UNIVERZITA PAVLA JOZEFA ŠAFÁRIKA V KOŠICIACH

Financované Európskou úniou NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

# Počítačová biometria

## Bezpečnosť biometrických systémov a útoky

J. Majerník, L. Urbanská, A. Kačmariková

V-AR-24-25

# Útoky na systémy

- biometrické systémy sú vystavené systémovým útokom rôznymi formami hrozieb
- hrozba pre biometrický systém predstavuje bezpečnostný problém a znižuje jeho výkon

## Falošný biometrický znak

- falošná biometrická vzorka môže byť poskytnutá senzoru na získanie prístupu do systému (odtlačok prsta vyrobený zo silikónu, falošná maska na tvári, šošovka na dúhovke atď.)

# Útoky na systémy

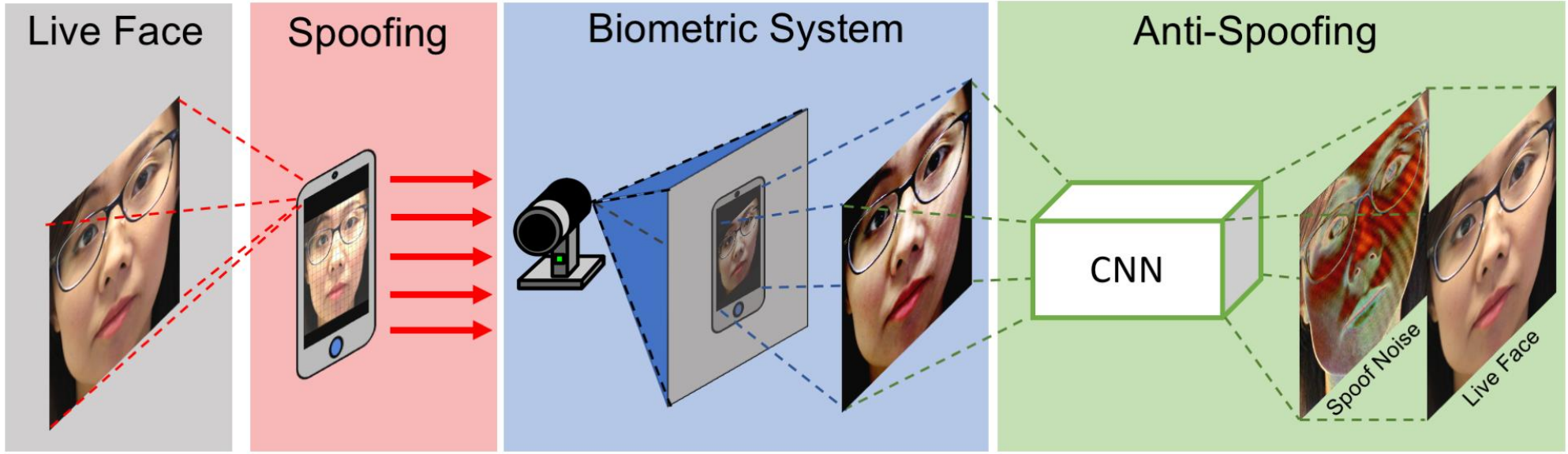
## Opakovaný útok

- útok v biometrickom systéme, pri ktorom sa medzi senzor a systém spracovania „vkladá“ dátový tok
  (útok opakovaním môže byť dvoj- alebo trojstupňový proces, najprv zachytenie alebo kopírovanie prenosu senzora, potom prípadná úprava údajov a nakoniec opätovné prehrávanie údajov)

