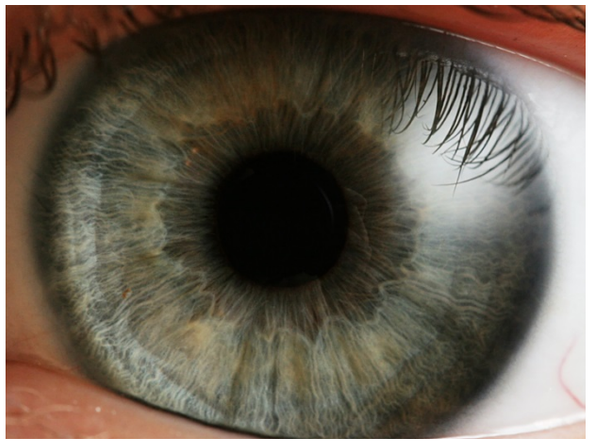
Dynamický podpis

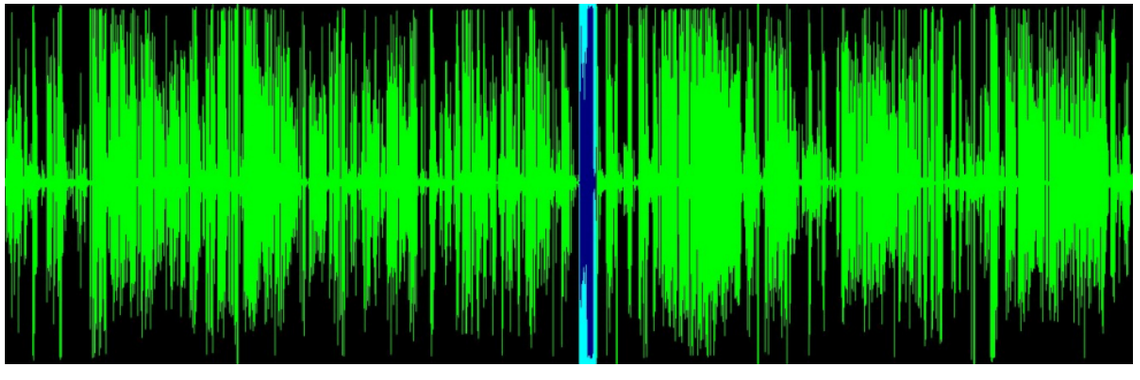
vycházející z přednášek **Dr. Andrzej Drygajlo,** http://scgwww.epfl.ch/courses/

Biometrické charakteristiky

- **Biologické**
  - **DNA, krev, sliny**
- **Biologické/Fyziologické**
  - **otisk prstu, zornice, tvář, sítnice**
- **Chování**
  - **podpis, chůze, psaní na klávesnici**
- **Složené**
  - **Řeč**

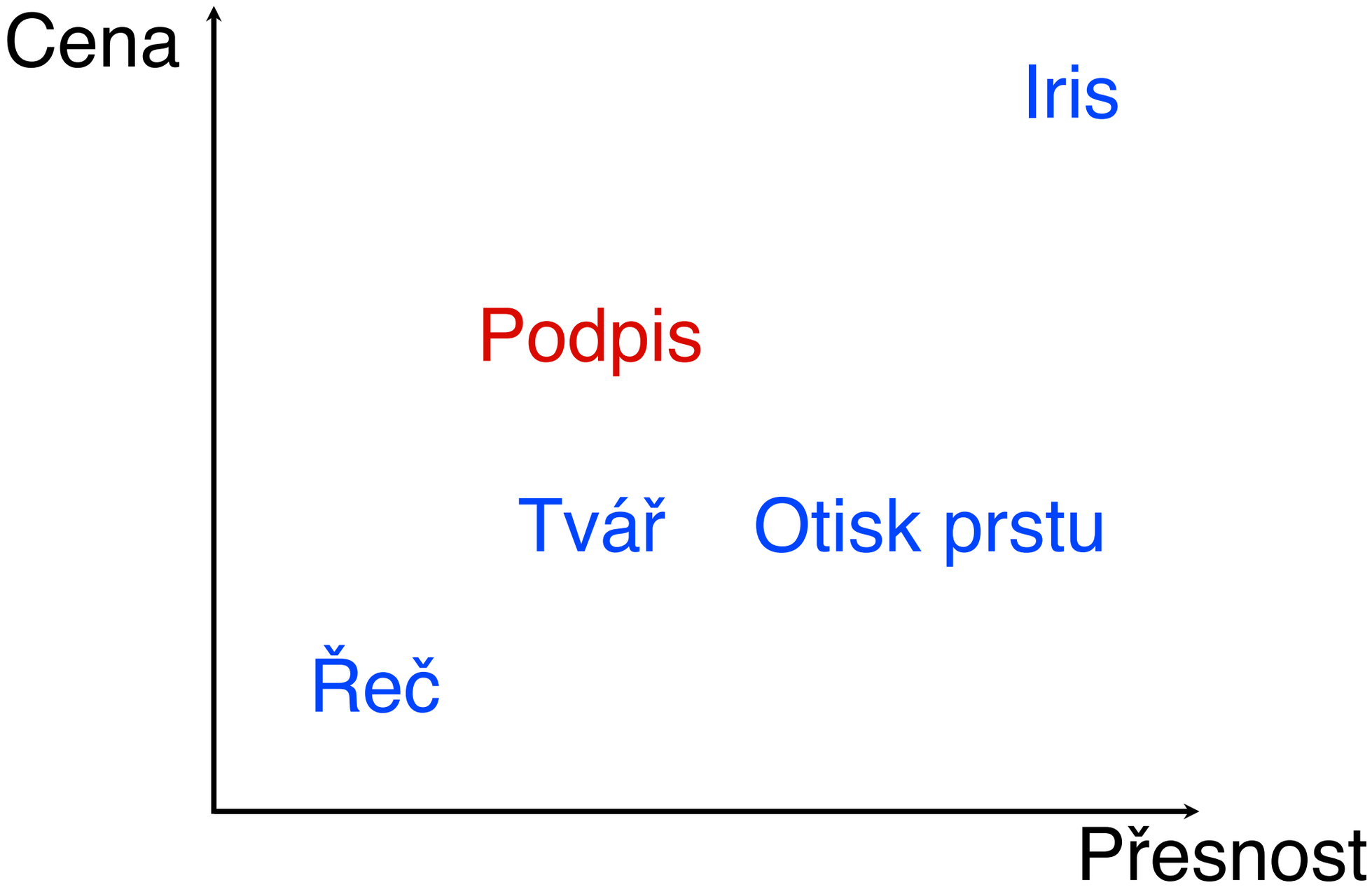
Různorodost charakteristik





Barack Obama

Porovnání charakteristik



Podpis

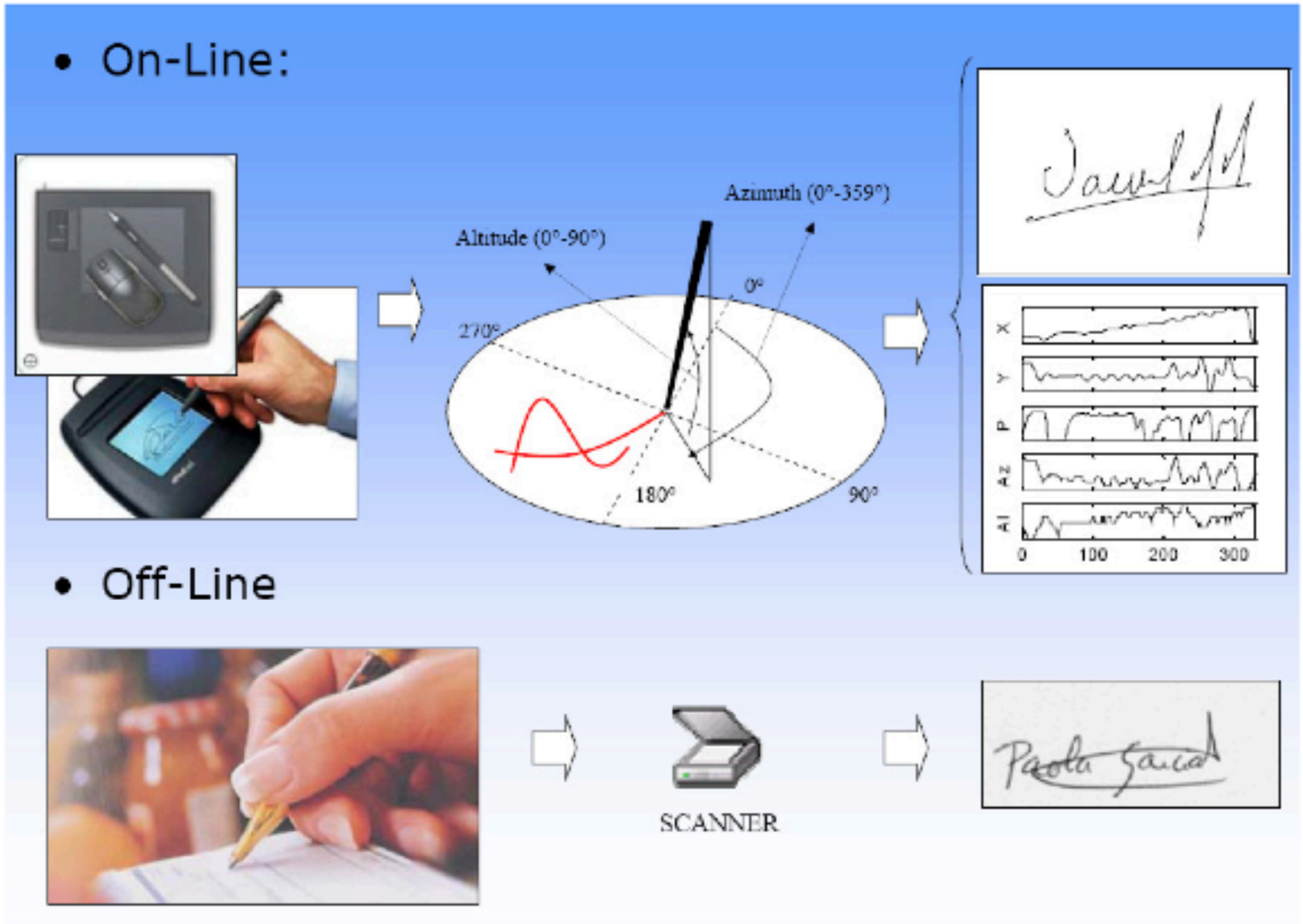
Statický

Dynamický

Podpis

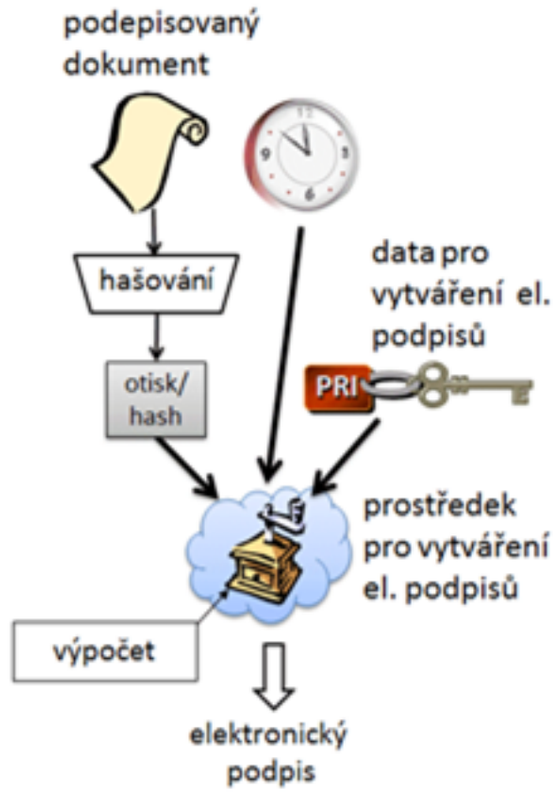
- **statický (offline)**
  - **běžný podpis naskenovaný z dokumentu**
- **dynamický (online)**
  - **podpis získaný pomocí tabletu, obsahující dynamické informace o *x,y,z* pozici pera v čase (případně další) ve vyšším rozlišení**
- **elektronický**
  - **Elektronický údaj (číslo), který slouží k ověření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

