# Biometrika

## Co je biometrika a jak to funguje

# Co je biometrika

- Slovo biometrie vzniklo spojením dvou řeckých slov **bio** a **metric**, kde prvně jmenované znamená život a druhé měření.
- Biometrie tedy měří určité charakteristiky člověka.
- Biometrické systémy pak slouží k automatické identifikaci nebo ověření identity člověka na základě jeho unikátních měřitelných fyziologických nebo behaviorálních vlastností.

# Fyziologické a behaviorální vlastnosti

- Mezi fyziologické vlastnosti každého z nás patří například otisk prstu  nebo geometrie ruky, příkladem je behaviorálních charakteristik, tedy týkajících se chování, mohou být dynamika podpisu či dynamika stisku kláves na klávesnici.

# Přehled základních biometrik

**FYZIOLOGICKÉ**

- Otisk prstu
- Geometrie ruky
- Rozpoznání obličeje
- Oční duhovka
- Oční sítnice
- Lůžko nehtu
- DNA

**BEHAVIORÁLNÍ**

- Ověřování hlasu
- Dynamka podpisu
- Dynamika stisku kláves

# Identifikace a verifikace

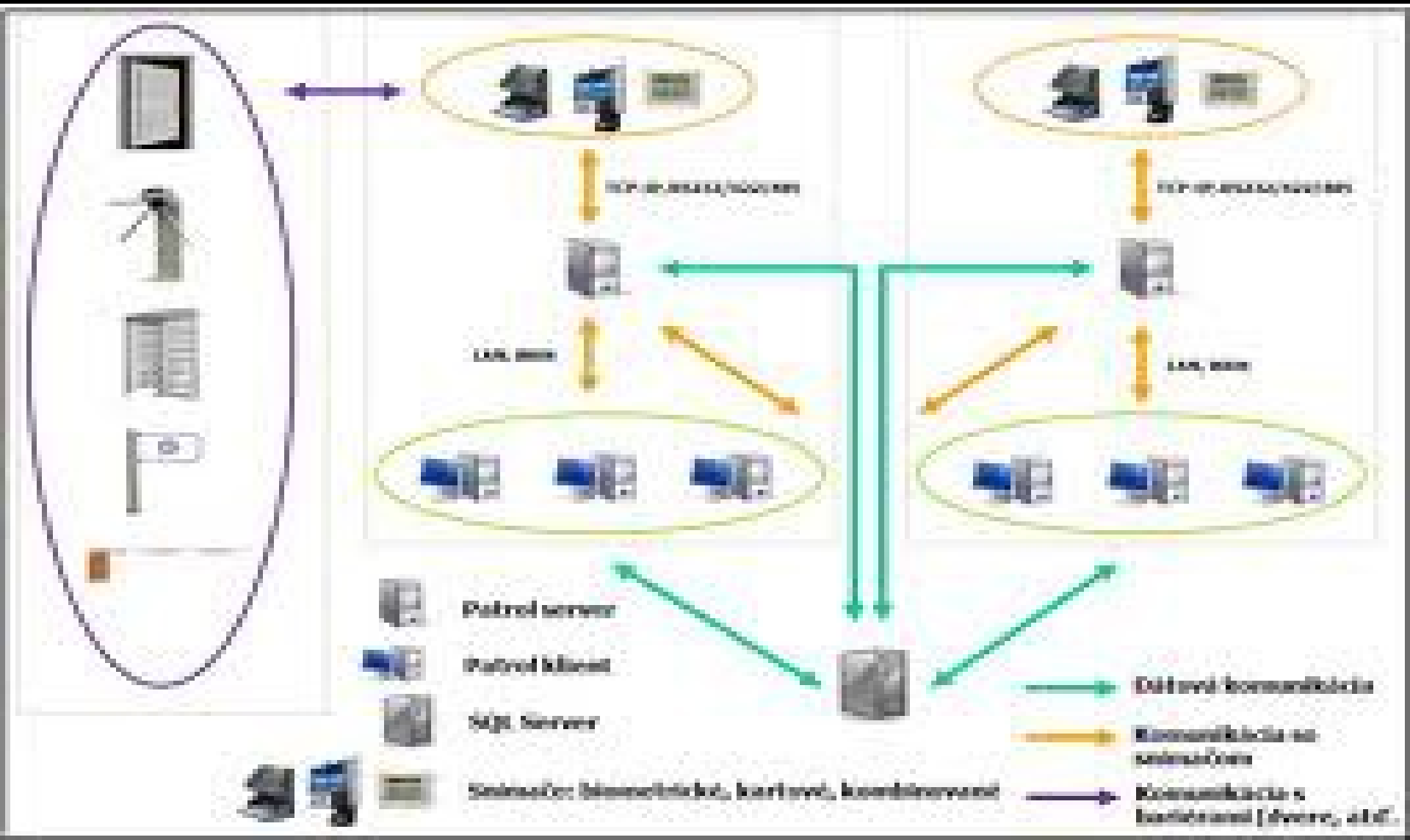
## VERIFIKACE

- Při **verifikaci** (ověřování identity) uživatel předkládá svojí totožnost a tu následně potvrzuje znalostí nějakého tajemství.
- S verifikací, byť ne přímo biometrickou, se tady potkáváme vždy během přihlašování k počítači pomocí hesla.
- Skutečná biometrická verifikace probíhá tak, že uživatel předloží svou identitu (login, identifikační kartu..) a poté mu čtení zařízení nasnímá danou biometriku.

