

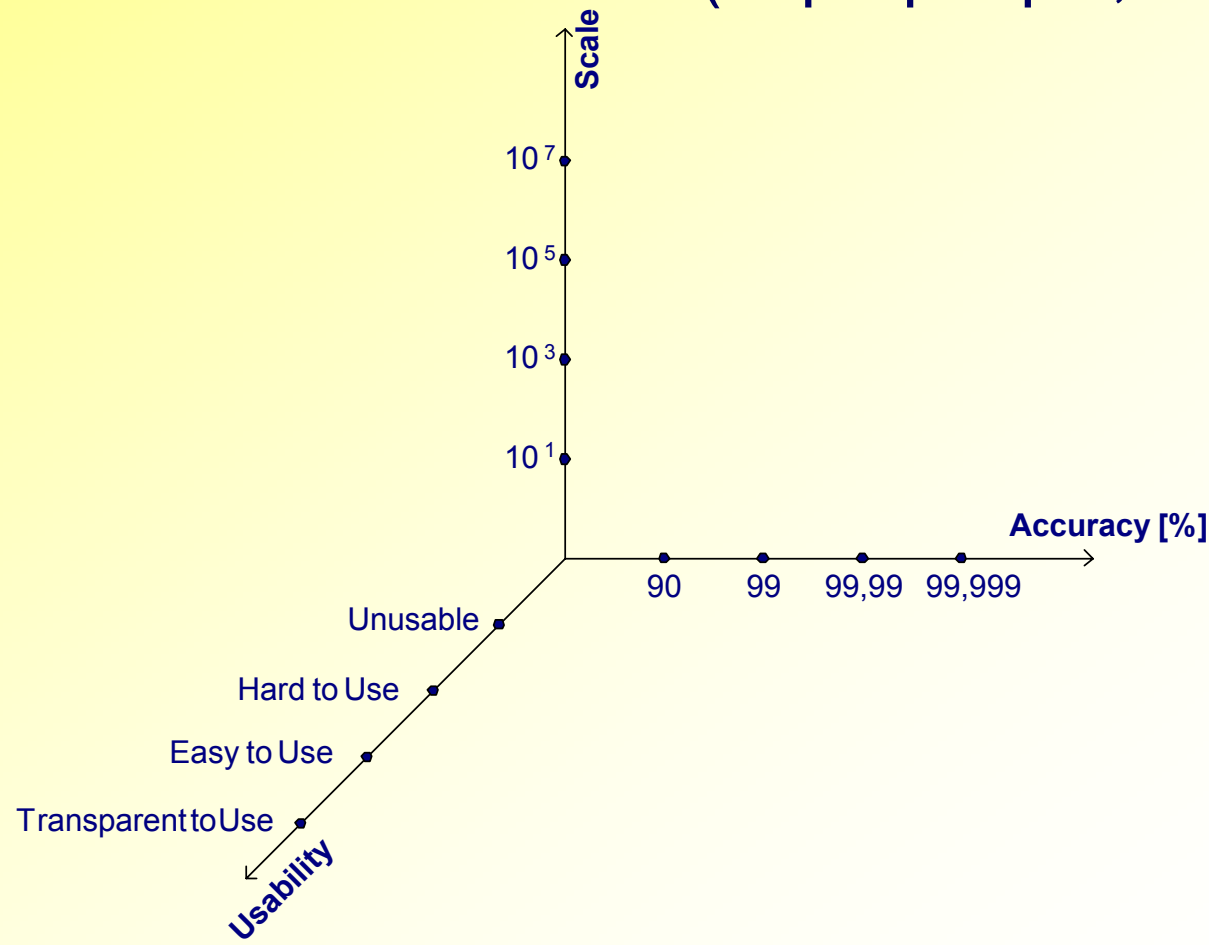


Přehled biometrických systémů a **testování jejich spolehlivosti**

Martin Dražanský (drahan@fit.vutbr.cz)
VUT v Brně, Fakulta informačních technologií, ÚITS

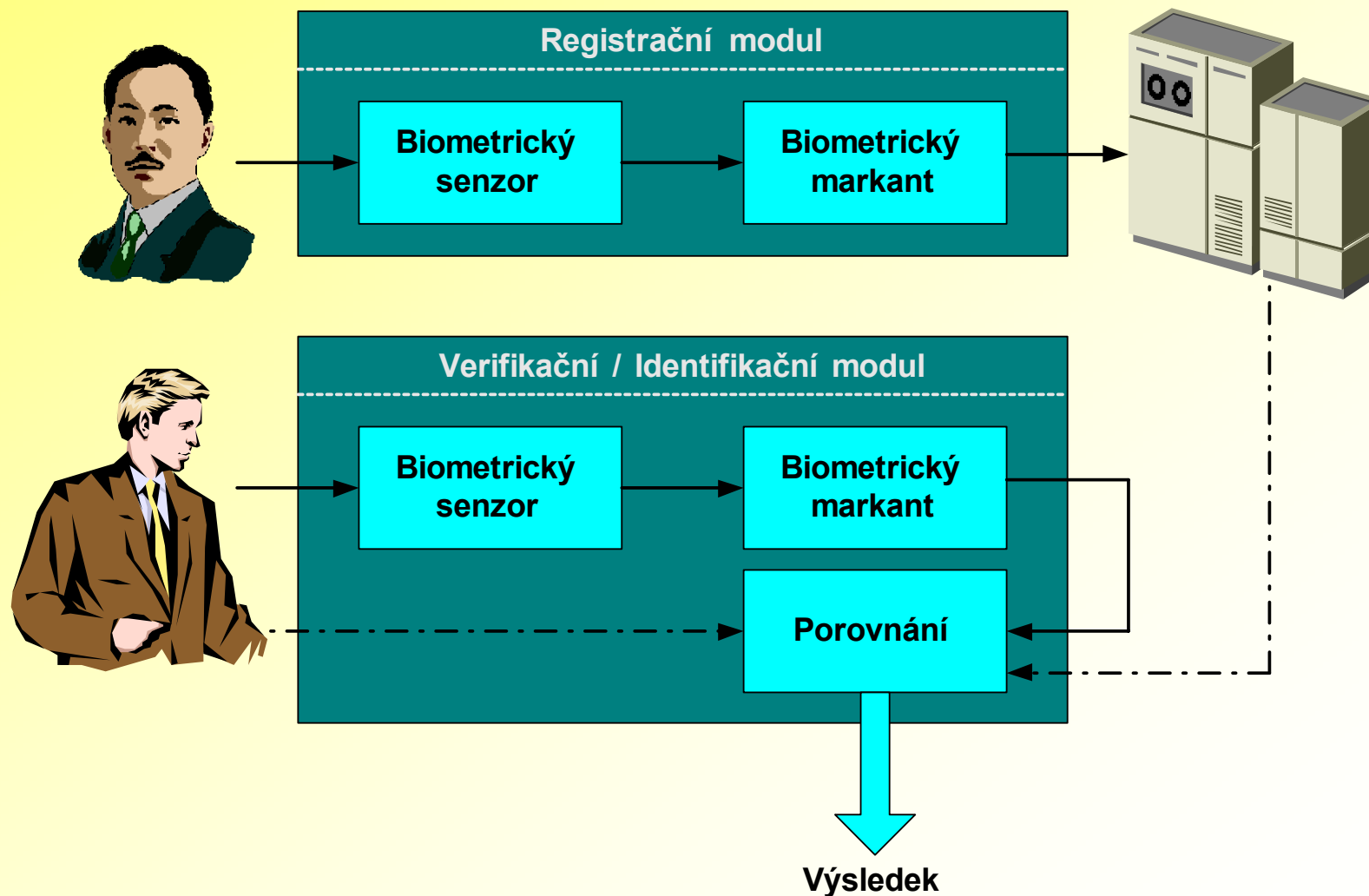
→ Definice biometrie:

Biometrie (IT) je automatické rozpoznávání lidí na základě jejich charakteristických *anatomických rysů* (např. obličej, otisk prstu, duhovka, sítnice) a charakteristického *chování* (např. podpis, chůze).



Biometrický systém

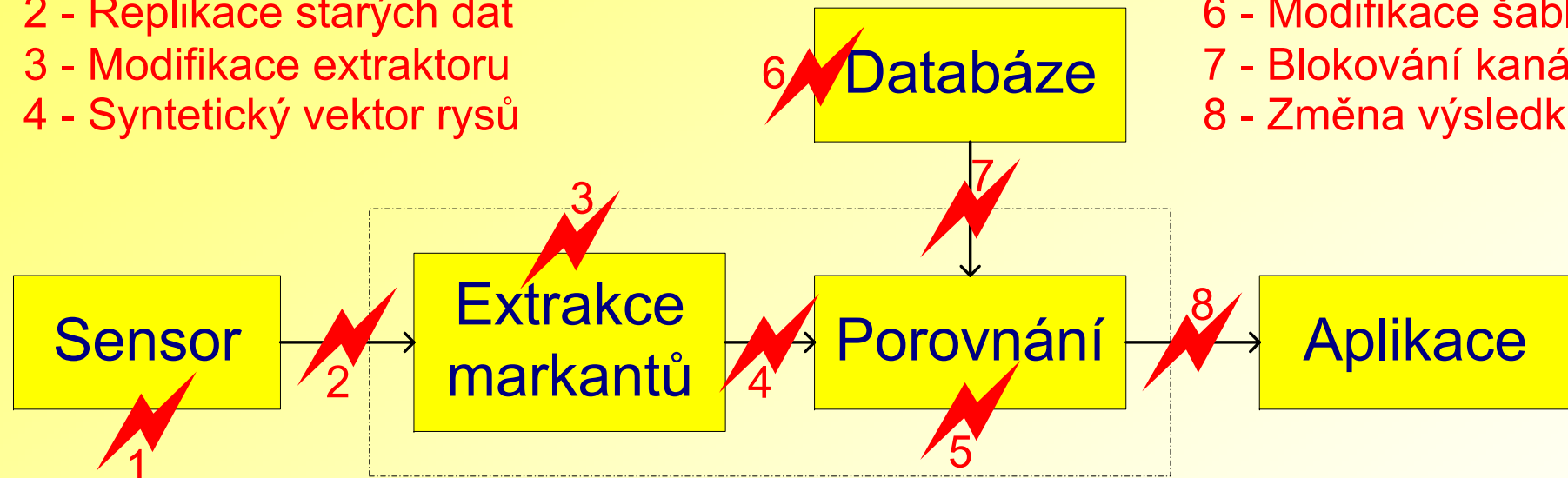
- ➔ Registrační modul - vložení identity uživatele
- ➔ Verifikační / Identifikační modul



Slabá místa biometrického systému

- 1 - Podvrh biom. vlastnosti
- 2 - Replikace starých dat
- 3 - Modifikace extraktoru
- 4 - Syntetický vektor rysů

- 5 - Změna porovnání
- 6 - Modifikace šablony
- 7 - Blokování kanálu
- 8 - Změna výsledku



- ➔ Příklad umělého otisku prstu
- ➔ Detekce živosti „*Liveness Recognition*“

Biometrické vlastnosti I.

Kongres Bezpečnosti sítí, Praha, 11.04.2007



DNA



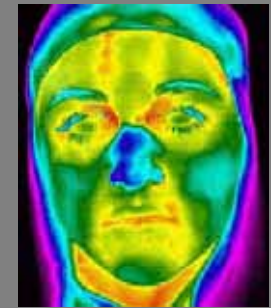
Otisk prstu



Duhovka



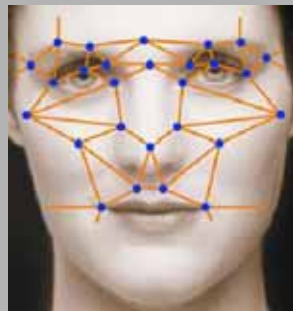
Sítnice



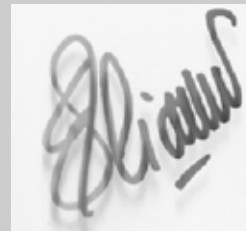
Termogram obličeje



Žíly ruky



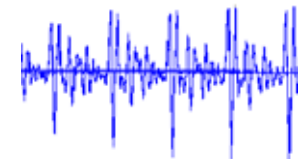
Obličej



Podpis



Geometrie ruky



Hlas

Biometrické vlastnosti II.

→ Anatomické (fyzické) vlastnosti:

→ Otisk prstu

→ Obličej

→ Duhovka oka

→ Sítnice oka

→ Geometrie ruky

→ Dlaň

→ Termogram obličeje

→ Termogram ruky

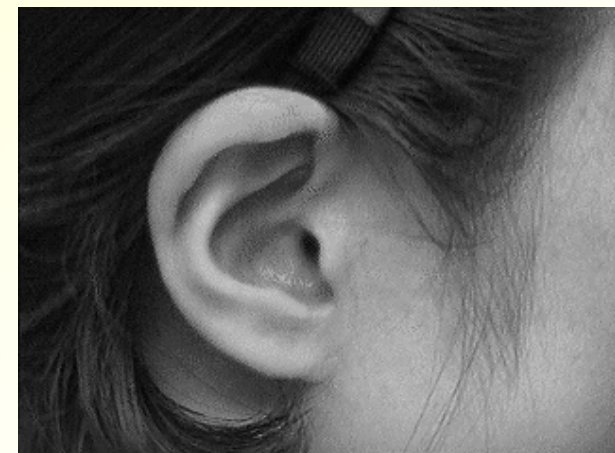
→ Dentální obraz

→ Podpis

→ Tvar ucha

→ Snímek nehtu

→ DNA



Biometrické vlastnosti III.

