Cvičení z předmětu Biometrie
Úloha: Verifikace osoby pomocí dynamického podpisu

Jiří Wild, Jakub Schneider
kontaktní email: schnejak@fel.cvut.cz

5. října 2015

1 Úvod

Úloha má za cíl seznámit vás s metodami verifikace identity člověka pomocí jeho dynamického podpisu. Jádro verifikačních metod leží ve srovnávání verifikovaného podpisu s ověřenými předlohami použitím různých algoritmů. Dva takové algoritmy budou tvořit jádro cvičení — algoritmus založený na statistickém modelování **Gaussian Mixture Model** (GMM) a algoritmus určující míru podobnosti dvou sekvencí **Dynamic Time Warping** (DTW). K úloze byl vytvořen Signature Toolbox pro Matlab, který obsahuje základní funkce s naimplementovaným algoritmem GMM a připravenou funkcí pro DTW, kterou, pro hlubší pochopení, bude úkolem implementovat. Oba algoritmy budou porovnány chybovostí nad databází podpisů SVC2004 (popis v [3]). Posledním úkolem bude falsifikovat vybraný podpis a určit úspěšnost.

2 Teorie

Každý zná klasický podpis jako běžně užívanou biometrickou veličinu pro stvrzení a ověření pravosti dokumentů. Dynamický podpis je rozšířením klasického podpisu snímaný elektronicky, čímž přidává časovou informaci o zápisu a informace o přítlaku nebo náklonu a natočení pera.

Ze dvou základních použití biometrických veličin pro identifikaci nebo verifikaci se podpis uplatňuje výhradně pro verifikaci. Verifikací je myšlena procedura ověření totožnost člověka podle jeho podpisu. Vstupem verifikační procedury je tedy podpis a identifikace osoby hlásící se k podpisu. Poté je potřeba mít z trénovací množiny (většinou čítající okolo deseti podpisů u nichž máme ověřený původ) vytvořený model podpisu. Větší množství podpisů potlačuje intervariabilitu v podpisech jedné osoby. Model příslušící k ověřované identitě je poté srovnáván se vstupním podpisem, v našem případě pomocí algoritmů GMM a DTW, a z výsledné míry podobnosti je rozhodnuto o pravosti podpisu. Práh pro zamítnutí podpisu je určen při tvorbě modelu tak, aby poměry falešně zamítnutých pravých podpisů (FRR) a falešně přijatých plagiátů (FAR) vyhovoval požadavkům systému.

2.1 Vstupní podpisy, předzpracování signálu

Jak bylo uvedeno, dynamický podpis snímaný speciálním tabletem dává k dispozici prostorovou informaci o kontuře a jejím vzniku v čase. Kromě toho také informaci o přítlaku, náklonu a natočení pera. Snímané veličiny se nazývají příznaky, snímané v časech $t = 1..T$. Jednotlivé příznaky si označíme x_t, y_t pro polohu a p_t, ϕ_t, θ_t pro přítlak, náklon a natočení. Dále je možné přidávat další příznaky odvozené z uvedených. Tradiční odvozené příznaky jsou hodnoty rychlosti a zrychlení, tedy: $v_t = \|[\frac{dx}{dt}, \frac{dy}{dt}]\|$ pro rychlost a $a_t = \|[\frac{d^2x}{dt^2}, \frac{d^2y}{dt^2}]\|$.

Z množinu příznaků je dobré zvolit jenom ty, které přinášejí nejvíce informace pro odlišení pravého podpisu od falsifikátu. Klasicky používané příznaky jsou poloha, rychlost, zrychlení. Případně ještě přítlak. Vyzkoušet různé kombinace příznaků bude jedním z vašich úkolů. Další vliv na výsledek modelování má počáteční předzpracování — umístit podpisy do podobného středu (např. těžiště) a normalizovat jejich velikost na definovaný rozsah. Posledním významným bodem je počet podpisů použitých pro tvorbu modelu. Všechny tyto parametry budete zkoušet nastavovat a sledovat jejich vliv na chybovost systému.

