MTAT.07.006 Krüptograafia uurimisseminar
Jääkriski hindamine turvatud arenduskeskkonnas

Lauri Tulmin

2. mai 2007. a.

Eesmärgid

- Anda ülevaade riskidest intellektuaalsele omandile.

Eesmärgid

- Anda ülevaade riskidest intellektuaalsele omandile.
- Kirjeldada turvatud arenduskeskkonda.

Eesmärgid

- Anda ülevaade riskidest intellektuaalsele omandile.
- Kirjeldada turvatud arenduskeskkonda.
- Info viimine turvatud arenduskeskkonnast digitaalkaamera abil.

Üldised riskid

- Piraatlus.

Üldised riskid

- Piraatlus.
- Tarkvara pahatahtlik muutmine.

Üldised riskid

- Piraatlus.
- Tarkvara pahatahtlik muutmine.
- Konkurents.

Üldised riskid

- Piraatlus.
- Tarkvara pahatahtlik muutmine.
- Konkurents.

Üldised riskid

- Piraatlus.
- Tarkvara pahatahtlik muutmine.
- Konkurents.
- Koodileke.

Ettevõtte töötajate liigitus

- *The Security Softie*.

Ettevõtte töötajate liigitus

- *The Security Softie*.
- *The Gadget Geek*.

Ettevõtte töötajate liigitus

- *The Security Softie*.
- *The Gadget Geek*.
- *The Squatter*.

Ettevõtte töötajate liigitus

- *The Security Softie*.
- *The Gadget Geek*.
- *The Squatter*.
- *The Saboteur*.

Turvatud arenduskeskkond

- Kaitstud väliste rünnete eest.

Turvatud arenduskeskkond

- Kaitstud väliste rünnete eest.
- Puudub internetiühendus.

Turvatud arenduskeskkond

- Kaitstud väliste rünnete eest.
- Puudub internetiühendus.
- Ei saa kasutada mälupulka, CD'd jms.

Turvatud arenduskeskkond

- Kaitstud väliste rünnete eest.
- Puudub internetiühendus.
- Ei saa kasutada mälupulka, CD'd jms.
- Mis jääb üle?

Info viimine digitaalkaamera abil

- Miks just digitaalkaamera?

Info viimine digitaalkaamera abil

- Miks just digitaalkaamera?
- Andmete esitamine pildil.

Info viimine digitaalkaamera abil

- Miks just digitaalkaamera?
- Andmete esitamine pildil.
  - Esitame andmed värviliste ruutudena.

Info viimine digitaalkaamera abil

- Miks just digitaalkaamera?
- Andmete esitamine pildil.
  - Esitame andmed värviliste ruutudena.
  - Iga baidi kodeerimiseks vajalik ruutude arv sõltub kasutatud värvide arvust.

