

Najnovšie trendy biometrie

*e*FOCUS

Najnovšie trendy biometrie

Ing. Peter Kopriva, Tatra banka, a.s.

: **najlepší** idú za nami



Member of Raiffeisen Bank International

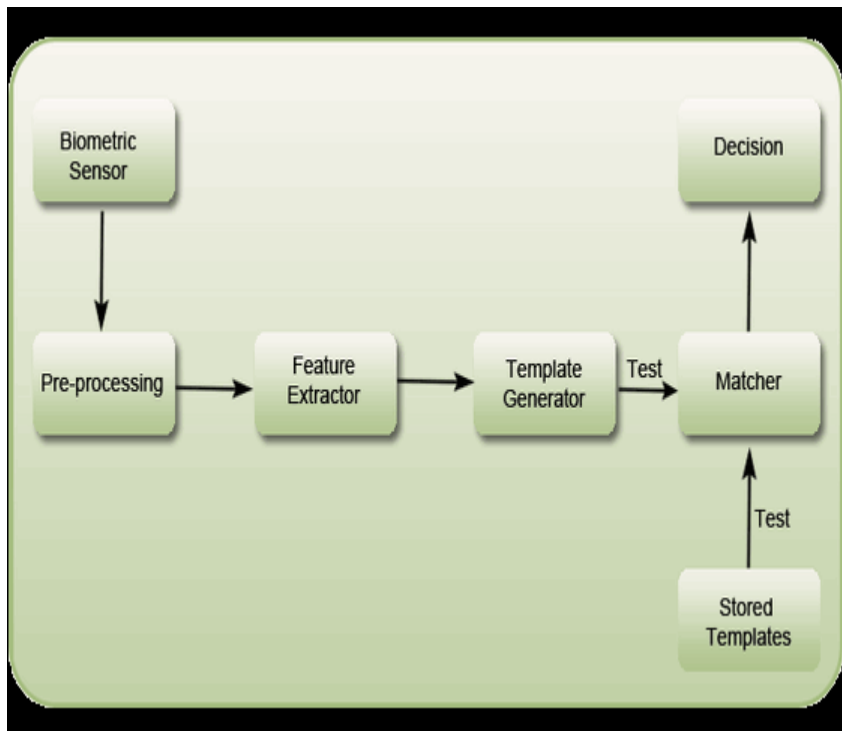


e **FOCUS**

Agenda

-
- A word cloud featuring various biometric identification methods. The most prominent word is 'biometria' in large blue letters at the bottom center. Other words include 'podpis' (signature) in green, 'dlaň' (palm) in brown, 'hlas' (voice) in green, 'ruka' (hand) in brown, 'očná sieťnica' (retina) in purple, 'ucho' (ear) in yellow, 'salinita' (salinity) in purple, 'duhovka' (iris) in blue, 'srd' (heart) in blue, 'veľ' (big) in green, 'veľ' (big) in green, 'DNA' in green, 'nechty' (nails) in purple, 'EKG' in pink, 'EEG' in purple, 'strojopis' (machine writing) in brown, 'nách' (foot) in red, 'chůza' (gait) in red, 'commit' in black, 'vault' in black, and 'a' in black. The words are arranged in a circular pattern around the central 'biometria' word.

Verifikácia v nedôveryhodnom prostredí



Jednoduchý spôsob

```
Test = TemplateGenerator();
```

```
if (Matcher(Test, Template) > ThresholdLevel )
```

```
    Decision = TRUE
```

```
else
```

```
    Decision = FALSE
```

Dá sa obísť!!

Nikdy nenastane!!

Verifikácia v nedôveryhodnom prostredí

Tradičný prístup s PINom

- odomkni PIN_key PINom => PIN_key = KDF(salt,PIN)
- voliteľné UDK = KDF (PIN_key, event_data...)
- verifikuj PIN_key alebo jedinečný UDK v banke tradičnou krypto cestou

Verifikácia v nedôveryhodnom prostredí

Bio prístup

- odomkni BIO_key biometriou
- voliteľný UDK = $KDF(BIO_key, event_data...)$
- verifikuj BIO_key alebo jeho odvodený UDK buď tradičnou krypto cestou

Ako derivovať BIO_key??

