



10. Dynamické biometrické vlastnosti

Dynamika stisku kláves

→ Úvod k dynamice stisku kláves

- Dynamika stisku kláves je proces analýzy způsobu psaní uživatele na klávesnici, jež je založená na identifikaci jeho přirozeného rytmu psaní (stisků kláves).
- Šablona psaného vzorku (dynamické vlastnosti) by měla být pro každého jedince jednoznačná, protože každý z nás má jiné neurofyzilogické faktory, které rytmus psaní ovlivňují.
- Dynamika stisku kláves patří do biometrie chování (dynamických biometrických vlastností).
- Přirozená vhodnost pro počítačový login a síťovou bezpečnost.

- Během 2. světové války objevila armáda tzv. metodu „*Fist of the Sender*“, kde telegrafisté byli schopni podle dynamiky vysílané Morseovy abecedy identifikovat telegrafistu na druhé straně.
- 1979 – *SRI International* – první HW implementace
- 1984 – *NIST* shledává tuto technologii z 98% efektivní
- 1988 – Nová technologie odpovídající definici NISTu z roku 1987 (*NIST Computer Security Act 1987*)
- 2000 – Společnosti *FSTC* / *IBG* verifikují technologii dynamiky stisku kláves
- 2001 – Integrace této technologie do telefonních aparátů a domácí bezpečnosti (*Home_PC*)

→ Průmyslové systémy



→ BioPassword

→ <http://www.biopassword.com/>



→ Rysy vzorů psaní (I.)

- Dynamika stisku kláves se nezabývá tím co píšete, ale tím **jak píšete**.
- Rysy používané k popisu vzoru psaní uživatele:
 - Časové prodlevy mezi úspěšnými stisky kláves (uběhnutý čas mezi uvolněním staré klávesy a stiskem nové klávesy)
 - Délka trvání každého stisku (jak dlouho je klávesa stisknuta)
 - Poloha prstu na klávese (je-li k dispozici)
 - Tlak aplikovaný na klávesu (je-li k dispozici)
 - Celková rychlost psaní

→ Rysy vzorů psaní (II.)

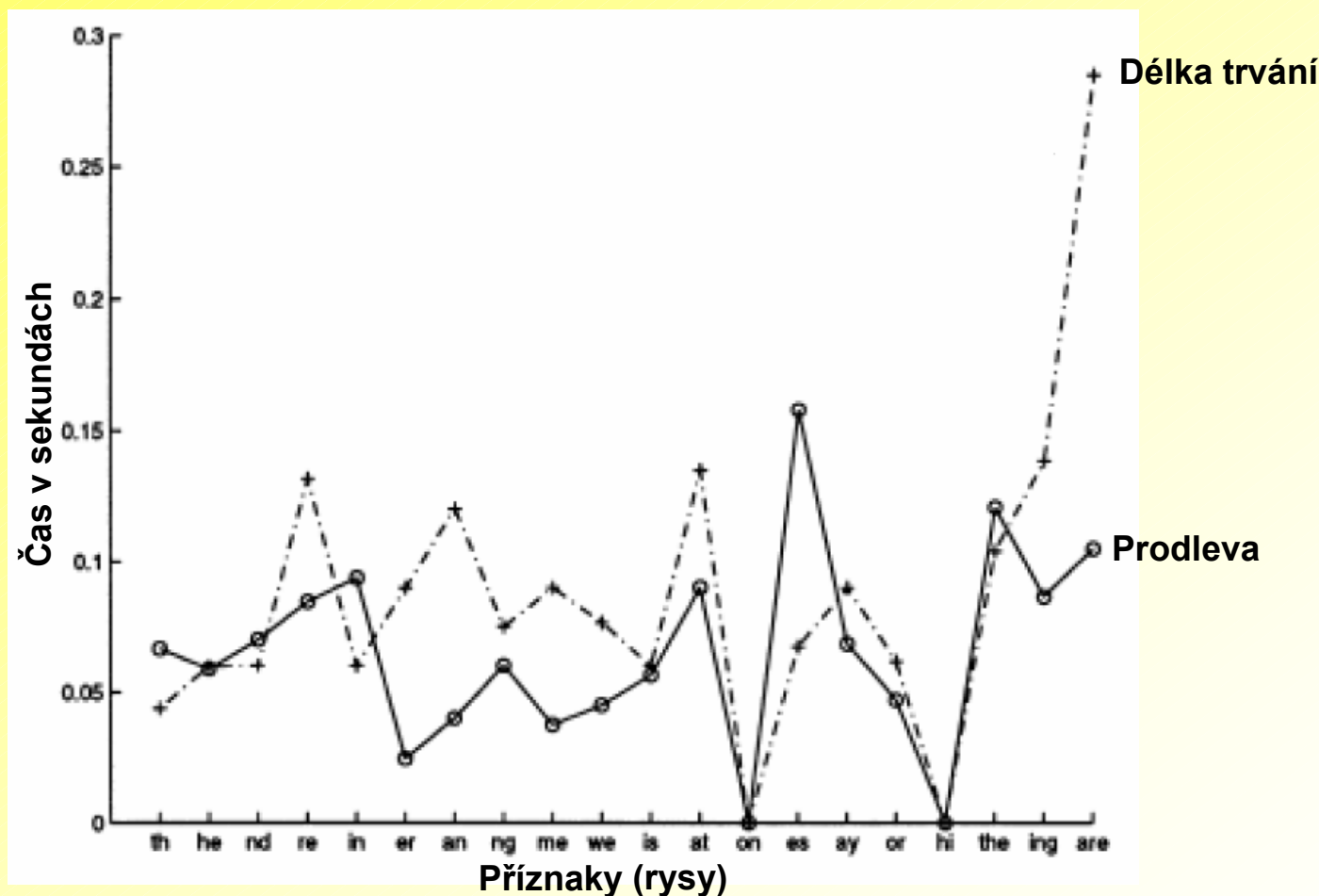
- Použití např. pro login k počítači, při psaní uživatelského jména a zadávání hesla.
- Rysy jsou funkcí uživatele a prostředí.
- Při záznamu dynamických vlastností úhozů hraje roli i samotné psané slovo, protože ergonomie klávesnice neumožňuje stejné napsání slova „Martin“ a např. „987654“. Proto je dynamika stisku kláves závislá i na psaném textu.



