

Dynamický podpis



Schneider



Jim Wild

Biometrické charakteristiky

▶ **Biologické**

- **DNA, krev, sliny**

▶ **Biologické/Fyziologické**

- **otisk prstu, zornice, tvář, sítnice**

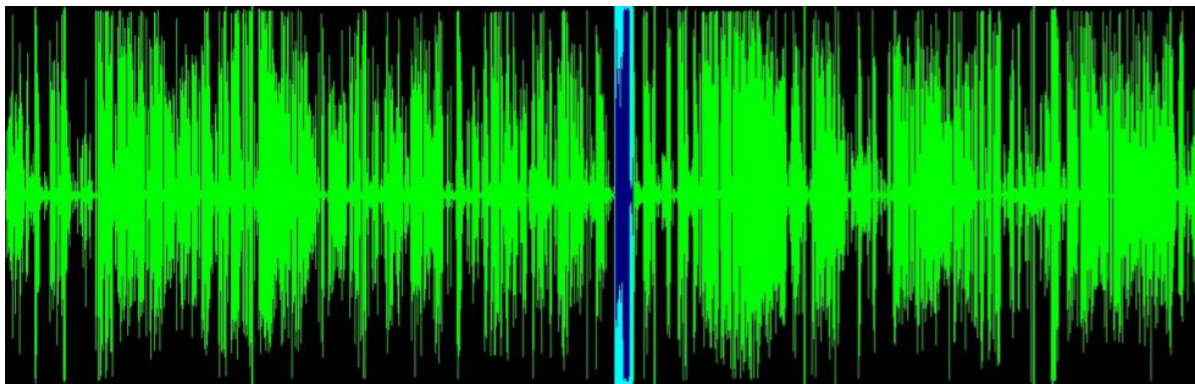
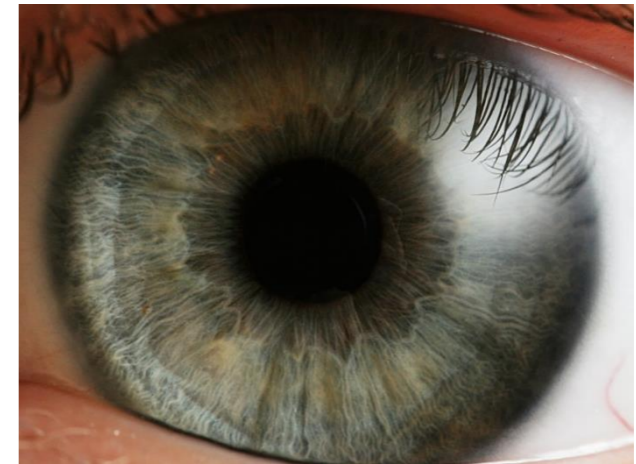
▶ **Chování**

- **podpis, chůze, psaní na klávesnici**

▶ **Složené**

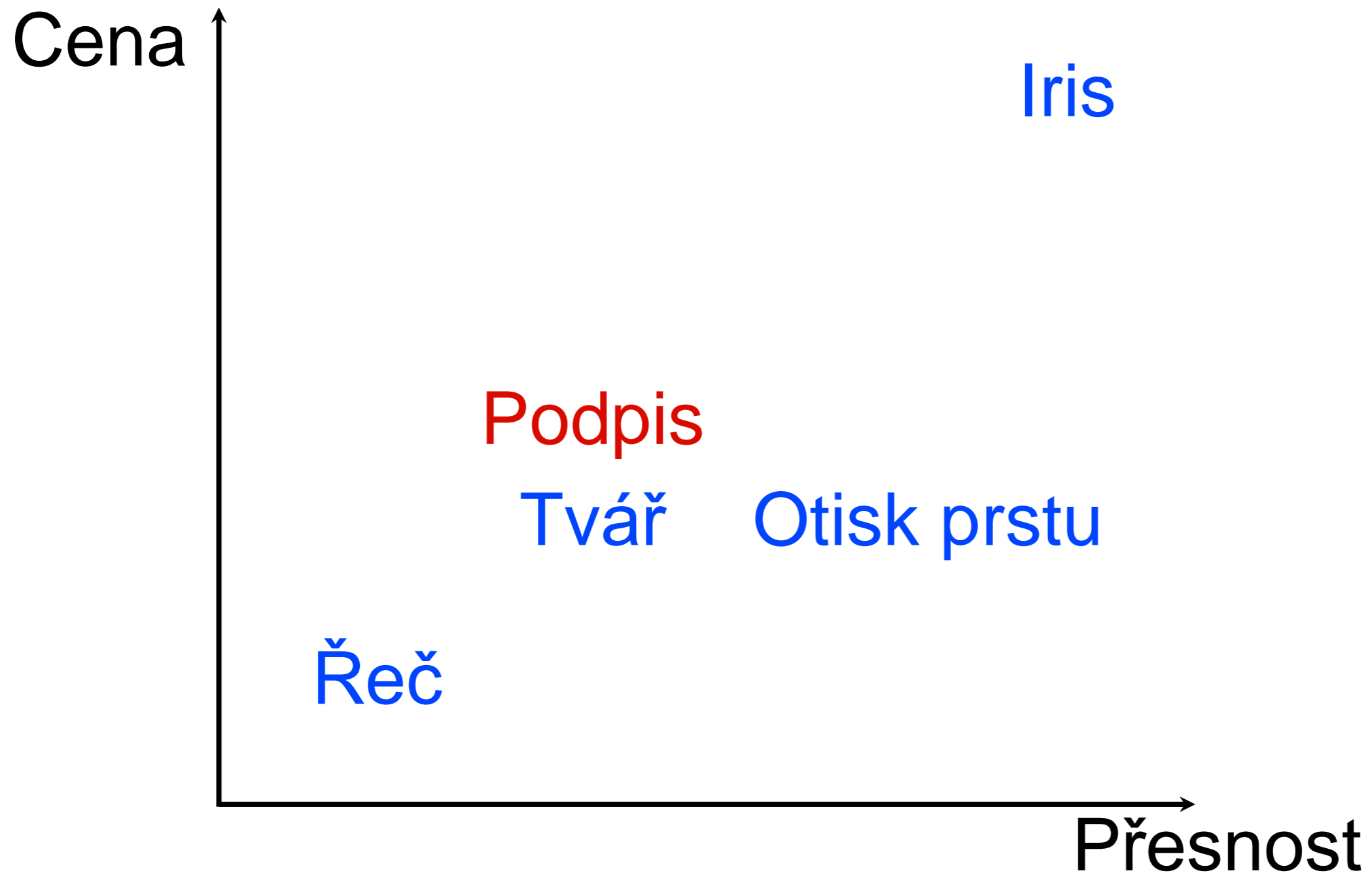
- **Řeč**

Různorodost charakteristik



Barack Obama

Porovnání charakteristik



Podpis

Statický



Dynamický

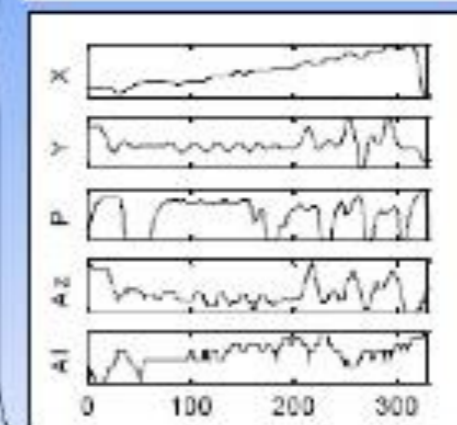
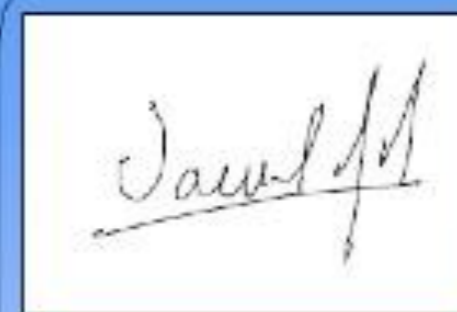
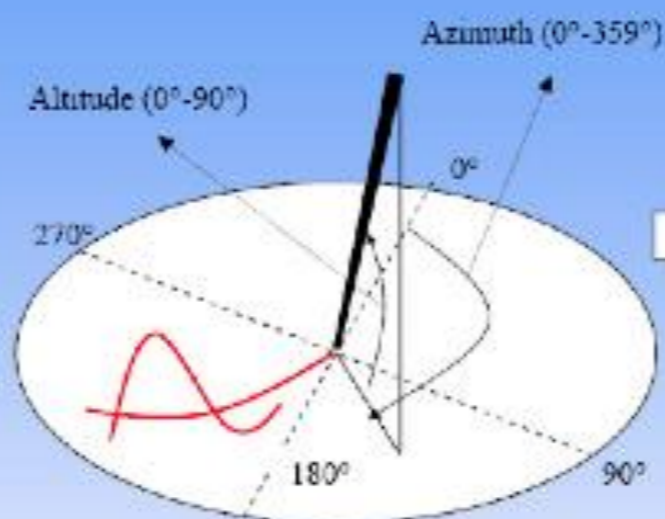


Podpis

- ▶ **statický (offline)**
 - **běžný podpis naskenovaný z dokumentu**
- ▶ **dynamický (online)**
 - **podpis získaný pomocí tabletu, obsahující dynamické informace o x,y,z pozici pera v čase (případně další) ve vyšším rozlišení**
- ▶ **elektronický**
 - **Elektronický údaj (číslo), který slouží k ověření identity podepsané osoby ve vztahu k datové zprávě**

Podpisy - porovnání

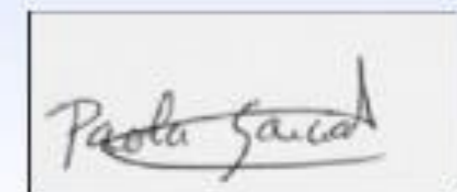
- On-Line:



- Off-Line



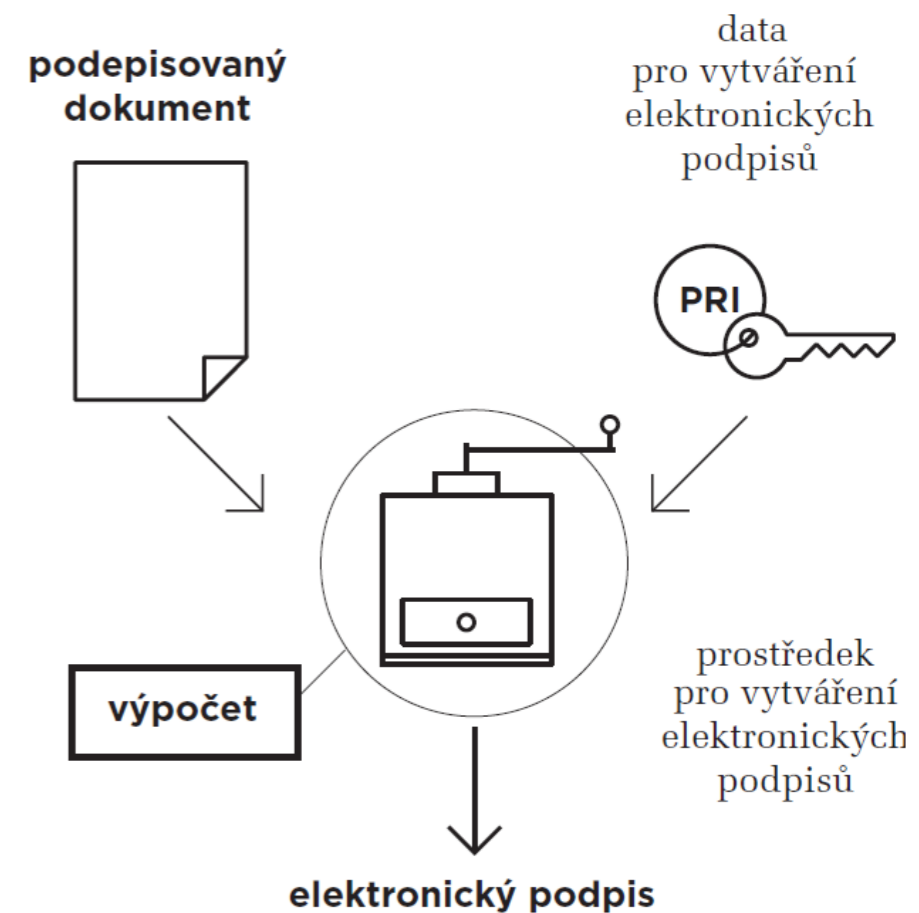
SCANNER



Elektronický podpis (zaručený)

► Princip

- **Asymetrické kryptografie**
- **Uživatel - privátní klíč (data)**
- **Organizace zajišťující potvrzení veřejného klíče (certifikát)**

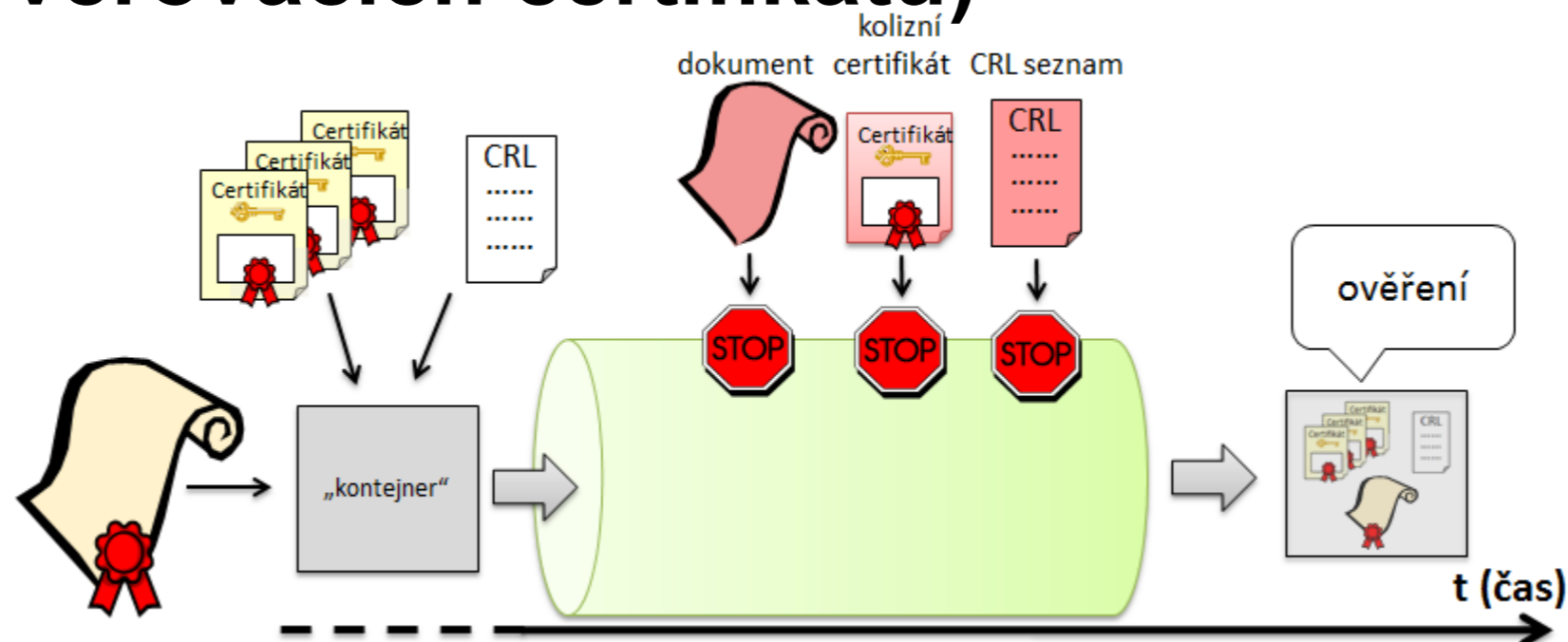


► Účel

- **Elektronické podepisování dokumentů**
- **Jistota identifikace a autentizace podepsaného**

