Univerza v Ljubljani

Fakulteta za Matematiko in Fiziko
Fakulteta za Računalništvo in Informatiko

Vizualna Kriptografija

Seminarska naloga pri predmetu Kriptografija in Teorija Kodiranja II

Avtor: Lovro Šubelj

Mentor: Aleksandar Jurišič

Ljubljana, 27. avgust 2008

Povzetek

Naloga podaja splošno predstavitev vizualne kriptografije, hkrati pa se posveti predvsem vizualnim shemam, ki jih je moč konstruirati iz Hadamardovih matrik prek bločnih designov. V tem pogledu predstavlja naloga nekakšen priročnik za konstrukcijo takih shem, v dodatku pa je predstavljenih tudi nekaj konstrukcij Hadamardovih matrik. V nadaljevanju naloge vizualne sheme nadgradimo z dodatnimi lastnostmi, predstavimo možne prevare ter podamo kratko kritično oceno. Na koncu sledi še pregled nekaterih drugih shem, ki se pojavljajo v literaturi, a niso predstavljene v tej nalogi.

Kazalo

1 Uvod

V realnem življenju nemalokrat naletimo na problem, da želimo neko skrivnost oziroma informacijo "deliti" med več oseb. Pri tem želimo, da skrivnost lahko razkrije le neko vnaprej določeno število oseb, ali vnaprej določena skupina oseb, dočim pa vsak posameznik zase ne pozna prav nobene informacije o skrivnosti. Tak način skrivanja informacije v kriptografiji imenujemo shema za deljenje skrivnosti, katere sta neodvisno vpeljala Blakley in Shamir (1979).

V nalogi se posvetimo posebni vrsti shem za deljenje skrivnosti, imenovanih vizualne sheme (Naor in Shamir, 1994). Pri teh skrivno informacijo predstavlja poljubna slika, vsi potrebni kriptografski postopki pa temeljijo zgolj na uporabi človeškega vida. Omenjene sheme so tako uporabne predvsem v primerih, ko ni na voljo nobenega kriptografskega stroja (npr. računalnika) oziroma "uporabniki" niso kriptografsko vešči.

V nadaljevanju najprej v razdelku 2 predstavimo nekatere znane kombinatorične objekte potrebne pri konstrukciji vizualnih shem, samim shemam se posvetimo v razdelku 3 ter jih v razdelku 4 razširimo z dodatnimi lastnostmi. Sledi pregled varnosti ter možnih prevar (razdelek 5) in pa nekaj besed o praktičnosti in uporabi samih shem v razdelku 6.

2 Hadamardove matrike in designi

Vizualne sheme je moč skonstruirati s pomočjo Hadamardovih matrik oziroma prek njihovih bločnih designov[1]. Konstrukcija samih shem je opisana v 3, sledi pa predstavitev omenjenih kombinatoričnih objektov ter njihovih konstrukcij.

2.1 Hadamardova matrična domneva

Hadamardova matrika reda n (Sylvester, 1867) je $n \times n$-dimenzionalna matrika H_n, $(H_n)_{ij} \in \{-1, 1\}$, za katero velja

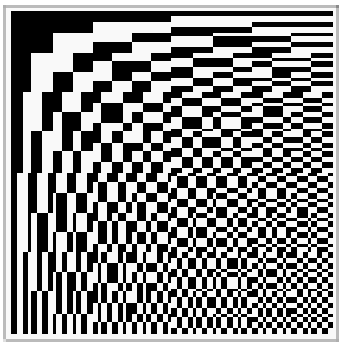
$$H_n H_n^T = nI_n.$$

Opazimo, da so vrstice matrike H_n med sabo pravokotne ter vse dolge natanko $\sqrt{n}$ (enako seveda velja za stolpce). Tako sledi, da je H_n rešitev Hadamardovega problema največje determinante oziroma natančneje, matrika H_n ima največjo determinanto med vsemi kompleksnimi $n \times n$-dimenzionalnimi matrikami A za katere velja $|(A)_{i,j}| \leq 1$ (Hadamard, 1893).

$$|\det(H_n)| = n^{n/2}$$

Praktično iz definicije H_n sledi, da matrika ostane Hadamardova v kolikor permutiramo njene vrstice oziroma stolpce, ali pa če neko vrstico oziroma stolpec pomnožimo z -1. Vse te matrike smatramo za ekvivalentne, zatorej definiramo normalizirano obliko Hadamardove matrike kot matriko H_n, kjer sta prva vrstica in prvi stolpec sestavljena iz samih enic (tako matriko je z omenjenimi operacijami vedno moč dobiti iz ustrezne ekvivalentne matrike). Bralec naj predpostavi, da so vse Hadamardove matrike v nadaljevanju normalizirane.

[1] Pravilen slovenski izraz za angleški *block design* je sicer bločni načrt, vendar pa zaradi uveljavljenosti pojma design v nadaljevanju uporabljamo kar tega.



Slika 1: Hadamardova matrika v normalizirani obliki (črni kvadratki predstavljajo 1, ter beli -1).

Lema: Naj bo H_n Hadamardova matrika reda n. Tedaj velja $n \in \{1, 2\} \cup \{4s | s \in \mathbb{N}\}$.

Dokaz: V kolikor velja $n \in \{1, 2\}$ je Hadamardova matrika enaka

$$H_1 = [1], H_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}.$$

Sicer velja $n \geq 3$ in naj bo H_n^3 $3 \times n$-dimenzionalna matrika sestavljena iz prvih treh vrstic matrike H_n. Zaradi normalizirane oblike H_n z ustrezno permutacijo stolpcev matrike H_n^3 dobimo

$$\begin{bmatrix} \overbrace{11\ldots11}^{a} & \overbrace{11\ldots11}^{b} & \overbrace{11\ldots11}^{c} & \overbrace{11\ldots11}^{d} \\ 11\ldots11 & 11\ldots11 & -1\ldots-1 & -1\ldots-1 \\ 11\ldots11 & -1\ldots-1 & 11\ldots11 & -1\ldots-1 \end{bmatrix}.$$

Očitno je, da velja $a+b+c+d = n$, iz zahteve po ortogonalnosti vrstic pa dobimo še naslednje tri enačbe.

$$a + b - c - d = 0$$

$$a - b + c - d = 0$$

$$a - b - c + d = 0$$

Rešitev dobljenega sistema je enaka $a = b = c = d = n/4$ in očitno celoštevilska, zatorej obstaja tak $s \in \mathbb{N}$, da je $n = 4s$.

□

Iz leme sledi naslednja znana domneva.

Hadamardova matrična domneva (1893): Naj bo $s \in \mathbb{N}$. Tedaj obstaja Hadamardova matrika reda $n = 4s$.

Domneva ni bila nikoli dokazana, kljub temu pa poznamo kar nekaj konstrukcij Hadamardovih matrik s pomočjo katerih dobimo vse matrike za $n < 668$ (ter pa seveda tudi nekatere večje). Hadamardova matrika reda 668 tako trenutno velja za najmanjšo matriko, katere še ne znamo konstruirati. Opisov samih konstrukcij na tem mestu ne podajamo, le te je moč najti v dodatku A.

2.2 *BIBD*

Uravnotežen nepopoln bločni design oziroma *BIBD* (*Balanced Incomplete Block Design*) je kombinatoričen objekt sestavljen iz b blokov ter v točk z naslednjima dvema lastnostma:

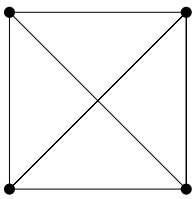
1. vsak blok vsebuje natanko k točk, $k < v$
2. vsaki dve različni točki nastopata v natanko λ blokih

Izkaže se, da vsaka točka takega designa leži v natanko r blokih, v kolikor pa velja še $v = b$ (oziroma $k = r$), tedaj pravimo, da je design simetričen. Omenjene designe tako označimo z (v, b, r, k, λ)-*BIBD* oziroma še krajše z (v, k, λ)-*BIBD*, saj z nekaj štetja hitro ugotovimo, da velja

$$bk = rv,$$

$$r(k-1) = \lambda(v-1). \tag{1}$$

Prvo enakost dobimo tako, da na dva načina preštejemo vse točke designa, pri drugi pa štejemo vse pare točk, ki vsebujejo neko določeno točko.



Slika 2: $(4, 2, 1)$-*BIBD* - bloke designa predstavljajo premice oziroma krivulje.

Eden temeljnih dosežkov v teoriji designov je prav gotovo izrek Brock-Ryser-Chowla (Bruck in Ryser, 1949, Ryser in Chowla, 1950), ki sledi v nadaljevanju. Izrek podaja potrebne pogoje parametrov za eksistenco simetričnega bločnega designa, zato je mogoče z njegovo uporabo dokazati neobstoj marsikaterega designa. Dolgo se je tudi verjelo, da so pogoji v izreku zadostni za obstoj določenega designa, vendar pa je bilo le to ovrženo - z obsežnim računalniškim iskanjem je bil dokazan neobstoj simetričnega $(111, 11, 1)$-*BIBD* oziroma projektivne ravnine reda 10 (Lam, Thiel in Swiercz, 1989). Tega pa sam izrek ne predvidi (v izreku nastavimo $x = 1, y = 1$ in $z = 3$).

