Uvod
Izazovi
Problem privatnosti u biometriji
Usporedba lozinke - biometrijski uzorci
Biometrija u percepciji javnosti
Kako povećati razinu privatnosti?
Biometrija i kriptografija
Biometrijski sažetak
Biometrijska enkripcija
Problemi sa sažimanjem i enkripcijom
Samoispravljajući kodovi
Otkaziva biometrija
BKI
Zaključak

Otkaziva biometrija, biometrijska enkripcija i očuvanje privatnosti korisnika

Mr. sc. Markus Schatten

Centar za biometriju
Fakultet organizacije i informatike,
Sveučilište u Zagrebu
Pavlinska 2, 42000 Varaždin
http://cb.foi.hr markus.schatten@foi.hr

26.11.2009.

Sadržaj

1. Uvod
   - Izazovi
2. Problem privatnosti u biometriji
   - Usporedba lozinke - biometrijski uzorci
   - Biometrija u percepciji javnosti
   - Kako povećati razinu privatnosti?
3. Biometrija i kriptografija
   - Biometrijski sažetak
   - Biometrijska enkripcija
   - Problemi sa sažimanjem i enkripcijom
   - Samoispravljajući kodovi
4. Otkaziva biometrija
5. BKI
6. Zaključak

Uvod
Izazovi
Problem privatnosti u biometriji
Usporedba lozinke - biometrijski uzorci
Biometrija u percepciji javnosti
Kako povećati razinu privatnosti?
Biometrija i kriptografija
Biometrijski sažetak
Biometrijska enkripcija
Problemi sa sažimanjem i enkripcijom
Samoispravljajući kodovi
Otkaziva biometrija
BKI
Zaključak

Uvod

Uvod
Izazovi
Problem privatnosti u biometriji
Usporedba lozinke - biometrijski uzorci
Biometrija u percepciji javnosti
Kako povećati razinu privatnosti?
Biometrija i kriptografija
Biometrijski sažetak
Biometrijska enkripcija
Problemi sa sažimanjem i enkripcijom
Samoispravljajući kodovi
Otkaziva biometrija
BKI
Zaključak

- Biometrija postaje ozbiljna tehnologija na različitim područjima gdje valja osigurati CIA

Uvod

Uvod
Izazovi
Problem privatnosti u biometriji
Usporedba lozinke - biometrijski uzorci
Biometrija u percepciji javnosti
Kako povećati razinu privatnosti?
Biometrija i kriptografija
Biometrijski sažetak
Biometrijska enkripcija
Problemi sa sažimanjem i enkripcijom
Samoispravljajući kodovi
Otkaziva biometrija
BKI
Zaključak

- Biometrija postaje ozbiljna tehnologija na različitim područjima gdje valja osigurati CIA
  - Confidentiality (povjerljivost)
  - Integrity (integritet – cjelovitost, nepromjenjenost)
  - Availability (dostupnost)

Uvod

Uvod
Izazovi
Problem privatnosti u biometriji
Usporedba lozinke - biometrijski uzorci
Biometrija u percepciji javnosti
Kako povećati razinu privatnosti?
Biometrija i kriptografija
Biometrijski sažetak
Biometrijska enkripcija
Problemi sa sažimanjem i enkripcijom
Samoispravljajući kodovi
Otkaziva biometrija
BKI
Zaključak

- Biometrija postaje ozbiljna tehnologija na različitim područjima gdje valja osigurati CIA
  - Confidentiality (povjerljivost)
  - Integrity (integritet – cjelovitost, nepromjenjenost)
  - Availability (dostupnost)
- Državne institucije – biometrijske putovnice, osobne iskaznice, identifikacija zaposlenih ...
- Financijske institucije – POS identifikacija kupaca, potvrda financijskih transakcija ...
- Zdravstvene institucije – biometrijska zdravstvena iskaznica, karton pacijenta, povijest bolesti ...
- ...

