Vizuelno kriptogragski algoritmi dijeljenja tajne

SPECIJALISTIČKI RAD

Mentor:
dr Vladimir Božović

Student:
Dragoje Božović

Uvod

- Motivacija
  - Kriptografija počinje da se razvija kad i potreba za tajnošću pisanih informacija
- Hronološka upotreba kriptografskih tehnika
  - Razvijanje u vojne, industrijske svrhe, zaštita privatnosti krajnjih korisnika računara
- Kriptografski primitivi
  - Prevaziđene tehnike: shift, substitution
- Primjena kritografije:
  - Zaštita od uništenja i krađe informacija, autentičnost pošiljaoca i podataka

Podjela kriptografskih algoritama

- Podjela kriptografskih algoritama čija je namjena zaštita informacija prema tipu ključa:
  - Asimetrični
  - Simetrični
- Podjela simetričnih algoritama prema načinu primjene ključa na ulazni podatak:
  - Blok (fiksirana dužina ključa)
  - Bajt (promjenjiva dužina ključa)
    - najsigurniji, uz pravilnu implementaciju
- Vizuelno kriptografski algoritmi mogu se svrstati u simetrične bajt algoritme.

Zaštita podataka

- Podatak pravimo rezilijentnim povećavajući mu broj kopija
- Direktna implementacija povećava rizik od neovlašćenog pristupa
- Tehnologije za zaštitu podataka, zavisno od potrebe:
  - Enkripcija kopija:
    - AES, DES, 3DES
  - Algoritmima dijeljenja tajne:
    - Šamirov algoritam (interpolacija polinoma)
    - Bleklijev algoritam (geometrija hiperravni)

Problem dijeljenja tajne

- Podatak *S* dijelimo na određen broj djelova *n* (ključevi), tako da ga rekonstruišemo spajanjem dovoljnog broja ključeva *k* (prag)
- Ključevi ne smiju sadržati čitljive djelove podatka *S*
- Spajanjem *k* ključeva moramo rekonstruisati *S*
- Spajanjem *k-1* ne smije nam odati nikakvu informaciju o *S*
- Uništavanjem *n-k* ključeva možemo povratiti podatak
- Vrsta ključeva:
  - Ravnopravni
  - Familije kvalifikovanih podskupova

Model slike u matematici

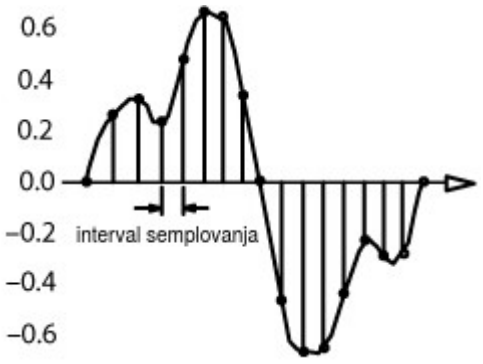
- Dvodimenzionalna funkcija inteziteta svjetla u vremenu
- Matematički model slike :

$$f(x, y) = i(x, y)\, r(x, y),\ 0 < i(x, y) < \infty,\ 0 < r(x, y) < 1$$

- Direktna implementacija nemoguća

Računarski model slike

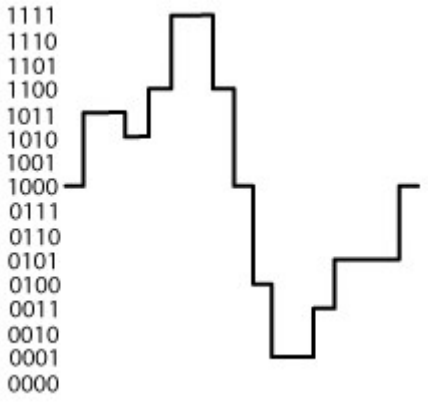
- Diskretizujemo domene
- Semplovanje, diskretizovanje vremena, x-osa
- Proizvod diskretizovanja matrični zapis, elementi funkcije
- Ova transformacija određuje broj piksela na digitalizovanoj slici



$$f(x,y) \approx \begin{bmatrix} f(0,0) & f(0,1) & \dots & f(0,M) \\ f(1,0) & f(1,1) & \dots & f(1,M) \\ \vdots & \vdots & & \vdots \\ f(N,0) & f(N,1) & \dots & f(N,M) \end{bmatrix}$$