Izrek (Bruck, Ryser, Chowla, 1950): Naj obstaja simetričen (v, k, λ)-*BIBD* ter naj bo $q = n - \lambda$. Tedaj velja:

v je liho: q je popoln kvadrat

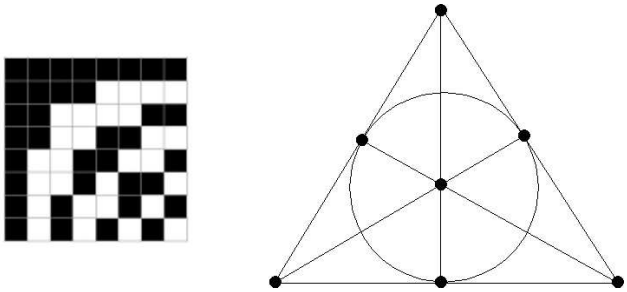
v je sodo: naslednja diofantska enačba $z^2 = qx^2 + (-1)^{\frac{1}{2}(v-1)}\lambda y^2$ ima netrivialno rešitev za x, y, z

Dokaz: Dokaz izreka najdemo v dodatku B.

Naslednji izrek pa predstavlja jedro tega razdelka, saj, v kolikor predpostavimo resničnost Hadamardove matrične domneve, podaja možno konstrukcijo neskončne družine designov. Le te v nadaljevanju uporabimo za konstrukcijo vizualnih shem.

Izrek: Hadamardova matrika reda $n = 4s$ je ekvivalentna simetričnemu $(4s-1, 2s-1, s-1)$-*BIBD* (Hadamardov design).

Dokaz izreka izpustimo, vseeno pa povejmo, da v dokazu zgolj proglasimo vrstice Hadamardove matrike za točke designa, ter stolpce za njegove bloke. Lastnosti designa tedaj sledijo iz lastnosti Hadamardovih matrik, in obratno.



Slika 3: Hadamardova matrika reda 8 ter ekvivalenten $(7, 3, 1)$-*BIBD* (Fanova ravnina).

3 Vizualne sheme

3.1 Sheme za deljenje skrivnosti

Vizualne sheme spadajo v skupino splošnejših kriptografskih objektov imenovanih sheme za deljenje skrivnosti (Blakley in Shamir, 1979). Kot je bilo že omenjeno s slednjimi rešujemo problem "deljenja" skrivnosti med več oseb, pri čimer pa želimo, da skrivnost lahko razkrije zgolj neko v naprej določeno število oseb oziroma skupina oseb. Zaradi splošnosti pojma "deljenje skrivnosti" so omenjene sheme uporabne na številnih področjih in zatorej pomemben del kriptografije.

Formalno sedaj definirajmo (k, n) stopenjsko shemo za deljenje skrivnosti (v nadaljevanju (k, n) shema). Naj bo S skrivnost katero želimo deliti med n oseb. Tedaj i-ta oseba dobi "delež" skrivnosti S_i, tako da velja:

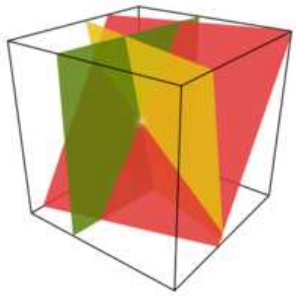
1. poljubnih k oseb lahko izračuna skrivnost S
2. poljubnih $t < k$ oseb ne more razkriti prav nobene informacije o S

Pri točki 2. navadno zahtevamo popolno (brezpogojno) varnost - shema je varna ne glede na kriptografsko znanje in pa računsko moč napadalca. Ker pa slednje zahteva, da je velikost deleža vsake osebe večja ali enaka velikosti skrivnosti, včasih ne zahtevamo popolne varnosti v zameno za manjše deleže.

Na tem mestu omenimo, da lahko sheme za deljenje skrivnosti definiramo tudi za splošno strukturo dovoljenj (Ito, Saito in Nishizeki, 1987). S tem mislimo, da lahko skrivnost razkrijejo le neke v naprej določene skupine oseb, pri čimer pa ni nobenih omejitev glede teh skupin. Splošna struktura dovoljenj je tako poljubna podmnožica potenčne množice vseh oseb. Opazimo, da so omenjene sheme splošnejše od stopenjskih shem za deljenje skrivnosti.

Za lažjo predstavo povedanega podajmo dve (k, n) shemi, kot sta jih sprva predlagala Blakley in Shamir.

Blakleyjeva (k, n) shema: Blakleyeva shema temelji na dejstvu, da se k paroma nevzporednih hiperravnin v k-dimenzionalnem prostoru seka v natanko eni točki, pri čimer pa slednje ni moč doseči z manj kot k hiperravninami. (k, n) shemo dobimo tedaj tako, da vsaki izmed n oseb dodelimo naključno hiperravnino v k-dimenzionalnem prostoru tako, da se vseh n hiperravnin seka v natanko eni točki P. Točka 1. iz definicije (k, n) sheme je tako zadoščena, treba pa je biti pazljiv pri zadostitvi točke 2. Skrivnost S zato definiramo kot poljubno koordinato točke P, saj bi v primeru $S = P$ vsaka oseba poznala določeno informacijo o sami skrivnosti - skrivnost, oziroma točka P, leži na vsaki izmed hiperravnin S_i. Primer Blakleyjeve sheme je viden na sliki 4.

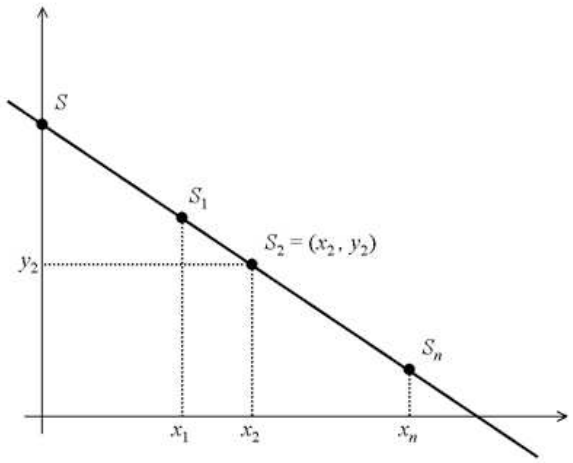


Slika 4: Trije deleži Blakleyjeve $(3, n)$ sheme - poljubna koordinata njihovega presečišča predstavlja skrivnost.

Shamirjeva (k, n) shema: Podobno kot Blakley, tudi Shamir predlaga zelo elegantno rešitev za (k, n) shemo. Naj bo $p(x)$ polinom stopnje k nad nekim končnim obsegom. Tedaj vsaki izmed n oseb priredimo naključno točko na tem polinomu (brez izgube za varnost lahko osebi i priredimo kar $(i, p(i))$), skrivnost pa predstavlja odsek polinoma na ordinatni osi $S = p(0)$ (glej sliko 5). Poljubnih k oseb lahko tedaj izračuna skrivnost z uporabo Lagrangeove iterpolacijske formule

$$S = \sum_{i=1}^{k} p(i) \prod_{j=1, j\neq i}^{k} \frac{j}{j-i}.$$

Izrek o enoličnosti polinomov nam zagotavlja oba pogoja iz definicije (k, n) sheme. Ponovno pa je potrebno biti pazljiv pri uporabi. V kolikor $p(x)$ ni polinom nad nekim končnim obsegom, ampak zgolj nad celimi števili, lahko na primer dve osebi v $(3, n)$ shemi izračunata določeno informacijo o skrivnosti (Shmitz, 2007). Shema tako v tem primeru nebi zadoščala točki 2. iz definicije.



Slika 5: Shamirjeva $(2, n)$ shema.

3.2 Vizualne sheme za deljenje skrivnosti

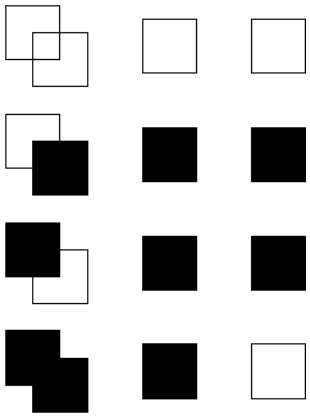
Splošne sheme za deljenje skrivnosti navadno zahtevajo uporabo določenih računskih postopkov (npr. računanje v končnih obsegih). Le te je v večini primerov nemogoče, ali pa vsaj zelo težko, opraviti brez nekega kriptografskega stroja ter pa ustreznega znanja. Slednje pa ne velja za vizualne sheme, katerih glavna prednost napram ostalim shemam je prav to, da je moč vse potrebne kriptografske postopke opraviti zgolj z uporabo človeškega vida.