→ Dynamické vlastnosti (chování):

→ Hlas / Řeč

→ Gestikulace obličeje

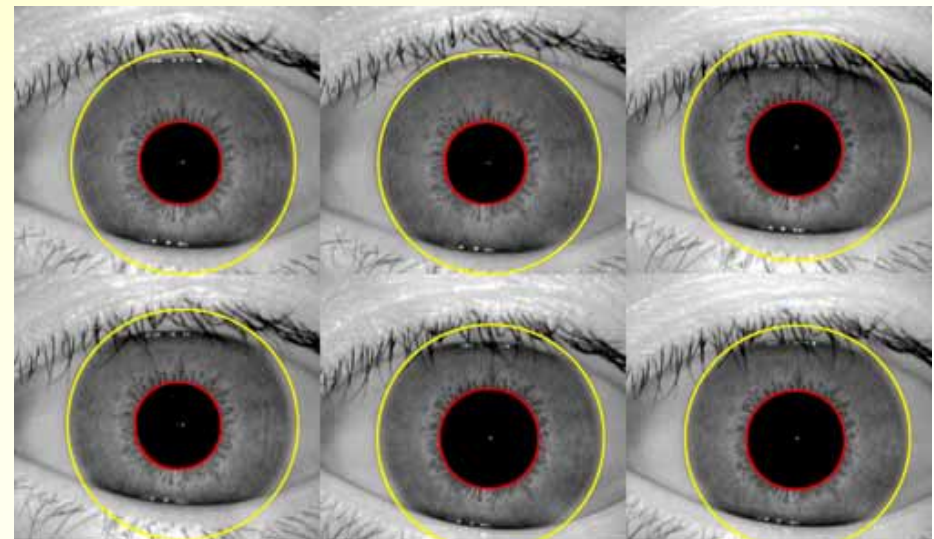
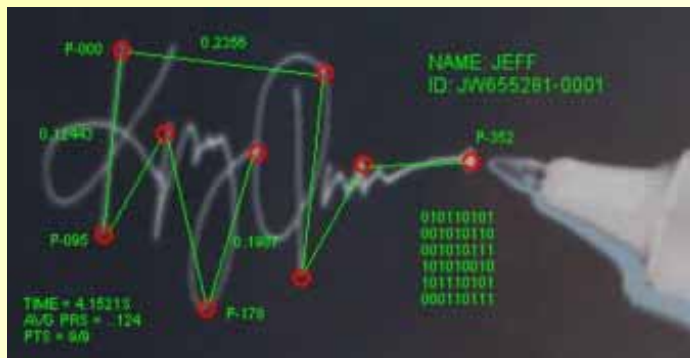
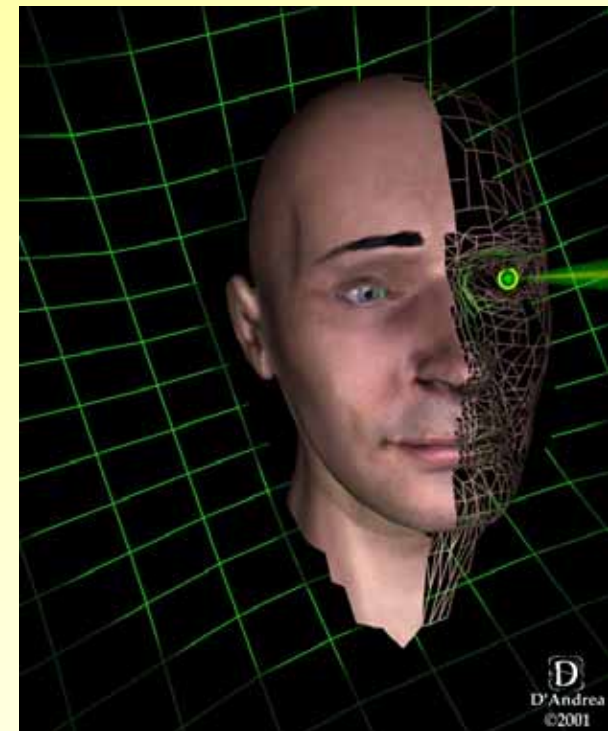
→ Podpis (dynamika)

→ Dynamika stisku kláves

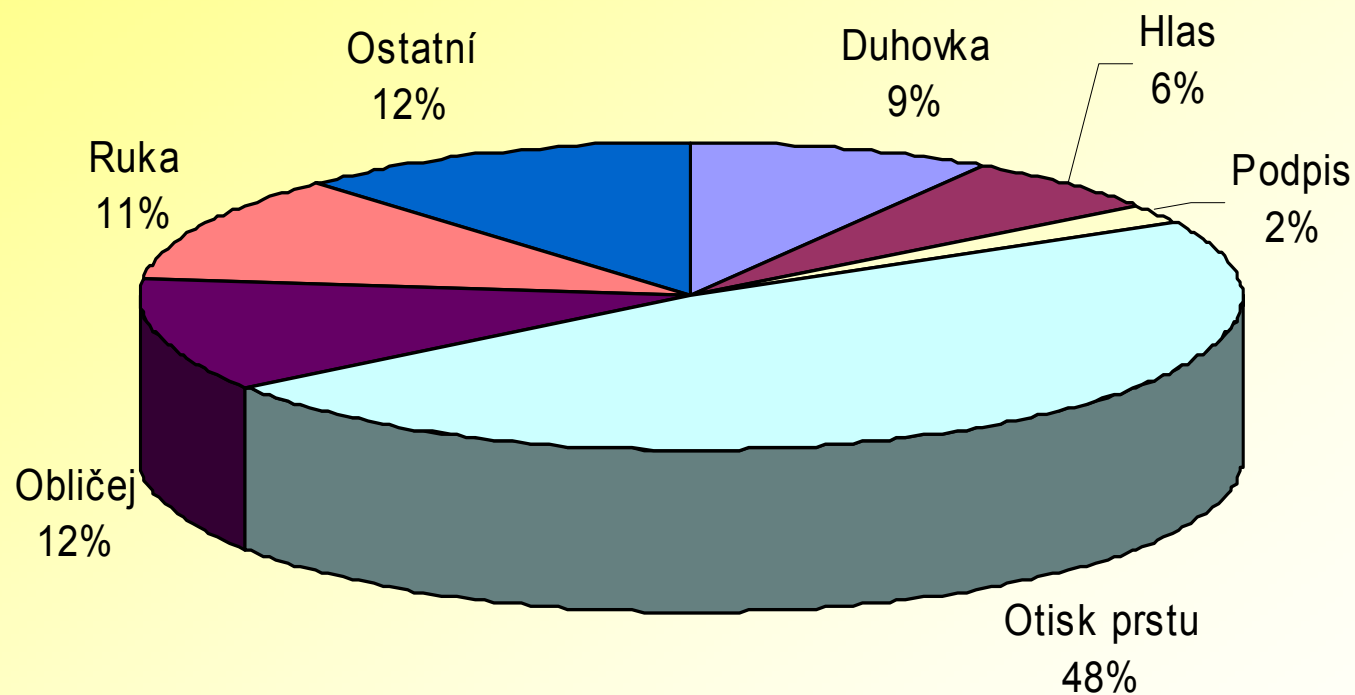
→ Pohyby rtů

→ Chůze

→ *Zužování duhovky*



Podíl jednotlivých biometrických vlastností na trhu



Zdroj: IBG, 2004

→ Identita

→ Rozlišovat fyzickou identitu od elektronické

→ Identifikace

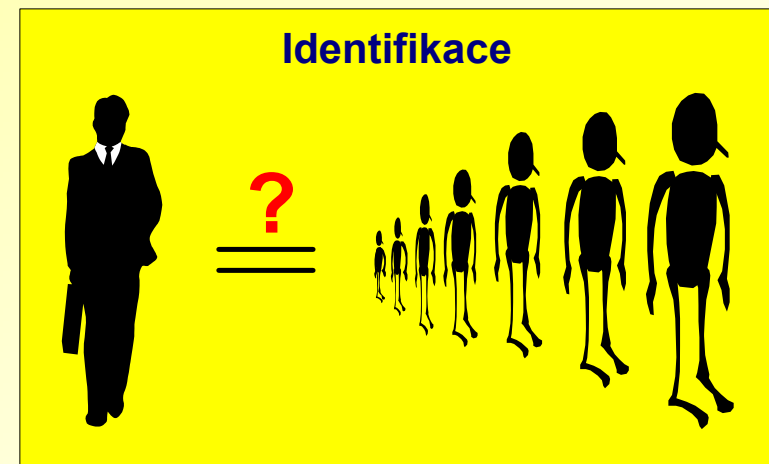
→ Porovnání 1:N

→ Verifikace

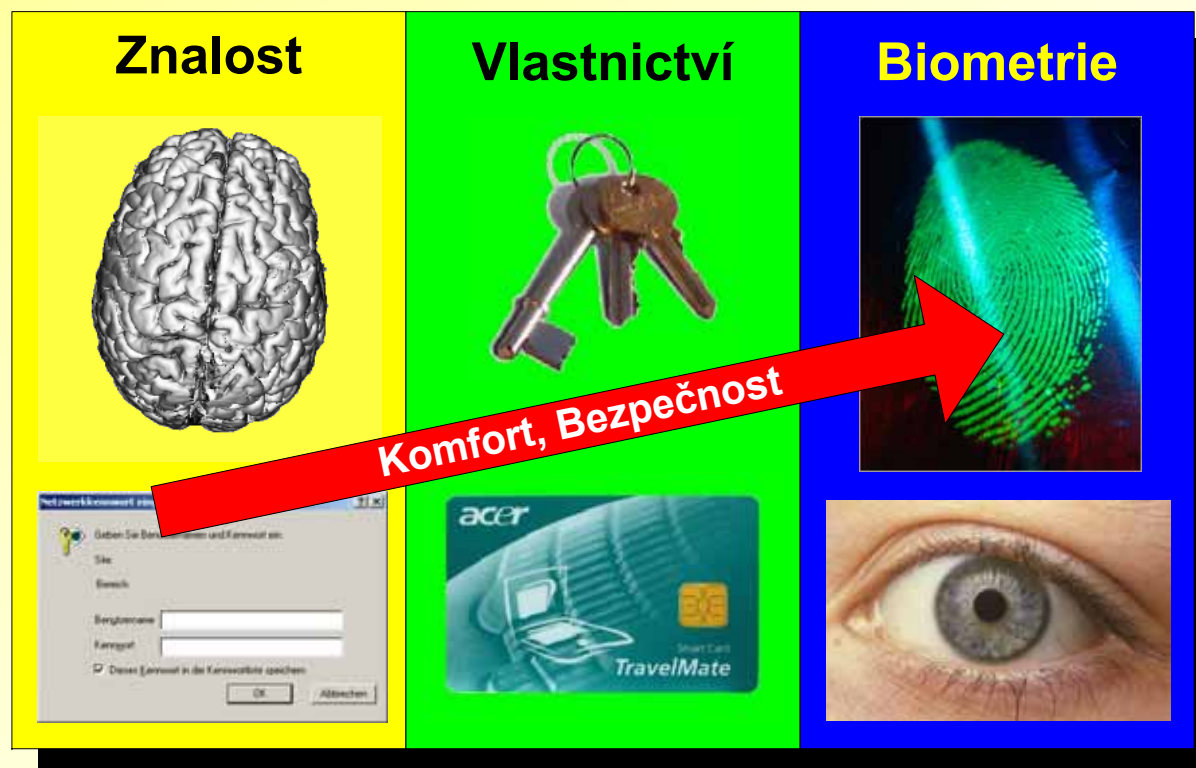
→ Porovnání 1:1

→ Autentizace

→ Potvrzení identity

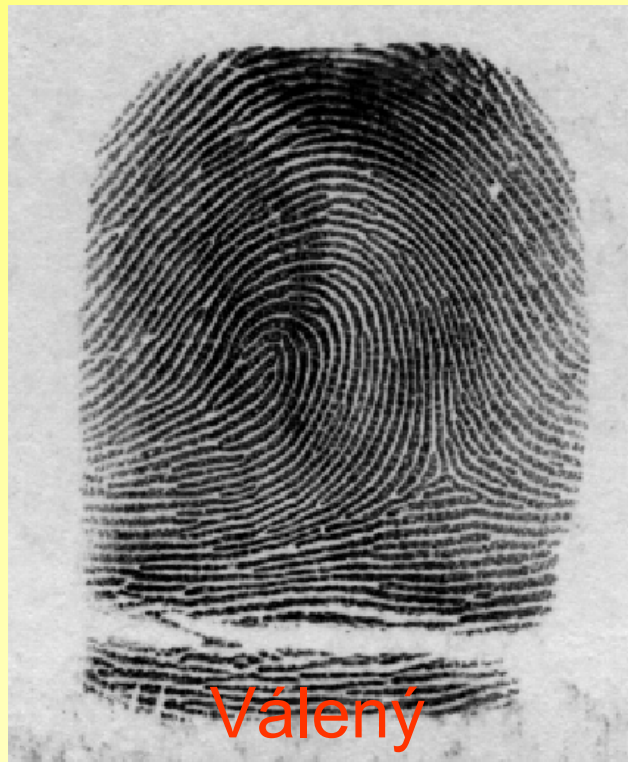


- Identita je založena na
 - něčem co víme („*we know*“)
 - něčem co máme („*we have*“)
 - něčem co jsme („*we are*“)