## IDENTIFIKACE

- Naproti tomu při **identifikaci** je uživatel rozpoznán systémem automaticky, tj. bez předchozího předkládání totožnosti, a jedná se tedy o časově, tak výpočetně náročnější proces než v případě verifikace

# Základní model biometrického systému



# Obecné výhody a nevýhody biometriky

- Výhody biometriky  je, že nemůžou být zapomenutí, ztraceny a jsou nepřenosné (v kontrastu s hesly a tokeny). Princip biometrické autentizace poskytuje relativně vysoký stupeň zabezpečení, a proto je často vhodné nasazovat biometrické systémy jako jednu z funkcí pro řízení přístupu.
- Důležitou roli při volbě vhodného biometrického systému hraje také uživatelská přívětivost – snímání uživatelova biometrického vzorku při identifikaci musí být rychlé a nesmí působit nepříjemně. Rychlost snímání bývá preferována především při frekventovaném využívání systému mnoha uživateli.
- Při masovém rozšířit jedné vybrané biometrické technologie pro běžné každodenní použití, například k mezinárodní identifikaci osob, je třeba řešit  co s uživatel, kteří danou biometrikou nedisponují – ne všichni lidé totiž mohou poskytnout otisk prstu či vzorek hlasu.

# Proces práce s biometrikou

Aby se biometrický systém dal každodenní používat v praxi, je třeba nejprve provést několik základních kroků, když vše extrakcí charakteristických vlastností.

## FÁZE REGISTRACE

- Během této etapy se uživatel registruje do biometrického systému.
- Poskytuje data reprezentující biometrický vzorek, který se nazývá **šablona** nebo **etalony.**
- Většinou dochází k několika snímání a z těchto snímků je poté vybrán pouze ten nejlepší.
- Pokud je šablona při praktickém používání shledána nedostatečnou , musí se uživatel registrovat znovu.
- V šabloně není uložen biometrický vzorek jako takový ale pouze jeho odpovídající matematický kód.
- Šablony se uchovávají na bezpečném místě.

## FÁZE VERIFIKACE/IDENTIFIKACE

- Po vytvoření databáze šablon během registrace lze přistoupit k vlastní verifikaci nebo identifikaci uživatele
- Z biometrického vzorku získaného za pomocí čtecího zařízení se opět vytvoří odpovídající šablona a ta je následně porovnána s dříve uloženým etanolem.

# Negativní versus pozitivní identifikace

- Při detailnějším zkoumání identifikace lze rozlišit dvě varianty – pozitivní a negativní identifikaci.
- Při pozitivní identifikaci tak uživatel například tvrdí, že je zaměstnancem tajné laboratoře.
- Biometrické čtecí zařízení mu sejme otisk prstu a získání data srovná s referenční šablony.
- Pokud je vše v pořádku (nastala shoda), zaměstnanec má povolen přístup.
- Při negativní identifikaci uživatel systému tvrdí, že není někdo systému už známý, například že není v databázi hledaných zločinců.

# Chyby biometrického systému

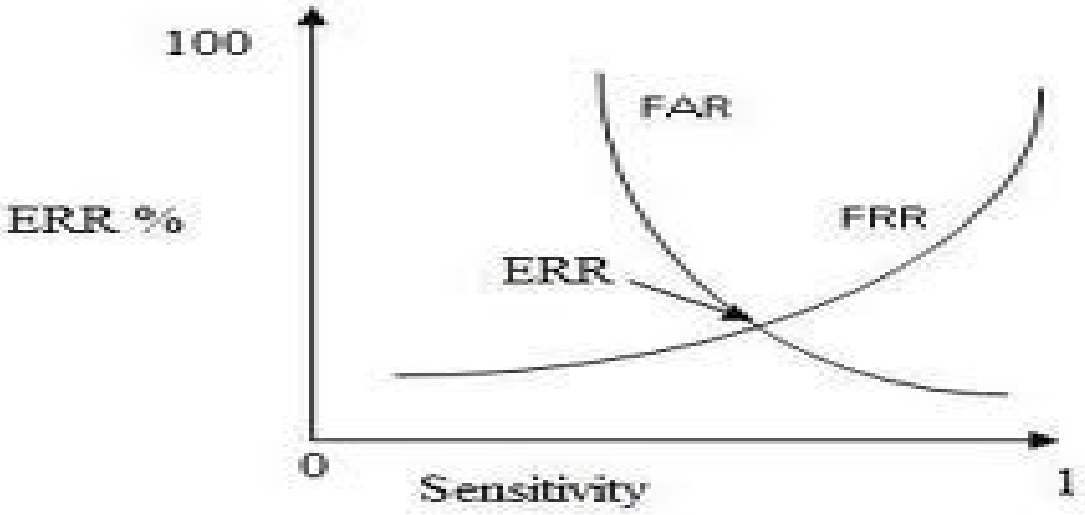
- Biometrické systémy se používají především k řízení přístupu a prosazování bezpečnostní politiky.
- Důraz je kladen na vysokou bezpečnost a spolehlivost této technologie.
- Jako jakýkoliv jiný systém ani biometrie bohužel není stoprocentně bezpečná.

# Chybná přijetí a chybné odmítnutí

- Jak již bylo zmíněno při popisu fáze registrace, referenční šablona se získává jako nejreprezentovanější z několika vzorků.
- Při následné identifikaci pak nezískáme úplnou shodu.
- Z tohoto důvodu může dojít ke dvěma chybám – chybnému přijetí a chybnému odmítnutí.
- Při chybném přijetí je podvodník nesprávně identifikován jako oprávněný uživatel, při chybném odmítnutí naopak není autorizování uživatel rozpoznán a je označen za podvodníka.
- Výskyt těchto dvou chyb je úzce spjat s vlastnostmi konkrétního biometrického systému a nastavenou úrovní zabezpečení. Je-li prahová hodnota příliš vysoká, dochází častěji k chybným odmítnutím a méně k chybným přijetím.
- Na druhou stranu při nízké prahové hodnotě se uživatelé mohou frekventovaněji setkat a méně často s chybným odmítnutím.