Pri vizualni (k, n) shemi (v nadaljevanju zgolj (k, n) shemi) skrivnost S tako predstavlja poljubna slika, ki naj bo zaenkrat še črno-bela. Deleži oseb so prav tako črno-bele, prosojnice z lastnostjo, da če postavimo poljubnih k prosojnic eno nad drugo, se nam razkrije skrivnost oziroma slika S. Poleg tega zopet zahtevamo, da manj kot k prosojnic ne razkrije nobene informacije o skrivnosti (glej 3.1).

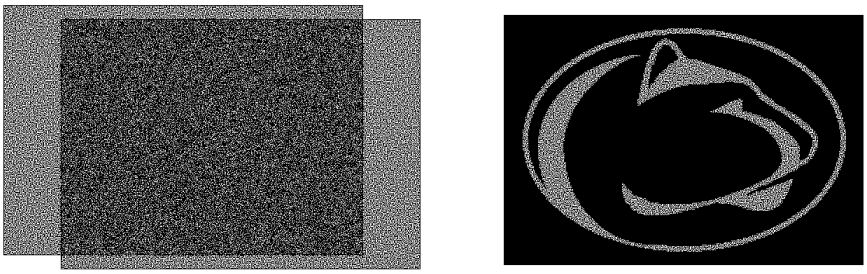
Deleži oseb so pravzaprav prosojnice potiskane zgolj s črno barvo, tako da izraz črno-bele v tem kontekstu dejansko pomeni črno-prosojne. Zaradi enostavnosti pa vseeno tudi v nadaljevanju uporabljamo izraz črno-bele.

Predpostavimo da so piksli slike S med seboj neodvisni, tako lahko brez izgube za splošnost obravnavamo vsakega posebej (predpostavka morda ni vedno resnična). Takoj pa naletimo na glavni problem pri vizualnih shemah, da če prekrijemo dva piksla človeški vid naredi njun logični *ali* in ne logični *xor* (ekskluzivni ali), kot bi želeli (glej 6). Tako na primer vsaka oseba ve, da je nek piksel skrivnosti S črn, takoj ko je ustrezen piksel črn na njeni prosojnici. To pa pomeni, da 2. točka iz definicije shem za deljenje skrivnosti ni zadoščena.

Rešitve sta se domislila Naor in Shamir leta 1994. Vsak piksel skrivnosti S na deležih S_i predstavimo z $m > 1$ podpiksli. Ko deleže (prosojnice) prekrijemo, je tako vsak piksel razkrite skrivnosti R dejansko predstavljen z m podpiksli (slika se poveča). Definirajmo sivino piksla $x \in R$ kot delež črnih podpikslov, ki ustrezajo pikslu x. V kolikor velja, da je sivina vseh pikslov v R, ki ustrezajo črnim pikslom v S, večja kot pa sivina tistih, ki ustrezajo belim pikslom, tedaj je slika oziroma skrivnost razpoznavna (glej 7). Minimalno razliko med omenjenima sivinama imenujemo relativni kontrast γ.



Slika 6: Logični *ali* (sredina) in pa logični *xor* (desno) dveh pikslov. Logični *ali* ustreza človeškemu vidu.



Slika 7: Prekriti prosojnici razkrijeta skrivnost ((2, 2) shema). Ker je sivina pikslov, črnih v S, večja kot pa sivina tistih, ki ustrezajo belim pikslom v S, je slika razpoznavna (črni piksli ostanejo črni, beli postanejo sivi).

Bralec lahko takoj sam opazi, da je smiselno izbrati m tako, da je le ta popoln kvadrat. V nasprotnem primeru bi težko dosegli enako razmerje stranic na originalni in razkriti skrivnosti (sliki S in R).

3.2.1 Formalna definicija ter uporaba

Podajmo še formalno definicijo vizualne (k, n) sheme. Le ta je definirana z dvema $n \times m$ 0-1 matrikama B^0 in B^1 (bazni matriki), tako da za vsako podmnožico $G \subseteq \{1, 2, \ldots n\}$ velja:

$|G| = k$**:** razlika Hammingovih tež logičnega *ali* vrstic matrik $B^0(G)$ in $B^1(G)$ je enaka vsaj γm

$|G| < k$**:** matriki $B^0(G)$ in $B^1(G)$ sta enaki do permutacije stolpcev natančno

Oznaka $B^{\cdot}(G)$ predstavlja $|G| \times m$ matriko, ki jo dobimo tako, da matriko $B^{\cdot}$ omejimo na vrstice določene z G. Prvi pogoj iz definicije imenujemo *kontrast*, saj nam zagotavlja, da je relativni kontrast sheme enak vsaj γ. Drugemu pravimo *varnost*, saj je ekvivalenten trditvi, da manj kot k oseb ne more razkriti prav

nobene informacije o skrivnosti. Pogoja tako tudi zaporedoma ustrezata zahtevama iz definicije splošnih shem za deljenje skrivnosti predstavljenih v 3.1.

Sledi primer baznih matrik za $(3, 3)$ shemo z razširitvijo piksla $m = 4$ in relativnim kontrastom $\gamma = \frac{1}{4}$. Enostavno je preveriti, da matriki ustrezata pogojema iz definicije vizualne (k, n) sheme. Na sliki 8 so prikazani še možni piksli na deležih S_i.

$$B^0 = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix} \text{ in } B^1 = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix}$$

Slika 8: Možni piksli na deležih S_i za shemo definirano z zgornjima matrikama.

Distribucija deležev S_i: Naj bosta B^0 in B^1 bazni matriki (k, n) sheme. Deleže S_i tedaj ustvarimo tako, da za vsak piksel x skrivnosti S ponovimo naslednji postopek:

1. ustvari naključno permutacijo π množice $\{1, 2, \ldots n\}$
2. uporabi π nad stolpci matrike B^i, kjer je $i = \begin{cases} 0 & \text{če je } x \text{ bel piksel} \\ 1 & \text{če je } x \text{ črn piksel} \end{cases}$
3. naj bo B matrika dobljena na prejšnjem koraku. j-ti podpiksel piksla x v deležu i-te osebe S_i je tedaj enak B_{ij}

Ponovitve postopka, za vsak piksel skrivnosti S, morajo biti med seboj neodvisne - vsaka ponovitev mora uporabljati svoje naključne bite. Slednje nam tedaj skupaj z definicijo baznih matrik zagotavlja drugo zahtevo iz definicije (k, n) shem. Prva zahteva prav tako neposredno sledi iz definicije baznih matrik.

3.3 Relativni kontrast ter razširitev piksla

Večina raziskovanja na področju vizualnih shem je temeljila na izboljšanju obeh parametrov shem - relativnega kontrasta γ ter razširitve piksla m. Želeli bi, da je razširitev piksla čim manjša, saj je vsak delež dejansko m-krat večji kot pa sama skrivnost. Enako seveda velja za rekonstruirano skrivnost R. Prav tako je želja ohraniti γ čim večji in tako zagotoviti prepoznavnost skrivnosti (slike). Vpliv obeh parametrov je moč lepo videti na sliki 9. Glede kontrasta ne tem mestu omenimo še, da večina shem ohrani črne piksle popolnoma črne, beli pa postanejo sivi (lastnost popolne črnosti).

Lema (Blundo, De Santis in Stinson, 1996): Poljubni dve različni vrstici bazne matrike B^1 $(2, n)$ sheme vsebujeta vzorca $[1\ 0]^T$ in $[0\ 1]^T$ (neizogibni vzorci), vsakega vsaj γm-krat.

Slika 9: Originalna skrivnost S (levo) ter pa rekonstruirana skrivnost R (desno). Opazimo občutno povečanje slike ter pa izgubo kontrasta.

Dokaz: Dokaz najdemo v [9].

Naslednji izrek predstavlja enega od pomembenjših dosežkov na področju iskanja shem z optimalnim kontrastom. Podaja nam namreč zgornjo mejo za γ v primeru $(2, n)$ sheme.

Izrek (Blundo, De Santis in Stinson, 1996): Za vsako $(2, n)$ shemo velja

$$\gamma \leq \gamma^*(n) := \frac{\lceil \frac{n}{2} \rceil \lfloor \frac{n}{2} \rfloor}{n(n-1)}.$$

Dokaz: Naj bo X množica trojk definirana kot

$$X = \{(i, j, k) |\ B^1_{ik} = 0, B^1_{jk} = 1, i \neq j\}.$$

Trojke ustrezajo ravno neizogibnim vzorcem iz prejšnje leme in tako dobimo

$$|X| \geq 2\binom{n}{2}\gamma m = n(n-1)\gamma m.$$

Očitno je, da lahko vsak stolpec matrike B^1 pokriva več takih neizogibnih vzorcev. Če je i število enic v nekem stolpcu, tedaj le ta pokriva natanko $i(n-i)$ vzorcev. $i(n-i)$ doseže svoj maksimum pri $i = \lceil \frac{n}{2} \rceil$ oziroma pri $i = \lfloor \frac{n}{2} \rfloor$, tako velja

$$|X| \leq \lceil \frac{n}{2} \rceil \lfloor \frac{n}{2} \rfloor m.$$

Če združimo dobljeni neenakosti dobimo

$$n(n-1)\gamma m \leq |X| \leq \lceil \frac{n}{2} \rceil \lfloor \frac{n}{2} \rfloor m$$

in tako

$$\gamma \leq \frac{\lceil \frac{n}{2} \rceil \lfloor \frac{n}{2} \rfloor}{n(n-1)}.$$

□

V nadaljevanju se posvetimo še razširitvi piksla v primeru $(2, n)$ shem. Brez dokaza podajmo naslednji izrek.

