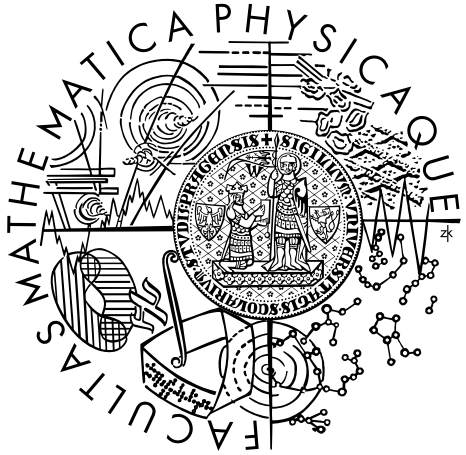
Univerzita Karlova v Praze
Matematicko-fyzikální fakulta

BAKALÁŘSKÁ PRÁCE



Marek Zpěváček

Audiovizuální kryptografie

Katedra algebry

Vedoucí bakalářské práce:	doc. RNDr. Jiří Tůma, DrSc.
Studijní program:	Matematika
Studijní obor:	Matematické metody informační bezpečnosti

Praha 2016

Děkuji Mgr. Marcelu Šebkovi za konzultace a pomoc s vypracováním této práce. Dále bych chtěl poděkovat doc. RNDr. Jiřímu Tůmovi, DrSc. za cenné připomínky během psaní práce.

Prohlašuji, že jsem tuto bakalářskou práci vypracoval samostatně a výhradně s použitím citovaných pramenů, literatury a dalších odborných zdrojů.

Beru na vědomí, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorského zákona v platném znění, zejména skutečnost, že Univerzita Karlova v Praze má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona.

V Praze dne 20. května 2016 Marek Zpěváček

Název práce: Audiovizuální kryptografie

Autor: Marek Zpěváček

Katedra: Katedra algebry

Vedoucí bakalářské práce: doc. RNDr. Jiří Tůma, DrSc., Katedra algebry

Abstrakt: Tato práce se zabývá vizuální kryptografií, kterou v roce 1995 uvedli Moni Naor a Adi Shamir. Jedná se o kryptosystém umožňující sdílet tajemství mezi více lidmi a toto tajemství rekonstruovat pouze pomocí zrakového vnímání člověka. Na začátku jsou definovány potřebné pojmy a dokázána související tvrzení. Poté popíšeme vybraná základní schémata a obecné (k, k)-schéma. Hlavní částí práce je odvození algoritmu pro vytvoření obecného (k, n)-schématu. U všech uvedených schémat dokážeme bezpečnost a korektnost rekonstrukce. Nakonec velmi stručně uvedeme i možná rozšíření.

Klíčová slova: vizuální kryptografie, sdílení tajemství

Title: Audiovisual cryptography

Author: Marek Zpěváček

Department: Departement of Algebra

Supervisor: doc. RNDr. Jiří Tůma, DrSc., Departement of Algebra

Abstract: This work examines the visual cryptography, which was introduced in 1995 by Moni Naor and Adi Shamir. It is a cryptosystem which allows us to share a secret among many users and reconstruction of secret can be done by human visual system only. Firstly, the relevant notations are defined and related theorems are proved. Additionally, some basic schemes and a general (k, k)-scheme are described. Main part of this work consists of an algorithm for creating general (k, n)-scheme. For every scheme, we prove its security and reconstruction correctness. Finally, we briefly mention a few possible extensions.

Keywords: visual cryptography, secret sharing

Obsah

Úvod

Většina dnes používané kryptografie využívá pro šifrování a dešifrování více či méně složité matematické modely a výpočty. Asymetrická kryptografie většinou reprezentuje data jako čísla a celý kryptosystém spoléhá na nějaké jednosměrné funkce (diskrétní logaritmus či rozklad na prvočísla). Dešifrování bez znalosti soukromého klíče by tak zabralo nepoměrné množství času. Také dešifrování se znalostí klíče, ale bez pomoci počítačů, by bylo prakticky nemožné. U symetrické kryptografie je situace podobná. Pro šifrování a dešifrování je sice potřeba méně výpočetního výkonu než u asymetrické kryptografie, ale kdyby měl člověk provádět matematické výpočty a operace sám na papíře, nejspíše by mu to zabralo velmi dlouhou dobu. Běžný uživatel často ani neví, co se děje na pozadí nějaké šifrované komunikace nebo při přihlašování do různých systémů. Jediné, co musí znát, je nějaké tajné heslo, a mít možnost využít počítač.

Jednou z oblastí kryptografie je problém sdílení tajemství, který může být uveden následovně: Mějme skupinu lidí, mezi které chceme rozšířit nějaké tajemství. Požadujme, aby každý účastník dostal svůj podíl (číslo, posloupnost znaků nebo třeba obrázek), a pokud se sejde nějaká oprávněná skupina účastníků, mohou pomocí svých podílů rekonstruovat tajemství. Sejde-li se však skupina, která není označená jako oprávněná, nemůže o tajemství zjistit vůbec nic. Poněkud zjednodušená verze tohoto problému je taková, že je celkem přítomno n účastníků a oprávněné skupiny jsou ty, které mají alespoň k členů. Kryptosystém řešící takovýto problém nazýváme (k, n)-schéma.

V této práci představíme kryptosystém, který řeší právě takový problém. Uživatelé tohoto kryptosystému nepotřebují k rekonstrukci tajemství žádné matematické znalosti ani počítač s jakýmkoli softwarem, rekonstrukce může probíhat pouze pomocí zrakového vnímání člověka. Tuto oblast kryptografie uvedli v roce 1995 Moni Naor a Adi Shamir (viz Naor a Shamir, 1995) a zároveň navrhli i nějaké konstrukce schémat. Na práci pak navazovalo mnoho dalších autorů nabízející efektivnější řešení nebo i různá rozšíření. Většina této práce vychází právě z tohoto článku. Naor a Shamir však přišli s velmi neefektivní konstrukcí (k, n)-schématu. Mnohem lepší řešení nabídl Stefan Droste (Droste, 1996), odkud tato práce také čerpá. Další použitou rozšiřující literaturou je (Hou, 2003) či (Socek a Magliveras, 2005).

Kapitola 1

Používaný model

1.1 Model

Každá zpráva je ve formě černobílého obrázku (může se jednat o samotný obrázek nebo o text do něj zakódovaný). Skládá se tedy z černých a bílých pixelů, což lze matematicky popsat jako matici nad tělesem $\mathbb{Z}_2$ (bílý pixel reprezentujeme jako 0 a černý jako 1). Celého kryptosystému se účastní n účastníků, každý z nich obdrží jeden obrázek, který často nelze rozeznat od náhodného šumu. Tento obrázek nazveme **podíl**.

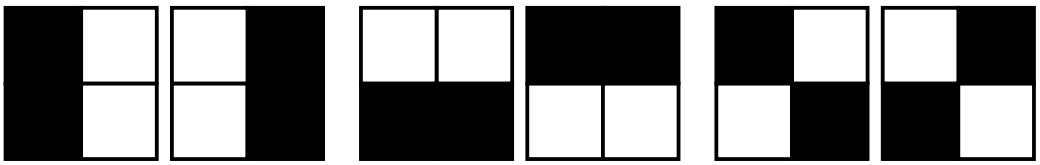
Dále definujeme tzv. **přístupovou strukturu**, která udává, jaké množiny účastníků mohou rekonstruovat původní obrázek pomocí svých podílů. Rekonstrukce probíhá pouze pomocí zrakového vnímání člověka. Musí se sejít předem definovaná skupina účastníků, která je oprávněná rekonstruovat. Tato skupina vytiskne své podíly například na průhlednou fólii, všechny je na sebe pečlivě poskládá a podívá se přes ně proti světlu nebo je položí na podsvícenou podložku.

