Biometrické a bezpečnostní systémy

Vlasta Radová
Západočeská univerzita v Plzni
katedra kybernetiky

Pojem *biometrie*

- Pod pojmem ***biometrie*** se rozumí soubor vědních poznatků založených především na statistickém a analytickém přístupu, jejichž předmětem je zkoumání a následné praktické využití měřitelných charakteristik živých organizmů s cílem jejich následné jednoznačné identifikace či verifikace. Nejčastějším objektem tohoto zkoumání je člověk.
- ***Biometrie*** je metoda využívající jedinečných, měřitelných, fyzikálních nebo fyziologických znaků (tzv. markantů) nebo projevů (např. chování) člověka k jednoznačnému zjištění (identifikaci) nebo ověření (verifikaci) jeho identity.

Základní pojmy – *identita*

Pojem **identita** (lat. *identitas*, odvozené od slova *idem* – *stejný*) neboli **totožnost** se používá tehdy, když porovnávané pojmy, objekty apod. jsou záměnné takovým způsobem, že mezi ně můžeme klást znaménko rovnosti. Identitu chápeme tedy jako totožnost něčeho s něčím anebo se sebou samým.

Příklad: trojúhelník rovnostranný = trojúhelník rovnoúhlý

Identita je tedy logický vztah mezi objekty, jež se shodují ve všech svých vlastnostech.

Základní pojmy – *identita osoby*

Identita osoby je kombinace biologických i psychických, vrozených i získaných individuálních a specifických vlastností a schopností vnímat sám sebe. Identita je ztělesněním našeho vlastního já. Z toho logicky vyplývá, že každý z nás je totožný (identický) právě a jen sám se sebou. Na identitu osoby lze pohlížet z různých hledisek.

Identita osoby z různých hledisek

- **Biologická identita osoby** je kombinace dědičných a získaných biologických charakteristik člověka nezávislých na vědomí člověka. Podle posledních vědeckých poznatků je biologická identita člověka dána lidským genomem, tj. strukturou DNA každého lidského jedince.
- **Identita osoby z hlediska psychologie** znamená totožnost vědomí. Duševně zdravý člověk si při všech změnách, které se s ním odehrávají v čase a prostoru uvědomuje totožnost (identitu) své osoby, svého já. (Člověk občas trpí i dočasnou ztrátou nebo změnou vlastní identity, např. v pubertě)
- **Identita osoby z hlediska filozofie** znamená ztotožnění bytí a myšlení.
- **Identita sociální** – osoba podle svých charakteristik, projevů a zvyků patří k sociální skupině osob, jejíž členové mají stejné vlastnosti společenské geografické, jazykové, kulturní i specifické. V této souvislosti se často také hovoří o identitě jazykové, kulturní, etnické, morální apod.

Základní pojmy – *identifikace*

- **Identifikace** je proces porovnávání rozmanitých objektů na základě jejich shody nebo rozdílu ve vlastnostech, formách, umístění, složení (struktuře), funkcích, projevech, významu nebo v čase s cílem zjistit, zda se jedná o shodné (identické) objekty.
- Podstatný rys identifikace je tedy rozhodování o shodě ve všech vlastnostech, funkcích, vztazích apod. Takové kritérium je velmi přísné, a to zejména z těchto důvodů:
  - Rozhodovací proces by měl být realizován v konečném čase, s konečnými kapacitami, rozlišovací přesností apod. Jde tedy o praktickou potřebu omezenosti rozhodovacího procesu.
  - Rozhodovací proces je obvykle motivován některými praktickými potřebami. Nalezne-li vyšetřovatel po delší době člověka, o němž všechny zjištěné důkazy potvrzují, že je pachatelem trestného činu, nebude se pozastavovat například nad tím, že pachatel je o danou dobu starší, narostl mu plnovous apod.

Základní pojmy – identita vs. shodnost

- V kriminalistice důsledně se rozlišují pojmy identita a shodnost.
  - **Identita** osoby se v čase nemění, tj. její identifikační charakteristiky jsou jednoznačné a časově neměnné.
  - Naproti tomu osoba je **shodná** sama se sebou pouze v jediném časovém okamžiku. S narůstajícím časem je osoba nestále pozměňována vlastními fyziologickými procesy – metabolismem, stárnutím, nemocemi, apod. Přesto se jedná o jednu a tutéž (identickou) osobu.
  - Z tohoto pohledu je **identita** člověka určena jen omezeným, ale plně dostačujícím množstvím identifikačních charakteristik (otisky prstů, struktury DNA apod.). Pojem **shodnost** pak odpovídá situaci, kdy je člověk ztotožněn na základě všech svých vlastností (tzn. i „méně“ významných vlastností).