Fuzzy commitment

Fuzzy commitment schéma je založená na lineárnych **error-correcting** kódoch
error-correcting kód pozostáva z

Priestoru správ $M \subseteq F^a$

Priestoru kódov $C \subseteq F^b$ s ($b > a$)

Bijekcie $\theta : M \leftrightarrow C$

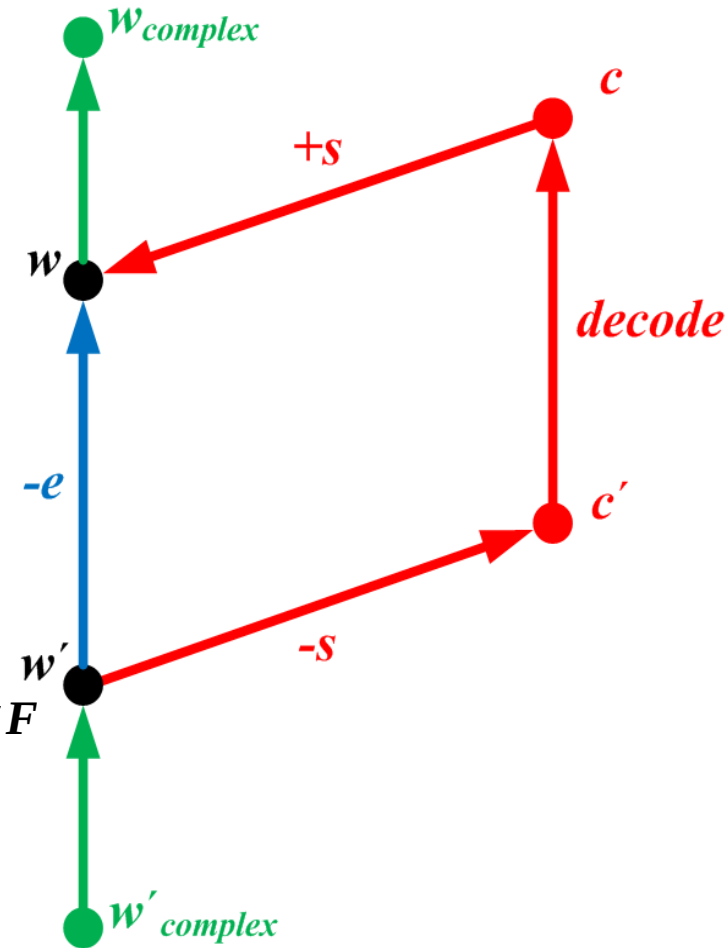
Dekódovacej funkcie $f : C' \rightarrow C \cup \perp$