Každý pixel obrázku se zpracovává (distribuce a rekonstrukce) zvlášť. V celém textu se tedy budeme zabývat zpracováním pouze jednoho pixelu, který bude rozdělen na m menších pixelů nazývaných **subpixely**. Nechť N značí počet pixelů v původním obrázku. Každý podíl účastníka bude tedy obsahovat $m \cdot N$ subpixelů. Díky malé rozlišovací schopnosti lidského oka vnímá mozek m-tice subpixelů jako jeden pixel v různých odstínech šedi.

Každou m-tici černých nebo bílých subpixelů (tj. jeden pixel z podílu jednoho účastníka) lze reprezentovat jako řádkový vektor délky m nad tělesem $\mathbb{Z}_2$. Celkově tak pro n-tici účastníků dostaneme $n \times m$ matici, která popisuje subpixely všech účastníků. V praxi mohou m-tice subpixelů tvořit čtvercové schéma, aby se nezměnil poměr stran výsledného obrázku. Například pro $m = 4$ lze vytvořit 2×2 čtvercový blok.

Rekonstrukce probíhá tak, že se na sebe složí jednotlivé podíly (viz výše). Pokud je alespoň jeden ze subpixelů černý, výsledný rekonstruovaný subpixel bude také černý (světlo neprosvítí žádný černý subpixel). To odpovídá operaci **OR**. Celkově lidské oko vnímá m-tici rekonstruovaných subpixelů jako jeden výsledný pixel v nějakém odstínu šedi. Stupeň šedi pak závisí na počtu černých subpixelů. Pokud je počet černých subpixelů v m-tici vetší než d, lidské oko to bude vnímat jako černý pixel (nebo jako nějaký tmavší odstín šedi). Pokud je tento počet menší než $d - \alpha \cdot m$, oko rozpozná pixel jako bílý (světle šedý). Hodnota α pak určuje, jaký bude kontrast výsledného obrázku.

Jako příklad si uvedeme ten nejjednodušší: $(2,2)$-schéma, tedy v celém kryptosystému jsou dva účastníci a mohou rekonstruovat pouze společně. Každý pixel bude rozdělen na 4 subpixely ($m = 4$), které budou uspořádány do 2×2 čtvercového bloku. Celkem máme šest variant, jak můžou jednotlivé pixely v podílech vypadat. Těchto šest variant je rozděleno do tří skupin po dvou pixelech (viz obrázek 1.1). Chce-li distributor distribuovat bílý pixel, náhodně vybere jeden ze šesti pixelů a oběma účastníkům sdělí ten samý. Složením těchto dvou pixelů dostanou ten samý pixel, vždy s dvěma černými subpixely. Pro distribuci černého pixelu distributor nejprve náhodně vybere jednu skupinu pixelů a poté prvnímu účastníkovi sdělí náhodně vybraný pixel z této skupiny a druhému ten druhý. Složením těchto dvou pixelů dostanou zcela černý pixel. Nyní nahlédněme, co lze zjistit z jednoho podílu o původním obrázku. Byl-li původní pixel bílý, pak se v jednotlivých podílech bude vyskytovat jeden ze šesti možných pixelů, každý se stejnou pravděpodobností. Úplně stejně tomu bude i v případě, že původní pixel byl černý. Z jednoho podílu tedy nelze zjistit nic o původním obrázku.



Obrázek 1.1: Vertikální, horizontální a diagonální skupina

1.2 Základní definice a tvrzení

Definice 1 (přístupová struktura)**.** *Nechť $\mathcal{P}$ je množina všech účastníků.* Přístupovou strukturou Γ na množině $\mathcal{P}$ *nazýváme libovolnou podmnožinu $\Gamma \subseteq 2^{\mathcal{P}} \setminus \{\emptyset\}$, pro kterou platí: $\forall A \in \Gamma$ a $\forall A'$ takové, že $A \subseteq A' \subseteq \mathcal{P}$, platí $A' \in \Gamma$.*

Dále předpokládejme $\mathcal{P} = \{1, \ldots, n\}, k \leq n$ a všechny k-tice mohou rekonstruovat tajemství. Dostáváme následující přístupovou strukturu:

$$\Gamma = \{A \subseteq \mathcal{P} \colon\ |A| \geq k\}\,.$$

Definice 2 (OR operace)**.** *Binární operaci* OR *nad tělesem $\mathbb{Z}_2$ definujeme následující tabulkou:*

a	b	$OR(a,b)$
0	0	0
1	0	1
0	1	1
1	1	1

n-ární OR definujeme induktivně:

$$OR(v_1, v_2, \ldots, v_n) = OR(v_1, v_2, \ldots, v_{n-2}, OR(v_{n-1}, v_n)).$$

Pro vektory stejné délky definujeme tuto operaci po složkách.

Operaci OR aplikovanou na dva či více vektorů (řádků matice) budeme také nazývat skládáním *vektorů (řádků matice).*

Definice 3 (Hammingova váha)**.** *Nechť* $V = (v_1, \ldots, v_n) \in \mathbb{Z}_2^n$. Hammingovou vahou vektoru V *myslíme hodnotu* $H(V) = |\{i \colon v_i = 1\}|$.

Definice 4. *Nechť* C *je matice typu* $n \times m$ *a nechť* $I = \{i_1, \ldots, i_k\} \subseteq \{1, \ldots, n\}$*, pak symbolem* $R_I(C)$ *myslíme matici, která vznikne vyškrtáním řádků* $\{1, \ldots, n\} \setminus \{i_1, \ldots, i_k\}$ *z matice* C*. Takové vyškrtávání řádků také budeme nazývat* restrikcí matice C na řádky $i_1, \ldots, i_k$.

Definice 5 (Pravděpodobnostní rozdělení na množině)**.** *Nechť* $\mathcal{C}$ *je konečná neprázdná množina. Zobrazení* $p \colon \mathcal{C} \to [0, 1]$ *nazveme* pravděpodobnostním rozdělením na množině $\mathcal{C}$*, pokud platí:*

$$\sum_{C \in \mathcal{C}} p(C) = 1.$$

Definice 6 (Uniformní rozdělení)**.** *Pravděpodobnostní rozdělení* p *na množině* $\mathcal{C}$ *nazveme* uniformní *(nebo též rovnoměrné) pokud:*

$$\forall C \in \mathcal{C} \colon p(C) = \frac{1}{|\mathcal{C}|}.$$

Uvažujme nyní $\mathcal{C}$ jako množinu $n \times m$ matic spolu s pravděpodobnostním rozdělením p na $\mathcal{C}$. Mějme $q < n, i_1, \ldots, i_q \in \mathbb{N}, 1 \leq i_1 < i_2 < \cdots < i_q \leq n$, $I = \{i_1, \ldots, i_q\}$. Vyškrtáním řádků $\{1, \ldots, n\} \setminus \{i_1, \ldots, i_q\}$ ze všech matic z $\mathcal{C}$ dostaneme novou množinu $q \times m$ matic $\mathcal{D}$ a příslušné pravděpodobnostní rozdělení p' na $\mathcal{D}$ definované takto:

$$\forall D \in \mathcal{D} \colon p'(D) = \sum_{C \colon R_I(C) = D} p(C).$$

Definice 7 (Vizuální (k, n)-schéma)**.** *Nechť* $k, n, m, d \in \mathbb{N}, k \leq n, \alpha \in \mathbb{R}, \alpha > 0$. Vizuálním (k, n)-schématem *myslíme dvě množiny* $n \times m$ *matic* $\mathcal{C}_0$ *a* $\mathcal{C}_1$ *nad tělesem* $\mathbb{Z}_2$ *spolu s pravděpodobnostními rozděleními* p_0 *a* p_1 *na* $\mathcal{C}_0$ *respektive* $\mathcal{C}_1$*, které splňují následující podmínky:*

1. *Vezmeme-li z libovolné matice* $C \in \mathcal{C}_0$ *libovolných* k *řádků, pak pro výsledek* V *operace OR těchto řádků platí* $H(V) \leq d - \alpha \cdot m$.
2. *Vezmeme-li z libovolné matice* $C \in \mathcal{C}_1$ *libovolných různých* k *řádků, pak pro výsledek* V *operace OR těchto řádků platí* $H(V) \geq d$.

