Biometrijski sistemi

Biometrics are the oldest form of identification.
Dogs have distinctive barks.
Cats spray.
Humans recognize faces.
On the telephone, your voice identifies you.
Your signature identifies you as the person who signed a contract.

Bruce Schneier

Sadržaj

- Načini autentifikacije i uvod u biometriju
- Generička šema biometrijskog sistema za kontrolu pristupa
- Mere performansi: tačnost i greške biometrijskih sistema
- Primeri ekstrakcije obeležja, generisanja templejta i poređenja (otisak prsta, iris, geometrija lica)
- Napadi na biometrijske sisteme i zaštita
- Poništiva (opoziva) biometrija
- Višemodalni biometrijski sistemi
- Biometrijska kriptografija
- Razvejavanje mitova o biometrijskoj tehnologiji – Dž. Ešburn

Četiri načina autentifikacije

- Četiri načina autentifikacije:
  - nešto što **znamo** (lozinka, PIN)
  - nešto što **imamo** (USB token, ID kartica)
  - nešto što **jesmo** (biometrija zasnovana na fizičkim karakteristikama)
  - nešto što **možemo** (biometrija zasnovana na karakteristikama ponašanja)
- Sve metode imaju prednosti i mane!
  - Primer: **USB token sa ključem**
    - Prednost: ne morate da pamtite lozinku
    - Problem: krađa usb tokena
- Pitanje: prednosti i mane lozinki?

Šta je biometrija?

- Biometrija je skup metoda za identifikovanje pojedinaca na osnovu **fizičkih karakteristika** i/ili **karakteristika ponašanja**.
- Grčki:
  - *bios* – život
  - *metron* – mera
- Biometrijska provera identiteta obuhvata postupke prikupljanja i analize fizičkih karakteristika (na primer, otisci prstiju i snimak irisa) i drugih karakteristika koje se teško mogu oponašati, a skoro jednoznačno identifikuju čoveka (na primer, rukopis).
- Biometrijski uzorci se prikupljaju pomoću specijalnih uređaja, digitalizuju i dalje softverski obrađuju.
  - Primer: otisak prsta je slika koja je nakon obrade predstavljena skupom tačka u dvodimenzionalnom prostoru.

Čime se opisuju biometrijske metode?

- **Jedinstvenost**
  - Koliko posmatrana karakteristika jednoznačno identifikuje pojedinca?
- **Trajnost**
  - Nepromjenjivost biometrijske karakteristike sa vremenom
  - Koliko dugo osoba zadržava navedenu karakteristiku?
- **Prikupljivost**
  - S kojom se lakoćom dobija uzorak navedene karakteristike?
- **Izvodljivost**
  - U kojoj je meri moguće praktično implementirati metode?
- **Prihvatljivost**
  - U kojoj je meri implementacija moguća a da se pri tome ne naruše ljudska prava.

Fizičke karakteristike: otisak prsta

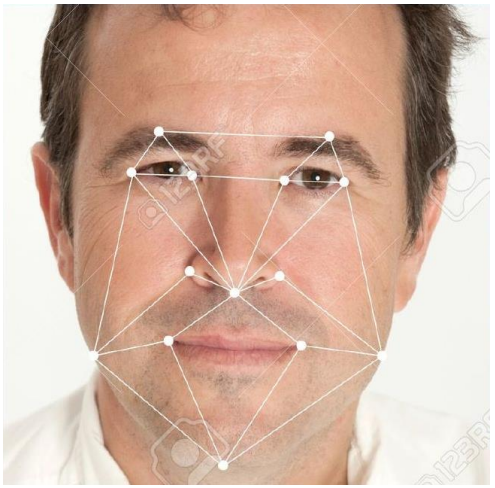
- Jedinstveni za svaki prst svake osobe.
- Formiraju se prenatalno u 8. mesecu trudnoće.
- Mogu se digitalno predstaviti sa određenim brojem tačaka u dvodimenzionalnom prostoru čiji raspored jedinstveno identifikuje osobu.
- Broj tačaka zavisi od primenjenih metoda ekstrakcije obeležja.
- Komercijalno najdostupnija biometrijskih tehnologija (uz verifikaciju lica).
- Postoje relativno jeftini uređaji za prepoznavanje otisaka prstiju.
- Karakteristike:
  - Jedinstvenost: visoka
  - Trajnost: visoka
  - Prikupljivost: osrednja
  - Izvodljivost: visoka
  - Prihvatljivost: osrednja

Fizičke karakteristike: iris

- Irisi jednojačanih blizanaca se znatno više razlikuju od njihove DNK!
- Šara irisa je haotična!
- Stabilan od 4-te godine (do tada se menja pigmentacija).
- Skeniranje irisa obavlja se pomoću namenskih kamera (mogu biti skupe).
- Dobijena slika se obrađuje pomoću relativno složenih algoritama.
- Iris se opisuje pomoću takozvanog iris koda.
- Tehnologija se koristi za identifikaciju osoba koje ulaze u prostorije od značaja (npr. skeniranje je obavezno je pri ulasku u Google Datacenter)
- Karakteristike:
  - Jedinstvenost: visoka
  - Trajnost: visoka (posle 4-te god.)
  - Prikupljivost: niska
  - Izvodljivost: visoka
  - Prihvatljivost: niska

Fizičke karakteristike: lice

- Jeftinija metoda biometrijske identifikacije / verifikacije.
- Ne zahteva skupu specijalnu opremu.
- Može se obaviti na računaru s kvalitetnijom video-kamerom, a za samo prepoznavanje zadužen je softver.
- Metode identifikacije / verifikacije mogu biti geometrijske (izdvajaju se karakteristične tačke lica) ili fotometrijske (filtriranje, PCA).
- Karakteristike:
  - Jedinstvenost: osrednja
    (problemi: promenljivost imidža, plastična hirurgija)
  - Trajnost: osrednja
  - Prikupljivost: visoka
  - Izvodljivost: osrednja
  - Prihvatljivost: visoka



Ponašajne karakteristike

- Prepoznavanje glasa
- Prepoznavanje rukopisa ili potpisa
- Prepoznavanje dinamike kucanja po tastaturi

	Glas	Rukopis	Din. kucanja
Jedinstvenost	Niska	Niska	Niska
Trajnost	Niska	Niska	Niska
Prikupljivost	Osrednja	Visoka	Osrednja
Izvodljivost	Niska	Niska	Niska
Prihvatljivost	Visoka	Visoka	Osrednja

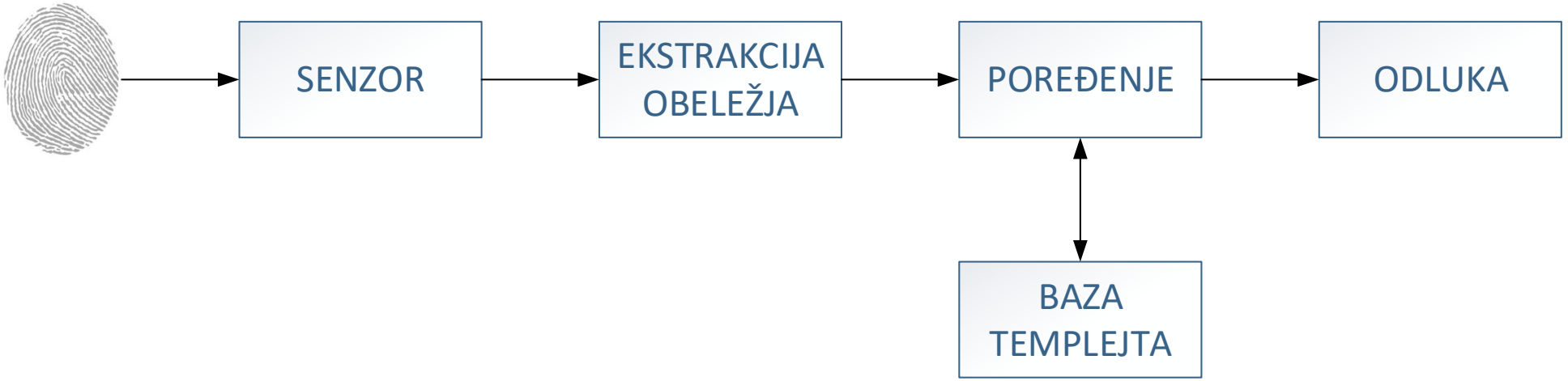
- Primetite da jedinstvenost i trajnost nameću nivo izvodljivosti!

Biometrija, fizička sigurnost i privatnost

- Dva aspekta u društvu stvaraju oprečna mišljenja o primeni biometrije.
- **Fizička sigurnost**.
  - Postoje mišljenja da biometrijske metode u nekim slučajevima mogu da dovedu do povređivanja korisnika.
  - 2005. godine kradljivci automobila u Maleziji odsekli su vlasniku prst u pokušaju da ukradu automobil, za čije je pokretanje bilo neophodno očitati otisak prsta.
- **Privatnost**.
  - Prikupljeni biometrijski podaci mogu se kasnije upotrebiti bez znanja I odobrenja korisnika, prodati trećem licu i slično.
  - Ovo narušava privatnost i može se iskoristiti za lažiranje pri izvođenju ilegalnih operacija.
  - Problem je rešiv upotrebom:
    - **Poništive biometrije** (engl. *cancelable biometrics*).
    - **Homomorfnog šifrovanja** (jako sporo, dva iris koda 1024bita na 2GHz CPU se porede 9.5min ukoliko se koristi homomorfni RSA)
    - Kombinovanim tehnikama: kriptografija sa javnim ključem, PRNG i ECC.