→ Statická vs. průběžná verifikace

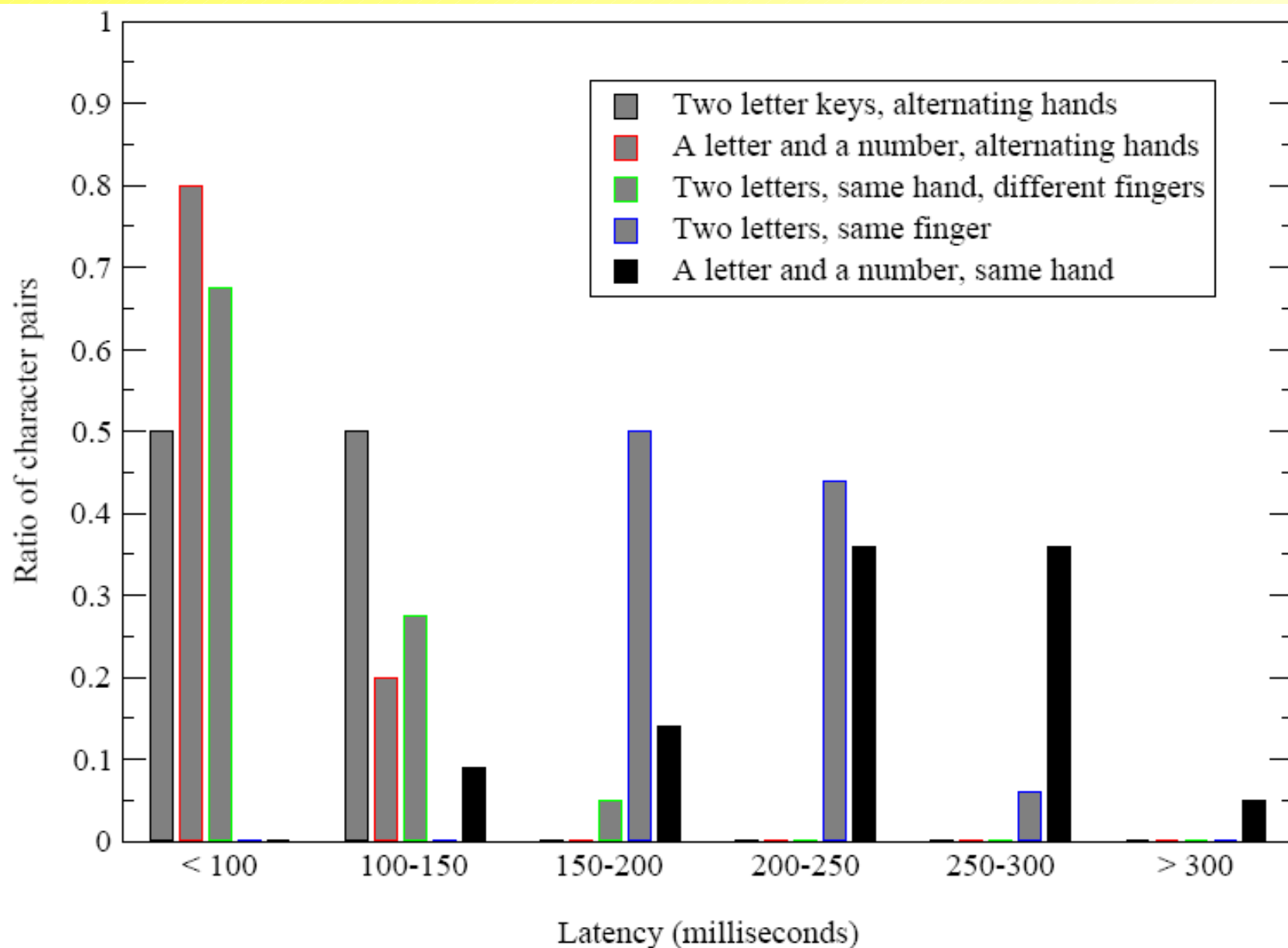
- Při **statické verifikaci** jsou stisky kláves analyzovány pouze ve specifikovaných časech, např. během loginu.
- Statické verifikační přístupy umožňují mnohem robustnější verifikaci, než samotné zadání hesla.
- Statické přístupy ovšem neposkytují průběžnou bezpečnost – neumí detekovat záměnu uživatelů po přihlášení k počítači.
- **Průběžná verifikace** monitoruje celkové chování uživatele během jeho práce s počítačem.
- U průběžné verifikace je ovšem nutný vyhodnocovací proces, který neustále běží – zatížení počítače.