Platnost těchto podmínek budeme také nazývat jako korektnost rekonstrukce*. Hodnotu* α *budeme nazývat* relativním kontrastem *a hodnotu* d prahovou hodnotou*. Jeden řádek matice z* $\mathcal{C}_0$ *nebo z* $\mathcal{C}_1$ *budeme nazývat* podíl.

Dále (k, n)-schématem budeme vždy myslet vizuální (k, n)-schéma.

Pro distribuci bílého respektive černého pixelu distributor pomocí pravděpodobnostního rozdělení p_0 respektive p_1 vybere matici z $\mathcal{C}_0$ respektive $\mathcal{C}_1$ a i-tému účastníkovi sdělí i-tý řádek.

Podmínky v definici zaručují korektnost rekonstrukce tajné zprávy. Říkají nám, že lze rozlišit bílý a černý pixel v rekonstruovaném obrázku. Také určují kontrast. Čím větší je hodnota α, tím větší kontrast výsledného obrázku získáme.

Lemma 1. *Hodnotu α v definici (k,n)-schématu stačí uvažovat pouze z množiny $\{1/m, 2/m, \ldots, d/m\}$.*

Důkaz. V potaz je nutno brát pouze podmínku 1 v definici (jinde se hodnota α nevyskytuje). Jelikož v nerovnosti $H(V) \leq d - \alpha \cdot m$ nabývá jak d, tak i Hammingova váha pouze celočíselných hodnot, stačí hodnotu $\alpha \cdot m$ uvažovat také celočíselnou. Pro dolní odhad $\alpha \cdot m$ dostáváme: $\alpha \cdot m \geq 1$, jelikož $\alpha > 0$ z definice a $m \in \mathbb{N}$. Horní odhad je $\alpha \cdot m \leq d$, jelikož Hammingova váha nabývá pouze nezáporných hodnot. Kombinací odhadů pro $\alpha \cdot m$ dostáváme požadované tvrzení. □

Definice 8. *Mějme libovolné (k,n)-schéma a nechť $q \in \mathbb{N}, q < k, i_1, \ldots, i_q \in \mathbb{N}, 1 \leq i_1 < i_2 < \cdots < i_q \leq n$. Jestliže pro dvě množiny $q \times m$ matic $\mathcal{D}_0$ a $\mathcal{D}_1$ vzniklé restrikcí matic z $\mathcal{C}_0$ respektive z $\mathcal{C}_1$ na řádky $i_1, \ldots, i_q$ a pro jejich příslušná pravděpodobnostní rozdělení p'_0 a p'_1 platí: $\mathcal{D}_0 = \mathcal{D}_1$ a $p'_0 = p'_1$, pak říkáme, že je toto schéma bezpečné.*

Tato definice nám říká, že z méně než k podílů nelze zjistit nic o původním obrázku.

Lemma 2. *Platí-li podmínka v předchozí definici pro $q = k - 1$, pak je toto schéma bezpečné (tj. podmínka platí pro všechna $q < k$).*

Důkaz. Mějme libovolné $q \in \mathbb{N}, q < k, i_1, \ldots, i_q$ po dvou různá. Potom existuje $(k-1)$-prvková nadmnožina $\{i_1, \ldots, i_q\} \subseteq \{i_1, \ldots, i_{k-1}\}$, pro kterou z předpokladu platí: Dvě množiny $(k-1) \times m$ matic $\mathcal{D}_0$ a $\mathcal{D}_1$ vzniklé restrikcí matic z $\mathcal{C}_0$ respektive z $\mathcal{C}_1$ na řádky $i_1, \ldots, i_{k-1}$ se rovnají a příslušná pravděpodobnostní rozdělení p'_0 a p'_1 na těchto množinách se také rovnají. Vyškrtáním řádků $\{i_1, \ldots, i_{k-1}\} \setminus \{i_1, \ldots, i_q\}$ v maticích z $\mathcal{D}_0$ a z $\mathcal{D}_1$ opět dostaneme stejné množiny matic a stejná pravděpodobnostní rozdělení. □

Definice 9. *Nechť C je matice typu $n \times m$ a nechť $\pi \in S_m$. Pak $\pi(C)$ značí matici, která vznikne permutací sloupců matice C pomocí permutace π. Neboli $\pi(C)[i, \pi(j)] = C[i,j]$, $i = 1, \ldots, n$ a $j = 1, \ldots, m$.*

Definice 10. *Dvě $n \times m$ matice C_0 a C_1 nazveme* bázovými maticemi *(k,n)-schématu, pokud množiny matic $\mathcal{C}_0$ a $\mathcal{C}_1$ definující toto (k,n)-schéma vzniknou následovně:*

$$\mathcal{C}_0 = \{\sigma(C_0) \colon \sigma \in S_m\},$$
$$\mathcal{C}_1 = \{\sigma(C_1) \colon \sigma \in S_m\}$$

a příslušná pravděpodobnostní rozdělení p_0 a p_1 jsou uniformní.

Lemma 3. *Nechť C_0 a C_1 jsou bázové matice nějakého (k,n)-schématu. Potom pro $i \in \{0,1\}$ a každou matici $C \in \mathcal{C}_i$ platí:*

$$p_i(C) = \frac{1}{|\mathcal{C}_i|} = \frac{|\{\sigma \in S_m \colon \sigma(C_i) = C\}|}{m!}.$$

Důkaz. Fixujme $i \in \{0,1\}$ a mějme matici $C \in \mathcal{C}_i$ libovolnou. První rovnost je definice uniformního rozdělení. K důkazu druhé rovnosti si rozepišme matici C_i pomocí sloupcových vektorů: $C_i = (v_1|\ldots|v_m)$. Označme $M = \{1,\ldots,m\}$ a na M zaveďme relaci $\sim$: $a \sim b \Leftrightarrow v_a = v_b$. Snadno ověříme, že $\sim$ je ekvivalence. Dostáváme tedy rozklad na třídy ekvivalence $M/\sim$. Nechť $E \in \mathcal{C}_i$ je libovolná. Pak dostáváme:

$$|\{\sigma \in S_m \colon \sigma(C_i) = E\}| = \prod_{X \in M/\sim} |X|!.$$

Tato hodnota nezávisí na E, můžeme tedy označit

$$|\{\sigma \in S_m \colon \sigma(C_i) = E\}| = T.$$

Snadno nahlédneme, že

$$S_m = \{\sigma \in S_m \colon \sigma(C_i) \in \mathcal{C}_i\} = \dot{\bigcup_{E \in \mathcal{C}_i}} \{\sigma \in S_m \colon \sigma(C_i) = E\}\,.$$

A tedy

$$m! = |\{\sigma \in S_m \colon \sigma(C_i) \in \mathcal{C}_i\}| = \sum_{E \in \mathcal{C}_i} |\{\sigma \in S_m \colon \sigma(C_i) = E\}| = \sum_{E \in \mathcal{C}_i} T = T \cdot |\mathcal{C}_i|\,.$$

Jelikož $E \in \mathcal{C}_i$ byla libovolná, dostáváme

$$m! = |\{\sigma \in S_m \colon \sigma(C_i) = C\}| \cdot |\mathcal{C}_i|\,.$$

□

Tvrzení 4. *Mějme bázové matice C_0 a C_1 definující nějaké (k,n)-schéma. Pak následující tvrzení jsou ekvivalentní:*

(1) Schéma je bezpečné.

(2) Matice D_0 a D_1 vzniklé restrikcí matic C_0 respektive C_1 na libovolných (v obou případech stejných) $k-1$ řádků se liší pouze v pořadí sloupců. Neboli existuje permutace π taková, že $D_1 = \pi(D_0)$.