Izrek: $(2, n)$ shema z razširitvijo piksla m in relativnim kontrastom $\gamma \geq \frac{1}{m}$ obstaja natanko tedaj, ko obstaja Spernerjeva družina velikosti n nad množico M, pri čimer velja $|M| = m$.

Spernerjeva družina velikosti n nad množico M je množica n podmnožic množice M za katere velja, da nobena izmed njih ne vsebuje druge.

Izrek (Sperner, 1928): Naj bo $\mathcal{A}$ Spernerjeva družina nad množico M moči m. Tedaj velja

$$\mathcal{A} \leq \binom{m}{\lceil \frac{m}{2} \rceil}.$$

Enakost je dosežena natanko tedaj, ko $\mathcal{A}$ vsebuje vse podmnožice moči $\lceil \frac{m}{2} \rceil$, oziroma $\lfloor \frac{m}{2} \rfloor$, množice M.

Dokaz: Dokaz na tem mestu izpustimo.

Iz izrekov neposredno sledi naslednja posledica.

Posledica: $(2, n)$ shema z razširitvijo piksla m in relativnim kontrastom $\gamma \geq \frac{1}{m}$ obstaja natanko tedaj, ko velja $n \leq \binom{m}{\lceil \frac{m}{2} \rceil}$.

Posledica podaja spodnjo mejo za razširitev piksla m, tako lahko na primer izberemo $m = O(\log n + \log \log n)$.

3.4 Konstrukcija vizualnih shem iz *BIBD*

Na tem mestu podajmo še konstrukcijo vizualnih (k, n) shem s pomočjo kombinatoričnih objektov predstavljenih v 2.

Izrek (Blundo, De Santis in Stinson, 1996): Naj obstaja (v, k, λ)-*BIBD*. Tedaj obstaja $(2, v)$ shema z razširitvijo piksla $m = b$ ter relativnim kontrastom $\gamma = (r - \lambda)/b$.

Dokaz: Naj bo bazna matrika B^1 enaka incidenčni matriki (v, k, λ)-*BIBD*, oziroma

$$B^1_{ij} = \begin{cases} 1 & \text{če } i\text{-ta točka leži v } j\text{-tem bloku} \\ 0 & \text{sicer} \end{cases}$$

in naj bo vseh v vrstic matrike B^0 sestavljenih iz r enic, katerim sledi $m - r$ ničel. Hammingova teža katerekoli vrstice matrik B^0, B^1 je enaka r, kar nam zagotavlja drugo zahtevo iz definicije vizualnih shem.

Poglejmo še Hammingovo težo logičnega *ali* poljubnih dveh vrstic. V primeru B^0 je ta očitno enaka r, v primeru B^1 pa $2r - \lambda$. Slednje sledi neposredno iz lastnosti *BIBD*. Tako dobimo, da je relativni kontrast konstruirane sheme enak

$$\gamma = \frac{2r - \lambda - r}{b} = \frac{r - \lambda}{b}.$$

S tem je zagotovljena tudi druga zahteva iz definicije vizualnih shem in izrek je dokazan.

□

Predpostavimo resničnosti Hadamardove matrične domneve. Tedaj iz izreka v 2.2, ter pa slednjega, naposredno sledi naslednja posledica.

Posledica: Za vsak $s \in \mathbb{N}$ obstaja $(2, 4s-1)$ shema z razširitvijo piksla $m = 4s-1$ ter optimalnim relativnim kontrastom $\gamma^* = s/(4s-1)$.

Še močnejši pa je naslednji izrek, ki predstavlja enega od glavnih delov naloge. Podajamo ga brez dokaza, le ta pa deloma sledi že iz prejšnih izrekov in zadnje posledice. Celoten dokaz je sicer moč najti v [9].

Izrek (Blundo, De Santis in Stinson, 1996): Predpostavimo resničnost Hadamardove matrične domneve. Tedaj za vsak $n \in \mathcal{N}\backslash\{1\}$ obstaja $(2, n)$ shema z optimalnim relativnim kontrastom γ^* ter razširitvijo piksla

$$m = \begin{cases} 2n-2 & \text{če je } n \equiv 2 \pmod 4 \\ n & \text{če je } n \equiv 3 \pmod 4 \\ 2n & \text{če je } n \equiv 1 \pmod 4 \end{cases}$$

Izrek nam tako da konstrukcijo prav vseh vizualnih $(2, n)$ shem, pri čimer imajo le te tudi optimalen kontrast. Poleg vsega pa velja tudi, da je razširitev piksla optimalna med vsemi shemami z optimalnim kontrastom. Tako bi m sicer lahko bil tudi manjši, vendar pa bi to zmanjšalo tudi γ. Omenimo še, da so vse sheme dobljene zgolj s uporabo Hadamardovih matrik, kar še enkrat dokazuje pomembnost teh kombinatoričnih objektov.

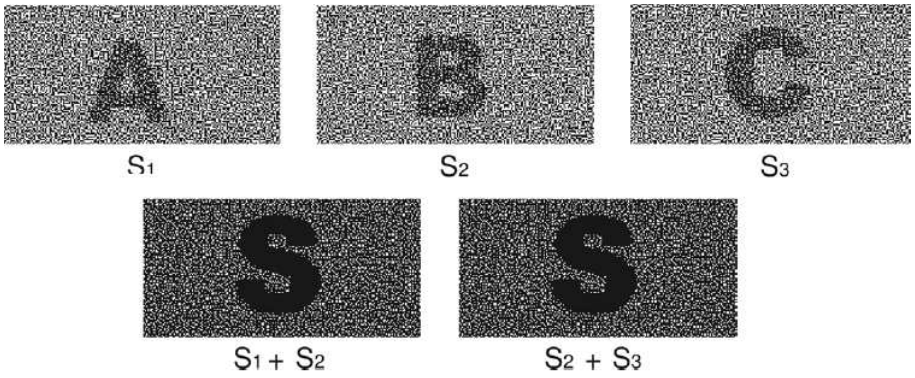
4 Razširjene vizualne sheme

Pomemben vidik skrivanja informacije, oziroma deljenja skrivnosti, pa predstavlja tudi skrivanje samega dejstva, da neka skrivnost sploh obstaja. Tako bi na primer želeli, da posamezni deleži skrivnosti S_i vsebujejo neke poljubne nedolžne slike in ne, da izgledajo kot naključen šum - napadalec lahko takoj sklepa, da delež skriva neko informacijo saj je sicer popolnoma naključen (glej sliko 7).

Vizualne sheme, katerih deleži vsebujejo nedolžne slike P_i, imenujemo razširjene vizualne sheme (Ateniese, Blundo et al., 1996). Sicer so v vseh ostalih pogledih popolnoma enake običajnim vizualnim shemam. Navadno pa jih naprej delimo še na šibke in močne - pri slednjih predpostavimo da morebiten napadalec pozna vse slike P_i dočim pri šibkih le ta pozna zgolj slike deležev, ki jih poseduje.

Predvsem šibke razširjene sheme pa poleg skrivanja dejstva o obstoju same skrivnosti preprečujejo tudi nekatere vrste napadov oziroma bolje rečeno prevar (glej 5). Povrhu vsega pa omogočajo tudi eleganten način razlikovanja med deleži, v kolikor neka oseba poseduje večje število deležev (za različne skrivnosti).

Kot primer najprej podajmo enostavno razširjeno $(2, 2)$ vizualno shemo, kot sta jo predlagala že Naor in Shamir (1994). Konstrukcija deležev za to shemo poteka popolnoma enako kot prej (glej 3) samo da na vsakem koraku uporabimo primerni bazni matriki. Natančneje, naj bo x piksel skrivnosti S, ter naj bosta p_1, p_2 ustrezna piksla na slikah P_1, P_2. Tedaj bazni matriki izberemo glede na:



Slika 10: Vsak izmed deležev razširjene $(2,3)$ sheme vsebuje neko nedolžno sliko P_i (zgoraj). Ko pa deleže prekrijemo vseeno dobimo skrivnost S brez sledov o prvotnih slikah P_i (spodaj).

p_1, p_2 sta bela:

$$B^0 = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix} \text{ in } B^1 = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \end{bmatrix}$$

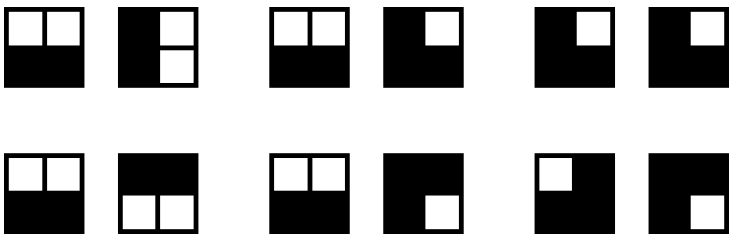
p_1 je bel in p_2 je črn:

$$B^0 = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 \end{bmatrix} \text{ in } B^1 = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix}$$

p_1, p_2 sta bela:

$$B^0 = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 \end{bmatrix} \text{ in } B^1 = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix}$$

Bralec lahko sam preveri, da vse bazne matrike ustrezajo zahtevam iz definicije vizualnih shem. Podobno lahko takoj opazimo, da je razširitev piksla enaka 4 dočim relativni kontrast znaša zgolj $\gamma = \frac{1}{4}$ (relativni kontrast obeh deležev oziroma slik P_i je prav tako enak $\gamma_i = \frac{1}{4}$). Možni piksli, ki jih dobimo na deležih S_1, S_2 s pomočjo zgornjih matrik so prikazani na sliki 11.