# Útoky na systémy

## Falšovanie sady funkcií

- nahradenie sady funkcií falošnou alebo zmenenou sadou funkcií



# Útoky na systémy

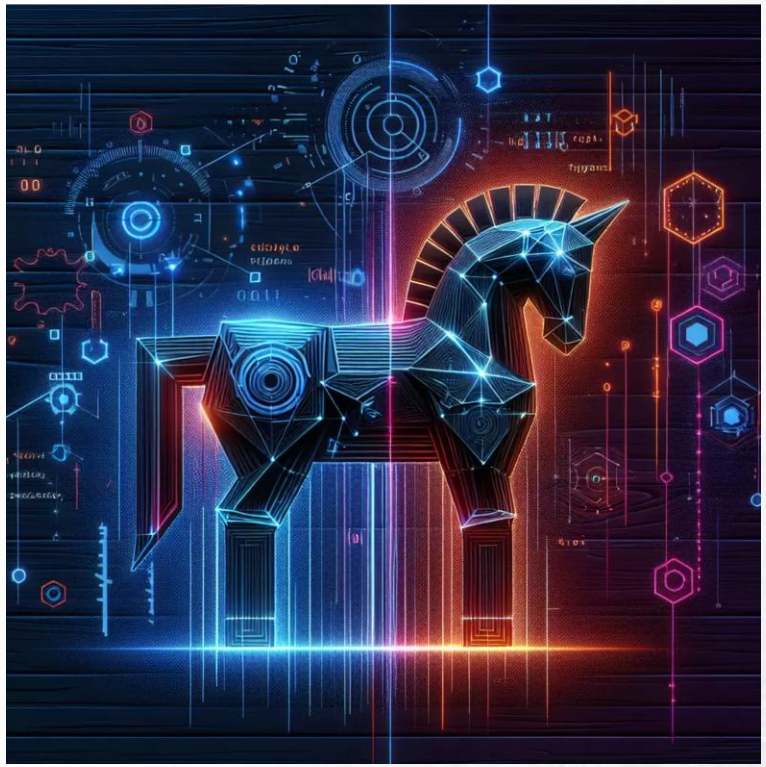
## Útok so šablónami

- šablóny uložené v databáze môžu byť ukradnuté, nahradené alebo upravené

# Útoky na systémy

## Útok trójskym koňom

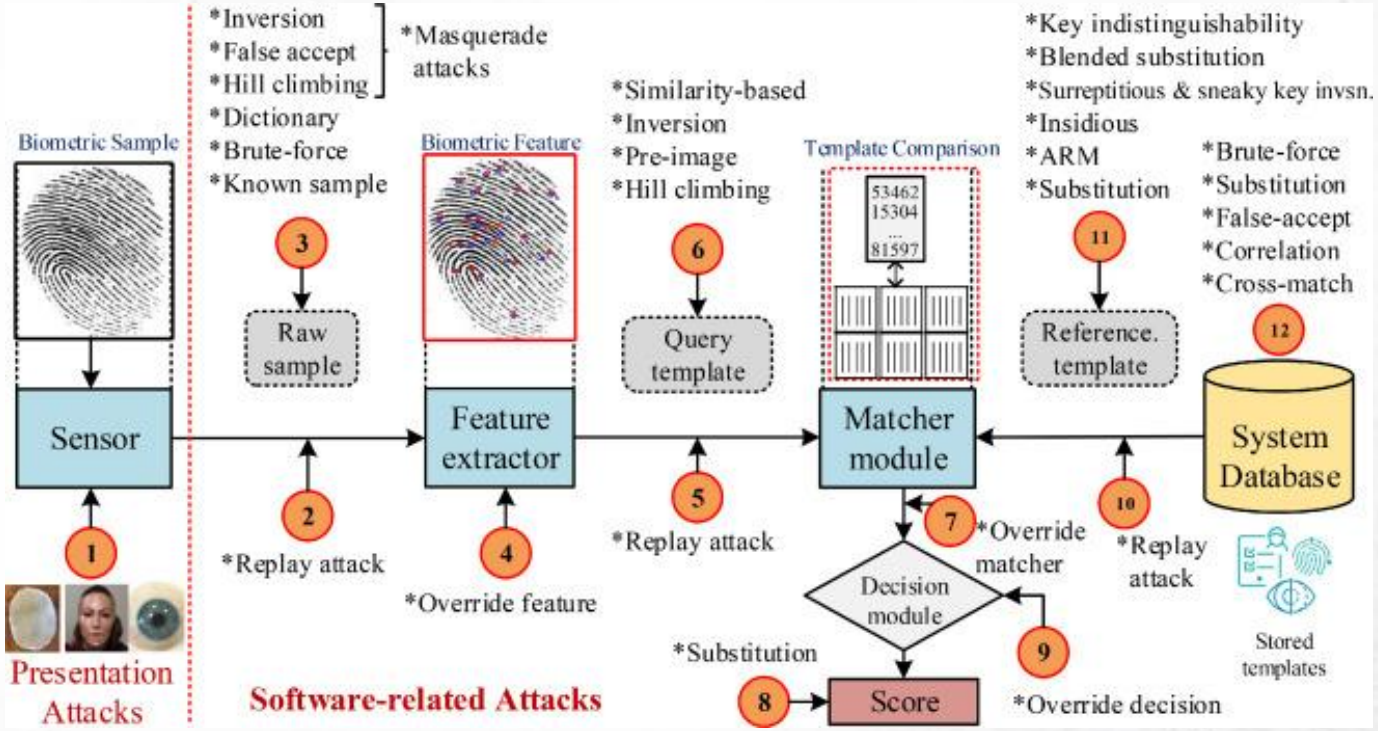
- samotný extraktor prvkov je nahradený tak, aby generoval požadované prvky a pridal ich do existujúcej databázy