# FAR, FRR A ERR I

- V praxi se hodnoty chybného přijetí a chybného odmítnutí neuvádějí v absolutních číslech, ale jejich relativní ekvivalentech.
- Jsou jimi míra chybného přijetí (False Acceptance Rate, FAR) a míra chybného odmítnutí (False Rejection Rate, FRR).
- FAR a FRR vyjadřují pravděpodobnost výskytu dané chyby v procentech.



# FAR,FER a ERR II

- Z povahy popisovaných chyb vyplývá, že čím nižší je FAR, tím vyšší je FRR, a naopak.
- Obě míry jsou závislé na nastavené prahové hodnotě.
- Toto nastavení závisí na konkrétním způsobu použití daného biometrického systému v praxi podle toho, zda je větší pohromou někoho chybně přijmout nebo chybně odmítnout.
- Hodnotám při které se FAR a FRR rovnají, se označují jako míra rovné chyby (Equal Error Rate, ERR).
- Podle ERR lze alespoň přibližně určit bezpečnost biometrického systému, nicméně FAR a FRR mají daleko vyšší vypovídací hodnotu.

# Biometrika

## Biometrika ruky

# Biometrika ruky

- Lidská ruka každého u nás hned několik unikátních a zároveň měřitelných vlastností.
- Nejznámější a v praxi nejrozšířenější z nich je bezesporu otisk prstu, ale kromě toho lze měřit také geometrii ruky, dynamiku podpisu, dynamiku psaní na klávesnici, vzor krevního řečiště,  tvar lůžka nehtu nebo absorpční spektrum lidské kůže.

# Biometrika Otisku prstu

- Technologie otisku prstu má mnoholetou bohatou historii, z níž pravděpodobně nejznámější je její aplikace ve forenzní sféře.
- Díky daktyloskopii bylo odhaleno mnoho zločinců – získávání, porovnávání a vyhodnocování shody otisku prstu se stalo nedílnou součástí většiny vyšetřování.

# Historie biometriky  otisku prstu

- Jedny z nejstarších vyobrazení otisků prstu sahají do doby několika set let před naším letopočtem.
- Právě z tohoto období totiž pocházejí asyrské hliněné tabulky, na jejichž úlomcích se nacházejí jména lidí s otisky jejich prstů.
- V roce 1880 publikoval Angličan Henry Faulds článek zabývající se snímáním otisku prstu pomocí inkoustu.
- Faulds je zároveň považován za prvního člověka, kterému se podařilo získat otisk prstu z předmětu – jednalo se o láhev.
- Základy moderní daktyloskopie publikoval v roce 1888 anglický přírodovědec Francis Galon.
- Za první úspěch je považován vyřešení případ v Argentině v roce 1892.