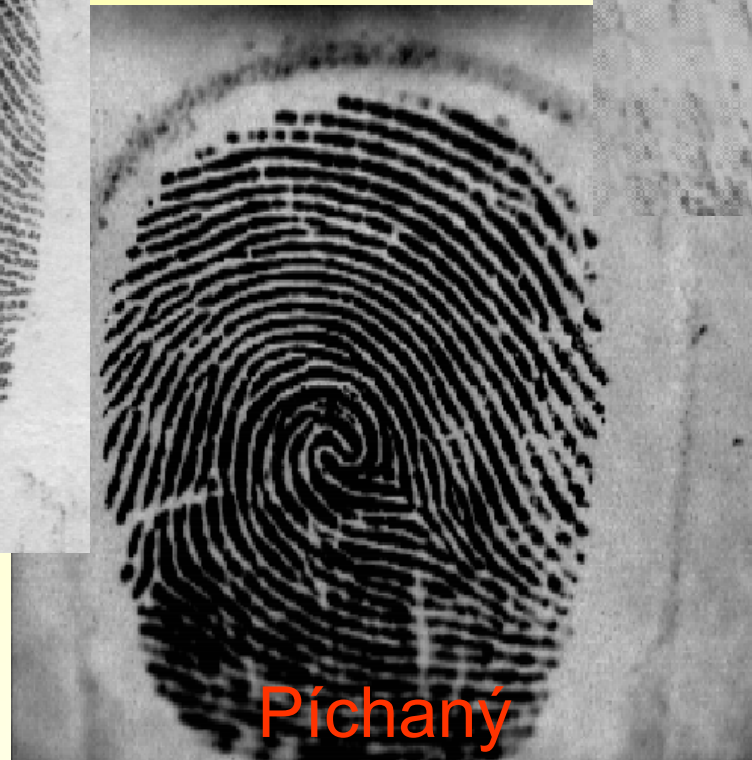


Rozpoznávání otisků prstů I.

- Existují 3 druhy otisků prstů:
 - Válený (barvený, rolovaný)
 - Píchaný (živý)
 - Latentní



Válený



Píchaný



Latentní

Rozpoznávání otisků prstů II.

→ Existuje relativně hodně principů technologií senzorů:

Optická technologie



Kapacitní technologie

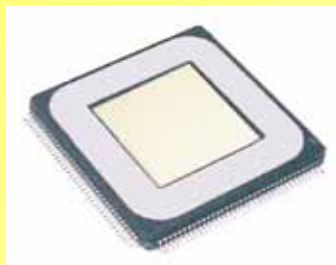


Ultrazvuková technologie



Rozpoznávání otisků prstů III.

Technologie E-Field



Elektrooptická technologie



Tlaková technologie

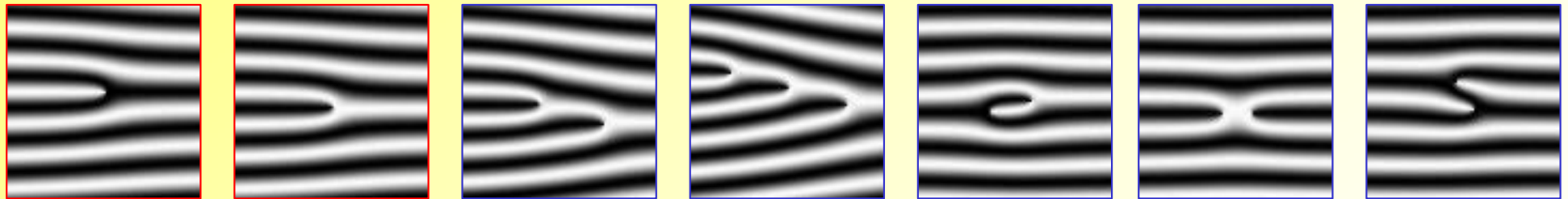


Termická technologie

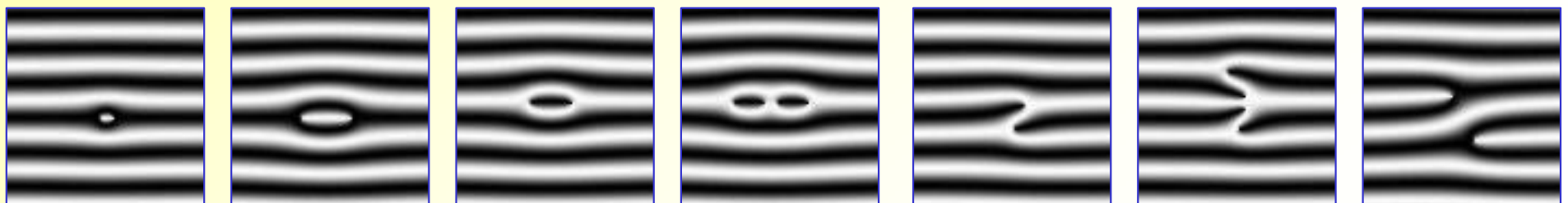


Rozpoznávání otisků prstů IV. (markanty)

- Ukončení (*Line Ending*), jednoduchá vidlička (*Simple Bifurcation*), dvojitá vidlička (*Double Bifurcation*), trojitá vidlička (*Triple Bifurcation*), hák (*Hook*), křížení (*Crossing*), boční kontakt (*Side Contact*)

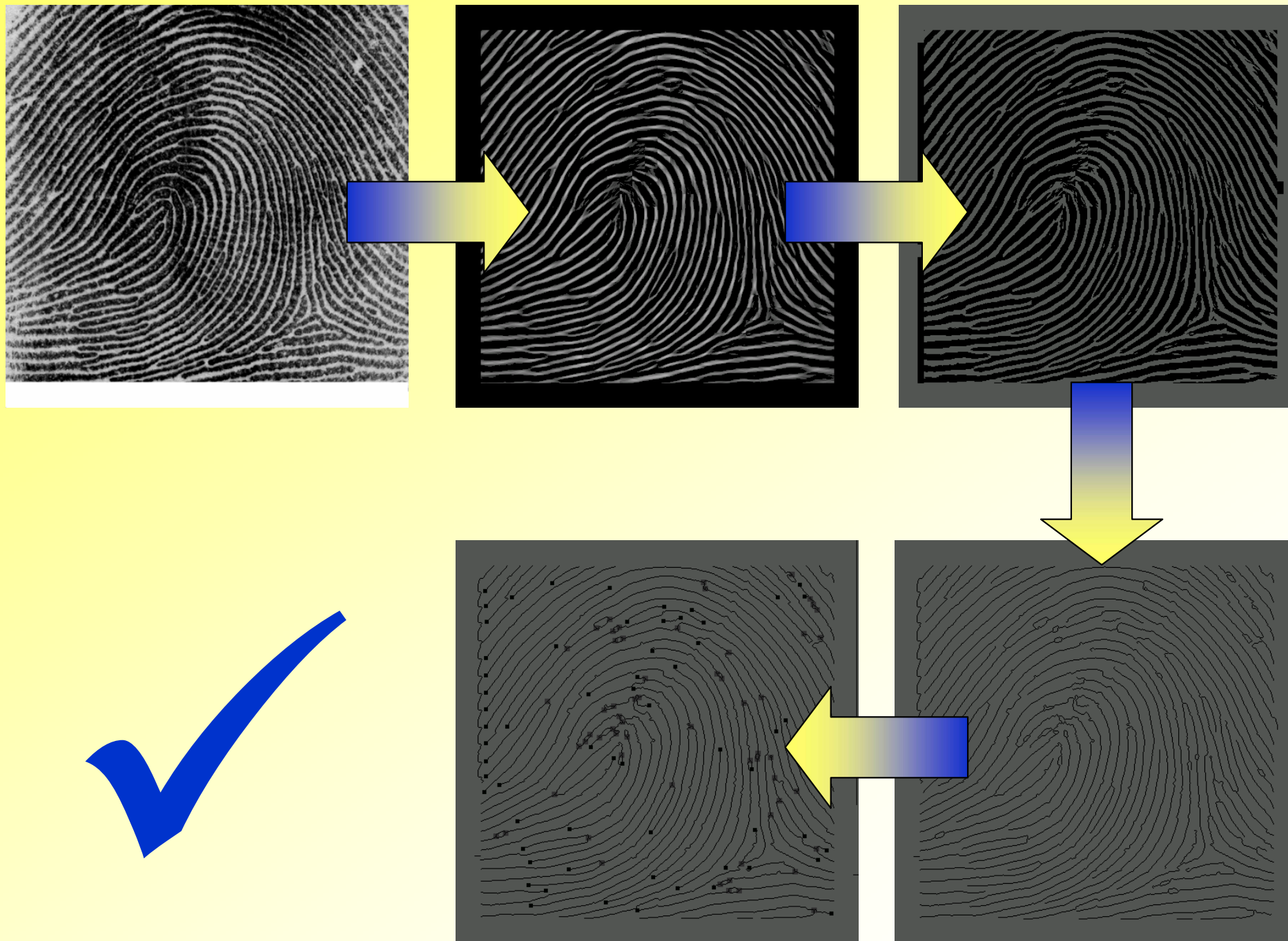


- Bod (*Point*), Interval (*Interval*), jednoduchá smyčka (*Single Whorl*), dvojitá smyčka (*Double Whorl*), jednoduchý most (*Single Bridge*), dvojitý most (*Twin Bridge*), průsečná linie (*Through Line*)

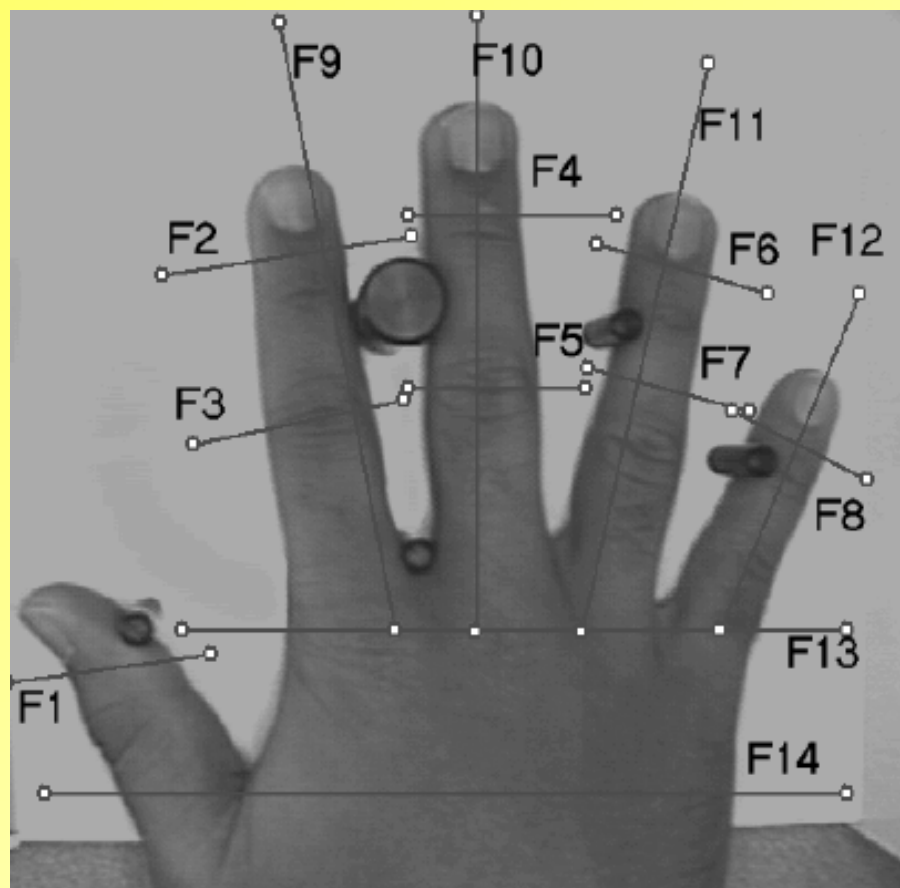


Rozpoznávání otisků prstů V.