Izazovi

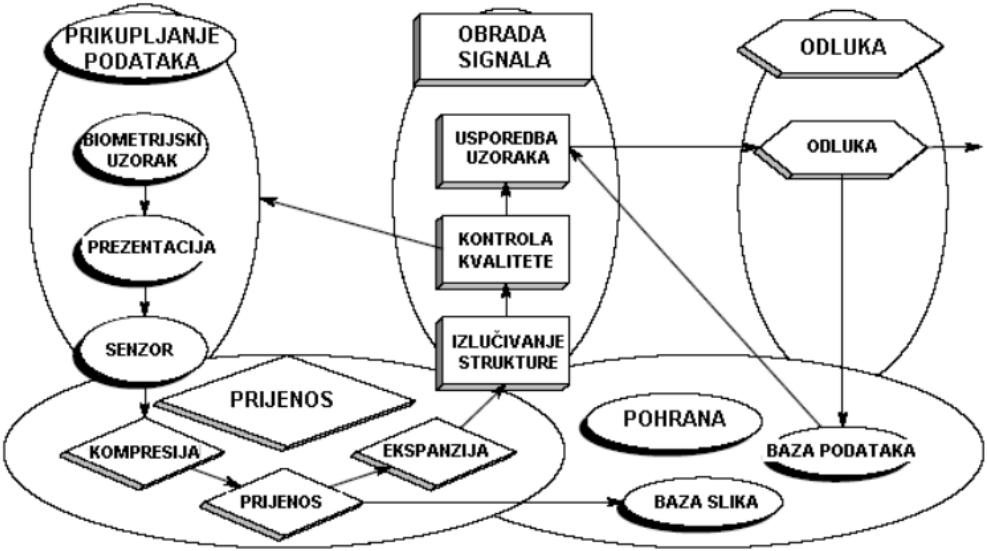
Uvod
Izazovi
Problem privatnosti u biometriji
Usporedba lozinke - biometrijski uzorci
Biometrija u percepciji javnosti
Kako povećati razinu privatnosti?
Biometrija i kriptografija
Biometrijski sažetak
Biometrijska enkripcija
Problemi sa sažimanjem i enkripcijom
Samoispravljajući kodovi
Otkaziva biometrija
BKI
Zaključak

- Usavršavanje tehnologije u pogledu egzaktnosti (FAR, FRR, ...)
- Usavršavanje tehnologije u pogledu performansi
- Razumijevanje i upravljanje privatnošću

Problem privatnosti u biometriji

Uvod
Izazovi
Problem privatnosti u biometriji
Usporedba lozinke - biometrijski uzorci
Biometrija u percepciji javnosti
Kako povećati razinu privatnosti?
Biometrija i kriptografija
Biometrijski sažetak
Biometrijska enkripcija
Problemi sa sažimanjem i enkripcijom
Samoispravljajući kodovi
Otkaziva biometrija
BKI
Zaključak

- Kao i svaki drugi sustav biometrijski je sustav podložan napadima na svojim podsustavima (Wayman, 2000):



Usporedba lozinke – biometrijski uzorci (Ratha et. al., 2006)

Uvod
Izazovi
Problem privatnosti u biometriji
Usporedba lozinke - biometrijski uzorci
Biometrija u percepciji javnosti
Kako povećati razinu privatnosti?
Biometrija i kriptografija
Biometrijski sažetak
Biometrijska enkripcija
Problemi sa sažimanjem i enkripcijom
Samoispravljajući kodovi
Otkaziva biometrija
BKI
Zaključak

	Biometrijski uzorak	**Lozinka**
Interna reprezentacija	Izlučena struktura (fiksne ili varijabilne veličine)	Sažetak (hash) znakovnog niza lozinke
Veličine	U pravilu 100 B ili više	Prosječno 6-8 alfanumeričkih znakova
Ulazni podaci	Uvijek drukčiji	Uvijek isti
Algoritam usporedbe	Neegzaktan, neizrazit (fuzzy), nikad 100% precizan	Egzaktan, 100% precizan
Neporecivost	Da (u većini slučajeva)	Ne
Otkazivost	Ne	Da (vrlo jednostavno)