Generička šema biometrijskog sistema

- Generički sistem za biometrijsku kontrolu pristupa sastoji se od sledećih komponenti:
  - **Senzor** (engl. *sensor*)
  - Modula za **ekstrakciju obeležja** (engl. *feature extractor*)
  - Modula za **poređenje** (engl. *matcher*)
  - **Baza podataka** o identitetima korisnika i odgovarajućim biometrijskim templejtima (engl. *stored templates*).



Faza upisa (*Erollment*)

- Da bi biometijski sistem za kontrolu pristupa uopšte mogao da funkcioniše, korisnik mora da priloži svoj identitet i da mu se očita biometrijski uzorak.
  1. Korisnik navodi svoj identitet.
  2. Korisnik prilaže biometrijski uzorak senzoru. Senzor očitava uzorak.
  3. *Feature extractor* izdvaja **obeležja** i generiše biometrijski **templejt**.
  4. Templejt se čuva u bazi podataka.
- Procedura je slična kreiranju korisničkih naloga na računaru!
  1. Korisniku se kreira nalog (odgovara identitetu).
  2. Korisnik unosi lozinku (odgovara biometrijskom uzorku).
  3. Računa se heš lozinke (odgovara generisanju biometrijskog templejta)
  4. Heš se čuva u bazi podataka.

Razlika između uzorka i templejta

- **Biometrijski uzorak** je ono što prilažete skeneru.
  - Primer: slika otiska prsta, zvučni zapis.
- **Templejt** nastaje kao rezultat složenih matematičkih operacija i algoritama koje je *feature extractor* izveo nad snimkom uzorka.
  - Primer: vektor tačaka predstavljenih *x* i *y* koordinatama, iris kod.
  - Veličina templejta zavisi od modaliteta, metoda i parametara izdvajanja obeležja!

Verifikacija korisnika

- Prilikom verifikacije korisnika, biometrijski sistem funkcioniše na sledeći način:
  1. Korisnik koji želi da pristupi određenim resursima navodi svoj identitet.
  2. Senzor prikuplja biometrijski uzorak korisnika.
  3. Iz uzorka se izdvajaju atributi i formira vektor obeležja.
  4. Računa sličnost između generisanog templejta i templejta smeštenog u bazi podataka koji odgovara navedenom identitetu.
  5. Na osnovu dozvoljene granice greške sistem donosi odluku, tj. određuje da li je to zaista taj korisnik i shodno odluci dozvoljava ili blokira pristup resursima.
- U slučaju biometrijske verifikacije generisani templejt se **poredi sa tačno jednim** templejtom u bazi!

Identifikacija korisnika

- Prilikom identifikacije korisnika, biometrijski sistem funkcioniše na sledeći način:
  1. Korisnik koji želi da pristupi određenim resursima prilaže svoje biometrijski uzorak senzoru
  2. Iz uzorka se izdvajaju atributi i formira vektor obeležja.
  3. Računa sličnost između generisanog templejta i SVIH templejta smeštenih u bazi podataka.
- U slučaju biometrijske verifikacije generisani templejt se **poredi sa SVIM templejtima u bazi**!
- Identifikacija je očigledno skupa po pitanju procesorskog vremena.
- Da bi se proces ubrzao, koriste se tehnike klasifikacije i indeksiranja kako bi se ograničio broj templejta sa kojima se poredi templejt generisan na osnovu priloženog uzorka.

Performanse prilikom upisa

- **FTA** (engl. *Failure to Acquire*) je greška prilikom uzimanja podataka.
  - FTA je procenat korisnika za koje sistem nije u mogućnosti da prezentuje korisne biometrijske uzorke tokom upisa.
  - FTA pokriva FTE i kvalitativno prihvatanje biometrijskih templejta.
- **FTE** (engl. *Failure to Enroll*) je greška koja nastaje prilikom upisa.
  - FTE predstavlja procenat korisnika za koje system nije u mogućnosti da generiše templejt dovoljnog kvaliteta za upis zbog tehnologijom nametnutih ograničenja.
- **TTE** (engl. *Time to Enroll*) nije greška već kvantitativni pokazatelj.
  - TTE označava trajanje procesa upisa od uzimanja biometrijskih uzoraka do kreiranja templejta I smeštanja templejta u bazu.

Performanse u procesu verifikacije

- Biometrijski uzorci, a samim tim i generisani templejt nikada nisu isti.
- Sistem mora da kvantifikuje i proceni sličnost između njih i da na osnovu određenih parametara donese odluku o prihvatanju ili odbijanju.
- **Rezultat poređenja** (engl. *matching score*) $s \in [0,1]$.
- Definiše se **prag prihvatanja** (*threshold*) t.
- Sistemske odluke se donose na osnovu praga prihvatanja.
  - Ako je $s > t$, rezultat je prihvatljiv a **prepoznavanje uspešno**.
  - Ako je $s < t$, rezultat je neprihvatljiv a **prepoznavanje neuspešno**.

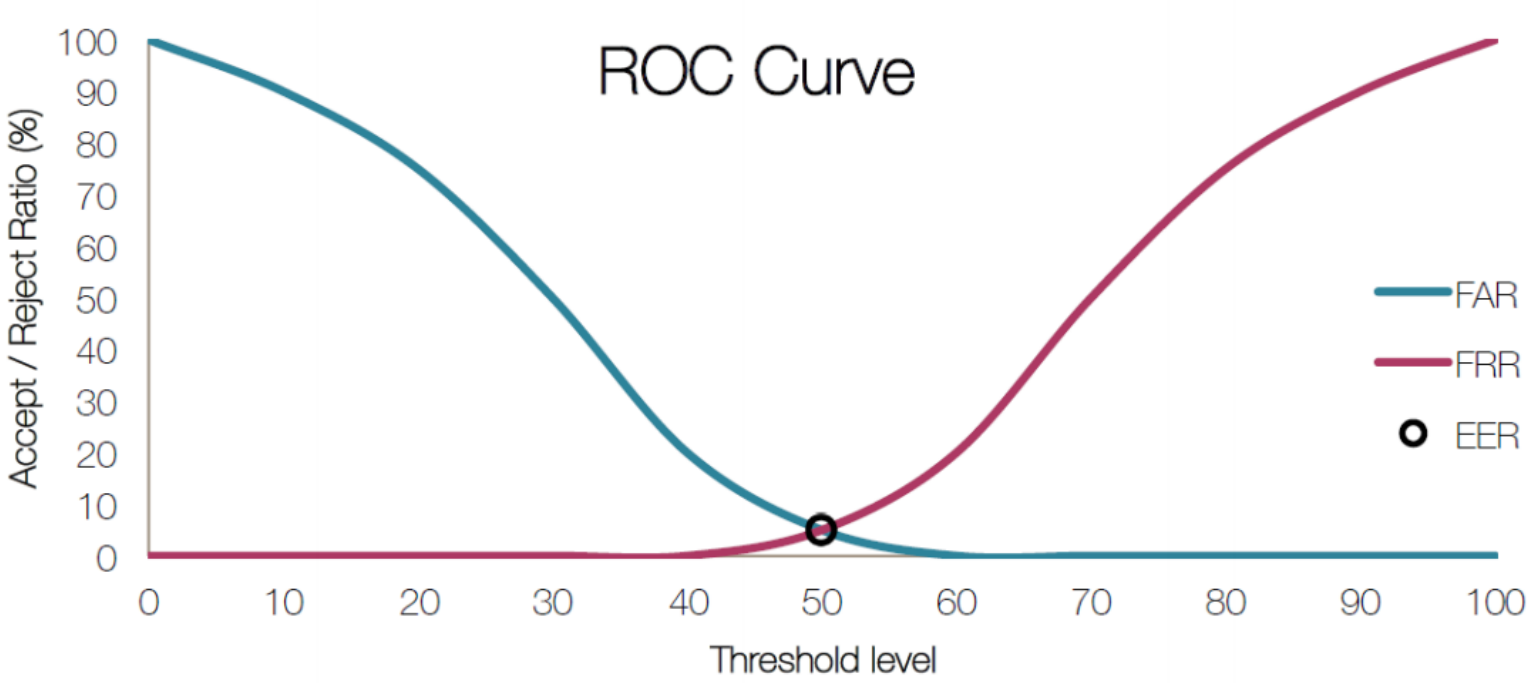
Performanse u procesu verifikacije

- **FRR** (engl. *False Reject Rate*) je **greška odbijanja**.
  - FRR je procenat legitimnih korisnika koje je sistem odbio.
  - FRR = broj legitimnih odbijenih / broj ukupnih legitimnih pokušaja.
  - Rezultat poređenja validnog templejta je ispod granice prihvatanja.
- **FAR** (engl. *False Accept Rate*) je **greška prihvatanja**.
  - FAR je procenat lažnih korisnika koje je sistem prihvatio kao legitimne.
  - FAR = broj lažnih prihvaćenih / broj ukupnih lažnih pokušaja.
  - Rezultat poređenja nevalidnog templejta je iznad granice prihvatanja.

Modalitet	Parametar	FRR	FAR
Otisak prsta	Znatna deformacija kože, rotacija	2%	2%
Crte lica	Izmena osvetljenja	10%	1%
Glas	Nezavistan tekst na više jezika	5-10%	2-5%

Performanse u procesu verifikacije

- **EER** (*Equal Error Rate*) je veza između FAR i FRR, tj. tačka preseka FAR i FRR.
- Formalno: **EER = *t***, na mestu gde FAR = FRR.
- Pitanje: gde je prihvatljiviji veći FAR, a gde veći FRR?