Kongres Bezpečnosti sítí, Praha, 11.04.2007

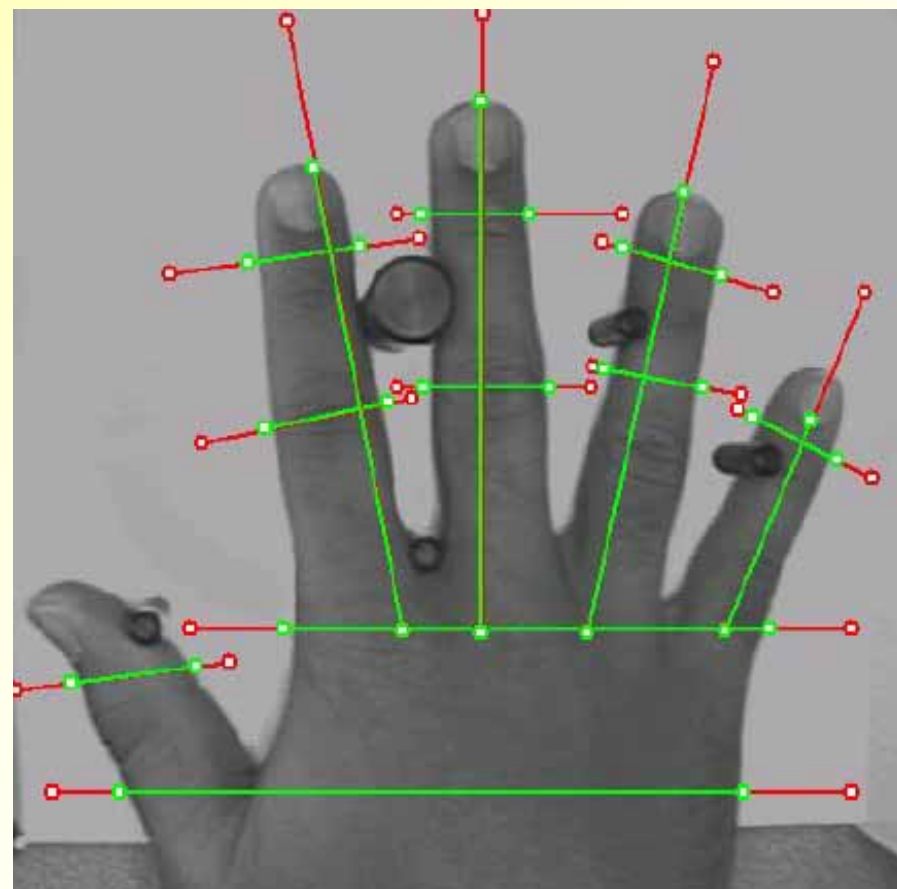


Rozpoznávání geometrie ruky I.



Osy měření

Hodnoty rysů



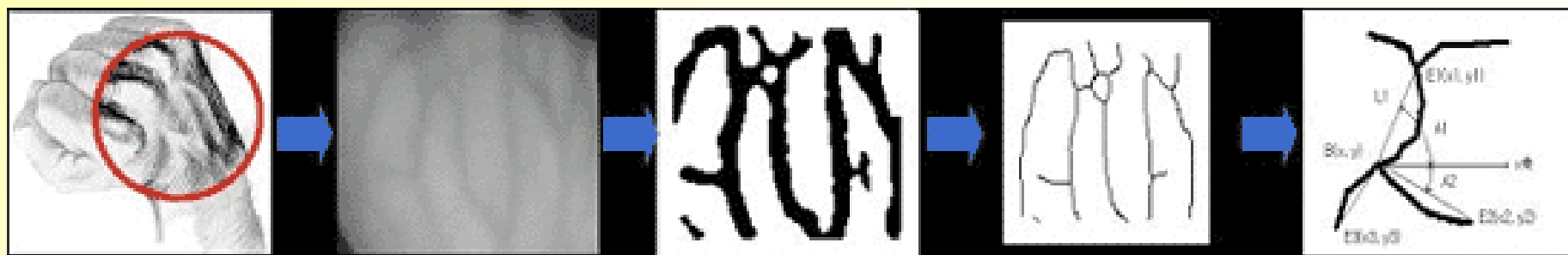
Rozpoznávání geometrie ruky II.

Kongres Bezpečnosti sítí, Praha, 11.04.2007



Rozpoznávání žil hřbetu / dlaně ruky

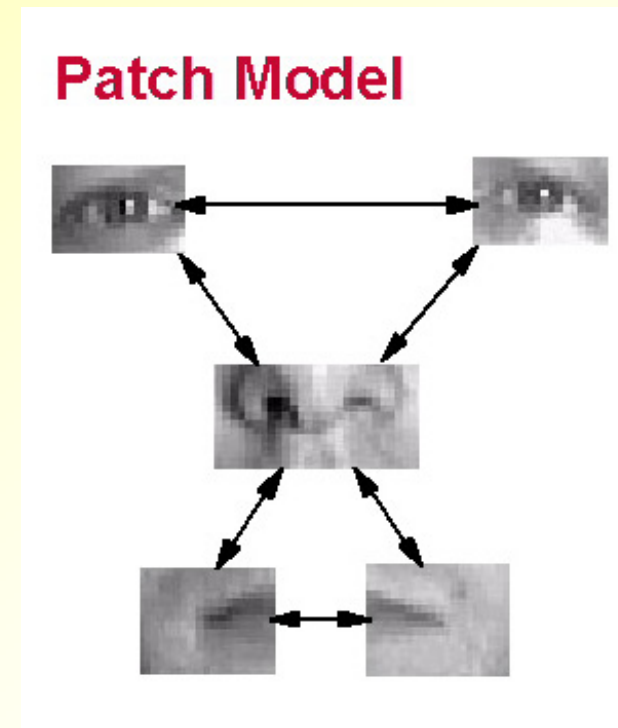
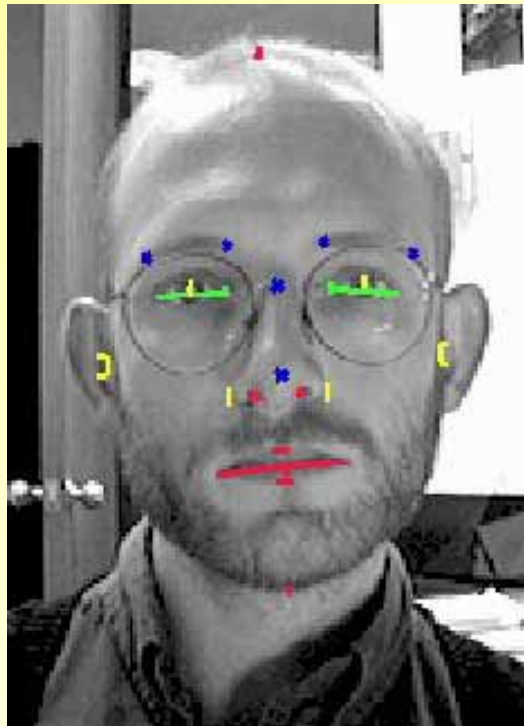
Kongres Bezpečnosti sítí, Praha, 11.04.2007



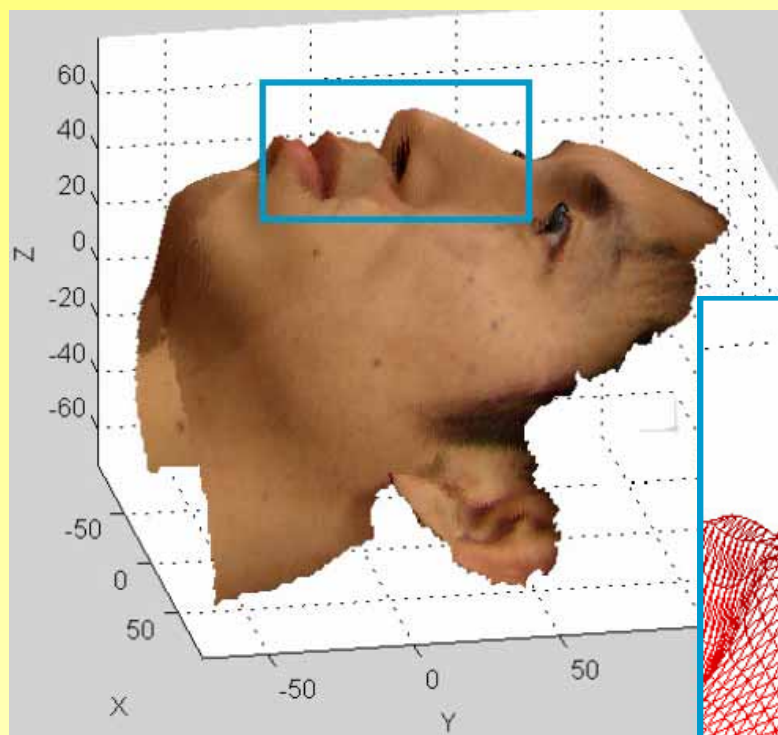


Rozpoznávání obličeje – 2D

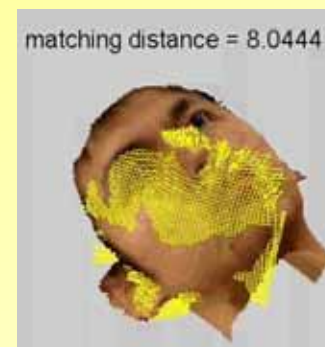
- ➔ V obličeji se hledají (po kroku detekce) hlavní rysy, jako poloha nosu, úst a očí. Potom přichází detekce obočí, uší, rtů apod.
- ➔ Porovnání probíhá na základě vzdáleností mezi jednotlivými body, přičemž se opět využívají toleranční limity – existuje však mnoho modelů rozpoznávání.



