Univerzita Karlova

1. lékařská fakulta

Disertační práce

Ing. Anna Schlenker

Bezpečnost IT v biomedicíně

Postgraduální doktorské studium biomedicíny

Vedoucí disertační práce: Ing. Milan Šárek, CSc.

Studijní obor: Biomedicínská informatika

Praha 2019

Poděkování

Ráda bych touto cestou vyjádřila poděkování Ing. Milanu Šárkovi, CSc. za jeho rady a trpělivost při vedení mého doktorského studia. Rovněž bych chtěla poděkovat RNDr. Janu Kalinovi, Ph.D. za vstřícnost a pomoc při získání potřebných informací a podkladů k tvorbě publikací.

Dále bych ráda poděkovala všem, kteří v jakékoliv míře pomohli a přispěli k dosažení výsledků práce.

Prohlašuji, že jsem závěrečnou práci zpracoval/a samostatně a že jsem řádně uvedl/a a citoval/a všechny použité prameny a literaturu. Současně prohlašuji, že práce nebyla využita k získání jiného nebo stejného titulu.

Souhlasím s trvalým uložením elektronické verze mé práce v databázi systému meziuniverzitního projektu Theses.cz za účelem soustavné kontroly podobnosti kvalifikačních prací.

V Praze dne 3. září 2019 Anna Schlenker

Název práce: Bezpečnost IT v biomedicíně

Autor: Ing. Anna Schlenker

Vedoucí disertační práce: Ing. Milan Šárek, CSc.

Abstrakt: Cílem disertační práce je navrhnout řešení strategie zabezpečení biomedicínských dat. Práce poskytuje přehled nejčastěji používaných biometrických metod určených k identifikaci či autentizaci uživatelů. Z těchto metod byla vybrána a v aplikačním řešení použita metoda dynamiky stisku počítačových kláves. Spolehlivost této metody byla testována klasickými a moderními klasifikačními metodami. Největším přínosem práce je pak použití vytvořené aplikace v kombinaci s měřením pomocí integrované elektromyografie pro objektivizaci hodnocení prací spojených s psaním na klávesnici z hlediska lokální svalové zátěže.

Klíčová slova: biometrie, bezpečnost dat, dynamika stisku počítačových kláves, lokální svalová zátěž.

Title: IT Security in Biomedicine

Author: Ing. Anna Schlenker

Supervisor: Ing. Milan Šárek, CSc.

Abstract: The aim of this work is to propose a solution to the biomedical data security strategy. The work provides an overview of the most commonly used biometric methods designed to identify or authenticate users. From these methods, the keystroke dynamics was chosen and used in the application solution. The reliability of this method has been tested by classical and modern classification methods. The greatest benefit of the work is the use of the created application in combination with the measurement using integrated electromyography to objectify the evaluation of the work related to keyboard typing in terms of local muscle load.

Keywords: Biometrics, Data Security, Keystroke Dynamics, Local Muscle Load.

Obsah

Předmluva

Na úvod své disertační práce bych čtenáře ráda ve zkratce seznámila s průběhem doktorského studia, jehož výsledkem je zde předložená práce.

Doktorské studium jsem zahájila v roce 2010 v rámci *Doktorských studijních programů v biomedicíně*, kdy jsem se při práci v Ústavu informatiky AV ČR, v.v.i. v tehdejším Oddělení medicínské informatiky pod vedením prof. RNDr. Jany Zvárové, DrSc. a po úspěšném ukončení magisterského studia na Fakultě biomedicínského inženýrství ČVUT, rozhodla pokračovat ve studiu biomedicíny a v působení v akademické sféře. Na vedení disertační práce jsem se domluvila s Ing. Milanem Šárkem, CSc. a téma práce jsme společně formulovali jako **Bezpečnost IT v biomedicíně**, protože v té době přesně toto tvořilo jeden z dílků zapadajících do plánovaných projektů v rámci tehdejšího „EuroMISE centra“.

Krátce po zahájení mého studia došlo k ukončení mezioborového výzkumu na ÚI AV ČR, v.v.i. a tak se postupně Oddělení medicínské informatiky transformovalo, až zaniklo. V té době jsem nastoupila na mateřskou dovolenou a po jejím návratu ještě do roku 2015 působila na ÚI AV ČR, v.v.i. jako hlavní řešitel projektu Fondu Rozvoje CESNET 494/2013/1 s názvem „Identifikace uživatele pomocí dynamiky stisku počítačových kláves“. V roce 2013 jsem se částečně vrátila na svoji „alma mater“, kterou je Fakulta biomedicínského inženýrství ČVUT, kde dodnes působím na Katedře biomedicínské informatiky jako odborný asistent a podílím se na výuce zejména v předmětech, které souvisí s informačními systémy a bezpečností medicínských dat. Ve stejném roce jsem díky paní profesorce Zvárové našla uplatnění také na Ústavu hygieny a epidemiologie, 1. lékařské fakulty, UK a VFN, kde také působím dodnes na pozici odborného asistenta a podílím se na výuce mediků v předstátnicové stáži z předmětu Hygiena a epidemiologie. Mé působení na tomto pracovišti také způsobilo rozšíření původního tématu. Jsem přesvědčena o tom, že jde o posun k lepšímu a potvrzují to i vydané publikace a zájem o využití navržené metody v praxi. Metoda, která byla původně zamýšlena pro použití v aplikacích podporujících vyšší zabezpečení medicínských dat, nakonec našla praktické uplatnění i v prostředí hygieny a pracovního lékařství, kde se nyní úspěšně používá pro objektivizaci měření a hodnocení lokální svalové zátěže při psaní na klávesnici.

Úvod

V době, kdy jsem začínala své doktorské studium, byla vzhledem k rychlému rozvoji informačních technologií velmi aktuální otázka jejích bezpečnosti. V současné době je situace pořád stejná, dokonce v mnoha ohledech i závažnější a problémy bezpečnosti IT palčivější. V předložené disertační práci je řešen problém výběru správné bezpečnostní strategie a její následná použitelnost zejména v oblasti biomedicíny.

Samotný text disertační práce je rozčleněn do následujících kapitol. Kapitola *Současný stav poznání a cíle výzkumu* formuluje cíle a hypotézy disertační práce. Tzv. „bílým místem“ řešeným v rámci disertační práce je již zmíněná dynamika stisku počítačových kláves a možnosti jejího použití, a to nejen při výběru správné bezpečností strategie.

Kapitola *Teoretická východiska* pojednává o současném stavu poznání a kriticky hodnotí stávající přístupy k řešení problematiky disertační práce. Konkrétně se věnuje obecným zásadám identifikace, autentizace a autorizace uživatelů a zejména pak biometrickým charakteristikám a dynamice stisku počítačových kláves. V této kapitole je popis neuronových sítí, které se používají ve spojení s dynamikou stisku počítačových kláves. Na závěr této kapitoly je uveden popis měření a hodnocení lokální svalové zátěže, a to z důvodu, že je oblastí aplikace výsledků disertační práce.

Kapitola s názvem *Použité metody zkoumání* se věnuje charakteristice metod použitých při řešení disertační práce. Jedná se zejména o metody klasifikační, které jsou použité při vyhodnocování výsledků snímání dynamiky stisku počítačových kláves. Dále se jedná o popis integrované elektromyografie jako jedné z metod pro měření a hodnocení lokální svalové zátěže. Důvodem zařazení popisu této metody je její současné použití se snímáním dynamiky stisku počítačových kláves v aplikaci používané v praxi pro měření a hodnocení lokální svalové zátěže při práci s počítačem.

Kapitola *Vlastní výsledky a přínosy* disertační práce se věnuje zejména popisu vlastní aplikace pro snímání dynamiky stisku počítačových kláves, kterou lze označit za jeden z originálních vlastních výstupů disertační práce. Je zde podrobně popsaná pilotní studie včetně sběru dat, analýzy dat a zhodnocení výsledků. Dále tato kapitola obsahuje stručný popis dalších provedených studií, jejichž výsledky jsou pak podrobně rozebírány v přiložených publikacích.

1. Současný stav poznání a cíle výzkumu

Bezpečnost dat je v současnosti tématem řešeným v mnoha oblastech, a to nejen na úrovni tzv. „vysokého zabezpečení“. Nejedná se pouze o bankovní či státní instituce, kde je potřeba chránit citlivé informace či finance. Všichni jsme si již zvykli na použití multifaktorového zabezpečení (uživatelské číslo, heslo, heslo zaslané sms-zprávou, ...), pokud z pohodlí domova nahlížíme do svého internetového bankovnictví nebo když provádíme platební transakce. Nikomu už nevadí přistupovat do svého zařízení, či do firemní sítě pomocí kombinace více druhů zabezpečení (uživatelské jméno, heslo, otisk prstu, ...).

Musíme si však uvědomit, že nejenom informace, které o nás mají úřady (jméno, datum narození, rodné číslo, číslo občanského průkazu, adresa trvalého či přechodného pobytu, záznamy v registru trestů, údaje o zaměstnavateli, záznamy v obchodním, živnostenským čí insolvenčním rejstříku, výpisy z katastru nemovitostí ...) a finanční instituce (přesné údaje o výškách příjmů a výdajů, informace o různých typech pojištění, ...), ale také informace, které o nás mají lékaři a zdravotní zařízení (záznamy o nemocech, operacích, alergiích, trvalých následcích, ...), je potřeba chránit.

Téma zabezpečení dat se stále více přenáší do oblasti biomedicíny a zdravotnictví. A v této oblasti se nejedná pouze o lékařské tajemství jako takové, ale řeší se řada dalších otázek souvisejících s elektronizací zdravotnictví. Dnes jsou již pracoviště bez počítače a bez informačního systému výjimkou. Řada lidí se začíná zajímat o to, kdo má přístup k těmto systémům a k informacím v něm. Není to tak dávno, kdy na odděleních v nemocnici lékař ráno zapnul počítač, přihlásil se do informačního systému a celý den všichni pracovníci na oddělení pracovali pod jeho identitou.

V současné době již většina informačních systémů na bezpečnost pamatuje a je možné nastavení různých práv pro různé uživatele. Uživatel, který se do systému hlásí, je většinou ověřený pouze jednou metodou, nejčastěji heslem. Toto heslo navíc často nesplňuje podmínky tzv. „bezpečného hesla“, například, aby nebylo snadno odhaleno slovníkovým útokem. A co to znamená? Jak již napovídá název „slovníkový útok“, jedná se o pokusy odhalit heslo tvořené slovy a jmény (které se dají najít ve slovnících). Pro útočníky samozřejmě není problém použít slovníky všech světových jazyků. Uživatelé by tudíž měli pamatovat na to, že jejich heslo by nemělo být tvořené jménem manžela/manželky, dětí či domácích mazlíčků. Obecně platí, že heslo má být dostatečně dlouhé (tj. alespoň 8 znaků)

složené z velkých i malých písmen, číslic a speciálních znaků. Pokud má být heslo bezpečné, uživatel ho nesmí nikomu prozradit (a to ani partnerovi/partnerce) a nesmí si ho nikam napsat. Není totiž nic jednoduššího, než opsat do systému heslo, které má uživatel zapsané v notýsku.

Další chybou většiny informačních systémů je to, že nedochází k automatickému odhlášení uživatele. Důvodem je nespíš „ztráta času“ zdravotníků při neustálém přihlašování se. Na druhou stranu by si však uživatelé těchto systémů měli uvědomit, že v takovémto případě není nic jednoduššího, než nechat zapnutý a přihlášený počítač bez dozoru, muset nutně odejít (což ve zdravotnictví asi není rarita) a tím vystavit počítač i se všemi citlivými údaji okolí. Stejně tak se tímto způsobem nedá zabránit tomu, aby jeden uživatel byl přihlášený na více počítačích najednou, co poskytuje případným útočníkům stejné možnosti.

Po uvědomění si všech rizik, které sebou nese používání všech zdravotnických informačních systémů, se nabízejí různé metody vysokého zabezpečení dat. Jedná se hlavně o biometrické charakteristiky, které se nedají nikam zapsat, nedají se zapomenout a nemůžeme je nikomu půjčit (samozřejmě pokud nepůjdeme do extrémů). Mezi nejběžněji používané biometrické charakteristiky patří anatomicko-fyziologické charakteristiky, jako například otisky prstů a dlaní, snímání krevního řečiště dlaně či hřbetu ruky, geometrie ruky, rozpoznávání obličeje, skenování sítnice atd. Další skupinou jsou takzvané behaviorální charakteristiky, které se zatím používají spíše v kriminalistice. Jedná se například o rozpoznávání lidí podle chůze či hlasu.