Enrollment

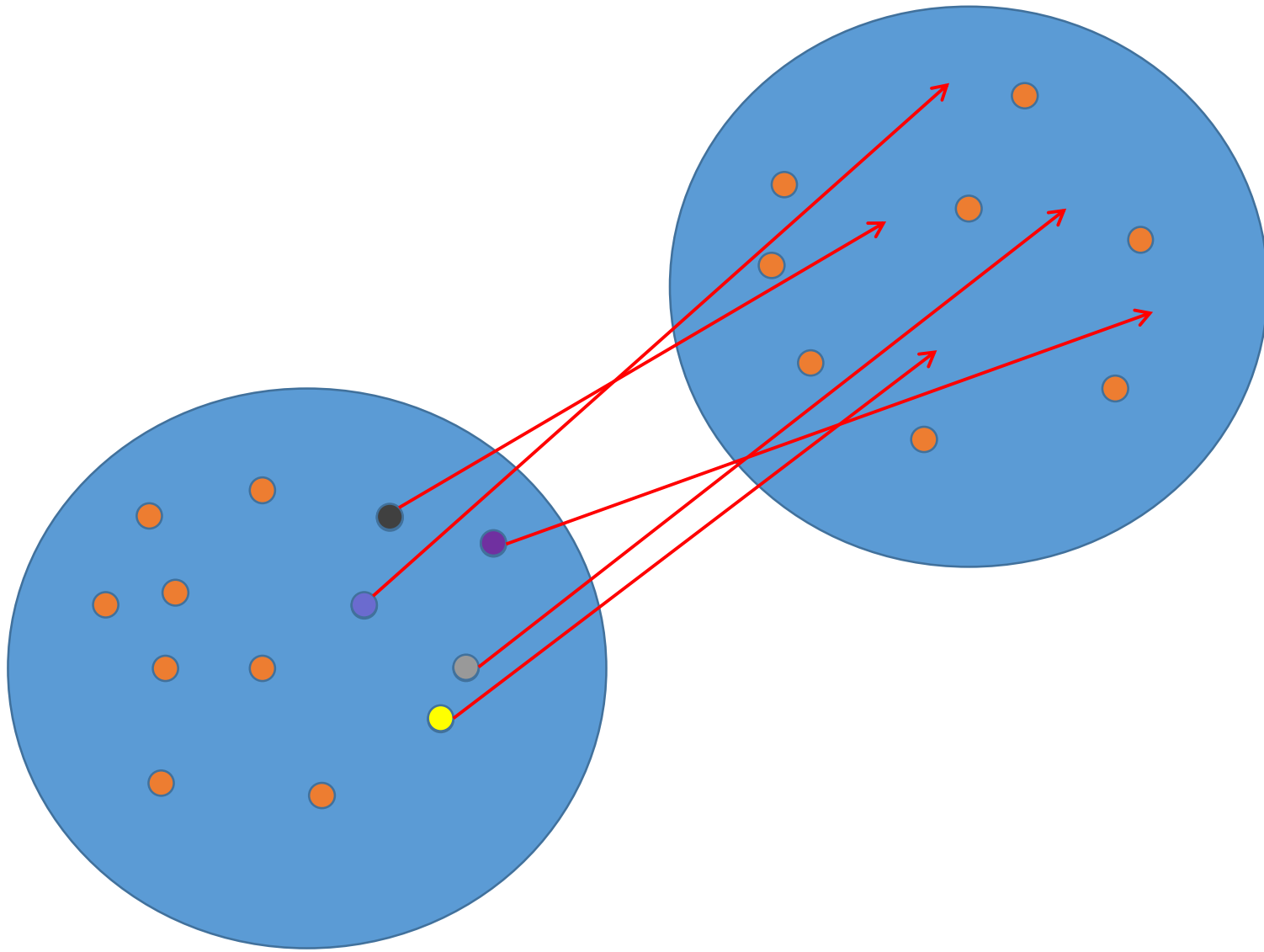
- náhodne zvol' $c \in C \subset F$
- získaj BIO vektor $w \in F$
- $s = w - c$
- $\text{BIO_key} = \text{KDF}(c)$
- ulož s pre používateľa