Biometrija u percepciji javnosti

Uvod
Izazovi
Problem privatnosti u biometriji
Usporedba lozinke - biometrijski uzorci
Biometrija u percepciji javnosti
Kako povećati razinu privatnosti?
Biometrija i kriptografija
Biometrijski sažetak
Biometrijska enkripcija
Problemi sa sažimanjem i enkripcijom
Samoispravljajući kodovi
Otkaziva biometrija
BKI
Zaključak

Prema (SEARCH, US Bureau of Justice Statistics, 2002)

- 88% ispitanika boji se zloupotrebe svojih biometrijskih podataka
- 80% ispitanika odobrava korištenje biometrije za prevenciju kriminala

Kako povećati razinu privatnosti?

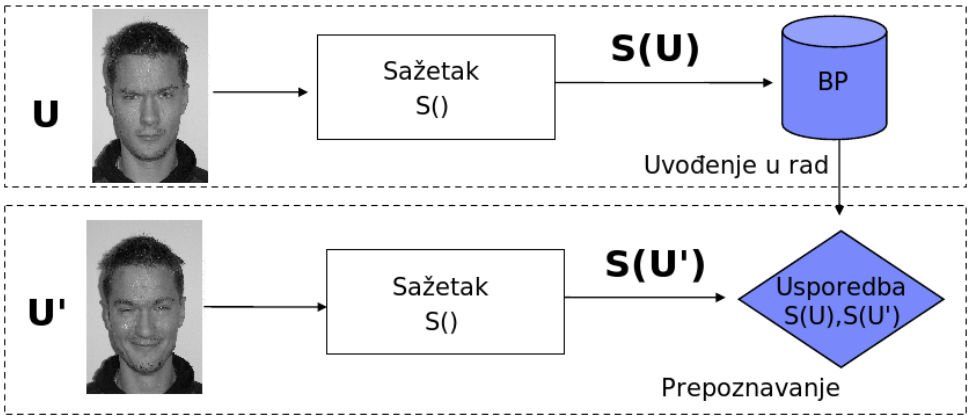
Uvod
Izazovi
Problem privatnosti u biometriji
Usporedba lozinke - biometrijski uzorci
Biometrija u percepciji javnosti
Kako povećati razinu privatnosti?
Biometrija i kriptografija
Biometrijski sažetak
Biometrijska enkripcija
Problemi sa sažimanjem i enkripcijom
Samoispravljajući kodovi
Otkaziva biometrija
BKI
Zaključak

- Potrebno je dati dio sebe koji je jedinstven
- Biometrijsku karakteristiku nije moguće zamijeniti
  - karakteristika nije tajna
  - "jednom kompromitirana, zauvijek kompromitirana"
- Ista karakteristika može biti ključ za različite vrste usluga (cross matching)
  - što ako netko iskoristi Vaše podatke iz jedne aplikacije kako bi dobio pristup drugoj (povijest bolesti, povijest financijskih transakcija, kriminalni i prekršajni dosijer)?

Je li moguće pronaći način jednostavne zamjene biometrijskih uzoraka, kao što je to s lozinkama ili kreditnim karticama?