→ Příklad profilu



→ Na ose x se nachází 20 nejčastěji se vyskytujících digrafů (písmenných dvojic) v psané frázi. Plná čára ~ *prodleva* a čerchovaná čára ~ *délka trvání* zápisu.

→ Latence stisků kláves



→ Měřítko vzdálenosti

→ L_1 norma: $D(R, U) = \sum_{i=1}^N |r_i - u_i|$

→ Eukleidovská vzdálenost: $D(R, U) = \left[\sum_{i=1}^N (r_i - u_i)^2 \right]^{1/2}$

→ Vážená pravděpodobnost:

$$Score(R, U) = \sum_{i=1}^N \frac{w_{u_i}}{o_{u_i}} \left[\sum_{j=1}^{o_{u_i}} Prob \left(\frac{X_{ij}^{(u)} - \mu_{r_i}}{\sigma_{r_i}} \right) \right]$$

→ w_{u_i} – váha rysu u_i ; o_{u_i} – počet výskytů u_i ; $x_{ij}^{(u)}$ – hodnota j -tého výskytu u_i ; μ_i a σ_i jsou střední a standardní odchylky od i -tého rysu

→ Bayesovský klasifikátor:

$$D(R, U) = \sum_{i=1}^N w_i \left(\frac{|r_i - u_i|}{\sigma_i} \right)^\alpha$$

→ Přesnost dynamiky stisku kláves (digrafy)

- Pro vyhodnocení [Jai04] byla použita databáze 63 uživatelů, přičemž data byla nasbírána během 11 měsíců.
- Účastníci pracovali na svých počítačích.
- Dvě varianty:
 - Volný text (klasická práce)
 - Fráze / předem definovaný text
- **FAR** = 0,01% a **FRR** = 3,0%
- Správné vyhodnocení pro:
 - Vážená pravděpodobnost: 87%
 - Bayesovský klasifikátor: 92%

→ Použití trigrafů (písmenných trojic)

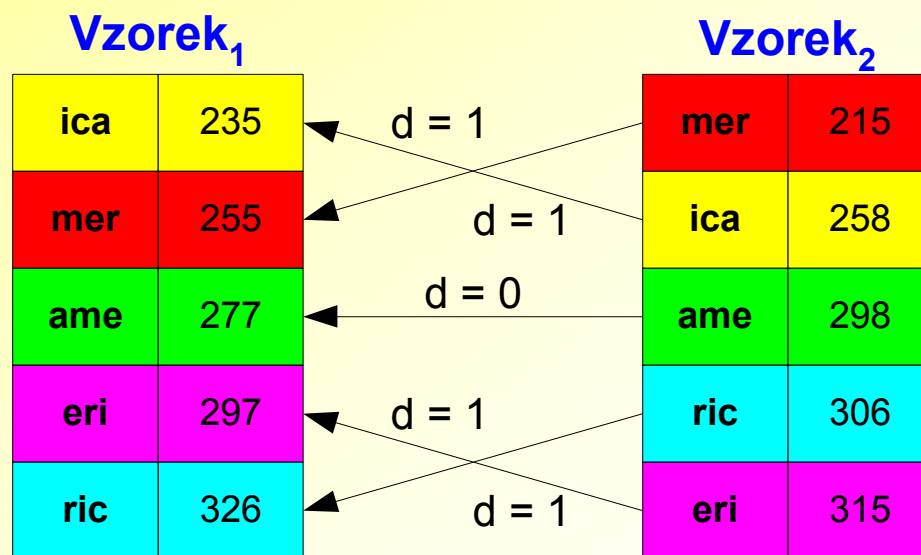
- Dvě po sobě napsaná písmena se nazývají **digraf**.
- Tři po sobě napsaná písmena se nazývají **trigraf**.
- Délka trvání u trigrafů – čas mezi stiskem první klávesy a uvolněním třetí klávesy.
- Předpokládejme např. text „*america*“:
 - *ame* = 277; *mer* = 255; *eri* = 297; *ric* = 326;
ica = 235
- Ve vektoru uloženo ve vzestupném pořadí:
 - *ica* = 235; *mer* = 255; *ame* = 277; *eri* = 297;
ric = 326

→ Porovnávání trigrafů

→ Stupeň „nepořádku“: suma absolutních změn v pozici mezi dvěma uspořádanými poli.

→ **Vzor₁**: *ica* = 235; *mer* = 255; *ame* = 277; *eri* = 297; *ric* = 326

→ **Vzor₂**: *mer* = 215; *ica* = 258; *ame* = 298; *ric* = 306; *eri* = 315



→ $D(\text{Vzor}_1, \text{Vzor}_2) = (1+1+0+1+1) / 12 = 0,33$

→ Výsledek se normalizuje, aby ležel v rozmezí $<0,1>$.