Performanse u procesu identifikacije

- Neka je *T* sačuvani biometrijski templejt neke osobe, *I* prikupljeni biometrijski uzorak.
- Postoje dve hipoteze:
  - H0: $I \neq T$, ulaz ne odgovara templejtu
  - H1: $I = T$, ulaz odgovara templejtu
- Asocirane odlule:
  - D0: osoba nije ona za koju tvrdi da jeste
  - D1: osoba je ona za koju tvrdi da jeste
- **Greška I vrste** (engl. *False Match*): doneta odluka D1, tačna hipoteza H1
- **Greška II vrste** (engl. *False Non-Match*): doneta odluka D0, tačna hipoteza H2
- Verovatnoće pojave grešaka prve i druge vrste:

  FMR = P (D1 | H0 = true)

  FNMR = P (D0 | H1 = true)

Performanse u procesu identifikacije

- Pretpostavka: baza sadrži N templejta, a za svakog korisnika postoji samo jedan templejt u bazi.
- Tada važi:
  - $FNMR_N = FNMR$
  - $FMR_N = 1 – (1 – FMR)^N$
  - Ako je FMR malo, FNMR se aproksimira kao N x FMR, što znači da verovatnoća greške raste linearno sa veličinom baze.
- Na primer, za bazu sa 10000 templejta i prihvatljivo FNMR i FMR od 10^{-5}, FMR_N iznosi oko 10% što je apsolutno neprihvatljivo!
- Ako su templejti klasifikovani / indeksirani, pretražuje se deo baze.
- Neka je **RER** (engl. *Retrieval Error Rate*) verovarnoća da je povučen pogrešan templejt, a P procenat baze koji se pretražuje.
  - $FNMR_N = RER + (1 – RER)\ FNMR$
  - $FMR_N = 1 – (1 – FMR)^{NP}$

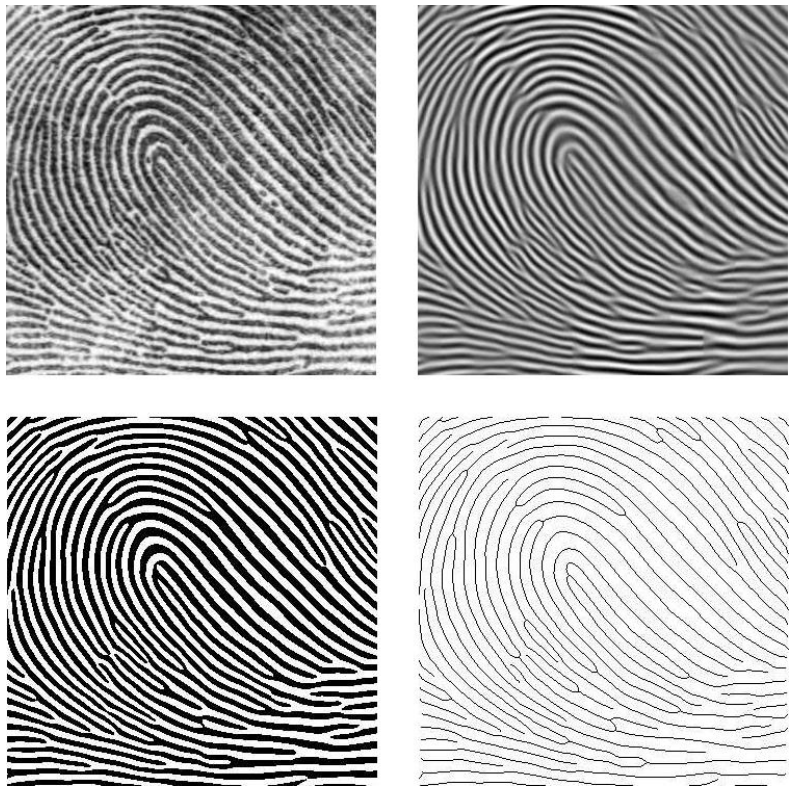
Otisak prsta

- Koraci u izdvajanju tačaka (jedan od standardnih algoritama):

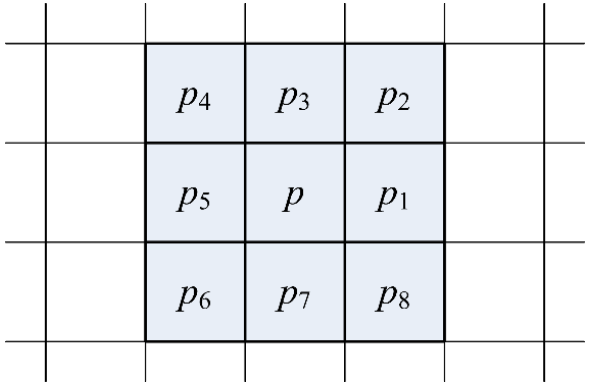
1. Histogram EQ (pojačanje lokalnog kontrasta slike)
2. Wiener filter (uklanja se blur i aditivni šum)
3. Segmentacija (izdvajanje regiona od interesa od ostatka slike)
4. Procena orijentacije (pomoću gradijent vektora)
5. Filtriranje Gaus low-pass filtrom
6. Filtriranja 2-D Gabor filtrom
7. Binarizacija slike
8. Primena morfoloških operatora
9. Algoritam stanjivanja linija
10. Određivanje *ridge ending* (*termination*) i *valley ending* (*bifurscation*) tačaka

Otisak prsta

- Originalna slika (gore levo), filtrirana slika (gore desno), binarizovana slika (dole levo) i slika sa utanjenim linijama (dole desno).



- Kako se na utanjenoj slici (linije debljine jednog piksela) uočavaju karakteristične tačke?
- Posmatra se piksel *p* okružen sa osam susednih piksela.

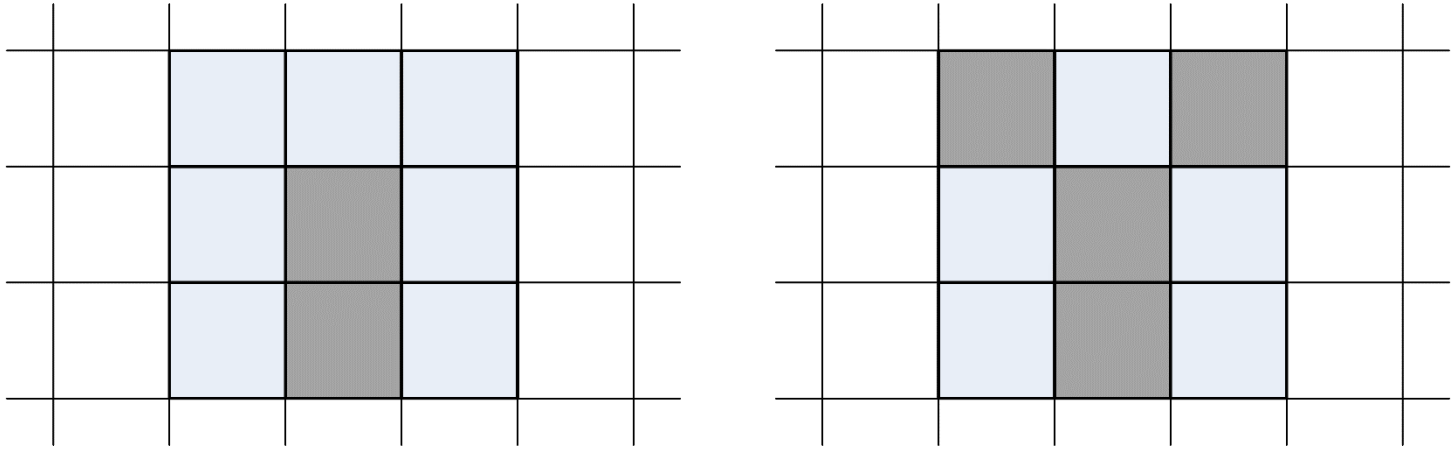


- Za dati piksel računa se tzv. "*Crossing number*" po definiciji Rutowitza kao broj tranzicija sa belog na crno polje i obrnuto.

$$X_R(p) = \sum_{i=1}^{8} |p_{i+1} - p_i|$$

Otisak prsta

- Piksel *p* je identifikovan kao *ridge termination point* ako je X_R (*p*) = 2 (levo).
- Piksel *p* je identifikocan *bifurscation point* ako je X_R (*p*) = 6 (desno).



Otisak prsta

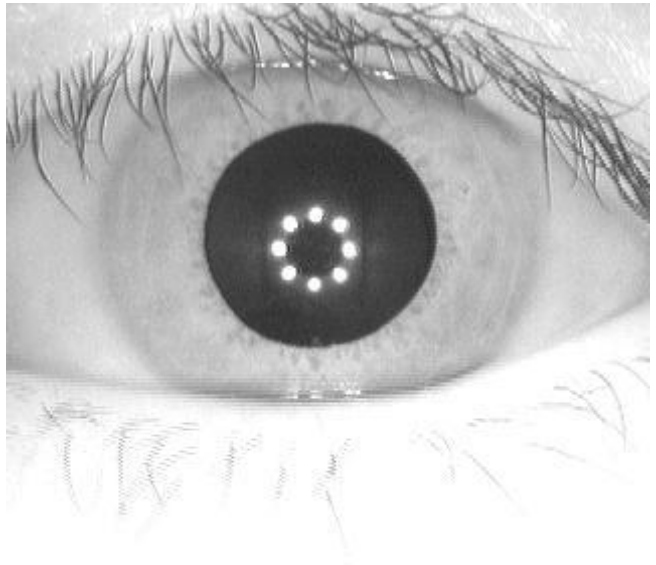
- Templejt otiska prsta je dat dvodimenzionalnim vektorom koji sadrži koordinate identifikovanih tačaka.