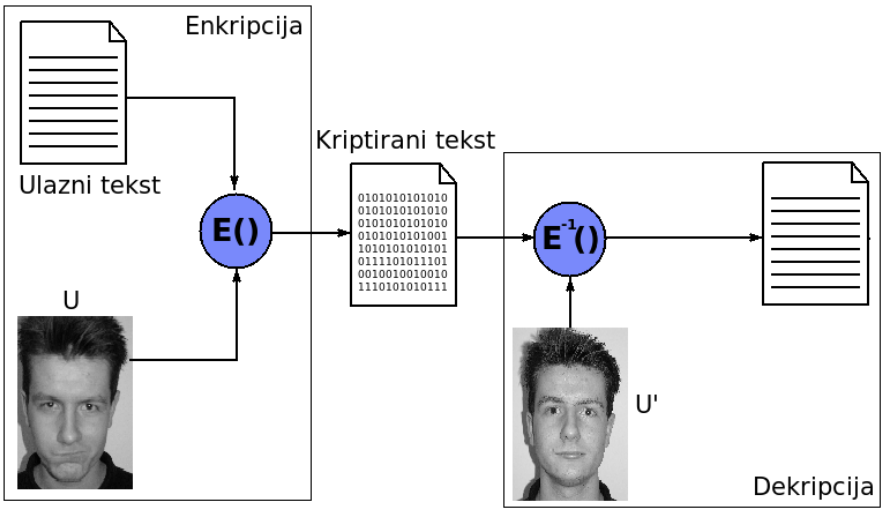
Biometrijski sažetak

Uvod
Izazovi
Problem privatnosti u biometriji
Usporedba lozinke - biometrijski uzorci
Biometrija u percepciji javnosti
Kako povećati razinu privatnosti?
Biometrija i kriptografija
Biometrijski sažetak
Biometrijska enkripcija
Problemi sa sažimanjem i enkripcijom
Samoispravljajući kodovi
Otkaziva biometrija
BKI
Zaključak



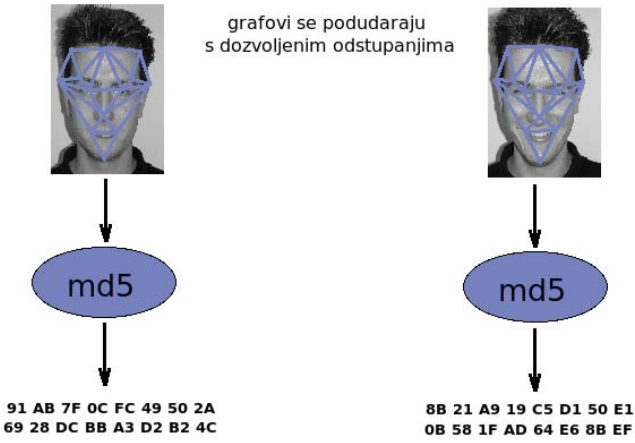
Biometrijska enkripcija

Uvod
Izazovi
Problem privatnosti u biometriji
Usporedba lozinke - biometrijski uzorci
Biometrija u percepciji javnosti
Kako povećati razinu privatnosti?
Biometrija i kriptografija
Biometrijski sažetak
Biometrijska enkripcija
Problemi sa sažimanjem i enkripcijom
Samoispravljajući kodovi
Otkaziva biometrija
BKI
Zaključak



Problemi sa sažimanjem i enkripcijom biometrijskih podataka

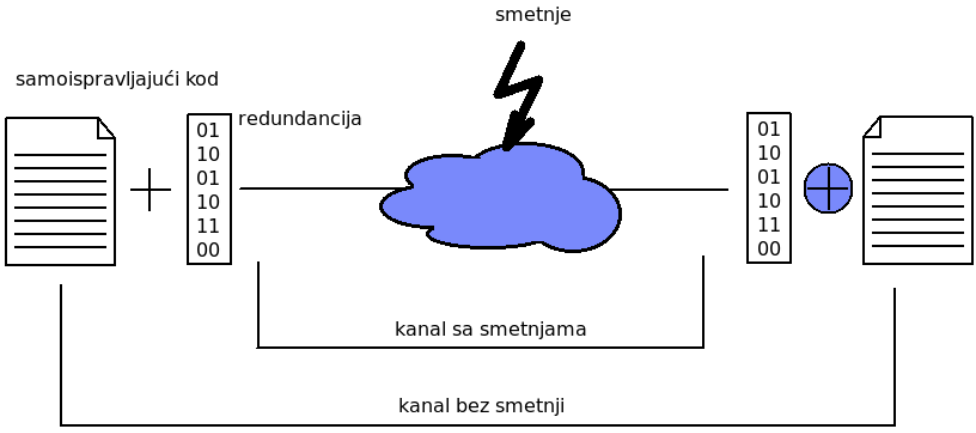
Uvod
Izazovi
Problem privatnosti u biometriji
Usporedba lozinke - biometrijski uzorci
Biometrija u percepciji javnosti
Kako povećati razinu privatnosti?
Biometrija i kriptografija
Biometrijski sažetak
Biometrijska enkripcija
Problemi sa sažimanjem i enkripcijom
Samoispravljajući kodovi
Otkaziva biometrija
BKI
Zaključak



Dovoljna promjena za samo 1b da bi sažetci bili različiti
Kako koristiti biometrijsku karakteristiku kao ključ?