Probíhají školení, kde jsou zdravotničtí pracovníci obeznámeni s potřebou multifaktorového zabezpečení citlivých pacientských dat. Jedná se hlavně o uvědomění si, že zadávání hesla není jen činnost, která je otravná a zdržuje od práce, ale také činnost, která může ochránit data a následně i pracovníky. Informační systém také není jen software, který pracovníka bez vyplnění některé kolonky nepustí dále, ale upozornění na nevyplnění má své opodstatnění a daná kolonka je třeba důležitá. Velmi příjemným řešením, který nabízí vysokou úroveň zabezpečení bez zbytečného obtěžování personálu, je dynamika stisku počítačových kláves.

Cílem této práce je analyzovat současný stav používání biometrických údajů v oblasti počítačové bezpečnosti, zejména v oblasti biomedicíny a zdravotnictví a navrhnout řešení, které by zvýšilo úroveň zabezpečení zdravotnických informačních systému. Mezi další cíle patří vytvoření vlastní aplikace, která umožní snímání a vyhodnocení dynamiky stisku počítačových kláves. Hlavním a nejdůležitějším cílem práce je nasazení aplikace v praxi, čímž se prokáže její unikátnost, důležitost a hlavně použitelnost v reálné praxi.

2. Teoretická východiska

V dnešní době jsou počítače zapojeny do většiny každodenních činností v životě lidí. Potřeba vhodného zabezpečení počítačových systémů se značně zvyšuje spolu se stále rostoucím významem počítačů v mnoha aplikacích [1]. V oblasti počítačové bezpečnosti je zásadním úkolem zabránit prohlížení, úpravě a kopírování citlivých dat.

Citlivé osobní údaje jsou podle GDPR [2] speciální kategorií, která zahrnuje údaje o rasovém či etnickém původu, politických názorech, náboženském nebo filozofickém vyznání, členství v odborech, o zdravotním stavu, sexuální orientaci a trestních deliktech či pravomocném odsouzení osob. Tyto údaje mohou subjekt údajů samy o sobě poškodit ve společnosti, v zaměstnání, ve škole či mohou zapříčinit jeho diskriminaci. Kategorie citlivých údajů GDPR nově zahrnuje genetické a biometrické údaje. Zpracování citlivých osobních údajů podléhá mnohem přísnějšímu režimu.

Při výběru bezpečnostní strategie je důležité si uvědomit principy metod, které nás provází po celou existenci lidské společnosti. Na jednu stranu můžeme jmenovat metody, které jsou přímo spojené s lidskou fyziognomií a odpovídají prvotnímu rozpoznání osob podle těla, obličeje, očí nebo hlasu. Tyto metody představují systém, který by dovolil detekci osob v relativně úzké skupině, kde každý každého zná. Má samozřejmě i své slabiny, například falešné paruky a vousy nebo dvojníky. Při srovnávání pouze jednoho fyziologického znaku může snadněji nastat chyba (například při srovnání jednoduchých znaků, jako je tvar obličeje). V případě snímání více než jednoho znaku nebo složitých znaků (duhovka nebo sítnice) může být zpracování pomalé a uživatelsky nepřívětivé.

Na druhé straně můžeme použít i některé vnější atributy, ať už je to formální oblečení (uniformy), pečetní prsteny nebo hesla. Tento systém má však velkou nevýhodu, že vnější atributy můžou být odcizeny neoprávněnou osobou, a to bez ohledu na to, zda se jedná o pečetní prsten nebo token[1].

Oba typy nevýhod můžeme minimalizovat použitím multifaktorové autentizace, díky které lze neoprávněný přístup vyloučit. Může se jednat například o kombinaci anatomických nebo behaviorálních charakteristik s vnějším atributem nebo heslem.

Biometrie, biometrická identifikace a verifikace jsou předmětem intenzivního výzkumu již od počátku 80. let minulého století. Na konci 20. století se díky rozvoji výpočetní techniky začaly masově nasazovat první rozsáhlé aplikace [4]. Behaviorální biometrie pro autentizaci uživatelů tvoří vznikající trend ve

[1]Token (bezpečnostní klíč) může být fyzické zařízení, které vlastní oprávněný uživatel počítačových služeb pro snadnou autentizaci [3].

výzkumu bezpečnosti IT. Dynamika stisku počítačových kláves je v současné době jednou z nejoblíbenějších biometrií pro autentizaci uživatelů, a to zejména díky její nízké ceně a možnosti nepřetržité kontroly [5]. Výzkum v této oblasti rychle roste také kvůli rostoucí poptávce po zabezpečeném přístupu k počítačům a jiným zdrojům.

Jednou z behaviorálních charakteristik, která se nabízí, je dynamika stisku počítačových kláves. Tato metoda může být velmi dobře používána ve spojení s dalšími autentizačními metodami, zejména s přihlašovacím jménem a heslem. Tato metoda ukazuje dle [5] kvalitní bezpečnostní výsledky. Jako příklad lze uvést produkt BioPassword [6] společnosti Net Nanny.

Monrose [7] se domnívá, že dynamika stisku počítačových kláves může být použita jako možný útok na PGP[2], protože se čísla použitá k inicializaci generátoru pseudonáhodných čísel vypočítávají z charakteristiky psaní uživatele. To může být nevýhoda, pokud jsou charakteristiky psaní uživatele známé [5].

Monrose [7] také uvádí, že mohou existovat určité rozdíly mezi leváky a praváky, nicméně vzorek leváků v jeho zkušební skupině je příliš malý na důkaz tohoto tvrzení [5].

Dalším ideálním využitím této metody je dynamické nebo průběžné sledování interakce uživatelů při přístupu k vysoce důvěrným dokumentům nebo plnění úkolů v prostředí, kde uživatel musí být „bdělý“ za všech okolností (např. řízení přístrojů na operačním sále, řízení letového provozu, atd.). Dynamika stisku počítačových kláves může být použita i k detekci netypického rytmu psaní u uživatele (způsobeného ospalostí, únavou apod.) a následnému informování třetí osoby [7].

[2]Pretty Good Privacy (PGP) je počítačový program, který umožňuje šifrování a ověřování. PGP je často používán pro podepisování, šifrování a dešifrování elektronické pošty (e-mailů) z důvodu zvýšení bezpečnosti e-mailových sdělení (viz [8]).

2.1 Identifikace a autentizace

V biomedicíně je potřeba chránit informace a data. Data v informatice jsou jednotlivé údaje zpracovávané počítačem [9]. Informace jsou data prezentovaná v takovém kontextu, který dává smysl a význam. Informace tedy slouží ke zpracování, skladování nebo přenášení dat [9].

Existují dvě nezbytné podmínky k zajištění toho, aby pouze oprávněná osoba mohla přistupovat k datům nebo je měnit [10]:

1. identifikace a
2. ověření osoby,

které společně zajišťují kontrolu přístupu k informacím.

Proces *identifikace* stanoví, kdo je daná osoba a probíhá při prvním přihlášení do systému, zatímco *ověřování* potvrzuje nebo popírá identitu dané osoby. To také vyžaduje stejný důkaz identity pro získání jistoty, že osoba je opravdu ta, za kterou se vydává [10].

Identita osoby je definována jako nezbytná podmínka bytí každé konkrétní osoby, nebo jako podmínka být sám sebou a nikým jiným. Lidská identita je kombinace biologických a psychických, vrozených i získaných, individuálních a specifických vlastností a schopností vnímat sám sebe. Identita je ztělesněním našeho vlastního já, z čehož logicky vyplývá, že každý z nás je identický (totožný) právě a jen sám se sebou [4].

Pojem identita znamená totožnost a k jejímu ověřování je zapotřebí [4]:

Identifikace uživatele – proces *určení identity* (totožnosti) uživatele. Může se jednat buď o udání identity samotným uživatelem, nebo se identifikující systém snaží určit identitu uživatele hledáním v předem daném množství uživatelů. Systém prochází buď databázi těžko podvrhnutelných záznamů všech uživatelů (biometrické informace) nebo databázi tajných informací (například identifikační kód).

Autentizace uživatele – proces *ověření identity* uživatele. Uživatel obvykle udá svou identitu (například přihlašovací jméno) a bezprostředně na to nějakým způsobem umožní její ověření.

Rozdíl mezi identifikací a autentizací lze nejlépe ilustrovat na příkladu biometrických veličin [4].

- Při autentizaci (verifikaci) se jedná o proces, při kterém subjekt předkládá tvrzení o své identitě (například zadáním identifikátoru nebo vložením

karty) a na základě takto udané identity se porovnávají aktuální biometrické charakteristiky s uloženými charakteristikami, které této identitě odpovídají podle záznamu v autentizační databázi.

- Při identifikaci (vyhledávání) naopak člověk identitu sám nepředkládá, systém prochází všechny relevantní záznamy v databázi, aby našel příslušnou shodu a identitu člověka sám rozpoznal.

Ověřovat však můžeme nejen identitu uživatelů, ale i původ dat, pak hovoříme o tzv. **autentizaci dat**. V tomto případě ověřujeme, zda jsou data platná, tj. že známe autora či odesílatele daných dat [4].

Dalším důležitým pojmem je **autorizace uživatele**, tj. proces přiřazení oprávnění (na základě identity a bezpečnostní politiky) pro práci v systému, který specifikuje, co daný uživatel může, případně nemůže v systému dělat. Jedná se o proces, který obvykle následuje po autentizaci [4].

2.1.1 Základní kategorie obecné identifikace

Aplikace systémů automatické identifikace můžeme rozdělit podle publikace [11] do několika základních kategorií:

1. *Záznam informací* – Informace je odvozena z činnosti a z identifikačních symbolů. Po záznamu informace nenásleduje bezprostředně další činnost. Informace vyplývající z přečtených identifikačních symbolů a výsledků dané činnosti je zaznamenávána a uložena pro budoucí použití.

2. *Identifikace a vyhledávání informací* – Informace je v této kategorii odvozena pouze z identifikačních symbolů a po jejím záznamu nenásleduje bezprostředně žádná další činnost. Kromě aktu vyhledávání informací není další činnost spojená přímo s požadavkem vyhledávání nositele informace i když může být nepřímým výsledkem získané informace. Zdroj informace je zcela obsažen v identifikačním symbolu, což tuto kategorii odlišuje od záznamu informace, kde zdroj informací zahrnuje symbol a související činnost.

3. *Identifikace a vyhledávání předmětů* – Tato kategorie je z hlediska společných charakteristik obdobná jako předcházející kategorie.

4. *Řízení a kontrola stavů* – Informace je v této kategorii odvozena pouze z identifikačních symbolů. Po záznamu informace se může uskutečnit činnost spojená s objektem identifikace.

5. *Sledování a řízení pracovních procesů* – Informace je v této kategorii odvozena z činnosti a identifikačních symbolů. Po záznamu informace se může uskutečnit činnost. Podstatné je to, že se jedná vždy o systémy automatické identifikace, které zahrnují vyhledávání, případně uložení informace s následnou řídící činností, která je bezprostředním a přímým výsledkem činnosti automatické identifikace.

6. *Identifikace, sledování a kontrola osob* – Informace v této kategorii může být odvozena buď pouze z identifikačních symbolů nebo ze symbolů činnosti. Po záznamu nebo vyhledání informace se může uskutečnit činnost, která se týká lidí. Do této kategorie patří například aplikace ve zdravotnictví určená pro sledování pohybu lidí v nemocnicích nebo při absolvování řady zdravotnických prohlídek či testů u specialistů na poliklinikách.

7. *Transakční procesy* – Informace v této kategorii může být odvozena buď pouze z identifikačních symbolů, nebo ze symbolů a činností. Po záznamu nebo vyhledání informace se může uskutečnit činnost, která se týká peněz nebo hodnot. Podstatné pro tuto kategorii je, že v průběhu procesu peníze nebo hodnoty mění svého majitele.

2.1.2 Identifikace uživatele

Slovo **identifikace** znamená důsledné rozlišování a exaktní ztotožňování nejrůznějších jevů a jejich projevů (důsledků), akce a činnosti, zájmy a potřeby, osoby, zvířata, předměty, různé materiály apod. [4]. Dle Raka [4] můžeme identifikaci chápat několika způsoby:

- Jako akt nebo proces prokázání nebo zjištění identity.
- Jako vyhodnocení identity jednoho objektu ve vztahu k dalším objektům.
- Jako akt nebo proces zjištění nebo prokázání existence konkrétní osoby.
- Jako akt nebo proces vyhodnocení, jehož cílem je stanovit, zda jsou porovnávané objekty identické nebo ne.

Identifikace je tedy proces porovnávání rozmanitých objektů na základě jejich shod nebo rozdílů ve vlastnostech, formách, umístěních, složení (struktuře), funkcích, projevech, významu nebo v čase, s cílem zjistit, zda se jedná nebo nejedná o shodné (identické) objekty [4].