Slika 11: Vsi možni piksli (brez vseh permutacij) na deležih S_1, S_2 za razširjeno $(2,2)$ shemo, ki sta jo predlagala Naor in Shamir (1994).

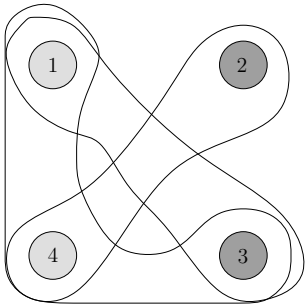
4.1 Splošna konstrukcija

V nadaljevanju sledi izrek, ki podaja konstrukcijo razširjene sheme iz poljubne enostavne sheme. Izrek pa dejansko podaja konstrukcijo za sheme s splošno strukturo dovoljenj (glej 3), zato najprej povejmo še nekaj besed o tem. Kot že omenjeno, gre za običajno shemo za deljenje skrivnosti, kjer pa skrivnost lahko razkrijejo le neke v naprej določene skupine oziroma množice ljudi (pri (k, n) shemi so te množice vse k-elementarne podmnožice $\{1, 2, \ldots n\}$). Strukturo dovoljenj tako določa množica Γ, ki vsebuje omenjene množice.

$$\Gamma \subseteq \mathcal{P}^{\{1,2,\ldots n\}}$$

Naj opozorimo, da je zgornja definicija shem za splošno strukturo dovoljenj nekoliko okrnjena, a popolnoma zadošča potrebam v tej nalogi.

Najnaravnejši način predstavitve strukture dovoljenj Γ je s pomočjo hipergrafov. Hipergraf H je običajen graf, kot ta pojem razumemo v matematični teoriji, s to razliko, da so njegove povezave lahko tudi več, oziroma manj, kot 2-elementarne podmnožice množice vozlišč $V(H)$. Pri običajnem grafu G so povezave vedno 2-elementarne podmnožice $V(G)$. Primer hipergrafa lahko vidimo na sliki 12.



Slika 12: Hipergraph s tremi povezavami $\{1, 3\}$, $\{1, 3, 4\}$ in $\{2, 4\}$.

Definirajmo še pojem barvanje hipergrafa. q-barvanje hipergrafa H je običajno barvanje vozlišč grafa s q barvami, pri čimer pa mora veljati naslednje ($c(i)$ je barva vozlišča i):

$$\forall e \in E(H) : |e| = 1 \vee |\{c(i)|\ i \in e)\}| \geq 2$$

Pogoj pomeni, da morajo biti vozlišča vsake povezava moči vsaj 2 pobarvana z vsaj 2-ema barvama, v kolikor želimo da je barvanje regularno. Na sliki 12 lahko vidimo regularno 2-barvanje prikazanega hipergrafa.

Sedaj lahko končno podamo napovedan izrek.

Izrek (Ateniese, Blundo et al., 1996): Naj obstaja shema za strukturo dovoljenj Γ z razširitvijo piksla m ter naj obstaja q-barvanje hipergrafa induciranega s strukturo dovoljenj Γ. Tedaj obstaja razširjena shema za Γ z razširitvijo piksla $m + q$.

Dokaz: Glej [11].

Dokaz izreka podaja splošno konstrukcijo razširjenih shem za poljubno običajno shemo. Izrek pa se seveda močno poenostavi v primeru stopenjskih (k, n) shem, oziroma $(2, n)$ shem, katerim smo se v večini posvečali v 3. Neposredno iz izreka tako dobimo naslednjo posledico.

Posledica (Ateniese, Blundo et al., 1996): Naj obstaja običajna $(2, n)$ shema z razširitvijo piksla m. Tedaj obstaja razširjena $(2, n)$ shema z razširitvijo piksla $m + n$.

5 Varnost

Vizualne sheme so s stališča informacijske teorije popolnoma varne. Slednje pomeni, da morebitni napadalec kljub neomejeni računski moči, znanju ter pa poznavanju deležev $\{S_{i_1}, S_{i_2}, \ldots S_{i_j}\}$, $j < k$, ne more pridobiti prav nobene informacije o sami skrivnosti S. Formalno to zapišemo kot

$$H(S = s) = H(S = s|S_{i_1}, S_{i_2}, \ldots S_{i_j}), j < k,$$

kjer je $H(\cdot)$ funkcija entropije definirana kot

$$H(X) = -\sum_i P(X = x_i) \log P(X = x_i).$$

Lastnost popolne varnosti je nekako tudi očitna, saj so vizualne sheme v svoji zasnovi močno podobne enkratnemu ščitu oziroma Vernamovi šifri. Omeniti pa je potrebno, da sama lastnost zahteva, da so vsi deleži vsaj tako veliki kot sama slika oziroma skrivnost. Ker pa je slednje zagotovljeno že v sami zasnovi vizualnih shem ($m > 1$), dejansko ne predstavlja njihove slabosti.

Kot pa smo omenili že prej, se včasih zadovoljimo že zgolj z računsko varnostjo neke sheme, saj nam to navadno prinese precej manjše deleže.

5.1 Prevare

Iz prejšnjega razdelka neposredno sledi, da bi bili kakršnikoli napadi na vizualne sheme brezpredmetni (lastnost popolne varnosti). Kljub temu pa lahko pride do ”napadov”, ki bi jih bilo bolje poimenovati prevare. V večini primerov gre za to, da želi napadalec zavesti (ostale) osebe tako, da se pri rekonstrukciji skrivnosti prikaže napačna slika oziroma skrivnost. (Ostale) osebe tega seveda ne morejo zaznati, saj ne poznajo same skrivnosti.

V literaturi so predstavljene različne prevare, tako za običajne kot za razširjene vizualne sheme. Slednje se navadno izkažejo za bolj trdožive, vendar pa vseeno obstaja cela vrsta prevar. Predstavljene so bile tudi različne sheme odporne na take prevare, vendar pa pogosto niso odporne prav na vse.

Prevare delimo glede na vlogo samega napadalca. Le ta je lahko:

1. *zloben udeleženec* - oseba, ki sodeluje pri deljenju skrivnosti
2. *zloben ”tvorec” deležev* - oseba, ki ustvari same deleže
3. *zlobna tretja oseba*

V nadaljevanju predstavimo dve prevari za običajne stopenjske (k, n) sheme (Hu in Tzeng, 2007). V prvem primeru je napadalec *zloben udeleženec*, v drugem pa *zlobna tretja oseba*. Obe prevari izkoriščata dejstvo, da so deleži oseb popolnoma naključni in zato njihove prosojnice izgledajo kot naključen šum. Napadalec lahko tako ustvari lažne deleže, ki izgledajo popolnoma enako kot pristni.

5.1.1 Prevara *zlobnega udeleženca*

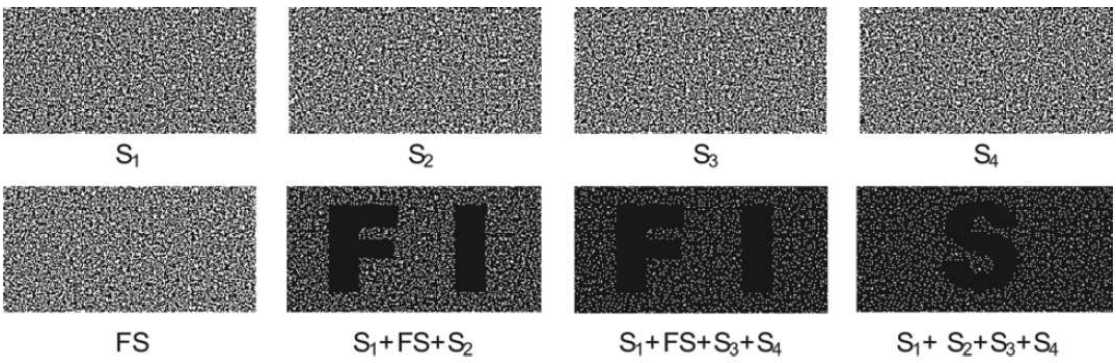
Naj bo napadalec prva oseba, ki si deli skrivnost. Njegov delež je tako enak S_1, FS pa naj označuje lažno sliko oziroma skrivnost. Predpostavimo še, da ima uporabljena shema lastnost popolne črnosti ter, da vsaka vrstica bazne matrike B^1 sestoji iz natanko e enic ter $m-e$ ničel oziroma, sivina vsakega piksla, ki skriva nek črn piksel v S, je enaka $\frac{e}{m}$. Napadalec tedaj ustvari $r = \lceil \frac{e}{m} \rceil - 1$ lažnih deležev FS_i tako, da za vsak piksel x lažne slike FS ponovi naslednje:

x je bel: kopiraj ustrezen piksel S_1 na vse FS_i

x je črn: na vsak FS_i naključno razporedi e črnih ter $m-e$ belih podpikslov tako, da bo prekritju vseh FS_i ustrezen piksel črn