Problematika El. podpisu

- ▶ **Datové schránky – povinný přechod k EP**
- ▶ **Dlouhodobé uchování záznamu – dohledatelnost certifikátů**
- ▶ **Řešení**
- ▶ **Long Term Validation (přiřazení ověřovacích certifikátů)**



Elektronický a dynamický podpis

▶ **Není úplně dořešená legislativou**

▶ **Podpisové vzory**

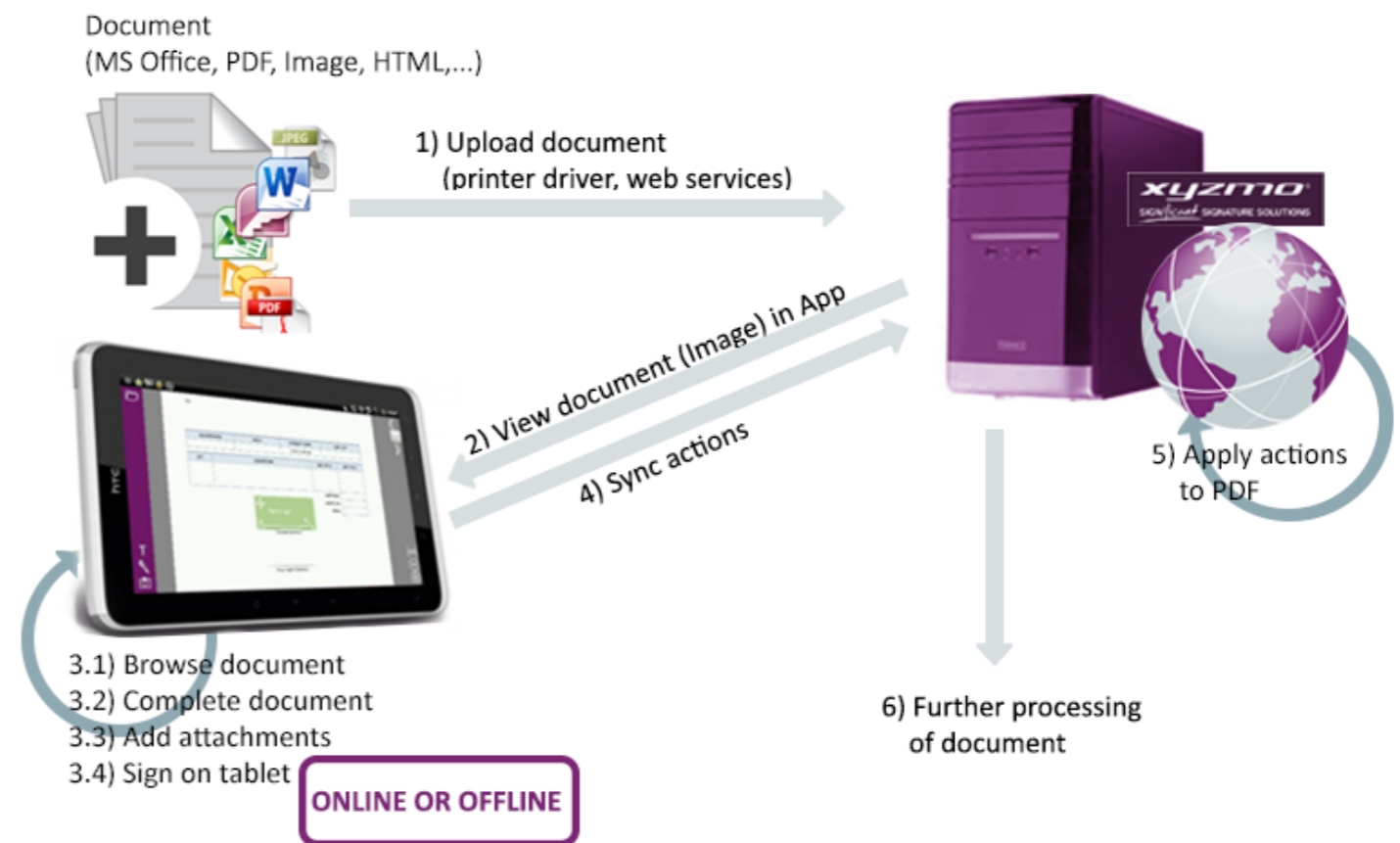
• **Správa a uchovávání**

▶ **Řešení stárnutí**

▶ **Integrita s dokumentem**

• **Časové razítko**

▶ **Strojové použití?**



<http://www.xyzmo.com/en/products/Pages/digital-signature-ipad-android.aspx>

Legislativa

- ▶ **Společná pro dynamický a el. podpis**
- ▶ **Spadá pod direktivu 1999/93/EC**
obnovenou regulací No 910/2014
- ▶ **Česká legislativa**
 - **zákon 297/2016 Sb o službách vytvářejících důvěru pro elektronické transakce**
 - **Zákon 298/2016 Sb**
 - Dřívější zákon o elektronickém podpisu 227/2000 Sb. byl zrušen v roce 2016
- ▶ **Standardizace ISO/IEC 19794-11**
(https://webstore.iec.ch/preview/info_isoiec19794-11%7Bed1.0%7Den.pdf)

Autentizace

▶ Způsoby autentizace:

- **založené na vlastnictví**
 - kreditní karta, klíče (něco nosíme u sebe)
- **založené na znalosti**
 - heslo, PIN (něco si pamatujeme)
- **biometrické**
 - ... (část toho, co jsme)

Podpis je kombinace **znalosti** (co a jak píšeme) a **biometrie**.

Ideální biometrický ukazatel

- ▶ **Univerzálnost** - lze jej měřit u kohokoliv?
- ▶ **Unikátnost**
- ▶ **Stálost** - ukazatel by se neměl v čase měnit
- ▶ **Dostupnost** - lze data měřit běžně dostupným přístrojem?
- ▶ **Etika** - získání dat musí být společností považováno za etické

Podpis není ideální biometrický ukazatel.

Aplikace

▶ Online

- Přihlašování (Tablet)
- Ověření dokumentu (podepsání)
- UPS

▶ Offline

- Ověření dokumentu (banky, smlouvy, závěti, etc)
- Forenzní analýza

IKEA - elektronická účtenka

IKEA chooses Wacom's SignPad (STU-500) to reduce costs and paperwork

Area: [Business Solutions](#) » [Electronic Signatures](#)

Location: [Europe](#)



if using paper.

The major home furnishings retailer IKEA has adopted the electronic receipt storage solution from TeleCash GmbH & Co. KG based on Wacom's LCD signature tablet technology - the STU-500 (or SignPad) - across Germany. In pioneering this solution, TeleCash is using the market leading technology from Wacom for generating electronic signatures. TeleCash has chosen the STU-500 due to its accuracy, its ability to significantly reduce process costs, simplify service at the point of sale and reduce the amount of paperwork needed for a transaction. The STU-500 accuracy in particular allows customers to sign naturally as

T-Mobile a další



Přístroje



Společnosti - odkazy

▶ Online

- **SOFTPRO** - www.softpro.de
- **CYBERSIGN** - www.cybersign.com
- **CIC** - www.cic.com
- **SIGNOTEC** - www.signotec.com

▶ Offline

- **SIGNATURENET** - www.signaturenet

Dynamický podpis na normálním tabletu/mobilu

- Xyzmo
- <http://www.xyzmo.com>
- SignoTec
- <http://en.signotec.com/>

Document
(MS Office, PDF, Image, HTML,...)



1) Upload document
(printer driver, web services)



5) Apply actions
to PDF

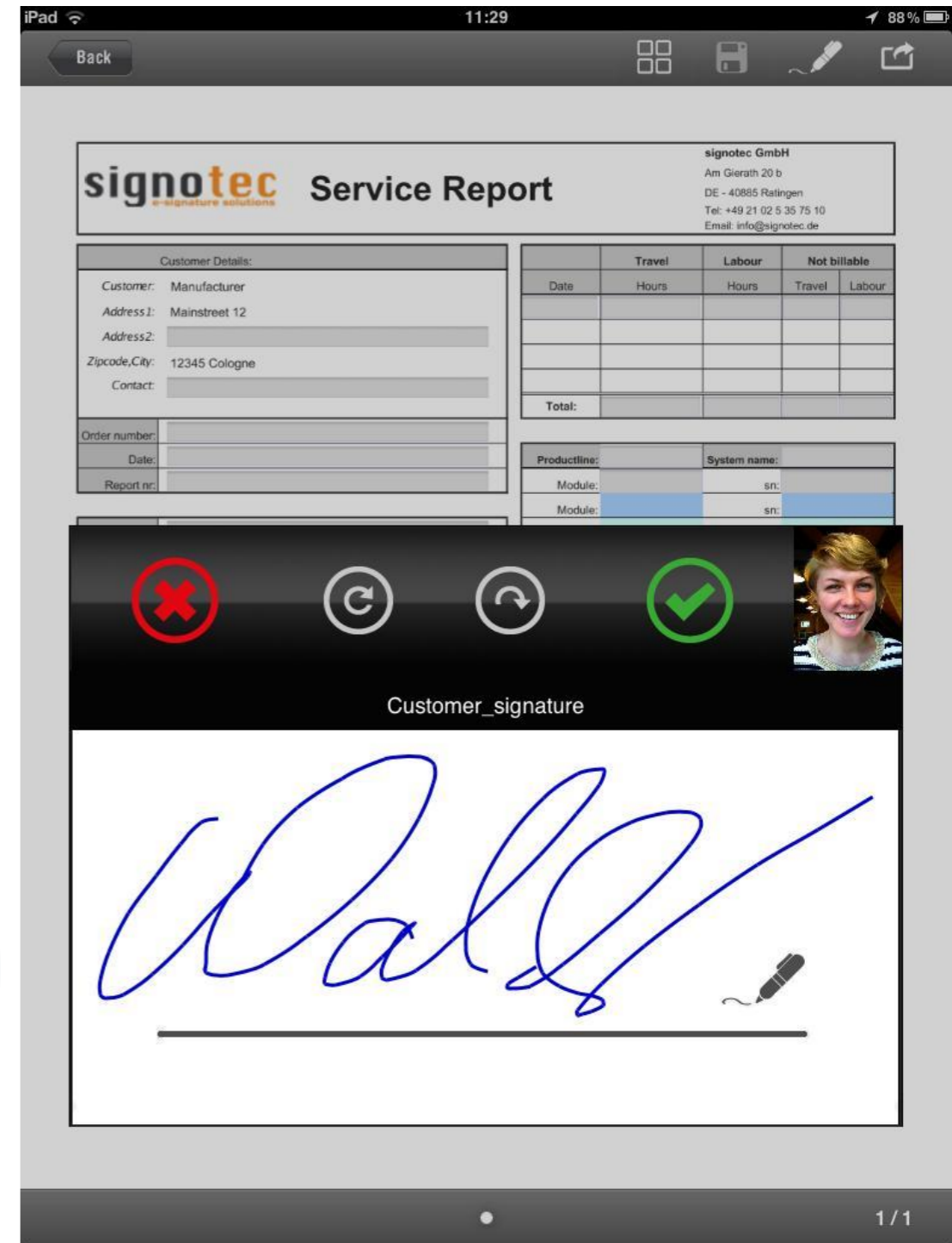
2) View document (Image) in App

4) Sync actions

6) Further processing
of document

- 3.1) Browse document
3.2) Complete document
3.3) Add attachments
3.4) Sign on tablet

ONLINE OR OFFLINE



Speciální pera (stylus)

- **Běžná neměří přítlak**
 - Nepotřebují napájení
 - Levné (10+)\$
- **S přítlakem**
 - Nutné napájení
 - USB akumulátor
 - Komunikace
 - Bluetooth (bezpečí)



BlueSniper (2005)

- Odposlech na více než míli (1,6km)
- Výroba popsaná na internetu
- <http://www.smallnetbuilder.com/content/view/24256/98/>
- Cena součástek pod 400 \$
- Mění pouze dosah z udávaných 10 m



Na trhu – s přitlakem

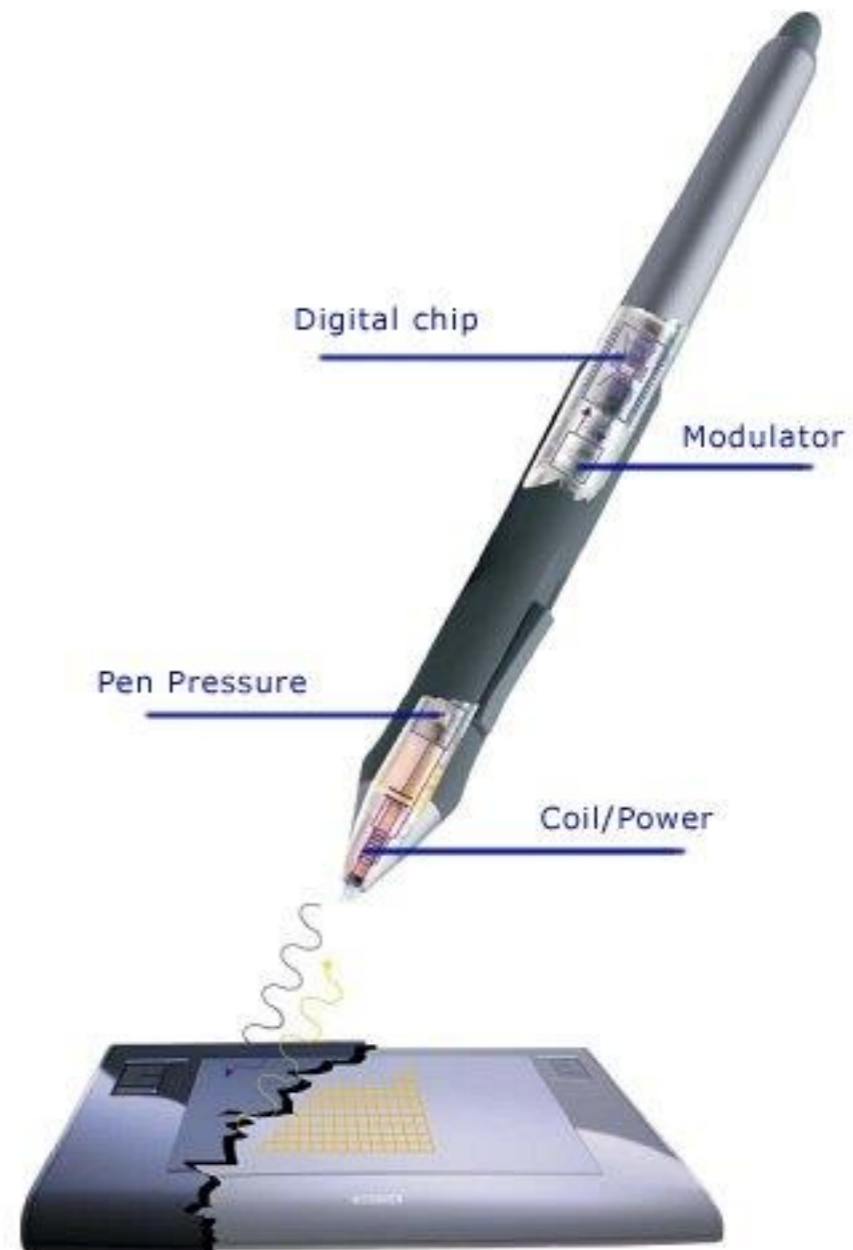
- Wacom Intuos Creative Stylus 2 (80 \$)
 - <http://intuoscreativestylus.wacom.com/en/>
- Pogo Connect
 - <http://www.tenonedesign.com/connect.php>
- Jaja Hex3
 - <http://www.hex3.co/products/jaja>
- Jot Touch (55 \$)
 - <http://adonit.net/jot/touch/>