Důkaz. (1) $\Longrightarrow$ (2): Mějme libovolnou $k-1$ prvkovou podmnožinu $I = \{i_1,\ldots,i_{k-1}\} \subseteq \{1,\ldots,n\}$. Z předpokladu bezpečnosti máme: Dvě množiny $(k-1) \times m$ matic $\mathcal{D}_0$ a $\mathcal{D}_1$ vzniklé restrikcí matic z $\mathcal{C}_0$ a z $\mathcal{C}_1$ na řádky $i_1,\ldots,i_{k-1}$ se rovnají. Neboli:

$$\mathcal{D}_0 = \{R_I(C) \colon C \in \mathcal{C}_0\} = \{R_I(C) \colon C \in \mathcal{C}_1\} = \mathcal{D}_1,$$

což lze přepsat jako:

$$\{R_I(\sigma(C_0)) \colon \sigma \in S_m\} = \{R_I(\sigma(C_1)) \colon \sigma \in S_m\}\,.$$

Jelikož $R_I(C_1) \in \{R_I(\sigma(C_1)) \colon \sigma \in S_m\}$ (pro σ identickou permutaci), dostáváme, že $R_I(C_1) \in \{R_I(\sigma(C_0)) \colon \sigma \in S_m\}$. Tedy existuje permutace $\pi \in S_m$ taková, že: $R_I(C_1) = R_I(\pi(C_0))$, neboli $D_1 = \pi(D_0)$.

(2) $\implies$ (1): Dle lemmatu 2 stačí podmínku bezpečnosti ověřit pouze pro $q = k-1$. Mějme tedy libovolnou $k-1$ prvkovou podmnožinu $I = \{i_1, \ldots, i_{k-1}\} \subseteq \{1, \ldots, n\}$. Bez újmy na obecnosti můžeme předpokládat, že $\{i_1, \ldots, i_{k-1}\} = \{1, \ldots, k-1\}$. Pak lze psát $C_0 = \left(\frac{D}{A_0}\right)$ a $C_1 = \left(\frac{\pi(D)}{A_1}\right)$ pro nějaké matice A_0 a A_1 typu $(n-(k-1) \times m)$ a nějakou permutaci $\pi \in S_m$.

Nyní dokážeme, že se množiny matic $\mathcal{D}_0$ a $\mathcal{D}_1$ vzniklé restrikcí matic z množin $\mathcal{C}_0$ a $\mathcal{C}_1$ na řádky $i_1, \ldots, i_{k-1}$ rovnají.

$$\begin{aligned}
\mathcal{D}_0 &= \{R_I(C)\colon C \in \mathcal{C}_0\} = \{R_I(\sigma(C_0))\colon \sigma \in S_m\} = \left\{R_I(\sigma(\left(\frac{D}{A_0}\right)))\colon \sigma \in S_m\right\} = \\
&= \{\sigma(D)\colon \sigma \in S_m\} = \{\sigma(\pi(D))\colon \sigma \in S_m\} = \left\{R_I(\sigma(\left(\frac{\pi(D)}{A_1}\right)))\colon \sigma \in S_m\right\} = \\
&= \{R_I(\sigma(C_1))\colon \sigma \in S_m\} = \{R_I(C)\colon C \in \mathcal{C}_1\} = \mathcal{D}_1
\end{aligned}$$

Zbývá dokázat, že se rovnají i příslušná pravděpodobnostní rozdělení p'_0 a p'_1 na $\mathcal{D}_0 = \mathcal{D}_1$. Nechť $E \in \mathcal{D}_0$.

$$\begin{aligned}
p'_0(E) &= \sum_{C \in \mathcal{C}_0\colon R_I(C)=E} p_0(C) \overset{\text{lemma 3}}{=} \\
&= \frac{\sum_{C \in \mathcal{C}_0\colon R_I(C)=E} |\{\sigma \in S_m\colon \sigma(C_0) = C\}|}{m!} = \\
&= \frac{|\{\sigma \in S_m\colon R_I(\sigma(C_0)) = E\}|}{m!} = \\
&= \frac{\left|\left\{\sigma \in S_m\colon R_I(\sigma(\left(\frac{D}{A_0}\right))) = E\right\}\right|}{m!} = \\
&= \frac{|\{\sigma \in S_m\colon \sigma(D) = E\}|}{m!} = \\
&= \frac{|\{\sigma \in S_m\colon \sigma(\pi(D)) = E\}|}{m!} = \\
&= \frac{\left|\left\{\sigma \in S_m\colon R_I(\sigma(\left(\frac{\pi(D)}{A_1}\right))) = E\right\}\right|}{m!} = \\
&= \frac{|\{\sigma \in S_m\colon R_I(\sigma(C_1)) = E\}|}{m!} = \\
&= \frac{\sum_{C \in \mathcal{C}_1\colon R_I(C)=E} |\{\sigma \in S_m\colon \sigma(C_1) = C\}|}{m!} \overset{\text{lemma 3}}{=} \\
&= \sum_{C \in \mathcal{C}_1\colon R_I(C)=E} p_1(C) = \\
&= p'_1(E)
\end{aligned}$$

□

Kapitola 2

Vybrané konstrukce

Po celou kapitolu předpokládejme, že pravděpodobnostní rozdělení p_0 a p_1 jsou uniformní. Nebudeme je tedy psát vůbec a každá matice bude mít stejnou pravděpodobnost výskytu, tj. $1/|\mathcal{C}_0|$ respektive $1/|\mathcal{C}_1|$.

2.1 $(2,2)$-schéma

$(2,2)$-schéma jsme popsali již v úvodu, zde pro něj doplníme množiny $\mathcal{C}_0$ a $\mathcal{C}_1$:

$$\mathcal{C}_0 = \left\{ \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 \end{pmatrix}, \right.$$
$$\left. \begin{pmatrix} 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \end{pmatrix} \right\},$$

$$\mathcal{C}_1 = \left\{ \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}, \right.$$
$$\left. \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix} \right\}.$$

Snadno nahlédneme, že parametry schématu jsou: $m = 4, d = 4, \alpha = 2/m = 2/4$.

$(2,2)$-schéma lze vytvořit i pro dva subpixely na originální pixel ($m = 2$) a to následovně:

$$\mathcal{C}_0 = \left\{ \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} \right\},$$

$$\mathcal{C}_1 = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\}.$$

Jedná se o speciální případ obecného $(2,n)$-schématu. Opět snadno vidíme, že parametry schématu jsou: $m = 2, d = 2, \alpha = 1/m = 1/2$.

2.2 Obecné $(2, n)$-schéma

Nechť C_0 a C_1 jsou matice typu $n \times n$:

$$C_0 = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 1 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 0 & \cdots & 0 \end{pmatrix}, C_1 = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}.$$

$(2, n)$-schéma pak vytvoříme následovně:

$$\mathcal{C}_0 = \{\sigma(C_0) \colon \sigma \in S_m\},$$
$$\mathcal{C}_1 = \{\sigma(C_1) \colon \sigma \in S_m\}.$$

Každý řádek matice jak z $\mathcal{C}_0$ tak i z $\mathcal{C}_1$ obsahuje právě jeden černý subpixel. Tedy pouze z jednoho podílu nelze určit, zda se původně jednalo o bílý či černý pixel. Nyní ještě spočtěme pravděpodobnost, že bude i-tý subpixel v daném podílu černý. Pro matice z $\mathcal{C}_0$ snadno nahlédneme, že je to $1/n$. Jelikož jsou matice z $\mathcal{C}_1$ permutací sloupců identické matice, je tato pravděpodobnost také $1/n$. Toto schéma je tedy bezpečné.