Konstrukcija nam zagotavlja, da že samo deleži FS_i ter pa S_1 razkrijejo lažno skrivnost FS. Ustrezni piksli so popolnoma črni (lastnost popolne črnosti) zatorej bo tudi ob prekritju vseh FS_i, S_1, ter pa nekaterih ostalih $S_{i>2}$ (ne vseh), lažna skrivnost vidna. Na mestih, ki ustrezajo belim pikslom v FS, pa so vsi FS_i popolnoma enaki kot S_1, kar nam zagotavlja, da ti piksli po rekonstrukciji ne morejo postati črni - pri rekonstrukciji ne sodelujejo vse osebe oziroma vsi deleži $S_{i>2}$ in bi bilo tako slednje v protislovju z drugo zahtevo stopenjskih shem za deljenje skrivnosti.

Iz opisanega lahko zaključimo, da prevara vedno uspe, prav tako je očitno, da lažni deleži izgledajo enako kot pristni. Napadalec pa mora vseeno rešiti problem, da pri rekonstrukciji ne smejo sodelovati vse osebe. V nasprotnem primeru bi se seveda hkrati razkrile obe skrivnosti FS in S. Primer prevare za $(4,4)$ shemo je viden na sliki 13.



Slika 13: Napadalec s pomočjo svojega deleža S_1 ustvari lažen delež FS, ter tako zavede poštene osebe oziroma udeležence (sredina, spodaj).

5.1.2 Prevara *zlobne tretje osebe*

Prevara *zlobne tretje osebe* je podobna prejšnji s to razliko, da sedaj ne poznamo distribucije črnih in belih podpikslov za nek črn piksel skrivnosti (vrednost e). Podobno ne poznamo same velikosti deležev oziroma vrednosti m. Prvi problem rešimo tako, da uporabimo optimalno $(2,2)$ shemo, kot smo jih predstavili v 3.4, ter tako ustvarimo dva deleža FS_1, FS_2 na podlagi lažne skrivnosti FS. Ta dva deleža uporabljamo tako kot prej in prevara bo očitno uspela.

Edini problem, ki ga je še potrebno rešiti, je kako ustvariti deleže prave velikosti m. Avtorja prevare predlagata ustvariti deleže za vsako možno vrednost m. Ideja se sprva zdi absurdna, vendar pa je ob predpostavki, da so deleži natisnjeni z običajnimi tiskalniki, ki za predstavitev slike uporabljajo piksle, potrebno ustvariti zgolj deleže velikosti $1, 4, 9, 16, 25, \ldots$

Obe opisani prevari seveda ne delujeta za razširjene vizualne sheme, saj v tem primeru ne poznamo distribucije črnih in belih pikslov na samih deležih oziroma ne vemo kakšne so slike P_i na pristnih deležih S_i.

6 Predlagane sheme v praksi

Vizualne sheme za deljenje skrivnosti so uporabne predvsem tam, kjer ni na voljo nekega računskega stroja, ki bi izvajal potrebne postopke pri rekonstrukciji skrivnosti. Tu gre predvsem za osebe na terenu, oziroma v okolju brez električne napeljave. Podobno se sheme izkažejo tedaj, ko so osebe kriptografsko nevešče ali celo računalniško nepismene - starejši, otroci, umsko zaostali,... Enostavnost rekonstrukcije skrivnosti je tako glavna prednost vizualnih shem pred ostalimi shemami za deljenje skrivnost.

Težava pa se pojavi pri distribuciji deležev. Ker so deleži natisnjeni na običajne prosojnice, se le te lahko zaradi zunanjih vplivov deformirajo. Deformacija je lahko celo tako velika, da skrivnosti enostavno ni več moč rekonstruirati. Problema se navadno loteva tako, da uporabljamo neke vrste okvir za poravnavo prosojnic oziroma da deleže natisnemo na prosojne ploščice, na katere zunanji dejavniki ne vplivajo.

Povejmo še nekaj besed o vizualnih shemah pridobljenih iz *BIBD*, katere na nek način predstavljajo jedro te naloge. Kot smo videli že v 3.4 so sheme optimalne s stališča relativnega kontrasta, prav tako pa imajo optimalno razširitev piksla med vsemi takimi shemami. V kolikor predpostavimo še resničnost Hadamardove domneve poznamo tudi učinkovito konstrukcijo prav vseh takih $(2, n)$ shem. Poleg omenjenega pa veliko pove tudi močna povezanost teh shem z znanimi kombinatoričnimi objekti kot so Hadamardove matrike in pa bločni designi.

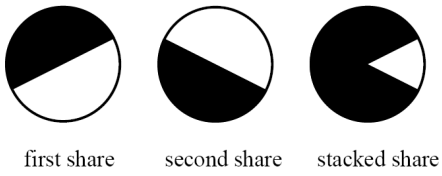
7 Druge vizualne sheme

V tem razdelku zgolj omenimo še druge vrste vizualnih shem, ki se pojavljajo v literaturi. Naor in Shamir sta že leta 1994 predlagala način, kako uporabiti vizualne sheme tudi v primeru sivinskih slik. Ideja pa se ni obnesla saj ni primerna za predstavitev z današnjimi računalniki (glej 14). Predlagala sta tudi, da bi lahko sliko "razbili" na 256 slik, za vsak nivo sivine eno, ter da v nadaljevanju nato skrivamo vsak nivo sivine posebej (dejansko vse naredimo nad eno zelo veliko sliko).

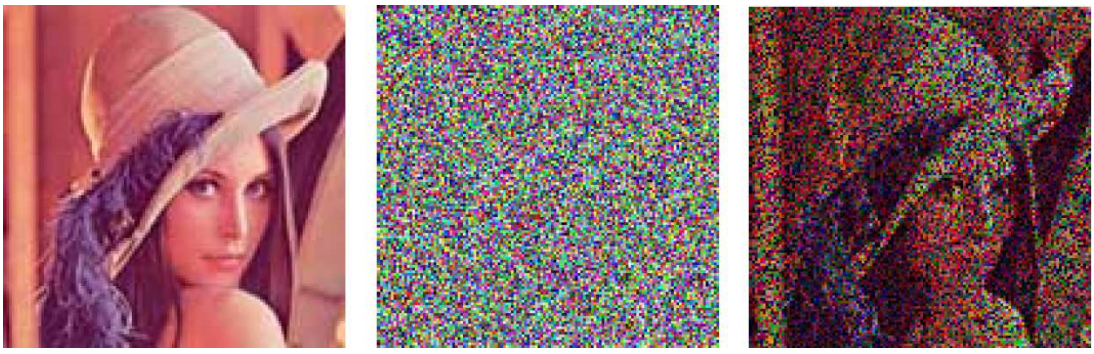
Danes obstajajo tudi splošne sheme za sivinske slike (Blundo, De Santis et al., 2000) ter pa tudi za barvne slike (glej sliko 15). Omenimo še sheme za splošne strukture dovoljenj (omenjene v 4), sheme na osnovi logičnega *ali* ter pa sheme pri katerih skrivnost predstavlja več različnih slik.

8 Zaključek

Naloga podaja nek splošen pregled vizualne kriptografije, na drugi strani pa predstavi konstrukcijo vizualnih shem skozi bločne designe in Hadamardove matrike in je tako na nek način tudi vodič pri



Slika 14: Vsak delež naj bo predstavljen s krožnim izsekom (levo in sredina). Velikost krožnega izseka po prekritju deležev predstavlja sivino nekega ”piksla” (desno).



Slika 15: Primer vizualne sheme za barvne slike. Originalna skrivnost na levi, eden od deležev na sredi ter pa rekonstruirana skrivnost na desni. Opazimo, da je izguba kontrasta v primeru barvnih slik lahko zelo moteča.

konstrukciji takih shem. Kljub dejstvu, da je področje še relativno mlado (od leta 1994), pa obstaja še cela vrsta drugih zanimivosti, ki niso omenjene v tej nalogi.

A Konstrukcije Hadamardovih matrik

A.1 Kroneckerjev produkt in Sylvestrove matrike

Ena od najenostavnejših konstrukcij Hadamardovih matrik uporablja Kroneckerjev produkt $\otimes$ definiran kot

$$A \otimes B = \begin{bmatrix} a_{11}B & \dots & a_{1n}B \\ \vdots & \ddots & \vdots \\ a_{n1}B & \dots & a_{nn}B \end{bmatrix}.$$

Izrek: Naj bosta H_n, H_m Hadamardovi matriki redov n in m zaporedoma. Tedaj je $H_n \otimes H_m$ Hadamardova matrika reda nm.