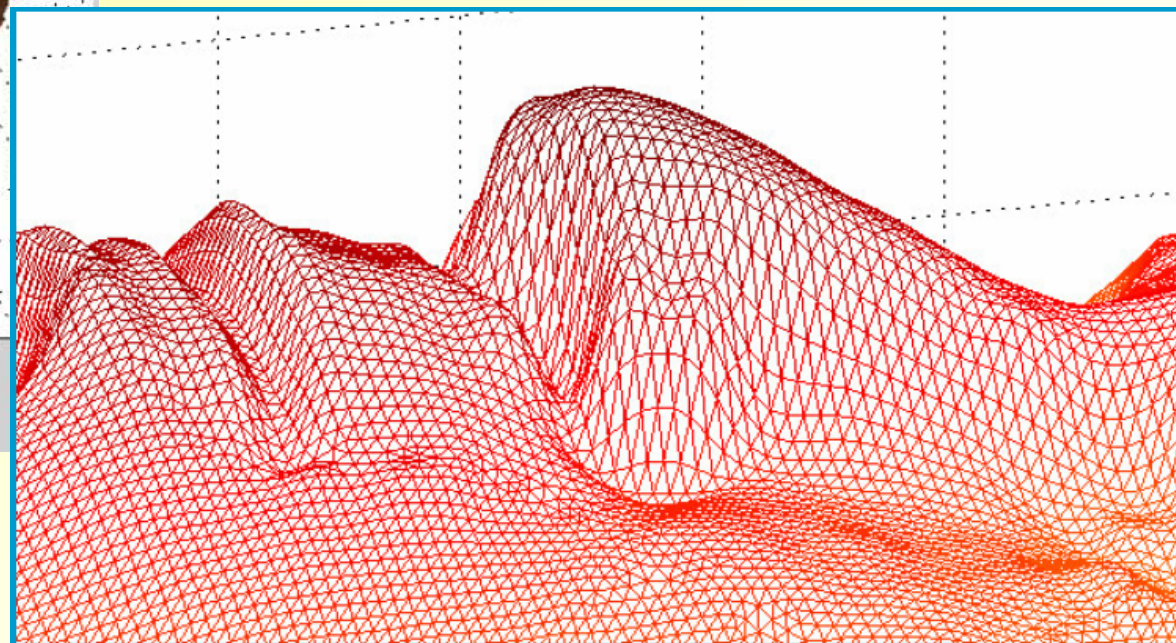
Rozpoznávání obličeje – 3D



3D model s texturou

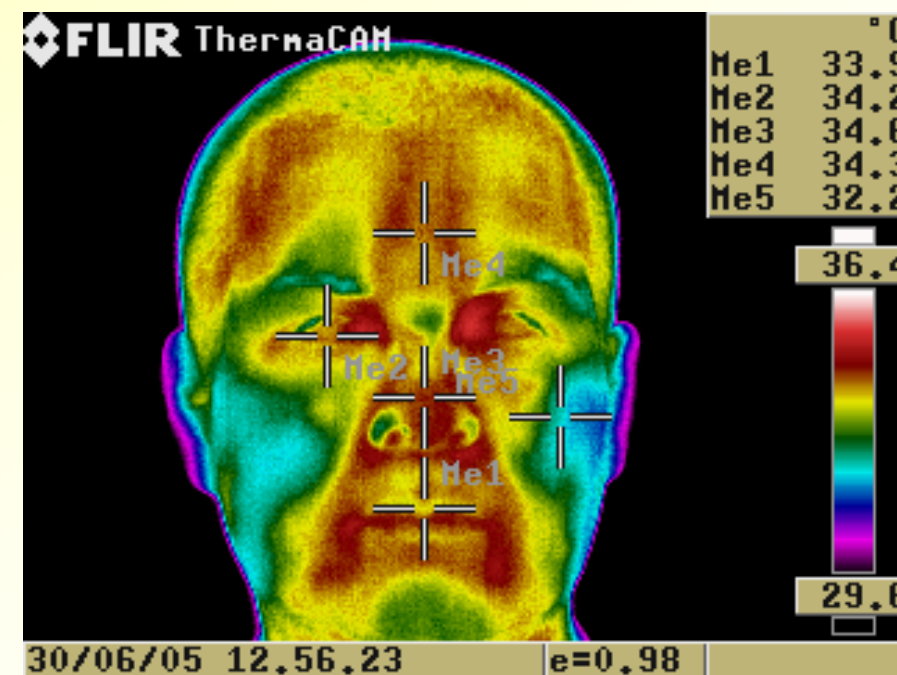
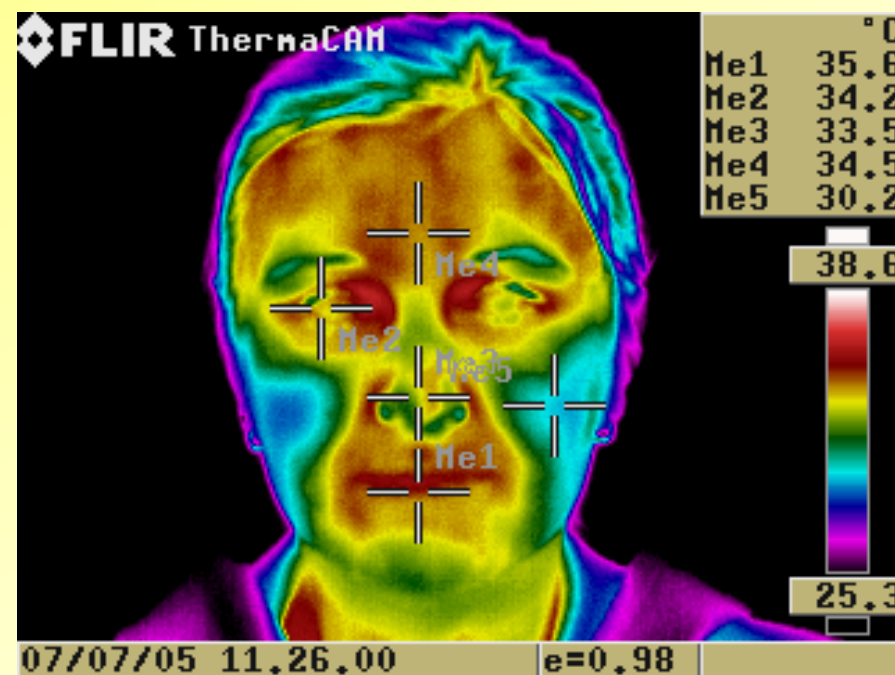
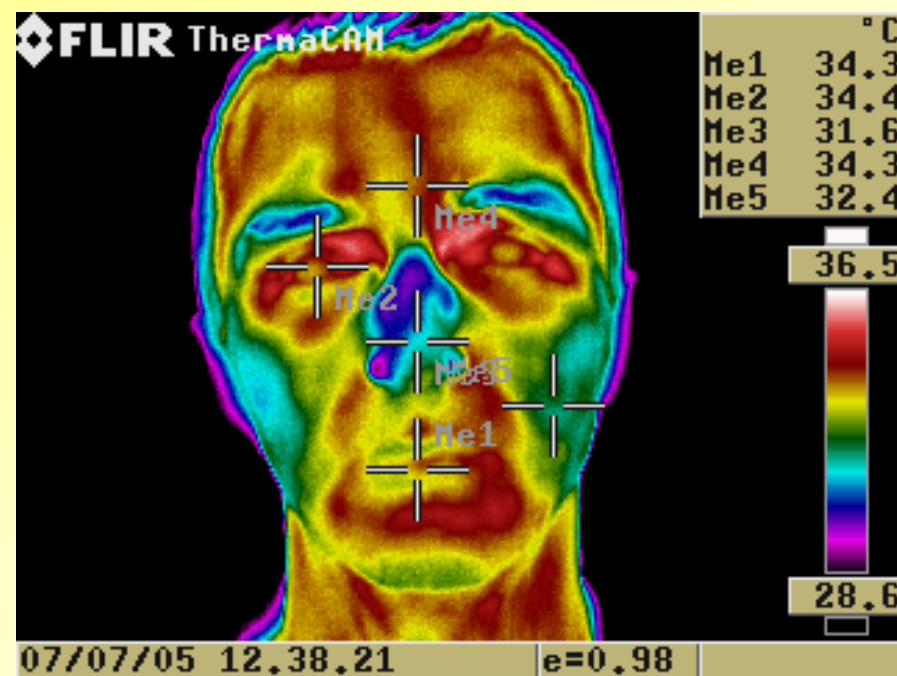
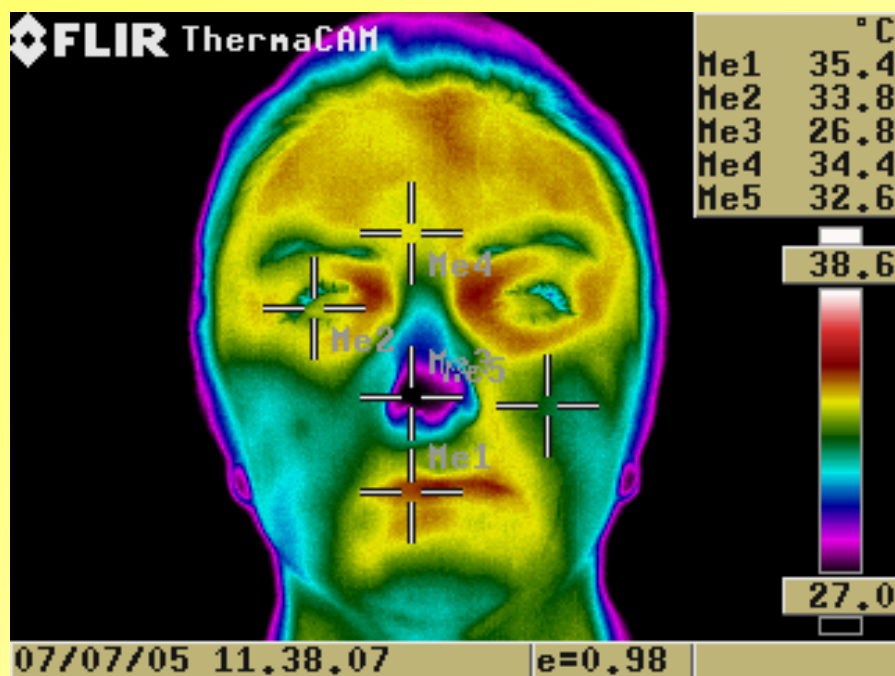


Asociovaná mřížka polygonů



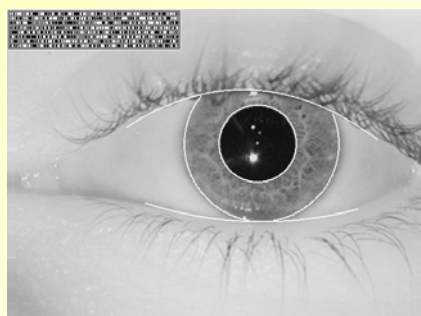
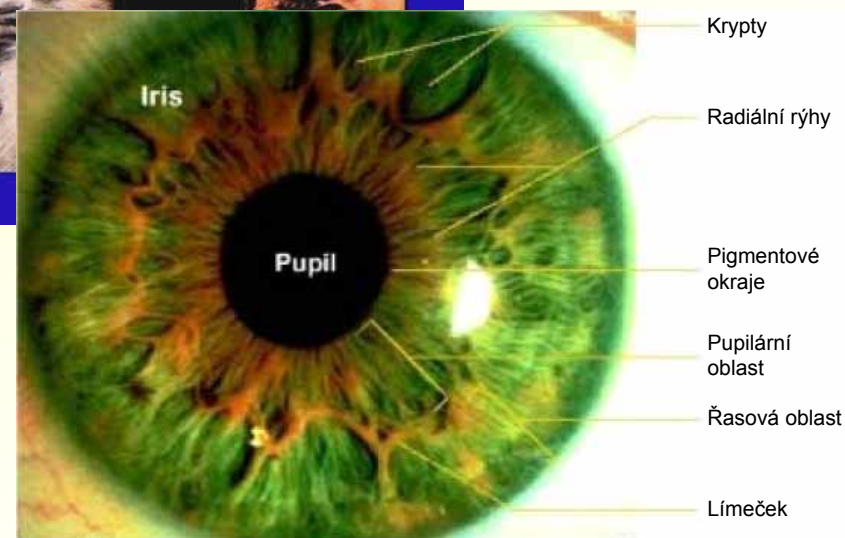
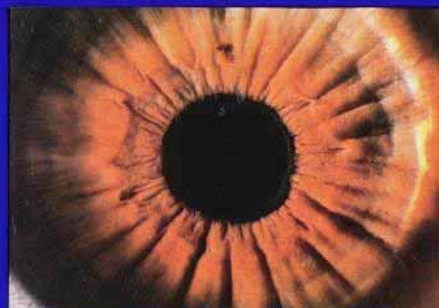
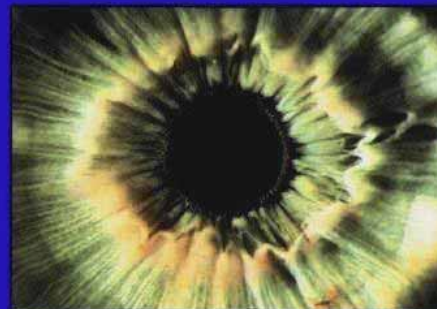
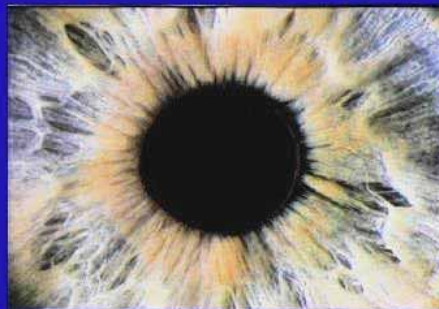
Rozpoznávání termosnímků obličeje

Kongres Bezpečnosti sítí, Praha, 11.04.2007



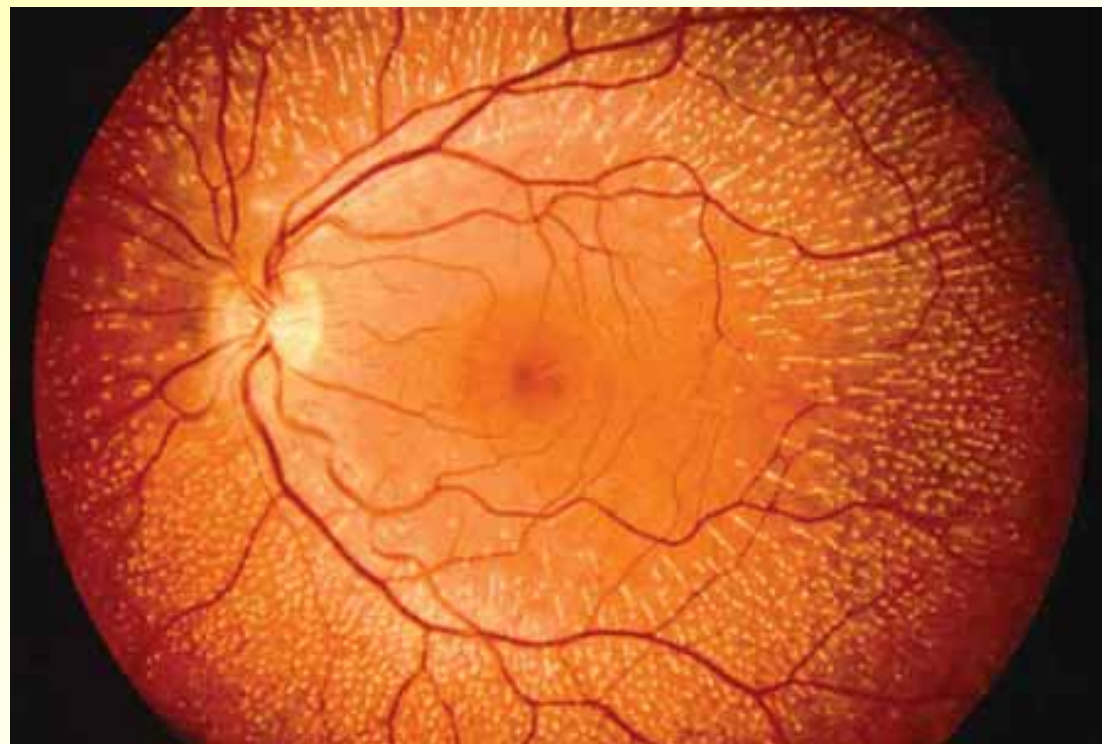
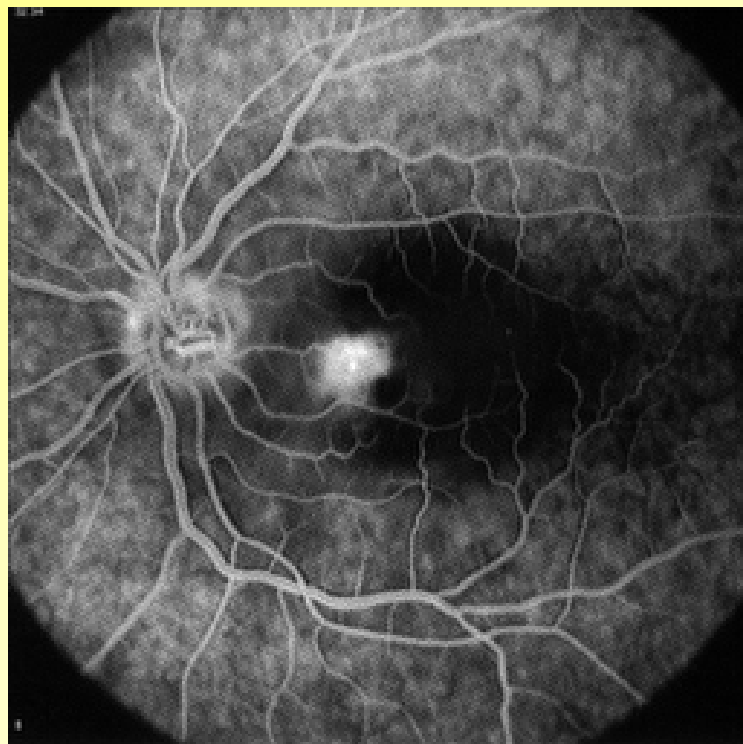
Rozpoznávání duhovky oka