Podpisy - porovnání



Elektronický podpis (zaručený)

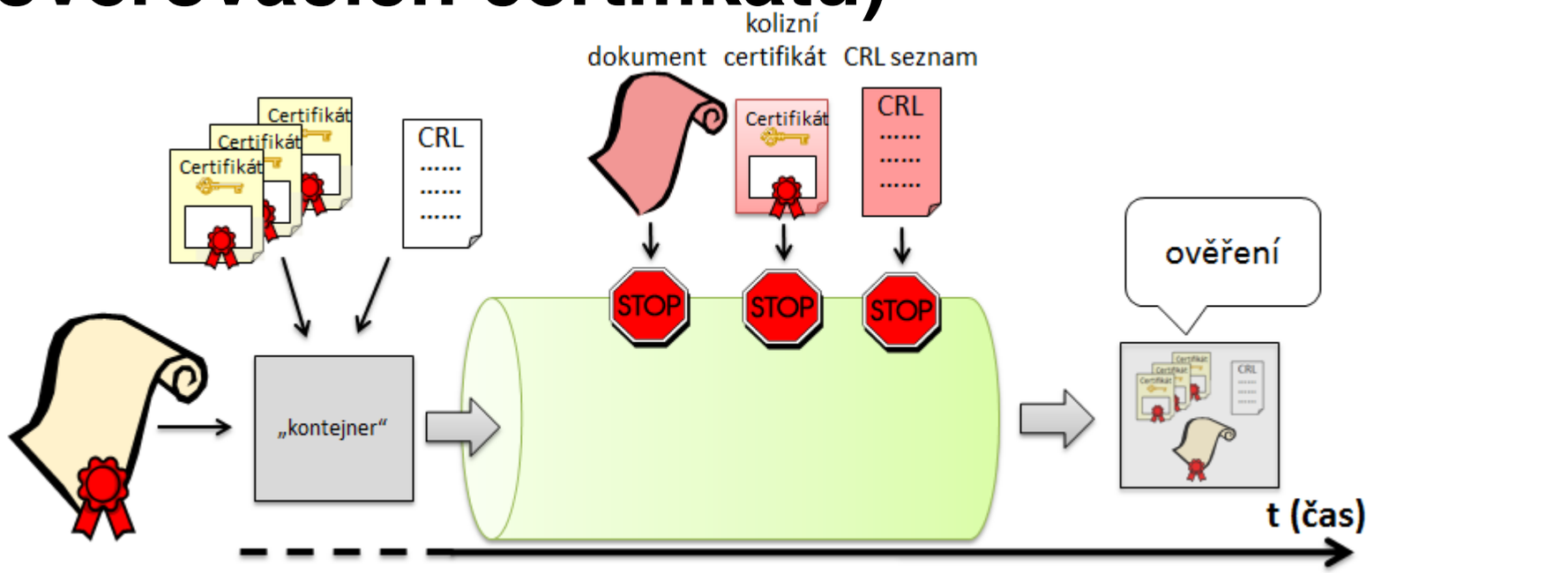
- **Princip**
  - **Asymetrické kryptografie**
  - **Uživatel - privátní klíč (data)**
  - **Organizace zajišťující potvrzení veřejného klíče (certifikát)**



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

Problematika El. podpisu

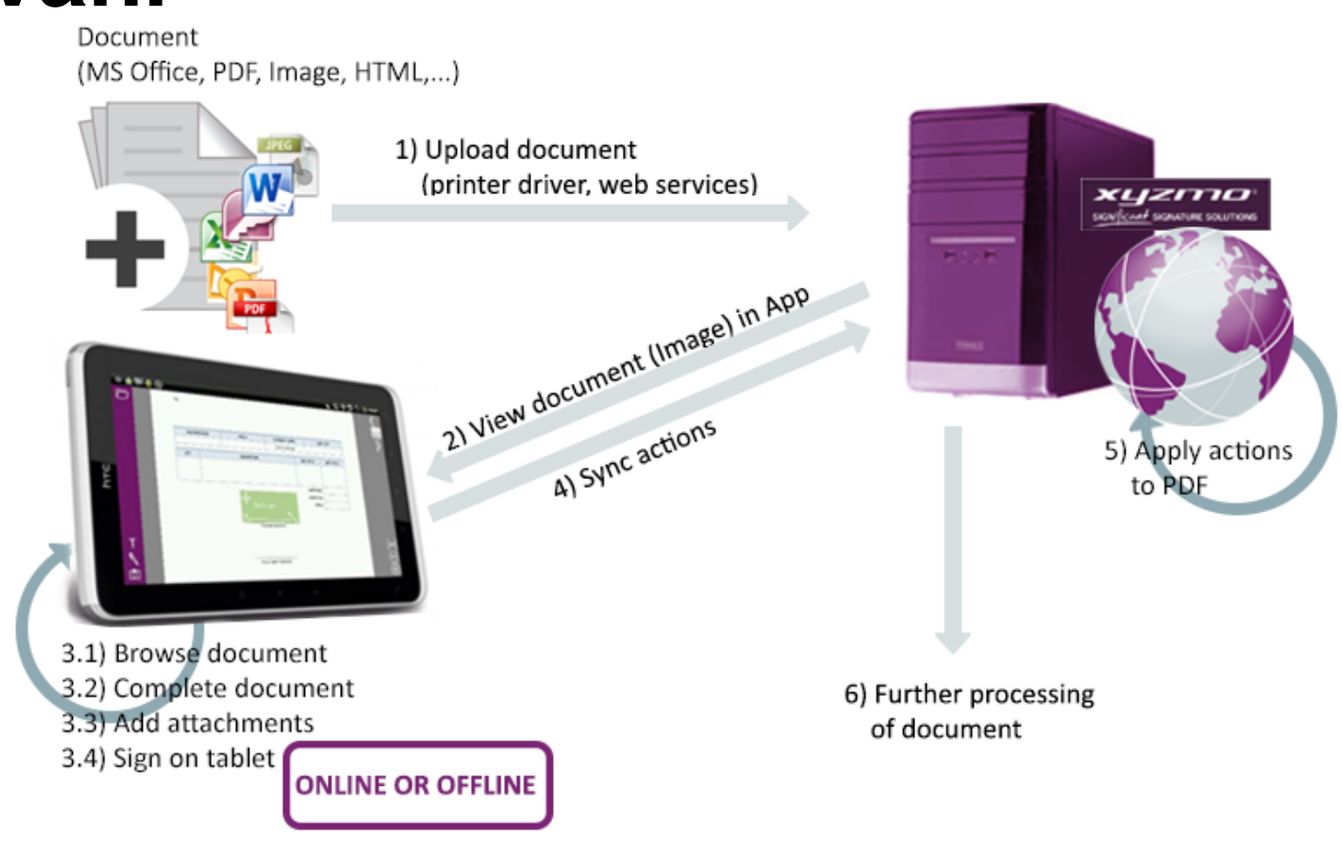
- **Datové schránky – povinný přechod k EP**
- **Dlouhodobé uchovávání záznamu – dohledatelnost certifikátů**
- **Řešení**
  - **Long Term Validation (přiřazení ověřovacích certifikátů)**



http://www.bajecnysvet.cz/obsah/4x10x3.php

Elektronický a dynamický podpis

- **Není úlpně 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**
- **Česká legislativa**
  - **zákon 227/2000 Sb o elektronickém podpisu**

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**
  - **Forenzní analýza**

Podpis v dokladech

INFORMACE PRO OBČANY ČESKÉ REPUBLIKY

NOVÝ CESTOVNÍ PAS SE DVĚMA BIOMETRICKÝMI ÚDAJI

V nosiči dat pasu, který se bude vydávat od 1. dubna 2009, budou uloženy dva biometrické údaje.

3. biom. údaj

Od 1. dubna 2009 se budou vydávat cestovní pasy se strojově čitelnými údaji a s nosičem dat s biometrickými údaji obsahujícím dva biometrické údaje.

IKEA - elektronická účtenka

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

Area: Business Solutions » Electronic Signatures
Location: Europe

STU-500 S

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 electronical 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 if using paper.