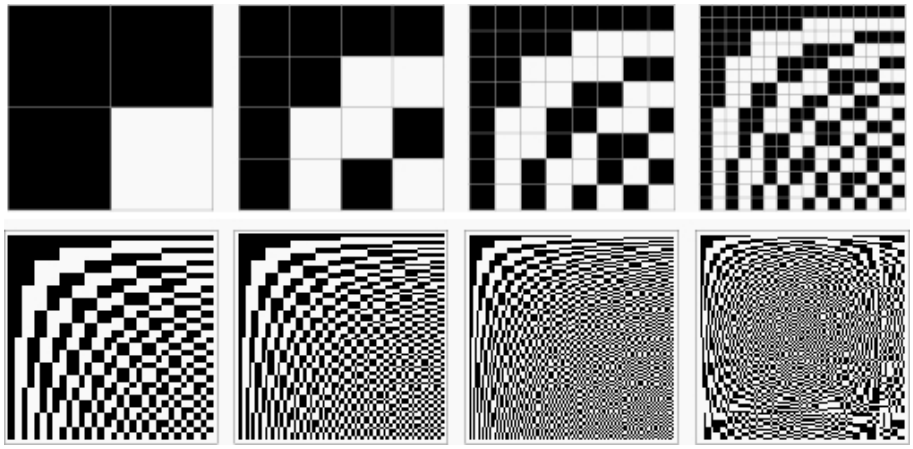
Dokaz: Očitno so vsi elementi $H_n \otimes H_m$ enaki 1 oziroma -1. Preverimo še ortogonalnost vrstic, oziroma stolpcev, ter njihovo dolžino

$$(H_n \otimes H_m)(H_n \otimes H_m)^T = (H_n \otimes H_m)(H_n^T \otimes H_m^T) =$$

$$= H_n H_n^T \otimes H_m H_m^T = nI_n \otimes mI_m = nmI_{nm}.$$

□

Izrek nam da konstrukcijo velike družine Hadamardovih matrik, med drugim tudi vse matrike reda 2^n, $n \in \mathbb{N}$ (Sylvestrove matrike). Slednjo družino pa je moč konstruirati tudi prek Walshovih funkcij - s pomočjo vseh 2^n Walshovih funkcij reda n lahko konstruiramo Hadamardovo matriko reda 2^n (glej sliko 16).



Slika 16: Hadamardove matrike konstruirane s pomočjo Walshovih funkcij (Sylvestrove matrike).

A.2 Paleyjeve matrike

Naj bo q potenca praštevila in naj velja $q \equiv 3 \pmod 4$. Tedaj velja, da je polovica elementov iz polja $\mathbb{F}_q$ kvadratnih ostankov po modulu q in polovica elementov kvadratnih ne-ostankov. Za vsak $x \in \mathbb{F}_q \backslash \{0\}$ tako definiramo preslikavo χ kot

$$\chi(x) = \begin{cases} 1 & \text{če je } x \text{ kvadratni ostanek po modulu } q \\ -1 & \text{sicer} \end{cases}$$

Naslednji izrek predstavlja Paleyevo konstrukcijo Hadamardovih matrik.

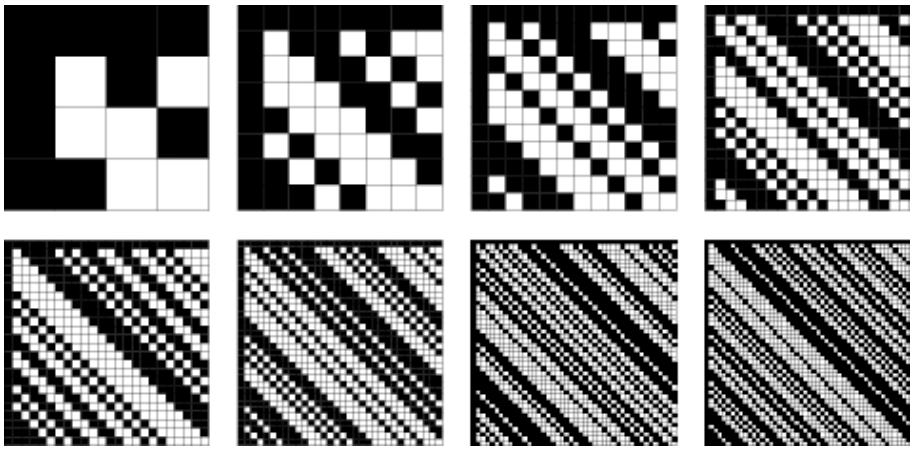
Izrek (Paley, 1933): Naj bo q potenca praštevila in naj velja $q \equiv 3 \pmod 4$. Tedaj je matrika

$$H_{q+1} = \begin{bmatrix} 1 & 1 & \dots & 1 \\ 1 & & & \\ \vdots & & Q - I_q & \\ 1 & & & \end{bmatrix}$$

Hadamardova matrika reda $q + 1$ (Paleyeva matrika), kjer je Q $q \times q$-dimenzionalna matrika definirana z $(Q)_{ij} = \chi(j - i)$.

Dokaz: Za dokaz glej [19].

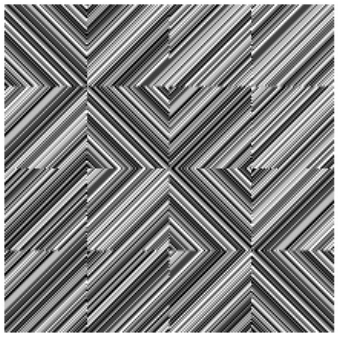
Poleg omenjenega, Paley poda še dva izreka o obstoju Hadamardovih matrik oziroma še dve konstrukciji le teh. Z uporabo vseh treh konstrukcij in pa Kroneckerjevega produkta iz prejšnjega razdelka lahko konstruiramo že zelo veliko družino Hadamardovih matrik. Najmanša matrika, ki jo omenjene konstrukcije ne pokrijejo, je matrika reda 92.



Slika 17: Paleyjeve matrike.

A.3 Druge konstrukcije

Poleg omenjenih obstaja še kar nekaj drugih konstrukcij. Med najbolj znanimi sta gotovo Williamsonova konstrukcija in pa konstrukcija z Baumert-Hall tabelami, sicer pa lahko Hadamardove matrike konstruiramo tudi iz ortogonalnih designov, latinskih kvadratov, Steinerjevih trojk, itd. Kot je bilo že povedano, je trenutno najmanjša matrika, ki jo še ne znamo konstruirati, matrika reda 668 - leta 2004 je bila konstruirana tedaj najmanša neznana matrika reda 428 (Kharaghani in Tayfeh-Rezaie).



Slika 18: Hadamardova matrika reda 428.

B Izrek Bruck-Ryser-Chowla

Za dokaz izreka Bruck-Ryser-Chowla potrebujemo enega od Lagrangeovih izrekov ter pa identiteto. Slednje brez dokaza podamo v nadaljevanju, nato pa sledi sam izrek in dokaz le tega.

Izrek (Lagrange, 1770): Vsako pozitivno celo število $q \in \mathbb{N}$ je moč zapisati kot vsoto štirih popolnih kvadratov.

$$q = b_1^2 + b_2^2 + b_3^2 + b_4^2, b_i \in \mathbb{Z}$$

Identiteta: Velja

$$(b_1^2 + b_2^2 + b_3^2 + b_4^2)(x_1^2 + x_2^2 + x_3^2 + x_4^2) = y_1^2 + y_2^2 + y_3^2 + y_4^2,$$

kjer je

$$\begin{aligned} y_1 &= b_1x_1 - b_2x_2 - b_3x_3 - b_4x_4, \\ y_2 &= b_2x_1 + b_1x_2 - b_4x_3 + b_3x_4, \\ y_3 &= b_3x_1 + b_4x_2 + b_1x_3 - b_2x_4, \\ y_4 &= b_4x_1 - b_3x_2 + b_2x_3 + b_1x_4. \end{aligned} \tag{2}$$

Identiteto je moč pokazati z uporabo kvaternionov.

Izrek (Bruck, Ryser, Chowla, 1950): Naj obstaja simetričen (v, k, λ)-*BIBD* ($v = b$, $k = r$) ter naj bo $q = k - \lambda$. Tedaj velja:

v je sodo: q je popoln kvadrat,

v je liho: diofantska enačba $z^2 = qx^2 + (-1)^{\frac{1}{2}(v-1)}\lambda y^2$ ima netrivialno celoštevilsko rešitev za x, y, z.

