, dus een kant in K_i. Dan zit deze kant in één van de sterren van K_i en voor sterren hebben we absoluut contrast 2.

□

Stap 2: GEVCS voor G
Laat $K_1, \ldots, K_\ell$ de hierboven gemaakte graafoverdekking van G zijn. Maak een GEVCS voor iedere K_i met behulp van Stap 1. Voor iedere K_i vullen we de sharematrix aan door de rijen $i \in V \setminus V_i$ te vullen met enen. Zo krijgt iedere sharematrix n rijen. Vervolgens plakken we de sharematrices van alle K_i achter elkaar om de sharematrix voor G te krijgen.

Stelling 3.15. *Voor G kunnen we een GEVCS maken met:*

- *Pixelexpansie hoogstens $\ell \cdot (5d + 1)$*
- *Absoluut contrast voor de shares gelijk aan $d_i + 1$ waar d_i de graad van punt i is. Dit is minimaal 2.*
- *Absoluut contrast voor de gereconstrueerde geheime afbeeldingen gelijk aan 4.*

Bewijs. We bewijzen de verschillende onderdelen:

- Als d de maximale graad in G is dan heeft iedere K_i hoogstens pixelexpansie $5d + 1$. Omdat we ℓ kleuren gebruiken plakken we ℓ keer de matrices van iedere K_i achter elkaar dus is de som maximaal $\ell \cdot (5d + 1)$.
- Het punt i komt voor in K_i en in de K_j's waar j buren van i zijn. Omdat we geen geisoleerde punten hebben is d_i ten minste 1, dus voor G hebben we minimaal contrast 2.
- Iedere kant is aan twee uiteinden gekleurd en komt dus voor in twee van de K_i. Voor iedere K_i hebben we absoluut contrast 2 vanwege de vorige claim dus krijgen we contrast 4.

□

Wanneer we nemen $\ell = \chi$ dan krijgen we precies het gewenste resultaat uit het artikel terug.

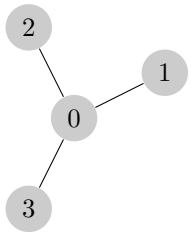
Claim 3.16. *De sharematrix die we met bovenstaande constructie krijgen is veilig.*

Bewijs. Vanwege de gladheidseigenschap hebben we veiligheid voor de constructie voor een ster. Vervolgens bekijken we de veiligheid na Stap 1. Voor deelnemers binnnen één ster hebben we al veiligheid, dus bekijk twee deelnemers uit verschillende sterren van K_i. Vanwege Claim 3.12 bestaat er geen geheim tussen deze deelnemers, dus maakt het niet uit wat het overlappen van hun shares oplevert. De veiligheid van een geheim tussen een deelnemer in K_i en een deelnemer buiten K_i wordt gegeven doordat we de rijen buiten K_i vullen met enen. Overlappen levert dan altijd enen waardoor geen informatie wordt vrijgegeven. Nu volgt direct veiligheid van Stap 2, want het achter elkaar plakken van veilige sharematrices behoudt veiligheid. □

Hoofdstuk 4

Voorbeeld: Share van een ster

We willen een share maken bij de volgende ster:



De pixels van de vier bronafbeeldingen hebben de volgende kleuren:
$a_0 = 0, a_1 = 1, a_2 = 0, a_3 = 1$

De pixels van de drie geheime afbeeldingen hebben de volgende kleuren:
$b_{0,1} = 0, b_{0,2} = 1, b_{0,3} = 1$

We maken de matrices bij deze graaf:

$$U = \begin{bmatrix} a_0 & 1 & 1 & 1 \\ 1 & a_1 & 1 & 1 \\ 1 & 1 & a_2 & 1 \\ 1 & 1 & 1 & a_3 \end{bmatrix}$$

$$T_0 = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 \\ b_{0,1} & 0 & 0 & 1 - b_{0,1} & 0 & 0 \\ 0 & b_{0,2} & 0 & 0 & 1 - b_{0,2} & 0 \\ 0 & 0 & b_{0,3} & 0 & 0 & 1 - b_{0,3} \end{bmatrix}$$

$$T_1 = \begin{bmatrix} b_{1,0} & 1 - b_{1,0} \\ 0 & 1 \\ 0 & 0 \\ 0 & 0 \end{bmatrix}$$

$$T_2 = \begin{bmatrix} b_{2,0} & 1 - b_{2,0} \\ 0 & 0 \\ 0 & 1 \\ 0 & 0 \end{bmatrix}$$

$$T_3 = \begin{bmatrix} b_{3,0} & 1 - b_{3,0} \\ 0 & 0 \\ 0 & 0 \\ 0 & 1 \end{bmatrix}$$

We krijgen de graaf G door de waarden a_i en $b_{i,j}$ in te vullen en de matrices achter elkaar te plakken. $S = U|T_0|T_1|T_2|T_3$ De sharematrix van de graaf G ziet er dus zo uit:

$$S = \left[\begin{array}{cccc|ccccccc|cc|cc|cc} 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{array}\right]$$

Hoofdstuk 5

Afsluiting

De constructie in het voorgaande hoofdstuk maakt gebruik van het kleurgetal van G^3 terwijl het vinden van dit kleurgetal een NP-volledig probleem is. We kunnen het kleurgetal afschatten met behulp van de maximale graad van de graaf. In het slechtste geval is G^3 een graaf met maximale graad d^3 en kunnen we slechts zeggen dat $\chi \leq d^3 + 1$. Daarmee kan de pixelexpansie enorm groeien terwijl de contrasten slechts 2 en 4 blijven. Dit zal er dus voor zorgen dat de afbeeldingen slecht zichtbaar worden.

Een ander probleem bij het gebruik van χ is dat het maken van de steroverdekking op deze manier 'duur' is. Stel dat de graaf G een ster is, maar je dat niet hebt opgemerkt. Als je de steroverdekking maakt volgens de gegeven constructie krijg je, naast de oorspronkelijke ster, ook sterren van graad 1 voor alle omliggende punten. Voor al deze sterren wordt een sharematrix gemaakt en met het achter elkaar plakken van deze sterren groeit de pixelexpansie weer enorm.

Het is een interessante vraag of er een meer efficiente methode is om een graaf met sterren te overdekken. Een andere vraag is of er een betere afschatting is voor de term $(5d + 1)$ in de pixelexpansie. Bij de gegeven constructie wordt de pixelexpansie voor iedere K_i afgeschat met de maximale graad van G, terwijl het voldoende zou zijn om te kijken naar de maximale graad van iedere K_i.

Bibliografie

[1] Steve Lu, Daniel Manchala & Rafail Ostrovsky, *Visual Cryptography on Graphs*. In: COCOON 2008, 225–234, 2008

[2] Giuseppe Ateniese, Carlo Blundo, Alfredo De Santis & Douglas R. Stinson, *Constructions and Bounds for Visual Cryptography*. In:Lecture Notes in Computer Science **1099**, 416–428, 1996

[3] Moni Naor & Adi Shamir, *Visual Cryptography*. In: Advances in Cryptology - EUROCRYPT'94, 1–12, 1994

[4] Stelvio Cimato, *Visual Cryptography and Secret Image Sharing*. CRC Press, 2011