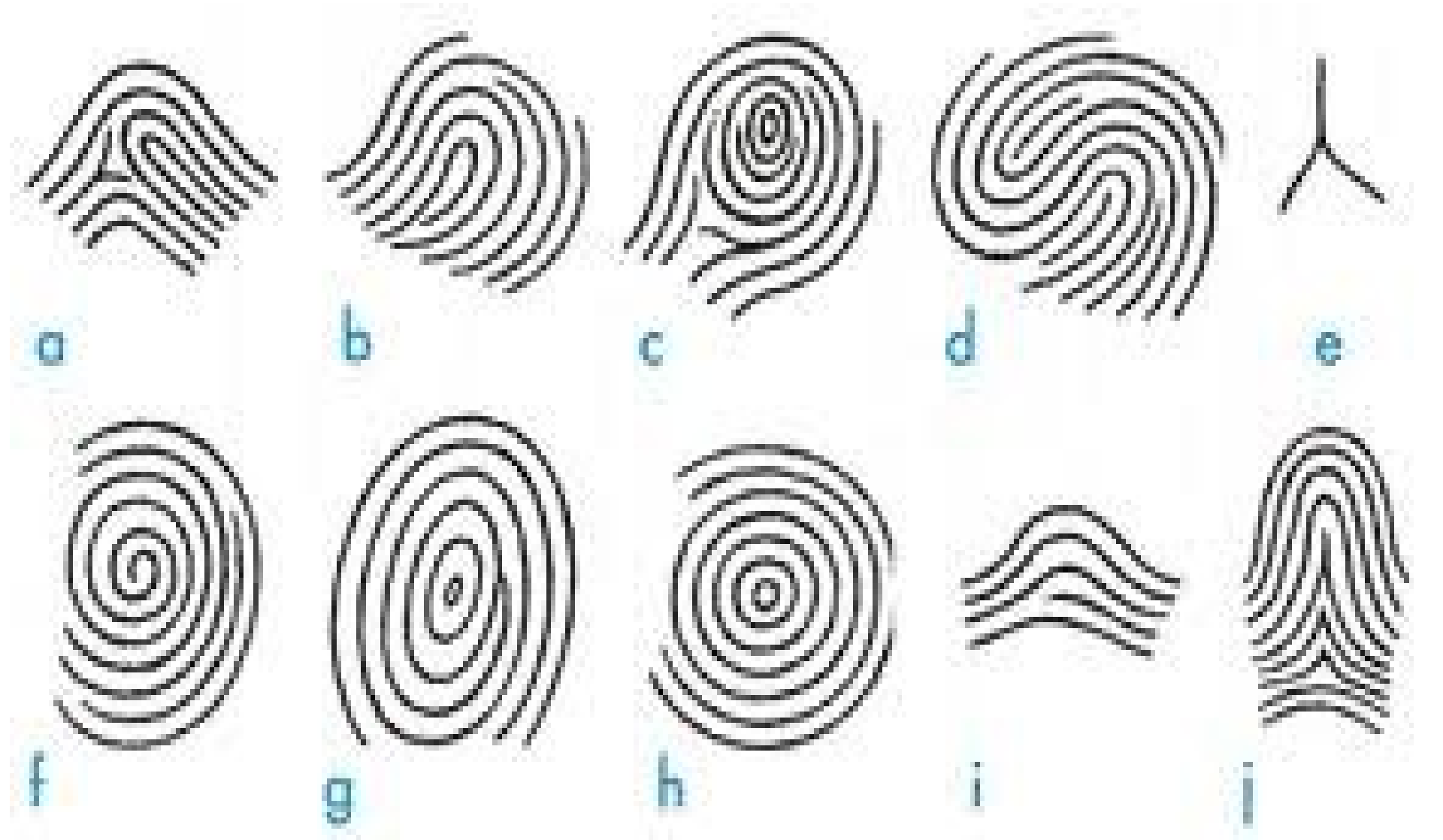
# Klasifikace vzorů otisku prstu

- Podíváte-li se zblízka na bříška svých prstů, zaregistrujete drobné prolákliny a vyvýšeniny.
- Vznikají tak, že škára  vybíhá proti pokožce v takzvaných papilách – odtud také pochází používaný výraz papilární linie.
- Vzory se dělí do tří základných skupin:
- **Oblouk** – papilární linie vytvářejí jednoduché oblouky. Vzor neobsahuje tzv. delty, útvary, v nichž se papilární linie rozbíhají do tří směrů.
- **Vír** – papilární linie vytvářejí kruhové, oválné nebo spirálovité obrazce s jádrem uprostřed. Vzor musí obsahovat alespoň dvě delty a alespoň jednu samostatně probíhající linii.
- **Smyčka** – Papilární linie vytvářejí smyčku. Mezi deltou a středem musí být alespoň jedna probíhající linie.

# Význačné znaky

- Rozdělením otisků prstů do podskupin podle uvedené klasifikace se redukuje množství relevantních vzorů.
- Vlastní identifikace je však založena na nalezení a porovnání význačných znaků, takzvaných markantů, které papilární linie vytvářejí.
- Existuje několik druhů markantů, např. body (velmi malé rýhy), ostrůvky (rýhy a málo větší než body ležící v prostoru mezi rozdvojenou rýhou) či můstky (malé rýhy spojující dvě sousední rýhy).
- Otisk prstu většinou obsahuje mezi 75 až 175 markanty, přičemž některé z nich se vyskytují častěji než jiné.

# Vzory papilárních linií



# Algoritmy rozpoznání otisků I

- Při rozpoznávání otisků prstů se používají dva základní principy – zkoumání podle globálního vzoru nebo podle podrobností.
- V případě zkoumání globálních vzorů je daný otisk zařazován do některé ze skupin klasifikace.
- V otisku prstu se vyhledává základní vzor, oblast vzoru, delty a počítají se také např. jednotlivé papilární linie.
- Zkoumání globálního vzorů nemá příliš vysoké nároky na rozlišení pořízených snímků, většinou postačuje hustota kolem 250dpi, a rozpoznání je úspěšné i při drobných poraněních prstů.

# Algoritmy rozpoznání otisků II

- Oproti tomu zkoumání otisku podle podrobností využívá přítomnost markantů, kdy se ukládá např. jejich typ, pozice v otisku a orientace.
- Při porovnávání podrobností snímaná předloha otisku prstu nejprve upravena a až poté se vyhledávají jednotlivé markanty.
- První fáze představuje takzvanou binarizaci obrazu otisku prstu, při níž se z nasnímané předlohy vytvoří černobílý obraz a vzory jednotlivých papilárních linií se ztenčují až na velikost jednoho pixelu.
- V předpracovaném obrazu již lze přistoupit k vyhledávání a extrakci identifikačních bodů.

# Algoritmy rozpoznání otisků III

- Na konec může konečně proběhnout vlastní porovnání otisků prstů, když se zkoumají a porovnávají vlastnosti nalezených markantů.
- Zkoumání podrobností vyžaduje zhruba dvojnásobné rozlišení použitého snímače než u globálních vzorů.
- Při poranění prstu mohou být následné změny otisku chybně detekovány jako markanti a oprávněný uživatel neidentifikován.