→ Přesnost dynamiky stisku kláves (trigrafy)

- Pro vyhodnocení [Jai04] byla použita databáze 44 oprávněných uživatelů a 110 útočníků.
- Pevně stanovený text o 683 znacích; 5 vzorků na uživatele. Všechna data nahrána na stejné klávesnici.
- Pro psaní se používalo pouze vybraných kláves.
- Všichni uživatelé byli zkušení v práci s PC.
- Výsledky:

- **FRR** $\cong 1,8\%$

- **FAR** $\cong 0,042\%$

- Vnitrotřídní variabilita uživatele šablony A :

$$md(A, B) = [d(A_1, B) + d(A_2, B) + d(A_3, B)] / 3$$

→ Výhody dynamiky stisku kláves

- Neinvazivní
- Dobře akceptované uživateli
- Přirozený způsob autentizace u počítačů a sítí
- Je možné průběžné monitorování
- Nutnost minimálního tréninku (učení)
- Žádný přídavný hardware
- Možnost tvorby **silného hesla**:
 - Textové heslo + dynamický vzorek jeho psaní
 - Vyšší bezpečnost
 - Nebezpečí **FRR** díky změně stylu psaní

→ Nevýhody dynamiky stisku kláves

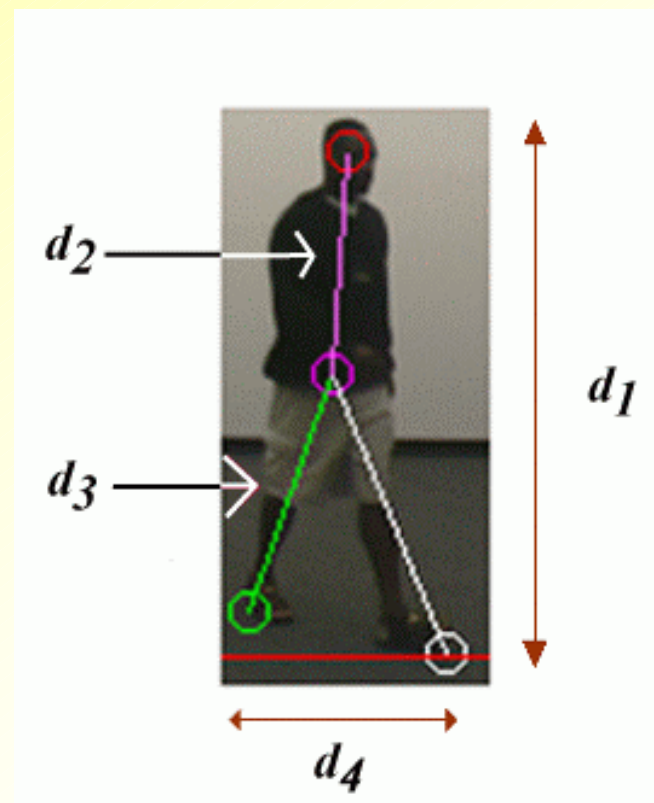
- Vysoká míra **FRR**
- Citlivá metoda na změny klávesnice, fyzického či psychického stavu uživatele a příp. vlivů okolí
- Úzká oblast použitelných aplikací
- Musí umět zahrnovat problémy jako jsou překlepy či opravy při psaní



Rozpoznávání chůze

→ Rozpoznávání chůze (I.)

- Účelem je rozpoznat osobu na základě chůze.
- K rozpoznání by mělo být využito běžných typů kamer.
- Rozpoznávání chůze může sloužit k identifikace osob na dálku.
- Malá rozlišovací schopnost.
- Dříve bylo nutné používat speciální označovače na oblečení (*test-dummy*).
- Požadovaným výsledkem je rozpoznání v každé situaci.
- *DARPA program*



→ Rozpoznávání chůze (II.)

→ Rozpoznávání je závislé na těchto faktorech:

→ Oblečení

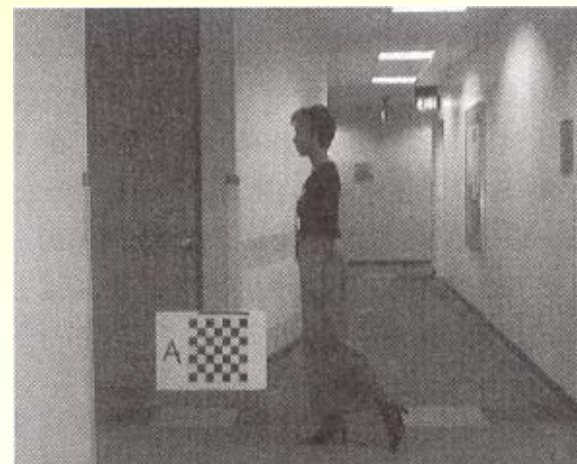
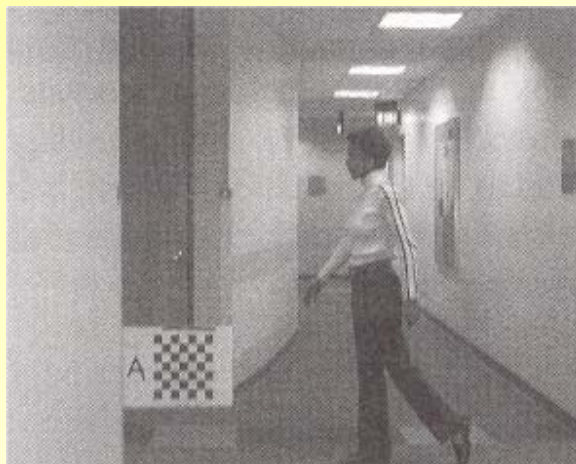
→ Obutí

→ Fyzický stav uživatele

→ Okolní prostředí + osvětlení

→ Množství osob v daném prostředí

→ Vážná onemocnění / úrazy



→ Rozpoznávání chůze (III.)