Tablet

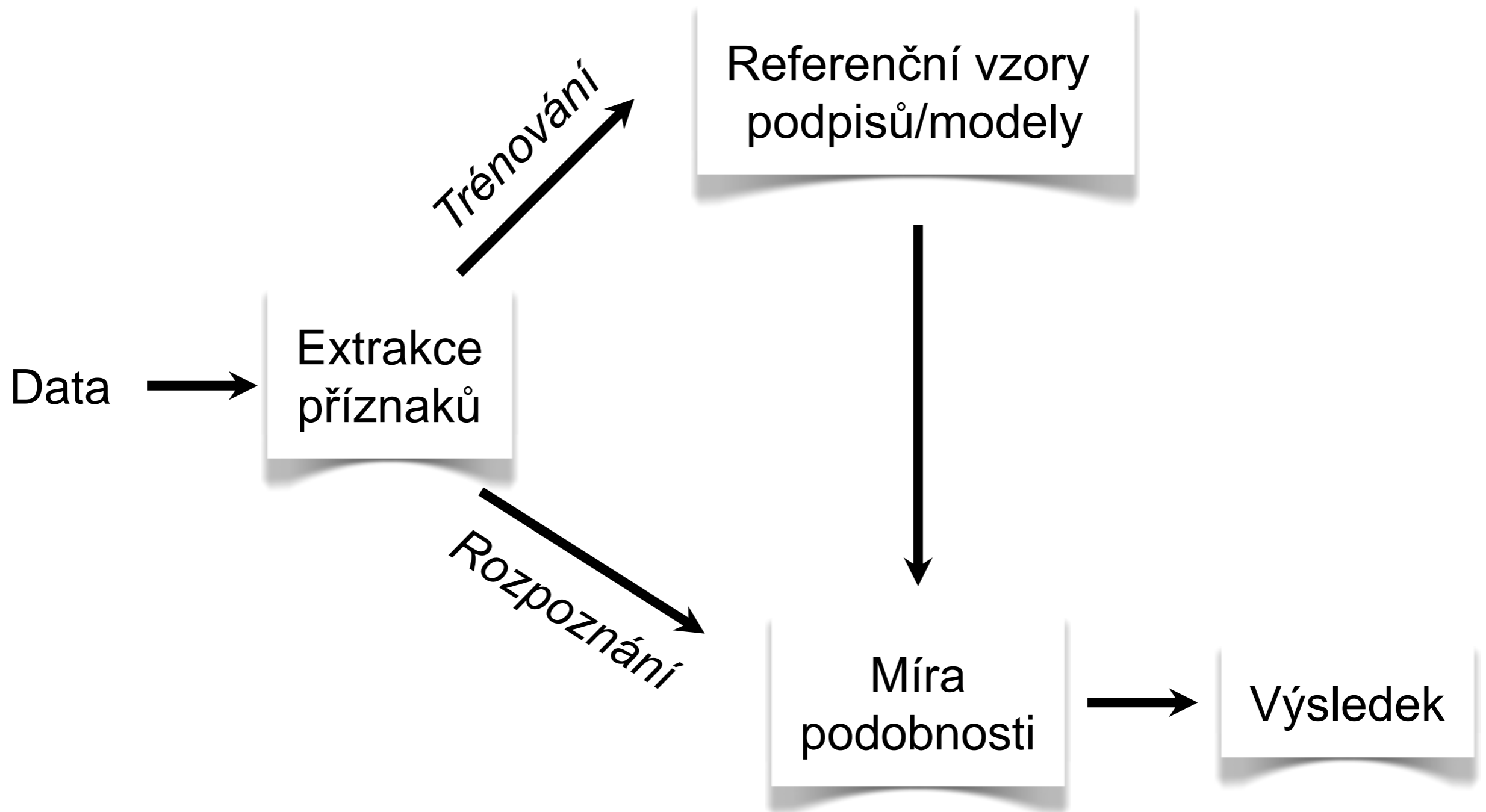


Jak funguje grafický tablet

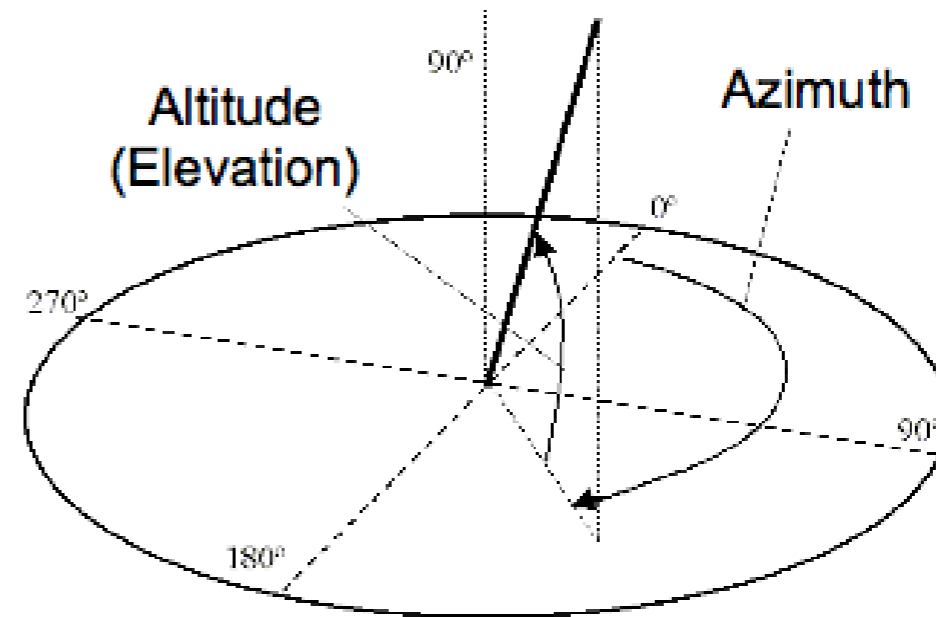
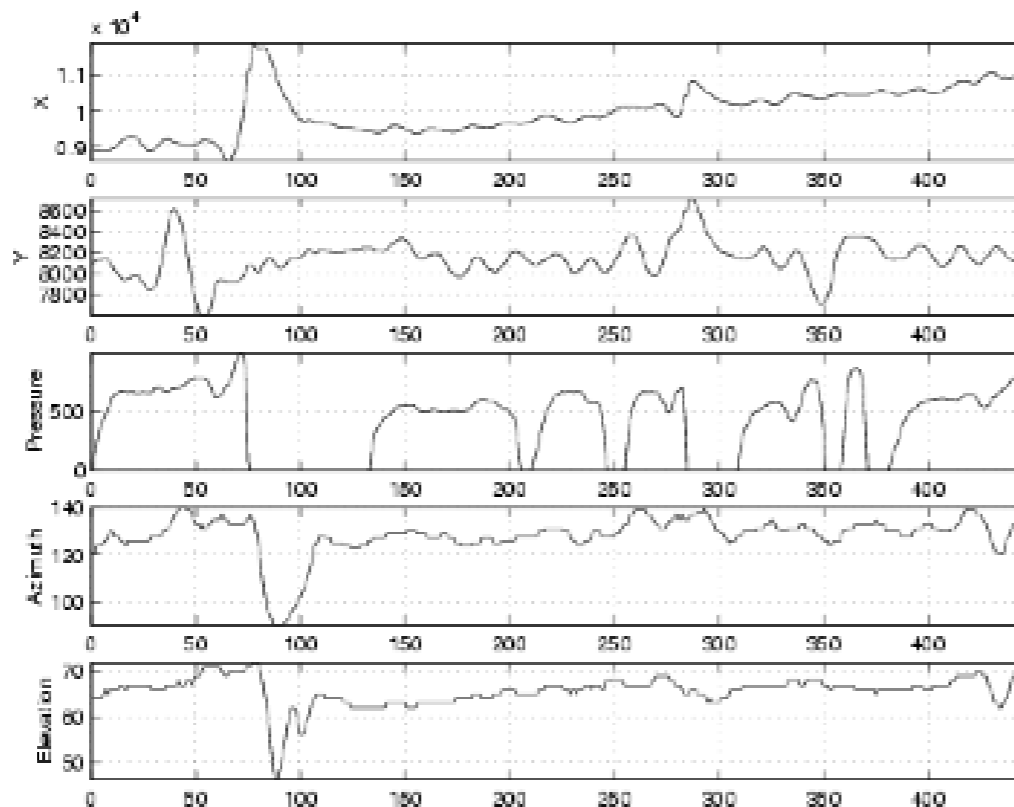
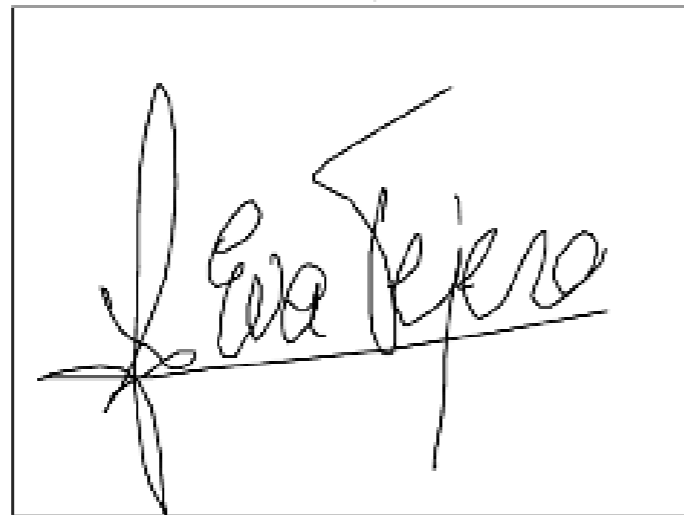
- ▶ Elektromagnetická rezonance
- ▶ Tablet
 - vysílá/přijímá
- ▶ Pero
 - rezonanční obvod
cívka-kondenzátor
 - modulace přitlaku,
stisku tlačítek



Rozpoznání podpisu



Dynamický podpis



Příznaky:

- souřadnice X
- souřadnice Y
- přítlak
- natočení pera (0° - 359°)
- náklon pera (0° - 90°)

Další příznak - Stisk

U.S. Patent

May 21, 1991

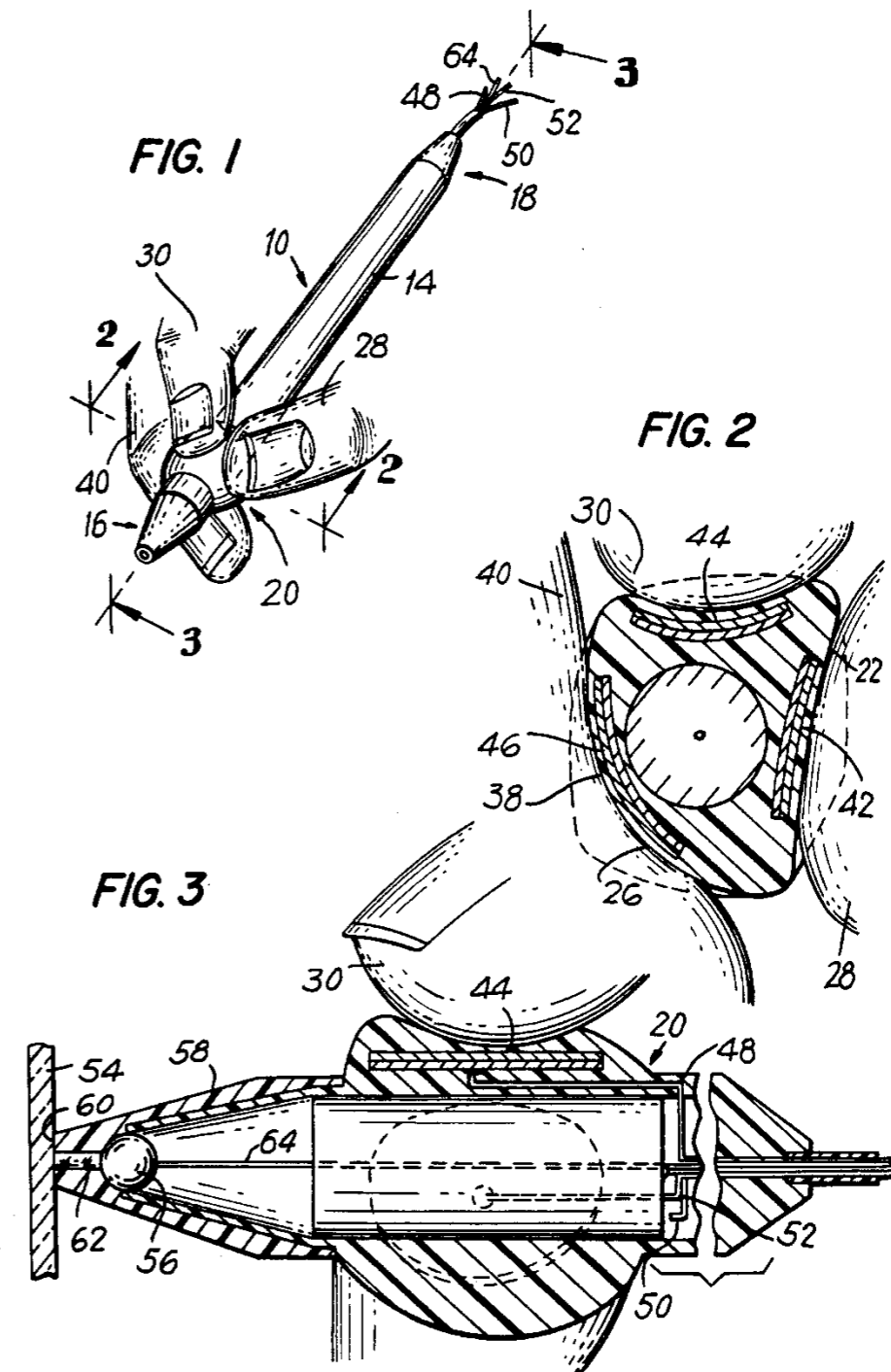
Sheet 1 of 2

5,018,208

► Input device for dynamic signature verification systems

- Patent US 5018208 A
- „Finger pressure exerted by a writer's fingers on the barrel of a hand-held instrument is employed to dynamically verify a signature.“

► Atd...