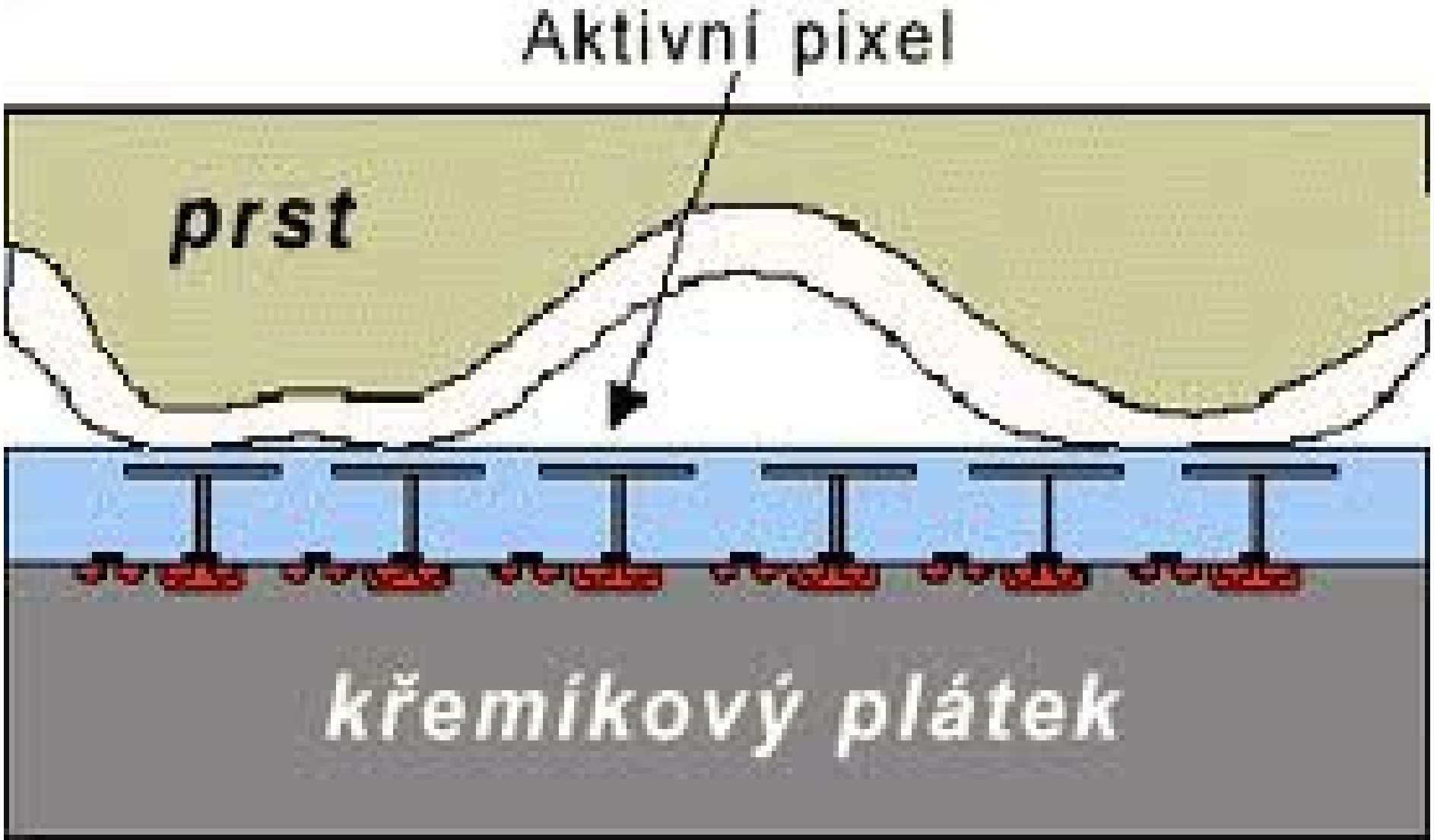
# Typy snímání otisků prstů I

- Optické snímače otisků –
  - Jedná se o nejstarší a nejrozšířenější způsob snímané prstů. Funguje na základě rozdílného rozptylu nebo odrazu světla v bodech, kde se stýkají papilární linie přiloženého prstu se snímací plochou.
  - Prst přiložený na plochu snímače je nejprve osvícen. Světlo se odrazí od pokožky prstu a po postupném průchodu hranolem, optickým filtrem a čočkou dopadá na CCD detektor.
  - Pomocí něho je obraz otisku digitalizován a následně zpracován algoritmem pro rozpoznání otisku prstu.
  - Světlo, které po průchodu snímací, hranolem dopadne do rýhy prstu, není odraženo zpět směrem k CCD detektoru, naopak je odraženo světlo, jež dopadlo na papilární linii.

# Typy snímání otisků prstů II

- Kapacitní snímače
  - Tento typ snímače (též nazývaných silikonové) měří kapacitní odpor v ploše dotyku.
  - Silikonový plátek snímacího zařízení funguje jako deska kondenzátoru a přiložený prst jako druhý.
  - Vyvýšené linie povrchu prstu jsou více přilehlé než prostory mezi nimi, a mají tak vyšší kapacitní odpor.
  - Měřením napětí na kondenzátoru lze určit místa (pixely), na kterých se prst dotýká snímače těsněji než na jiných, a podle získaných hodnot následně sestavit obraz otisku.

# Kapacitní snímač otisků



# Typy snímání otisků prstů III

- Ultrazvukový snímač
  - Ultrazvukový snímače nejsou tolik rozšířené jako jejich optičtí nebo kapacitní kolegové.
  - Mezi důvody patří také fakt, že se jedná o poměrně novou metodu snímání otisků prstů.
  - Čtecí zařízení při použití této technologie vysílá ultrazvukové vlny a díky následnému měření odporu získá vzor papilárních linií na snímaném prstu.
  - Ultrazvukové snímače mají větší rozměry, tato nevýhoda je však vyvážena odolností vůči potu a nečistotám zachycením na prstu.

# Biometrika

## Geometrie ruky

# Biometrie Geometrie ruky

- Každý člověk má jinak tvarovanou ruku a tento tvar se u dospělého člověka během života nemění (pokud neutrpěl zranění).
- Toho využívají biometrické systémy založené na geometrie ruky.

# Proces snímání I

- Jako první vytvoříme celkový obraz ruky.
- K tomuto účelu bývají nejčastěji využívány optické snímače, které vytvoří černobílý snímek obsahující siluetu ruky.
- Jen málo uživatelů je schopno správně vložit ruku na snímač a proto jsou zde speciální kuličky do, kterých člověk vloží ruku a to zaručuje přesnou identifikaci.
- Tento postup má výhodu, že do snímání nevstupují detaily jako škrábance nebo zachycené nečistoty.
- Výsledná šablona obsahuje informace o měřitelných prvcích ruky, tedy např. o délce a šířce prstů.
- Pro porovnávání vzorků lze použít např. algoritmus vzájemné konfrontace nasnímaných siluet.