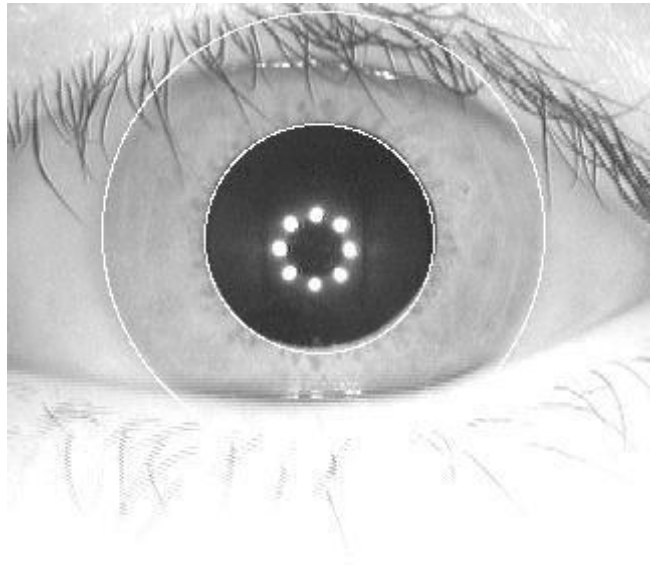
$$F = \left\{ \left(x_1, y_1 \right), \left(x_2, y_2 \right), \ldots, \left(x_n, y_n \right) \right\}$$

- Prilikom poređenja generisanog templejta sa templejtom sačuvanim u bazi:
  1. odbacuju se tačke koje nedostaju,
  2. računa se zbirno odstojanje između neodbačenih tačaka,
  3. rastojanje se deli sa brojem neodbačenih tačaka,
  4. rezultat se poredi sa pragom prihvatanja.

Iris

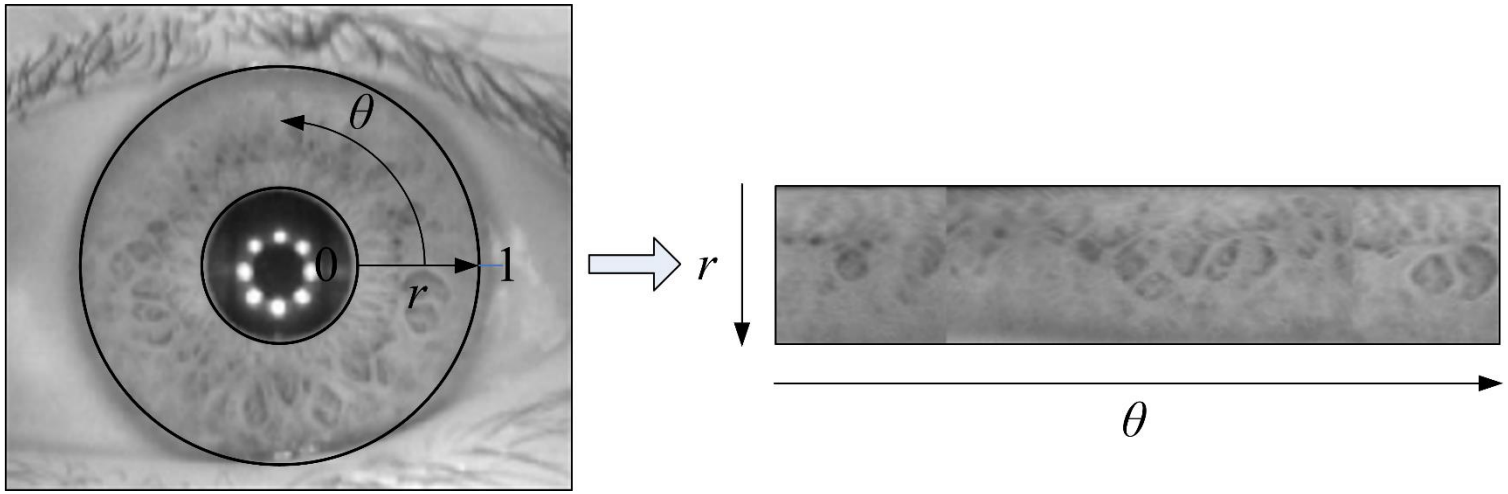
- Slika se pretprocesira i uzima se *gray-scale* slika.
- Lokalizacija irisa (Hough transform + Canny edge detector).





Iris

- Normalizacija irisa (tzv. *Daugman rubber-sheet model*).



- Šara irisa je prilično “haotična”.
- Iris kod se dobija primenom se 1-D log Gabor ili 2-D wavelet transformacijom na normalizovani iris.

Preuzeto iz [3]

Iris

- Merenje sličnosti irisa zasniva se na **Hamming-ovom rastojanju**.
- Hamingovo rastojanje $d(x,y)$ kao količnik broja ne poklapajućih bita sa ukupnim brojem bita koji se porede.
- Na primer:
  - $d(0010, 0101) = 3/4$
  - $d(101111, 101001) = 2/6$
- Računa se d(x,y) na za generisani iris kod i iris kod koji se čuva u bazi templejta.
  - Perfektno poklapanje daje rastojanje d(x,y) = 0.
  - Za identičan iris, očekivano rastojanje je 0.08.
  - Poklapanje se prihvata, ako je rastojanje manje od 0.32.
  - Za slučajne nizove, očekivano rastojanje je 0.50.

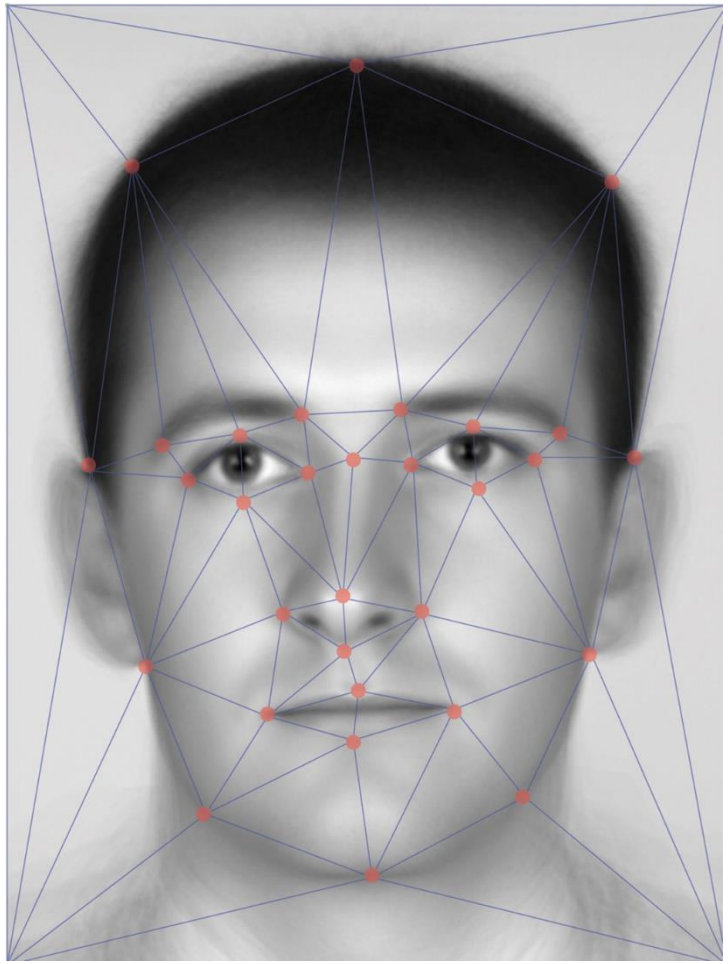
Geometrija lica

- Karakteristike lica koje se mogu meriti i koristiti za kasniju identifikaciju / verifikaciju nazivaju se **ključni detalji**.
- Na licu postoji oko 80 ključnih detalja, a neki su:
  - rastojanje između očiju,
  - širina nosa,
  - dubina očnih udubljenja,
  - jagodice,
  - vilična linija,
  - brada.
- Ključni detalji se mere i formira se numerički kod koji predstavlja lice u bazi templejta.
  - Ova predstava se naziva tzv. ***faceprint***.
- Faza upisivanja traje oko 10-30 sekundi i tokom nje se uzima veći broj slika, poželjno iz blago različitih uglova.
- Nakon toga se izdvajaju karakteristične osobine i kreira *faceprint*.