Za podstatný rys identifikace musíme považovat rozhodování o shodě ve všech vlastnostech, vztazích, funkcích apod. Jde tedy o rozhodovací proces, který může

mít velmi rozmanitou povahu, tzn. že se nemusí jednat jen o empiricky ověřitelnou shodu [4].

Vzhledem k tomu, že osoba se v průběhu času mění (fyziologické změny – stárnutí, nemoci, váha, ale i duševní změny – psychický stav, znalosti), mění se i její identita. Ta musí být z tohoto důvodu určena pouze omezeným, ale plně dostačujícím množstvím identifikačních charakteristik (například otisky prstů, struktura DNA, atd.) [4].

Člověk může být subjektem i objektem identifikace, může identifikovat nejen entity ve svém okolí, ale i sebe samého. Identifikaci můžeme rozdělit na vnitřní a vnější [4]:

1. *Vnitřní identifikace osoby* (sebe identifikace) je nalezení a vnímání vlastní identity psychologické, filozofické, sociální apod.

2. *Vnější identifikace osoby* je stanovení fyzické (biologické) identity člověka. Vnější identifikace osoby je tedy jen souhrn některých dostupných technologických postupů, metod a algoritmů, při kterých vyhodnocujeme, porovnáváme, ztotožňujeme apod. určité vzájemně srovnatelné vnější lidské charakteristiky, které jsou pro tento účel jedinečné, neopakovatelné, mají dostatečnou vypovídací schopnost, jsou technicky proveditelné a přijatelné specialisty i laickou veřejností na základě vědeckých poznatků, aktů nebo některých interních předpisů.

2.1.3 Autentizace uživatele

Jak již bylo řečeno, autentizace je proces ověření identity uživatele služeb nebo původce zprávy. V podstatě existují tři způsoby, jak může být osoba systémem ověřena [7, 12]:

1. První metoda ověřování, na základě tzv. *znalostního faktoru*, je založena na něčem, co člověk zná, např. heslo nebo osobní identifikační číslo (PIN).

2. Druhá metoda ověřování, tzv. *vlastnický faktor*, je založena na něčem, co osoba má, např. magnetický proužek karty nebo tajný klíč uložený na čipové kartě.

3. Třetí způsob ověřování, tzv. *biometrický faktor*, je založen na tom, že člověk existuje jako měřitelná biologická nebo behaviorální charakteristika, která spolehlivě odlišuje jednu osobu od druhé a která může být použita k ověření nebo rozpoznání uváděné identity osoby.

Bezpečnostní opatření, která spadají do prvních dvou kategorií, jsou nedostatečná, protože vlastnictví nebo znalosti mohou být obelhány, aniž by na to někdo přišel – informace nebo věc může být od jeho právoplatného majitele získána vydíráním. Stále více se tak pozornost přesouvá k identifikaci pomocí biometrických technik, které jsou řešením pro více spolehlivý způsob identifikace. V dohledné budoucnosti sice tyto spolehlivější biometrické řešení neodstraní potřebu ID karet, hesel nebo PINů, ale budou poskytovat podstatně vyšší úroveň identifikace a odpovědnosti než hesla a karty samotné, a to zejména v situacích, kdy je bezpečnost prvořadá [7].

Multifaktorová autentizace je bezpečnostní systém, v němž je za účelem prokázání totožnosti a umožnění přístupu k systému použita více než jedna forma ověření. Jednofaktorová autentizace, naopak vyžaduje pouze uživatelské jméno a heslo [13].

V dvoufaktorové autentizaci je uživatel vybaven dvěma způsoby identifikace, z nichž jeden je typicky fyzický token (například karta) a druhý obvykle záznam v paměti (například bezpečnostní kód) [13].

Další metody ověřování, které mohou být použity v multifaktorové autentizaci, zahrnují biometrické ověřování jako otisky prstů, rozpoznávání duhovky, rozpoznávání obličeje a hlasové ověřování. Kromě těchto metod mohou být použity čipové karty a další elektronické zařízení společně s tradičním uživatelským jménem a heslem [13].

2.2 Biometrické charakteristiky

Ve smyslu identifikace a autentizace má biometrie několik výhod oproti tradičním bezpečnostním technikám. Běžně dochází k ověření totožnosti na základě něčeho, co někdo zná (např. heslo) nebo něčeho, co někdo má (např. token). Výhodou biometrie je především to, že ji nejde zapomenout, odcizit nebo nesprávně umístit [14].

Pro všechny biometrické systémy je podstatné to, že rozeznají živého člověka (viz [15]) a zahrnují jak fyziologické, tak behaviorální charakteristiky. Fyziologické vlastnosti jako například otisky prstů jsou relativně stabilní fyzikální vlastnosti, které jsou neměnné, aniž by došlo k poškození jednotlivce (viz [15]). Na druhou stranu, behaviorální charakteristiky mají určitý fyziologický základ, ale také odráží psychologické rysy člověka. Unikátní behaviorální charakteristiky, jako je intenzita a amplituda hlasu, způsob, jakým se podepisujeme, a dokonce i způsob, jakým píšeme na klávesnici, tvoří základ nestálých biometrických systémů [7].

Biometrické technologie jsou definovány jako „automatizované metody ověřování nebo rozpoznávání identity žijící osoby založené na fyziologických nebo behaviorálních charakteristikách“ [16]. Biometrické technologie získávají na popularitě, protože při použití ve spojení s tradičními metodami ověřování poskytují vyšší úroveň bezpečnosti.

2.2.1 Anatomicko-fyziologické biometrické charakteristiky

Mezi nejčastěji používané anatomicko-fyziologické biometrické charakteristiky v běžné praxi patří například otisky prstů a dlaní, geometrie tvaru ruky a snímání krevního řečiště dlaně nebo hřbetu ruky.

Dnes je komerčně dostupných několik zařízení na bázi těchto biometrických technik. Nicméně, některé z nasazených technik je snadné oklamat, zatímco jiné, jako rozpoznávání duhovky, jsou příliš drahé a pro uživatele nepříjemné [15].

2.2.1.1 Otisky prstů a dlaní

Otisky prstů a dlaní jsou založeny na unikátnosti obrazců papilárních linií. Miniaturizace snímacích prvků i speciálních procesorů umožnila rozšíření využití biometrické identifikace založené na daktyloskopických poznatcích i pro široké komerční využití.

V komerční sféře probíhá vyhodnocování otisků prstů trošku jinak než v kriminalistice. Jedná se hlavně o dva rozdíly. Prvním je to, že probíhá buď verifikace, tj. porovnávání 1:1, nebo srovnávání 1:N, kde N je velmi malé číslo

na rozdíl od rozsáhlých databází v kriminalistice. Druhým rozdílem je to, že algoritmus sám vyslovuje závěrečný verdikt, tj. povolit nebo zamítnout přístup danému uživateli. Jestliže je srovnání neúspěšné, žadatel má možnost pokus opakovat.

Mezi typické příklady použití biometrických aplikací v praxi patří autentizace osob pro přístup k výpočetním a komunikačním prostředkům, pro zvýšení ochrany identifikačních nebo platebních karet, při autentizaci vstupu do objektů nebo při ochraně drahých nebo nebezpečných zařízení před jejich neoprávněným použitím.

Při počítačovém zpracování otisků prstů pro komerční bezpečnostní účely můžeme rozlišit tři technologické fáze [17]:

1. snímání otisku prstu (nejrůznější technologie pro načtení biometrických dat a jejich převod do elektronické formy),

2. počítačové zpracování otisku prstu (technologické postupy pro odstranění šumu, nalezení charakteristických znaků a vznik šablon, algoritmy pro porovnávání načtených a uložených biometrických šablon) a

3. závěrečné vyhodnocení (formulace výsledku porovnání, tj. verifikace, autentizace či identifikace).

Snímání daktyloskopických otisků se dá rozdělit do dvou základních skupin, na klasické a bezprostřední:

1. *Klasické snímání daktyloskopických stop* se používá hlavně v kriminalistice, a tak se mu nebudeme podrobně věnovat. Jedná se o snímání otisků pomocí tiskařské černé barvy a daktyloskopické karty. Ta se pak naskenuje a uloží v elektronické podobě.

2. Pro aplikace komerčně-bezpečnostního charakteru je dnes běžnější používání *bezprostředního snímání daktyloskopických otisků*. Pod tímto pojmem rozumíme snímání otisků z přikládaných prstů nebo dlaní živých a bezprostředně přítomných osob k snímači (senzoru).

Interaktivní snímání otisků prstů, které je dnes často implementováno do nejrůznějších technických zařízení, je realizováno pomocí senzorů. Tyto senzory mohou být kontaktní nebo bezkontaktní a mohou pracovat na různých fyzikálních principech [18].

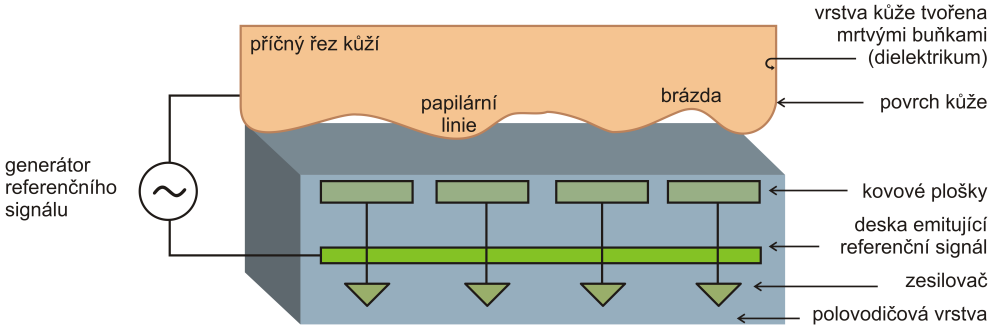
Kontaktní senzory pro snímání otisků prstů

Mezi kontaktní senzory patří senzory optické, elektronické, opto-elektronické, kapacitní, tlakové a teplotní. Některým typům těchto senzorů se budu v následujícím textu věnovat podrobněji.

Optické kontaktní senzory Optické senzory pracují na technologii FTIR (Frustrated Total Internal Reflection). Tato technologie funguje na principu, že laserový paprsek zespodu osvětluje povrch prstu, který se dotýká průhledné desky senzoru. Odrážený světelný tok je snímán CCD (Charge-Coupled Device) prvkem. Množství odraženého světla závisí na hloubce papilárních linií a brázd (výstupky a zářezy na prstu nebo dlani). Papilární linie odrážejí světlo více, brázdy méně.

Jiné optické snímače využívají hustý svazek optických vláken, které jsou postaveny kolmo k rovině snímací polohy senzoru. Zde se opět použije metoda osvitu a odrazu světelného toku. Dalším typem jsou pak senzory využívající technologii CMOS (Complementary Metal-Oxide-Semiconductor).

Elektronické kontaktní senzory Elektronické senzory pracují na principu vzniku elektrického pole mezi dvěma paralelními vodivými a elektricky nabitými deskami (viz obrázek 2.1). Pokud změníme původně plochý tvar horní desky na vlnitý (tvořený povrchem daktyloskopických papilár a brázd), změní se i tvar elektrického pole, který je na něm závislý. Horní desku elektronického senzoru tvoří povrch kůže, do které se přivádí řídící elektrický signál.



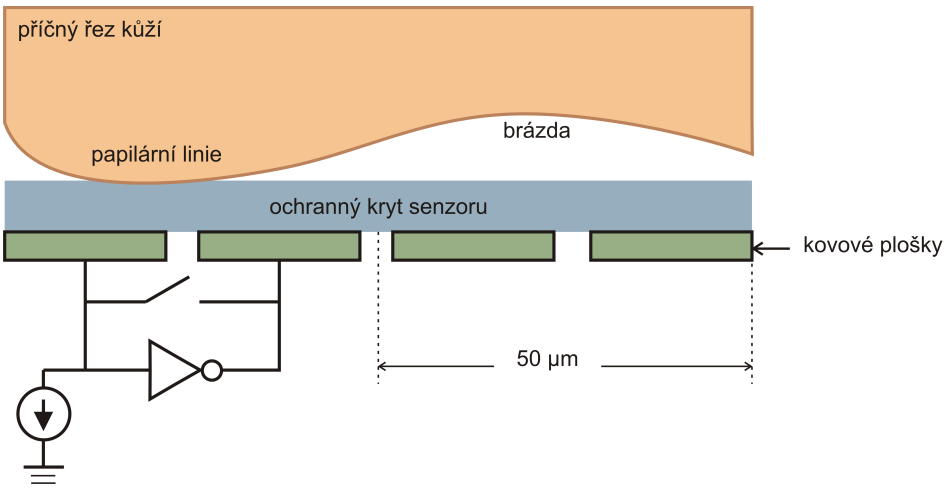
Obrázek 2.1: Zjednodušené schéma elektronických senzorů (podle [4]).