2.2 Signature Toolbox

Připravený systém Signature Toolbox pro Matlab slouží k načítání podpisů i jejich zpracování. Jsou připraveny funkce pro načítání podpisů a extrakci jednotlivých příznaků a také výpočet příznaků přidaných. Připraveny jsou také funkce na modelování podpisu pomocí GMM a ohodnocení kvality podpisu pomocí score. K algoritmu DTW je k dispozici prázdná funkce, kterou je potřeba implementovat. Popis použití toolboxu je v Příloze A.

2.3 Míra podobnosti využívající Gaussian mixture model

Princip systému založeném na GMM se dá shrnout v následujících bodech:

- Z podpisu je extrahováno n příznaků $x_{1,t} \dots x_{n,t}$, každý snímaný v časech $t = 1 \dots T$.
- Při učení modelu podpisu je pomocí GMM odhadnuto pravděpodobnostní rozdělení zvlášť pro každý příznak $x_1 \dots x_n$ ve všech jeho instancích (časových okamžicích). Pokud je v trénovací množině více podpisů, jsou do odhadu p. rozdělení postupně řazeny vzorky daného příznaku od všech podpisů. Tímto získáme n pravděpodobnostních rozdělení $P_1 \dots P_n$.
- Pokud poté rozpoznáváme neznámý podpis, ohodnotíme jej hodnotící funkcí pomocí log-likelihood: $score = \sum_{i=1}^{n} \sum_{j=1}^{T} ln[P_i(X = x_{i,j})]$

2.4 Míra podobnosti využívající Dynamic time warping

Při použití míry podobnosti podpisů DTW nedochází k učení modelu, ale pouze uložení zvoleného množství podpisů (trénovací podpisy) do registru. Při rozpoznávání podpisu je poté neznámý podpis porovnáván s trénovacími podpisy pomocí míry DTW (viz přednášky nebo [2]). Algoritmus výpočtu podobnosti dvou (obecně n-rozměrných) vektorů pomocí DTW je následující:

- Máme dva podpisy s_1, s_2 tvořené n příznaky, jejichž délky jsou t a s. Notace je stejná, jako v předchozím případě.
$$s_1 = \begin{bmatrix} x_{1,1}, x_{2,1}, \ldots, x_{n,1} \\ x_{1,2}, x_{2,2}, \ldots, x_{n,2} \\ \ldots \\ x_{1,t}, x_{2,t}, \ldots, x_{n,t} \end{bmatrix}, s_2 = \begin{bmatrix} x_{1,1}, x_{2,1}, \ldots, x_{n,1} \\ x_{1,2}, x_{2,2}, \ldots, x_{n,2} \\ \ldots \\ x_{1,s}, x_{2,s}, \ldots, x_{n,s} \end{bmatrix}.$$

- Porovnání pomocí DTW je možné spočítat následujícím algoritmem: *i)* Je vytvořena matice D o rozměrech $(t+1, s+1)$, která je iniciována $D(1,1) = 0, D(i,1) = \inf, D(1,j) = \inf, i = 2 \ldots n, j = 2 \ldots m$. *ii)* Další pole v matici D jsou počítána následovně:
$$D(i,j) = ||s_1(i-1,:) - s_2(j-1,:)|| + min \begin{cases} D(i,j-1) \\ D(i-1,j) \\ D(i-1,j-1) \end{cases},$$
$||s_1(i-1,:) - s_2(j-1,:)||$ označuje eukleidovskou vzdálenost mezi (i-1)-tým řádkem (vzorkem) podpisu s_1 a (j-1)-tým řádkem v podpisu s_2, tedy $\sqrt{\sum_{d=1}^{n} [s_1(i-1,d) - s_2(j-1,d)]^2}$.

- Vzájemná vzdálenost obou vektorů je na konci výpočtu naakumulována v $dist = D(t+1, s+1)$.