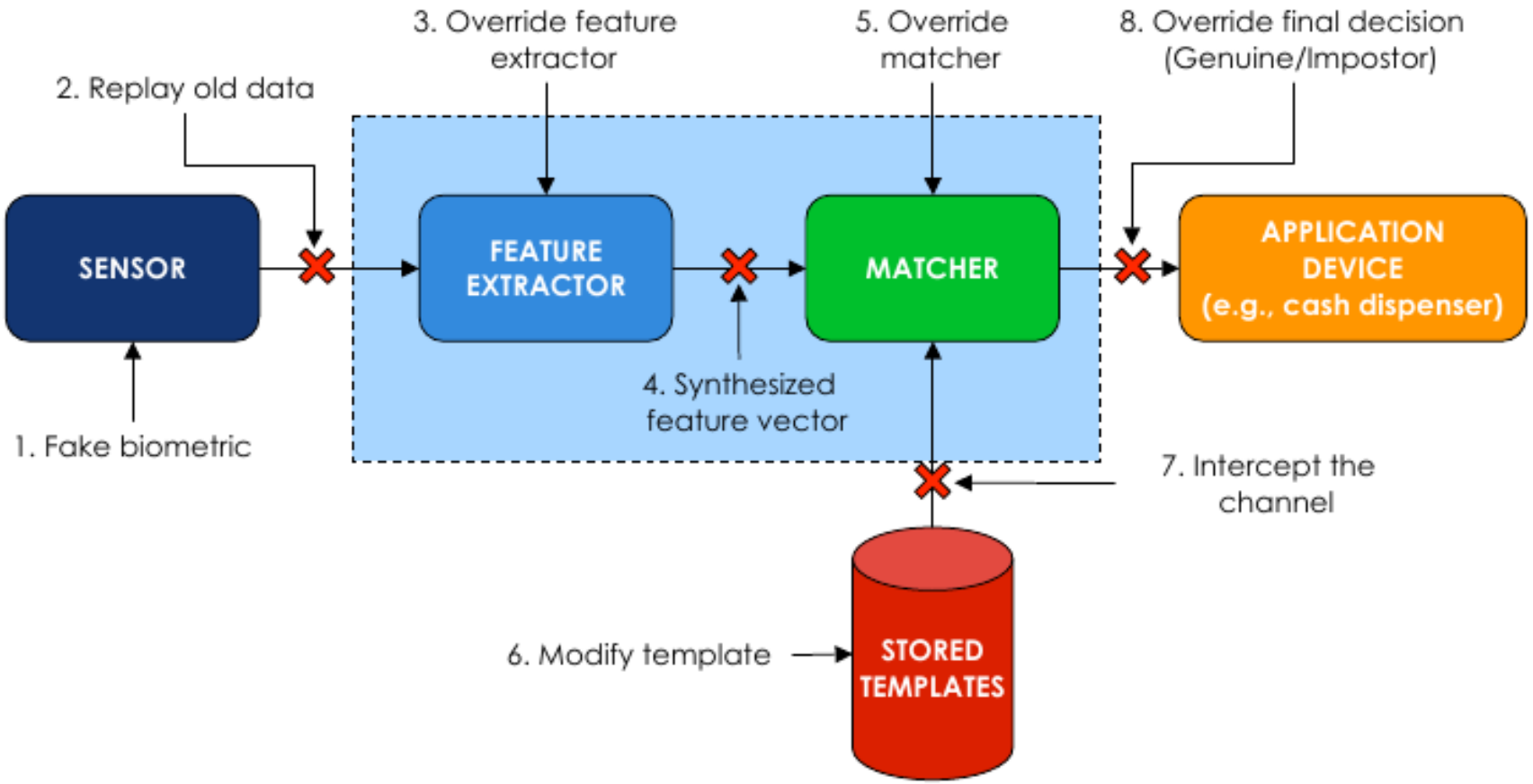
Geometrija lica

- Faze u algoritmima za prepoznavanje lica na osnovu geometrije:
  1. **Detekcija** (traženje lica u polju vidljivosti kamere).
  2. **Podešavanje**.
     - Određivanje pozicije, veličine i orijentacije glave.
     - Prevođenje 3D u 2D nefrontalnu sliku.
     - Prevođenje 2D nefrontalne u 2D frontalnu sliku.
  3. **Normalizacija**.
     - Primena statističkih tehnika kojima vrši korekcija razlika u licu iste osobe na različitim slikama.
     - Time se umanjuju razlike između različitih lica.
  4. **Kodiranje** (prevođenje ključnih detalja sa normalizovane 2D frontalne slike u jedinstveni digitalni kod).
  5. **Poređenje** sa drugim raspoloživim kodovima u bazi podataka.

Geometrija lica



Napadi na biometrijske sisteme i zaštita



Preuzeto iz [4]

Napadi na biometrijske sisteme i zaštita

- *Fake biometrics.*
  - Napadač prilaže lažni biometrijski uzorak senzoru.
  - ZAŠTITA: *liveness detector*.
- *Replay old data.*
  - Napadač prosleđuje snimljeni signal sa izlaza senzora ostatku sistema.
  - ZAŠTITA: šifrovanje veze *sensor – feature extractor*.
- *Override feature extractor.*
  - Napadač upotrebljava zlonamerni softver kako bi kompromitovao *feature extractor*; modul generiše vektore koje odabira napadač.
  - ZAŠTITA: *anti-malware*.
- *Synthetic feature vector.*
  - Napadač prosleđuje sintetički vektor *matcher*-u.
  - ZAŠTITA: šifrovanje veze *extractor – matcher* ili realizacija u vidu jednog modula.

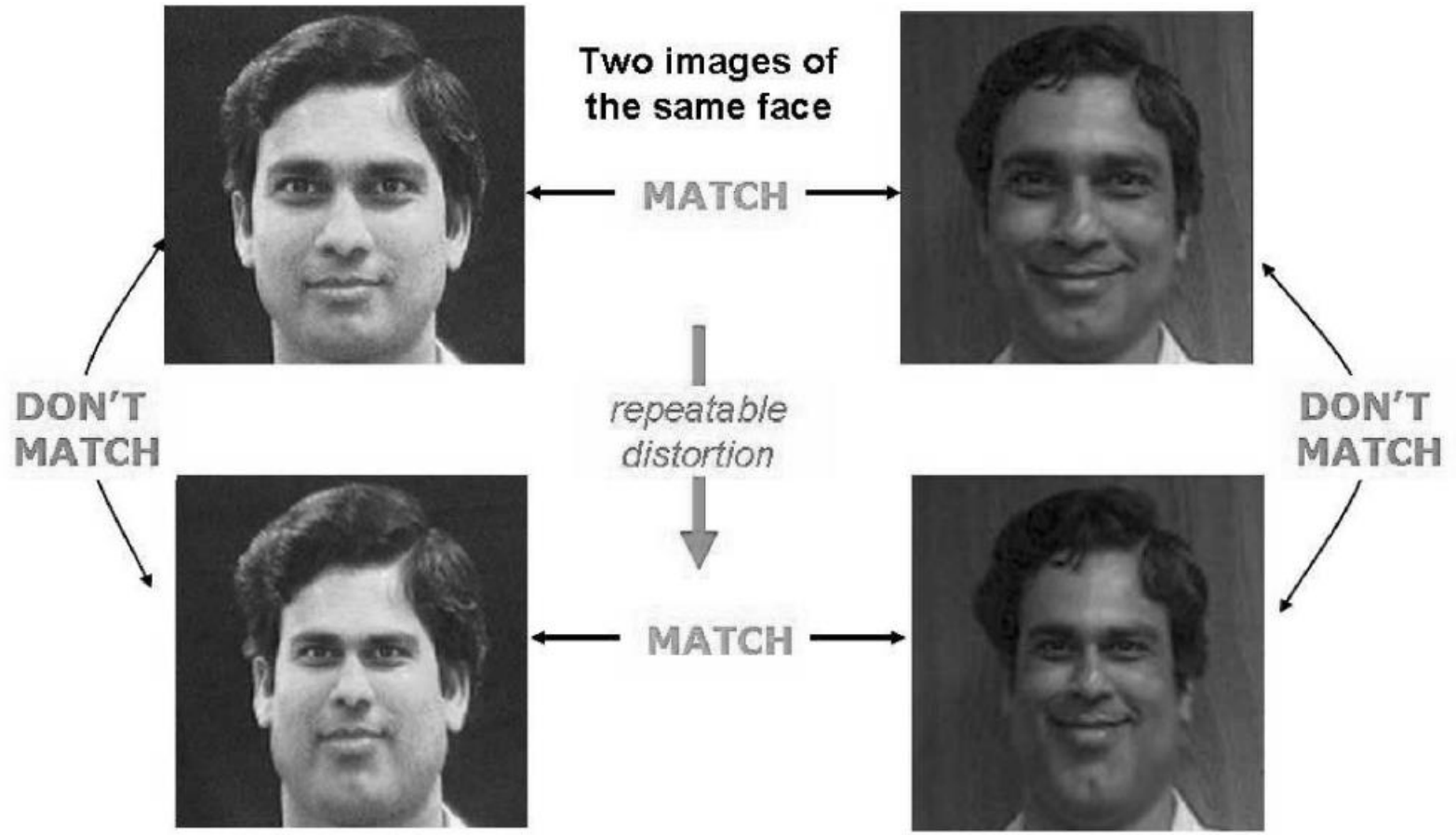
Napadi na biometrijske sisteme i zaštita

- *Override matcher.*
  - Napadač modifikuje rezultat koji generiše modul za poređenje.
  - ZAŠTITA: smeštanje *matcher*-a na zaštićenu lokaciju.
- *Modify template.*
  - Napadač modifikuje biometrijske uzorke legitimnih korisnika u bazi podataka, stiče pristup. DoS legitimnim korisnicima.
  - ZAŠTITA: smeštanje tamplate baze na zaštićenu lokaciju.
- *Intercept the channel.*
  - Napadač presreće komunikacioni kanal između baze podataka i modula za poređenje i podmeće lažne uzorke modulu za poređenje.
  - ZAŠTITA: šifrovanje veze *matcher – database*.
- *Override final decision.*
  - Napadač stiče administrativne privilegije i menja konačnu odluku sistema.