Základní pojmy – *identifikace osoby*

- **Identifikace osoby** je specifickým případem identifikace, kdy na základě příslušných vlastností, vztahů apod. identifikujeme lidské bytosti. Identifikaci osoby lze chápat dvojím způsobem:
  - **vnější identifikace osoby** znamená stanovení fyzické (biologické) identity člověka.
  - **vnitřní identifikace osoby (sebeidentifikace)** znamená nalezení a vnímání vlastní identity, tj. jak vnímáme sebe sama a s čím se vnitřně ztotožňujeme.

Základní pohled na identifikaci osoby

- Osoby rozlišujeme podle toho, jak fyzicky vypadají, jak se chovají, v jaké interakce vstupují se svým okolím, jaké mají jméno, jak je nazývají ostatní (jménem, příjmením, přezdívkou) v rodinném, přátelském či pracovním prostředí, apod.
- Osoby tedy můžeme identifikovat podle toho, co *mají*, *znají* nebo *dělají*.
- Základní identifikaci osoby tedy můžeme rozlišovat pomocí 3 přístupů:
  - **vlastnictví** určitých vnějších, přidělených charakteristik a věcí dané osobě;
  - **znalostí**, které osoba má;
  - **biometrických charakteristik** lidského těla a jeho projevů.

Identifikace osoby pomocí vlastnictví

- Mezi identifikační charakteristiky typu vlastnictví zařazujeme:
  - jména a příjmení
  - osobní doklady
  - identifikační čísla a kódy
  - identifikační karty a čipy
  - biočipy
- Nevýhody: jména nejsou jednoznačná, osobní doklady jsou odvozené od rodného listu (není dokladem identity osoby!), podobně identifikační čísla, kódy, karty a čipy. U biočipů nejsou vyřešeny etické otázky. Jakékoli vlastnictví lze ukrást.

Identifikace osoby pomocí znalostí (hesel)

- Hesla mohou být
  - statická
  - dynamická

- Nevýhody: lze je ukrást, odhadnout, odpozorovat.

Pravidla pro vytváření bezpečných hesel

- heslo nesmí obsahovat žádný údaj z našeho života (jméno, příjmení, přezdívku, datum narození, promoce, svatby, počet dětí apod.) nebo jinak běžné slovo
- doporučuje se, aby heslo mělo alespoň 8 znaků, pro bezpečnější použití alespoň 10 znaků
- heslo by mělo obsahovat znaky alespoň ze 2 skupin (malá písmena, velká písmena, číslice, apod.)
- heslo by mělo obsahovat speciální znaky (%, @, &, *, mezera, apod.) – některé crakovací programy tyto znaky nezkoušejí (používají klasické jazykové nebo encyklopedické slovníky), takže takové heslo nedokáží prolomit.

Identifikace osoby pomocí biometrických charakteristik

- Základní myšlenka biometrické identifikace: každá osoba identická jen a pouze sama se sebou.
- Jestliže vědecky prokážeme, že i naše fyzické a psychické charakteristiky jsou jedinečné, pak je lze úspěšně použít pro efektivní identifikaci osoby s velmi vysokým stupněm jedinečnosti a tedy následně i bezpečnosti a prokazatelnosti.
- Identitu osoby je pak téměř nemožné absolutně napodobit nebo pozměnit.
- Nelze ji ani odcizit, protože identifikační charakteristiky jsou bezprostředně spojené s identifikovanou osobou.
- Biometrická identita je pro každého člověka navíc přirozená – je s ním spojena již od narození.

Identifikace osoby pomocí biometrických charakteristik

- Výhody: Biometrické charakteristiky nelze zapomenout nebo ztratit, je těžké je napodobit nebo odcizit, jsou nepřenositelné, jsou lidsky přirozené. Identifikace s biometrickými charakteristikami je přesná, snadno a rychle použitelná, lze ji plně či částečně automatizovat.
- Nevýhody: Etické problémy