Padělání

► Typy padělků

1. náhodně napsaný text, podpis jiné osoby
2. podpis vytvořený na základě offline předlohy (s dostatečným časem na naučení)
3. podpis vytvořený na základě sledování, jak podpis vzniká (přes rameno)
4. kvalitní padělek: kombinace (2) a (3)

Padělky

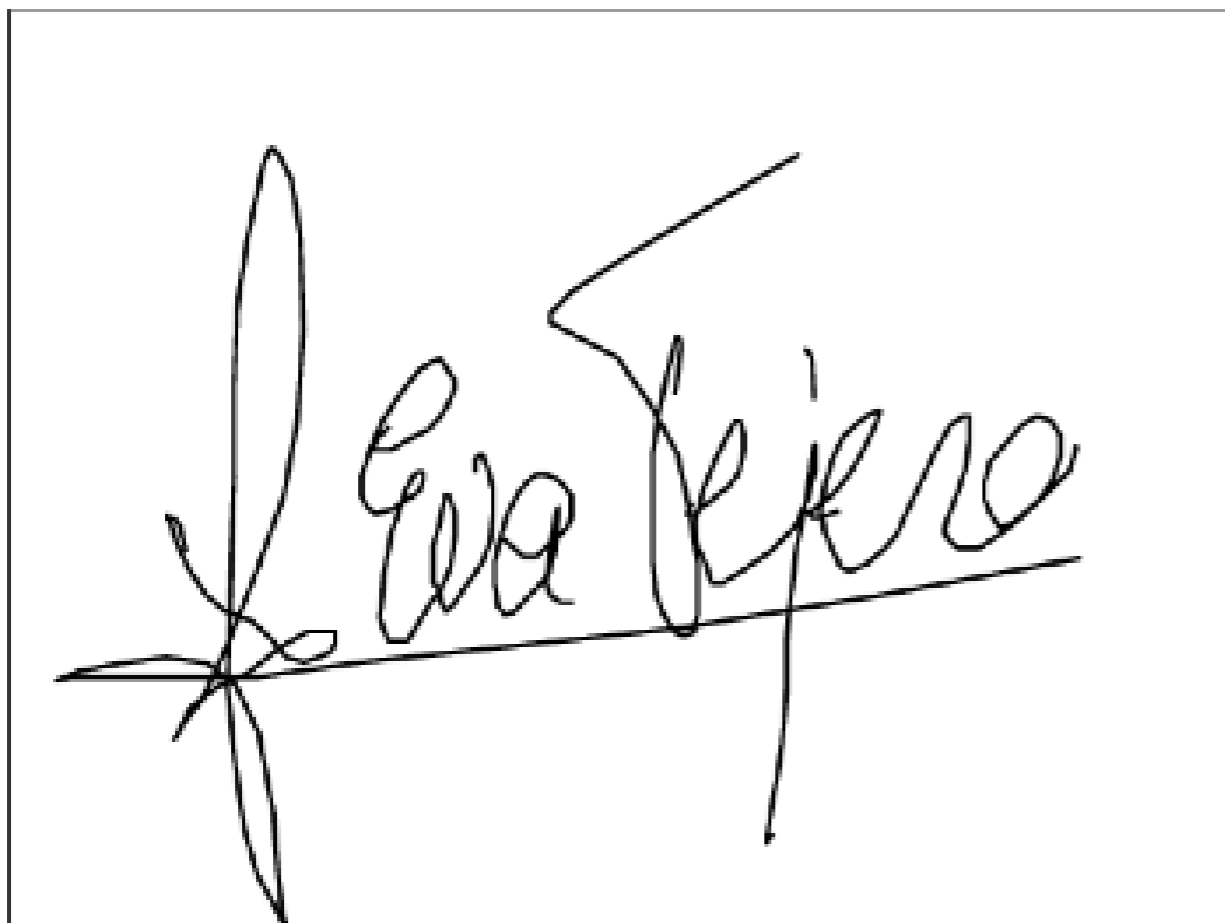


Originál

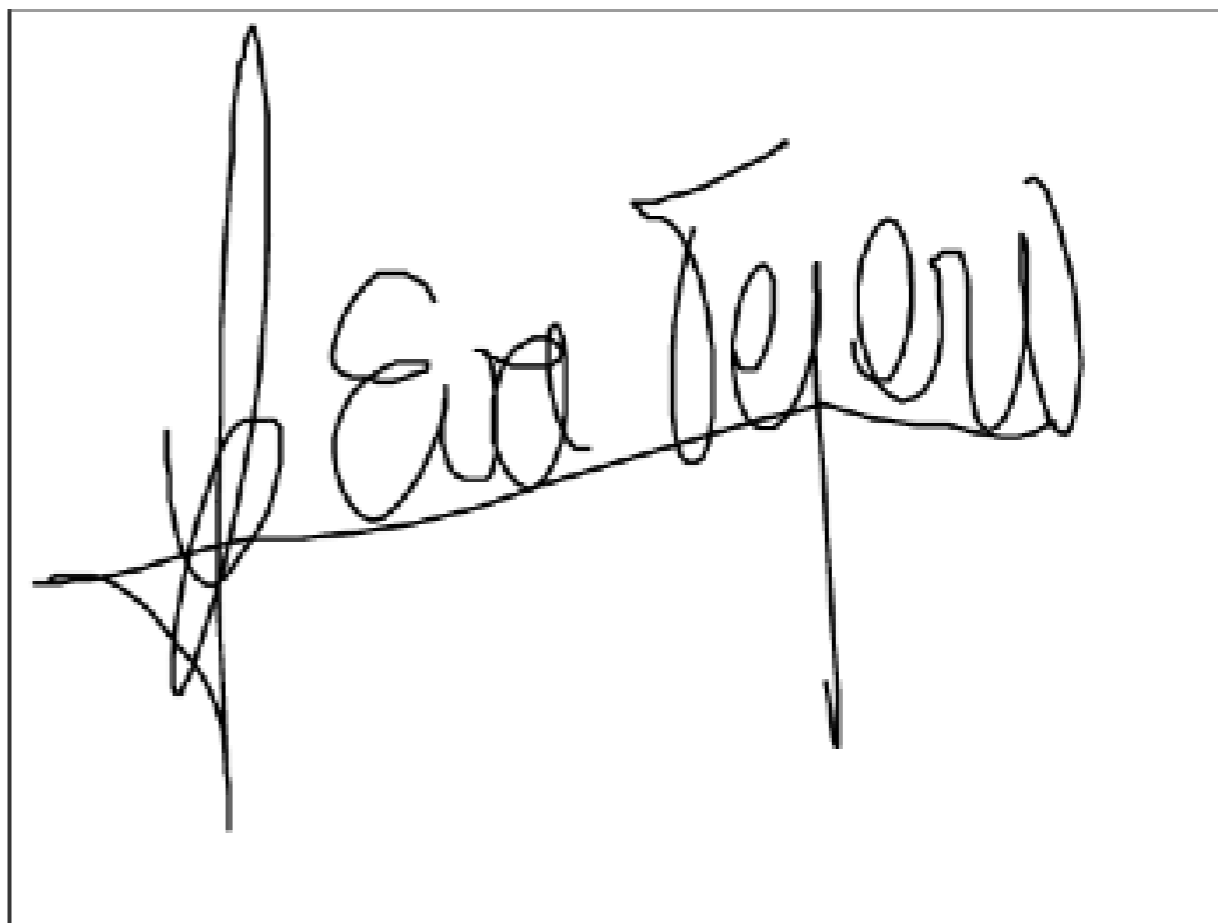
(3) Padělek
ze sledování

(2) Padělek
z předlohy

Originál a kvalitní padělek

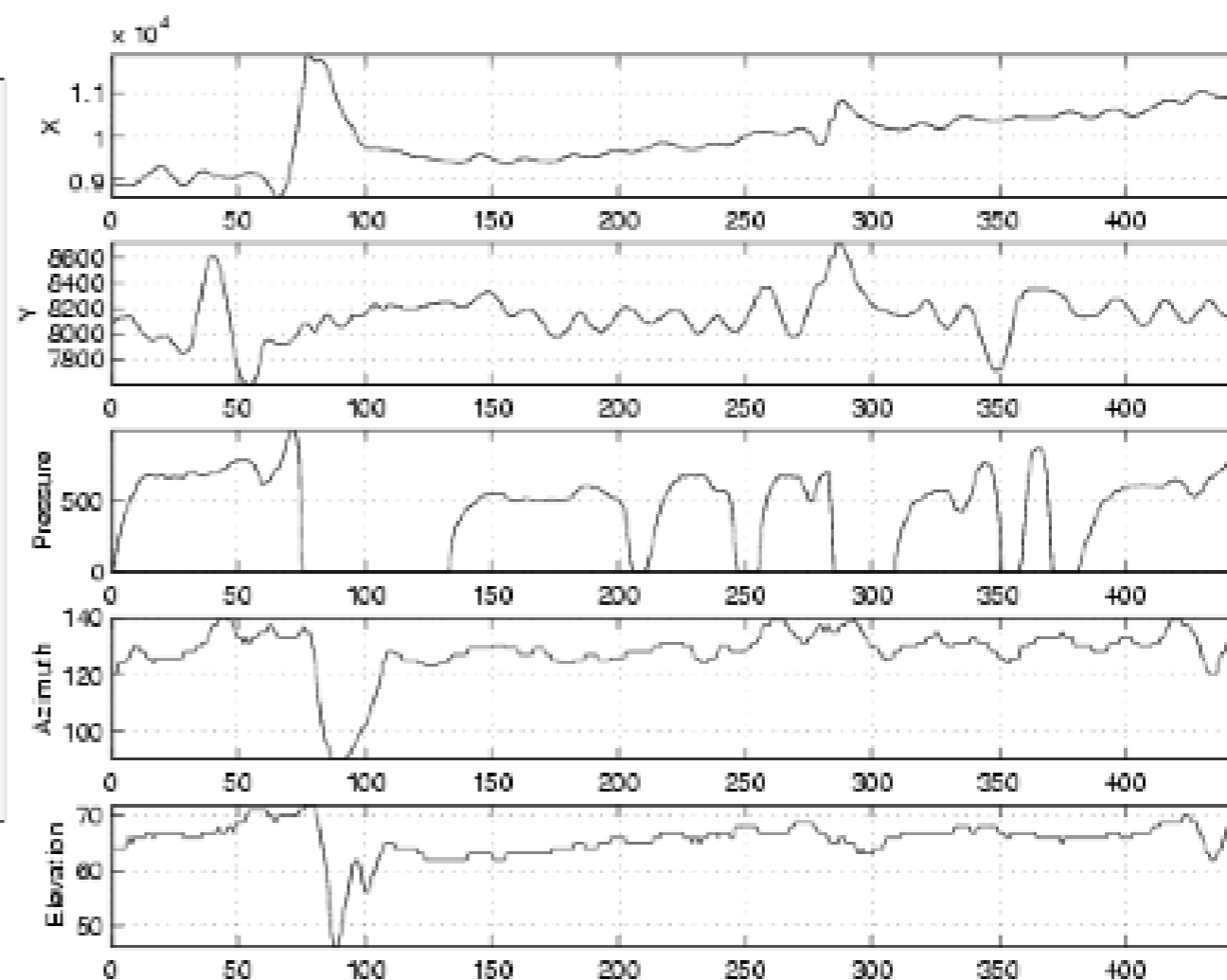
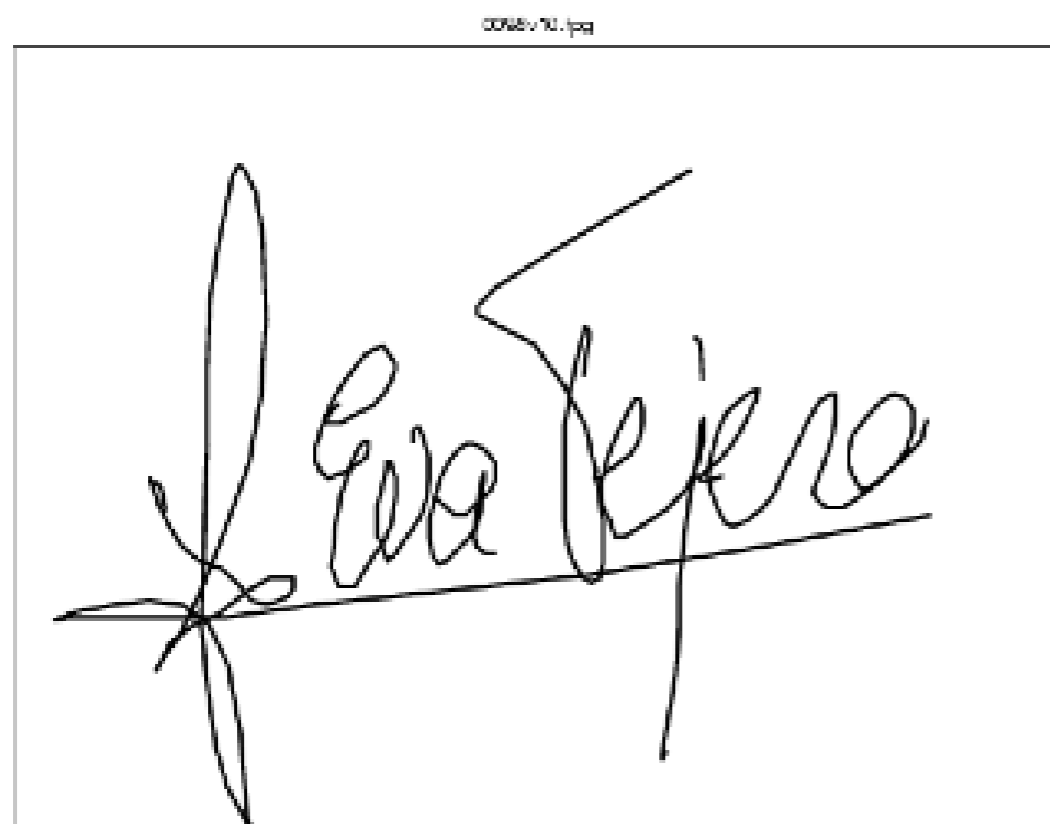