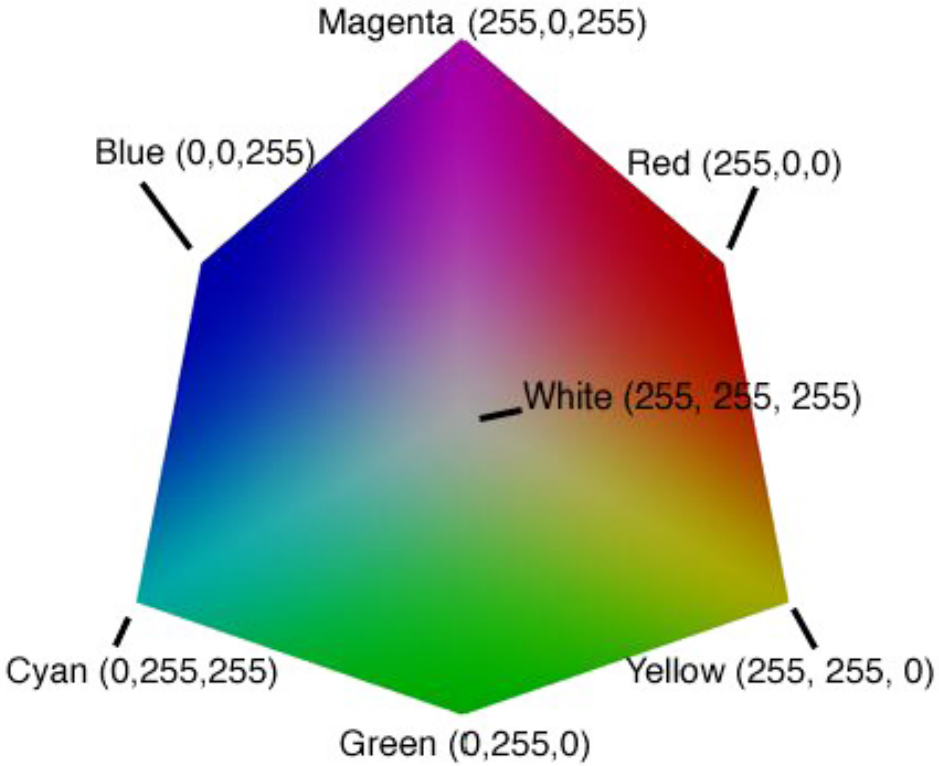
Info viimine digitaalkaamera abil

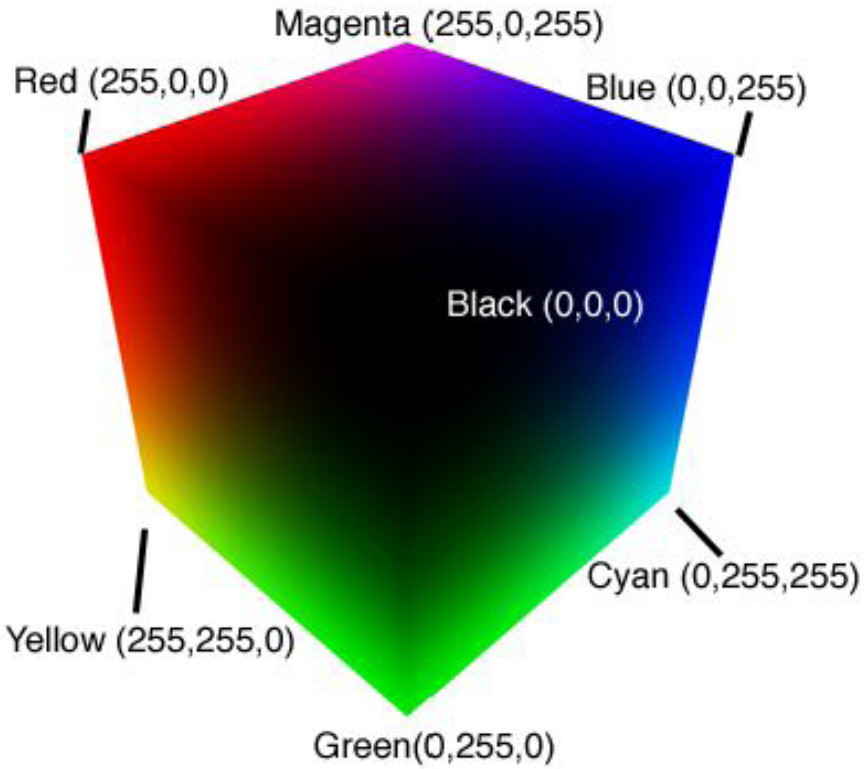
- Miks just digitaalkaamera?
- Andmete esitamine pildil.
  - Esitame andmed värviliste ruutudena.
  - Iga baidi kodeerimiseks vajalik ruutude arv sõltub kasutatud värvide arvust.
  - Pildile mahtuva info hulk sõltub värvide arvust, ruudu suurusest ja ruutude vahest.