Poništiva biometrija

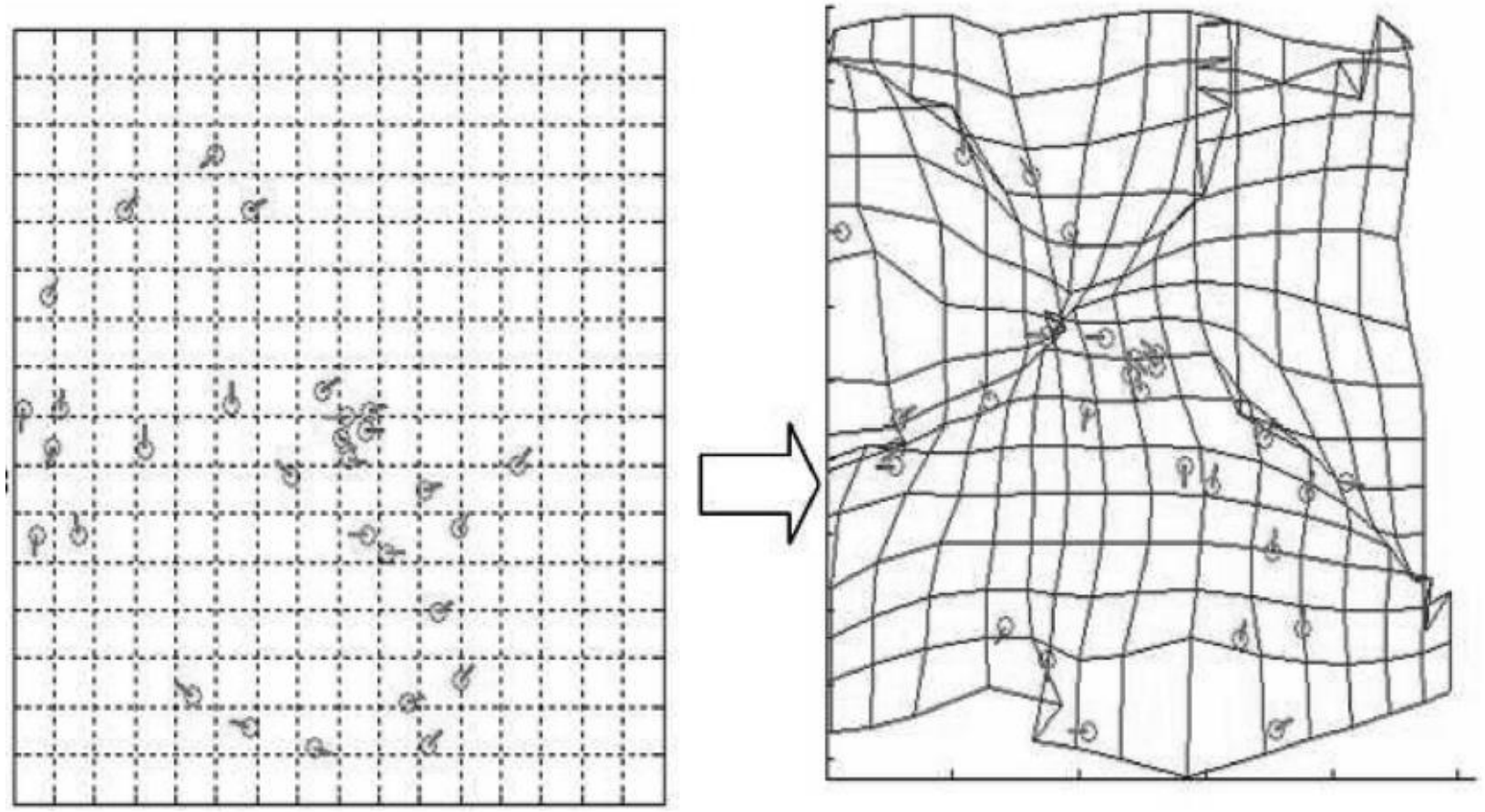
- **Poništiva (opoziva) biometrija** se odnosi na nanošenje jednosmernih, tj. **neinvertibilnih transformacija** biometrijskim obeležjima kako bi se zaštitila privatnost.
- Ukoliko je poništiv templejt kompromitovan, može se promeniti karakteristika neinvertibilne transformacije (na primer, ključ), novi templejt se ponovo generiše izmenjenom transformacijom.
- Algoritam koji generiše poništive biometrijske templejte mora da obezbedi:
  - ponovnu upotrebu u slučaju da nije došlo do kompromitovanja,
  - povlačenje uzoraka u slučaju kompromitovanja,
  - neinvertibilnost, tj sprečavanje generisanja originalnih biometrijskih podataka na osnovu templejta,
  - ne sme znatno da degradira performanse prilikom poređenja, tj ne sme znatno da uveća grešku.

Poništiva biometrija



Preuzeto iz [5]

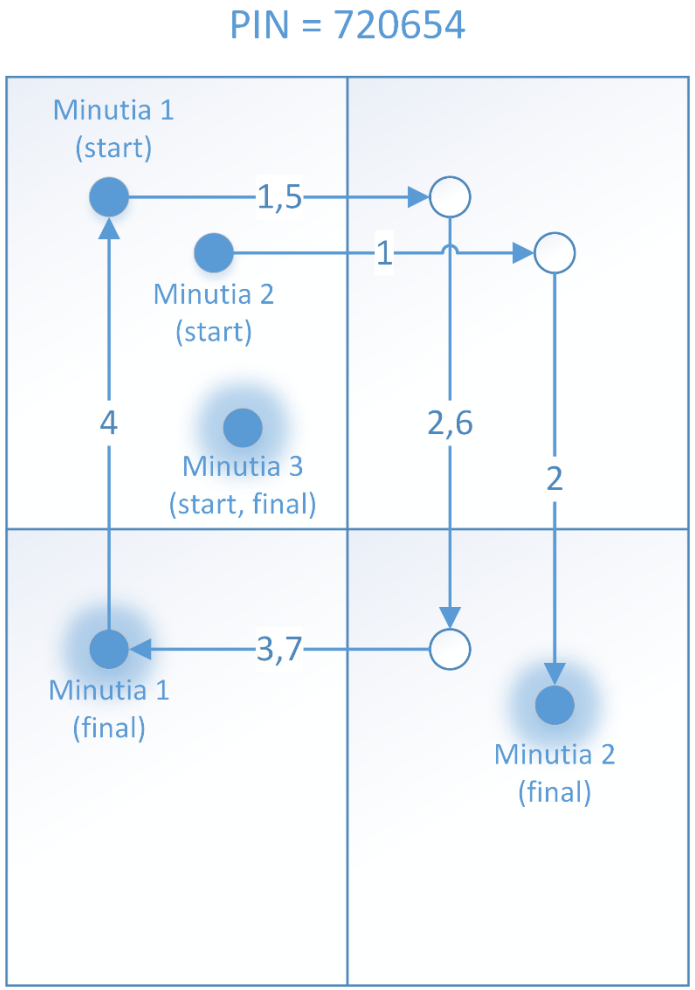
Poništiva biometrija



Preuzeto iz [5]

Poništiva biometrija (primer transformacije sa ključem)

- Primer transformacije sa ključem:
  - podeli koordinatni system na 4x4,
  - svaku tačku u smeru kazaljke na satu pomeri u susedno polje onoliko puta koliko je naznačeno pinom,
  - relativne pozicije ne menjaj,
  - kreni od tačke u gornjem levom uglu i završi sa tačkom u donjem desnom uglu.
- Pitanje: koliko je potrebno za napad grubom silom (engl. *brute-force*) da dođete do originalnog templejta ukoliko:
    - 1. znate dužinu PIN-a,
    - 2. ne znate dužinu PIN-a?