Přístroje


RightSignature
Sign Document
Submit Signature


FUJITSU


wacom
wacom
wacom

DIAD = super PDA

Delivery Information Acquisition Device

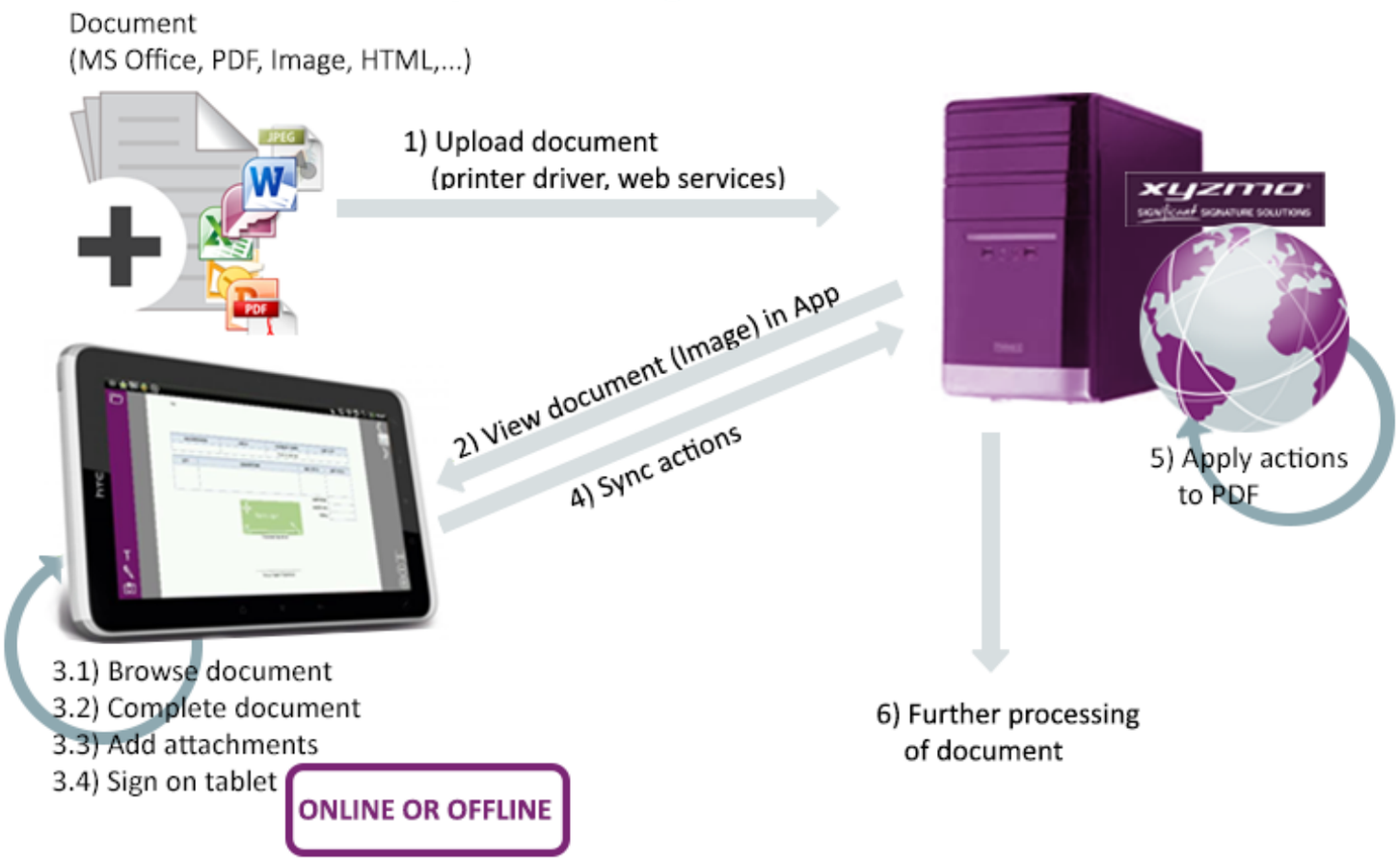
- WiFi
- Bluetooth
- GPRS/CDMA
- dialup modem
- GPS
- infra-red scanner

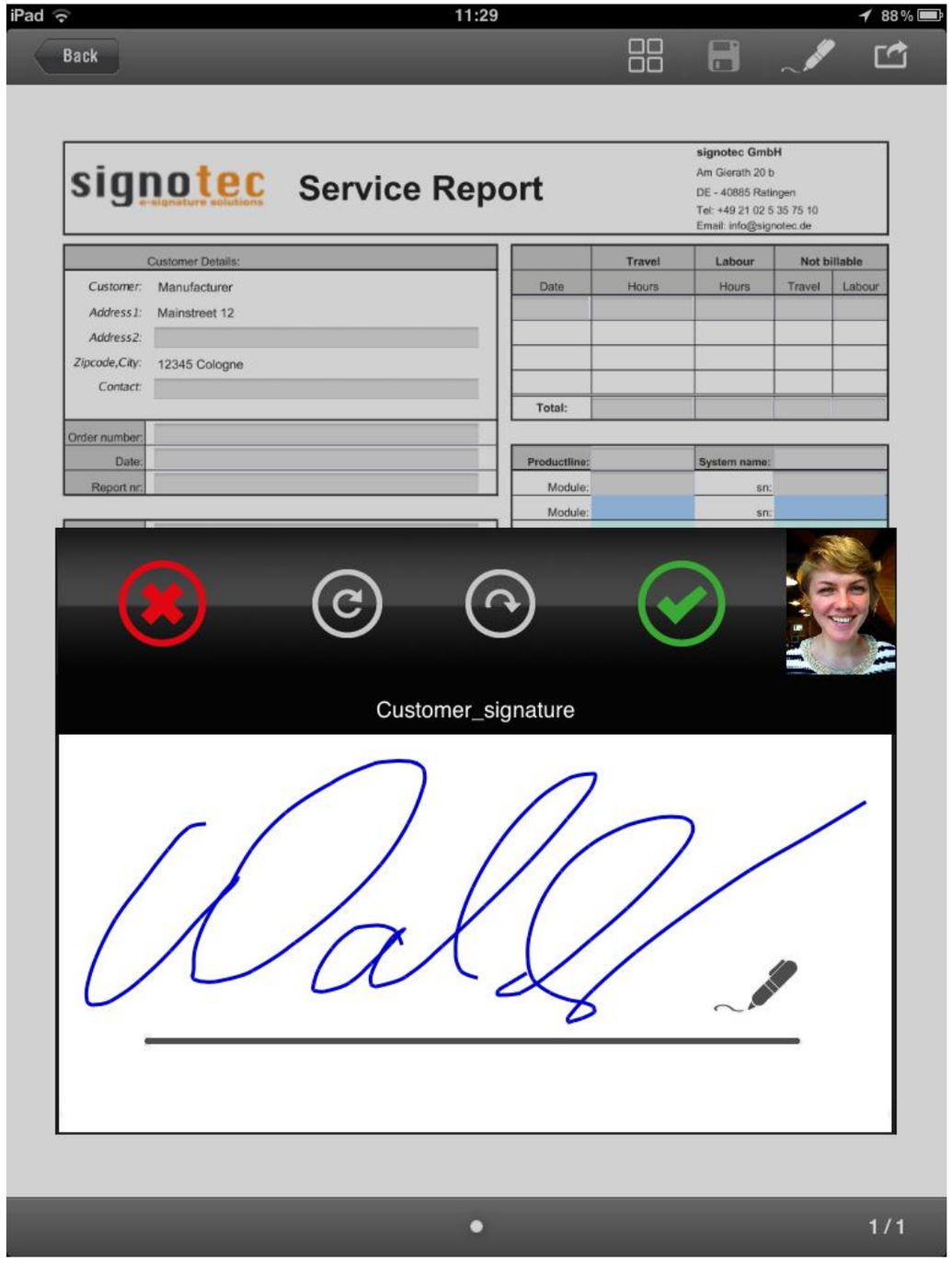
Společnosti - odkazy

- **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

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





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**

http://www.wired.com/politics/security/news/2004/08/64463

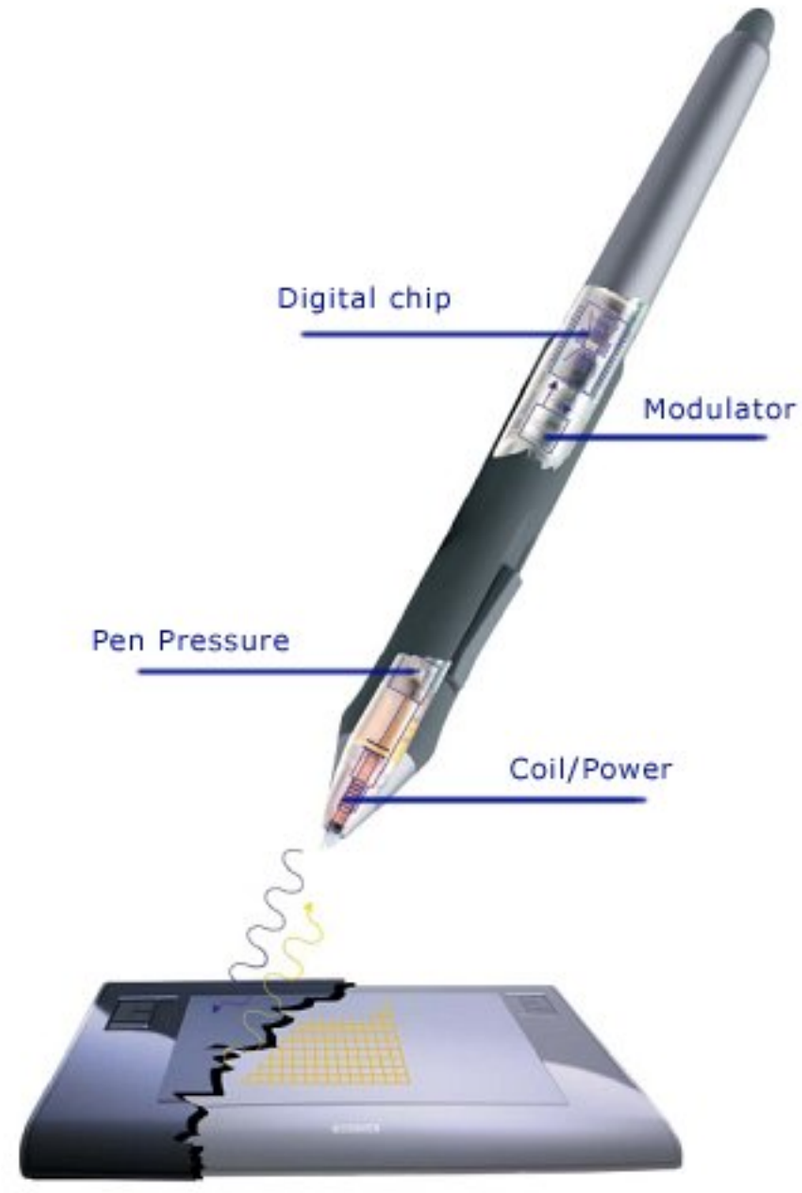
Na trhu – s přítlakem

- Wacom Intuos Creative Stylus (100 $)
  - http://intuoscreativestylus.wacom.com/en/
- Pogo Connect
  - http://www.tenonedesign.com/connect.php
- Jaja Hex3
  - http://www.hex3.co/products/jaja
- Jot Touch (90 $)
  - http://adonit.net/jot/touch/