Originál

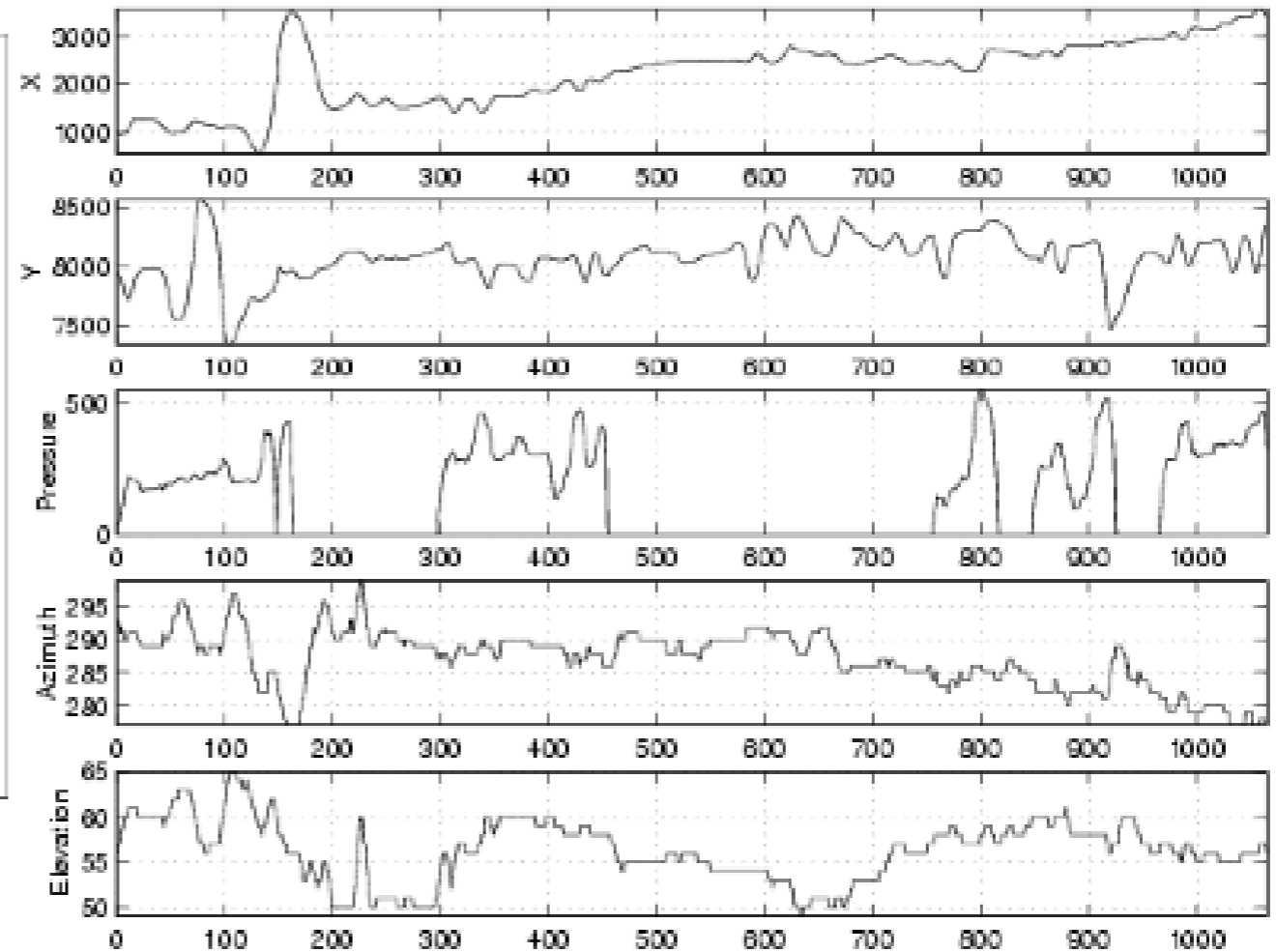
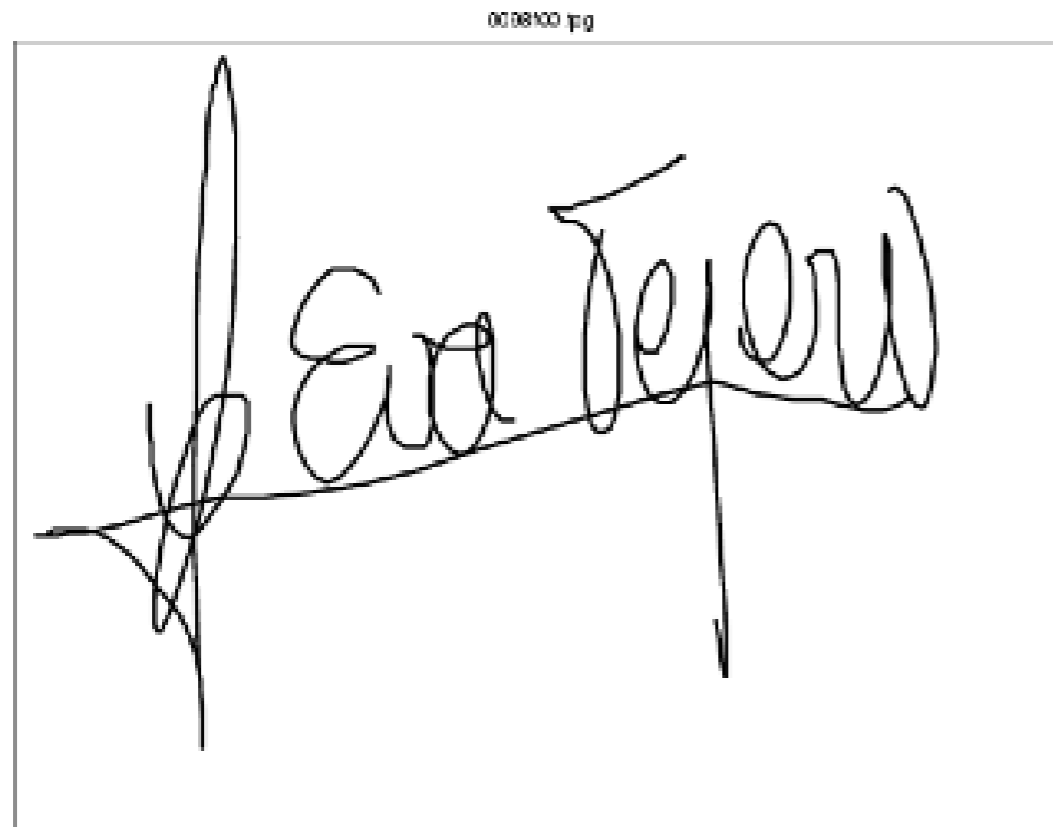


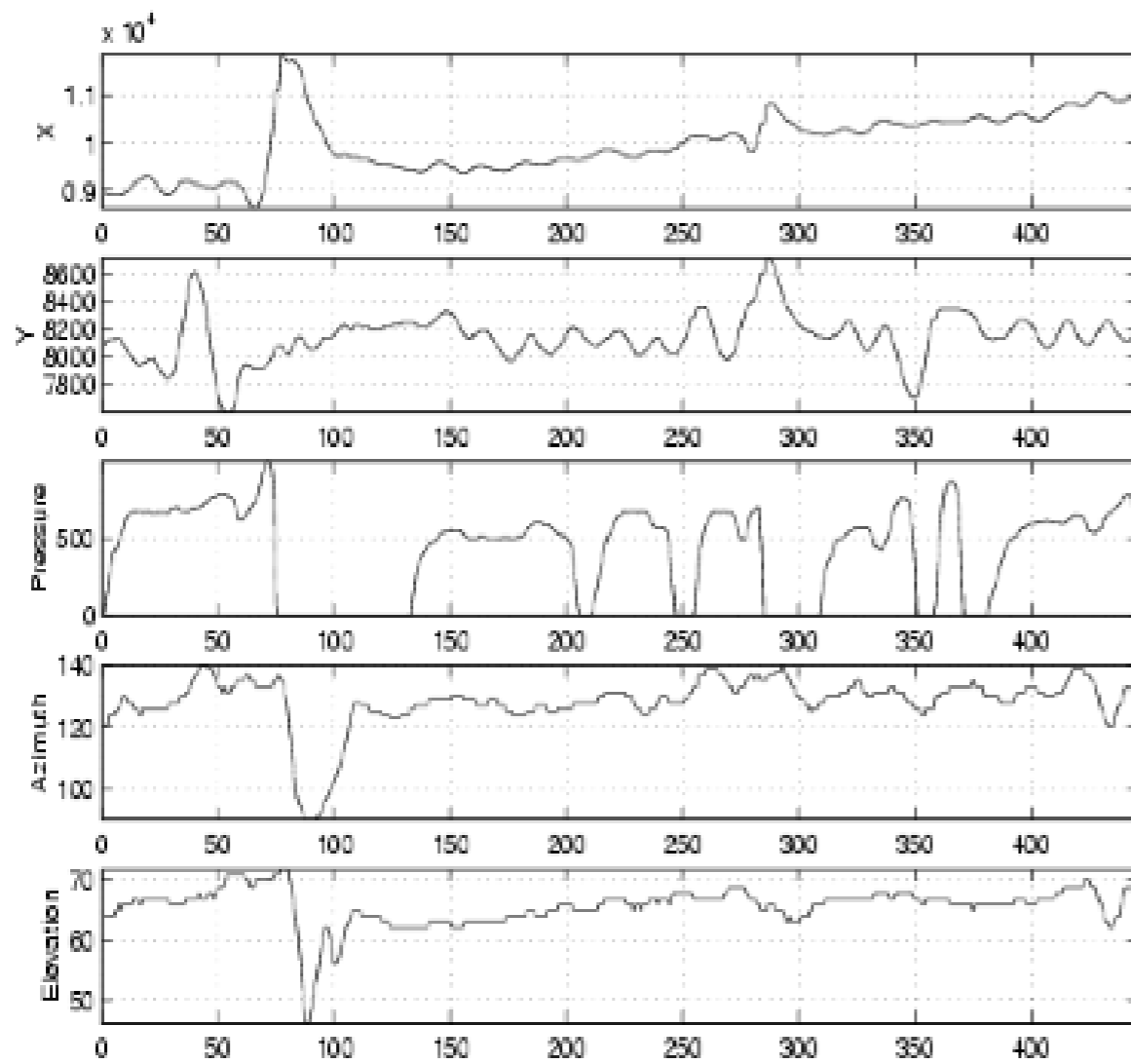
(4)Kvalitní padělek

Originální podpis

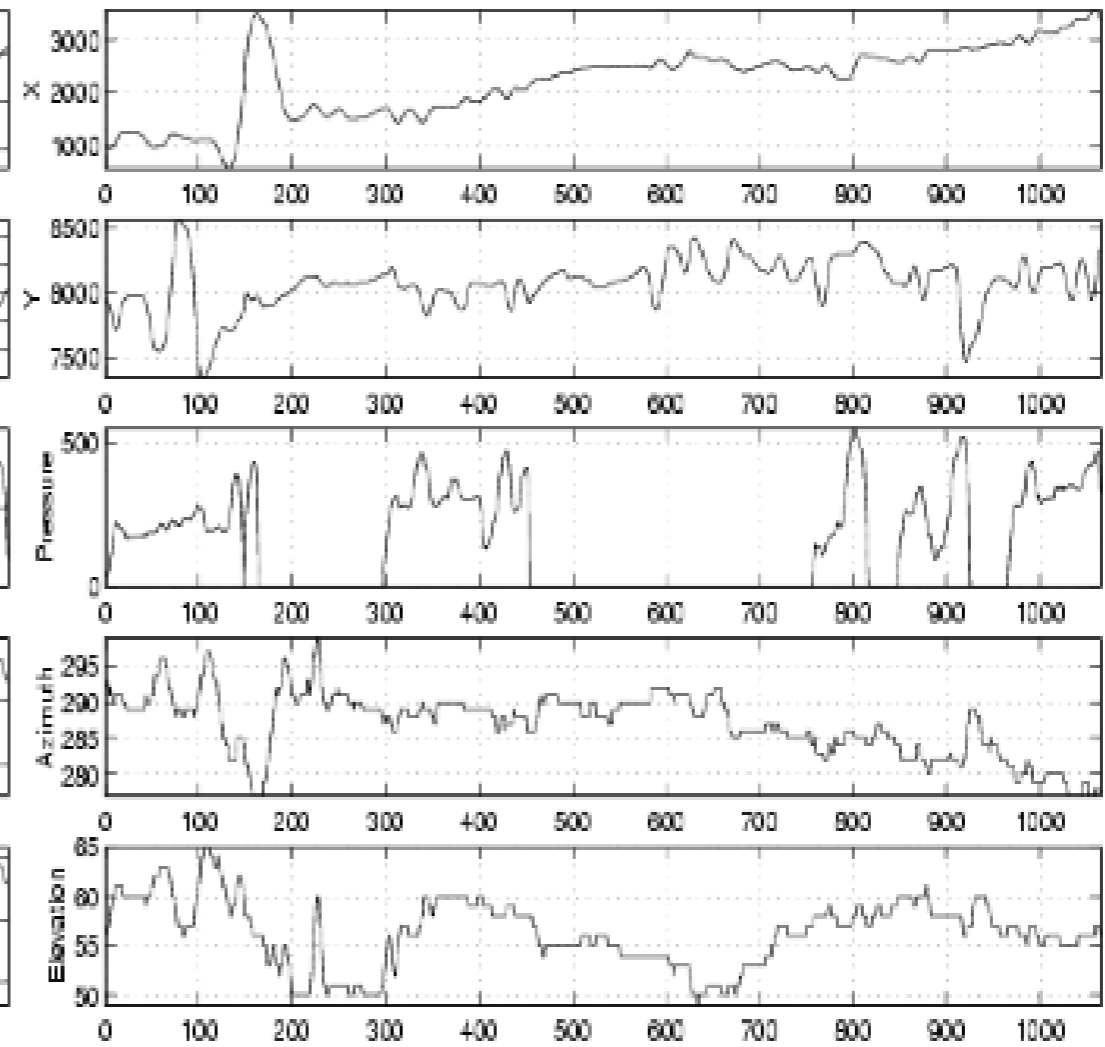


Kvalitní padělek



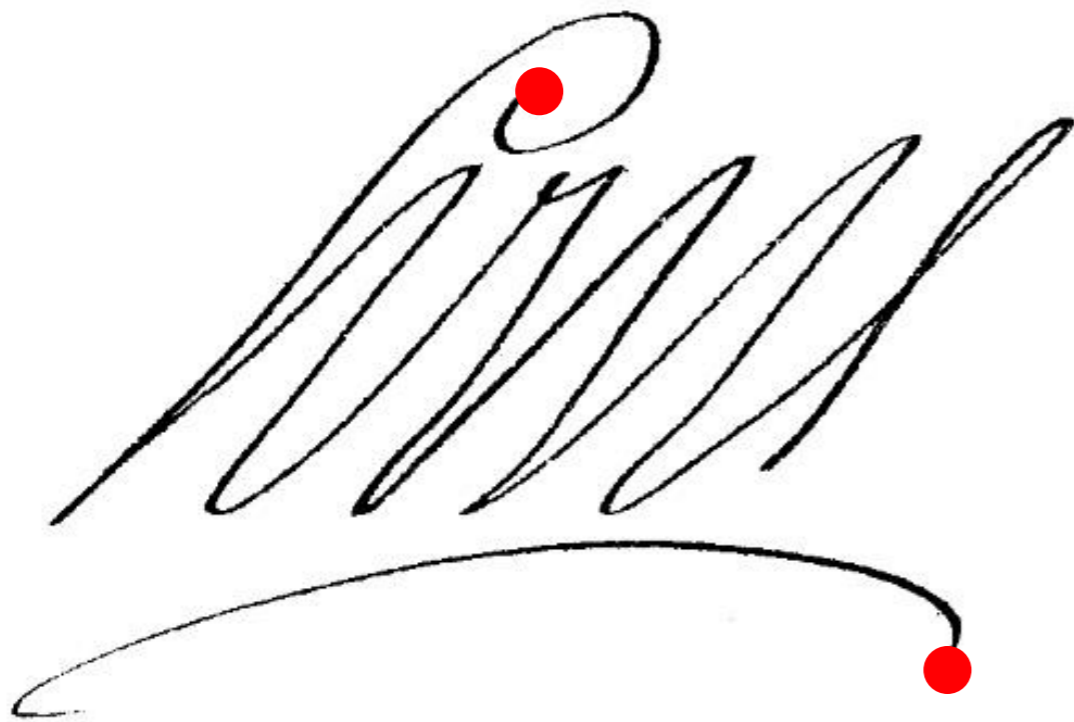


Originál



Kvalitní padělek

Předzpracování



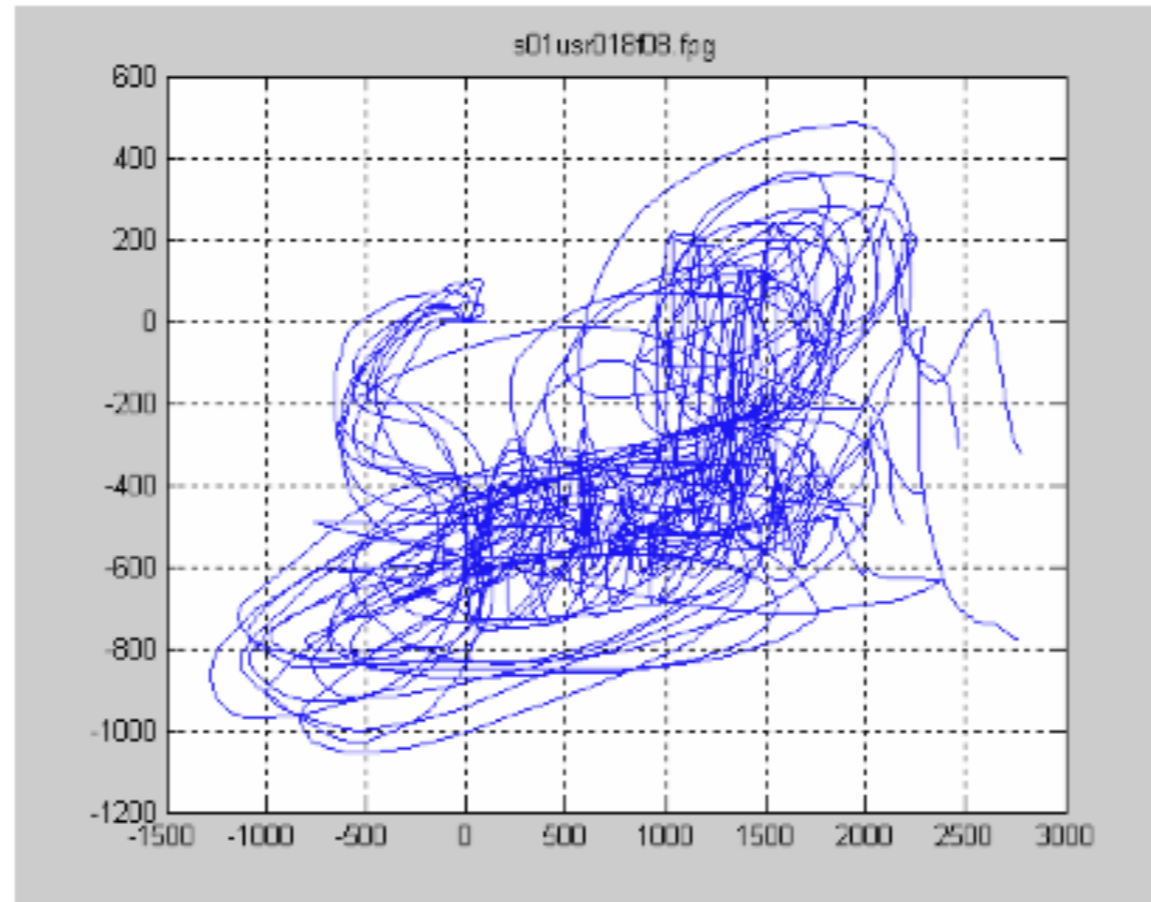
► Vyhlazování

- **vstupní signál bývá často velmi zubatý**

► Segmentace

- **začátek: první přitlak**
- **konec: poslední zvednutí pera (delší než ...s)**

Předzpracování



Všechny podpisy musí být zarovnány vzhledem k počátečnímu bodu (např. [0,0]).