Výhodou tohoto senzoru je to, že nesnímá jen povrch kůže, ale proniká i hlouběji pod povrch. Tím se stává odolný vůči znečištění nebo poškození povrchu kůže.

Opto-elektronické kontaktní senzory Opto-elektronické senzory se skládají ze dvou základních vrstev. Horní vrstva je v kontaktu s kůží a je schopná emitovat světlo. To je zachyceno v druhé skleněné vrstvě, do níž jsou zataveny fotodiody. Ty převádějí světelný impuls na elektrický.

Kapacitní kontaktní senzory Kapacitní senzory snímají otisk prstu pomocí měření elektrické kapacity (viz obrázek 2.2). Snímací senzor je složen z velkého množství snímacích ploch, které jsou od sebe izolovány. Dotykem kůže papilární

linie přemosťují jednotlivé vodivé plošky v závislosti na papilární kresbě a brázdy se chovají jako izolant. Měří se napětí a kapacitní úbytky mezi jednotlivými vodivými ploškami. Tak vzniká digitalizovaný obraz papilární kresby. Tyto senzory jsou velmi náchylné na různé druhy znečištění, které může podstatně měnit vodivost kůže.



Obrázek 2.2: Zjednodušené schéma kapacitního snímače (podle [4]).

Tlakové kontaktní senzory Tlakové kontaktní senzory reagují na tlak papilárních linií na povrchu snímacího senzoru. Povrch senzoru je tvořen elastickým piezoelektrickým materiálem, který tlak transformuje na elektrický signál a vytváří tak daktyloskopický obraz.

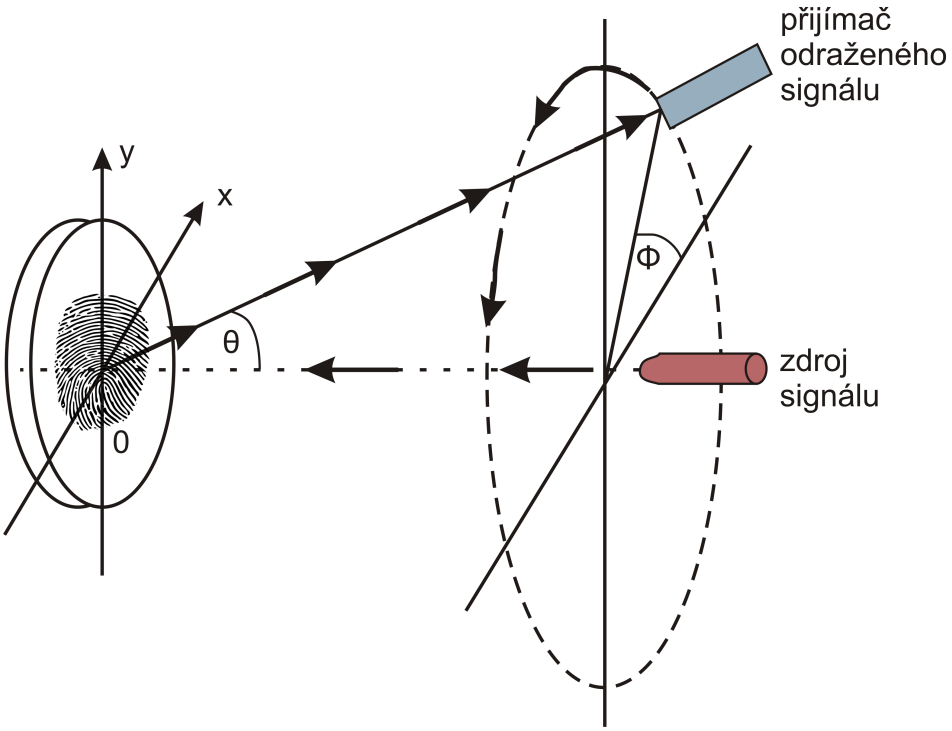
Teplotní kontaktní senzory Teplotní senzory reagují na teplotní rozdíly mezi papilárními liniemi a brázdami. Velkou výhodou tohoto senzoru je to, že teplota je důležitým faktorem, který může napovědět, zda snímaný otisk patří živé osobě.

Bezkontaktní senzory pro snímání otisků prstů

K nejznámějším skupinám bezkontaktních senzorů patří optické a ultrazvukové.

Optické bezkontaktní senzory Optické bezkontaktní senzory pracují na principu podobném dotykovým optickým senzorům, pouze s tím rozdílem, že světelný paprsek umožňuje snímat daktyloskopický otisk ze vzdálenosti 3 až 5 cm. Největší předností tohoto snímače je to, že zabraňuje jeho znečištění v důsledku dotyku špinavými prsty.

Ultrazvukové bezkontaktní senzory Ultrazvukové senzory jsou také založeny na principu podobném optickým, s tím rozdílem, že na povrch kůže dopadá namísto světelného paprsku svazek krátkých vln (viz obrázek2.3). Tento typ senzoru odstraňuje všechny nedostatky uvedené u předchozích typů senzorů [19].

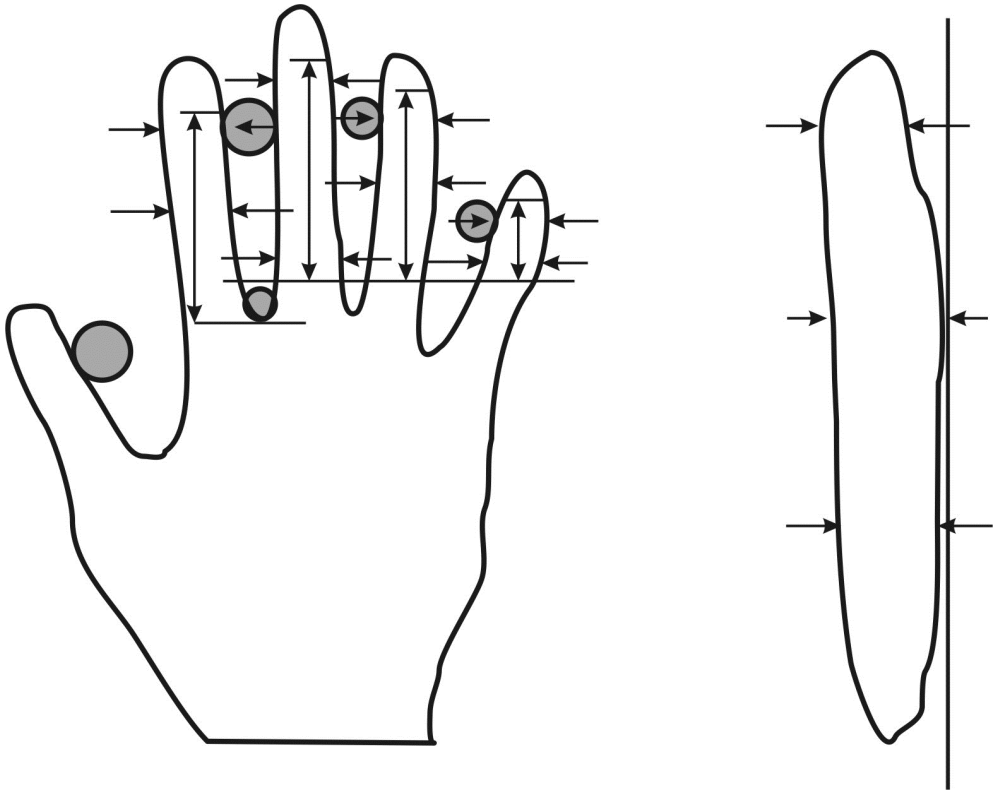


Obrázek 2.3: Zjednodušené schéma ultrazvukového senzoru (podle [4]).

2.2.1.2 Geometrie tvaru ruky

Další často používanou metodou je geometrie tvaru ruky, jejíž podstatou je měření délek nebo šířek prstů, kostí nebo kloubů ruky (viz obrázek 2.4). Tato metoda byla první, která byla použita na počítačovou verifikaci pro komerční účely [4]. Moderní trojrozměrné skenery snímají geometrické charakteristiky v desítkách bodů za sekundu. Ruka se přikládá na vodorovnou plochu skeneru, která má speciální fixační kolíčky, aby byla ruka přiložena vždy ve stejné poloze. Skener snímá jeden obraz shora kolmo na rovinu snímací desky a druhý z boku. Vzniknou dva černobílé snímky „siluety“ ruky.

Uživatel, který požaduje potvrzení své identity, zadá nejprve svůj identifikační kód (PIN) na klávesnici, nebo přiloží na čtečku magnetický proužek, čip nebo čárový kód ID karty. Následně přiloží ruku na stanovenou pozici podle vizuálního návodu, který je na každé klávesnici [20]. Skenery geometrie ruky jsou dnes již běžné v mnoha oblastech, včetně zdravotnictví [4].



Obrázek 2.4: Základní princip snímání geometrie tvaru ruky (podle [4]).

2.2.1.3 Snímání krevního řečiště dlaně nebo hřbetu ruky

Další metodou podobnou snímání geometrie ruky a vhodnou pro použití v počítačové bezpečnosti je snímání krevního řečiště dlaně nebo hřbetu ruky. Při této metodě se pomocí CCD kamer snímá specifický obraz cév na povrchu ruky. Jedná se o snímání celkového plošného obrazu rozložení všech cév v blízkosti povrchu hřbetu ruky.

Nespornou výhodou této metody je to, že zároveň ověřuje, zda je prověřovaný objekt živý. Snímání totiž probíhá v infračerveném pásmu, které je citlivé na teplotu. Cévy v těle jsou totiž teplejší než jejich okolí. Další zpracování nasnímaného obrazu je už pak podobné jako při otisku prstu (porovnávají se tvary cév). Další výhodou oproti snímání geometrie ruky je to, že není nutné ruku přikládat vždy ve stejné poloze.

Dalšími možnostmi u této metody je snímání krevního řečiště dlaně nebo bezkontaktní snímání (jak dlaně, tak hřbetu ruky), které zajišťuje vyšší čistotu senzoru a eliminaci přenosu některých onemocnění, na rozdíl od snímání geometrie ruky nebo kontaktního snímání otisků prstů [20].

2.2.1.4 Rozpoznávání obličeje a jeho částí

Namísto ruky může k identifikaci člověka posloužit například i jeho tvář nebo její část. Existují počítačové programy, které dokáží rozpoznávat lidské tváře podobně jako člověk. Rozpoznávání obličejů je v současnosti typické zejména pro kriminalistiku a existuje mnoho různých metod a algoritmů, které se pro tyto účely používají.

Velmi jednoduché může být i použití při zajišťování běžných výpočetních a telekomunikačních systémů. Na pořízení obrazu obličeje postačuje běžná videokamera, kterou má dnes již mnoho obrazovek integrovanou. Takto je vlastně klasické zadávání hesla nahrazeno pořízením snímku obličeje. Tento postup je velmi výhodný z hlediska toho, že není zapotřebí vůbec žádný přímý kontakt uživatele s čidlem [21].

V této oblasti však určitě výzkum není na konci. Rozpoznávání obličeje se dá ještě v mnoha směrech zdokonalovat. Jako příklad se dají uvést projevy emocí.

Zajímavou aplikací s ohledem na kontrolu bezpečnosti v IT by bylo průběžné snímání obličeje člověka při práci na počítači a vyhodnocování, zda s citlivými daty pracuje stále tatáž oprávněná osoba. Jiným příkladem by mohlo být zaznamenávání tváří všech, který se do daného systému nejen dostali, ale s ním i pracovali. (Někdo může nechat otevřenou aplikaci a na malou chvilku odejít, čehož může využít nepovolaná osoba.)

2.2.1.5 Snímání oční duhovky nebo sítnice

V poslední době se díky jednoduchému použití běžných videosystémů stává stále více rozšířenou metodou i snímání oční duhovky nebo sítnice. Rozpoznávání duhovky je možné bez ohledu na velikost, umístění a orientaci, ale je k tomu třeba složitý algoritmus [20].

Na zmapování krevního řečiště oční sítnice se používá světelný paprsek, jehož část sítnice pohltí a část odrazí. Speciální kamera potřebná pro snímání je poměrně drahá a samotné snímání není pro uživatele velmi příjemné (mnoho lidí se této technologie dokonce bojí) [20].

2.2.2 Behaviorální biometrické charakteristiky

Behaviorální biometrie má tu výhodu, že je méně obtěžující než ostatní biometrie a nevyžaduje na zachycení potřebných biometrických údajů speciální hardware [14]. Díky tomu je také levnější a jednodušší na použití.