Tablet

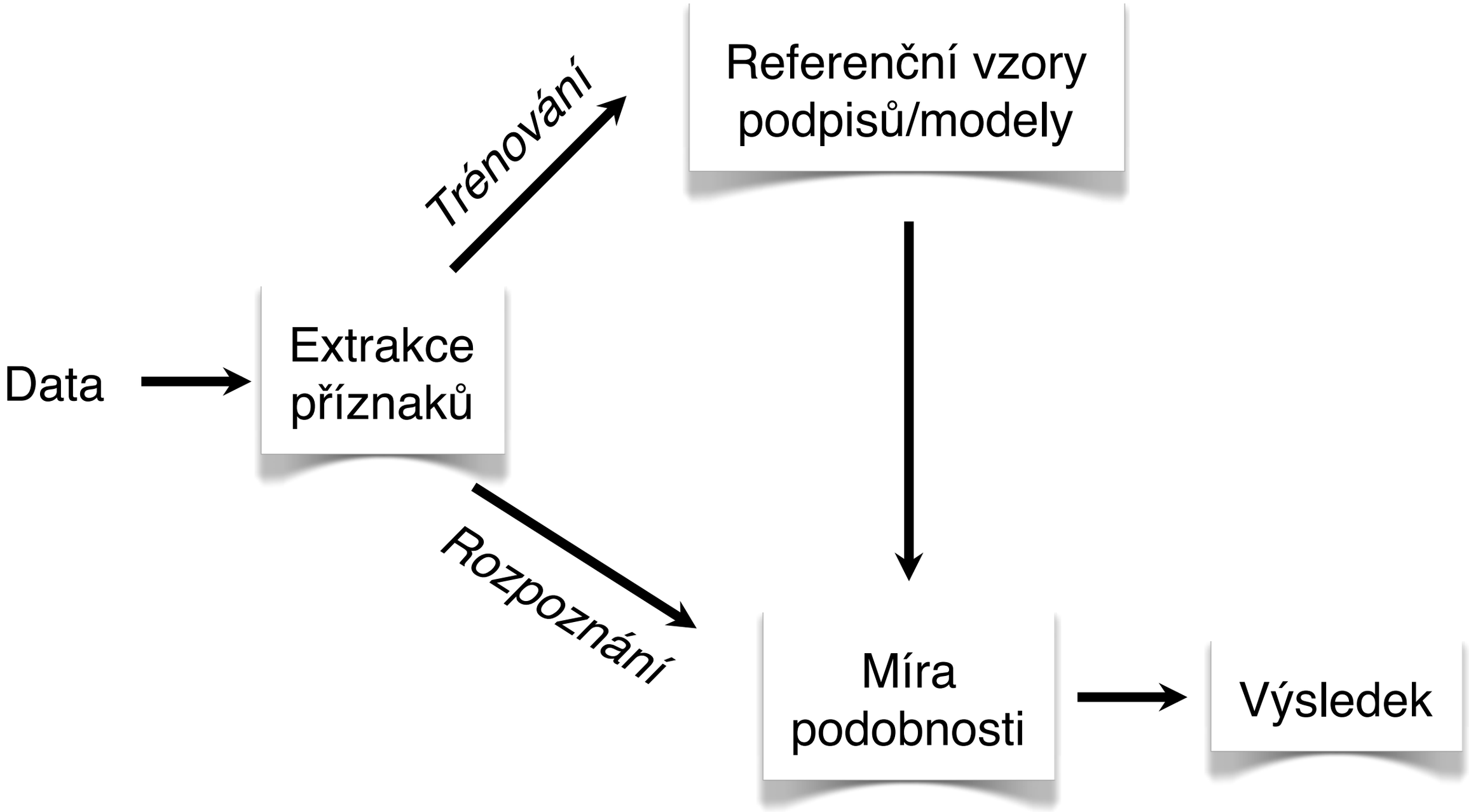
Jak funguje grafický tablet

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

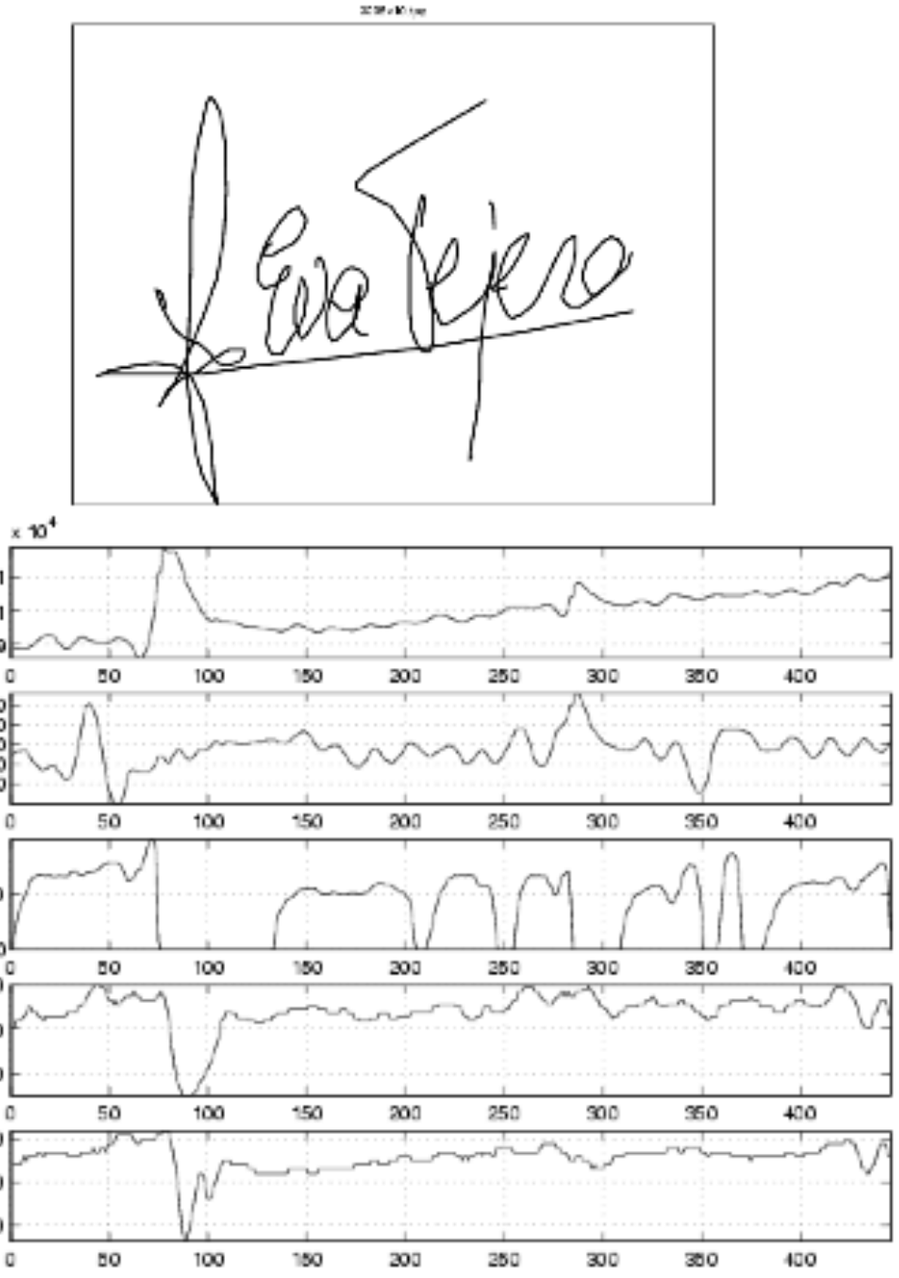


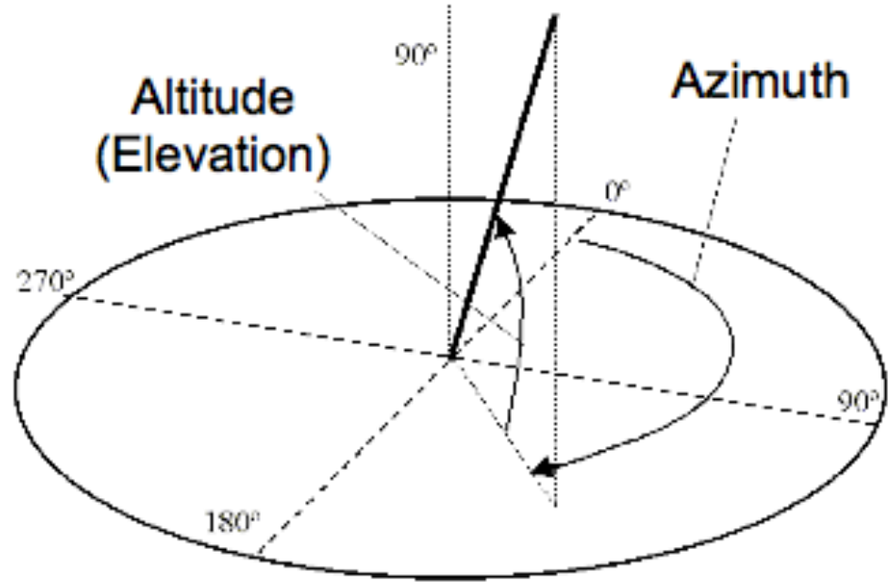
http://www.tablet4u.co.uk/techinfo.html

Rozpoznání podpisu



Dynamický podpis



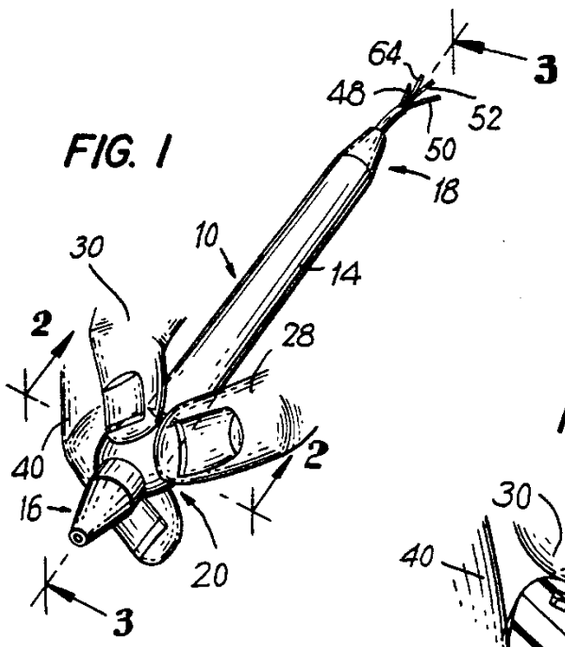


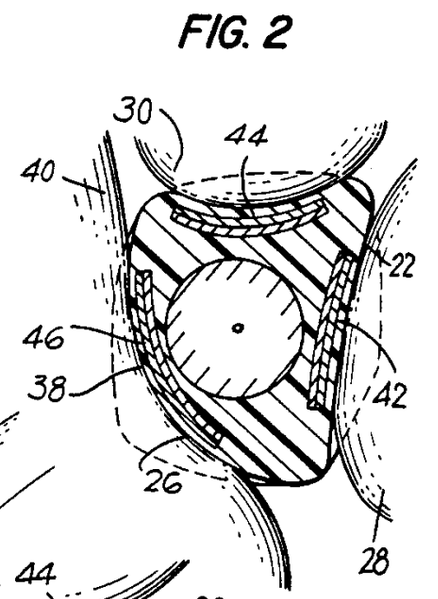
Příznaky:

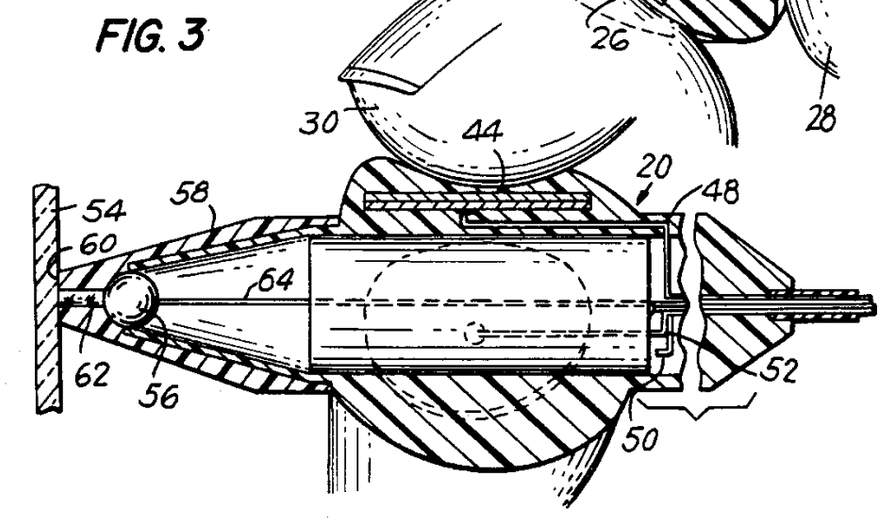
- souřadnice X
- souřadnice Y
- přítlak
- natočení pera (0º-359º)
- náklon pera (0º-90º)