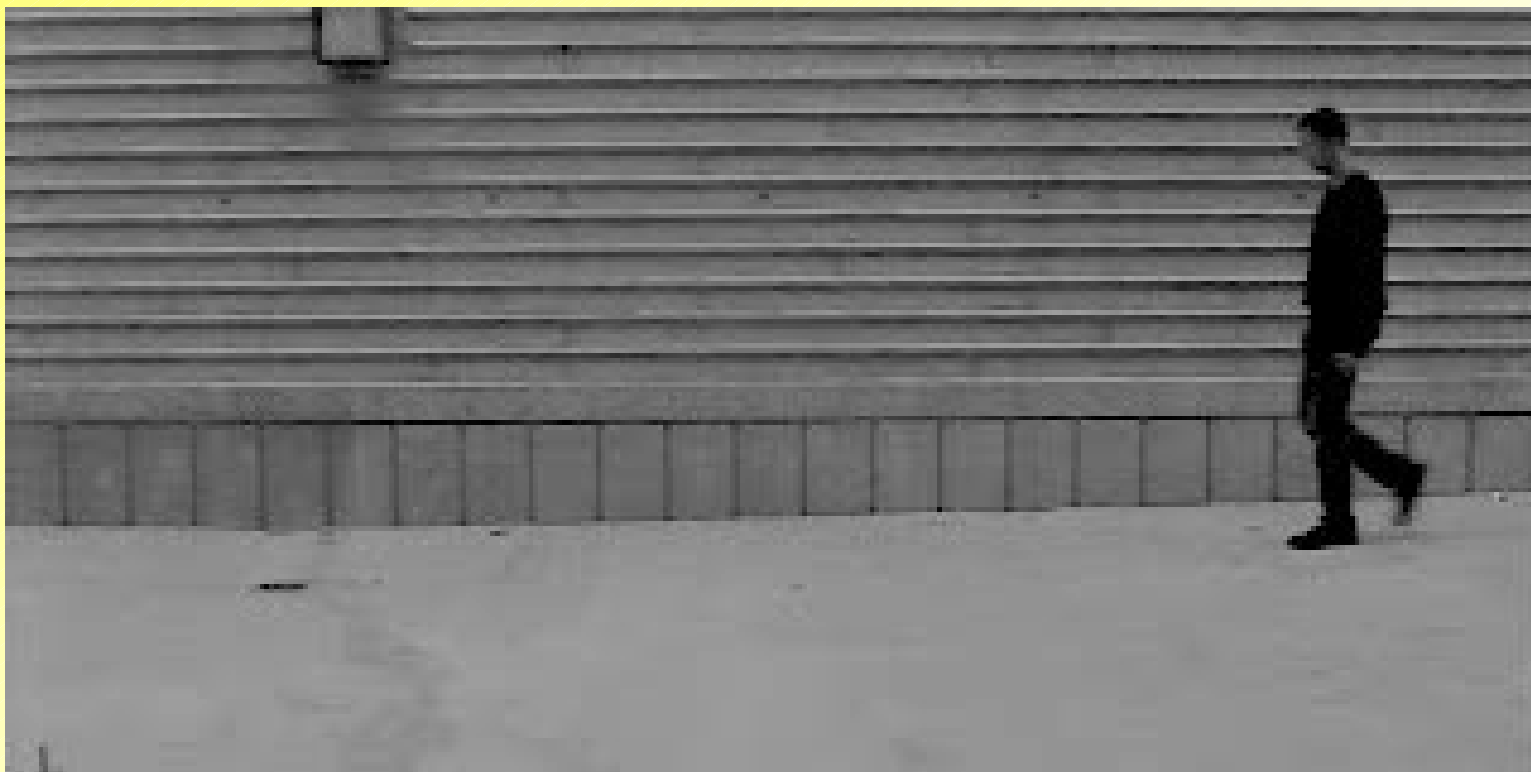
- Algoritmus funguje následovně:
 - Definování hraničních boxů pro postavu ve videosignálu
 - Extrakce siluety postavy dle hraničních boxů



- Změna rozlišení hraničních boxů na 128×88 pixelů, aby byl krok provedení korelace výpočetně nenáročný.

→ Praktická ukázka (I.)