Verifikácia

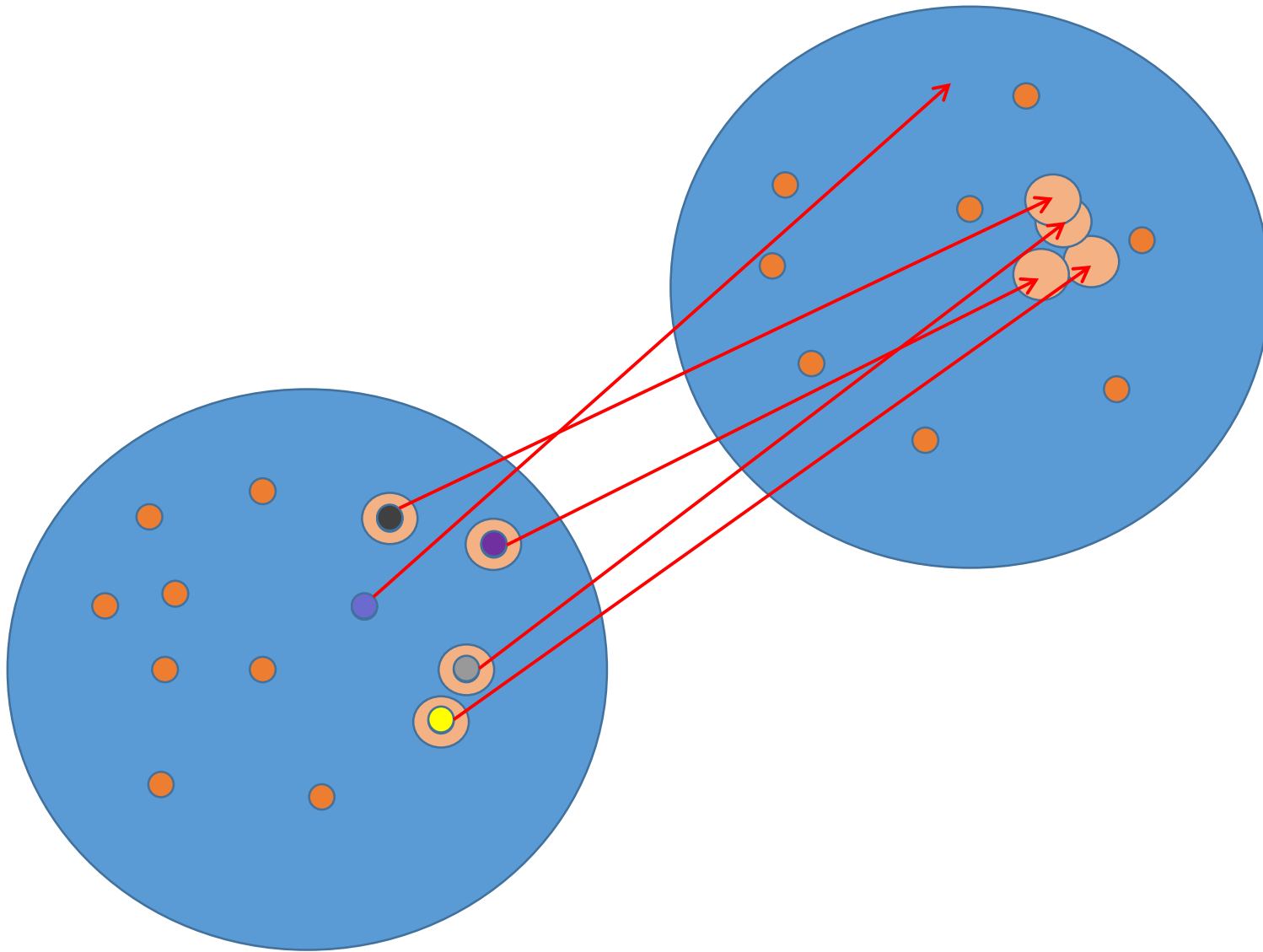
- získaj BIO vektor $w' \in F$
- $c' = w' - s$
- $c = \text{decode}(c')$
- $\text{BIO_key} = \text{KDF}(c)$



Fuzzy commitment

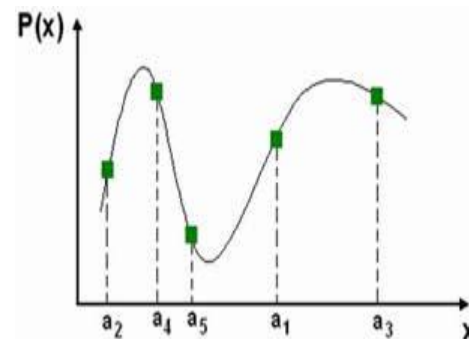
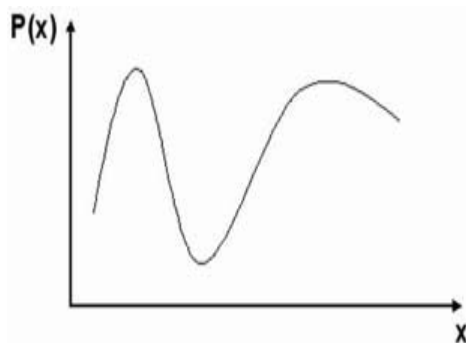


Fuzzy commitment

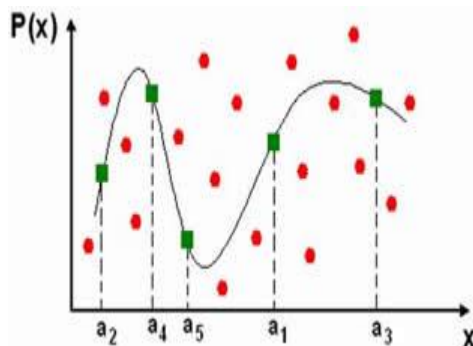


Kde je ukrytá soľ? - Fuzzy vault

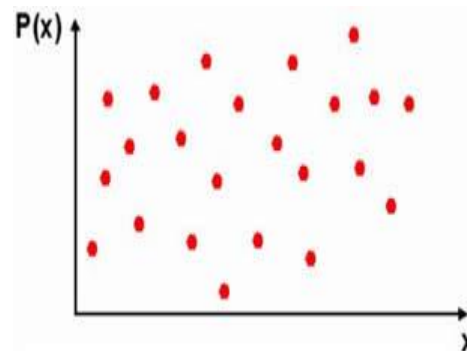
*s nemôžeme
považovať za úplne
verejné* „verejné“ pri
porovnaní s verejným
kľúčom PKI.