Provedeme-li operaci OR na libovolné dva řádky matice z $\mathcal{C}_0$, dostaneme řádek s Hammingovou vahou 1. Provedeme-li ale tuto operaci na dva různé řádky matice z $\mathcal{C}_1$, dostaneme řádek s Hammingovou vahou 2. Parametry schématu tedy jsou: $m = n$, $d = 2$ a $\alpha = 1/m$. Dostaneme tak velmi málo kontrastní obrázek.

2.3 Obecné $(3, n)$-schéma

Nechť A, B, I jsou matice nad tělesem $\mathbb{Z}_2$. A je typu $n \times (n-2)$ obsahující samé jedničky, B je typu $n \times (2n-2)$ obsahující také samé jedničky a I je identická $n \times n$ matice.

Definujme bázové matice $C_1 = (A|I)$ a $C_0 = B - C_1$. $(3, n)$-schéma pak vytvoříme následovně:

$$\mathcal{C}_0 = \{\sigma(C_0) \colon \sigma \in S_m\},$$
$$\mathcal{C}_1 = \{\sigma(C_1) \colon \sigma \in S_m\}.$$

Tvrzení 5. *Parametry výše popsaného schématu jsou:* $m = 2n-2, d = n+1, \alpha = 1/m$. *A toto schéma je bezpečné.*

Důkaz. Složíme-li 3 řádky z matice z $\mathcal{C}_0$, výsledkem bude řádek s vahou n, ale když vybereme matici z $\mathcal{C}_1$, vyjde nám řádek s vahou $n+1$. Tedy $d = n+1$ a $\alpha = 1/m$.

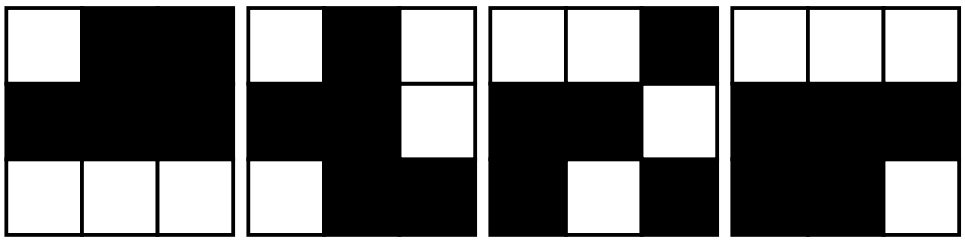
Matice D_1 vzniklá restrikcí matice C_1 na libovolné dva řádky obsahuje $(n-2)$-krát sloupec $\binom{1}{1}$, dále $(n-2)$-krát sloupec $\binom{0}{0}$, jednou sloupec $\binom{1}{0}$ a jednou sloupec $\binom{0}{1}$. Snadno nahlédneme, že matice D_0 vzniklá restrikcí matice C_0 na dva řádky (stejné jako v případě matice D_1) obsahuje ty samé sloupce. Tedy existuje permutace π taková, že $D_1 = \pi(D_0)$ a dle tvrzení 4 je toto schéma bezpečné. □

2.4 $(4,4)$-schéma

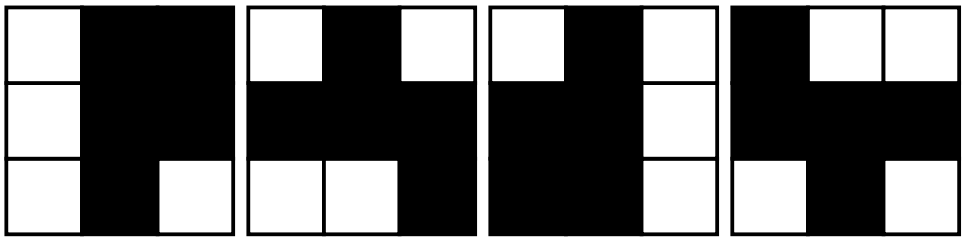
Bázové matice pro $(4,4)$-schéma mohou být zkonstruovány pomocí podílů v obrázku 2.1, neboli:

$$C_0 = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \end{pmatrix}, C_1 = \begin{pmatrix} 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 \end{pmatrix}.$$

Vidíme, že každý pixel je rozdělen na 9 subpixelů ($m = 9$) a uspořádán do 3×3 bloku, ale jelikož je prostřední subpixel vždy černý, lze ho úplně vynechat. Každý podíl obsahuje přesně 5 černých subpixelů, každá složená dvojice podílů obsahuje 7 černých subpixelů a každá složená trojice obsahuje 8 černých subpixelů, to vše nehledě na to, jestli jsme vybírali z černých či bílých. Zatímco pokud složíme všechny bílé podíly, dostaneme pixel s osmi černými subpixely, a pokud složíme všechny černé, dostaneme kompletně černý pixel. Parametry schématu jsou: $m = 9, d = 9, \alpha = 1/9$. Bezpečnost schématu plyne z tvrzení 4.



(a) Podíly bílého pixelu



(b) Podíly černého pixelu

Obrázek 2.1: $(4,4)$-schéma

Kapitola 3

Obecné konstrukce

3.1 Obecné (k, k)-schéma

Ke konstrukci obecného (k, k)-schématu uvažme libovolnou k-prvkovou množinu $W = \{w_1, \ldots, w_k\}$. Nechť $A_1, A_2, \ldots, A_{2^{k-1}}$ jsou všechny podmnožiny systému 2^W sudé velikosti a nechť $B_1, B_2, \ldots, B_{2^{k-1}}$ jsou všechny podmnožiny systému 2^W liché velikosti. Definujme matici C_0 typu $k \times 2^{k-1}$ nad tělesem $\mathbb{Z}_2$ následovně:

$$C_0[i, j] = 1 \Leftrightarrow w_i \in A_j,$$
$$C_0[i, j] = 0 \Leftrightarrow w_i \notin A_j$$

a obdobně $k \times 2^{k-1}$ matici C_1

$$C_1[i, j] = 1 \Leftrightarrow w_i \in B_j,$$
$$C_1[i, j] = 0 \Leftrightarrow w_i \notin B_j.$$

Nechť jsou nyní C_0 a C_1 bázové matice (viz definice 10), neboli:

$$\mathcal{C}_0 = \{\sigma(C_0) \colon \sigma \in S_m\},$$
$$\mathcal{C}_1 = \{\sigma(C_1) \colon \sigma \in S_m\}$$

a příslušná pravděpodobnostní rozdělení p_0 a p_1 na $\mathcal{C}_0$ respektive $\mathcal{C}_1$ jsou uniformní.

Pozorování 6. *Matice C_0 obsahuje všechny možné sloupce se sudým počtem jedniček a matice C_1 obsahuje všechny možné sloupce s lichým počtem jedniček.*

Pozorování 7. *Mějme prvek $w_i \in W$. Nechť D_0 respektive D_1 je matice, která vznikne z matice C_0 respektive C_1 vyškrtnutím i-tého řádku. Pak matici D_0 respektive D_1 lze zkonstruovat stejně jako matici C_0 respektive C_1 s tím rozdílem, že místo množin A_j a B_j použijeme množiny $A_j \backslash \{w_i\}$ a $B_j \backslash \{w_i\}$, $j \in \{1, \ldots, 2^{k-1}\}$.*

Pozorování 8. *Mějme prvek $w_i \in W$. Pak existuje právě 2^{k-2} (přesně polovina) množin z $A_1, \ldots, A_{2^{k-1}}$, respektive z $B_1, \ldots, B_{2^{k-1}}$ obsahující prvek w_i.*

Tvrzení 9. *Výše popsané schéma je bezpečné (k, k)-schéma s parametry: $m = 2^{k-1}, \alpha = 1/m$, $d = m = 2^{k-1}$.*

Důkaz. Nejprve dokážeme korektnost rekonstrukce. V matici C_0 je právě jeden sloupec celý nulový (ten, který je indexovaný prázdnou množinou). Ostatní tedy obsahují alespoň jednu 1. Složením všech řádků dostaneme sloupec s vahou $2^{k-1} - 1$. V matici C_1 není žádný sloupec celý nulový. Složením všech řádků tak dostaneme řádek s vahou 2^{k-1}. Tedy $d = 2^{k-1}, \alpha = 1/2^{k-1} = 1/m$.