Kongres Bezpečnosti sítí, Praha, 11.04.2007



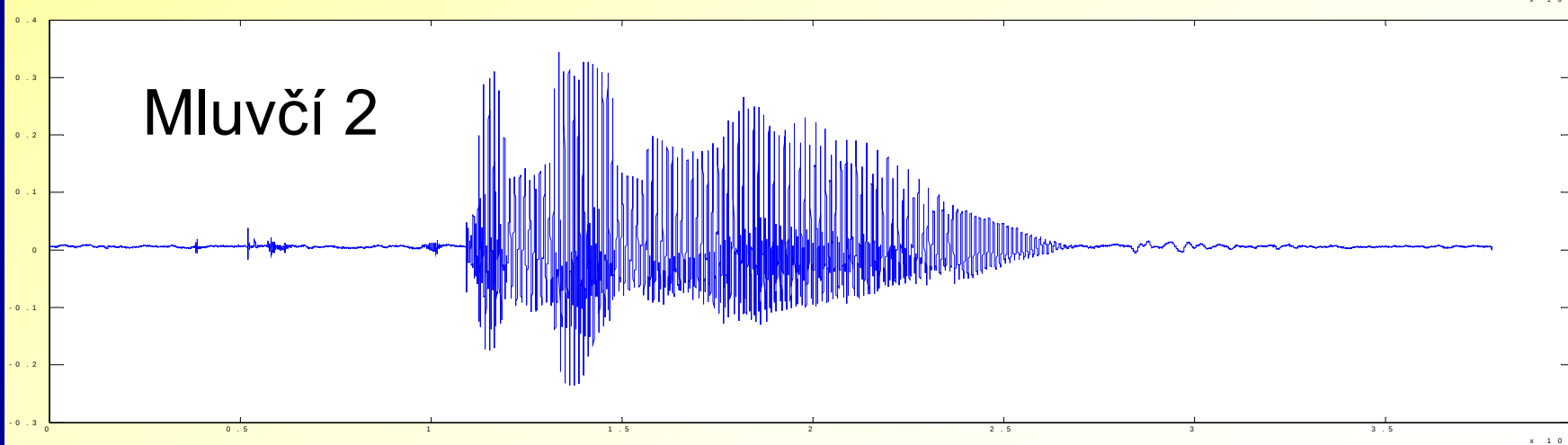
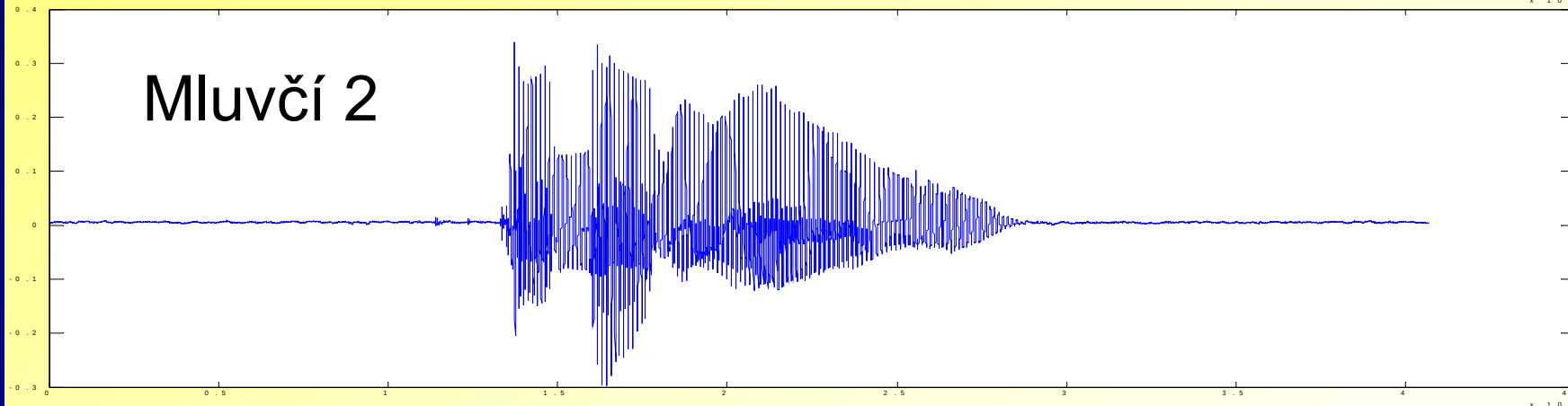
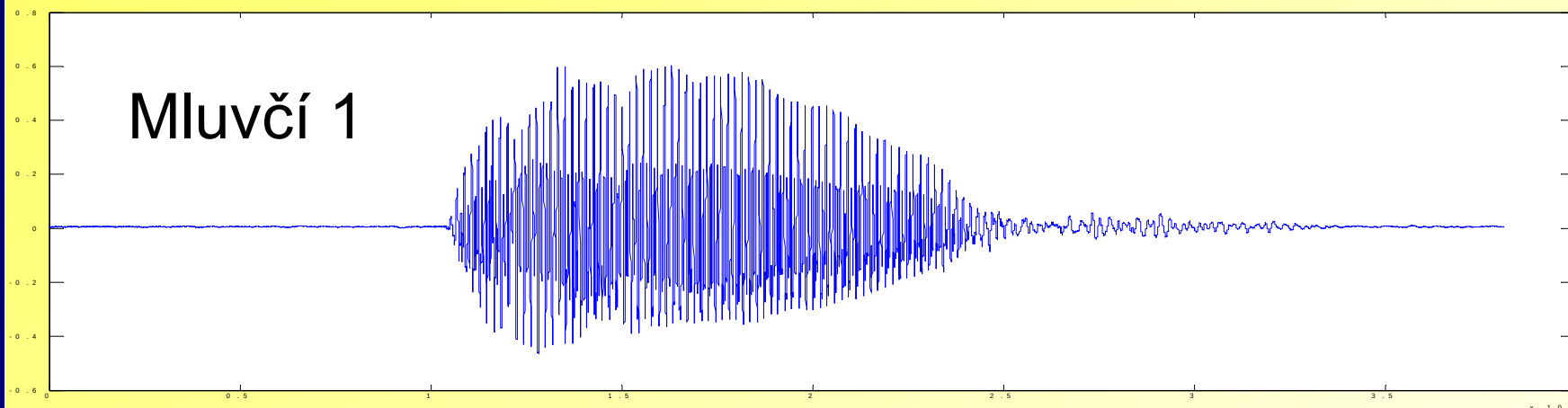
Rozpoznávání sítnice oka

Kongres Bezpečnosti sítí, Praha, 11.04.2007

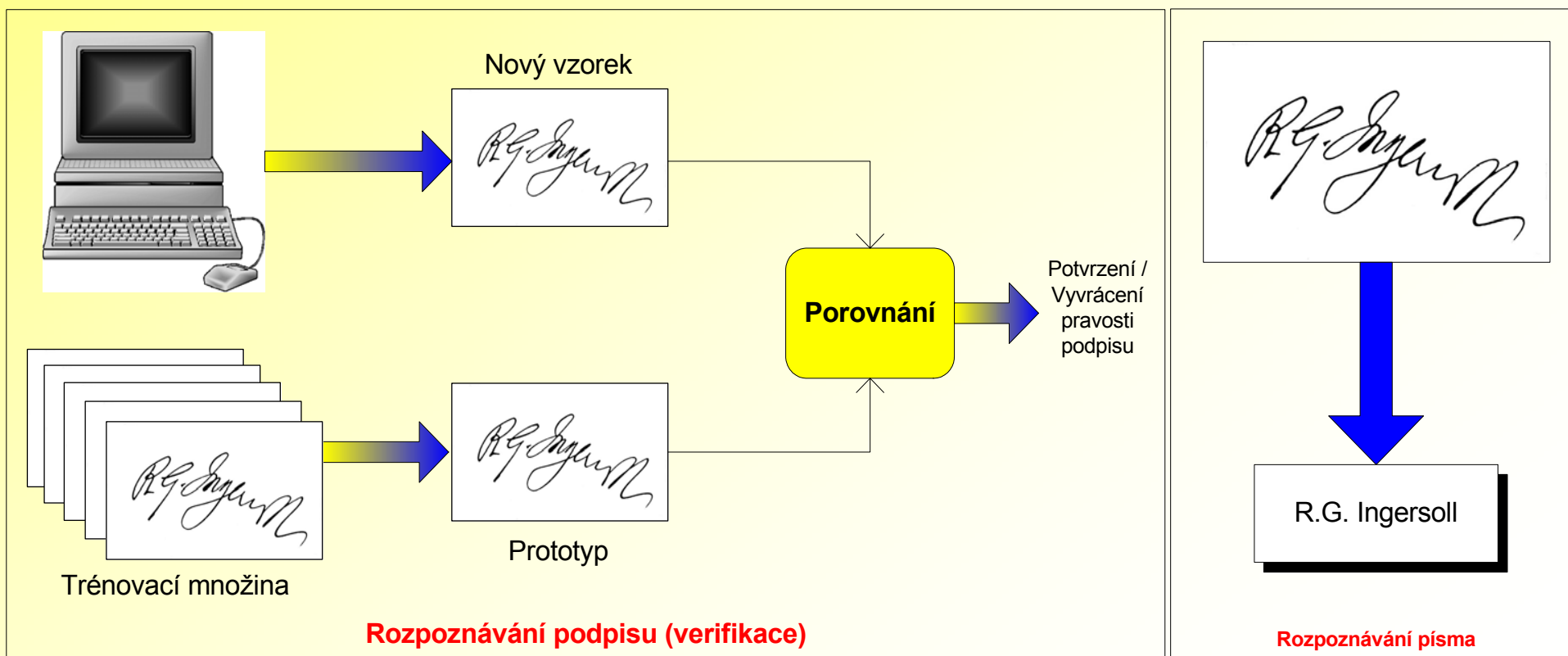
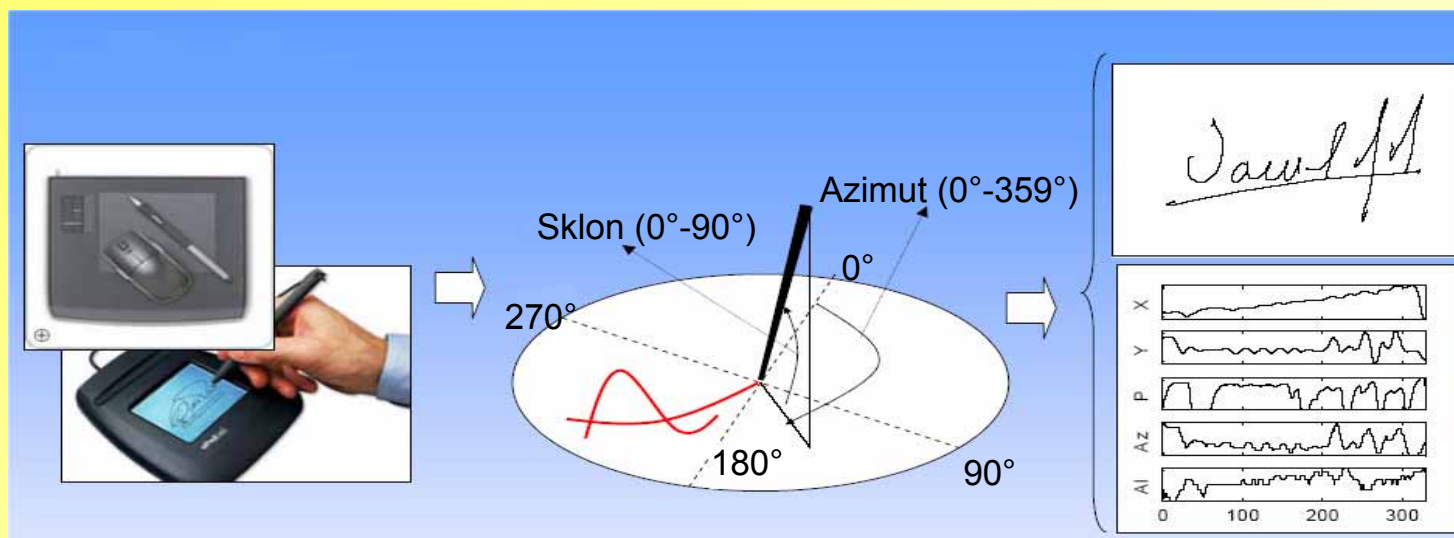