Lokální a globální příznaky

► Lokální příznaky

- souřadnice x, y

- rychlost v $v = \sqrt{\dot{x}_t^2 + \dot{y}_t^2}$

- zrychlení a

- tečný úhel $\Theta_t = \arctan\left(\frac{\dot{y}_t}{\dot{x}_t}\right)$

- natočení pera

- náklon pera

- 1. a 2. derivace příznaků

Globální příznaky

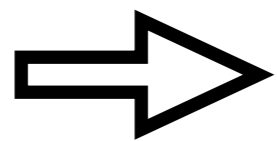
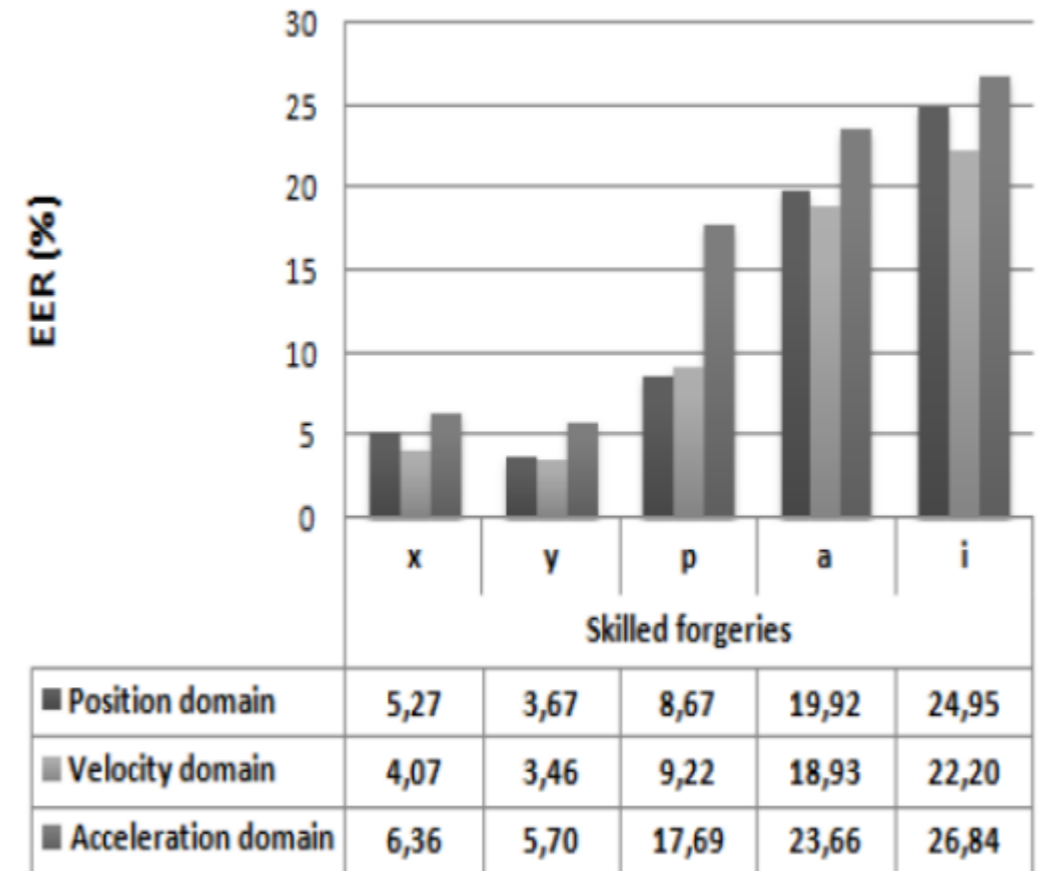
▶ Globální příznaky

- Délka, výška, šířka podpisu
- Jak dlouho trval podpis
- Jak dlouho byl/nebyl přítlak
- Průměrná rychlost
- Maximální rychlost
- Minimální rychlost
- atd.

Lokální příznaky

- ▶ **x, y**
- ▶ **p - přítlak**
- ▶ **a - natočení (azimuth)**
- ▶ **i - náklon (inclination)**

+ *1. a 2. derivace*



15 příznakových vektorů

(i když následně došlo k redukci)

Příklady extrakce lokálních příznaků

- ▶ **Derivaci** je vhodné aproximovat regresí druhého řádu - ne pouze jednoduchou diferencí vzorků.
Vzorec pro regresí ***N***-tého řádu v čase ***t*** pro parametr ***q*** je:

$$reg(q_t, N) = \frac{\sum_{\tau=1}^N \tau (q_{t+\tau} - q_{t-\tau})}{2 \sum_{\tau=1}^N \tau^2}$$

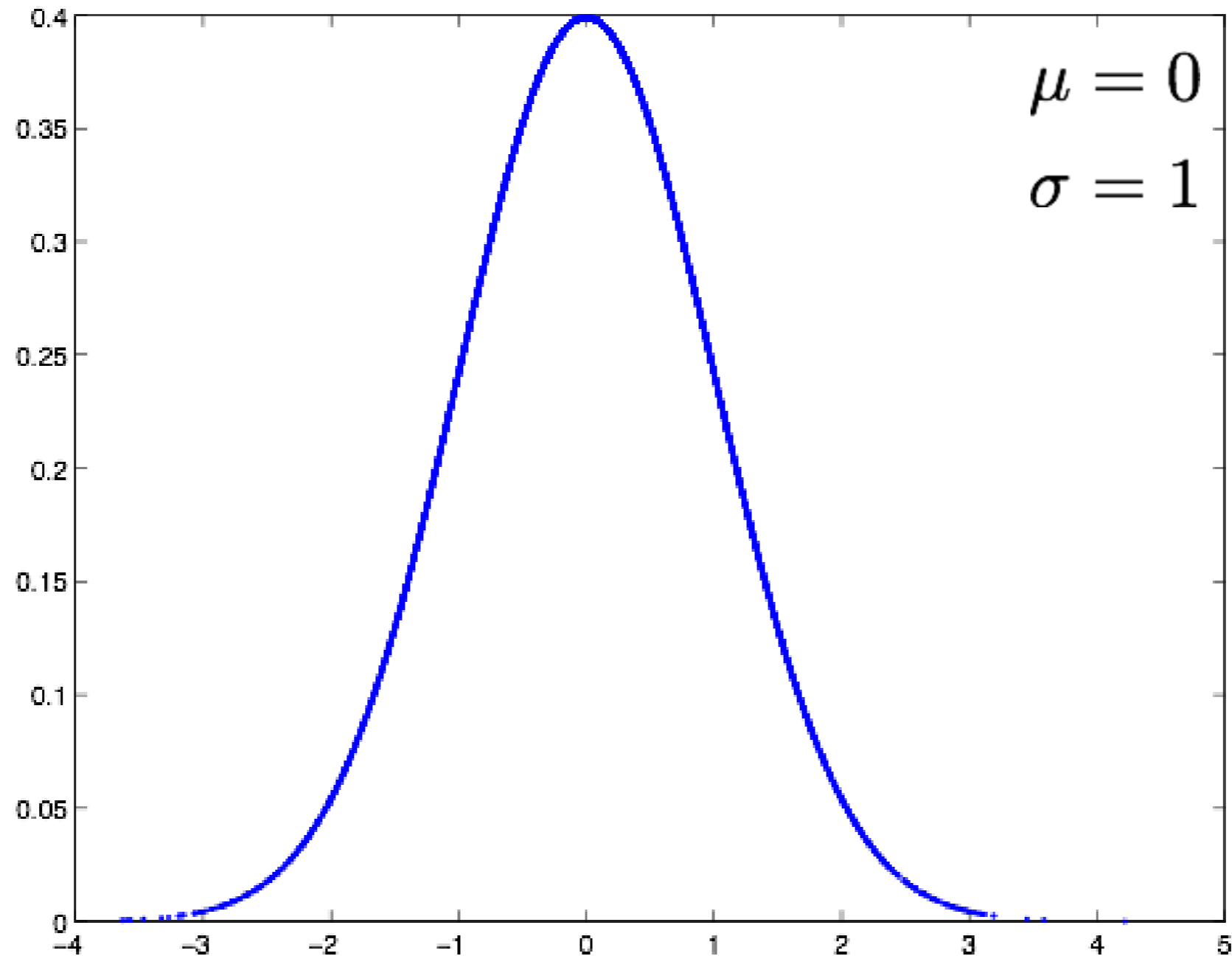
- ▶ **Rychlost a zrychlení** pak lze spočítat:

$$\Delta_{q_t} = \dot{q}_t = reg(q_t, 2)$$
$$\Delta\Delta_{q_t} = \dot{\Delta}_t = reg(\Delta_t, 2)$$

Použití modelů

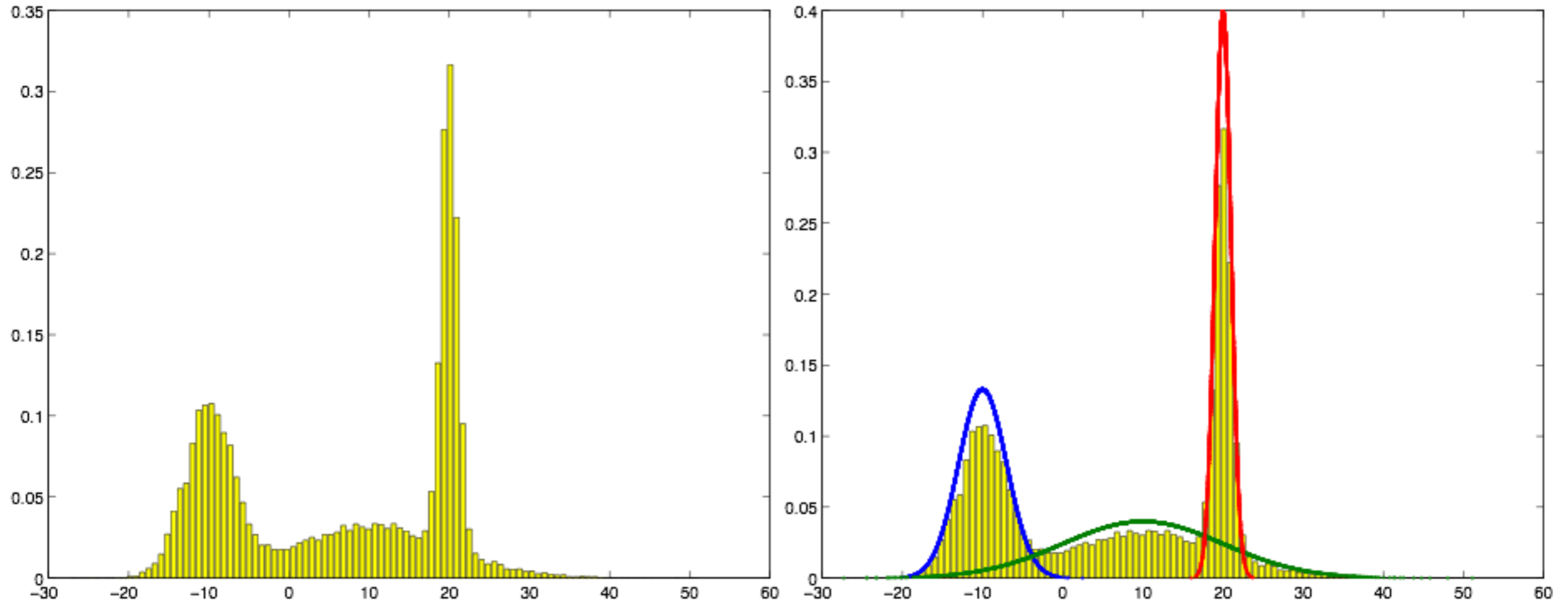
- ▶ **Deterministické metody**
 - **Dynamic Time Warping (DTW)**
 - **Vector Quantization (VQ)**
- ▶ **Statistické metody**
 - **Gaussian Mixture Model (GMM)**
 - **Hidden Markov Model (HMM)**

Gaussian (Mixture Model)



$$f(x) = \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{(x-\mu)^2}{2\sigma^2}}$$