K důkazu bezpečnosti využijeme tvrzení 4. Nechť $i \in \{1, \ldots, k\}$ a uvažujme matice D_0 a D_1 vzniklé z matic C_0 respektive C_1 vyškrtnutím i-tého řádku. Definujme množiny:

$$\begin{aligned}
\mathcal{A}_1 &= \{A_j \colon A_j \text{ neobsahuje prvek } w_i\}, \\
\mathcal{A}_2 &= \{A_j \setminus \{w_i\} : A_j \text{ obsahuje prvek } w_i\}, \\
\mathcal{B}_1 &= \{B_j \colon B_j \text{ neobsahuje prvek } w_i\}, \\
\mathcal{B}_2 &= \{B_j \setminus \{w_i\} : B_j \text{ obsahuje prvek } w_i\}.
\end{aligned}$$

Snadno nahlédneme, že množiny z $\mathcal{A}_1$ a z $\mathcal{B}_2$ mají sudý počet prvků, zatímco množiny z $\mathcal{A}_2$ a z $\mathcal{B}_1$ mají lichý počet prvků. Navíc z pozorovaní 8 vidíme, že množiny $\mathcal{A}_1$ a $\mathcal{A}_2$ mají 2^{k-2} prvků, jsou disjunktní a dohromady tvoří systém všech podmnožin množiny $W' = \{w_1, \ldots, w_k\} \setminus \{w_i\}$. Obdobně nahlédneme, že množiny $\mathcal{B}_1$ a $\mathcal{B}_2$ jsou disjunktní a společně také tvoří systém všech podmnožin množiny W'. Dohromady tedy máme $\mathcal{A}_1 = \mathcal{B}_2$ a $\mathcal{A}_2 = \mathcal{B}_1$, neboli existuje permutace π taková, že $B_j \setminus \{w_i\} = A_{\pi(j)} \setminus \{w_i\}$ pro $j = 1, \ldots, 2^{k-1}$. Z pozorování 7 dostáváme, že $D_1 = \pi(D_0)$, a tedy dle tvrzení 4 je toto schéma bezpečné.

□

3.2 Obecné (k, n)-schéma

Do této části práce jsme vycházeli z (Naor a Shamir, 1995). Nyní svou pozornost přesuneme k (Droste, 1996).

Obecné (k, n)-schéma se odvíjí od obecného (k, k)-schématu. K jeho konstrukci nám poslouží několik lemmat.

Lemma 10. *Nechť C_0 a C_1 jsou bázové matice typu $k \times m$ definující nějaké bezpečné (k, k)-schéma s relativním kontrastem α a prahovou hodnotou d. Nechť matice A je libovolná typu $k \times l$. Pak matice $(C_0|A)$ a $(C_1|A)$ jsou bázové matice bezpečného (k, k)-schématu s relativním kontrastem $\alpha' = \alpha \cdot m/(m+l)$ a prahovou hodnotou $d' = d + d_A$, kde d_A je Hammingova váha řádku, který vznikne jako složení všech řádků matice A.*

Důkaz. Nejdříve ověříme korektnost rekonstrukce. Snadno si rozmyslíme, že podmínky 1 a 2 stačí ověřit pouze pro matice C_0 a C_1 (permutace sloupců nemají na Hammingovu váhu vliv). Řádek (vektor) vzniklý složením všech řádků matice C_0 respektive C_1 označme c_0 respektive c_1. Přidáním matice A jsme tedy zvýšili váhu řádku c_0 respektive c_1 o d_A. K ověření podmínky 1 potřebujeme dokázat, že $H(c_0) + d_A \leq d' - \alpha' \cdot (m + l)$, neboli $H(c_0) \leq d - \alpha' \cdot (m + l)$, což po dosazení za α' dává: $H(c_0) \leq d - \alpha \cdot m$. Tato nerovnost platí, jelikož původní schéma má korektní rekonstrukci. Snadno ověříme, že pro d' platí nerovnost v podmínce 2.

Jelikož matice C_0 a C_1 definují bezpečné schéma a přidali jsme k nim stejnou matici A, je dle tvrzení 4 toto schéma bezpečné.

□

Lemma 11. *Mějme $\alpha \in \mathbb{R}, \alpha > 0, d \in \mathbb{N}$. Nechť C_0 a C_1 jsou $n \times m$ matice, pro které platí: Matice D_0 a D_1 vzniklé restrikcí matic C_0 respektive C_1 na libovolných (v obou případech stejných) k řádků jsou bázové matice bezpečného (k,k)-schématu s parametry α a d. Pak matice C_0 a C_1 jsou bázovými maticemi bezpečného (k,n)-schématu s relativním kontrastem α.*

Důkaz. Nejdříve ověříme korektnost rekonstrukce. Obdobně jako v předchozím důkazu stačí podmínky 1 a 2 ověřit pouze pro matice C_0 a C_1. Mějme libovolný výběr k řádků $\{i_1, \ldots, i_k\}$. Pak dle předpokladu platí, že matice D_0 a D_1 vzniklé restrikcí matic C_0 respektive C_1 na řádky $i_1, \ldots, i_k$ jsou bázové matice (k,k)-schématu s parametry α a d, neboli pro ně platí podmínky 1 a 2. Jelikož jsou parametry α a d vždy stejné, dostáváme korektnost rekonstrukce i pro schéma vytvořené maticemi C_0 a C_1.

K důkazu bezpečnosti využijeme tvrzení 4. Mějme libovolnou $k-1$ prvkovou podmnožinu $\{i_1, \ldots, i_{k-1}\} \subseteq \{1, \ldots, n\}$. Potom existuje k-prvková nadmnožina $\{i_1, \ldots, i_{k-1}\} \subseteq \{i_1, \ldots, i_k\}$, pro kterou z předpokladu platí, že matice D'_0 a D'_1 vzniklé restrikcí matic C_0 respektive C_1 na řádky $i_1, \ldots, i_k$ jsou bázové matice bezpečného (k,k)-schématu. Jelikož je toto (k,k)-schéma bezpečné, dostáváme: Matice D_0 a D_1 vzniklé restrikcí matic D'_0 respektive D'_1 na řádky $i_1, \ldots, i_{k-1}$ se liší pouze v pořadí sloupců. Neboli i matice D_0 a D_1 vzniklé restrikcí matic C_0 respektive C_1 na řádky $i_1, \ldots, i_{k-1}$ se liší pouze v pořadí sloupců. Dle tvrzení 4 dostáváme, že matice C_0 a C_1 jsou bázovými maticemi bezpečného (k,n)-schématu.
□

Tvrzení 12. *Nechť C_0 a C_1 jsou $n \times (2^{k-1}+l)$ matice a $v_1, \ldots, v_l$ sloupcové vektory délky k. Nechť platí následující: Matice D_0 respektive D_1 vzniklé restrikcí matic C_0 respektive C_1 na libovolných (v obou případech stejných) k řádků vždy obsahují všechny sloupce se sudým respektive lichým počtem jedniček a navíc všechny sloupce $v_1, \ldots, v_l$. Potom jsou matice C_0 a C_1 bázovými maticemi bezpečného (k,n)-schématu s relativním kontrastem $1/(2^{k-1}+l)$.*

Důkaz. Bez újmy na obecnosti můžeme předpokládat, že sloupce $v_1, \ldots, v_l$ v maticích D_0/D_1 jsou vždy na pozicích $2^{k-1}+1, \ldots, 2^{k-1}+l$ (tedy vektor v_i je na pozici $i+2^{k-1}$). Tvrzení 9 a lemma 10 (pro $A = (v_1|\ldots|v_l)$) nám říkají, že matice D_0 a D_1 jsou bázové matice (k,k)-schématu s relativním kontrastem $1/(2^{k-1}+l)$ a $d = 2^{k-1} + d_A$, kde d_A je Hammingova váha řádku, který vznikne jako složení všech řádků matice $(v_1|\ldots|v_l)$. Z lemmatu 11 pak už plyne požadované tvrzení.
□