Rozpoznávání hlasu / řečníka

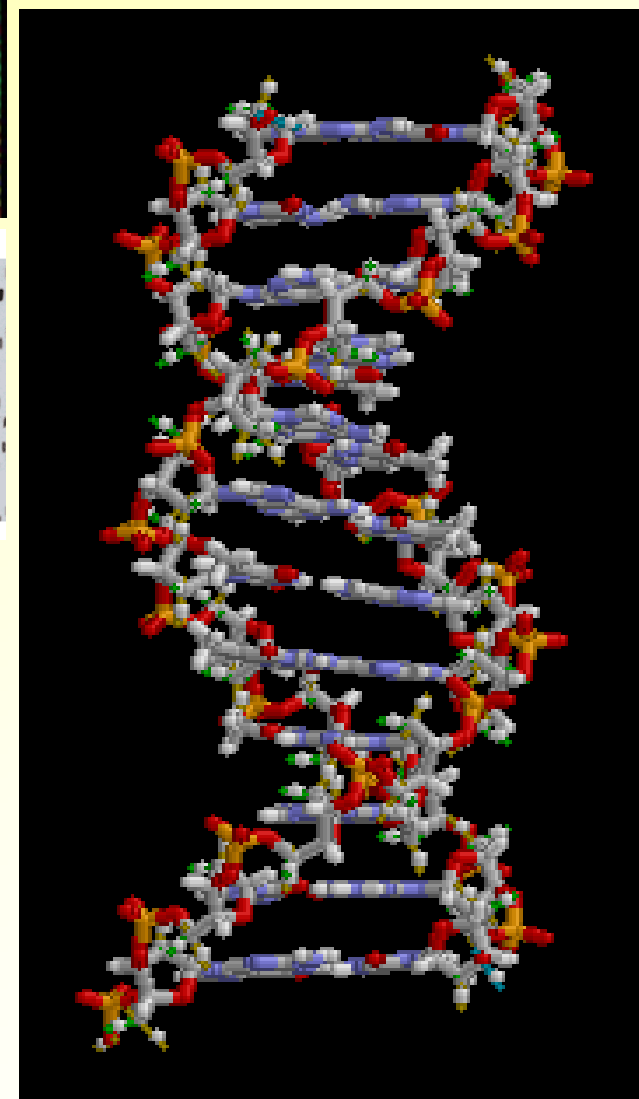
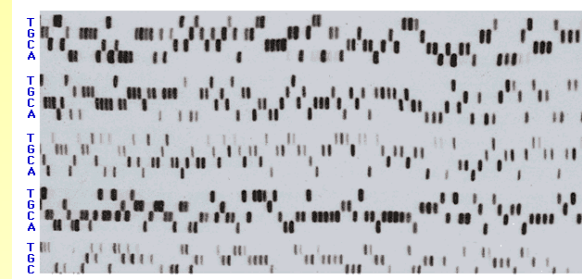
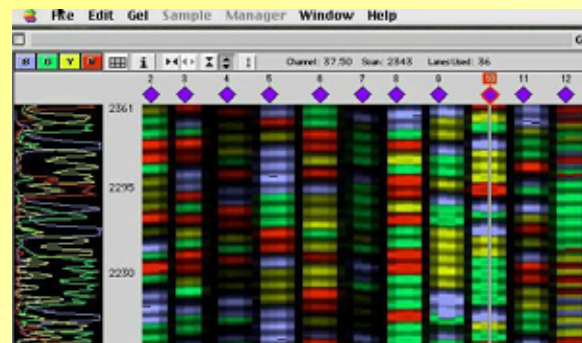
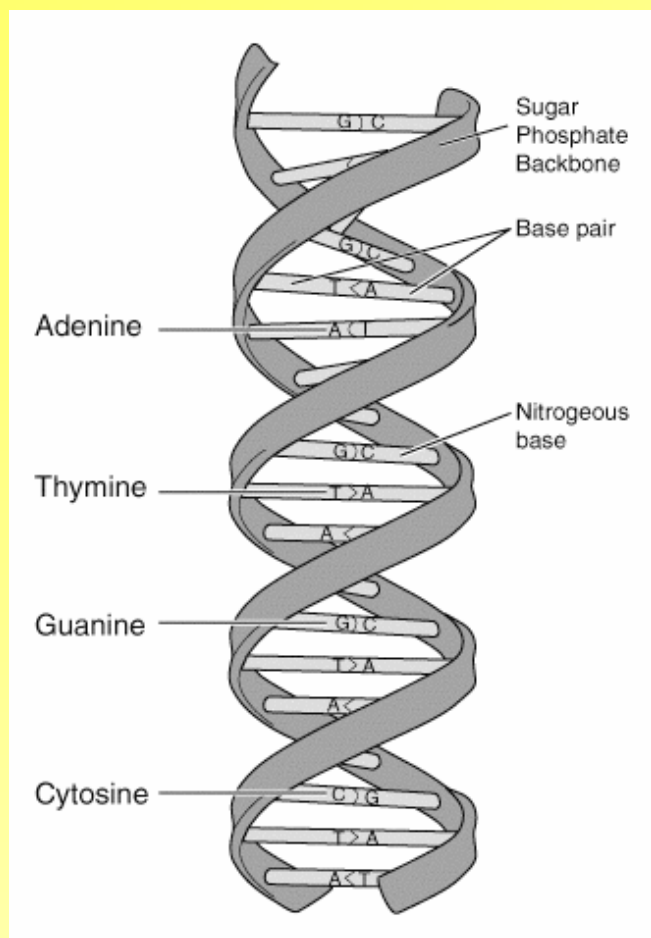
Kongres Bezpečnosti sítí, Praha, 11.04.2007



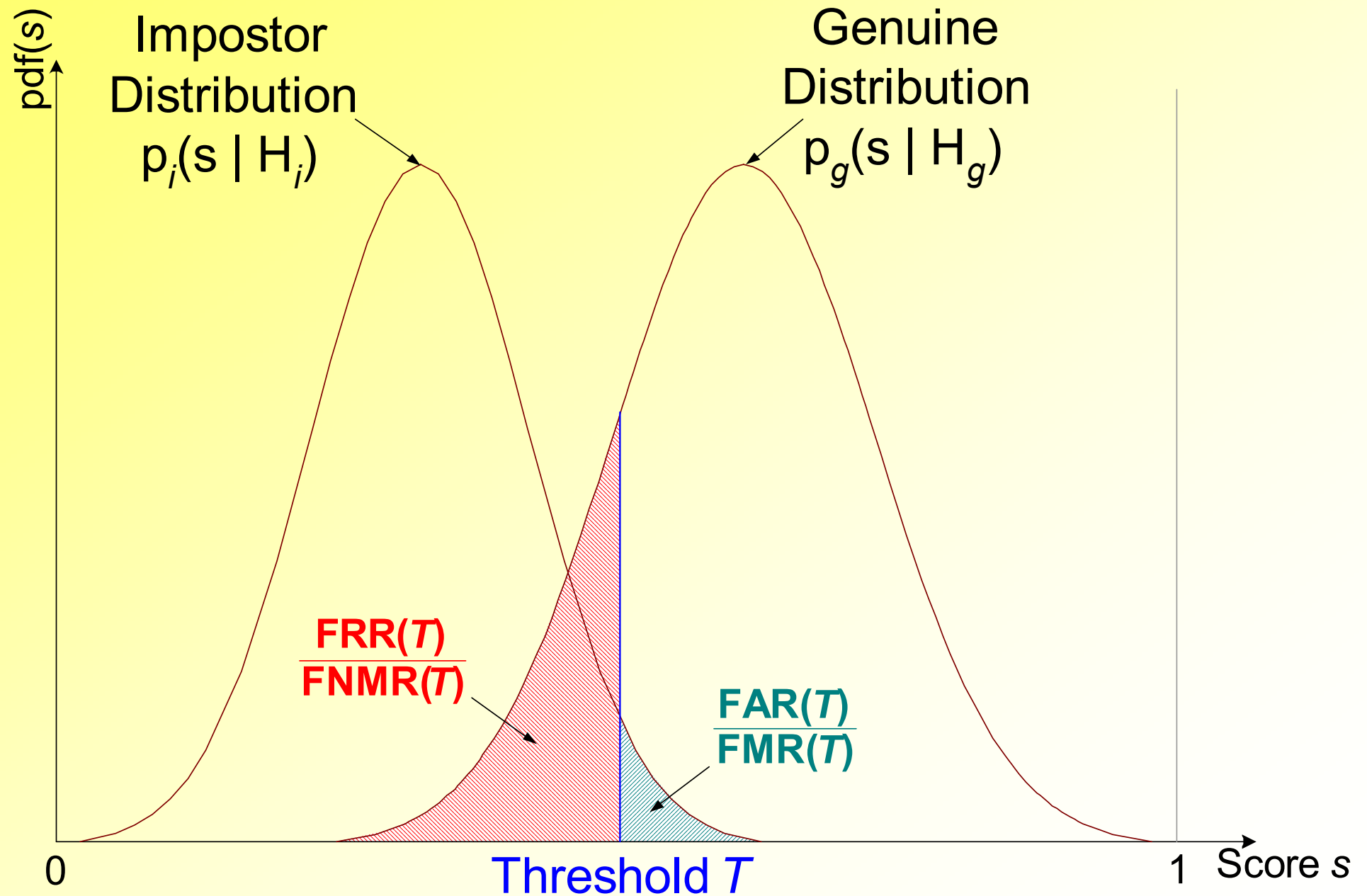
Rozpoznávání písma



Rozpoznávání DNA



Hitachi FMBIO II



→ Míra chybného přijetí - FAR

→ **FAR** je pravděpodobnost, že biometrický systém klasifikuje chybně dva odlišné biometrické vzory jako shodné a tím selže při odmítnutí možného útočníka.

$$\text{FAR} = \frac{\text{Počet shodných porovnání rozdílných vzorů}}{\text{Celkový počet porovnání rozdílných vzorů}}$$

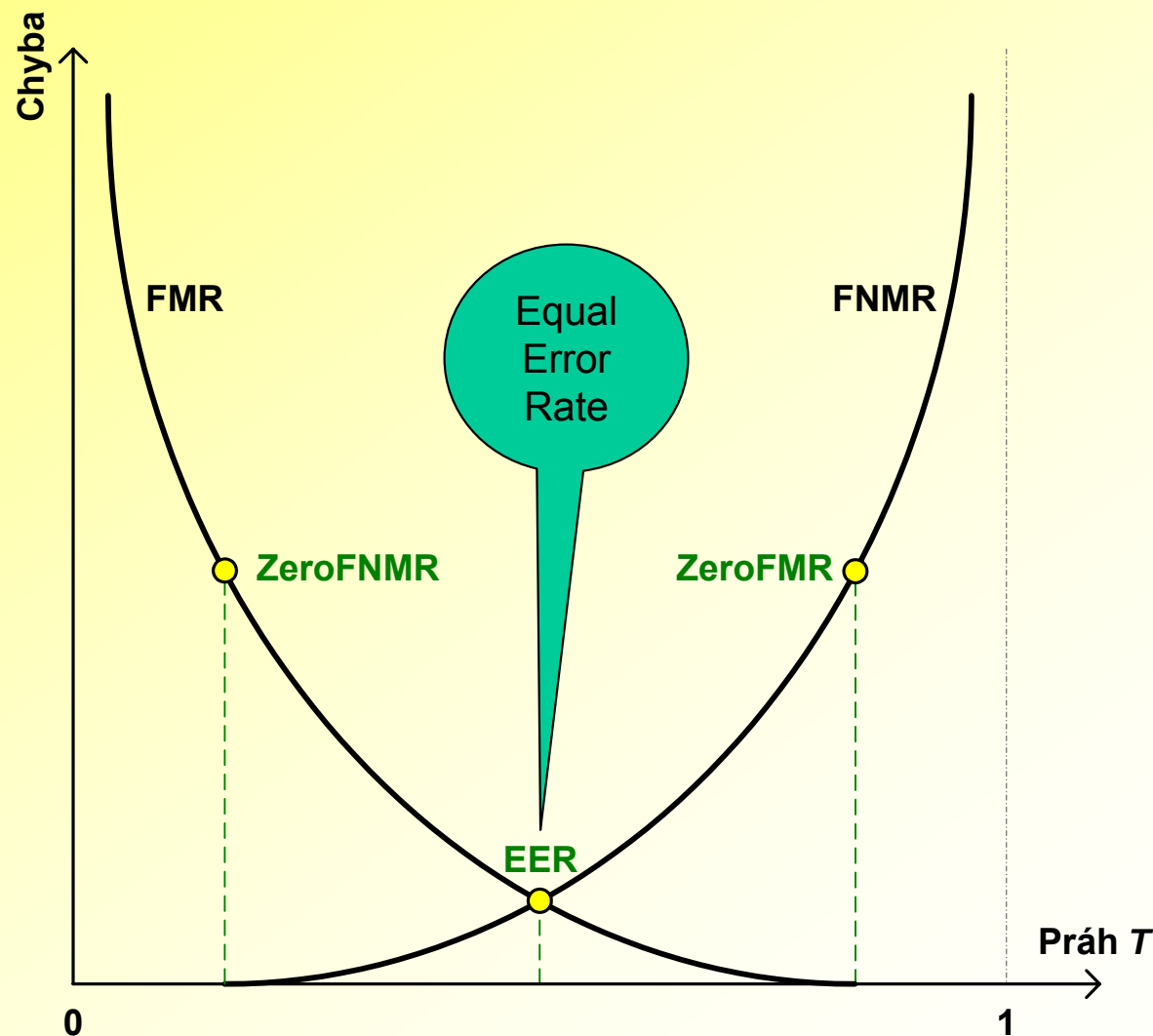
→ Míra chybného odmítnutí - FRR

→ **FRR** je pravděpodobnost, že biometrický systém klasifikuje chybně dva biometrické vzory od stejné osoby jako odlišné a tím selže při přijetí oprávněného uživatele.

$$\text{FRR} = \frac{\text{Počet porovnání vzorů osoby A vedoucích k neshodě}}{\text{Celkový počet porovnání vzorů osoby A}}$$

Testování III.