# Proces snímání II

- Při tomto postupu se nejprve z obrazu získaného kamerou musí odstranit obrazy kolíčků – což však není problém, protože ty mají při každém snímání stejnou polohu.
- Ze získaných obrazu ruky potom dochází k postupnému porovnávání jednotlivých prstů, jehož výsledkem je seznam bodů, ve kterých se obě siluety shodují.

# Snímání geometrie ruky

# Výhody a nevýhody

- Popisované biometrická technologie se nevyznačuje nijak vysokou přesností, a proto bývá používaná především při verifikaci, nikoliv identifikaci.
- Jak již bylo naznačeno výše, oproti snímání otisků prstů má tu výhodu, že ignoruje některé časem se měnící detaily jako pot, špínu či drobné poranění.
- Naopak lidé mající artritidu nebo jí podobnou vadu mohou mít problém s konkrétním vložením ruky do snímacího zařízení.

# Biometrie

## Dynamika podpisu

# Biometrie Dynamiky podpisu I

- Dynamika podpisu tato biometrická technika má původ v konvenčním pojetí podpisu, rozdíl je však v tom, že namísto vizuální podoby se vzorem dochází k porovnávání vlastního průběhu psaní.
- Měří se především rychlost, tlak na podložku, styl jednotlivých tahů apod.
- Oproti doposud popisovaným biometrickým technologiím patří dynamika podpisu mezi behaviorální charakteristiky.
- Klasický podpis lze např. oskenovat a takto pořízený falzifikát následně zneužít.
- Naproti tomu systémy měřící dynamiku podpisu porovnávají podpis se vzorem ve čtyřech rozměrech najednou.

# Biometrie Dynamiky podpisu II

- Oproti tradičním dvěma dimenzím roviny přibývá ještě tlak speciálního podpisového pera na podložku a čas.
- I v případě, že budete sledovat něčí styl podepisování, nemáte s následným kopírováním jeho pohybů příliš šancí na úspěch.
- Na rozdíl od některých jiných biometrických technologií má dynamika podpisu výhodu v tom, že se jedná o modernizaci konvenčního podpisu, společností již dlouhou dobu akceptovaného, a pro uživatele je tedy naprosto přirozená a důvěryhodná.
- Lidé, jejichž dynamika podpisu se vždy výrazně liší, mohou mít při použití této biometriky problémy s korektní verifikací.

# Biometrika

## Tvar krevního řečiště ruky

# Biometrie Tvaru krevného řečiště ruky

- Jedná se o velmi málo známou a rozšířenou biometrickou metodu, podle níž dokonce i jednovaječná dvojčata disponují odlišnými vzorky.
- Podobně jako u technologie dynamiky stisku kláves, ani pro snímání krevního řečiště ruky není zapotřebí nákladný hardware a taktéž algoritmy provádějící extrakci vzorů nejsou příliš náročné.
- Tvar krevního řečiště se měří buď na dlani, nebo na hřbetu ruky.

# Biometrika tvaru krevního řečiště postup I

1. Při snímání uživatel vloží ruku do čtecího zařízení. V něm umístěný zdroj infračerveného zařízení pořídí obraz snímané ruky. Výhodou je, že do snímání nevstupují nečistoty, aktuální vlhkost kůže či drobné poranění, které dokáží zapříčinit chybnou verifikaci při snímaní otisků prstů.
2. Díky infračervenému zařízení je pořízen snímek s barevnou hloubkou 256 odstínů šedi. Žíly toto zařízení pohlcují a vytvářejí zřetelnou síť tmavých čar, které reprezentují tvar krevního řečiště.
3. Obrázek tvořený odstíny šedi se ve třetím kroku zpracování převede na ekvivalent černobílý obraz. Rychlost tohoto procesu ve velké míře ovlivňují výslednou rychlost celého snímání.

# Biometrika tvaru krevního řečiště postup II

4. Vzor krevního řečiště se dále upravuje tak, aby jednotlivé žíly byly co nejtenčí. Tato fáze připomíná ztenčování papilárních linií až na velikost jednoho pixelu v případě snímání otisku prstu.
5. Nyní již lze konečně přistoupit k měření charakteristických znaků zkoumaného krevního řečiště a výsledná data porovnat s referenční šablonou.

# Biometrika

## Tvar lůžka nehtu

# Tvar lůžka nehtů

- Zástupce exotické biometrické technologie je tvar lůžka nehtů.
- Podíváme-li se na svůj nehet, zjistíme že jeho povrch zdaleka není rovný.
- Při svém růstu totiž nehet kopíruje tvar lůžka nehtu, které se nachází pod ním, a tím získávají svůj vlnitý tvar.
- Nejen že dva vybraní jedinci mají odlišný tvar lůžka nehtu vybraného prstu, ale dokonce každý prst má lůžko jinak tvarované, takže např. ukazováček, má jinak zvlněný nehet než prostředníček.
- Mezi nehtem a lůžkem pod ním se nachází přírodní polymer keratin, jenž dokáže měnit orientaci polarizovaného světla.
- Při osvícení pod správným úhlem tak lze analyzovat fázové změny paprsku po odrazu a jako výsledek získat reprezentaci lůžka nehtu, která připomíná čárový kód.

# Biometrika

## Biometrika hlavy

# Biometrika hlavy

- Hlava je také část těla, která obsahuje několik unikátních charakteristik. Například snímání oční duhovky nebo sítnici patří k nejpřesnějším biometrikám vůbec.
- Rozpoznání člověka podle obličeje sami provádíme několikrát denně, proto se asi není divu, že i tímto směrem se ubírá výzkum biometrických technologií.