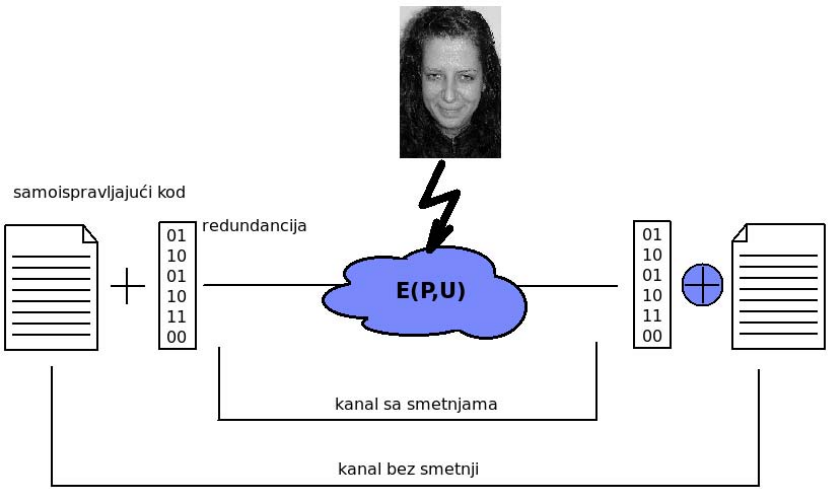
Moguće rješenje – samoispravljajući kodovi

Uvod
Izazovi
Problem privatnosti u biometriji
Usporedba lozinke - biometrijski uzorci
Biometrija u percepciji javnosti
Kako povećati razinu privatnosti?
Biometrija i kriptografija
Biometrijski sažetak
Biometrijska enkripcija
Problemi sa sažimanjem i enkripcijom
Samoispravljajući kodovi
Otkaziva biometrija
BKI
Zaključak



Moguće rješenje – samoispravljajući kodovi

Uvod
Izazovi
Problem privatnosti u biometriji
Usporedba lozinke - biometrijski uzorci
Biometrija u percepciji javnosti
Kako povećati razinu privatnosti?
Biometrija i kriptografija
Biometrijski sažetak
Biometrijska enkripcija
Problemi sa sažimanjem i enkripcijom
Samoispravljajući kodovi
Otkaziva biometrija
BKI
Zaključak



Model

Uvod
Izazovi
Problem privatnosti u biometriji
Usporedba lozinke - biometrijski uzorci
Biometrija u percepciji javnosti
Kako povećati razinu privatnosti?
Biometrija i kriptografija
Biometrijski sažetak
Biometrijska enkripcija
Problemi sa sažimanjem i enkripcijom
Samoispravljajući kodovi
Otkaziva biometrija
BKI
Zaključak

P - Poruka
U - biometrijski uzorak
$S(U)$ - ekstrahirana struktura (ključ)
$EC(P)$ - poruka s dodanom redundancijom
KP – kriptirana poruka
Enkripcija:

$$E(EC(P), S(U)) = KP$$

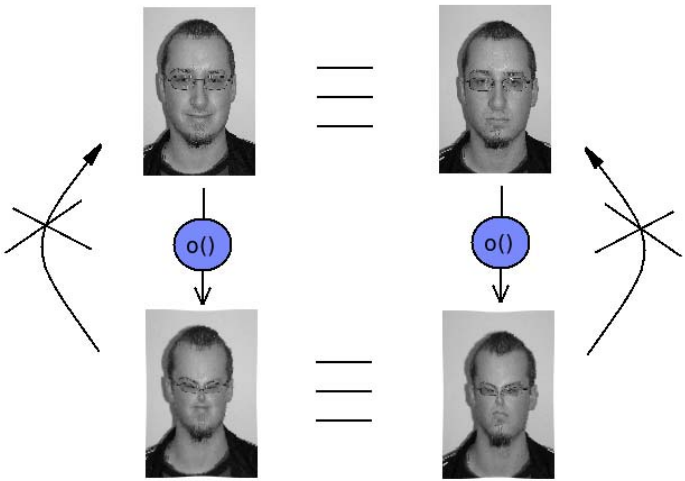
Dekripcija:

$$EC^{-1}(E^{-1}(KP, S(U'))) = P$$

?