Gaussian Mixture Model



Gaussian Mixture Model

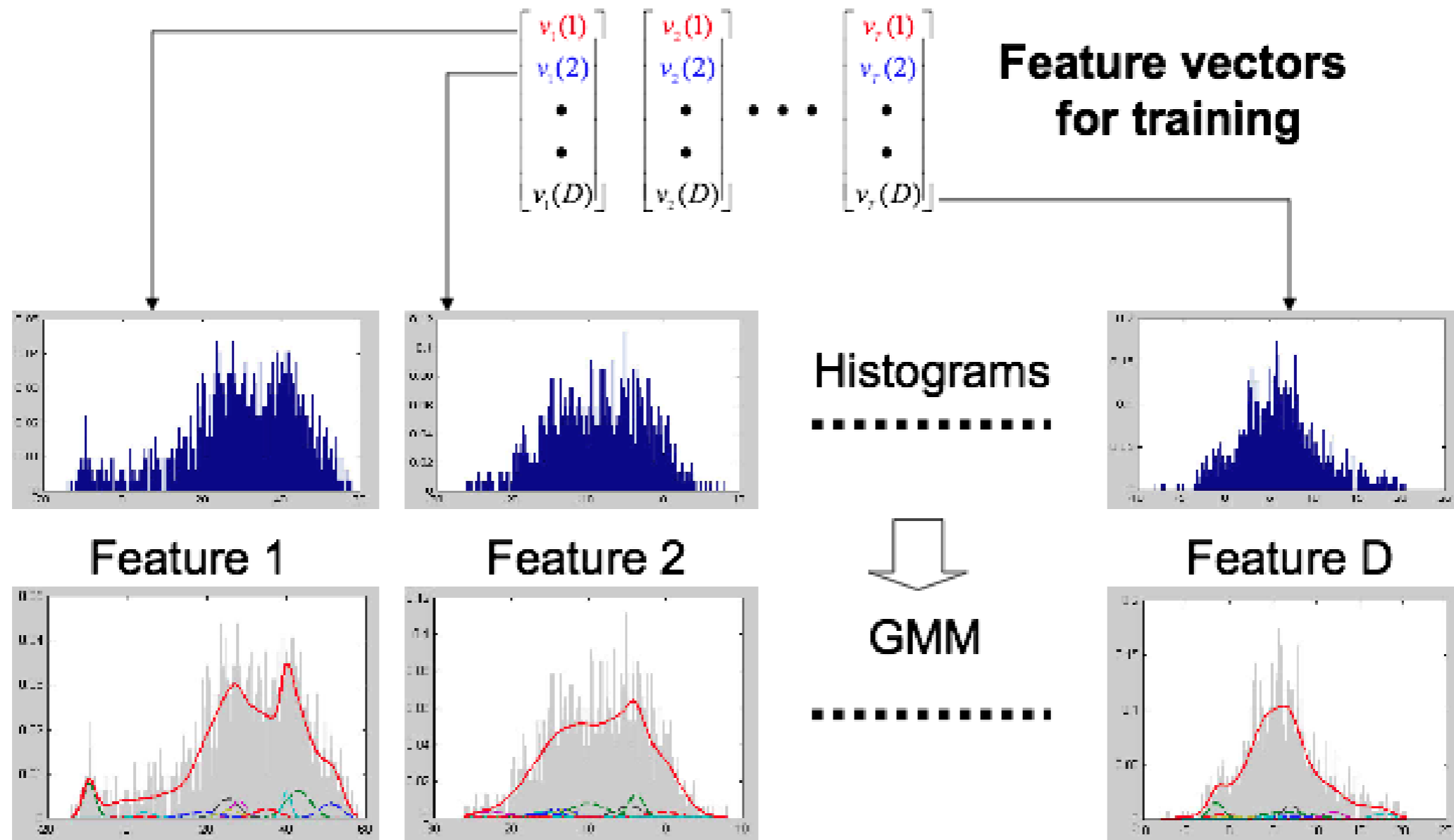
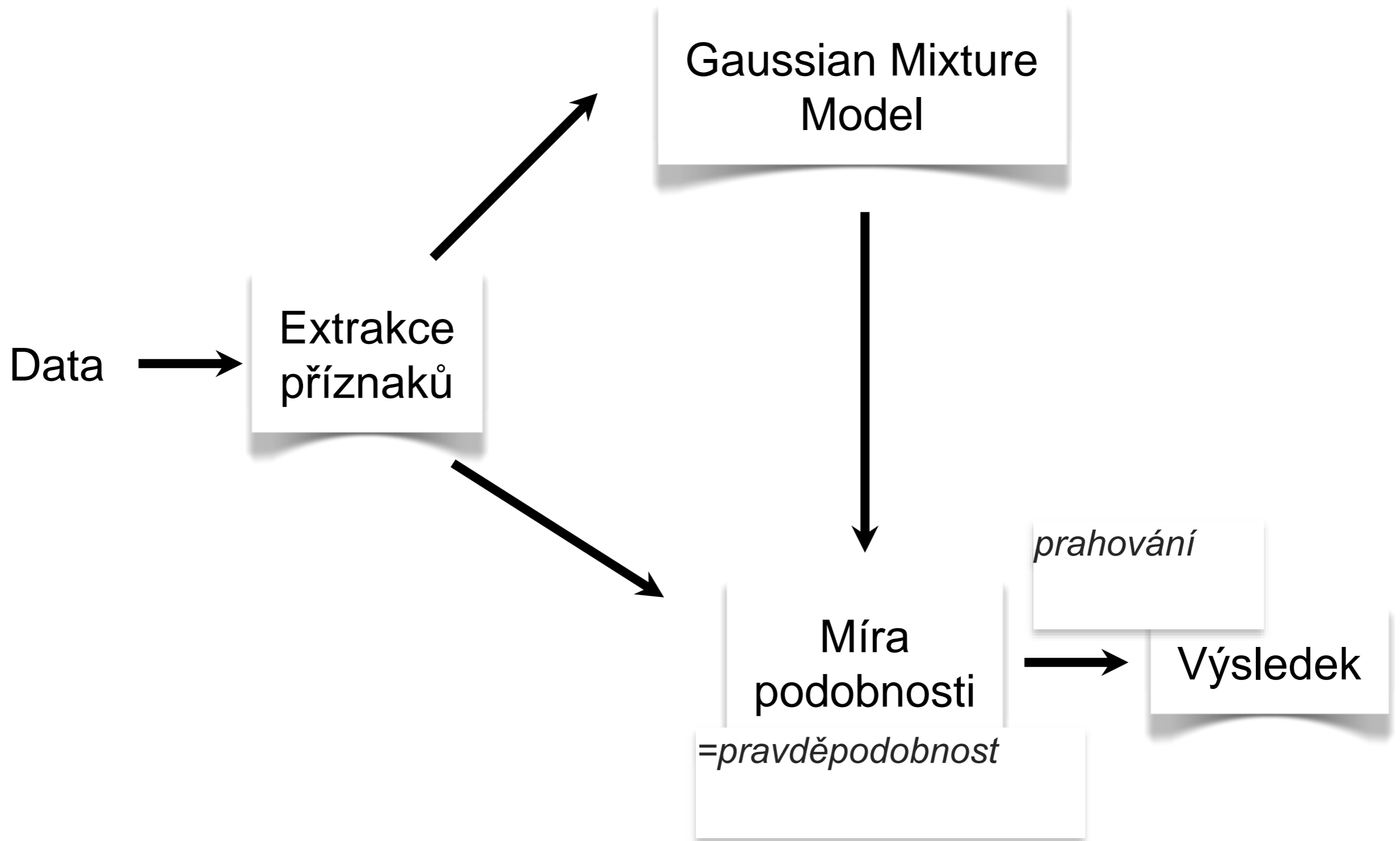


Schéma rozpoznání podpisu GMM



Metody rozpoznávání

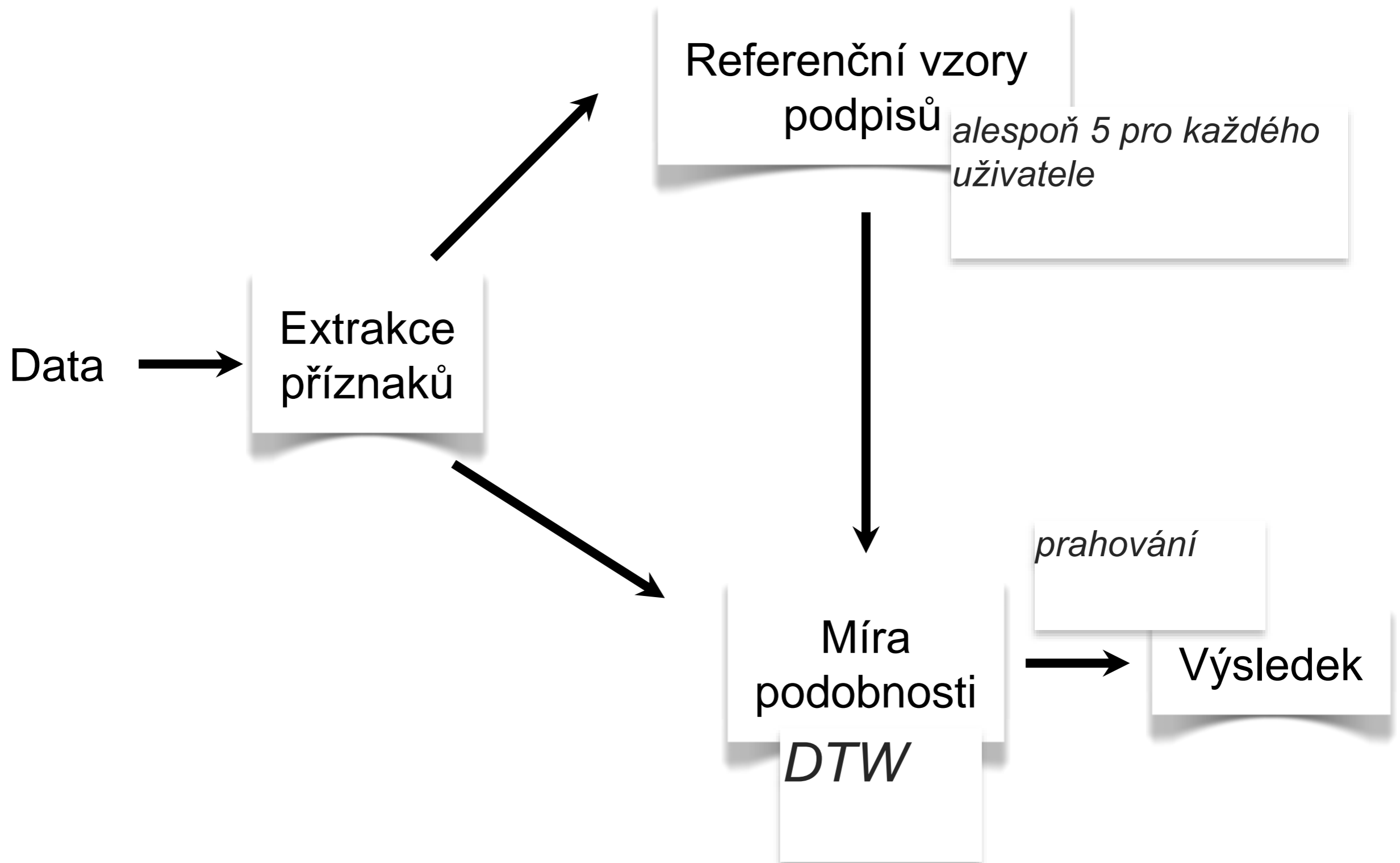
▶ Deterministické metody

- **Dynamic Time Warping (DTW)**
- **Vector Quantization (VQ)**

▶ Statistické metody

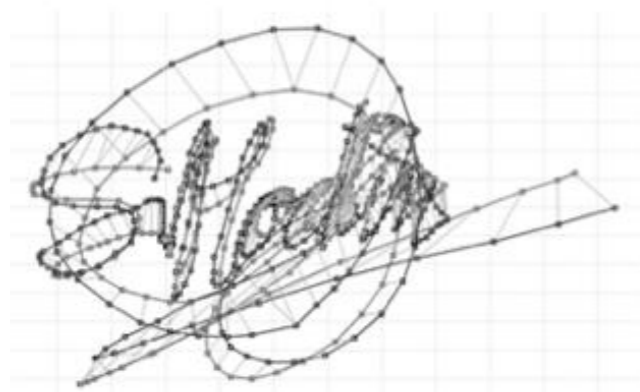
- **Gaussian Mixture Model (GMM)**
- **Hidden Markov Model (HMM)**