Členění biometrických charakteristik

- **anatomicko-fyziologické** – oční duhovka, oční sítnice, tvář, tvar vnějšího ucha, daktyloskopické otisky prstů, dlaní a chodidel, geometrie prstů a ruky, topografie žil zápěstí, pach lidského těla, obsah solí v lidském těle, rozměry a váhy lidského těla, DNA
- **behaviorální** (angl. to behave = chovat se) – hlas, lokomoce (pohyb v prostoru pomocí svalové činnosti), písmo, podpis, dynamika psaní na klávesnici

Aplikace biometrik

- **ve forenzních vědách**, tj. využití biometrických principů a aplikací pro potřeby orgánů činných v trestním řízení (policisté, kriminalisté, vyšetřovatelé, soudní znalci, obhájci a soudci)
  - Velký důraz je kladen na vyloučení jakékoli chyby, protože chyba může negativně ovlivnit lidský osud.
  - Zpracování je podporováno laboratorními a počítačovými technologiemi, výsledek však vždy zhodnocuje člověk (specialista – soudní znalec), který jej v případě potřeby obhajuje před soudem.

Aplikace biometrik

- **v komerčně využitelných aplikacích** pro privátní ochranu osob a majetku
  - důraz se klade především na rychlost při akceptovatelné chybovosti.
  - Jejich základním rysem je plně automatické zpracování.

- **v administrativně-správním procesu**, tj. identifikační průkazy (občanské průkazy, pasy), řidičské průkazy, apod., kde je vyžadována rychlost a bezchybnost verifikace osob v mezinárodním měřítku (minimálně v rámci EU), včetně maximálního omezení přenositelnosti průkazu na neoprávněnou osobu

Podíl jednotlivých biometrických aplikací na trhu v roce 2006

Technologie	Podíl na trhu [%]
Podpis	2
Násobná biometrie	4
Hlas	4
Oční duhovka	7
Geometrie ruky	9
Tvář	19
Otisk prstů	44

(podle Rak, Roman; Matyáš, Václav; Říha, Zdeněk. Biometrie a identita člověka ve forenzních a komerčních aplikacích. 1. vyd. Praha : Grada, 2008. ISBN 978-80-247-2365-5, str. 25)

Kritéria pro biometrické technologie

- Operační kritéria
- Metodologická, algoritmická a bezpečnostní kritéria
- Technická kritéria
- Finanční kritéria
- Výrobní kritéria

Operační kritéria

- **Jedinečnost (unikátnost)**. Biometrické charakteristiky musí být dostatečně jedinečné (unikátní), aby bylo možné odlišit jednu osobu od druhé s vysokým stupně přesnosti a spolehlivosti
- **Neměnnost**. Charakteristiky (markanty), na kterých je založena biometrická identifikace, musí být v čase neměnné. Optimální je absolutní stálost (neměnnost) identifikačních znaků po celou dobu života člověka, v praxi se obvykle vyžaduje neměnnost alespoň po dobu od začátku produktivního života do důchodového věku.
- **Měřitelnost**. Charakteristiky, na kterých je založena identifikace, musí být měřitelné a symbolicky vyjádřitelné. Musí být dopředu známa chybovost měření, než je příslušná biometrická metoda zavedena do rutinní praxe.
- **Uchovatelnost**. Naměřené charakteristiky musí být možné uchovávat (archivovat) s přijatelnými náklady, aniž by došlo ke ztrátě jejich kvality.

Operační kritéria (pokr.)

- **Spolehlivost**. Proces měření, zpracování, ukládání a vyhodnocování biometrických charakteristik musí být dostatečně spolehlivý a kdykoli zopakovatelný se stejnými výsledky.
- **Exkluzivita**. Identifikační metoda by měla být úplná takovým způsobem, aby nebyla nutná další podpůrná identifikační činnost (založená např. na jiné metodě identifikace).
- **Praktičnost**. Uživatel by měl být v minimálním kontaktu s vlastním technologickým zařízením. Měření by mělo být co nejjednodušší, měřených a ukládaných charakteristik by mělo být co nejméně. Požadavky na vyškolení uživatele by měly být co nejmenší.
- **Přijatelnost.** Získávání, zpracování, uchovávání a vyhodnocování biometrických údajů by mělo být pro vysoké procento lidí přijatelné (osobně, společensky, sociálně, nábožensky, politicky, eticky atd.) Nesmí se používat takové technologické postupy a metody, které by vyžadovaly část lidského těla, tj. prováděly by zásah do jeho integrity a jakýmkoli způsobem by poškozovaly nebo oslabovaly lidský organizmus.
- **Uživatelská přívětivost**. Proces snímání a vyhodnocování nesmí být vtíravý