Další příznak - Stisk

- **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…**







http://www.google.vu/patents/US5018208

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

  4. kvalitní padělek: **kombinace (2) a (3)**

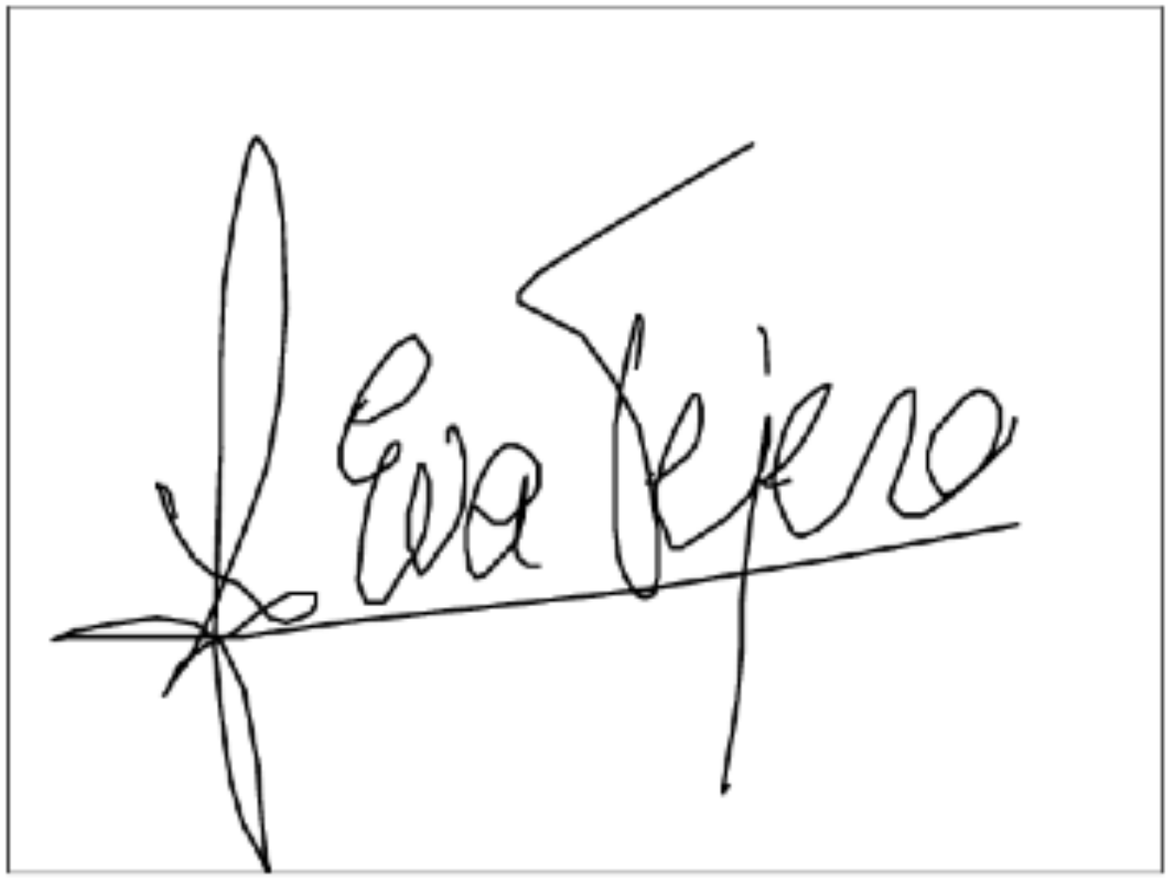
Padělky

Originál

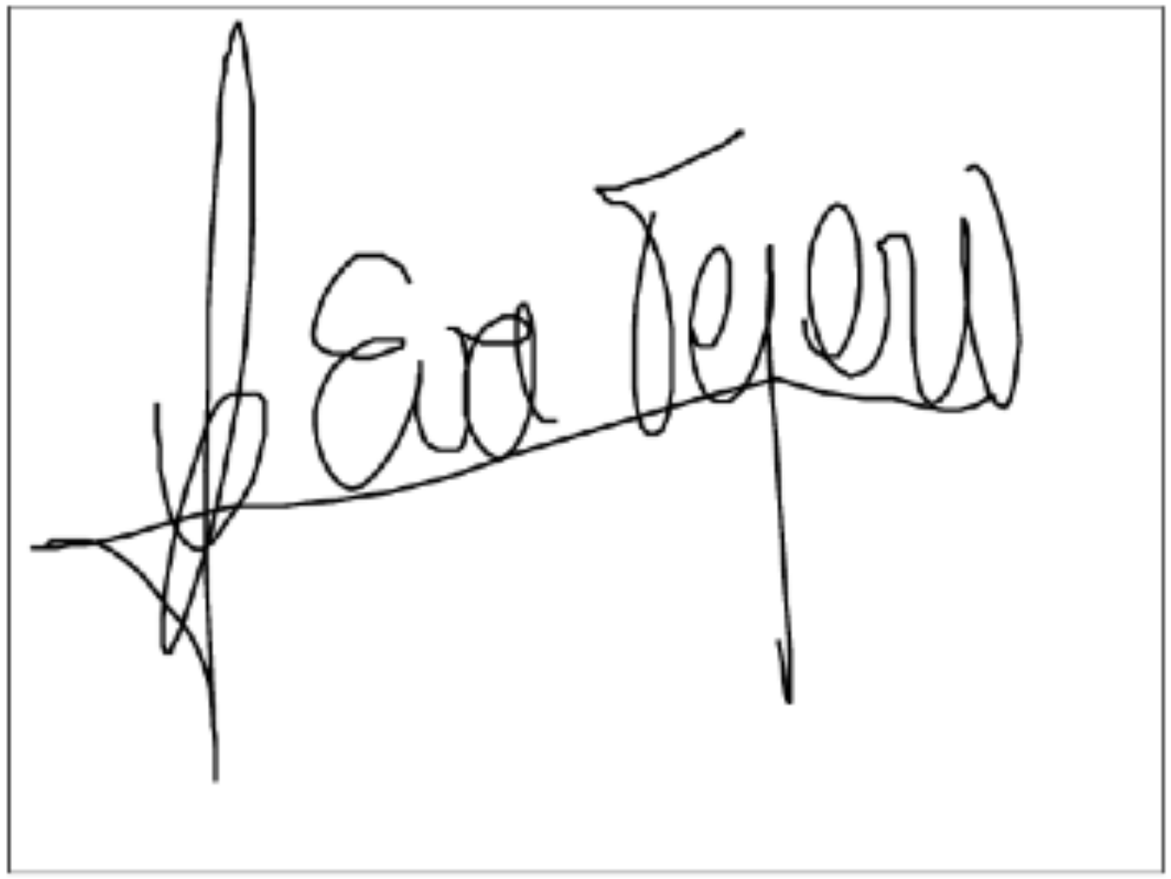
(3) Padělek ze sledování

(2) Padělek z předlohy

Originál a kvalitní padělek

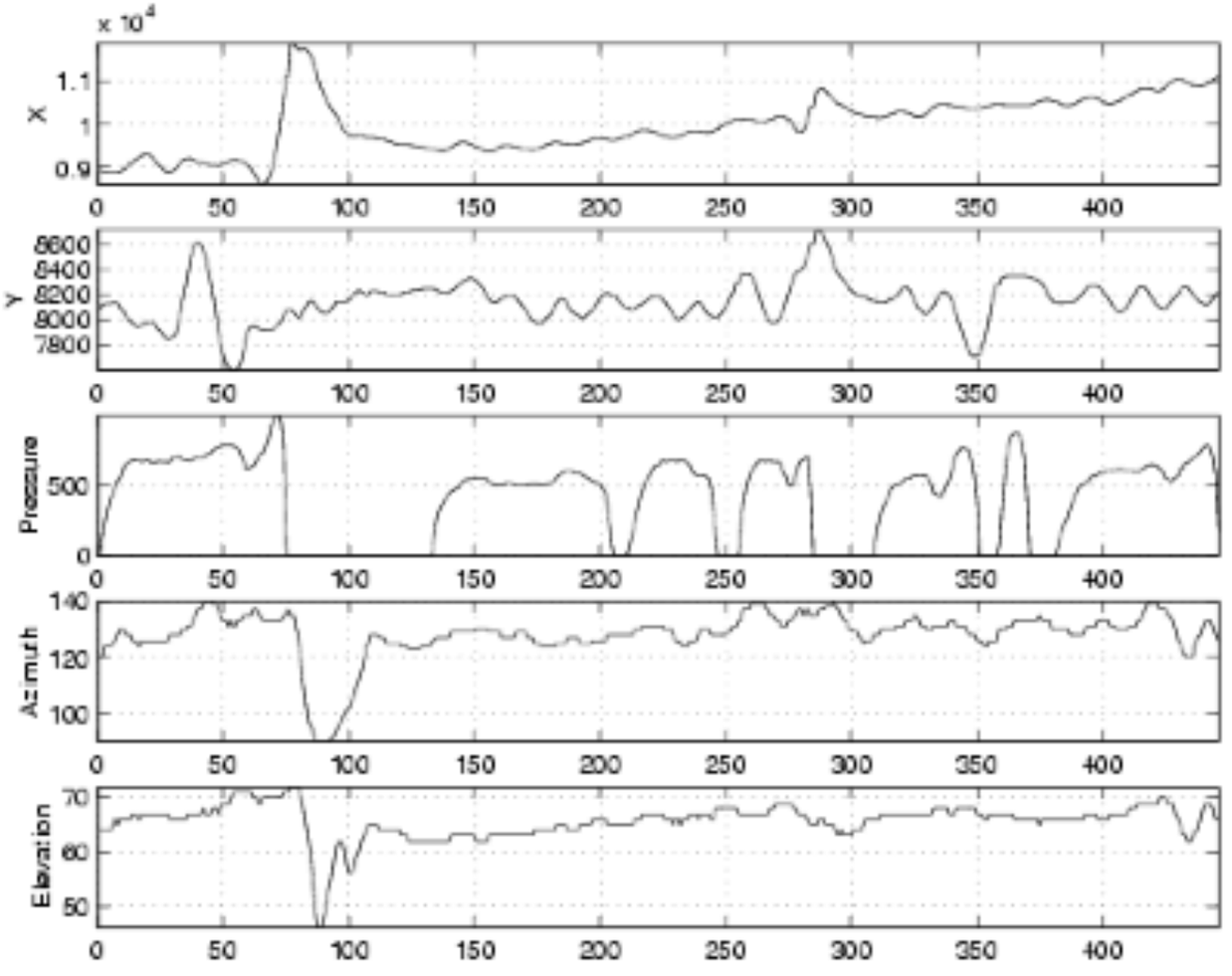


Originál

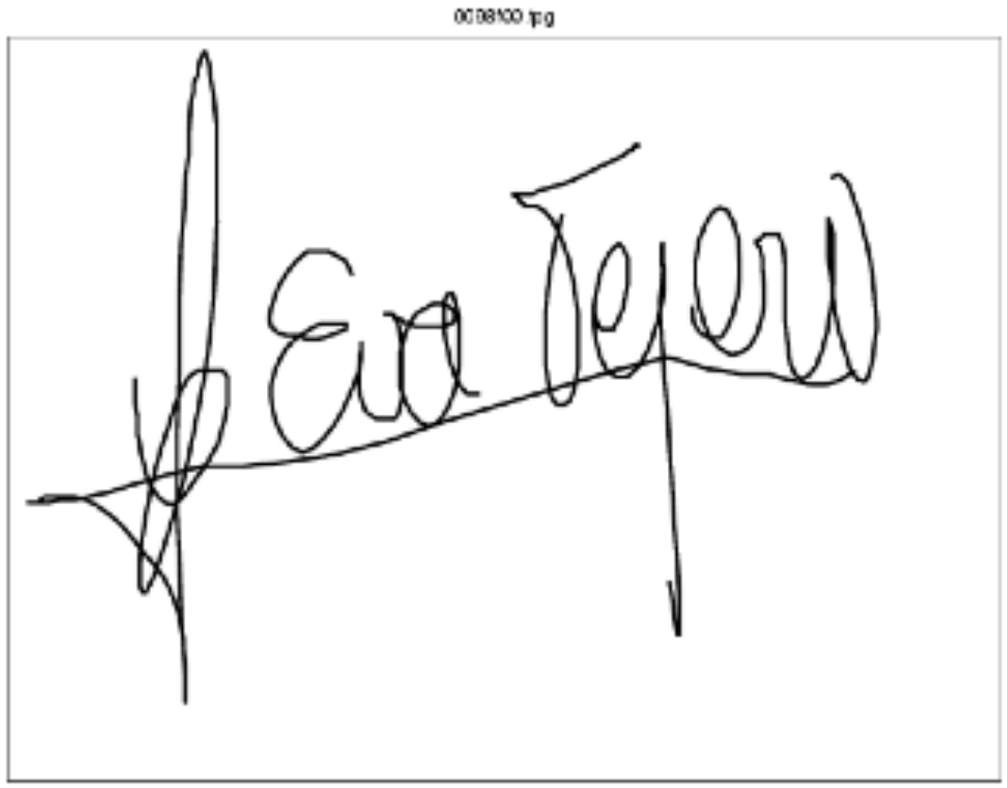


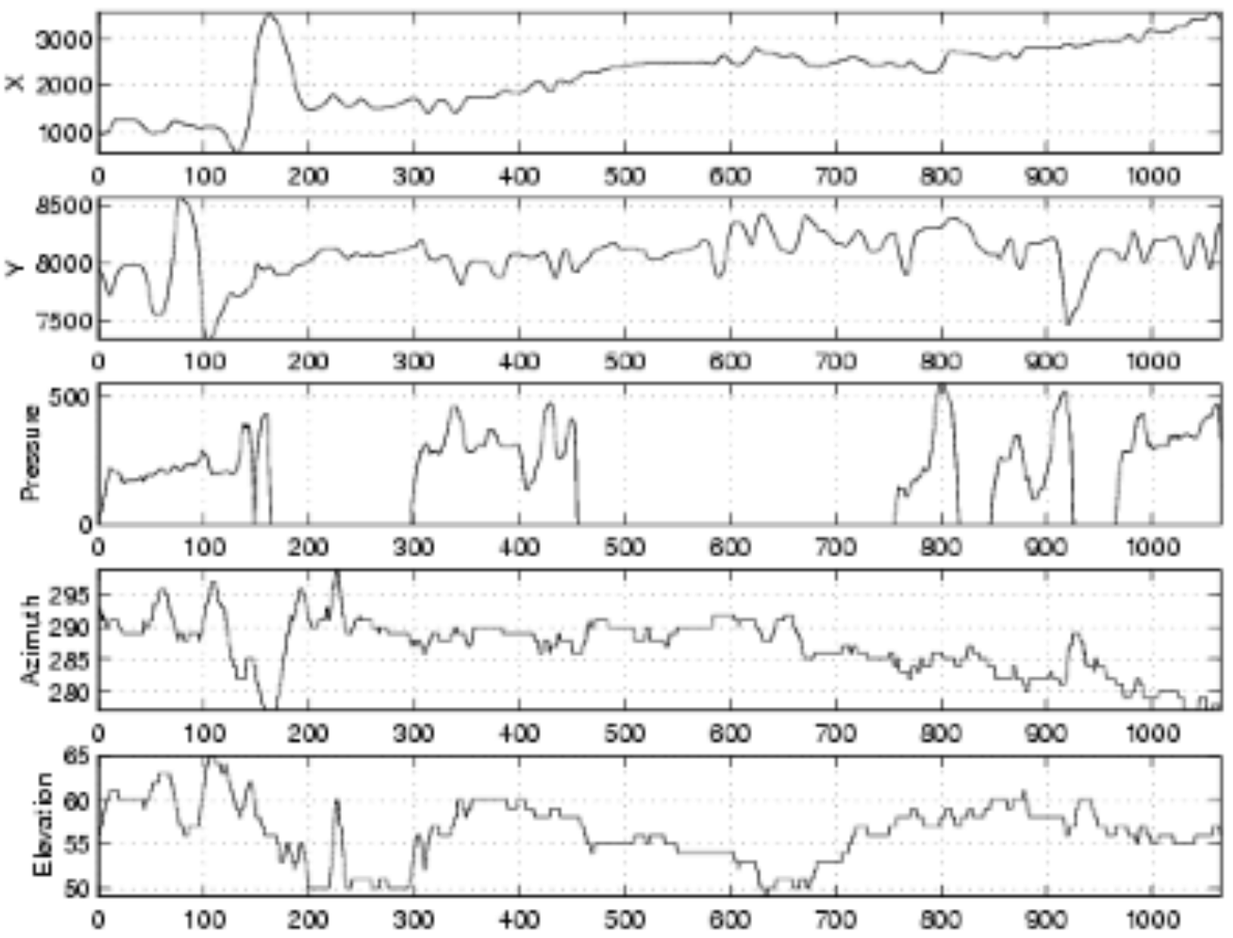
(4)Kvalitní padělek

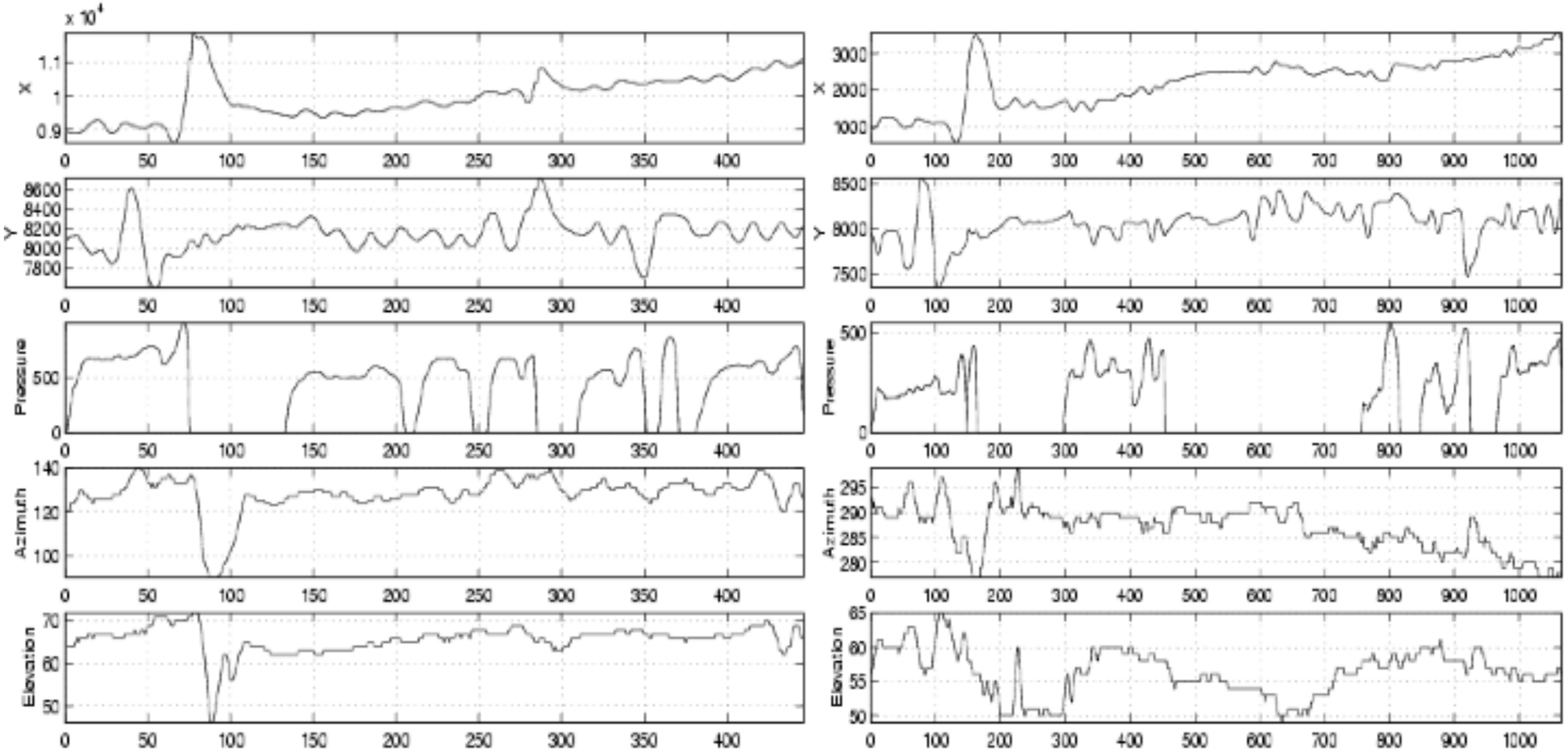