Info viimine digitaalkaamera abil

- Miks just digitaalkaamera?
- Andmete esitamine pildil.
  - Esitame andmed värviliste ruutudena.
  - Iga baidi kodeerimiseks vajalik ruutude arv sõltub kasutatud värvide arvust.
  - Pildile mahtuva info hulk sõltub värvide arvust, ruudu suurusest ja ruutude vahest.
  - Võib kodeerida ka plokkidena.

RGB värviruum





HSV värviruum

- 3 komponenti nagu RGB'l.

HSV värviruum

- 3 komponenti nagu RGB'l.
- toon(*hue*) - määrab ära värvuse(sinine, punane jne.). Kui koonuse põhi esitada polaarkoordinaatides, siis tooni määrab nurk.

HSV värviruum

- 3 komponenti nagu RGB'l.
- toon(*hue*) - määrab ära värvuse(sinine, punane jne.). Kui koonuse põhi esitada polaarkoordinaatides, siis tooni määrab nurk.
- kirkus/tooni puhtus(*saturation*) - määrab värvi erksuse. Vähese kirkusega värvid tunduvad hallina olenemate toonist.

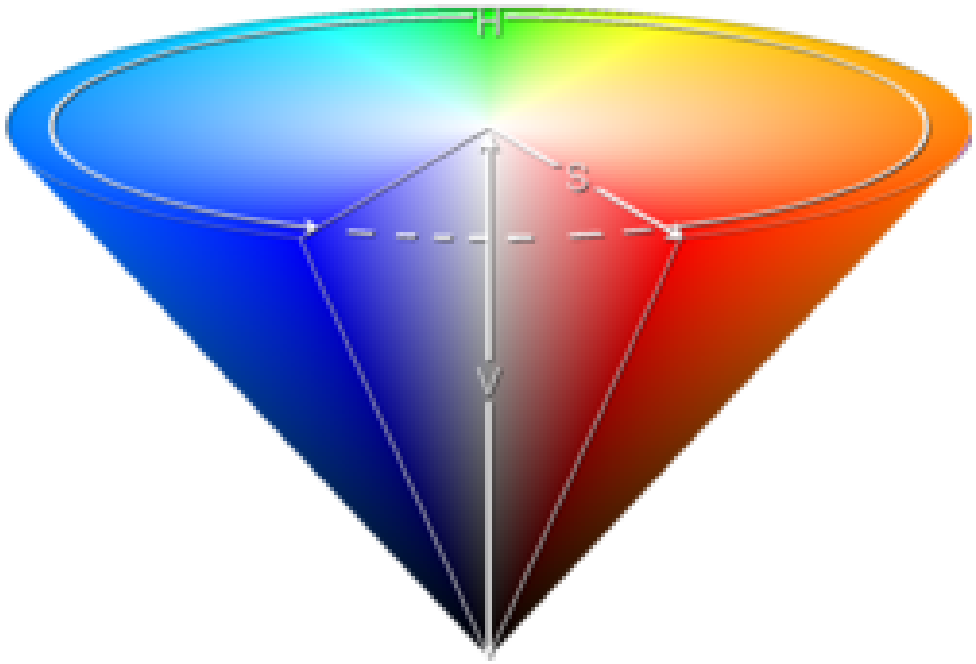
HSV värviruum

- 3 komponenti nagu RGB'l.
- toon(*hue*) - määrab ära värvuse(sinine, punane jne.). Kui koonuse põhi esitada polaarkoordinaatides, siis tooni määrab nurk.
- kirkus/tooni puhtus(*saturation*) - määrab värvi erksuse. Vähese kirkusega värvid tunduvad hallina olenemate toonist.
- heledus(*value/brightness*) - värvi heledus.

HSV värviruum

- 3 komponenti nagu RGB'l.
- toon(*hue*) - määrab ära värvuse(sinine, punane jne.). Kui koonuse põhi esitada polaarkoordinaatides, siis tooni määrab nurk.
- kirkus/tooni puhtus(*saturation*) - määrab värvi erksuse. Vähese kirkusega värvid tunduvad hallina olenemate toonist.
- heledus(*value/brightness*) - värvi heledus.
- võib ette kujutada kui koonust.