# Útoky na systémy

S rastúcim záujmom o bezpečnosť je potrebné identifikovať, kontrolovať a minimalizovať biometrické útoky. Výskumníci vyvinuli rôzne prístupy k zabezpečeným biometrickým systémom.

Systém postupného útoku, steganografické techniky a techniky vodoznaku na zvýšenie bezpečnosti biometrickej šablóny, mechanizmus detekcie živosti na zmarenie útokov, mäkká biometria, multimodálna biometria atď. sú rôzne prístupy používané na zabezpečenie spoľahlivého biometrického systému.

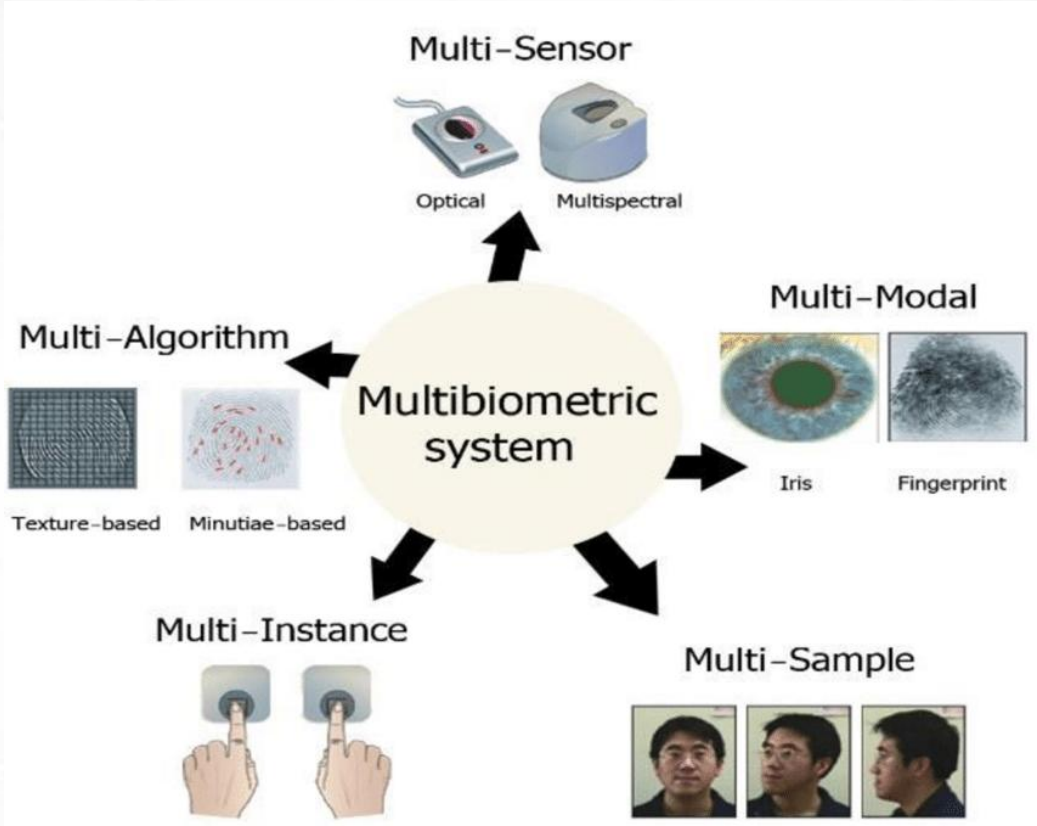


# Multimodálna biometria

Použitie multibiometrických údajov môže zlepšiť výkon jednotlivých biometrických systémov alebo modalít a zvýšiť odolnosť voči útokom.