Po porovnání testovaného podpisu se všemi trénovacími podpisy spočítáme průměrnou vzdálenost a zápornou hodnotu této vzdálenosti použijeme jako míru hodnocení kvality podpisu (záporná hodnota proto, že čím jsou podpisy podobnější, tím je hodnota menší, u je míry podobnosti je třeba tuto závislost převrátit).

3 Vypracování úlohy

1. Každý student dostane zadány podpisy od 15 různých osob včetně jejich identifikace. Jako první vytvořte model podpisu pro každého zadaného člověka metodou GMM. (použijte přednastavené parametry) Dále zvolte práh míry podobnosti (*score*), při kterém určíme podpis jako pravý (pro celý set a pro pět ze zadaných osob - porovnejte). Statisticky vyhodnoťte kolik poměrně podpisů je nesprávně zamítnuto (FRR) a kolik falsifikátů je falešně označeno za pravé podpisy (FAR) na celé databázi pro Vámi zvolenou hodnotu prahu *s*core. [3 b]

2. Dalším krokem bude implementace metody DTW do Sign Toolboxu. Metodu tak, jak je popsána v Sekci 2.4 implementujte do příslušné funkce v toolboxu. Poté stejně jako v předchozím kroku vytvořte model pro zadané podpisy a stejně statisticky zpracujte. [7 b]

3. Posledním krokem bude optimalizace systémů. Pro oba implementované systémy vyzkoušejte, jaký vliv na získané chybové statistiky má nejprve normalizace vstupních podpisů (nulová střední hodnota příznaků a jednotkový rozptyl). Dále vyzkoušejte přidat další příznaky, kromě klasických — poloha, rychlost, zrychlení — přidejte postupně přítlak a časovou derivaci polohy x a polohy y. [4 b]

4. Po nalezení nejlepších výsledků změnou používaných příznaků vyzkoušejte jak se změní situace přidáním většího počtu trénovacích podpisů při tvorbě modelu. [1 b]

5. Nakonec zkuste vlastním falsifikátem podpisu spolužáka prolomit rozpoznávací systém. (Po párech jeden se pokouší falsifikovat podpis druhého a obráceně) [5 b]

O postupu zpracování úlohy sepište stručný protokol, kde ilustrujte postup řešení jednotlivých bodů zadání. Předpokládá se samostatná práce na úloze.

3.1 Bonusy:

1. Implementujte jinou metodu rozpoznávání podpisu např. z literatury (veliký přehled metod je v [1]). [5 b]

A Příloha: Struktura Sigature Toolboxu.

Ke cvičení je přiložen částečně vytvořený systém s již implementovaným porovnáváním podpisu v Matlabu pomocí GMM a sadou testovacích podpisů. Celý systém je možné používat pomocí následujících funkcí:

- *load_data* — funkce k načítání podpisů tak, jak byly uloženy od počítače. Výstupem je cell-array s načtenými podpisy, např. $S = \{s_1, s_2, \ldots\}$, kdy s_i odpovídá podpisu tak, jak je definován v předchozí kapitole o DTW. K jednotlivým podpisům se v Matlabu přistupuje následovně: $s_i = S\{i\}$.
- *preprocess* — funkce k předzpracování vstupních dat.
- *extract_features* — funkce k získání příznaků ze vstupních dat.
- *make_model* — funkce k naučení modelu.
- *score* — funkce pro výpočet ohodnocení rozpoznávaného podpisu.
- *ukazka* — funkce s ukázkovým kódem použití.

Všechny funkce i jejich použití jsou dokumentovány v nápovědě funkcí.

Reference

[1] Donato Impedovo. Automatic signature verification: The state of the art. Ke stazeni: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4603099 (dostupne pres dialog.cvut.cz).

[2] J M Pascual-Gaspar. Practical on-line signature verification. Ke stazeni: http://www.springerlink.com/content/n0x73333061702u4/ (dostupne pres dialog.cvut.cz).

[3] SVC2004. Svc 2004: First international signature verification competition, detailed instructions for participants. Ke stazeni: http://www.cse.ust.hk/svc2004/instructions.pdf.