Računarski model slike, nastavak

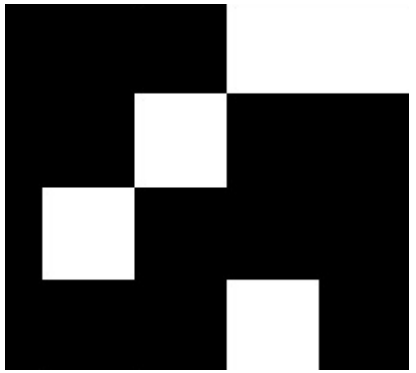
- Kvantizacija, diskretizovanje inteziteta, y-osa
- Proizvod semplovanja i kvantizacije matrica
- Elementi matrice pikseli, imaju konačnu vrijednost sa fiksiranim brojem bitova 2^n



$$f(x,y) \approx \begin{bmatrix} f[0,0] & f[0,1] & \dots & f[0,M] \\ f[1,0] & f[1,1] & \dots & f[1,M] \\ \vdots & \vdots & & \vdots \\ f[N,0] & f[N,1] & \dots & f[N,M] \end{bmatrix}$$

Tipovi slika po dubini boje

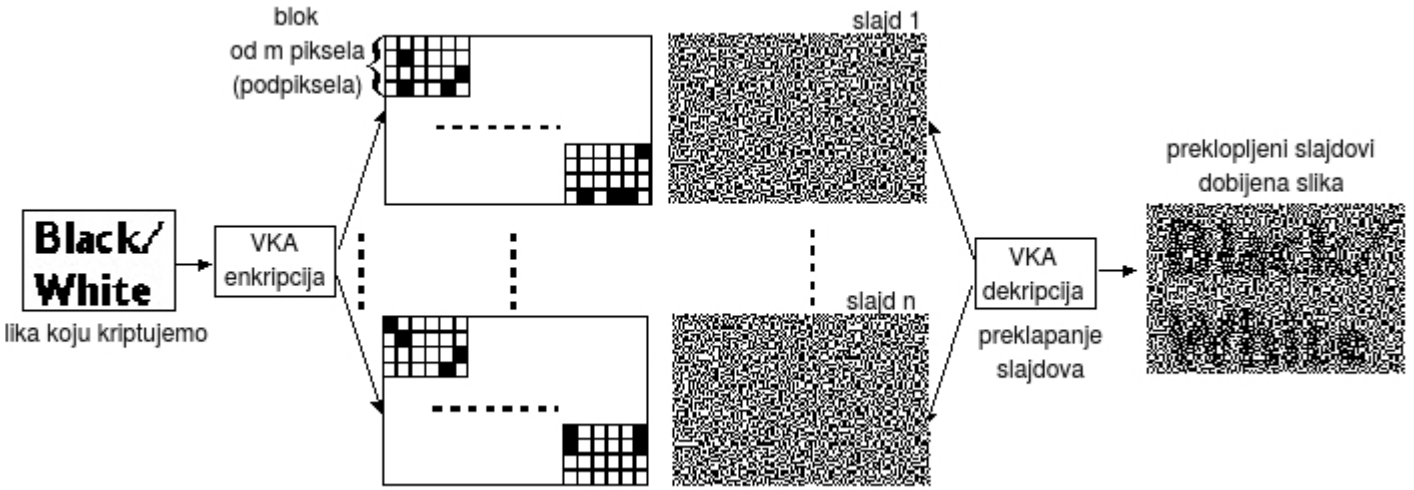
- Slike koje nisu u boji
  - 1-bit monochrome, binarna slika
  - 8-bit grayscale, “crno bijela” slika
- Binarne slike na računaru predstavljaju se Bulovom matricom 0-1



$$\begin{bmatrix} 1 & 0 & \dots & 0 \\ 1 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 0 & \dots & 0 \end{bmatrix}$$

Vizuelno kriptografski algoritmi

- Proces kriptovanja kod vizuelno kriptografskih algoritama:
  - Ulazni podatak “slika”
  - Dijeljenje podatka na slajdove (dijeljenje tajne)
  - Enkripcija piksela
    - Zamjena sa jednim pikselom (Kafri-Karen)
    - Zamjena sa blokom piksela (Naor-Šamir)



  - Dekripcija (preklapanje, vizuelna detekcija)