Nejznámější příklady behaviorálních biometrických charakteristik jsou [22]:

- dynamika podpisu – měření kombinace vzhledu, tvaru, načasování a tlaku v průběhu psaní podpisu uživatelem,
- ověření hlasu – tón, intenzita a rytmus hlasu,
- dynamika pohybu myší – měření vzdálenosti, rychlosti a úhlu při práci s myší,
- dynamika stisku počítačových kláves – doba trvání každého stisku klávesy a doba mezi stisky kláves.

2.2.2.1 Dynamika stisku počítačových kláves

Dynamika stisku počítačových kláves je proces analýzy způsobu, jakým uživatel píše na klávesnici, sledováním vstupů na klávesnici tisíckrát za sekundu ve snaze identifikovat uživatele na základě navyklých vzorů psacího rytmu [7]. Již bylo prokázáno, že styl psaní na klávesnici je dobrým znakem pro určování identity [23].

Navíc na rozdíl od jiných biometrických systémů, jejichž implementace může být nákladná, programy zaznamenávající stisky počítačových kláves jsou téměř zdarma – jediným požadovaným hardwarem je klávesnice [7, 24].

Použití dynamiky stisku počítačových kláves pro zabezpečení přístupu do počítačů je relativně nové. Nicméně, Joyce a Gupta [23] již v roce 1990 předložili první komplexní přehled prací souvisejících s tematikou dynamiky stisku počítačových kláves obecně. Stručné shrnutí těchto prací a výzkumu, který byl prováděn, lze nalézt i v práce Monrose [7].

Techniky ověřování podle stisku počítačových kláves mohou být klasifikovány buď jako *statické* nebo *kontinuální* [7].

- *Statické ověřování* přístupu analyzuje dynamiku stisku počítačových kláves pouze v určité době, například v průběhu přihlašování. Statické přístupy poskytují silnější ověřování uživatele, než jednoduché heslo, ale neposkytují nepřetržitou bezpečnost – nemohou detekovat záměnu uživatele po prvotním ověření.
- *Kontinuální ověřování* naopak sleduje psaní uživatele v průběhu celé interakce s počítačem.

Dynamika stisku počítačových kláves umožňuje tzv. kontinuální (dynamické) ověřování, které je založeno na použití klávesnice jako prostředku průběžné interakce mezi uživatelem a počítačem [25]. To nabízí možnost průběžné kontroly

po celou dobu, kdy je počítač používán. Tato metoda je užitečná v situacích, pokud je ponechání počítače na chvíli bez kontroly riskantní [26].

Z dynamiky stisku počítačových kláves lze extrahovat několik typů parametrů [10, 15]:

- doba trvání stisku klávesy – viz obrázek 2.5,
- doba mezi stlačeními jednotlivých kláves – viz obrázek 2.5,
- rychlost stisku tlačítka,
- četnost chyb,
- styl psaní velkých písmen,
- umístění prstů a
- tlak, který člověk použije při stisku klávesy.

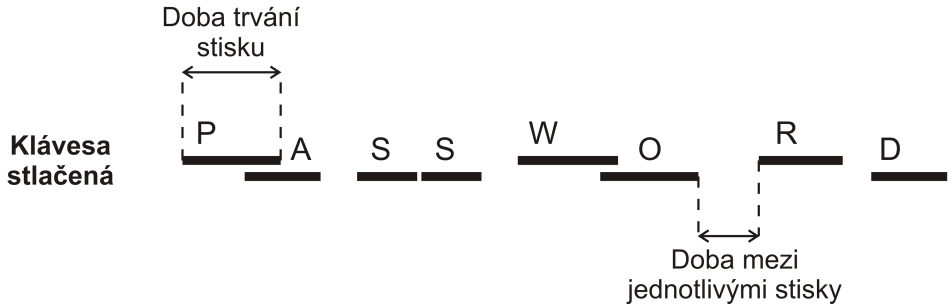
Obrázek 2.5: Doba trvání stisku a doba mezi jednotlivými stisky počítačových kláves.

Poslední zmíněný parametr vyžaduje speciální klávesnici, která umožňuje měřit sílu, která byla na stisk použita. Všechny ostatní metody mohou být hodnoceny pomocí speciálního programu bez jakýchkoliv modifikací hardwaru [7, 24].

Historii zkoumání dynamiky stisku počítačových kláves lze nalézt také v pracích Monrose [7], Joyce [23] nebo Boechat [10].

Charakteristiky psaní se můžou lišit i u jednoho uživatele a to s ohledem na to, jaký text píše. Velké rozdíly budou mezi charakteristikami při chatování s přáteli a programováním například v jazyce Java [27]. Při programování musí uživatel myslet, analyzovat a poté zadávat text, zatímco při chatování je situace jiná. Při programování se bude také používat více speciálních znaků, než při psaní formálního dopisu. Tato problematika je podrobně řešená v práci Barghouthi [27].

Při psaní uživatelského jména nebo hesla můžeme měřit tzv. **časový vektor** [28], který se skládá z časů trvání stisků kláves a časů mezi jednotlivými stisky [29]. *Doba trvání stisku* je doba, během níž je klávesa držena (viz obrázek 2.5 nebo 2.6), a *doba mezi jednotlivými stisky* je doba mezi uvolněním jedné klávesy a stlačením druhé (viz obrázek 2.5 nebo 2.6). Během rychlého psaní můžeme naměřit i zápornou hodnotu doby mezi jednotlivými stisky, a to v případě, že je další klávesa stlačena dřív, než je předchozí uvolněna [28] (viz obrázek 2.6). Obrázek 2.6 zobrazuje časový vektor zadaného hesla o osmi znacích. Tento časový vektor se skládá z osmi dob trvání stisku a sedmi intervalů mezi jednotlivými stisky (dva z nich jsou negativní).



Obrázek 2.6: Časový vektor odpovídající psaní hesla „password“.

Výhody dynamiky stisku počítačových kláves

1. Nejvyšším cílem použití dynamiky stisku počítačových kláves je schopnost neustálé kontroly totožnosti osoby v průběhu psaní na klávesnici [7, 25].
2. Ani přihlášení, ani ověření nemá vliv na pravidelný pracovní tok, protože uživatel bude stejně psát potřebný text. Snadné je také použití např. s přihlašovacím jménem a heslem během procesu přihlášení [5].
3. Na rozdíl od jiných biometrických systémů, programy zaznamenávající dynamiku stisku počítačových kláves jsou téměř zdarma. Jediným požadovaným hardwarem je klávesnice [7, 24].
4. Čas na školení uživatelů je minimální a snadnost použití je velmi vysoká [5].
5. Veřejná přijatelnost je velmi vysoká. U této metody neexistují žádné předsudky, jako v případě kriminalistického vzoru v ověření otisků prstů, nebo nepohodlí, jako u skenování sítnice [15].
6. Dynamika stisku počítačových kláves je ideální také pro uživatele počítačové sítě.

Nevýhody dynamiky stisku počítačových kláves

1. Dynamika stisku počítačových kláves je nestatická biometrie stejně jako například hlas. Může se měnit poměrně rychle v průběhu času, například při psaní jednou rukou (kvůli zranění) [7].
2. Nízká přesnost – dynamika stisku počítačových kláves je jedna z méně unikátních biometrik [5].
3. Malá komerční rozšířenost technologie [5].
4. Závislost na vlastnostech klávesnice, například na rozložení kláves. Někteří uživatelé mohou být zvyklí psát na běžné klávesnici, zatímco jiní používají notebook, kde bude psaní pravděpodobně velmi odlišné [30].
5. Psaní v cizím jazyce [27].

2.2.2.2 Dynamika pohybu myší

Zatímco autentizace pomocí dynamiky stisku počítačových kláves byla intenzivně studována v průběhu posledních třiceti let, dynamika pohybu myší si začala získávat zájem teprve v posledním desetiletí [14].

Dynamika pohybu myší popisuje chování jedince s pomocí polohovacích zařízení, jako je myš nebo touch-pad [14]. Podobně jako dynamika stisku počítačových kláves, ani dynamika pohybu myší nevyžaduje žádný speciální hardware pro sběr dat [31].

Dynamika pohybu myší je behaviorální biometrická charakteristika představena teprve nedávno [32]. Myšlenkou této biometriky je sledovat všechny akce myší generované v důsledku interakce uživatele s grafickým rozhraním, poté zpracovat získaná data s cílem analyzovat chování uživatele [32].

Akce myší lze zařadit do následujících čtyř kategorií [33]:

- pohyb myší – odpovídá obecnému pohybu,
- drag and drop – akce začíná tlačítkem myši dolů, následuje pohyb, pak tlačítko myši nahoru,
- point and click – pohyb myší následuje kliknutím nebo dvojklikem, a
- ticho – žádný pohyb.

Behaviorální analýza využívá neuronové sítě a statistické přístupy ke generování řady faktorů ze zachyceného souboru akcí. Tyto faktory jsou použity

k vytvoření tzv. MDS (Mouse Dynamics Signature, podpis pohybu myší). Jedná se o jedinečný soubor hodnot charakterizujících chování uživatele v průběhu monitorovacího období. Některé faktory se skládají z výpočtu průměrné rychlosti na ujeté vzdálenosti, nebo výpočtu průměrné rychlosti ve směru pohybu [32].

Při sběru akcí je třeba vzít v úvahu několik faktorů, které mohou ovlivnit přesnost analýzy biometrických vzorků získaných z pohybu myší. Tyto faktory jsou uvedeny níže [33]:

1. *Rozlišení obrazovky* – Pokud byly vzorky snímány při jiném rozlišení než je rozlišení obrazovky na které se provádí analýza, může to ovlivnit validitu výsledků.

2. *Rychlost kurzoru myši* – Jedná se o nastavení rychlosti a zrychlení kurzoru v operačním systému. Jakékoli změny provedené v těchto nastaveních mohou mít vliv na vypočtené hodnoty a také na chování samotného uživatele v souvislosti s myší jako vstupním zařízením.

3. *Nastavení tlačítek myši* – Za účelem dosažení reprodukovatelných výsledků by měla být konfigurace tlačítek myši stanovena pro každého uživatele stejně.

4. *Charakteristika hardware* – Faktory jako rychlost pracovní stanice, typ a rychlost vstupního zařízení můžou mít také vliv na proces sběru dat.

2.3 Srovnání biometrických metod

Většina současných systémů zabezpečení dat ověřuje oprávnění uživatele pro přístup do systému pouze v době přihlášení. V případě, že je otázka identifikace uživatele řešena pouze na základě biometrických údajů, je ve většině případů pro ověření použitý pouze jeden biometrický prvek (nebo jen některé z nich).

Řešení by mělo prioritně zahrnovat metody uvedené v úvodu a zdůraznit ty z nich, které se ukážou dlouhodobě stabilní nebo co nejméně obtěžující zdravotnický personál. Metoda musí být také pro uživatele dostatečně rychlá. Do úvahy se samozřejmě musí vzít i požadovaný výpočetní výkon a požadavky kladené na hardware.

Tabulka 2.1: Porovnání kontaktních a bezkontaktních senzorů otisků prstů.

Typ senzoru	**Výhody**	**Nevýhody**
Optický kontaktní	– velmi rychlý – uživatelsky přívětivý	– není odolný vůči nečistotám – není hygienický – nerozpozná živou tkáň
Elektronický kontaktní	– odolný vůči nečistotám – velmi rychlý – uživatelsky přívětivý	– není hygienický – nerozpozná živou tkáň
Kapacitní kontaktní	– velmi rychlý	– není odolný vůči nečistotám – nerozpozná živou tkáň – není hygienický
Teplotní kontaktní	– rozpozná živou tkáň – velmi rychlý	– není hygienický
Optický bezkontaktní	– odolný vůči nečistotám – hygienický – velmi rychlý	– nerozpozná živou tkáň
Ultrazvukový bezkontaktní	– odolný vůči nečistotám – hygienický – velmi rychlý	– nerozpozná živou tkáň

Tabulka 2.1 ukazuje hlavní výhody a nevýhody různých typů kontaktních a bezkontaktních senzorů pro snímání otisků prstů. Všechny senzory pro snímání otisků prstů jsou poměrně uživatelsky přívětivé a rychlé v porovnání s ostatními biometrickými metodami.

Hlavní rozdíly jsou v odolnosti vůči znečištění senzoru, což je důležité z následujících dvou důvodů:

1. Senzor by měl být schopen pracovat i v případě, že je na povrchu znečištěný nebo když je znečištěn povrch prstu, který je snímán.

2. Druhým důvodem je samozřejmě hygienické hledisko.

Největším přínosem je schopnost snímače odlišit živou tkáň od neživé nebo od syntetických materiálů. V tomto případě se senzor stává velmi odolným vůči možnému zneužití.