HSV värviruum (2)



Värvide vaheline kaugus HSV värviruumis

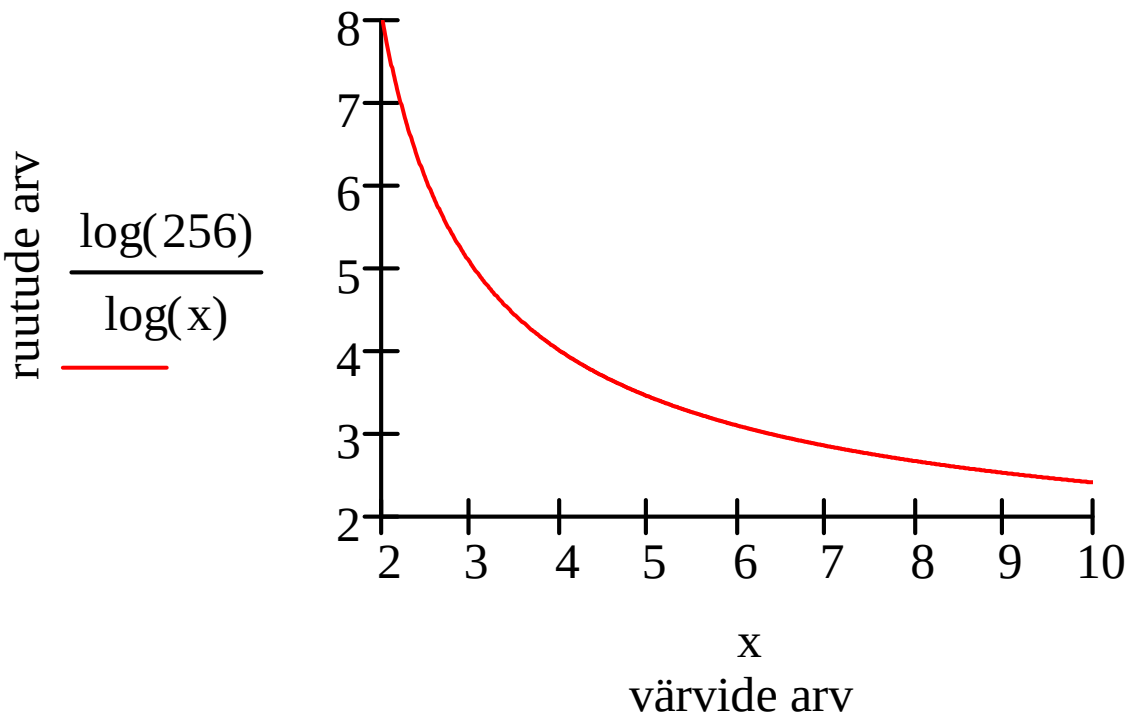
Olgu antud värvid $c = (h, s, v)$ ja $c' = (h', s', v')$, siis nende vaheline kaugus on

$$d = \left| c - c' \right|$$

Kui $0 \leq h \leq 1$, $0 \leq h' \leq 1$, $0 \leq s \leq 1$, $0 \leq s' \leq 1$, $0 \leq v \leq 1$ ja $0 \leq v' \leq 1$ siis saab eelmise valemi esitada kujul:

$$\begin{aligned} d = \quad & ((v - v')^2 + (s \times cos(2\pi h) - s' \times cos(2\pi h'))^2 + \\ & (s \times sin(2\pi h) - s' \times sin(2\pi h'))^2)^{\frac{1}{2}} \end{aligned}$$