(1) Vytvoríme polynóm kódujúci BIO_Key prostredníctvom
jeho koeficientov



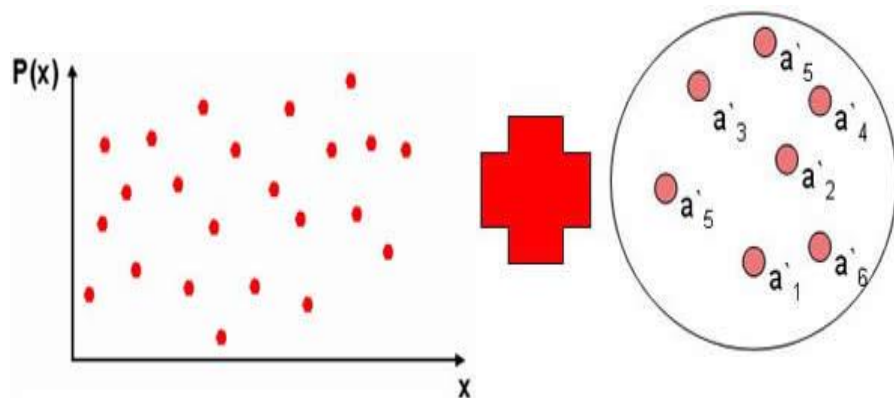
(2) Náhodne vytvoríme šum
(červene)



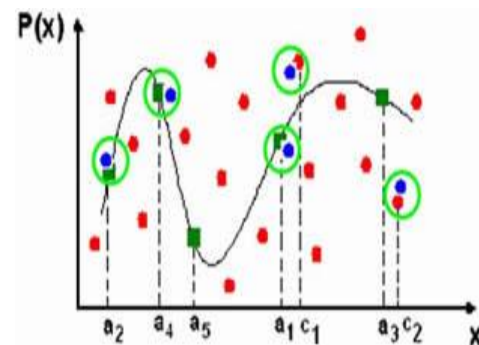
(3) Finálny vault uložený v
zariadení

Two images of a handwritten signature 'Alet'. The top image shows the signature as a continuous line. The bottom image shows the same signature with small black dots placed along the strokes, representing the points used in the fuzzy vault scheme.

Fuzzy vault



(1) Fuzzy Vault referenčného ID (vľavo) a odomykacia množina bodov (vpravo)



(2) Porovnanie odomykacej množiny s vaultom. Dekodované body označené zelene. Polynóm skonštruovaný LEN cez dekodované body.