Tabulka 2.2 ukazuje hlavní výhody a nevýhody ostatních anatomicko-fyziologických a behaviorálních charakteristik. Kromě výše uvedených aspektů je zde porovnána také možnost průběžného ověřování, nutnost snímání ve stejné pozici (v tabulce 2.2 použita zkratka SP) a obtížnost/snadnost použití.

Tabulka 2.2: Porovnání anatomicko-fyziologických a behaviorálných biometrik.

Charakteristika	**Výhody**	**Nevýhody**
Geometrie tvaru ruky	– odolný vůči nečistotám	– nerozpozná živou tkáň – vyžaduje skenování ve SP – není hygienický
Bezkontaktní snímání krevního řečiště	– nevyžaduje skenování ve SP – rozpozná živou tkáň – hygienický – odolný vůči nečistotám	– bez možnosti průběžné kontroly
Snímání obličeje	– odolný vůči nečistotám – rozpozná živou tkáň – nevyžaduje skenování ve SP – s možností průběžné kontroly	– časově náročný
Snímání duhovky	– rozpozná živou tkáň – nevyžaduje skenování ve SP – uživatelsky přívětivý	
Snímání sítnice	– odolný vůči nečistotám – nevyžaduje skenování ve SP	– uživatelsky nepřívětivý – časově náročný
Dynamika stisku počítačových kláves	– uživatelsky přívětivý – s možností průběžné kontroly – nenáročný na hardware	

Tabulka 2.3: Porovnání metod z hlediska stability a časové náročnosti.

Metoda	**Stabilita**	**Časová náročnost**
	vysoká = více než 80 %, střední = více než 60 %, nízká = méně než 60 %	vysoká = více než 3 s, střední = méně než 3 s, nízká = méně než 1 s
Otisk prstu	střední	nízká
Geometrie tvaru ruky	střední	střední
Snímání krevního řečiště	střední	střední
Snímání obličeje	nízká	vysoká
Snímání duhovky	vysoká	střední
Snímání sítnice	vysoká	vysoká
Dynamika stisku PC kláves	nízká	nízká

Tabulka 2.3 porovnává vybrané metody z hlediska stability biometrických charakteristik a časové náročnosti. V tabulce jsou uvedené empirické odhady. Ukazuje se, že neexistuje žádná metoda, která by byla „ideální“, tzn., že by nabízela vysokou stabilitu biometrických charakteristik a nízkou časovou

náročnost. Skenování sítnice, které však není v současné době běžně používané, se tomuto ideálu blíží nejvíc.

2.3.1 Metriky pro srovnání aplikací využívajících dynamiku stisku počítačových kláves

Vzorky pro hodnocení jsou získávány od uživatelů, kteří zadávají své jméno nebo uživatelské jméno. Tyto vzorky jsou následně porovnány se vzorky získanými od ostatních uživatelů, kteří se snaží napodobit reálné uživatele zadáváním stejného jména nebo uživatelského jména [34].

Základem pro srovnání jsou pak dvě jednoduché metriky: **zamítnutí oprávněného uživatele** a **přijetí neoprávněného uživatele**.

Pro *míru odmítnutí oprávněných uživatelů* se používají následující metriky:

- FAR (False Alarm Rate) zastupuje počet vzorků oprávněných uživatelů zamítnutých autentizační metodou a je použita například v publikaci Brown a Rogers [34] nebo Lin [35].
- FRR (False Rejection Rate) je míra pravděpodobnosti, že biometrický bezpečnostní systém nesprávně odmítne přístupový pokus oprávněného uživatele a je použit například v publikaci Loy a kol. [36] nebo Cho a kol. [28].

Pro *míru přijetí neoprávněných uživatelů* se také používá několik metrik:

- IPR (Imposter Pass Rate) představuje počet vzorků neoprávněných uživatelů označených systémem za pravé a je použit například v publikaci Brown a Rogers [34] nebo Lin [35].
- FAR (False Acceptance Rate) je metrika použita například v publikaci Loy a kol. [36] nebo Cho a kol. [28]. FAR je míra pravděpodobnosti, že biometrický bezpečnostní systém nesprávně přijme pokus o přístup neoprávněného uživatele.

Různé biometrické systémy mají definované různé hodnoty prahu pro chybné přijetí (FAR) a chybné odmítnutí (FRR). Proto se zavedla další metrika – EER (Equal Error Rate) [36]. EER určuje bod, ve kterém se podíl chybných přijetí rovná podílu chybných odmítnutí. Čím je hodnota této proměnné nižší, tím je přesnost biometrického systému vyšší.

Existuje také další pohled a další terminologie pro měření chyb způsobených biometrickým systémem [27]:

1. FMR (False Match Rate) nastane, když biometrický systém určí dvě různé osoby jako jednu stejnou. Je zřejmé, že neoprávněný uživatel bude systémem chybně přijat.

2. FNMR (False Non Match Rate) nastane, když biometrický systém určí dva různé vzorky od stejné osoby jako vzorky pocházející od různých osob. Zde je pak legitimní uživatel systémem chybně odmítnut.

U těchto parametrů lze nastavit různou prahovou hodnotu v závislosti na použité aplikaci. Pro zajištění vysoké senzitivity metody, musí být většina neoprávněných uživatelů odmítnuta, a to i s vyšším rizikem odmítnutí skutečných uživatelů. Toto nastavení lze posunout pomocí vysoké citlivosti nebo vysoké specifičnosti pomocí křivky ROC. Bohužel různí autoři používají různé metriky pro určení autentizační chyby, a proto není možné porovnávat různé studie přímo na základě odhadů chyby při autentizaci.

2.3.2 Porovnání systémů založených na dynamice stisku počítačových kláves

Jak bylo ukázáno v části 2.2.2.1, existují dva typy ověřování na základě dynamiky stisku počítačových kláves: statické a kontinuální. V této oblasti existuje řada publikací, a to zejména na téma statického ověřování dynamiky statického stisknutí kláves. Nicméně je velmi obtížné tyto různé biometrické systémy porovnat, protože autoři používají různé přístupy k experimentálnímu nastavení systémů. Navíc autoři používají různé metriky pro počítání chyb, jak je vidět v kapitole 2.3.1.

V tabulce 2.4 je srovnání prací pro statické ověřování a v tabulce 2.5 pro kontinuální ověřování. Obě tabulky ukazují výsledky parametrů, které jsou v citovaných studiích uvedené. Většina prezentovaných prací byla realizována v rámci teoretického výzkumu a měla podobu „černé skříňky“, takže podrobný popis parametrů systémů zůstává obvykle neznámý. Různé studie se také liší v počtu jednotlivců ve studii nebo v délce hesla nebo psaného textu. Navíc je často nemožné opakovat výsledky v nezávislé studii.

2.3.2.1 Statické ověřování

Statické ověřování přistupuje k analýze charakteristik dynamiky stisku počítačových kláves pouze v určitých časech, například při přihlašování uživatele do informačního systému. Statické přístupy poskytují robustnější ověření uživatelů

než jednoduchá hesla, ale neposkytují nepřetržitou kontrolu – nemohou odhalit nahrazení uživatele po počátečním ověření jeho přihlášení.

Tabulka 2.4: Srovnání dynamiky stisku počítačových kláves – statické ověření.

	FAR	FRR	IPR	FAR	EER	FMR	FNMR
Araujo et al. [37]		1,45%		1,89%	1,60%		
Bergadano et al. [25]	4%		< 0,01%				
Bleha et al. [38]	3,10%		0,50%				
Bleha et al. [38]						2,80%	8,10%
Boechat et al. [10]		4,44%		0%			
Brown and Rogers [34]	4,20%		0%				
Loy et al. [36]					11,78%		
Cho et al. [28]					1%		
Furnell et al. [39]						8%	7%
Garcia et al. [40]	50%		0,01%				
Hocquet et al. [41]						0,50%	6%
Joyce and Gupta [23]	16,36%		0,25%				
Leggett et al. [42]	5,50%		5%				
Lin et al. [35]	1,10%		0%				
Monrose et al. [7]						0%	20,90%
Monrose et al. [7]						0%	14,40%
Monrose et al. [7]						0%	9,30%
Obaidat et al. [43]	0,00%		0%				
Rundhaug [44]						2,56%	10,26%
Shimshon et al. [45]		0%		3,47%			

Společným rysem analýzy dat je naučit se klasifikační pravidlo, které umožňuje identifikaci jednotlivce na základě dynamiky stisku počítačových kláves. Zpracovaná data tvoří obdélníkovou matici [46]. Řádky mohou odpovídat různým objektům (mohou to být např. sady zadaných hesel v určitém dni) a sloupce mohou odpovídat různým prozkoumávaným proměnným (např. doba mezi jednotlivými stisky, trvání úhozu). Data mohou být buď binární nebo reálná čísla (čas v mikrosekundách). Podle metodiky použité pro učení se ověřovacího pravidla, rozlišujeme mezi *statistickými přístupy* a *metodami strojového učení*.

Statistický přístup byl použit např. v pracích [7, 26, 38, 39, 41, 43]. Autoři studie [38] testovali normalizovaný Bayesovský klasifikátor a normalizovaný klasifikátor minimální vzdálenosti. Autoři [41] testovali statistické metriky (střední a standardní odchylka), rozdíl mezi dvěma vektory a časovou klasifikaci. Autoři modelu [7] testovali euklidovskou, neváženou pravděpodobnost a váženou pravděpodobnost. Autoři softwaru [43] testovali za velmi zvláštních podmínek: každý pravý uživatel pravděpodobně zadal své uživatelské jméno v řádu tisíců, aby si vytvořil svůj vlastní přihlašovací profil, zatímco útočník pouze 15-krát napsal stejný text. Dále autoři [26] a [39] testovali statistický přístup analýzy volného textu.

Pro řešení problému identifikace uživatelů pomocí jejich typických vlastností lze použít i různé typy **neuronových sítí**. Zhou [47] popsal neuronové sítě jako hlavní přístup v této souvislosti již v roku 1990.

Vícevrstvá neuronová síť s učícím algoritmem zpětného šíření chyby (backpropagation), která je použitá například v práci Akila a Suresh Kumar [1], se skládá z jedné vstupní vrstvy, jedné výstupní vrstvy a nejméně jedné skryté vrstvy [1, 34, 43]. *Kohonenova samoorganizační mapa*, používaná například v práci Brownem a Rogers [34], je poměrně jednoduchá samoorganizační neuronová síť. Skládá se ze dvou vrstev, vstupní vrstvy a vrstvy Kohonen. *Counterpropagation* je hybridní síť, kterou vyvinul Robert Hecht-Nielsen, a který používá ve své studii například Obaidat [43]. Nejjednodušší verze této sítě se skládá ze dvou vrstev. První vrstvou je vrstva Kohonen učená v režimu bez dozoru. Druhá vrstva je jednotka outstar, nazývaná také Grossbergova vrstva. Vícevrstvá neuronová síť s učícím algoritmem zpětného šíření chyby *(backpropagation) s adaptivní dynamikou* je používaná například v práci Lin [35]. Výhodou této sítě je, že má změnitelný počet vstupních uzlů.

Všechny zmíněné typy neuronových sítí budou popsány v kapitole 2.4.

2.3.2.2 Kontinuální ověřování

Kontinuální ověřování, na rozdíl od statického ověřování, monitoruje chování uživatele při psaní po celou dobu interakce s klávesnicí.

Tabulka 2.5: Porovnání dynamiky stisku počítačových kláves – kontinuální ověřování.

	FAR	FRR	IPR	FAR	EER	FMR	FNMR
Dowland et al. [48]						4,90%	0%
Furnell et al. [39]						15%	0%
Gunetti et al. [26]	$< 5\%$		$< 0{,}005\%$				

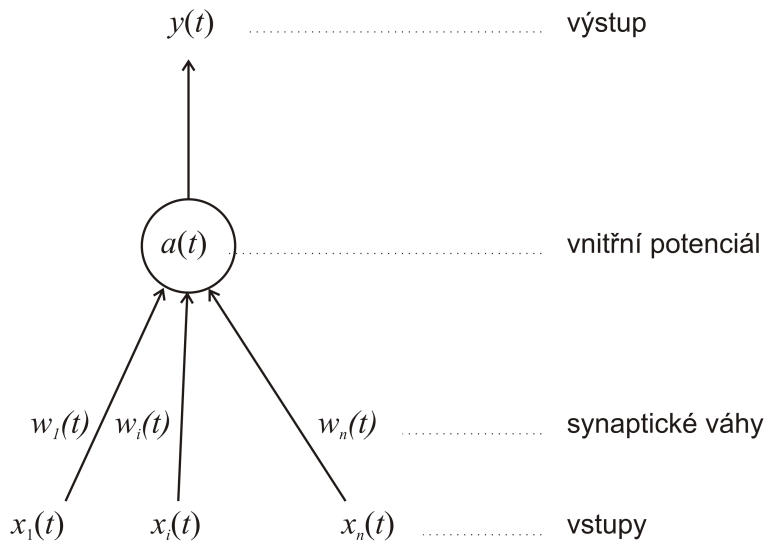
2.4 Neuronové sítě pro dynamiku stisku počítačových kláves

2.4.1 Základy neuronových sítí

Neuronová síť je jeden z výpočetních modelů používaných v umělé inteligenci. Jejím vzorem je chování odpovídajících biologických struktur: neuronu, nervové soustavy a mozku [49]. Skládá se z umělých (nebo také formálních) neuronů, jejichž předobrazem je biologický neuron. Neurony jsou vzájemně propojeny, předávají si signály a transformují je pomocí určitých přenosových funkcí. Neuron má libovolný počet vstupů, ale pouze jeden výstup [49].