Lemma 13. *Nechť $1 \leq q \leq n$ a nechť M je matice typu $n \times \binom{n}{q}$, která obsahuje všechny možné sloupce obsahující q jedniček. Pak každá matice vzniklá restrikcí matice M na k ($k \leq n$) řádků obsahuje všechny možné sloupce s p jedničkami, každý právě $\binom{n-k}{q-p}$-krát, pro všechna $p \in \{max(0, q-(n-k)), \ldots, min(q,k)\}$.*

Důkaz. Jelikož matice M obsahuje všechny sloupce s vahou q, stačí se podívat, jak vyškrtáváním řádků může vzniknout vektor s p jedničkami. Mějme tedy libovolný vektor délky k obsahující p jedniček. Možností, ze kterých mohl tento vektor vzniknout vyškrtáváním složek vektoru délky n a váhy q, je $\binom{n-k}{q-p}$.

Protože více jak q nebo k jedniček nemůže sloupec z vyškrtané matice obsahovat, dostáváme $p \leq min(q, k)$. Na druhou stranu každý sloupec musí obsahovat alespoň $q-(n-k)$ jedniček (vyškrtáváme $(n-k)$ řádků) a tato hodnota nemůže být záporná. Tedy $p \geq max(0, q-(n-k))$.

□

Předchozí lemma budeme využívat následovně: Připojíme-li k libovolné matici všechny sloupce obsahující $q = p$ nebo $q = p+n-k$ jedniček, pak tato nová matice bude po restrikci na libovolných k řádků navíc (oproti restringované původní matici) obsahovat všechny sloupce s p jedničkami právě jednou (neboť v těchto případech máme $\binom{n-k}{q-p} = 1$) a případně nějaké další sloupce.

Rozhodovat se mezi $q = p$ nebo $q = p+n-k$ budeme tak, abychom přidávali méně sloupců. K tomu si dokážeme následující lemma.

Lemma 14. *Nechť $n, k, p \in \mathbb{N}, p \leq k < n$. Pak $\binom{n}{p} \leq \binom{n}{p+n-k} \Leftrightarrow p \leq k-p$.*

Důkaz. $\Leftarrow$: Máme $p \leq k-p < n-p \Rightarrow p < \frac{n}{2}$. A nyní buď $p+n-k \leq \frac{n}{2}$, a tedy $p < p+n-k \leq \frac{n}{2}$, z čehož plyne $\binom{n}{p} \leq \binom{n}{p+n-k}$. A nebo $p+n-k > \frac{n}{2}$, a potom $\binom{n}{p+n-k} = \binom{n}{n-(p+n-k)} = \binom{n}{k-p}$, a protože $p \leq k-p < \frac{n}{2}$, dostáváme požadovanou implikaci.

$\Rightarrow$: Dokážeme sporem. Nechť tedy $p > k-p$, neboli $p > \frac{k}{2}$. Máme: $p+n-k > \frac{k}{2} + n - k = n - \frac{k}{2} > \frac{n}{2}$. Buď $p > \frac{n}{2}$, a pak máme $p+n-k > p > \frac{n}{2}$, a tedy $\binom{n}{p} > \binom{n}{p+n-k}$. Nebo $p \leq \frac{n}{2}$, a pak z nerovností $k-p < p \leq \frac{n}{2}$ dostáváme $\binom{n}{p} > \binom{n}{k-p} = \binom{n}{p+n-k}$. V obou případech dostáváme spor.

□

Dostáváme následující proceduru (proměnné k a n uvažujme globální).

Algoritmus 1: Přidej(C, p)

Input : matice C, $p \in \mathbb{N}$
Output: matice C obsahující požadované sloupce navíc
if $p \leq k-p$ **then**
  přidej všechny sloupce s $q = p$ jedničkami délky n k matici C
end if
if $p > k-p$ **then**
  přidej všechny sloupce s $q = p+n-k$ jedničkami délky n k matici C
end if
return C

Nyní se konečně dostáváme ke konstrukci bezpečného (k, n)-schématu. K tomu využijeme tvrzení 12, lemma 13 a proceduru Přidej. Dle tvrzení 12 budeme chtít zkonstruovat dvě bázové $n \times m$ matice C_0 a C_1 tak, aby po restrikci na libovolných ale v obou případech stejných k řádků obsahovaly všechny sloupce se sudou respektive lichou vahou a navíc nějakých $l = m - 2^{k-1}$ sloupců. Tyto další sloupce musí být stejné pro obě restringované matice a stejné pro každou restrikci.

Začneme s prázdnými maticemi a postupně k nim budeme přidávat sloupce pouze pomocí procedury Přidej. Lemma 13 nám mimo jiné říká, že nezáleží, na jakých k řádků budeme matice restringovat, neboť nám poskytuje přesný výčet sloupců, které matice po restrikci budou obsahovat. Restringované matice budou stejné až na permutaci sloupců, což nám dle předchozího odstavce nevadí. Fixujme tedy nějaký výběr řádků pro restrikci.

Nejprve přidáme sloupce s takovým počtem jedniček, abychom po restrikci na k řádků dostali všechny sloupce se sudým (pro matici C_0) či lichým (pro matici C_1) počtem jedniček. Toho docílíme zavoláním Přidej(C_0, p) pro sudá $p \leq k$ a Přidej(C_1, p) pro lichá $p \leq k$. Každé zavolání Přidej(C_i, p) $(i \in \{0, 1\})$ nám v restringované matici přidá sloupce s p jedničkami právě jednou a dále nějaké další sloupce, ty nazveme **zbytkové**. Je důležité si všimnout, že zbytkové sloupce tvoří skupiny a to tak, že daná skupina obsahuje všechny možné sloupce s r jedničkami právě jednou. Pro dané r se mohou tyto skupiny vyskytovat vícekrát.

Uvažme ty zbytkové sloupce z restringované matice C_0, které nejsou zbytkovými sloupci v restringované matici C_1. Protože tvoří výše popsané skupiny (daná skupina obsahuje všechny možné sloupce s r jedničkami právě jednou), použijeme pro „doplnění“ matice C_1 proceduru Přidej(C_1, r). Obdobně přidáme další sloupce k matici C_0. Tento proces budeme opakovat, dokud matice nebudou obsahovat stejné zbytkové sloupce.

Zbývá ukázat, že tento algoritmus skončí po konečně mnoha krocích. Přidáme-li k jedné matici nové sloupce volbou $q = r$ (v proceduře Přidej(C_i, r)), pak nové zbytkové sloupce po restrikci, které nebyly použity pro „doplnění“, budou obsahovat méně než r jedniček. Z lemmatu 13 totiž dostáváme, že přidané sloupce po restrikci budou obsahovat p jedniček, kde $p \in \{max(0, q - (n - k)), \ldots, min(q, k)\}$. Jelikož proceduru Přidej(C_i, r) voláme vždy s parametrem $r \leq k$, tak v tomto případě $(q = r)$ máme $min(q, k) = r$, a tedy $p \in \{max(0, q - (n - k)), \ldots, r\}$. Sloupce po restrikci, které obsahují r jedniček, jsou však použity na „doplnění“ dané matice, a tedy ostatní přidané sloupce budou po restrikci obsahovat méně než r jedniček. K druhé matici tak budeme muset přidat takové sloupce, aby po restrikci obsahovaly r' jedniček pro různá $r' < r$. Snadno nahlédneme, že v proceduře Přidej bude opět použita volba $q = r'$. Tedy od takového bodu tento proces skončí nejdéle po r krocích.