Naor-Šamirov algoritam

- Problem visokih rezolucija, nivo sive
- Hamingova težina jednog bloka za kodiranje
- S – matrica enkripcije jednog piksela

$$S = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1m} \\ \vdots & \vdots & \ddots & \vdots \\ a_{k1} & a_{k2} & \dots & a_{km} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nm} \end{bmatrix}; V_S = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1m} \\ \vee & \vee & \vee & \vee \\ \vdots & \vdots & \ddots & \vdots \\ \vee & \vee & \vee & \vee \\ a_{n1} & a_{n2} & \dots & a_{nm} \end{bmatrix} = \begin{bmatrix} h_1 & h_2 & \dots & h_m \end{bmatrix}$$

- Prag d, H(V) = d − αm, H(V) ≥ d
- m – širenje piksela, gubitak rezolicije
- α – relativna razlika, gubitak kontrasta

Naor-Šamir VKA, izbor matrica za enkripciju

- Skupovi za kriptovanje bijelih i crnih piksela: C_0 i C_1
- Uslovi za dobar VKA
  - Čitljivost : Detekcija bijele (manje sive) i crne (više sive) - Hamingova težina blokova
  - Sigurnost: način odabira matrica C_0 i C_1

$$C_0 = \{W_1, W_2, \ldots, W_r\}\ C_1 = \{B_1, B_2, \ldots, B_r\}$$

- N-Š 2 od n: C0 dobijamo permutacijom kolona M0, C1 permutacijom kolona M1

$$M_0 = \begin{bmatrix} 1 & 0 & \ldots & 0 \\ 1 & 0 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 0 & \ldots & 0 \end{bmatrix}; \; M_1 = \begin{bmatrix} 1 & 0 & \ldots & 0 \\ 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & 1 \end{bmatrix};$$

Naor-Šamirov VKA 2 od 2

- Odabir matrica za kriptovanje 2 od 2

$$M = \left\{ \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix} \right\}, \left\{ \begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} \right\}, \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \right\}$$

Piksel na slici	$P(C_t)$	Blok slajda 1	Blok slajda 2	Posle dekripcije	V(H)
□	0.5_0				2
□	0.5_0				2
■	0.5_0				4
■	0.5_0				4

Kafri-Keren VKA slučajne rešetke 2 od 2

- Zamjena jednog piksela na originalu jednim podpikselom na slajdu
- Slučajno generisanje prvog slajda
- Drugi slajd generišemo na osnovu originala i prvog slajda

$I[x,y]$	$S_1[x,y]$	$P(S_1[x,y])$	$S_2[x,y]$	$S_1[x,y]+S_2[x,y]$
□	□	0.5	□	□
□	■	0.5	■	■
■	□	0.5	■	■
■	■	0.5	□	■