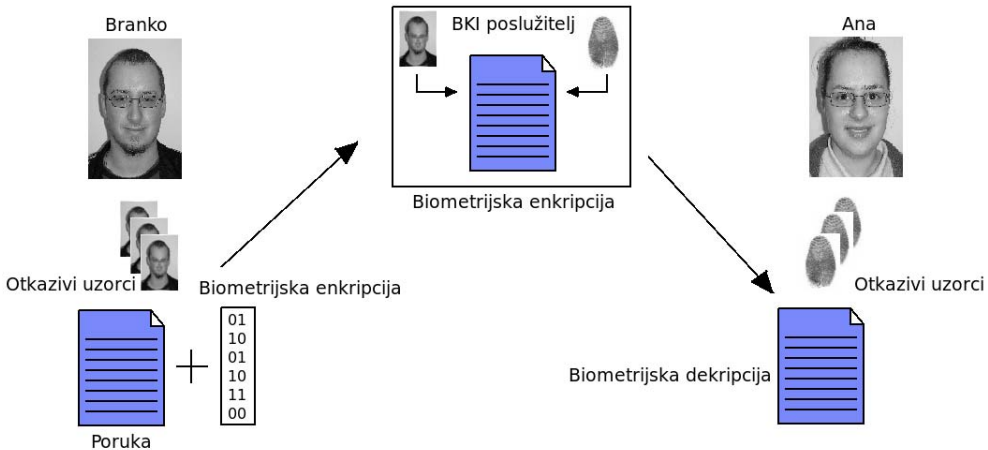
Otkaziva biometrija

Uvod
Izazovi
Problem privatnosti u biometriji
Usporedba lozinke - biometrijski uzorci
Biometrija u percepciji javnosti
Kako povećati razinu privatnosti?
Biometrija i kriptografija
Biometrijski sažetak
Biometrijska enkripcija
Problemi sa sažimanjem i enkripcijom
Samoispravljajući kodovi
Otkaziva biometrija
BKI
Zaključak



Biometric Key Infrastructure

Uvod
Izazovi
Problem privatnosti u biometriji
Usporedba lozinke - biometrijski uzorci
Biometrija u percepciji javnosti
Kako povećati razinu privatnosti?
Biometrija i kriptografija
Biometrijski sažetak
Biometrijska enkripcija
Problemi sa sažimanjem i enkripcijom
Samoispravljajući kodovi
Otkaziva biometrija
BKI
Zaključak



Zaključak

Uvod
Izazovi
Problem privatnosti u biometriji
Usporedba lozinke - biometrijski uzorci
Biometrija u percepciji javnosti
Kako povećati razinu privatnosti?
Biometrija i kriptografija
Biometrijski sažetak
Biometrijska enkripcija
Problemi sa sažimanjem i enkripcijom
Samoispravljajući kodovi
Otkaziva biometrija
BKI
Zaključak

- Biometrija može biti vrlo dobar mehanizam za očuvanje privatnosti korisnika, ali ...
- Biometrijski sažeci, enkripcija, otkazivost uzoraka - obećavajuće tehnologije

HVALA NA POZORNOSTI!

Uvod
Izazovi
Problem privatnosti u biometriji
Usporedba lozinke - biometrijski uzorci
Biometrija u percepciji javnosti
Kako povećati razinu privatnosti?
Biometrija i kriptografija
Biometrijski sažetak
Biometrijska enkripcija
Problemi sa sažimanjem i enkripcijom
Samoispravljajući kodovi
Otkaziva biometrija
BKI
Zaključak

- Pitanja?
- Komentari?
- Kritike?

Mr. sc. Markus Schatten
markus.schatten@foi.hr