Schéma rozpoznání podpisu DTW

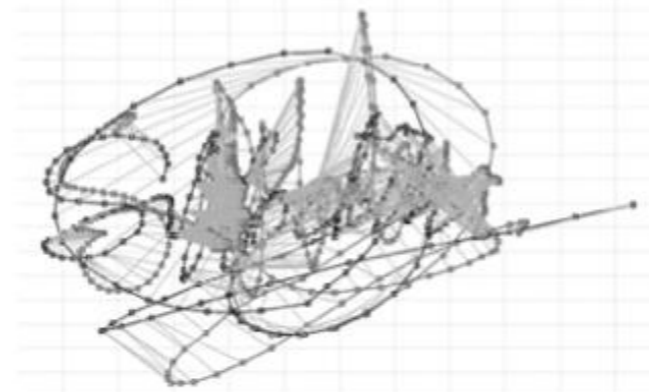


Rozpoznání podpisu

► Dynamic Time Warping



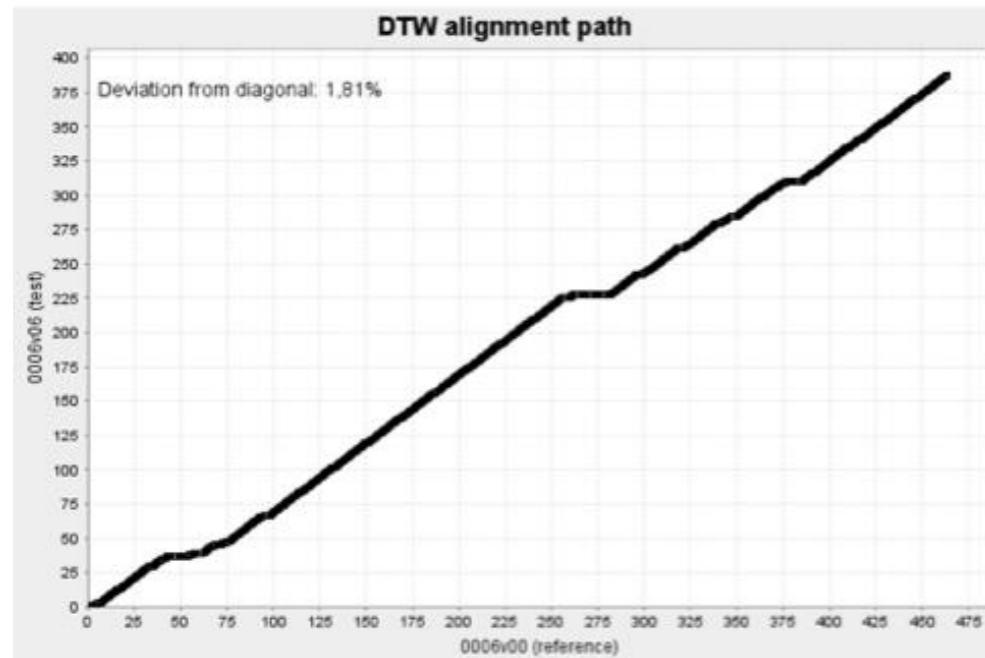
(a) Genuine-genuine



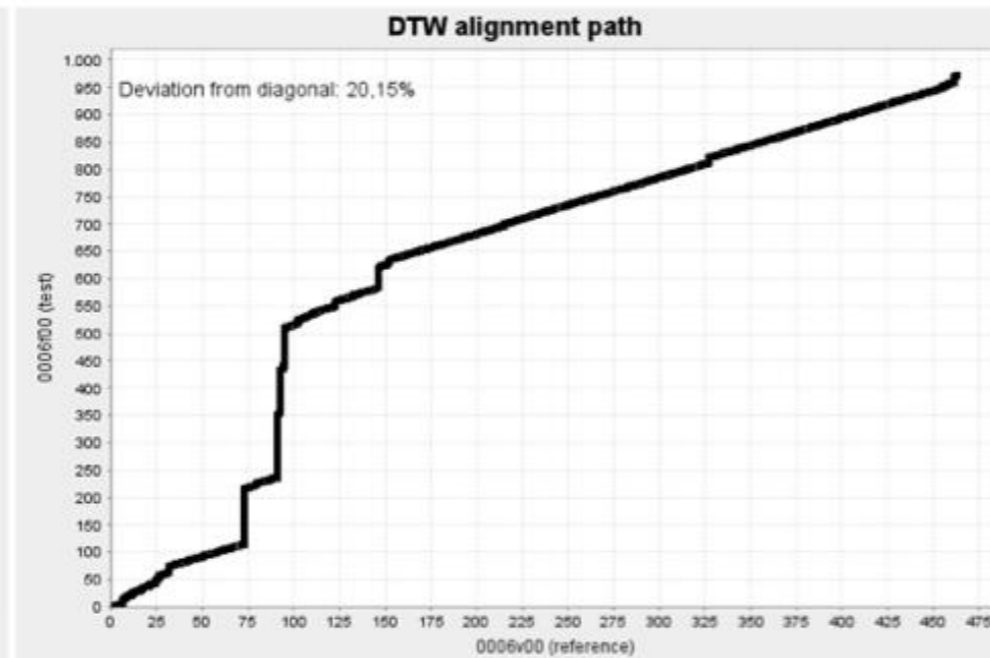
(b) Genuine-forgery



(c) Intra-class variability

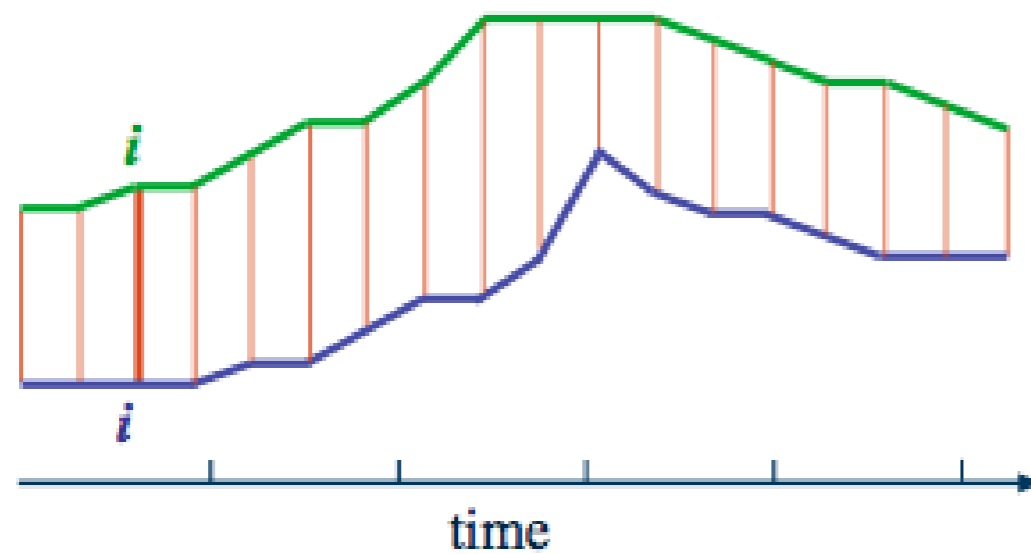


(d) Gen-Gen DTW path

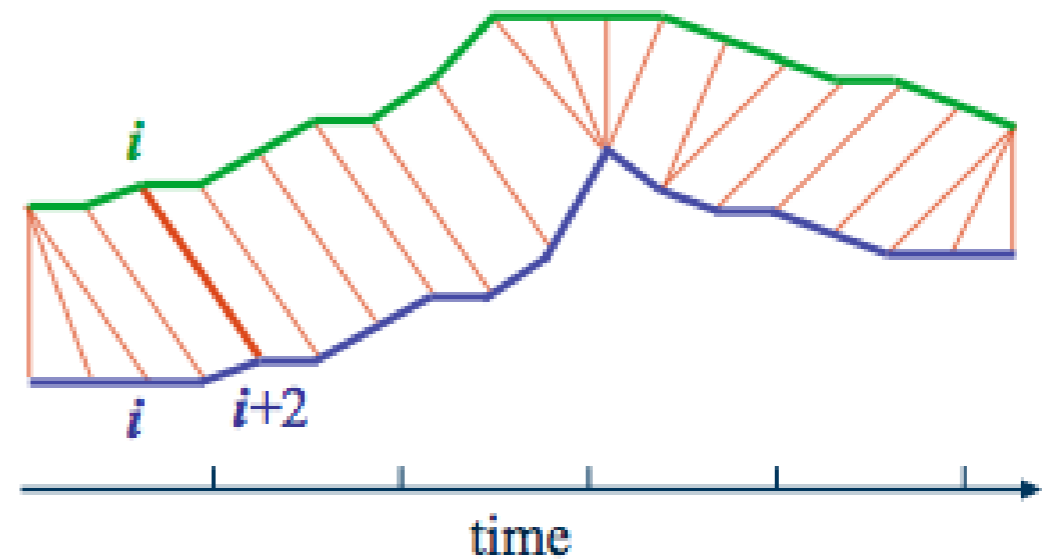


(e) Gen-Forg DTW path

Proč DTW?

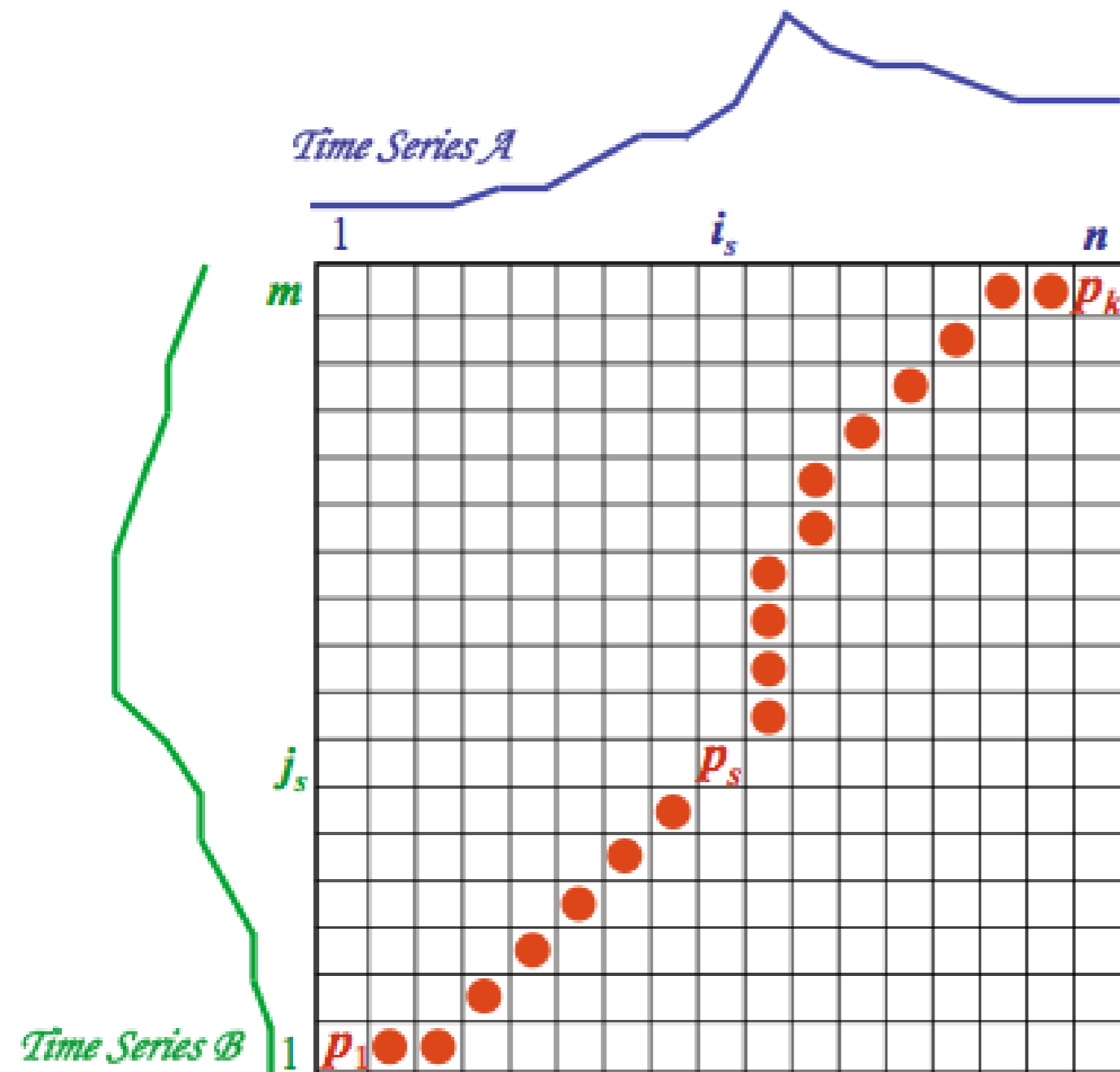


Porovnání *křivek*
(*standardně*)



Porovnání *křivek*
(*DTW*)

Warpovací funkce

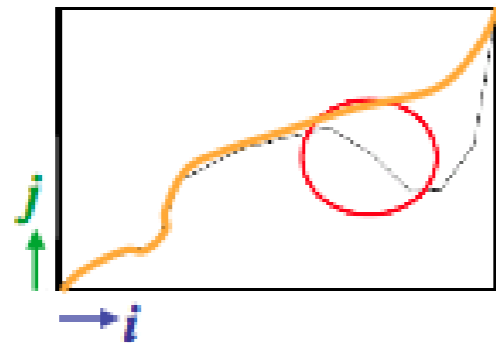


- ▶ mřížka ukazuje vzdálenost (podobnost) jednotlivých bodů (n -rozměrných) křivek
- ▶ snaha o nalezení minimální cesty z $[0,0]$ do $[n,m]$
- ▶ řeší dynamické programování

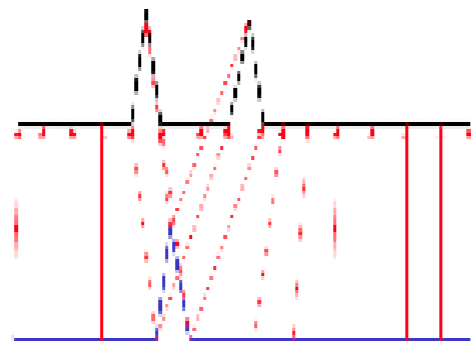
Omezení warpovací funkce

Monotonicity: $i_{s-1} \leq i_s$ and $j_{s-1} \leq j_s$.

The alignment path does not go back in “time” index.

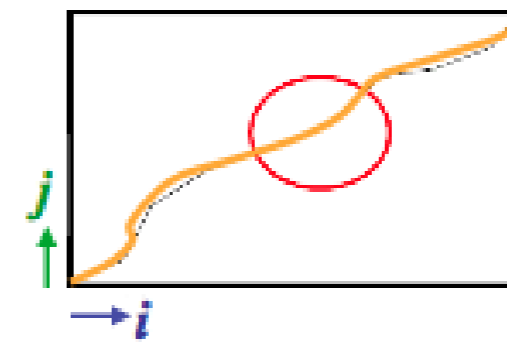


Guarantees that features are not repeated in the alignment.

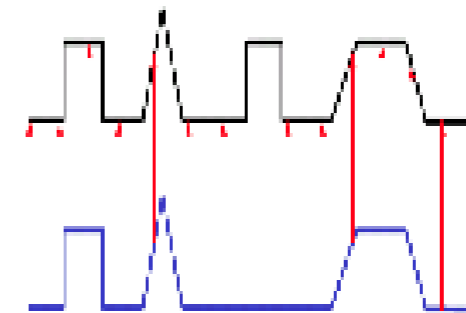


Continuity: $i_s - i_{s-1} \leq 1$ and $j_s - j_{s-1} \leq 1$.

The alignment path does not jump in “time” index.



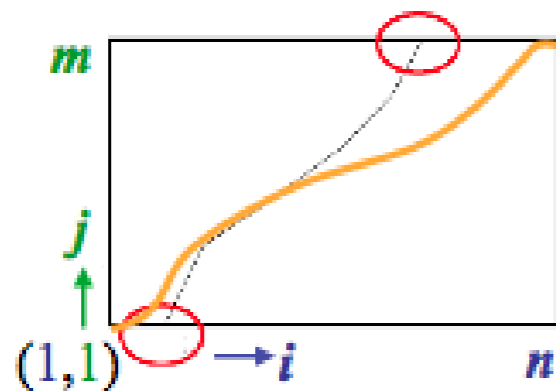
Guarantees that the alignment does not omit important features.



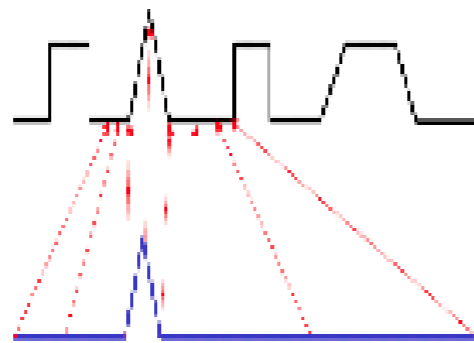
Omezení warpovací funkce

Boundary Conditions: $i_1 = 1, i_k = n$ and $j_1 = 1, j_k = m$.

The alignment path starts at the bottom left and ends at the top right.

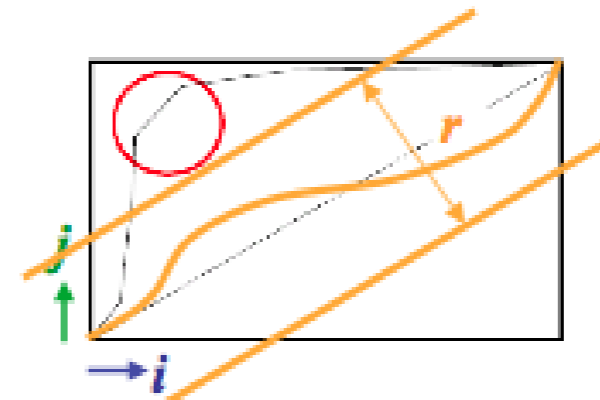


Guarantees that the alignment does not consider partially one of the sequences.

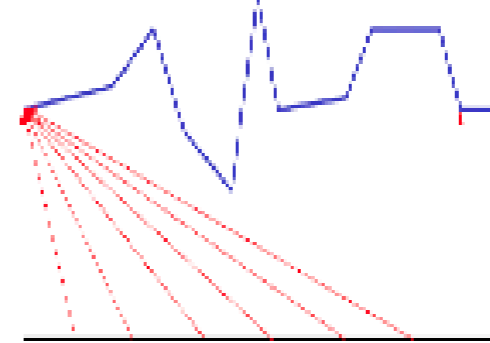


Warping Window: $|i_s - j_s| \leq r$, where $r > 0$ is the window length.

A good alignment path is unlikely to wander too far from the diagonal.



Guarantees that the alignment does not try to skip different features and gets stuck at similar features.



Databáze podpisů

Dataset	Database	Users	Signatures		Total
			Genuines	Forgeries	
DD	MCYT-A	50	25	25	2500
TD	MCYT-B	50	25	25	2500
	SVC2004	40	20	20	1600
	BIOMET	84	15	17	2688
	MYIDEA	69	18	36	3726
Total		293	5802	7212	13014

Výsledky

	Random forgery	Skilled forgery
EER	0.41%	2.26%

EER = Equal error rate

udává chybovost (jak chybného přijetí podpisu za pravý, tak i chybného zamítnutí pravého podpisu)

Výhody x nevýhody podpisu

- ▶ Ochrana proti padělání
- ▶ Používá zavedené procesy
- ▶ Neinvazivní
- ▶ Uživatelé mohou změnit podpis
- ▶ Nekonzistentní podepisování vede ke zvýšení chybovosti
- ▶ Uživatelé nejsou zvyklí podepisovat tablet
- ▶ Počet možných aplikací je omezen
- ▶ Uživatelé mohou změnit podpis

Výhody

- ▶ **Podpis je vytvořen lidmi a padělání (ochrana) je dobře prozkoumané**
- ▶ **Natrénování podpisu je rychlé a intuitivní**
- ▶ **Verifikace podpisu je rychlá nemá vysoké požadavky na úložný prostor**

Nevýhody

- ▶ **Používá se v podstatě jenom pro autentizaci dokumentů**
- ▶ **Pero s náklonem a natočením je drahé**
- ▶ **Komplikace u handicapovaných lidí a lidí, s nedostatečnou motorickou koordinací**

“Obyčejný” tablet

▶ **Genius EasyPen i405X ~ 900Kč**

- 2540 lpi
- 1024 úrovní přítlačku
- 125 bodů/s



▶ **Wacom Intuos Pro S A6 ~ 5000Kč**

- 5080 lpi
- 2048 úrovní přítlačku
- 200 bodů/s



“Biometrický” tablet

▶ **Wacom STU-530 LCD Signature ~ 9 000Kč**

- **LCD**
- **2540 lpi**
- **1024 úrovní přítlačku**
- **200 bodů/s**
- **náklon i natočení (grip pen)**



Děkuji za pozornost