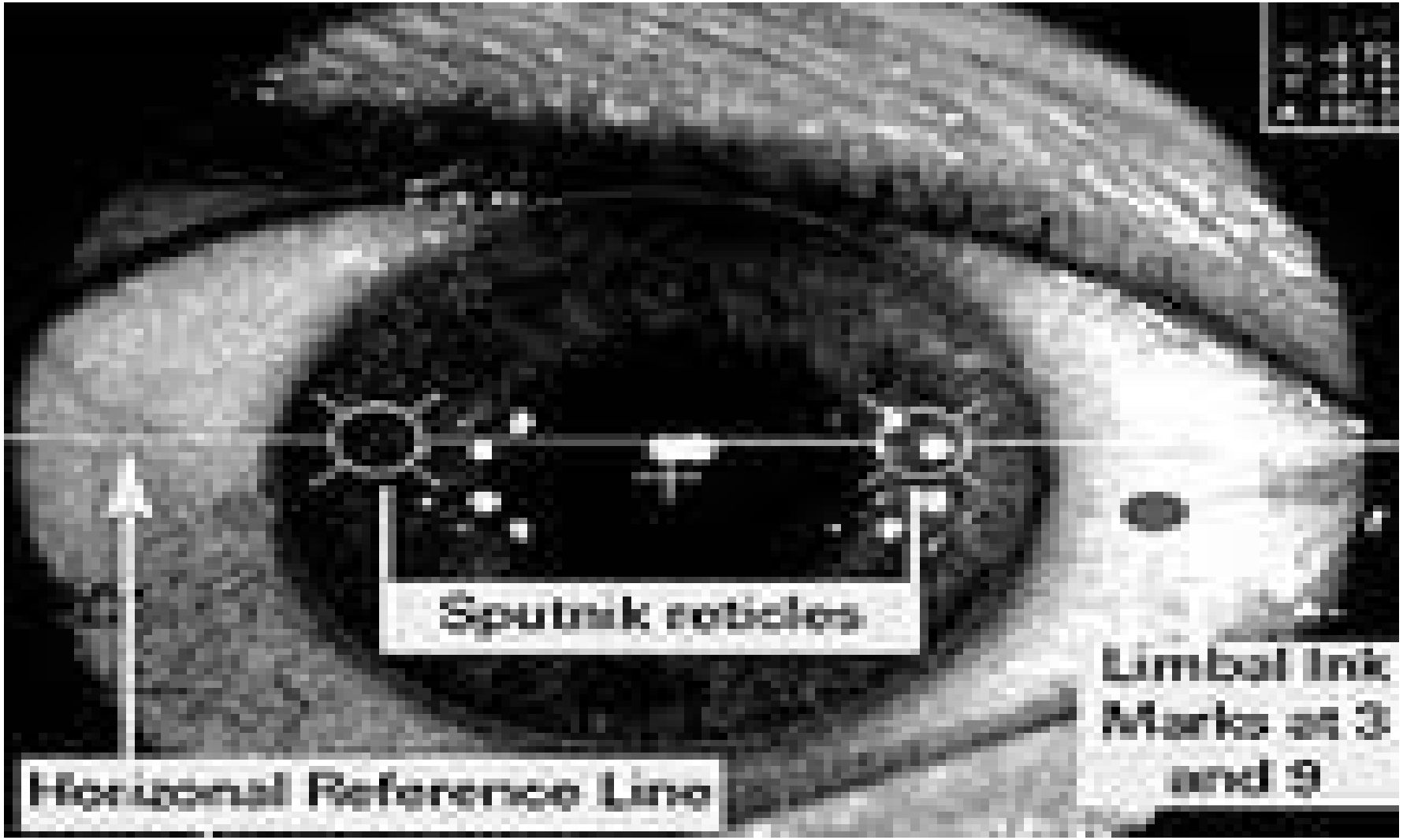
# Biometrika Oční duhovky I

- Oční duhovka každého člověka je jedinečná a nemění se během let.
- Jedná se o nejlepší a nejpřesnější biometrický systém.
- Jde o pigmentovanou membránu obklopující zřítelnici oka.
- Při detailním zkoumání lidského oka můžete zjistit, že duhovka má několik jasných charakteristik – jsem patří záhyby, skvrny, rýhy, krypty.
- Identifikace biometrickými systémy je založena na digitalizaci těchto rysů a jejich následné srovnání s registračními vzorky uložených v databázi.

# Biometrika Oční duhovky II

- Vyjmenované charakteristiky:
  - Krypty – jedná se o velmi tmavá místa, kde je duhovka poměrně tenká. Zpravidla se nalézají poblíž rozhraní mezi řasnatou a zornicovou oblastí.
  - Radiální rýhy – Začínají poblíž zornice a paprskovitě vybíhají směrem k okraji duhovky.
  - Pigmentové skvrny – náhodné shluky pigmentových buněk u povrchu duhovky. Vyskytují se v řasnaté oblasti.
  - Pigmentové záhyby – vznikají jako důsledek vystupující spodní vrstvy duhovky v blízkosti zornice.

# Oční duhovka



# Biometrika Oční duhovky III

- Postup čtení:
  - Digitální kamera umístění uvnitř čtecího zařízení pořídí černobílý snímek lidského oka, který se vyznačuje vysokým rozlišením.
  - Získána fotografie je dále zpracována softwarem lokalizující vnitřní a vnější okraje duhovky a dochází k výpočtu šablony.
- Současnost:
  - V současnosti je tento způsob využíván ve vládních agenturách, ale i ve věznicích.
  - Výhodou je identifikaci s velkou přesností, ale vysokými náklady na pořízení.