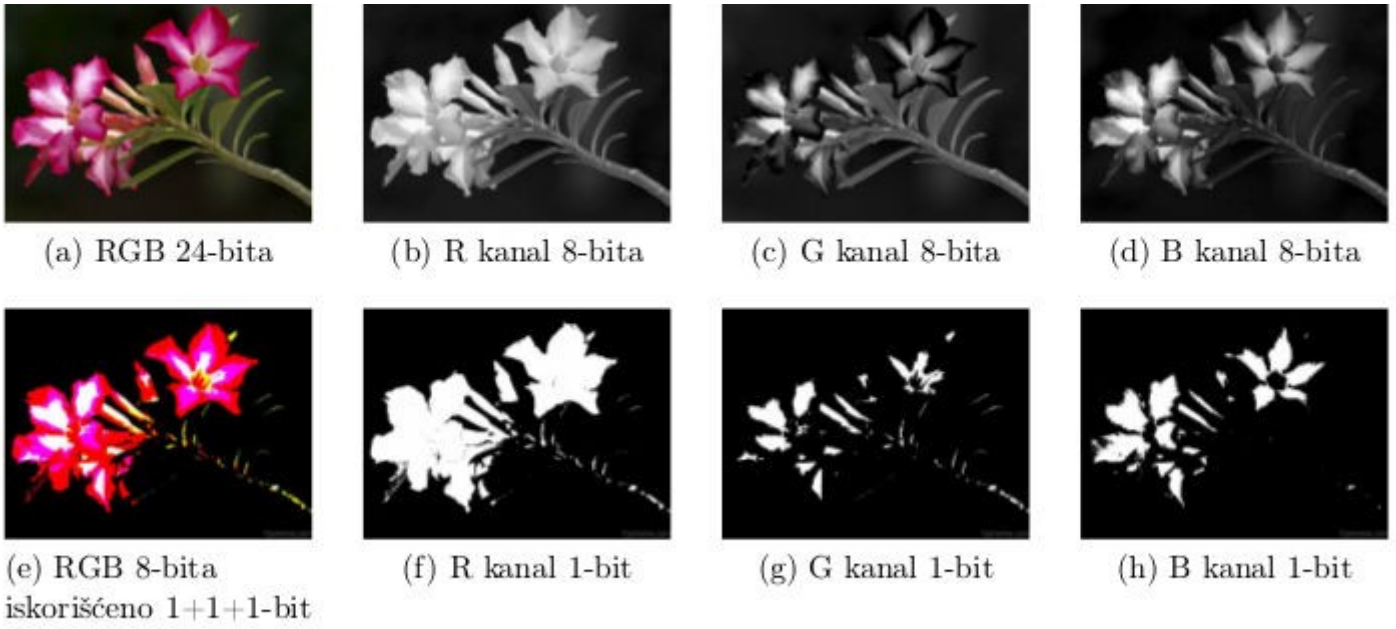
Čen-Tsao VKA n od n

- Proširenje Karen-Kenfri 2 od 2
- Ideja se može iskoristiti i za Naor-Šamir 2 od 2
- Uništava originalnost pri povećanju n za 25% u svakom koraku
- U *n* koraka ponavljamo *n-1* put K-K 2 od 2

Korak	Slajd	Dodijeljena vrijedost
1	S_1	Random
2	S'_2	S_1 XOR I
3	S_2	Random
4	S'_3	S_2 XOR S'_2
5	S_3	S'_3

VKA binarnih slika za rad sa slikama u boji

- RGB model, 1 piksel = 2^n : n = R_{bita} + G_{bita} + B_{bita}
- Raslojavanje po osnovnim kanalima
- Rad sa S x n slika posebno

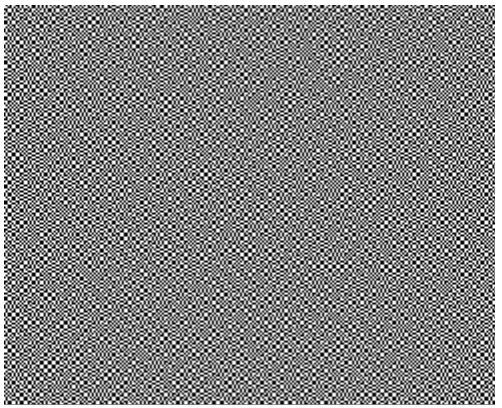
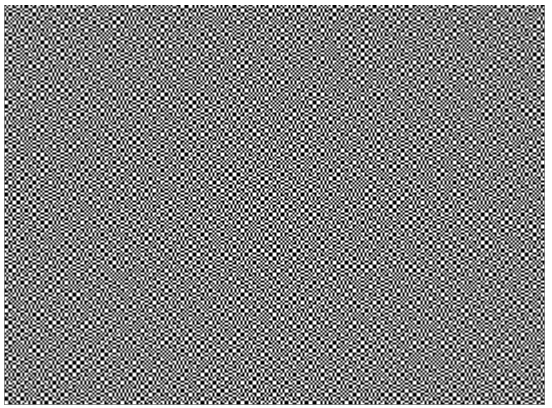


(a) RGB 24-bita (b) R kanal 8-bita (c) G kanal 8-bita (d) B kanal 8-bita

(e) RGB 8-bita iskorišćeno 1+1+1-bit (f) R kanal 1-bit (g) G kanal 1-bit (h) B kanal 1-bit

Zaključak

- Pouzdani i brzi algoritmi.
- Kriptoanaliza se svodi na analizu random funkcije
- Jednostavna dekripcija koja ne zahtijeva korišćenje računara
- Za identično preslikavanje ulaznog podatka u podatak koji je dobijen dekripcijom, zahtijevaju post procese za popravku šumova i proporcije


Original Slajd 1 Slajd 2 Dekriptovana slika

VKA Naor Šamir

- **2 od 2**

Hvala na pažnji.