Višemodalni biometrijski sistemi

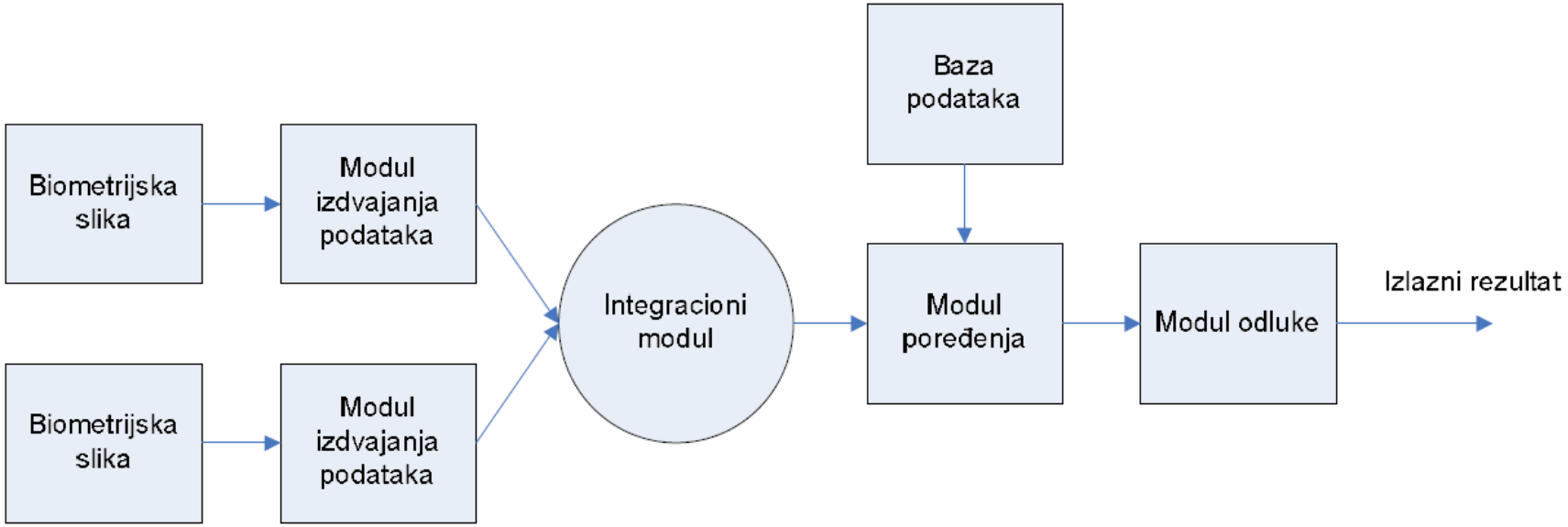
- Višemodalna biometrija zasnovana je na sjedinjavanju biometrijskih karakteristika sa **više izvora**.
- Ti izvori mogu biti:
  - više **senzora** (npr. tri kamere snimaju lice),
  - više **modaliteta** (npr. iris i otisak prsta),
  - više **snimaka iste biometrijske karakteristike** (više snimak istog irisa),
  - više **uzoraka iste biometrijske karakteristike** (uzimanje otisaka dva ili više prsta),
  - više **načina obrade istog biometrijskog podatka**.
- Istraživanja u oblasti višemodalne biometrije je uglavnom fokusirano na **sjedinjavanje više modaliteta na nivou obeležja**.
- Dizajn višemodalnog sistema zavisi od toga:
  - koji će se modaliteti sjediniti,
  - broja modaliteta,
  - načina na koji će se sjediniti.

Višemodalni biometrijski sistemi

- Osnova višemodalne biometrije je **sjedinjavanje informacija**.
- Sjedinjavanje se može grubo kategorisati na:
  - sjedinjavanje **pre poređenja**,
  - sjedinjavanje **posle poređenja**.
- Sjedinjavanje **pre poređenja** izvodljivo je na:
  - nivou **senzora**,
  - nivou **modula za izdvajanje obeležja**.
- Sjedinjavanje **posle poređenja** izvodljivo je na:
  - nivou **modula poređenja**,
  - nivou **donošenja odluke**.

Višemodalni biometrijski sistemi

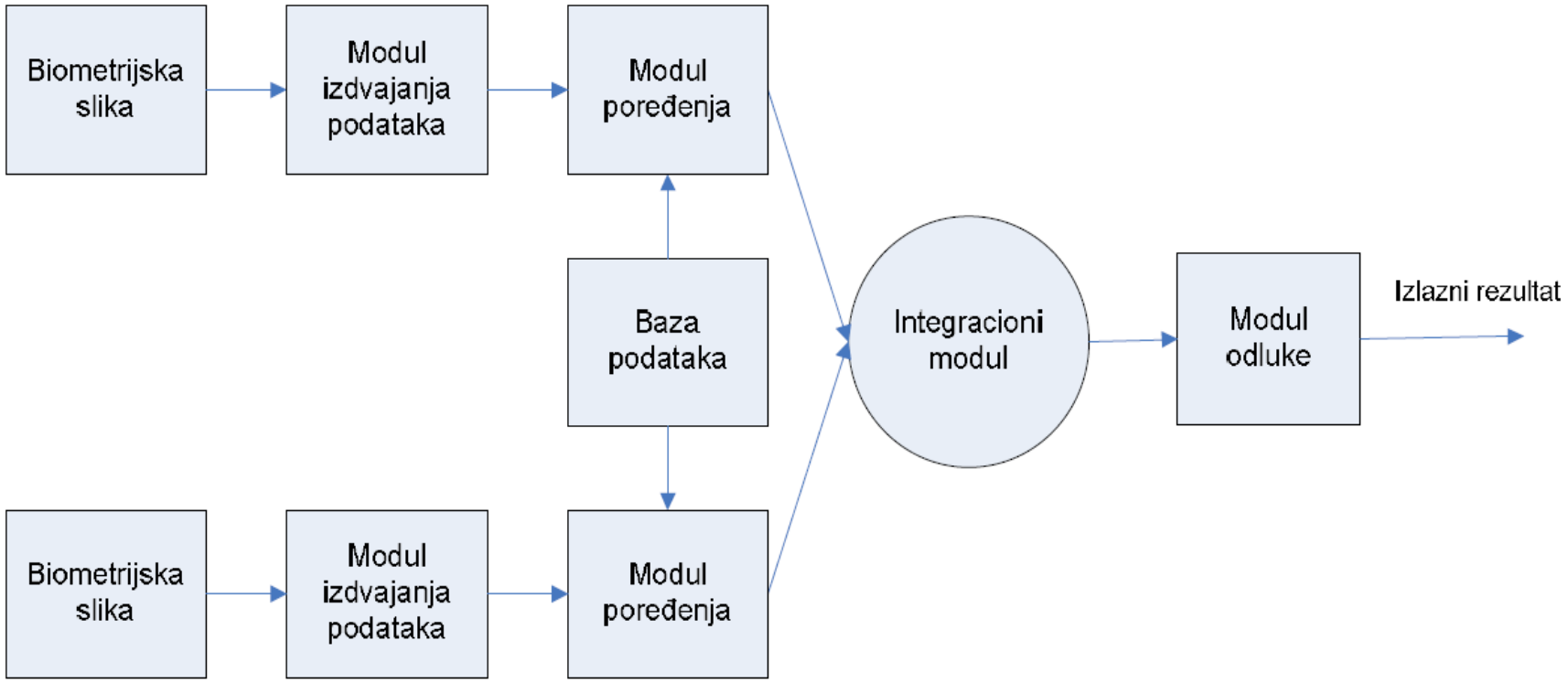
- Sjedinjavanje na nivou modula za izdvajanje obeležja.
- Problemi:
  - nekompatibilnost vektora (npr. iris kod i tačke templejta otiska prsta),
  - dobijanje vektora visoke dimenzionalnosti.



Slika preuzeta iz [7]

Višemodalni biometrijski sistemi

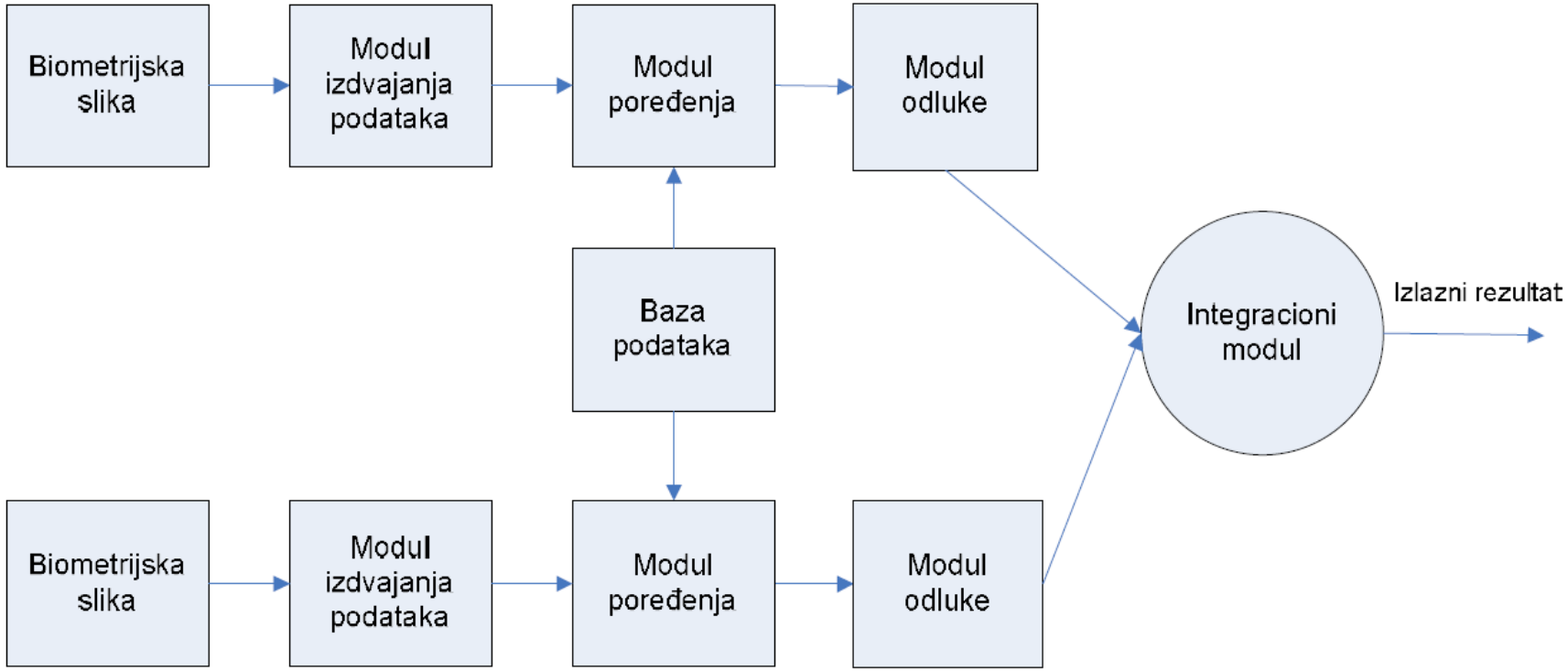
- Sjedinjavanje na nivou modula poređenja.