2.4.1.1 Matematický model neuronu a neuronové sítě

Základem matematického modelu neuronové sítě je formální neuron, který získáme přeformulováním zjednodušené funkce neurofyziologického neuronu do matematické řeči [49]. Jeho struktura je schematicky znázorněna na obrázku 2.7 [49].

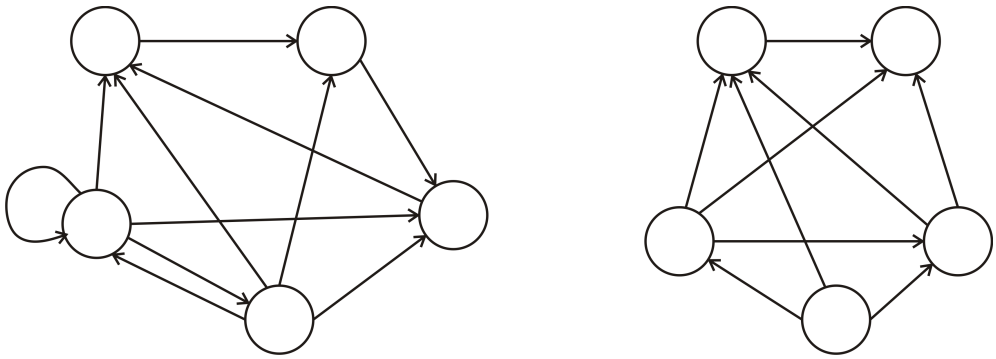


Obrázek 2.7: Matematický model formálního neuronu (podle [49] a [50]).

Matematický neuron je podle [50] jednotka mající n vstupů a jeden výstup. Hodnoty jeho vstupů jsou definovány vstupním vektorem $\mathbf{x}(t) = (x_1(t), \ldots, x_n(t))$ a výstup skalární funkcí $y(t)$. Neuron je v čase t ve vnitřním stavu charakterizován funkcí $a(t)$, která vyjadřuje stupeň elektrické aktivity (excitace) neuronu. Každý vstup neuronu $x_i(t)$ přispívá k excitaci neuronu určitým příspěvkem. Velikost

tohoto příspěvku je dána jednak hodnotou $x_i(t)$ a jednak reálným číslem $w_i(t)$, tzv. váhou vstupu. Váha vstupu modeluje vlastnosti synapse, přes kterou je vstup k neuronu připojen. Excitačním synapsím odpovídají kladné váhy, inhibičním synapsím záporné váhy. Váhy vstupů se obvykle popisují vektorem $\mathbf{w}(t)$.

Pokud mezi sebou vzájemně propojíme dva nebo více neuronů, dostaneme neuronovou síť. Neurony se mezi sebou propojují tak, že výstup neuronu je spojen se vstupem stejného nebo jiného neuronu. Obvykle je neuron propojen s více neurony najednou. Počet neuronů sítě a způsob propojení mezi nimi určuje tzv. *topologii (architekturu) neuronové sítě*. Graficky lze topologii neuronové sítě vyjádřit orientovaným grafem, jehož uzly reprezentují jednotlivé neurony a hrany vzájemná propojení neuronů (viz obrázek 2.8) [50]. Stavy všech neuronů v síti určují tzv. stav neuronové sítě a synaptické váhy všech spojů představují tzv. konfiguraci neuronové sítě [49].



Obrázek 2.8: Příklad cyklické (vlevo) a acyklické (vpravo) architektury neuronové sítě (podle [49]).

Neuronová síť se v čase vyvíjí, mění se propojení a stav neuronů, adaptují se váhy. V souvislosti se změnou těchto charakteristik v čase je účelné celkovou dynamiku neuronové sítě rozdělit do do tří dynamik a uvažovat pak tři režimy práce sítě [49]:

1. **Organizační dynamika** specifikuje architekturu sítě a její případnou změnu. *Změna topologie* se většinou uplatňuje v rámci adaptivního režimu tak, že síť je v případě potřeby rozšířena o další neurony a příslušné spoje. Rozlišujeme zde v zásadě dva typy architektury [49]:

   (a) *Cyklická (rekurentní) topologie* – v síti existuje skupina neuronů, která je zapojena v kruhu (viz obrázek 2.8).

   (b) *Acyklická (dopředná) topologie* – v síti neexistuje cyklus a všechny cesty vedou jedním směrem (viz obrázek 2.8). U acyklické neuronové sítě lze neurony rozdělit do tzv. vrstev, které jsou uspořádány tak, že spoje mezi neurony vedou jen z nižších vrstev do vyšších a obecně

mohou přeskočit jednu nebo více vrstev [49]. Speciálním případem takové architektury je tzv. **vícevrstvá neuronová síť**.

2. **Aktivní dynamika** specifikuje *počáteční stav sítě a způsob jeho změny* v čase při pevné topologii a konfiguraci. Podle toho, zda neurony mění svůj stav nezávisle na sobě nebo je jejich aktualizace řízena centrálně, rozlišujeme *asynchronní* a *synchronní* modely neuronových sítí [49].

3. **Adaptivní dynamika** specifikuje *počáteční konfiguraci sítě a jakým způsobem se mění váhy v síti* v čase. Všechny možné konfigurace sítě tvoří tzv. váhový prostor sítě [49]. Cílem adaptace je nalézt takovou konfiguraci sítě ve váhovém prostoru, která by v aktivním režimu realizovala předepsanou funkci. Adaptivní režim tedy slouží k „učení“ této funkce. Existují dva základní způsoby učení [50]:

   (a) *Učení s učitelem*, kde adaptivní mechanismus informuje vzorové vstupy sítě o správném výstupu sítě.

   (b) *Učení bez učitele* znamená, že učitel není k dispozici, tzn. že tréninková množina obsahuje jen vstupy sítě. Tomuto typu adaptace se říká také *samoorganizace*.

Neuronové sítě často obsahují velké množství parametrů a v důsledku toho mohou trpět přeučením [51]. Problémem stále zůstává, jak proti přeučením bojovat, když se neuronová síť naučí pravidlo s využitím příliš speciálních vlastností trénovacích dat [52]. Mezi možné prevence patří regularizace [53] nebo křížová validace [54].

2.4.1.2 Vícevrstvé neuronové sítě

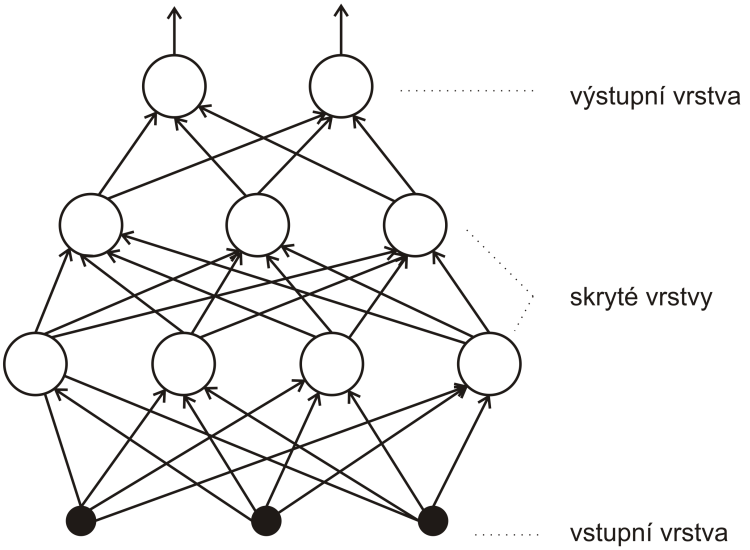
Vícevrstvá neuronová síť (viz obrázek 2.9) se skládá z těchto vrstev neuronů [50, 49]:

1. vstupní vrstva (nultá, dolní) – tvořena vstupními neurony,

2. skryté (mezilehlé) vrstvy – jsou složeny ze skrytých neuronů,

3. výstupní vrstva (poslední, horní) – tvořena výstupními neurony.

Vrstvy ve vícevrstvé neuronové síti číslujeme od nuly, která odpovídá vstupní vrstvě. Tu potom nepočítáme do počtu vrstev sítě (např. dvouvrstvá neuronová síť se skládá ze vstupní, jedné skryté a výstupní vrstvy). V topologii vícevrstvé sítě jsou neurony jedné vrstvy spojeny se všemi neurony bezprostředně následující vrstvy (chybějící spoje lze chápat jako spoje s nulovými váhami) [49]. Sítě bez



Obrázek 2.9: Příklad topologie vícevrstvé neuronové sítě (podle [49]).

vnitřní vrstvy mají omezené schopnosti a proto se používají vícevrstvé sítě, jejichž neurony jsou navzájem propojeny pomocí hran [55].

Princip fungování vícevrstvého perceptronu je následující. Vstupní vrstva dostává vstupní údaje, jimiž jsou pozorovaná mnohorozměrná data. Každý neuron vnitřní vrstvy pak dostává mnoho vstupních signálů a vyhodnocuje je svým vnitřním vyvažovacím systémem. Každému propojení jednotlivého neuronu s neuronem z některé další vrstvy přísluší váha, regresní parametr, který může nabývat libovolných reálných hodnot. Váhy se určují v průběhu procesu učení. Neuronová síť přiřadí vstupům takovou hodnotu výstupu, která odpovídá hodnotě aktivační neboli přenosové funkce spočítané pro vstupní hodnoty přenásobené určitými vahami. Výstup je pak typicky zaslán jako vstup jinému neuronu. Výstupní vrstva vytváří konečný výstup [55].

2.4.2 Výběr neuronové sítě

V předchozích studiích (např. [4, 56, 57]) se používají různé typy neuronových sítí pro řešení problému souvisejícího s identifikací uživatele prostřednictvím biometrických charakteristik, například v oblasti analýzy obrazu (tj. identifikace na základě rozpoznávání obličejů) a charakteristiky psaní.

Neuronové sítě se často označují jako „černé skříňky“ s velkým množstvím parametrů, které nelze jednoznačně interpretovat. Pro nalezení jejich vhodných odhadů se vyžaduje hodně velký počet pozorování. U neuronových sítí nejsou k dispozici testy hypotéz o významnosti parametrů a navíc jsou vychýlené

v přítomnosti odlehlých hodnot. Proto je žádoucí odhadovat parametry odlišným, robustním způsobem [58].

V některých aplikacích vadí, že neuronovou síť nelze popsat jednoduchým modelem, na kterém lze interpretovat, které ze vstupů průkazně ovlivňují variabilitu odezvy. To je důvodem, proč neuronové sítě nejsou optimálními metodami například při klasifikaci, kde je postupně nahradila metoda *support vector machines*, popsaná v kapitole 3.1.3.

2.4.2.1 Zpětná propagace

Metoda zpětné propagace (back-propagation) je metoda pro odhad parametrů vícevrstvé neuronové sítě s učícím algoritmem zpětného šíření chyby používaná například v Akila a Suresh Kumar [1]. Tato neuronová síť se skládá z jedné vstupní vrstvy, jedné výstupní vrstvy a alespoň jedné skryté vrstvy [34, 1, 43].

Z obrázku 2.9 vyplývá, že se vždy mezi dvěma sousedními vrstvami nachází tzv. úplné propojení neuronů, tedy každý neuron nižší vrstvy je spojen se všemi neurony vrstvy vyšší. Algoritmus dopředného šíření (feedforward) signálu podle [59]:

1. Nejprve jsou neurony excitovány na odpovídající úroveň vstupní vrstvy.
2. Tyto excitace jsou pomocí vazeb přivedeny k následující vrstvě a upraveny (zesíleny či zeslabeny) pomocí synaptických vah.
3. Každý neuron této vyšší vrstvy provede sumaci upravených signálů od neuronů nižší vrstvy a je excitován na úroveň danou svou aktivační funkcí.
4. Tento proces probíhá přes všechny vnitřní vrstvy až k vrstvě výstupní, kde pak získáme excitační stavy všech neuronů.