## Multisenzory

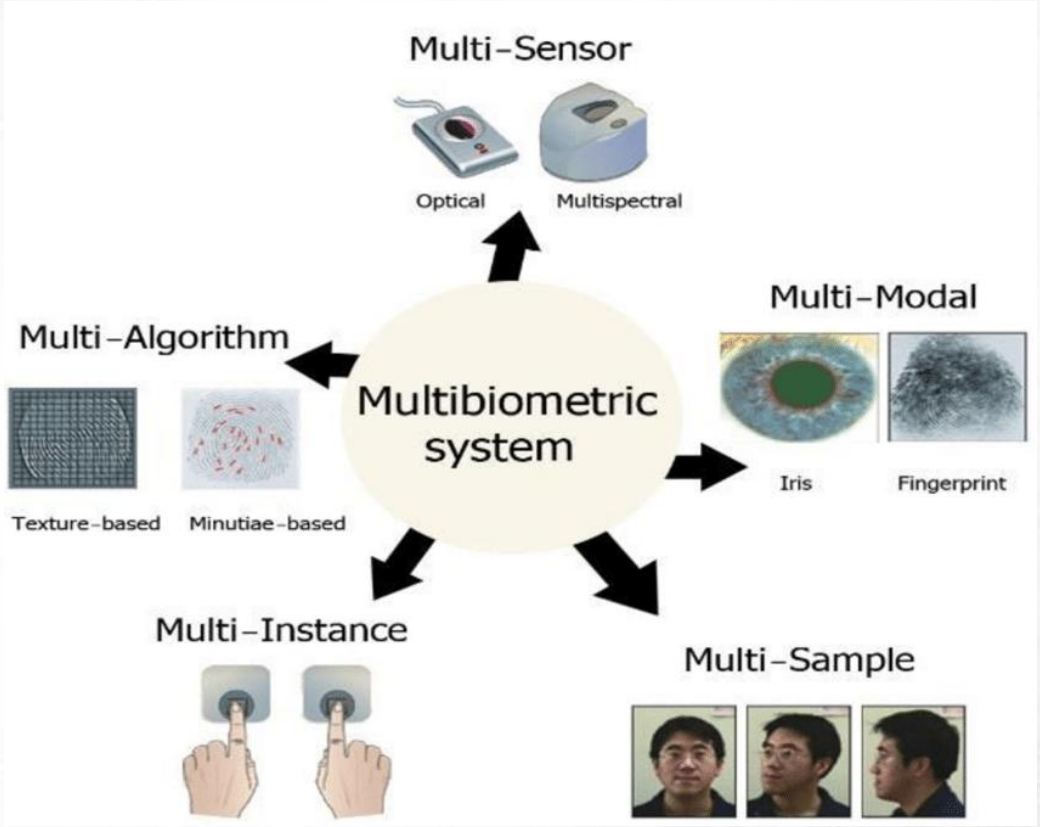
- na zachytávanie údajov sa používa viacero senzorov
  (systém rozpoznávania tváre môže použiť viacero kamier na zachytávanie rôznych uhlov tváre)