→ Záznam z kamery



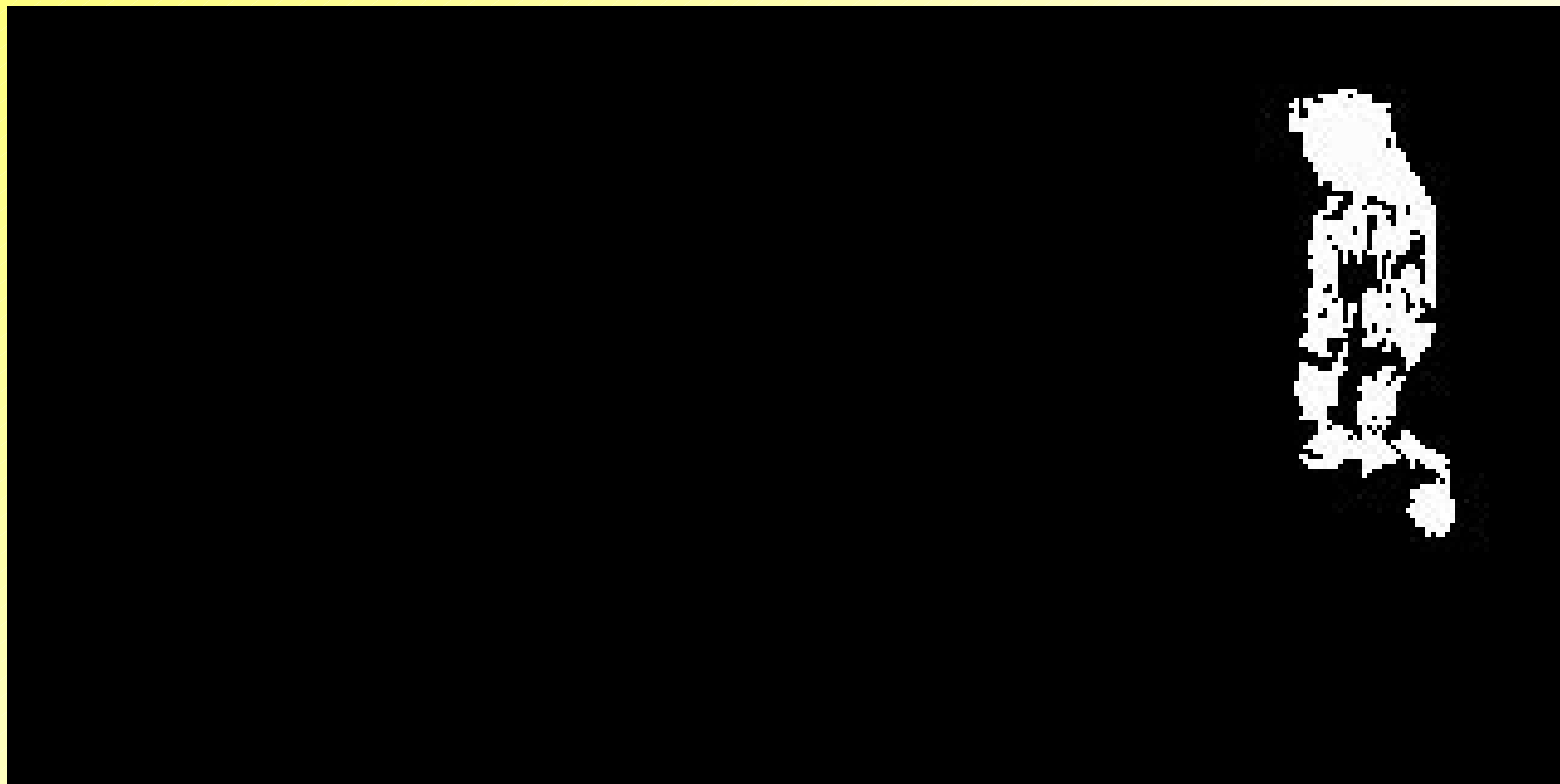
→ Praktická ukázka (II.)

→ Optický tok u , v a $|u+v|$



→ Praktická ukázka (III.)

→ Binarizace – „*Moving blobs*“



→ Praktická ukázka (IV.)

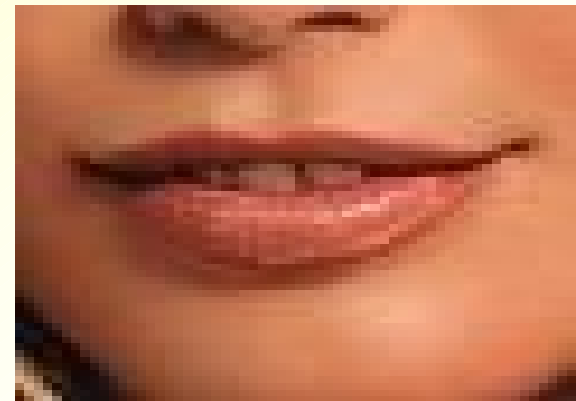
- Pohyb (+ je centrum; *čtverec* je vážený centroid $|u+v|$; *plná elipsa* vyjadřuje poměr stran pohybujícího se objektu; *čárkovaná elipsa* vyjadřuje poměr stran váženého centroidu $|u+v|$)



Pohyby rtů

→ Pohyby rtů (I.)