- ZeroFMR je dolní hranice FNMR, tj. $FMR = 0$.
- ZeroFNMR je dolní hranice FMR, tj. $FNMR = 0$.

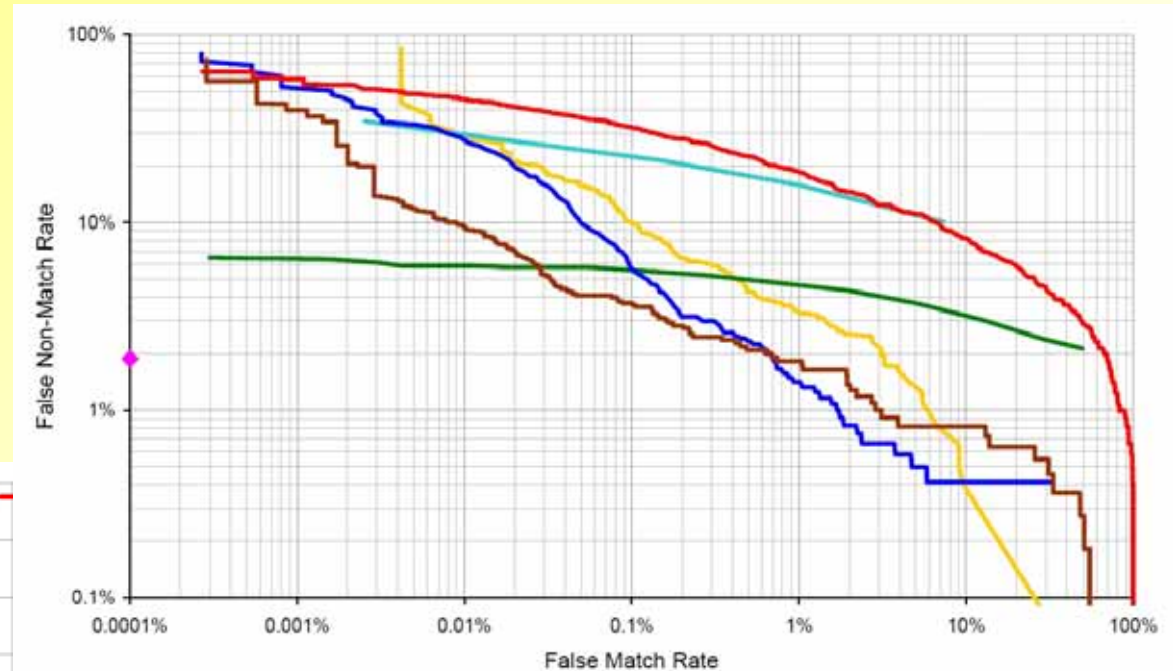
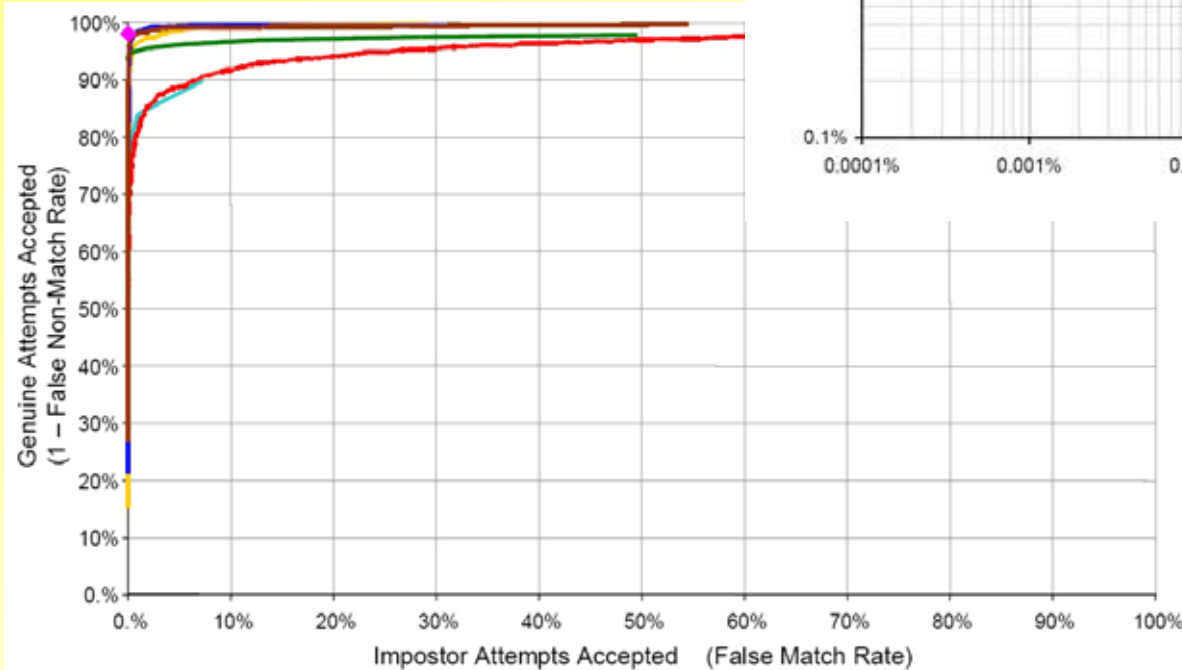


Testování IV.

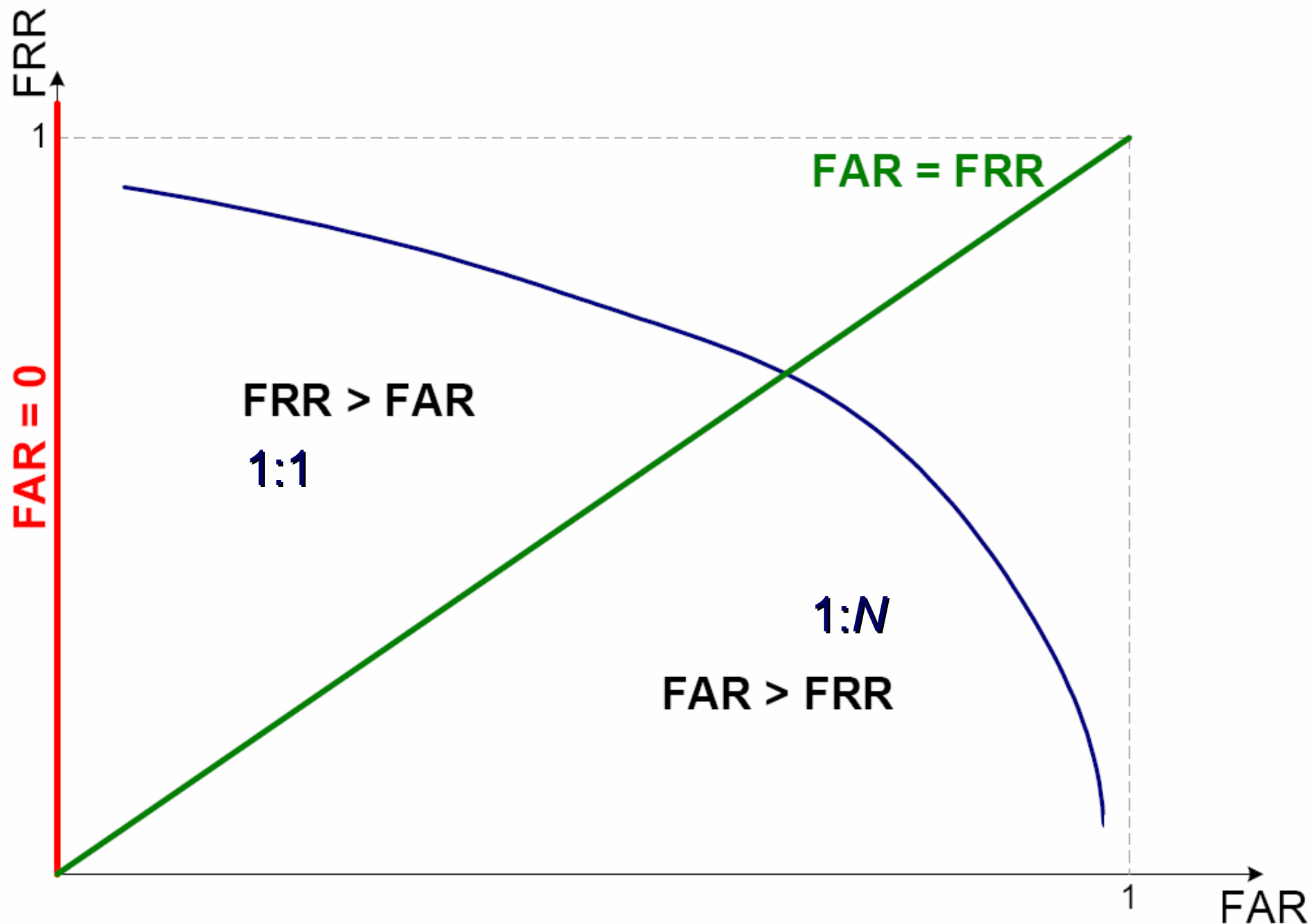
→ ROC = *Receiver Operating Curve*

→ DET = *Detection Error Trade-off*

DET →



← ROC



- ➔ Evaluace technologie spočívá v testování vybraných algoritmů, které používá daný biometrický systém a jsou obvykle provedeny v laboratorních systémech či prototypch budoucích systémů.
- ➔ Evaluace scénáře testuje celkovou výkonnost a spolehlivost daného biometrického systému v prototypových situacích. Tato evaluace obsahuje snímání biometrické vlastnosti, provedení registrace a porovnání, vč. generování a předání výsledku.
- ➔ Provozní evaluace spočívá v testování zvoleného biometrického systému pro nějakou konkrétní specifickou aplikaci. Tím pomáhá určit, zda daný systém bude pracovat v reálném světě v daném konkrétním prostředí.

- ➔ **Míra neschopnosti nasnímat - FTA**
- ➔ **FTA** udává podíl chybných záznamů v automatickém módu záznamu daného senzoru. Tj. zaznamenání biometrické charakteristiky je odmítnuto, ačkoliv je biometrická charakteristika přítomna. Čím vyšší je tato hodnota, tím méně je daný senzor vhodný pro záznam uvedené biometrické charakteristiky. Tím pádem slouží tato míra k hodnocení kvality senzorů.
- ➔ **Příklad:** Z celkového počtu 50 pokusů o nasnímání sítnice oka se nepodařilo získat data ze senzoru celkem 3×. Tedy **FTA** = $3 / 50 = 6\%$.

- ➔ **Míra neschopnosti zaregistrovat - FTE**
- ➔ **FTE** udává procentuální podíl uživatelů, které není systém schopen se naučit. Míry **FTE** se často vyskytují u systémů, které mají kontrolu kvality biometrické charakteristiky. Tj. biometrické charakteristiky s nedostatečnou kvalitou nejsou systémem naučeny. V tomto smyslu představuje **FTE** údaj, který ohodnocuje schopnost algoritmu pracovat i s nekvalitními biometrickými charakteristikami.
- ➔ **Příklad:** Z celkového počtu 200 pokusů o nasnímáním hlasu se nepodařilo z důvodu velkého hluku v pozadí rozpoznat řečový signál z mikrofonu celkem 9×. Tedy **FTE** = $9 / 200 = 4,5\%$.

- ➔ **Míra neschopnosti porovnat - FTM**
- ➔ **FTM** udává procentuální podíl biometrických charakteristik, které nemohly být porovnány se šablonou a nebo jakkoliv jinak zpracovány (po procesu zaregistrování). Tato míra poukazuje na neschopnost systému učinit rozhodnutí, tj. porovnání nepřinese žádný výsledek.
- ➔ **Příklad:** Z celkového počtu 3000 pokusů o porovnání zaregistrovaných otisků prstů se nepodařilo z důvodu nedostatečného počtu markantů srovnat celkem 25 z nich. Tedy **FTM** = $25 / 3000 = 0,83\%$.

→ Děkuji za Vaši pozornost!