Metodologická, algoritmická a bezpečnostní kritéria

- Správnost teorie (biometrické algoritmy jsou obvykle založeny na statistických metodách modelování, dynamickém programování, nebo neuronových sítích)
- Správnost algoritmů
- Bezpečnost algoritmů
- Správnost výběru markantů
- Efektivita a zabezpečení kódování biometrických dat
- Zabezpečení databáze s biometrickými daty
- Bezpečnost přenosových protokolů
- Bezpečnost síťového a distribuovaného prostředí

Technická kritéria

- čas na zpracování/vyhodnocení markantů,
- chybovost,
- flexibilita,
- odolnost,
- efektivnost,
- výkonnost,
- standardizace (kompatibilita s jinými zařízeními),
- skladovatelnost markantů,
- požadovaný prostor na uložení a zpracování markantů,
- velikost tzv. šablony,
- přesnost,
- jednoduchost,
- rychlost,
- nezávislost na vnějším prostředí

Finanční kritéria

- pořizovací cena technologie,
- cena instalace,
- náklady spojené s uvedením do provozu (školení a trénink obsluhy),
- udržovací náklady,
- cena návazných systémů,
- cena dalších zamýšlených zařízení (budoucího rozvoje systému),
- cena obsluhy,
- ...

Výrobní kritéria

- Zohledňuje se zde náročnost výroby příslušného zařízení.

Rozdělení biometrických aplikací ve vztahu k uživatelům a prostředí (1)

- Podle toho zda uživatel s aplikací spolupracuje či ne, rozeznáváme ***aplikace spolupracující a nespolupracující***.
- V případě spolupracujících aplikací se předpokládá, že uživatel si přeje být rozpoznán, a proto může být požádán o nějakou informaci typu vlastnictví nebo znalostí, na základě které má být jeho identita prokázána.
- U nespolupracujících osob nelze takovou informaci požadovat, protože se předpokládá, že by tato informace mohla být nepravdivá.

Rozdělení biometrických aplikací ve vztahu k uživatelům a prostředí (2)

- Jestliže si uživatel uvědomuje, že se získávají jeho biometrické charakteristiky, mluvíme o ***zjevné aplikaci*** (např. přístup do budov apod.).
- Naopak u ***skrytých aplikací*** není tato skutečnost uživateli známa (např. forenzní aplikace).

Rozdělení biometrických aplikací ve vztahu k uživatelům a prostředí (3)

- Pokud uživatel přichází do přímého fyzického kontaktu s aplikací (pokládá prst na snímací zařízení, dívá se přímo do kamery apod.) mluvíme o ***aplikaci aktivní***.
- ***Pasivní aplikace*** funguje bez přímého fyzického kontaktu (uživatel je např. snímám kamerou z velké vzdálenosti). Pasivní aplikace bývají většinou skryté.

Rozdělení biometrických aplikací ve vztahu k uživatelům a prostředí (4)

- Jestliže je proces identifikace kontrolován nebo řízen obsluhou, mluvíme o ***aplikaci s obsluhou***.
- V opačném případě jde o ***aplikaci bez obsluhy***.
- Někdy se používá též název ***aplikace řízená*** či ***neřízená uživatelem***.
- Nespolupracující aplikace musí být vždy s obsluhou, spolupracující aplikace může být i bez obsluhy.

Rozdělení biometrických aplikací ve vztahu k uživatelům a prostředí (5)

- Za ***aplikace ve standardním prostředí*** se považují aplikace, které obvykle pracují při průměrné teplotě vzduchu 20-25°C, průměrném atmosférickém tlaku, průměrné světelnosti, prašnosti, hlučnosti apod.
- Za ***aplikace v nestandardním prostředí*** lze považovat například systémy pro přístup do budov z vnějšku, které jsou celoročně vystaveny vnějším klimatickým podmínkám (mrazu, větru, prachu, vlhkosti, intenzivnímu slunečnímu záření apod.)

Rozdělení biometrických aplikací ve vztahu k uživatelům a prostředí (6)

- Pokud biometrické zařízení komunikuje s dalšími vzdálenými prvky (např. databázemi, informačními systémy apod.), se kterými dochází k vzájemné výměně dat, hovoříme o ***otevřené aplikaci***.
  - U otevřených aplikací musí být věnována pozornost bezpečnosti jak přenosových kanálů, tak vzdálených zařízení.
- V ***uzavřených aplikacích*** k výměně dat nedochází.