Originální podpis



Kvalitní padělek



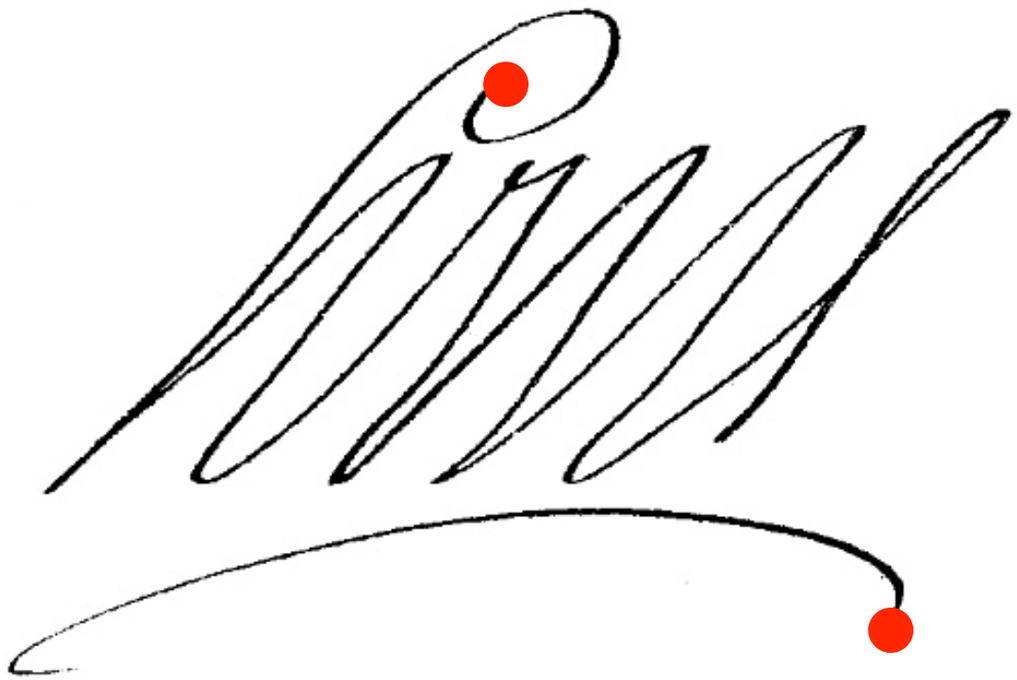




Originál

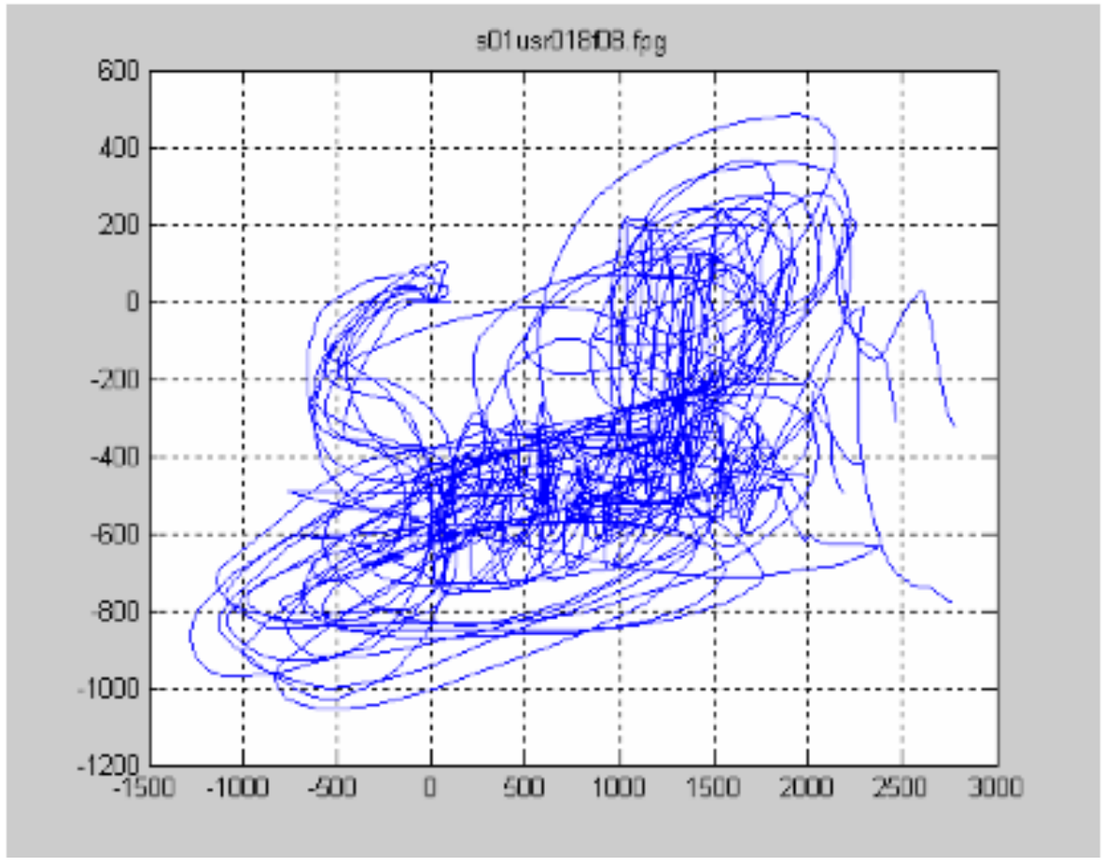
Kvalitní padělek

Předzpracování



- **Vyhlazování**
  - **vstupní signál bývá často velmi zubatý**
- **Segmentace**
  - **začatek: první přítlak**
  - **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**

Příklady lokálních příznaků

- **Derivaci** je vhodné aproximovat regresí druhého řádu - ne pouze jednoduchou diferencí vzorků.
  Vzorec pro regresi ***N***-tého řádu v čas ***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:

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

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

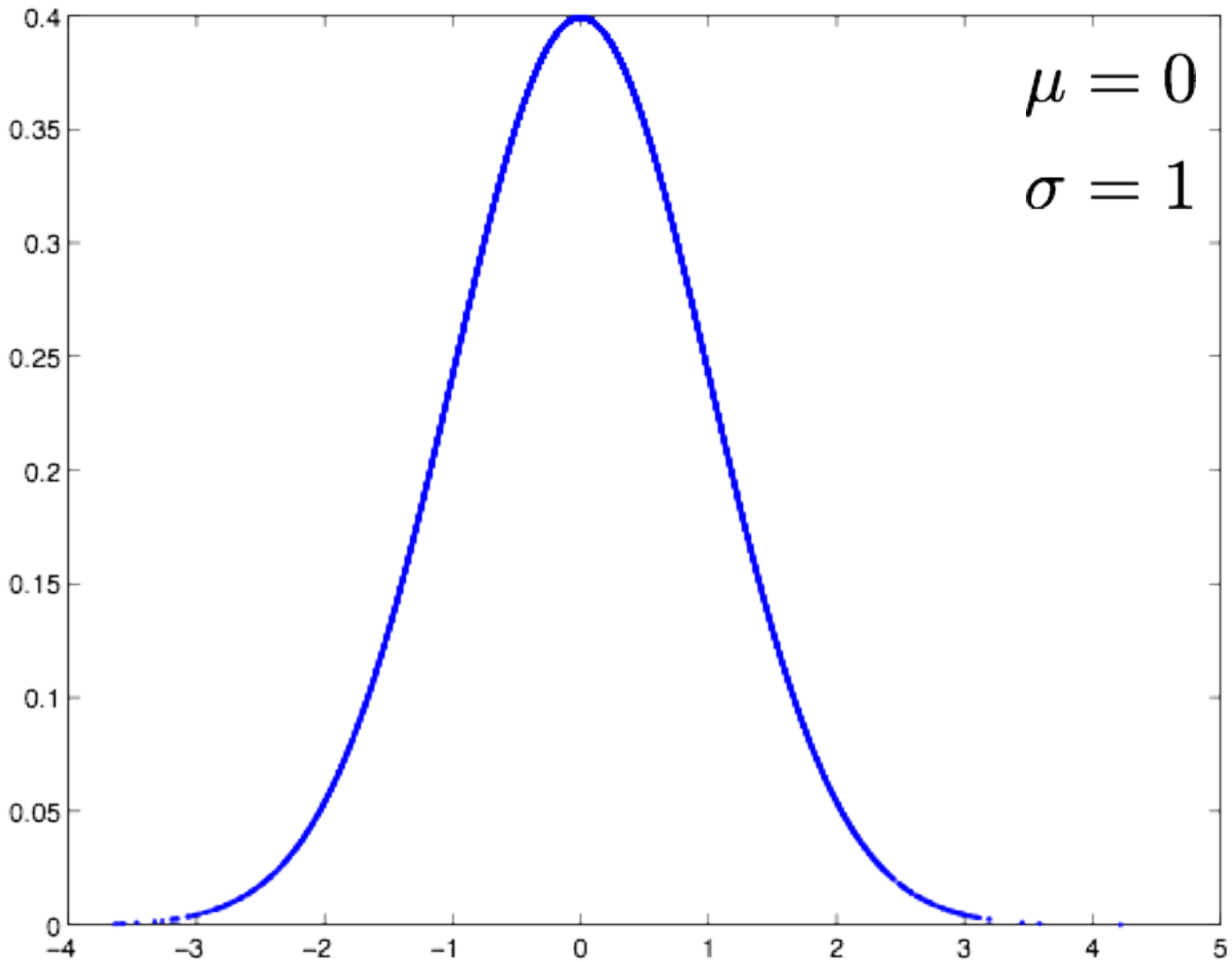
Lokální a globální příznaky

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

Použití modelů

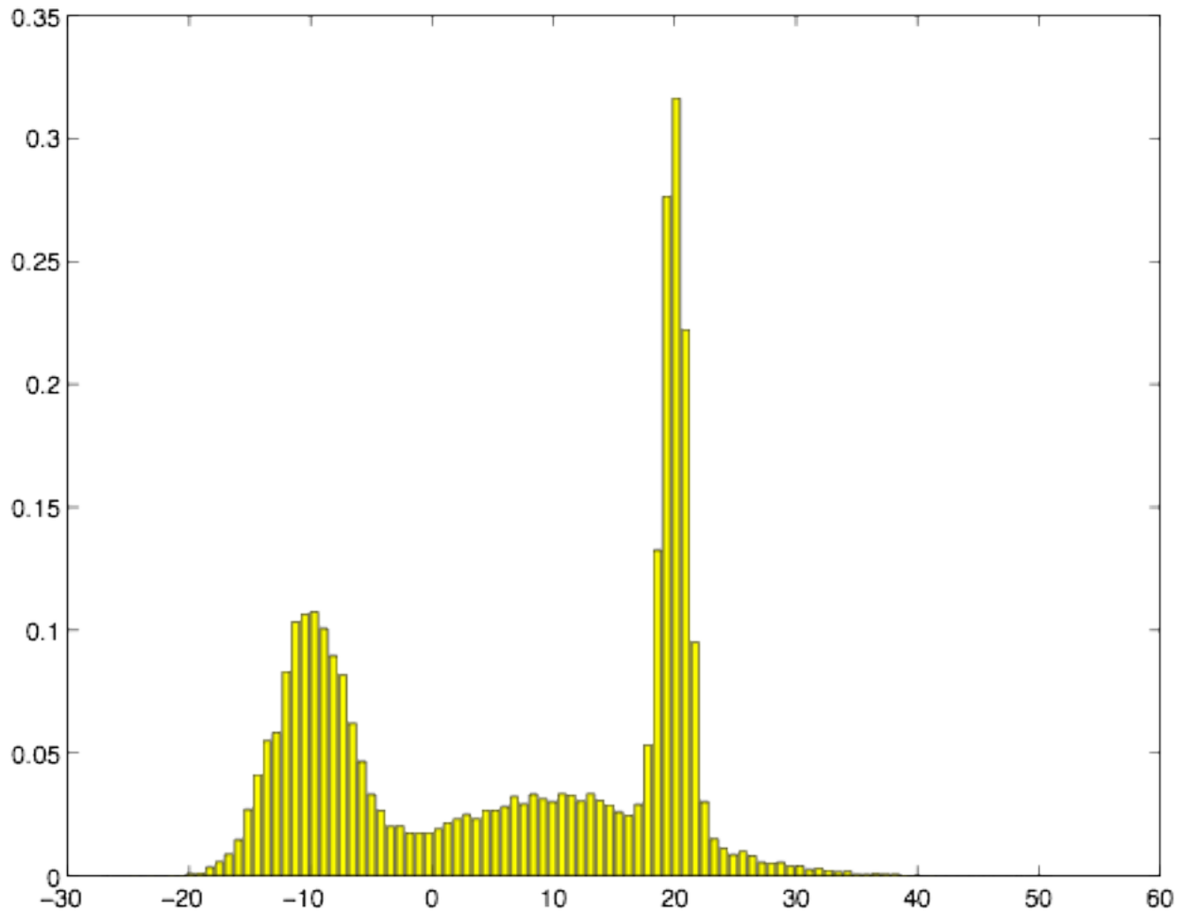
- **Deterministické metody**
  - **Dynamic Time Warping (DTW)**
  - **Vector Quantization (VQ)**
- **Statistické metody**
  - Gaussian Mixture Model (GMM)
  - **Hidden Markov Model (HMM)**

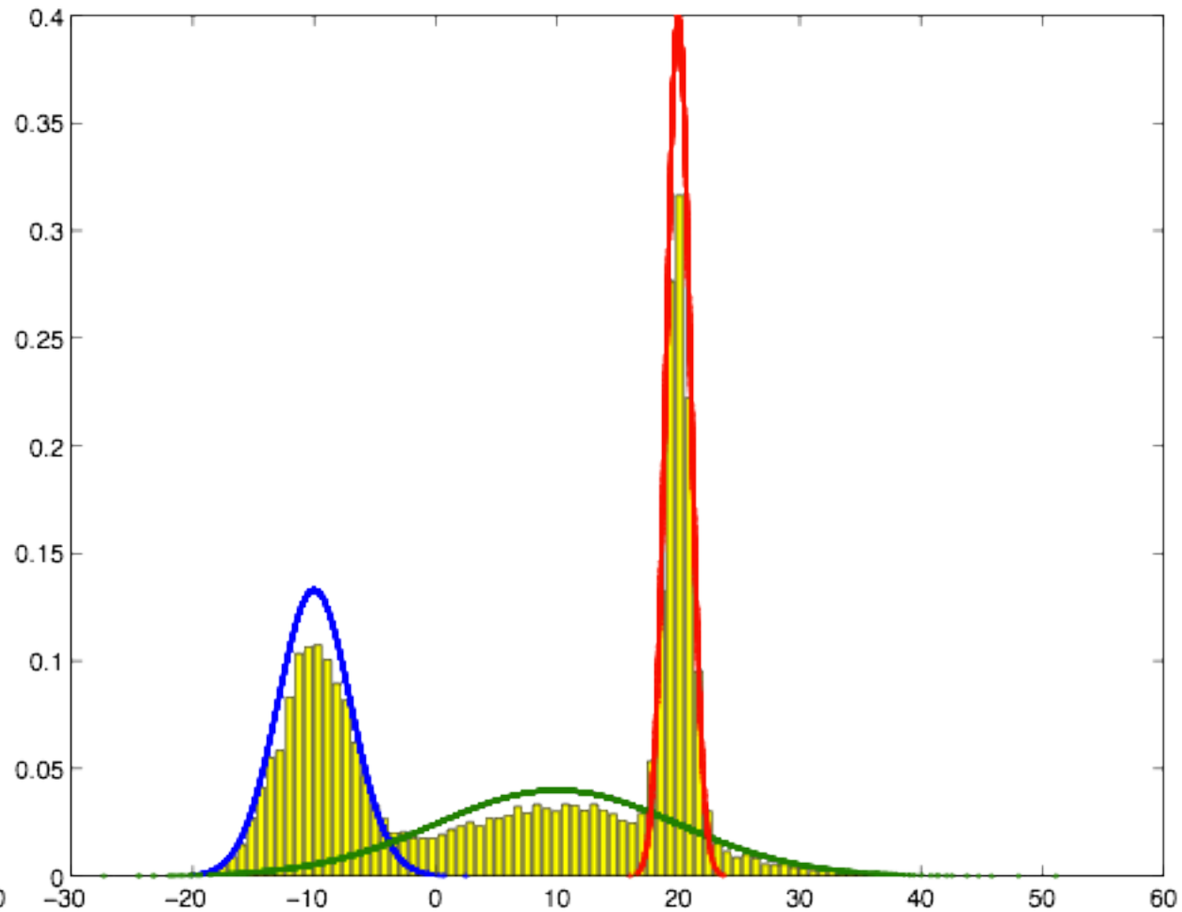
Gaussian Mixture Model



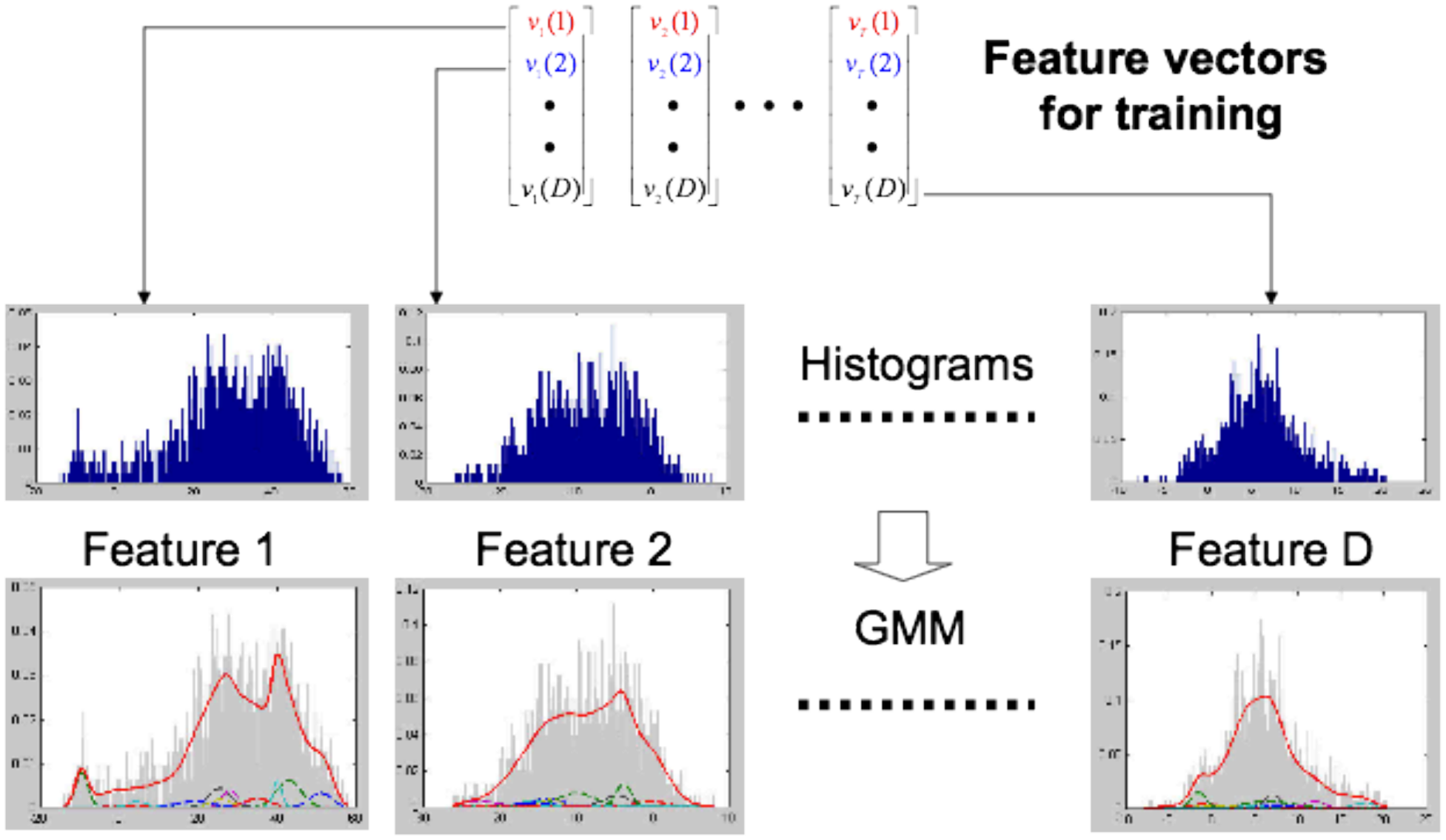
$$f(x) = \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{(x-\mu)^2}{2\sigma^2}}$$

Gaussian Mixture Model





Gaussian Mixture Model



score = log-likelihood (signature | model)

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**
- **Handicapovaní lidé a lidé, s nedostatečnou motorickou koordinací**

“Obyčejný” tablet

- **Genius G-Pen F509 ~ 1 100Kč**
  - **2000 lpi**
  - **1024 úrovní přítlaku**
  - **125 bodů/s**

- **Wacom STU-520 LCD Signature ~ 6 000Kč**
  - **LCD**
  - **2540 lpi (neinterp.)**
  - **512 úrovní přítlaku**
  - **200 bodů/s (neinterp.)**

“Biometrický” tablet

- **Wacom Intuos4 S A6 ~ 4 700Kč**
  - **5080 lpi**
  - **2048 úrovní přítlaku**
  - **200 bodů/s**
  - **náklon i natočení (grip pen)**

Děkuji za pozornost