- Účelem je rozpoznat osobu na základě pohybu rtů.
- Porovnání probíhá na základě charakteristik pohybů rtů během rozhovoru / vyřčení předdefinované fráze.
- Pomáhá při identifikaci řečníka na základě hlasu.
- Možnosti osvětlení a snímání:
 - **FIR** (*Far-InfraRed*) – vysoká bezpečnost a také vysoké finanční náklady
 - **NIR** (*Near-InfraRed*) – levné, nejčastěji použito pro aktivní snímání

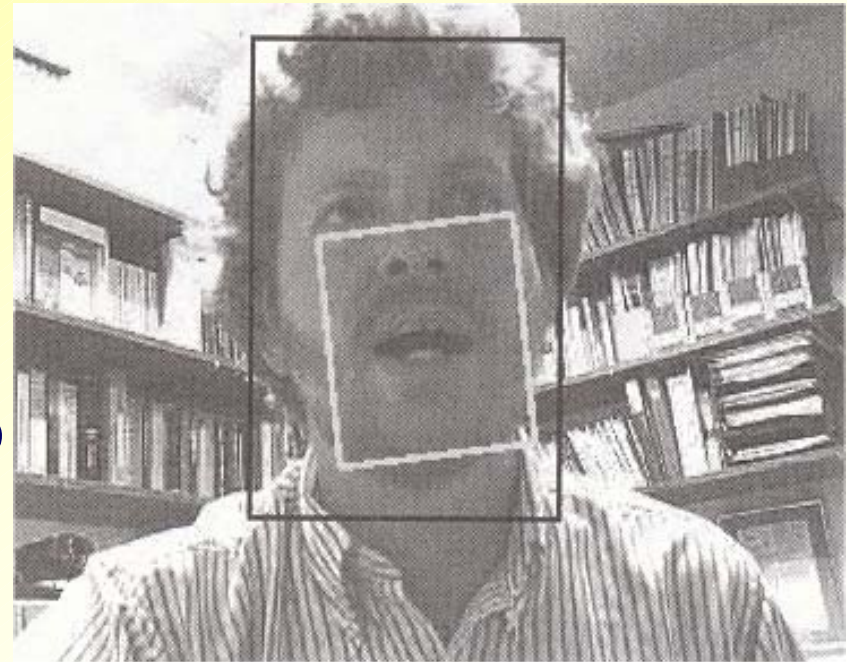


→ Pohyby rtů (II.)

- Velmi výhodnou možností je tvorba multimodálního biometrického systému, který slučuje:
 - Rozpoznávání hlasu
 - Rozpoznávání obličeje
 - Rozpoznávání pohybů rtů
- Takový systém nabízí velmi vysoký stupeň bezpečnosti.
- Téměř každý počítač má mikrofon a minimálně webovou kamerku → realizace nenákladná.
- Profesionální produkt se jmenuje *Biold*.
- K testování byly využity databáze M2VTS (*Multi Modal Verification for Teleservices and Security Applications*)

→ Pohyby rtů (III.)

- Detekce úst v obličeji může být provedena algoritmem na zpracování obličeje (viz. přednáška o obličeji).
- Jednotlivé pohyby jsou nahrány z posloupnosti snímků ve videu.
- Pro nahrání snímků pohybu rtů lze použít také termokameru, čímž stoupnou náklady na celý systém.
- Nutné zajištění vhodného osvětlení, není-li použito infračervené světlo (webová kamera).