Ruutude arv ühe baidi kodeeerimiseks



Ruutude arv ühe kilobaidi kodeeerimiseks

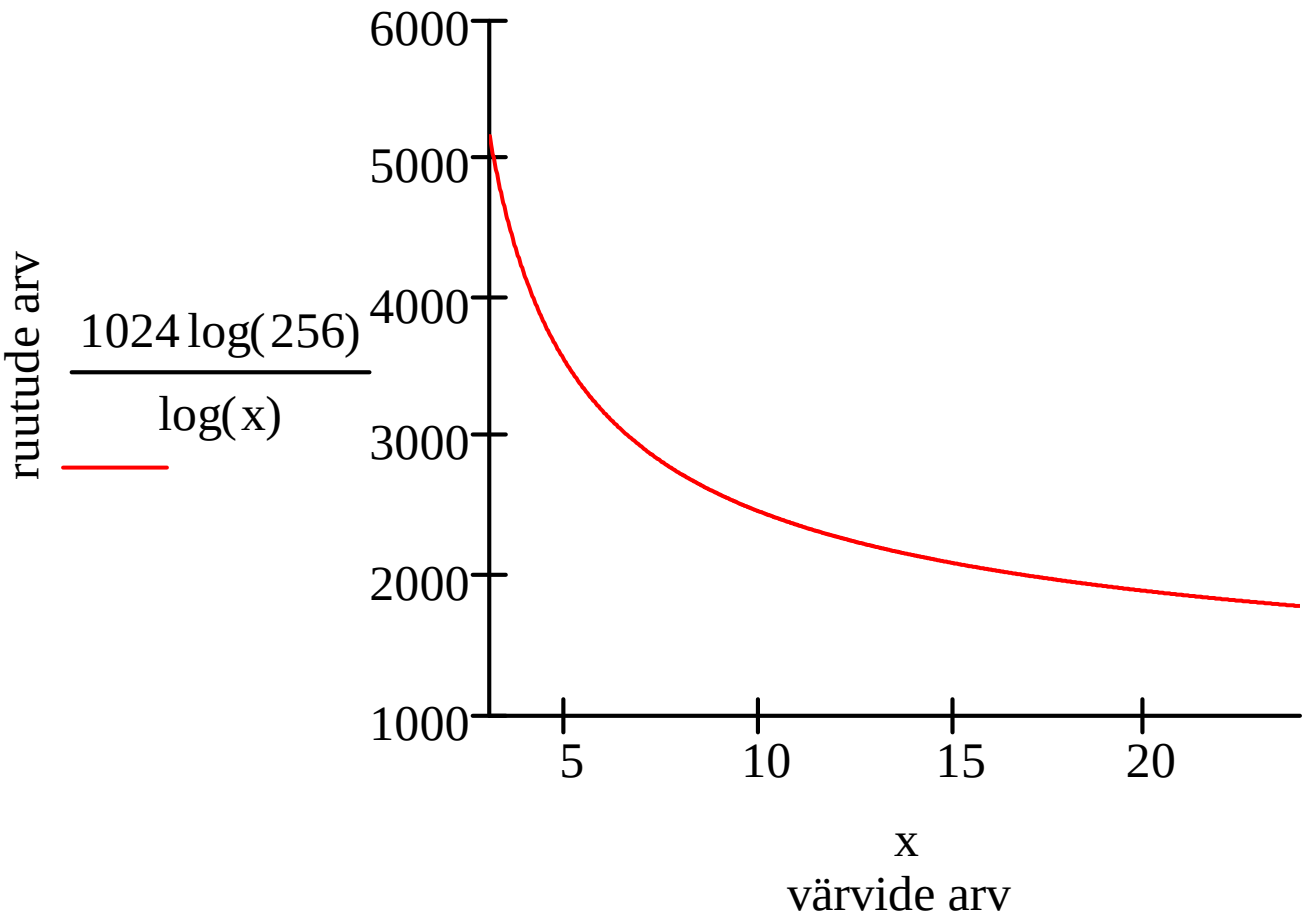


Foto töötlemine

- Kõigi pikslite, mille saturation ≤ 25, saturation $= 0$.

Foto töötlemine

- Kõigi pikslite, mille saturation ≤ 25, saturation $= 0$.
- Kõigi pikslite, mille brightness ≥ 25, brightness $= 100$.