# Biometrika

## Oční sítnice

# Biometrika Oční sítnice I

- Jedná se o světlo citlivý povrch zadní strany oka.
- Je složen z nervových buněk tyčinky a čípků, které převádějí přicházející světelné paprsky na nervové signály.
- Tyčinky poskytují černobílý a čípky barevné vidění.
- Oční nerv vystupuje z oka v místě, kde se nenacházejí žádné tyčinky ani čípky.
- Označujeme je pojmem slepá skvrna.
- Popisovaná biometrická technologie porovnává právě struktura sítnice v okolí slepé skvrny.
- Vlastní snímání se provádí zaměřením infračerveného paprsku o nízké intenzitě skrz zornici na vzor cév nacházející se na zadní straně oka.

# Biometrika Oční sítnice II

- Mezi výhody skenování oční sítnice patří vysoká přesnost.
- Nevýhody však tuto dispozici převáží, a biometrické systémy snímající tuto charakteristiku tak nejsou příliš oblíbené ani rozšířené.
- Vstupní čtecí zařízení je primárně konstruováno pro uchycení na zeď, což automaticky znepříjemňuje nebo znemožňuje identifikaci osob „nevhodné“ výšky.
- Vlastní snímání dokonce patří j nejvíce nepříjemným a nepohodlným ze všech biometrických systémů.
- Jeho vysoká cena je nejvyšší nevýhodou této biometrické techniky.

# Biometrie

## Rozpoznání obličeje

# Biometrie Rozpoznání obličeje I

- Rozeznávání lidí podle jejich obličeje patří ke každodenní rutině každého z nás.
- V tomto ohledu se jedná o nejpřirozenější biometrickou technikou vůbec.
- Rozeznávání obličejů pomocí počítače se používá několik algoritmů, z nichž nejznámější je srovnávání šablon a měření geometrie obličeje.
- Technika srovnávání šablon není nepodobná klasickému policejnímu postupu porovnávání fotografií – právě pořízení šablona uživatelova obličeje je konfrontována s referenční šablonou uloženou v databázi.

# Biometrie Rozpoznání obličeje II

- Databáze obsahuje několik šablon obličejů a při srovnávání se určuje míra podobnosti s každou z nich.
- Pokud databáze obsahuje kolem 150 šablon, pak je pro rekonstrukci obličeje s přesností 99% zapotřebí pouze čtyřicet nejvíce se shodujících.
- V případě měření geometrie obličeje dochází k určování pozic vyznačených části obličeje, jakými jsou například oči, nos, ústa apod.
- Měřením vzdálenosti mezi nimi.
- Při použití této metody se z těchto snadno rozlišitelných prvků obličeje vytvoří číselný vektor, který uchovává naměřené hodnoty.

# Biometrika

## Biometrika ověřování hlasu

# Biometrika ověřování hlasu I

- Biometrická technologie ověřování hlasu se zakládá na odlišnosti vokálního traktu jednotlivých osob.
- Tvar a rezonance ústní dutiny, hlasivek, jazyka a zubů dokáží jednoznačně zformovat náš biometrický vzorek.
- První výzkumy a experimenty s identifikací pomocí verifikace hlasu proběhly již začátkem sedmdesátých let a v současné době je tato technologie stále velice intenzivně zkoumání a zdokonalována.
- Ačkoliv je to na první pohled možná méně zřejmě, rozpoznávání hlasu člověk vysloví slovo, systém následně prohledá databázi a určí, které slovo odpovídá dané výslovnosti.

# Biometrika ověřování hlasu II

- Naproti tomu při ověřování hlasu je uživatelem vyslovená fráze porovnává s dříve pořízeným registračním vzorkem a systém určí, co bylo řečeno, nikoliv však kdo je mluvčím.
- Během fáze registrace každý uživatel vytvoří svůj vzorek, tzv. „otisk hlasu“. Z bezpečnostního hlediska je zřejmé, že delší věty a fráze poskytují vyšší stupeň zabezpečení něž krátká slova.
- V průběhu identifikace je člověk vyzván, aby vyslovil svou větu.
- Výhodou biometrického systému založených na verifikaci hlasu je jejich nízká hardwarová náročnost.
- Nevýhoda je pokud je člověk nemocní, systém poté špatně identifikuje uživatele.

# Biometrika

## Biometrika DNA

# Biometrika DNA I

- DNA je nový způsob identifikace osoby díky jeho DNA neboli krve.
- Pro identifikaci člověka podle jeho DNA ve skutečnosti postačuje obdržet jeho jednu jakoukoliv jadernou buňku.
- Mezi takovéto jaderné buňky patří např. bíle krvinka (leukocyt), kterou lze poměrně snadno získat ze slin nebo krve.

# Biometrika

## Biometrika Dynamika pohybu myši

# Biometrika Dynamika pohybu myši

- Podobně jako dynamika podpisu nebo stisku kláves snaží se také dynamika pohybu myši zařadit mezi akceptovatelné biometrické technologie.
- Uživatel je při verifikaci vyzván, aby pomocí myši nakreslil nějaký ( ve fázi stanovený( vzor).
- Verifikační proces tedy navenek připomíná např. použití nástroje tužky v programu malování ve Windows.

# Biometrika

## Biometrika Ucha

# Biometrika Ucha

- Biometrika ucha se zaměřuje na analýzu dvou charakteristik: tvaru ucha a ozvěny vracené kanálkem.
- V prvním případě se jedná o zkoumání vzdálenosti mezi význačnými body.
- Druhým způsobem je čtecí zařízení ve tvaru sluchátka do kterého se pustí určité zvuky a podle ozvěny se identifikuje uživatel.