# Multimodálna biometria

## Viacero algoritmov

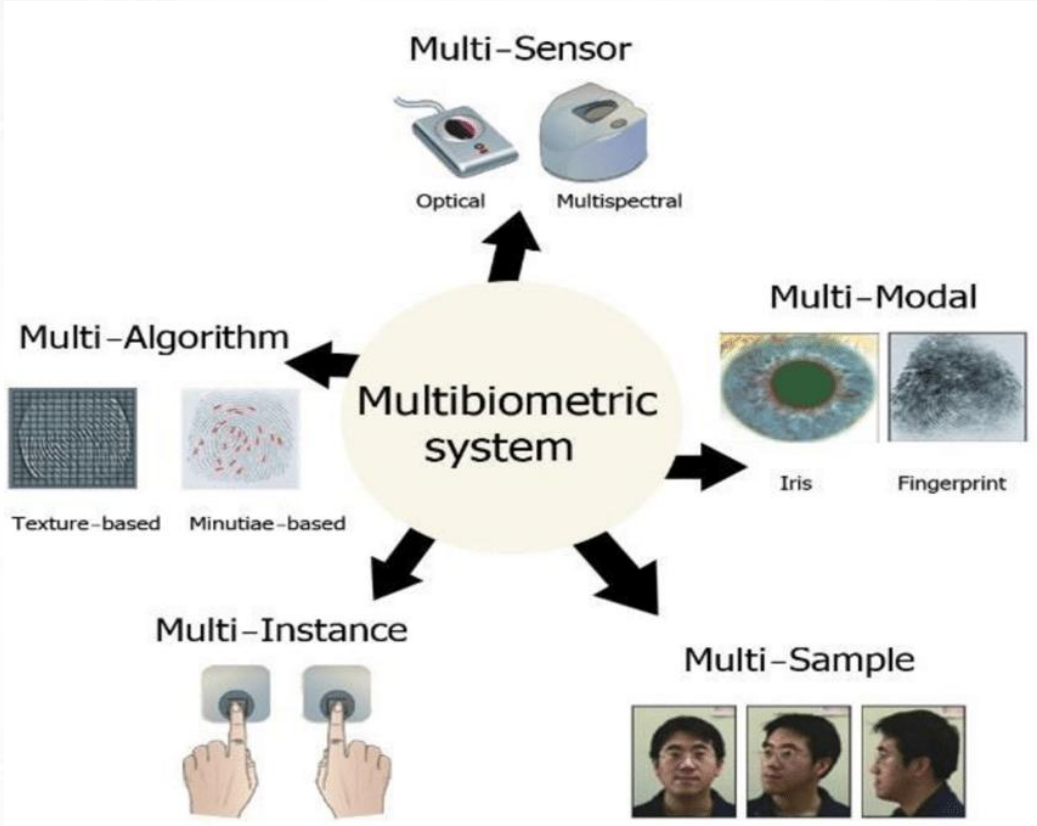
- rovnaké zachytené údaje sa spracovávajú pomocou rôznych algoritmov
  (jeden odtlačok prsta sa môže spracovať pomocou minúcií a textúry)



# Multimodálna biometria

## Viacero inštancií

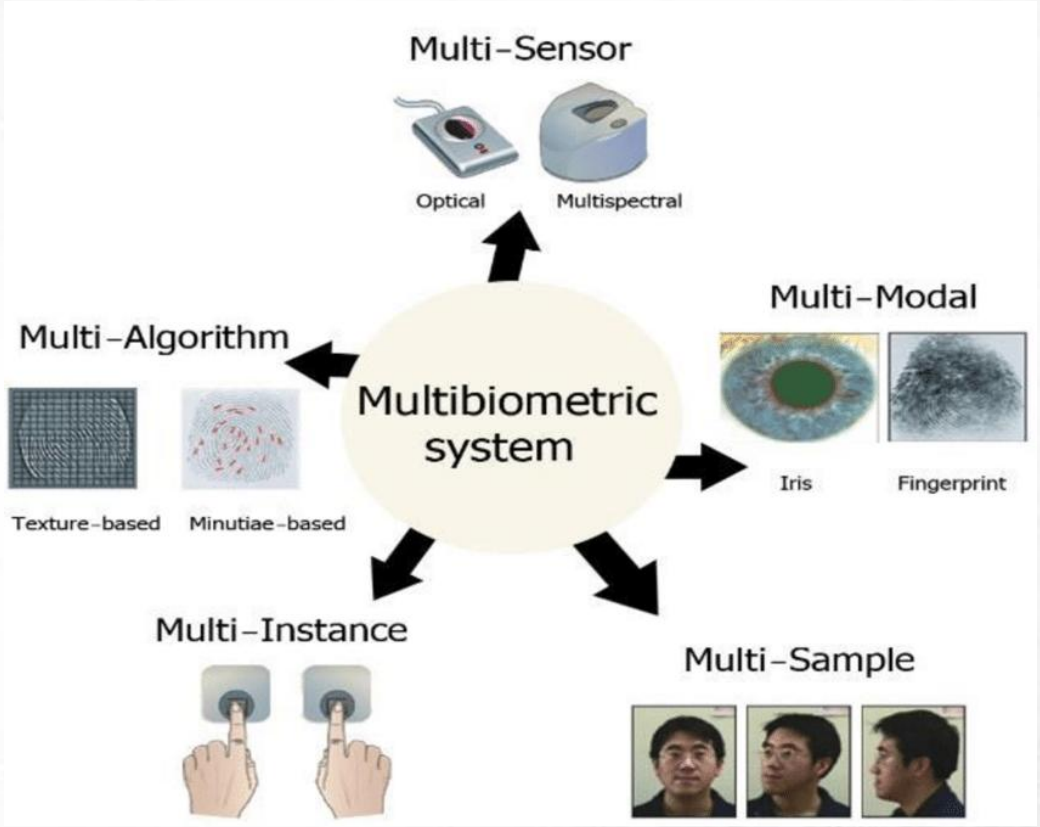
- používa sa viacero inštancií tej istej modality (môže sa porovnávať viacero odtlačkov prstov namiesto jedného)