Slika preuzeta iz [7]

Višemodalni biometrijski sistemi

- Sjedinjavanje na nivou modula odluke.



Slika preuzeta iz [7]

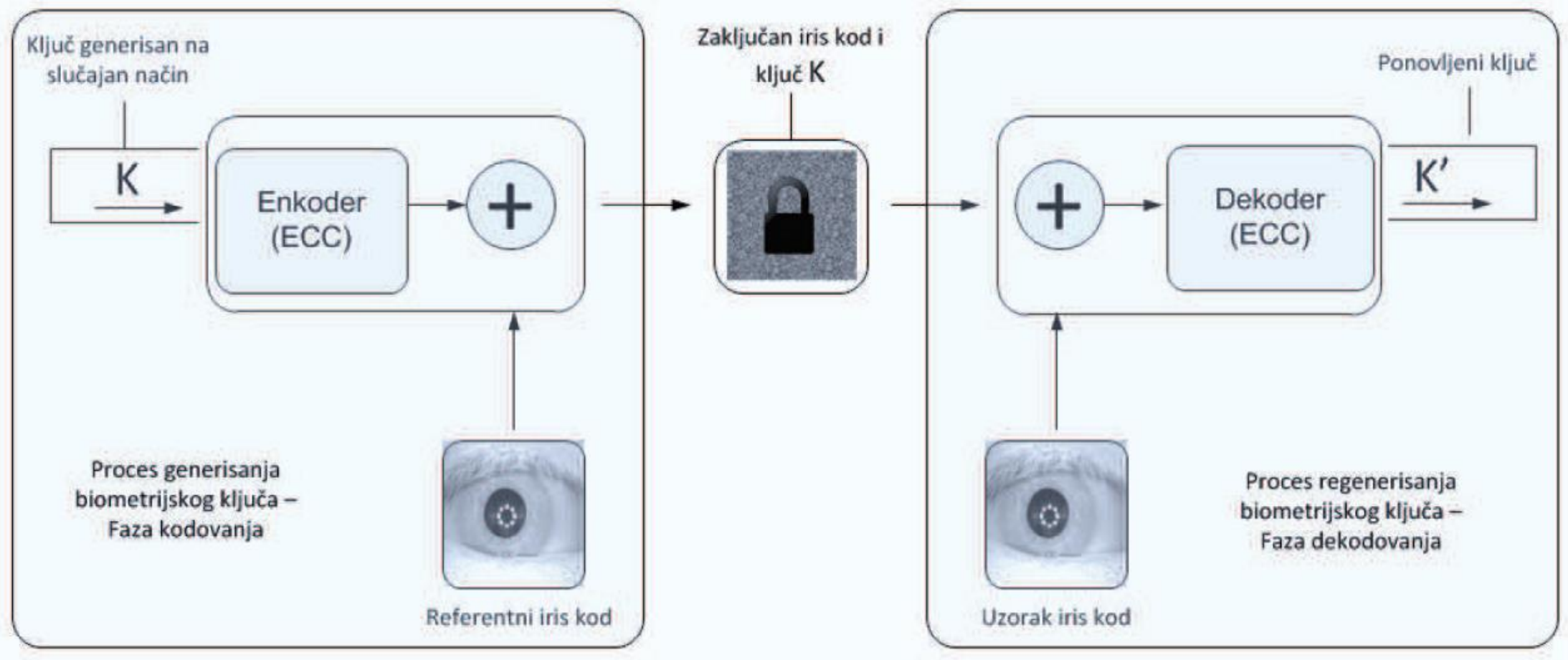
Višemodalni biometrijski sistemi

- **Prednosti** višemodalnih sistema:
  - manji FRR (manja šansa za prevaru),
  - manji FAR (manji broj ljudi koji ne može da se prijavi na system),
  - mogućnost prilično pogodne upotrebe (koristite na primer nešto što jeste i nešto što možete: lice i glas)
- **Nedostaci** višemodalnih sistema:
  - veća cena senzora, licenci i implementacije,
  - potrebno veće osnovno znanje o performansama biometrijskih sistema,
  - složenost sistema,
  - komplikovaniji razvoj.

Generisanje ključeva na osnovu biometrijskih podataka

- **Biometrijsko šifrovanje** je proces u kome se kriptološki ključ čvrsto vezuje za biometrijski templejt, tj. ključ je šifrovan sa biometrijskim podatkom primenom XOR operacije.
- Rezultat je **biometrijski kodovani ključ** koji predstavlja **javnu informaciju** (pomoćni podatak – engl. *helper data*).
  - Formom pomoćnog podatka obezbeđena je zaštita privatnosti, kao i sigurnost ugrađenih kriptoloških ključeva.
  - Pomoćni podaci mogu da budu sačuvani na nekom memorijskom prostoru, bez sigurnosnih rizika.
- Kriptološki ključ se može regenerisati XOR operacijom na osnovu pomoćnog podatka sa biometrijskim templejtom generisanim u fazi verifikacije.
- Dva biometrijska templejta ne moraju da budu identična – važno je da oba templejta potiču od istog biometrijskog izvora da bi bilo moguće regenerisati ključ.
- Korišćenjem ove tehnike moguće je napraviti određen kompromis između biometrijske varijabilnosti i zahtevane kriptografske preciznosti!

Generisanje ključeva na osnovu biometrijskih podataka



Slika preuzeta iz [6]

Razvejavanje mitova o biometrijskoj tehnologiji – Dž. Ešburn

- Biometrija dokazuje da ste vi ona osoba koja tvrdite da jeste.
  - Netačno. Biometrija ne radi ništa slično, ona jednostavno pruža veću pouzdanost podudarnosti individue sa prethodno definisanim identifikacionim profilom.
  - Druga je stvar da li je taj profil tačan ili da li je naknadno izmenjen.
- Test biometrijske identifikacije je nepogrešiv.
  - Netačno. Tehnologija je uvek podložna greškama, a biometrijska tehnologija ne predstavlja nikakav izuzetak.
  - Štaviše, još uvek ne postoji opšte razumevanje za sijaset razloga za moguće neuspehe u procesima biometrijskog proveravanja identiteta.
- Biometrija doprinosi privatnosti.
  - Netačno. Sama po sebi, biometrija niti povećava niti ugrožava privatnost. Radi se o načinu njene upotrebe u kontekstu definisane tehničke arhitekture i operativnog procesa.

Razvejavanje mitova o biometrijskoj tehnologiji – Dž. Ešburn

- Biometrijski podaci ne mogu da budu ukradeni.
  - Netačno. Biometrijski podaci se vrlo lako mogu ukrasti.
  - Glavno pitanje je za koje sve svrhe se oni mogu koristiti u slučaju krađe.
- Biometrija ne može da otkrije lične informacije.
  - Netačno. Lične informacije se mogu izvući iz samih biometrijskih podataka, kao i iz podataka koji su sa njima povezani.
  - Ovo drugo je potencijalno kompleksniji problem, s obzirom na mogućnost da se sa tim podacima manipulisalo ili da su prošireni bez znanja ili odobrenja ličnosti na koju se odnose.
- Elektronski čipovi su po svojoj prirodi bezbedni.
  - Netačno. Čip je običan mehanizam za skladištenje podataka. Relativna bezbednost tih podataka zavisi od kombinacije tehnološke kontrole i operativnog procesa.

Razvejavanje mitova o biometrijskoj tehnologiji – Dž. Ešburn

- Skladišteni biometrijski podaci nisu podložni manipulaciji.
  - Netačno. Skladišteni biometrijski podaci mogu biti predmet raznih vrsta manipulacije.
- Moderna tehnologija za baze podataka je sama po sebi bezbedna.
  - Netačno. Bezbednost skladištenih podataka zavisi od mnogih činilaca ali, sama po sebi, baza podataka ne mora automatski da bude i bezbedna.
  - Štaviše, može postati veoma nebezbedna kao posledica neadekvatne kontrole, nepromišnjenog povezivanja sa drugim izvorima podataka, lose politike i nerazumevanja osnova IT tehnologije i prakse uopšte.

Literatura

1. D. Pleskonjić, N. Maček, B. Đorđević, M. Carić (2007): Sigurnost računarskih sistema i mreža. Mikro knjiga, Beograd.
2. M. Milosavljević, S. Adamović (2015): Kriptologija 2. Univerzitet Singidunum.
3. N. Maček, B. Đorđević, J. Gavrilović, K. Lalović: An Approach to Robust Biometric Key Generation System Design. Acta Polytechnica Hungarica, Vol. 12, No. 8, pp. 43-60, 2015.
4. B. Biggio (2010). Adversarial Pattern Classification. Doctoral Dissertation.
5. N. K. Ratha, S. Chikkerur, J. H. Connell, R. M. Bolle: Generating Cancelable Fingerprint Templates. Pattern Analysis and Machine Intelligence, IEEE Transactions on, 29(4), pp. 561-572, 2007.
6. S. Adamović (2013): Jedna klasa sistema za generisanje kriptoloških ključeva na osnovu biometrijskih podataka. Doktorska disertacija, Univerzitet Singidunum.
7. S. Mesarović (2007): Multimodalni biometrijski sistemi. Magistarska teza, Univerzitet Singidunum.

Hvala na pažnji

Pitanja su dobrodošla.