Fingerprint sample



Odtlačok



Minutiae x

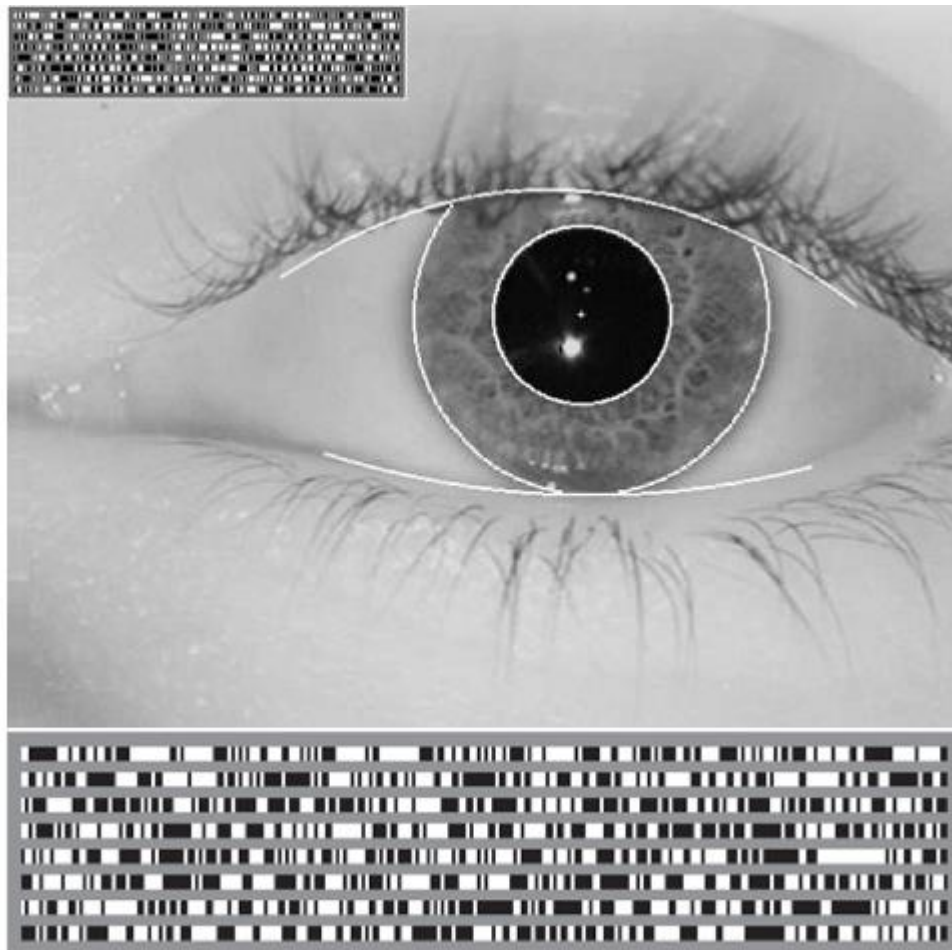


Transformovaná
vzorka $f(x, k)$



Fuzzy Vault
 $f(x, k)$

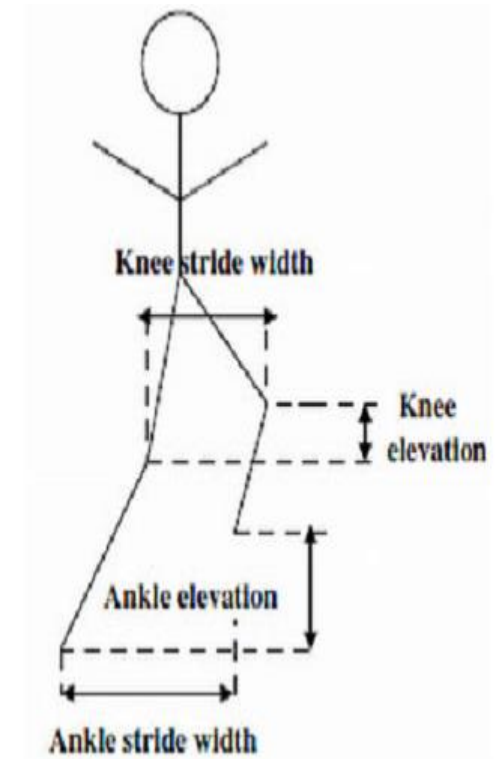
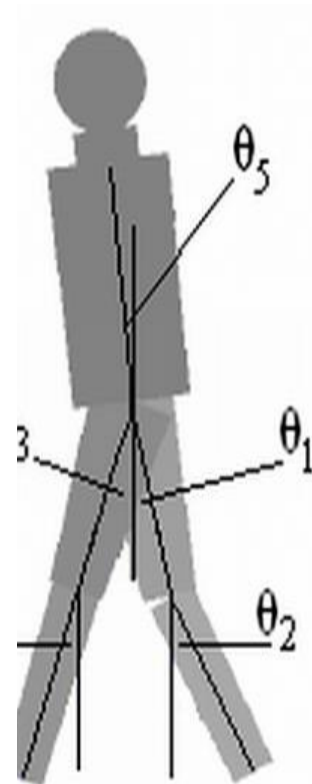
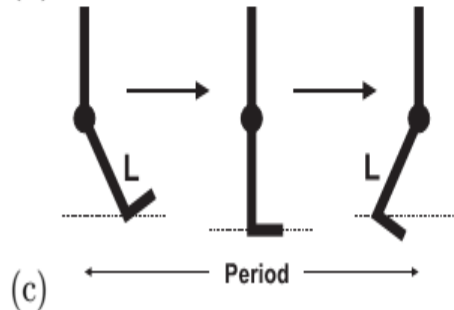
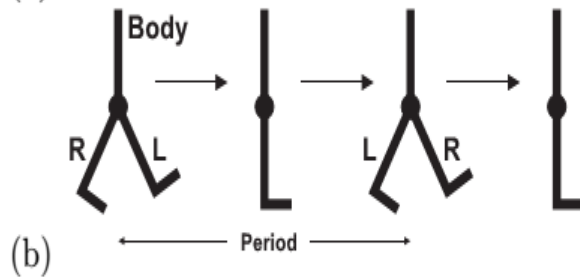
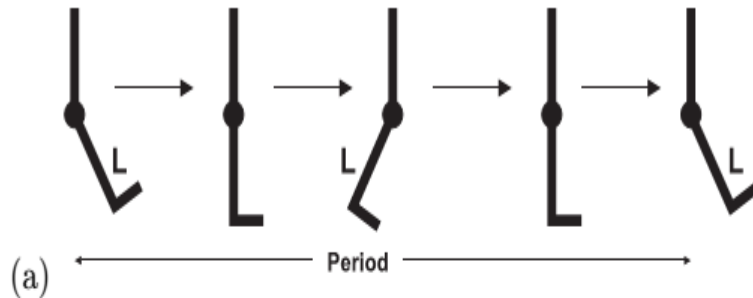
Očná dúhovka