# Multimodálna biometria

## Multivzorky

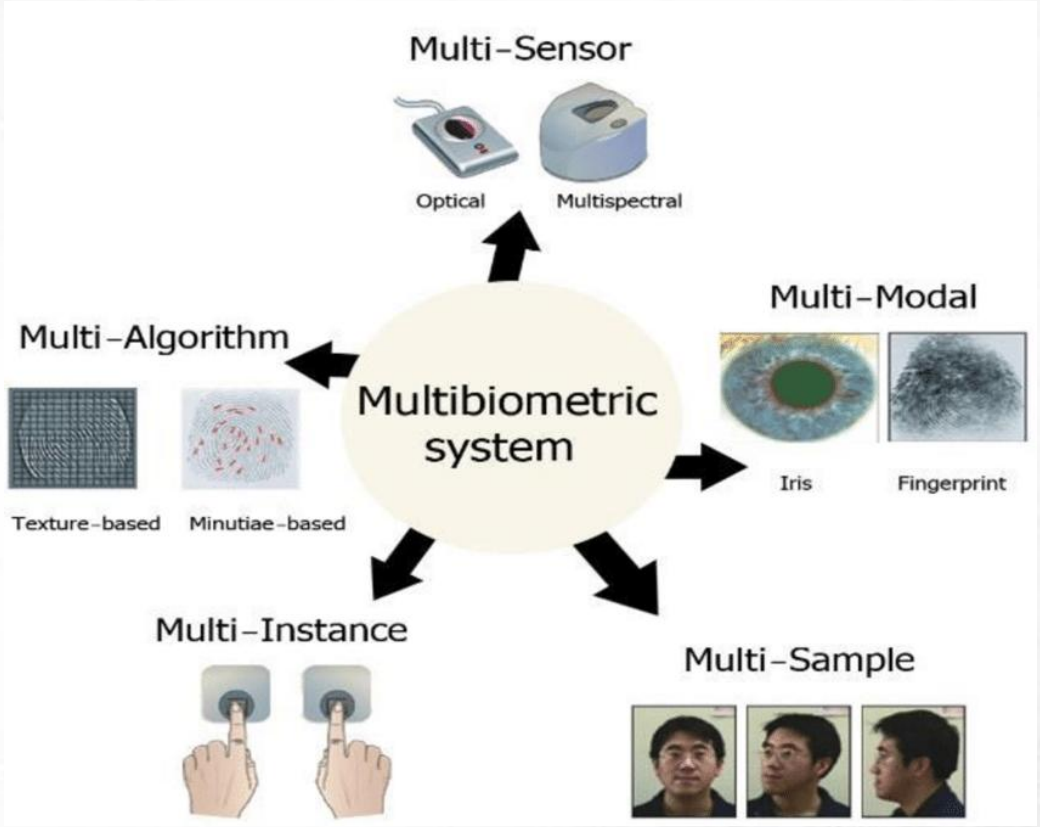
- získava sa viacero vzoriek tej istej vlastnosti (zachytáva sa viacero obrázkov rôznych častí toho istého odtlačku prsta)



# Multimodálna biometria

## Multimodálne

- kombinujú sa údaje z rôznych modalít
  (tvár a odtlačok prsta, dúhovka a hlas...)



KCKB UPJS

UNIVERZITA PAVLA JOZEFA ŠAFÁRIKA V KOŠICIACH

Financované Európskou úniou NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

# Ďakujeme za pozornosť

jaroslav.majernik@upjs.sk
lenka.urbanska@upjs.sk
andrea.kacmarikova@upjs.sk