Dokaz (sledimo dokazu v [4]): Bločni design najenostavneje opišemo z incidenčno matriko A. Vrstice matrike A ustrezajo točkam, stolpci pa blokom designa. V kolikor i-ta točka designa leži v j-tem bloku je $(A)_{ij} = 1$, v naprotnem primeru pa je $(A)_{ij} = 0$. Neposredno iz definicije designa sledi, da je AA^T enako

$$AA^T = B = \begin{bmatrix} r & \lambda & \dots & \lambda \\ \lambda & r & & \\ \vdots & & \ddots & \vdots \\ \lambda & & \dots & r \end{bmatrix} = (r - \lambda)I + \lambda J, \tag{3}$$

kjer je I matrika identitete in J matrika samih enic. Enostavno lahko izračunamo tudi determinanto matrike B (prvi stolpec odštejemo od vseh drugih ter nato prvi vrstici prištejemo ostale).

$$\det AA^T = (\det A)^2 = \det B = (r - \lambda)^{v-1}(v\lambda - \lambda + r).$$

Sedaj smo pripravljeni, da dokažemo sam izrek.

v je sodo: Ker velja $r = k$ lahko zapišemo

$$(\det A)^2 = (k-\lambda)^{v-1}(v\lambda - \lambda + k),$$

iz enačbe (1) pa še nadalje sledi

$$(\det A)^2 = (k-\lambda)^{v-1}k^2.$$

Ker je leva stran enačbe popoln kvadrat mora enako veljati tudi za desno oziroma, izraz $(k-\lambda)^{v-1}$ je prav tako popoln kvadrat. Ker je $v-1$ liho pa to dejansko pomeni, da je popoln kvadrat že sam $k - \lambda = q$. S tem je prvi del izreka dokazan.

v je liho: Dokaz drugega dela izreka je nekoliko daljši. Temelji na dejstvu, da je moč relacijo (3) zapisati tudi s pomočjo kvadratnih form. V ta namen točkam designa priredimo spremenljivke $x_1, \dots x_v$, blokom pa linearne forme L_j,

$$L_j = \sum_{i=1}^{v} (A)_{ij} x_i,$$

kjer je A incidenčna matrika designa. Enačbo (3) lahko sedaj zapišemo kot

$$\begin{aligned} L_1^2 + \ldots + L_v^2 = (k-\lambda)(x_1^2 + \ldots + x_v^2) + \lambda(x_1 + \ldots + x_v)^2 = \\ = q(x_1^2 + \ldots + x_v^2) + \lambda(x_1 + \ldots + x_v)^2. \end{aligned} \tag{4}$$

V nadaljevanju najprej dokažemo izrek za primer $v \equiv 1 \pmod 4$, nato pa še za $v \equiv 3 \pmod 4$.

v ≡ 1 (mod 4): Naj bo $q = b_1^2 + b_2^2 + b_3^2 + b_4^2$ za neka cela števila b_i (obstoj le teh nam zagotavlja Lagrangeov izrek). Z uporabo identitete iz začetka razdelka lahko desno stran enačbe (4) korakoma poenostavimo, saj velja

$$q(x_i^2 + x_{i+1}^2 + x_{i+2}^2 + x_{i+3}^2) = y_i^2 + y_{i+1}^2 + y_{i+2}^2 + y_{i+3}^2, \tag{5}$$

kjer so x-i in y-i povezani glede na enačbe (2). Tako $(v-1)/4$-krat uporabimo enačbo (5) nad desno stranjo (4) (vsakič nad novo četverico x-ov) ter dobimo

$$L_1^2 + \ldots + L_v^2 = y_1^2 + y_2^2 + \ldots + y_{v-1}^2 + qx_v^2 + \lambda(x_1 + \ldots + x_v)^2. \tag{6}$$

Naj bo $y_v = x_v$ ter $w = x_1 + \ldots + x_v$. Zadnjo enačbo (6) lahko sedaj prepišemo v

$$L_1^2 + \ldots + L_v^2 = y_1^2 + \ldots + y_{v-1}^2 + qy_v^2 + \lambda w^2. \tag{7}$$

Opazimo, da lahko x-e izrazimo s pomočjo y-ov, tedaj pa $L_1, \dots L_v$ in w postanejo racionalne linearne forme v spremenljivkah $y_1, \dots y_v$. Naj tako velja $L_1 = c_{11}y_1 + \ldots c_{1v}y_v$. Če je $c_{11} \neq 1$ lahko dodamo relacijo $L_1 = y_1$ (y-oni so še prosti), sicer dodamo $L_1 = -y_1$, v vsakem primeru pa tedaj velja $L_1^2 = y_1^2$, y_1 pa je določena kot racionalna linearna forma v spremenljivkah $y_2, \dots y_v$. (7) tako sedaj postane enačba nad spremenljivkami $y_2, \dots y_v$ oziroma

$$L_2^2 + \ldots + L_v^2 = y_2^2 + \ldots + y_{v-1}^2 + qy_v^2 + \lambda w^2. \tag{8}$$

Na tak način zaporedoma dodamo relacije $L_i = \pm y_i$ za vse $i = 2, \dots v-1$, ter na koncu dobimo

$$L_v^2 = qy_v^2 + \lambda w^2, \tag{9}$$

kjer sta L_v in w (racionalna) večkratnika y_v. Slednjega definiramo kot x, ki je enak produktu imenovalcev v zapisu L_v in w ($y_v = x \neq 0$). Tako pa sledi, da obstajata taka y, z, da velja

$$z^2 = qx^2 + \lambda y^2$$

pri čimer je vsaj en od y, z različen od 0. S tem je izrek v primeru $v \equiv 1 \pmod 4$ dokazan.

$v \equiv 3 \pmod 4$: Dokaz je podoben kot v prejšnjem primeru. Najprej definiramo novo spremenljivko x_{v+1} in na obe strani enačbe (4) dodamo qx_{v+1}^2. Z uporabo (5) tedaj dobimo

$$L_1^2 + \ldots + L_v^2 + qx_{v+1}^2 = y_1^2 + \ldots + y_{v+1}^2 + \lambda w^2, \tag{10}$$

nato pa postopamo tako kot pri prejšnjem primeru. Na koncu velja

$$qx_{v+1}^2 = y_{v+1}^2 + \lambda w^2, \tag{11}$$

kjer sta x_{v+1} in w (racionalna) večkratnika y_{v+1}, slednji pa je neodvisna spremenljivka. Podobno kot prej definiramo y_{v+1} kot z, ki je enak produktu imenovalcev v zapisu x_{v+1} in w ($z \neq 0$). Tako obstajata taka x, y da velja

$$qx^2 = z^2 + \lambda y^2,$$
$$z^2 = qx^2 - \lambda y^2.$$

Ker gotovo niso vsi x, y, z enaki 0, je izrek dokazan tudi v primeru $v \equiv 3 \pmod 4$.

□

Literatura

[1] D. R. Stinson. *Cryptography Theory and Practice*, Chapman & Hall/CRC, 2006.

[2] K. H. Rosen, C. J. Colbourn, J. H. Dinitz, etc. *Handbook of Combinatorial Designs*, CRC Press, 2007.

[3] K. H. Rosen, J. G. Michaels, J. L. Gross, etc. *Handbook of Discrete and Combinatorial Mathematics*, CRC Press, 2000.

[4] M. Hall. *Combinatorial Theory*, Blaisdell Publishing Company, 1967.

[5] H. J. Ryser. *Combinatorial Mathematics*, Mathematical Association of America, 1963.

[6] A. Shamir. *How to Share a Secret*, 1979.

[7] M. Naor, A. Shamir. *Visual Cryptography*, 1994.

[8] R. Stinson. *Visual Cryptography and Threshold Schemes*, 1998.

[9] C. Blundo, A. De Santis, etc. *On the Contrast in Visual Cryptography Schemes*, 1996.

[10] M. Bose, R. Mukerjee. *Optimal (2, n) Visual Cryptographic Schemes*, 2006.

[11] G. Ateniese, C. Blundo, etc. *Extended Schemes for Visual Cryptography*, 1996.

[12] G. Ateniese, C. Blundo, etc. *Visual Cryptography for General Access Structures*, 1996.

[13] G. Horng, T. Chen, etc. *Cheating in Visual Cryptography*, 2005.

[14] C.-M. Hu, W.-G. Tzeng. *Cheating Prevention in Visual Cryptography*, 2007.

[15] C. Blundo, A. De Santis, etc. *Visual Cryptography for Grey Level Images*, 2000.

[16] P. Tuyls, H. D. L. Hollmann, etc. *XOR-based Visual Cryptography Schemes*, 2004.

[17] E. Tressler. A Survey of the Hadamard Conjecture. *Master Thesis*, 2004.

[18] P. J. Cameron. Hadamard Matrices. *The Encyclopaedia of Design Theory*, 2006.

[19] E. F. Assmus, J. D. Key. Hadamard Matrices and Their Designs: A Coding Theoretic Approach, 1989.

[20] N. J. A. Sloane. *Library of Hadamard Matrices*, at *http://www.research.att.com/~njas/hadamard*.

[21] A. Shmitz. *A Flaw in Shamir's Secret Sharing method*, at *http://lardbucket.org/blog/archives/2007/10/30/a-flaw-in-shamirs-secret-sharing-method*.