Obdobně nahlédneme, že pro volbu $q = r + n - k$ budou mít zbytkové sloupce po restrikci více než $r + n - k$ jedniček a při dalším „doplňování“ bude opět vybrána volba $q = r' + n - k$, kde $r' > r$. Tedy i v tomto případě je tento proces konečný. Dostáváme tak výsledný algoritmus.

Algoritmus 2: Algoritmus pro vytvoření (k, n)-schématu

Input : $k, n \in \mathbb{N}$
Output: Bázové matice C_0 a C_1 bezpečného (k, n)-schématu
$C_0 \leftarrow$ prázdná matice
$C_1 \leftarrow$ prázdná matice
forall *sudá* $p \in \{0, \ldots, k\}$ **do**
  Přidej(C_0, p); `// 1. krok`
end forall
forall *lichá* $p \in \{0, \ldots, k\}$ **do**
  Přidej(C_1, p); `// 2. krok`
end forall
while *matice* C_0 *a* C_1 *obsahují různé zbytkové sloupce* **do**
  Na základě zbytkových sloupců matic C_0 a C_1 přidej k matici C_0 sloupce pomocí procedury Přidej(C_0, r) pro daná r a přidej k matici C_1 sloupce pomocí procedury Přidej(C_1, r') pro daná r'
end while
return C_0, C_1

Algoritmus si ještě předvedeme na příkladu. Zkonstruujeme $(4, 5)$-schéma. Začneme s maticemi C_0 a C_1, které neobsahují žádné sloupce. V prvním kroku algoritmu přidáme k matici C_0 sloupce pomocí pomocí procedury Přidej a to s parametrem $p = 0, 2, 4$. Budeme tedy přidávat všechny sloupce s žádnou, dvěma a pěti ($4 > 5-4$, tedy v proceduře Přidej je vybrána druhá možnost) jedničkami. V druhém kroku zavoláme dvakrát proceduru Přidej a to Přidej$(C_1, 1)$ a Přidej$(C_1, 3)$. Po těchto krocích máme tyto matice:

$$C_0 = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}, C_1 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

Nyní matice C_0 po restrikci na libovolné čtyři řádky obsahuje všechny sloupce s žádnou, dvěma a čtyřmi jedničkami (všechny se sudou vahou). A dále obsahuje zbytkové sloupce: všechny sloupce s jednou jedničkou. Matice C_1 po restrikci na libovolné čtyři řádky obsahuje všechny sloupce s jednou a třemi jedničkami (všechny s lichou vahou) a dva zbytkové sloupce: sloupec se čtyřmi jedničkami a sloupec bez jedniček. V prvním průběhu while cyklu k matici C_1 přidáme sloupce zavoláním metody Přidej(C_1, 1) a k matici C_0 přidáme sloupce zavoláním metody Přidej(C_0, 0) a Přidej(C_0, 4). V matici C_0 budeme mít po restrikci všechny sloupce se sudou délkou, všechny sloupce s jednou jedničkou, sloupec se čtyřmi jedničkami a sloupec bez jedniček. Matice C_1 bude po restrikci obsahovat všechny sloupce s lichým počtem jedniček, všechny sloupce s jednou jedničkou, sloupec se čtyřmi jedničkami a dva sloupce bez jedniček. V druhém průběhu while cyklu tedy k matici C_0 přidáme sloupec se samými nulami (pomocí Přidej(C_0, 0)). Po restrikci těchto matic máme stejné zbytkové sloupce a algoritmus tak končí. Tyto matice splňují předpoklady tvrzení 12 a jsou tedy bázovými maticemi $(4, 5)$-schématu.

$$C_0 = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 \end{pmatrix}$$

$$C_1 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

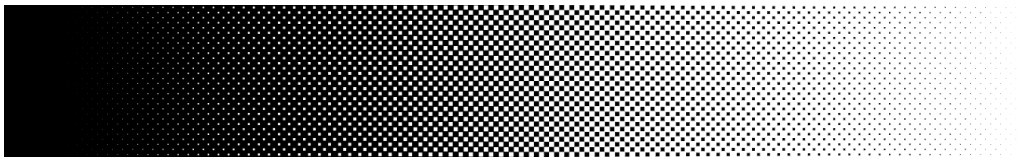
Kapitola 4

Rozšíření

V této kapitole si stručně popíšeme možná rozšíření výše uvedené vizuální kryptografie. Čerpat budeme z (Hou, 2003) pro obrázky v odstínech šedi a z (Socek a Magliveras, 2005) pro zpracování zvuku.

Pro obrázky, které jsou v různých odstínech šedi, použijeme techniku zvanou *halftone*, kterou využívají například inkoustové tiskárny. Obrázek v odstínech šedi bude převeden na černobílý a to tak, že čím tmavší šedá je v dané oblasti, tím větší tam bude hustota černých pixelů (viz obrázek 4.1). Poté lze obrázek už zpracovat standardním způsobem.

(a) Spojité stínování



(b) Halftone

Obrázek 4.1

Dalším rozšířením, které stojí za zmínku, je zpracování zvukové zprávy. Představíme si pouze základní model. Jako zprávu uvažujme posloupnost zvukových signálů – krátkých nebo dlouhých pípnutí. Obdobně jako u vizuálního modelu bude krátké pípnutí reprezentováno jako 0 a dlouhé jako 1. Každé pípnutí se zpracovává zvlášť a je rozděleno na m dalších (ne nutně kratších) signálů – opět krátké nebo dlouhé pípnutí. Skládání signálů se provádí přehráním jednotlivých podílů zároveň. Je-li alespoň jedno pípnutí v podílů dlouhé, výsledné pípnutí je také dlouhé. Takové skládání opět odpovídá operaci OR. Na tento zvukový model se dají aplikovat schémata popsaná pro vizuální kryptografii. K reprezentování dat zprávy může být použita Morseova abeceda nebo Huffmanovo kódování.

Závěr

Práce uvedla čtenáře do problematiky vizuální kryptografie a jako hlavní výsledek ukázala, jak zkonstruovat bezpečné (k, n)-schéma.

Některé definice jsou v porovnání s texty, ze kterých práce vychází, pozměněny. Například definice samotného (k, n)-schématu připouští libovolné pravděpodobnostní rozdělení, ne pouze uniformní jako v (Naor a Shamir, 1995). Dále není v této definici zahrnuta podmínka bezpečnosti, tu najdeme v definici 8. S tím souvisejí i příslušná tvrzení a lemmata, která se v jiné literatuře nevyskytují (například tvrzení 4 a lemma 3). Také je značně pozměněn důkaz bezpečnosti (k, k)-schématu.

Omezený rozsah práce bohužel neumožnil více se věnovat problematice šifrování zvuku.

Na práci je možné dále navázat. Jelikož všechna schémata v práci využívají uniformní rozdělení, dalo by se zabývat tím, jaký přínos by měla i jiná, nerovnoměrná rozdělení. V (Naor a Shamir, 1995) se autoři také zabývají tím, jakého maximálního relativního kontrastu lze dosáhnout. Dále v (Ateniese a kol., 1996) můžeme najít konstrukci schématu pro obecnou přístupovou strukturu.

Literatura

Ateniese, G., Blundo, C., De Santis, A. a Stinson, D. R. (1996). Visual cryptography for general access structures. *Information and Computation*, **129**, 86–106.

Droste, S. (1996). New results on visual cryptography. *Advances in Cryptology - CRYPTO '96*, **1109**, 401–415.

Hou, Y. C. (2003). Visual cryptography for color images. *Pattern Recognition*, **36**, 1619–1629.

Naor, M. a Shamir, A. (1995). Visual cryptography. *Advances in Cryptology - EUROCRYPT '94*, **950**, 1–12.

Socek, D. a Magliveras, S. S. (2005). General access structures in audio cryptography. *2005 IEEE International Conference on Electro Information Technology*, pages 1–6.