Foto töötlemine

- Kõigi pikslite, mille saturation ≤ 25, saturation $= 0$.
- Kõigi pikslite, mille brightness ≥ 25, brightness $= 100$.
- Kõigi pikslite, mille saturation ≥ 25, saturation $= 100$.

Foto töötlemine

- Kõigi pikslite, mille saturation ≤ 25, saturation $= 0$.
- Kõigi pikslite, mille brightness ≥ 25, brightness $= 100$.
- Kõigi pikslite, mille saturation ≥ 25, saturation $= 100$.
- Kõik piisavalt heledad ruudud muudetakse valgeks, üksikud pikslid visatakse minema.

Foto töötlemine

- Kõigi pikslite, mille saturation ≤ 25, saturation $= 0$.
- Kõigi pikslite, mille brightness ≥ 25, brightness $= 100$.
- Kõigi pikslite, mille saturation ≥ 25, saturation $= 100$.
- Kõik piisavalt heledad ruudud muudetakse valgeks, üksikud pikslid visatakse minema.
- Kõigi järelejäännud ruutude kohta arvutatakse keskmine värv ja leitakse algsete värvide hulgast kõige lähedasem. Kui ruut on liiga väike, siis visatakse minema.

Foto töötlemine

- Kõigi pikslite, mille saturation ≤ 25, saturation $= 0$.
- Kõigi pikslite, mille brightness ≥ 25, brightness $= 100$.
- Kõigi pikslite, mille saturation ≥ 25, saturation $= 100$.
- Kõik piisavalt heledad ruudud muudetakse valgeks, üksikud pikslid visatakse minema.
- Kõigi järelejäännud ruutude kohta arvutatakse keskmine värv ja leitakse algsete värvide hulgast kõige lähedasem. Kui ruut on liiga väike, siis visatakse minema.
- Kui pildi äärde on jäänud mingi tume ala, näiteks monitori serv vmt. või pildi ääres on heldedus liiga väike, siis proovitakse need alad ära kaotada.

Sisend : Andmed S, bloki suurus bs(korraga kodeeritavate baitide arv) ja värvide arv n

$vs = \lceil bs \times log_n(256) \rceil$

while S *on veel andmeid* **do**

  $(b, s) \longleftarrow$ loe sisendist S n baiti

  if $bs \neq s$ **then**

    $vs = \lceil s \times log_n(256) \rceil$

  end

  $d_0 d_1 d_2 ... d_{vs} \longleftarrow$ esita arv b alusel n

  for $v \longleftarrow d_0 ... d_{vs}$ **do**

    $JoonistaRuut(v)$

  end

end

Algoritm 1: Pildile andmete kodeerimine

Sisend : Pilt P, kodeerija bloki suurus bs ja värvide arv n
$T\ddot{o}\ddot{o}tlePilti(P)$

$vs = \lceil bs \times log_n(256) \rceil$
while *P on veel lugemata ruute* **do**
  $(b, s) \longleftarrow$ loe pildilt P vs ruutu
  if $vs \neq s$ **then**
    $bs = \lfloor s \times log_{256}(n) \rfloor$
  end
  $d_0 d_1 d_2 ... d_{bs} \longleftarrow$ esita arv b alusel 256
  for $v \longleftarrow d_0 ... d_{bs}$ **do**
    $V\ddot{a}ljastaBait(v)$
  end
end

Algoritm 2: Pildilt andmete dekodeerimine

Kokkuvõte

- Digitaalkaamera pole mõeldud ruudukeste pildistamiseks.

Kokkuvõte

- Digitaalkaamera pole mõeldud ruudukeste pildistamiseks.
- Pildilt ei õnnestu tuvastada üle 7 värvi.

Kokkuvõte

- Digitaalkaamera pole mõeldud ruudukeste pildistamiseks.
- Pildilt ei õnnestu tuvastada üle 7 värvi.
- Seni on pildile õnnestunud mahutada $\sim$ 3400 baiti.

Lõpp

Küsimusi?