→ Pohyby rtů (IV.) - Zpracování

Vstupní obrázek



HSL transformace



Median filtr



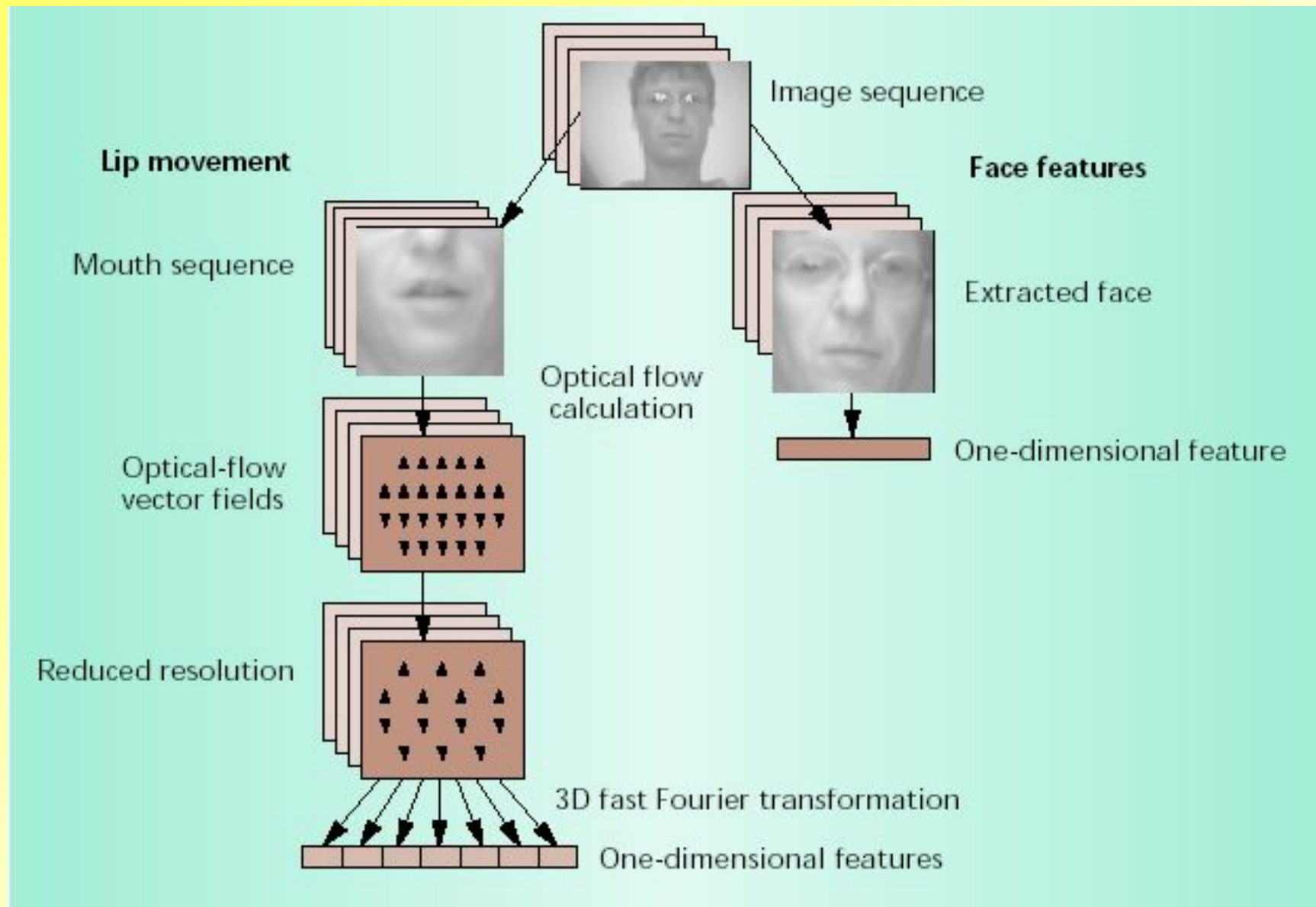
Expanze a redukce



Detekce rtů



→ Pohyby rtů (V.) - Rozpoznání



→ Jiné možnosti

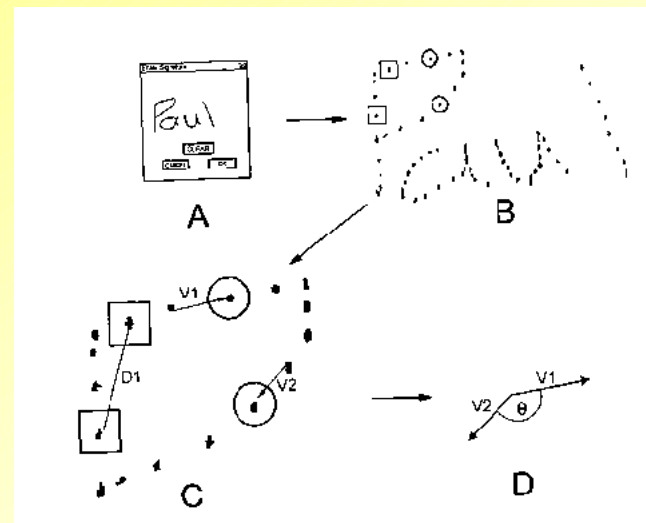
→ K jiným možnostem patří:

→ Dynamika pohybu myši

→ Gestikulace obličeje

→ Srdeční puls

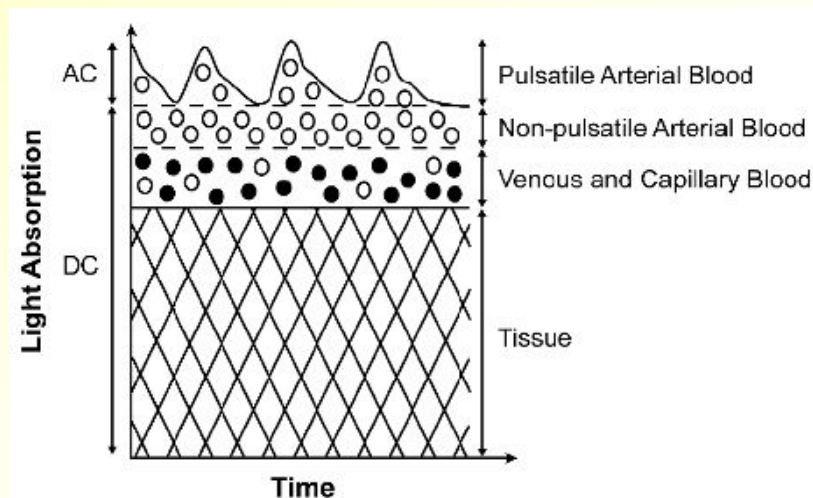
→ (Reakce duhovky na světlo)



→ Srdeční puls a duhovka → testování živosti

→ Gestikulace obličeje je obsažena zčásti v rozpoznávání 3D obličeje.

→ Hlas (řeč) a dynamika písma byly rozebrány v předešlých přednáškách.



→ Děkuji za pozornost!

→ Další termín: 07.12.2005

→ Přednáška: 11. DNA a její využití v biometrii

Použitá literatura: [Bol04], [Chi03], [Ilo03], [Jai04],
[Mon99], [Suu04]

<http://www.biopassword.com/>

<http://www-mitpress.mit.edu/e-journals/Videre/001/articles/Little-Boyd/gait/gait.html>

<http://chihara.aist-nara.ac.jp/people/94/yosiyu-o/research/research.html>