Chôdza

- Biometria je založené na spôsobe, akým osoba chodí. Jedná sa o behaviometrický systém. Nie je závislá na rýchlosti chôdze osoby.
- Výhody:
 - Dokáže rozpoznať osobu na diaľku, kedy sú ďalšie biometrické metódy nepoužiteľné.
 - Efektívna aj pri nízkom rozlíšení obrazu (CCTV)
 - Neinvazívna biometria
- Nevýhody:
 - Nefunkčná/zlyháva ak ma meraná osoba zakryté nohy (kabát) alebo nosí nevhodnú obuv (flip-flopy), ktoré ovplyvňujú chôdzu a skresľujú rozpoznávanie
 - Chôdza na nerovnom povrchu, z kopca, do kopca
- Rozpoznávanie chôdze nemá nahrádzať iné metódy, ale skôr ich vhodne dopĺňať. Napríklad keď si páchatel nasadí kuklu, nebude fungovať často využívaná metóda rozpoznávania tváre a chôdza zostane ako identifikátor jednou z mála použiteľných možností. Ďalší priestor pre využitie možno nájsť napríklad v bankách, na letiskách, v rôznych zabezpečených areáloch a podobne.

Chôdza



Ľudský pach

- Rozpoznávanie telesné pachu je bezkontaktná biometrická metóda, ktorý sa pokúša o overenie totožnosti osoby na základe analýzy vône ľudského tela. Podľa University of Cambridge (<http://www.cam.ac.uk>), senzory, ktoré vyvinuli sú schopné zachytiť telesnú vôňu z vonkajších častí tela, ako sú ruky. Každá chemická zložka ľudskej vône sa extrahuje a pomocou biometrického systému konvertuje na unikátny dátový blok.

Vonkajšie ucho

- Tvar vonkajšieho ucha, laloky, kostné štruktúry a veľkosť sú jedinečné pre každú osobu. Ušné rozpoznávanie vzorov sa používa ako fyzikálna bezkontaktná biometrická metóda (Carreira-Perpinan & Sanchez-Calle, 1995) a používa Optophone na overenie tvaru ucha. Jedná sa o špeciálne telefónne slúchadlo, ktoré sa skladá z dvoch komponentov (zdroj svetla a kamera). Podobne ako minútie na odlačkoch prstov, vonkajšie ucho má mnoho markantov, ktoré je možné merať a porovnávať.

Vonkajšie ucho



- (1) Helix Rim
- (2) Lobule
- (3) Antihelix
- (4) Concha
- (5) Tragus
- (6) Antitragus
- (7) Crus of Helix
- (8) Triangular Fossa
- (9) Incisure Intertragica

Poistka strelnej zbrane

Senzory a mikroprocesor analyzuje zložité vzájomné pohyby kostí a svalov zapojených do stláčania spúšte. Ide o dynamickú metódu.
V súčasnej dobe, prototyp dosahuje FAR 2% a FRR 3%



Ďakujeme za pozornost

: **najlepší** idú za nami



Member of Raiffeisen Bank International



TATRA BANKA

e **FOCUS**