K naučení neuronové sítě potřebujeme jednak trénovací množinu, která obsahuje prvky popisující řešenou problematiku, a dále pak metodu, která dokáže tyto vzorky zafixovat v neuronové síti formou hodnot synaptických vah.

Metoda, která umožňuje adaptaci neuronové sítě nad danou trénovací množinou, se nazývá *backpropagation*, což v překladu znamená metodu zpětného šíření. Na rozdíl od už popsaného dopředného chodu při šíření signálu neuronové sítě tato metoda adaptace spočívá v opačném šíření informace směrem od vrstev vyšších k vrstvám nižším [59].

Teď podle [59] popíšeme metodu zpětné propagace:

1. Nejprve vezmeme vektor jednoho prvku trénovací množiny, kterým excitujeme neurony vstupní vrstvy na odpovídající úroveň.

2. Již vysvětleným způsobem provedeme dopředné šíření tohoto signálu až k výstupní vrstvě neuronů.

3. Srovnáme požadovaný stav daný vektorem prvku trénovací množiny se skutečnou odezvou neuronové sítě.

4. Rozdíl mezi skutečnou a požadovanou odezvou definuje chybu neuronové sítě. Tuto chybu pak v určitém poměru vracíme zpět do neuronové sítě formou úpravy synaptických vah mezi jednotlivými vrstvami směrem od horních vrstev k vrstvám nižším tak, aby chyba při následující odezvě byla menší.

5. Po vyčerpání celé trénovací množiny, se vyhodnotí celková chyba přes všechny vzory trénovací množiny, a pokud je vyšší než požadovaná chyba, opakuje se celý proces znovu.

Exaktní definování metody zpětné propagace lze nalézt v [49, 50, 59].

Z hlediska klasifikace se požaduje, aby byly určeny počáteční odhady parametrů, tj. váhy jednotlivých uzlů neuronové sítě. Při dopředném průchodu sítí se postupně počítají váhy neuronů v dalších vrstvách, až je možné spočítat hodnotu výstupu a odtud i celkovou ztrátu, tj. klasifikační chybu nebo ztrátu při aproximaci funkce přes celou trénovací množinu dat. Snahou další iterace je pak tuto klasifikační chybu zmenšit. Proto metoda prochází celou síť zpětně a na základě hodnoty chyby upraví váhy pro jednotlivé uzly sítě. Používá se přitom optimalizační metoda největšího spádu. Celkově se tedy iterativně odečítá určitý násobek gradientu vah od počátečních vah [55, 60].

Parametrická zpětná propagace (dynamic backpropagation) je použita například v Lin [35]. Tato neuronová síť má proměnlivý počet vstupních uzlů.

2.4.2.2 Radial basis function network

Neuronové sítě typu RBF (radial basis function networks) jsou vhodné pro aproximaci neznámé nelineární funkce. Oproti vícevrstvému perceptronu se zde od vstupní vrstvy do skryté vnitřní vrstvy nepředávají původní vstupní data, ale míra vzdálenosti těchto dat od nějakého konkrétního bodu, která se nazývá radiální funkce. Typicky se používá jediná vnitřní vrstva a pro nalezení optimálních hodnot parametrů se používá analogie metody zpětné propagace. Tento typ sítě je pro vysoce dimenzionální data méně vhodný [61].

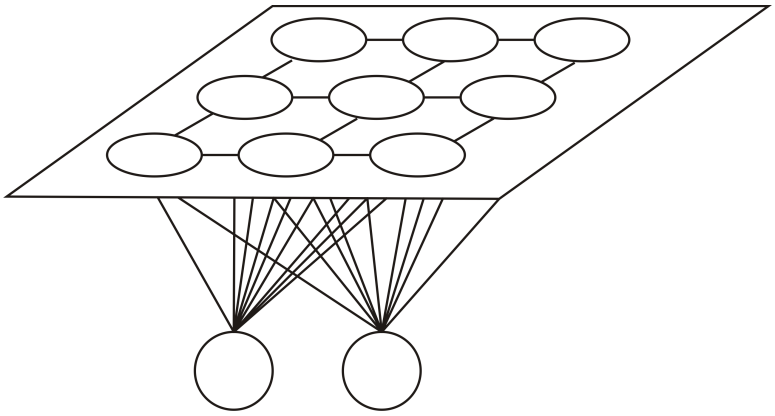
2.4.2.3 Samoorganizační mapy

Samoorganizační mapa (self-organizing map) je typ neuronové sítě, která hledá zobrazení mnohorozměrných dat obvykle do dvourozměrné mřížky se snadnou grafickou vizualizací. Schopností samoorganizace se zde rozumí, že jde o nesupervidovanou metodu. Metoda slouží jako nástroj pro exploraci a vizualizaci vysoce dimenzionálních dat, v nichž dokáže odhalit zákonitosti a souvislosti. Převádí tak složité nelineární vztahy z vysoce rozměrného prostoru do geometricky jednodušších vztahů [62, 63, 64].

Kohonenovy mapy používá Brown a Rogers [34] a jde o relativně jednoduché samoorganizující se mapy.

Kohonenova síť se skládá ze dvou vrstev neuronů [50]:

1. z vstupní vrstvy receptorů,
2. a z výstupní vrstvy neuronů.



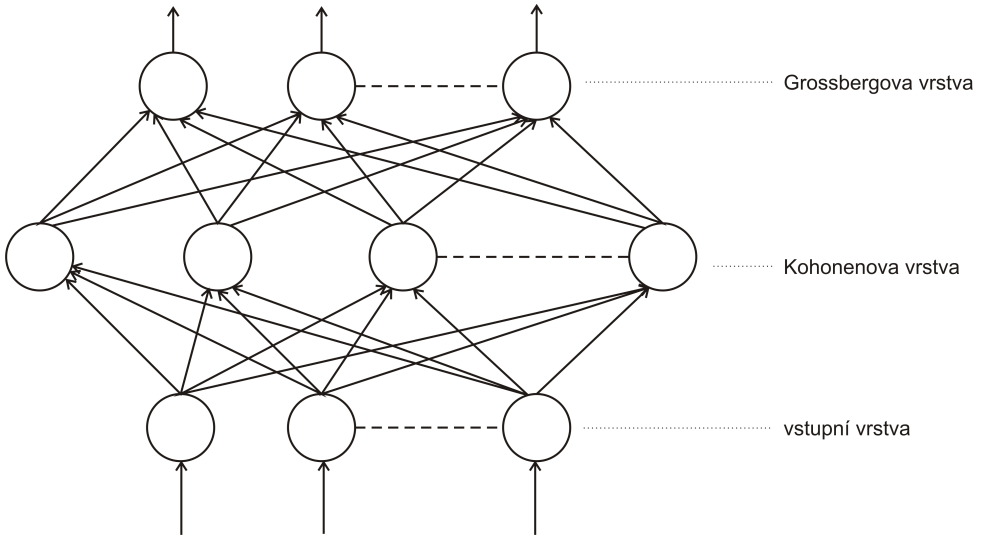
Obrázek 2.10: Příklad topologie dvoudimenzionální Kohonenovy mapy (podle [59]).

Výstupní neurony nemají fiktivní vstup. Výstup každého receptoru je propojen se všemi výstupními neurony. Kohonenova síť zobrazuje prostor hodnot vstupních vektorů do množiny výstupních neuronů. Při zobrazení by měla zachytit topologii a pravděpodobnostní distribuci vstupních dat [50].

Hlavní ideou těchto neuronových sítí je nalézt prostorovou reprezentaci složitých datových struktur. Tedy, aby třídy si podobných vektorů byly reprezentovány neurony blízkými si v dané topologii. Tímto způsobem je možné mnohorozměrná data zobrazit v jednodušším prostoru. Prvotní a nejčastější použití Kohonenova algoritmu je ve formě dvourozměrné implementace. Topologie takové sítě je zobrazena na obrázku 2.10 [59].

2.4.2.4 Counterpropagation

Counterpropagation, tzv. síť se vstřícným šířením při učení [65], je hybridní síť vyvinutá Robertem Hecht-Nielsenem a použitá například v Obaidat [43]. Nejjednodušší verze této sítě se skládá ze dvou vrstev. První vrstvou je Kohonenova vrstva učená v režimu bez dozoru. Druhá vrstva je tzv. Grossbergova hvězda. Topologii Grossbergovy hvězdy si lze představit jako vrstvu neuronů obklopujících jeden střed [59].



Obrázek 2.11: Příklad sítě counterpropagation (podle [65]).

Na obrázku 2.11 je znázorněna síť pouze s dopředným šířením. Tato síť má tři vrstvy:

1. vstupní,
2. vnitřní (Kohonenovu)
3. a výstupní (Grossbergovu).

Síť counterpropagation pracuje jako vyhledávací tabulka, která k danému vstupu najde nejbližšího reprezentanta a odpoví výstupní hodnotou, která je s tímto reprezentantem spojena [49].

2.4.3 Metoda GUHA

Metodu GUHA (General Unary Hypotheses Automaton) používanou v [46] lze transformovat a využít i pro dynamiku stisku počítačových kláves. GUHA je metoda automatického generování hypotéz založených na empirických datech, tedy způsob dolování dat [66].

Metoda pro výběr markerů (významných parametrů), představená v práci Šebesta a Straka [46], může být transformována a používána pro dynamiku stisku počítačových kláves. Vybrané markery (doba trvání stisku a doba mezi jednotlivými stisky) lze použít pro učení vícevrstvé neuronové sítě.

Metoda GUHA může být použita pro určení vztahů mezi experimentálními daty. Zpracovávané údaje tvoří obdélníkové matice [46]. Řádky mohou odpovídat různým objektům (např. sadě zadaných hesel za daný den) a sloupce mohou odpovídat různým zkoumaným proměnným (např. době trvání stisku nebo době mezi jednotlivými stisky). Data mohou být buď binární nebo mohou nabývat reálných hodnot[3] (čas v mikrosekundách). Podrobnosti o této metodě lze nalézt v [46].

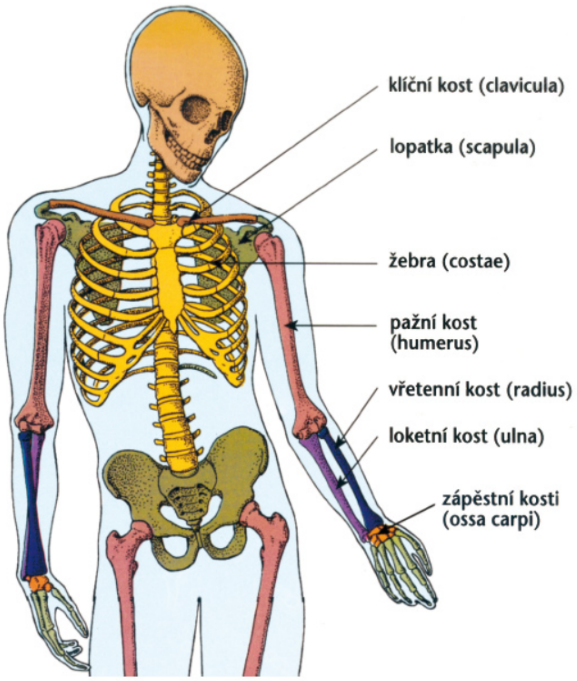
U psaní rukou i na klávesnici existuje podobná variabilita jako u řeči, dokonce i u stejného jedince/uživatele. Znamená to, že můžeme použít transformovanou vícevrstvou neuronovou síť prezentovanou v práci Tučková a Šebesta [67].

[3]V případě reálných dat odpovídající interval atributu musí být rozdělen do několika podintervalů a hodnota tohoto atributu je rovna jedné pouze v jednom příslušném podintervalu a hodnota je rovna nule ve všech ostatních podintervalech [46].

2.5 Pohybové ústrojí horní končetiny

Charakteristika písemného projevu ať již klasicky perem, tužkou nebo na klávesnici je v přímém vztahu k mikromotorice lidské ruky, která je tvořena jak pohybovým ústrojím ruky a paže (volné horní končetiny) tak jeho řízením centrální nervovou soustavou.

Centrální nervová soustava (CNS) je ústřední část nervové soustavy a spolu s periferními nervy hraje ústřední roli v řízení chování obratlovců. Skládá se z mozku a míchy. Mícha páteřní (medulla spinalis) je nervová trubice uložena v páteřním kanálku, předává informace do mozku a informace orgánům, je dlouhá 40-45 cm a vystupuje z ní 31 párů míšních nervů. Každý nerv obsahuje vlákna smyslová, motorická a některá vegetativní [68].



Obrázek 2.12: Kostra horní končetiny [69].

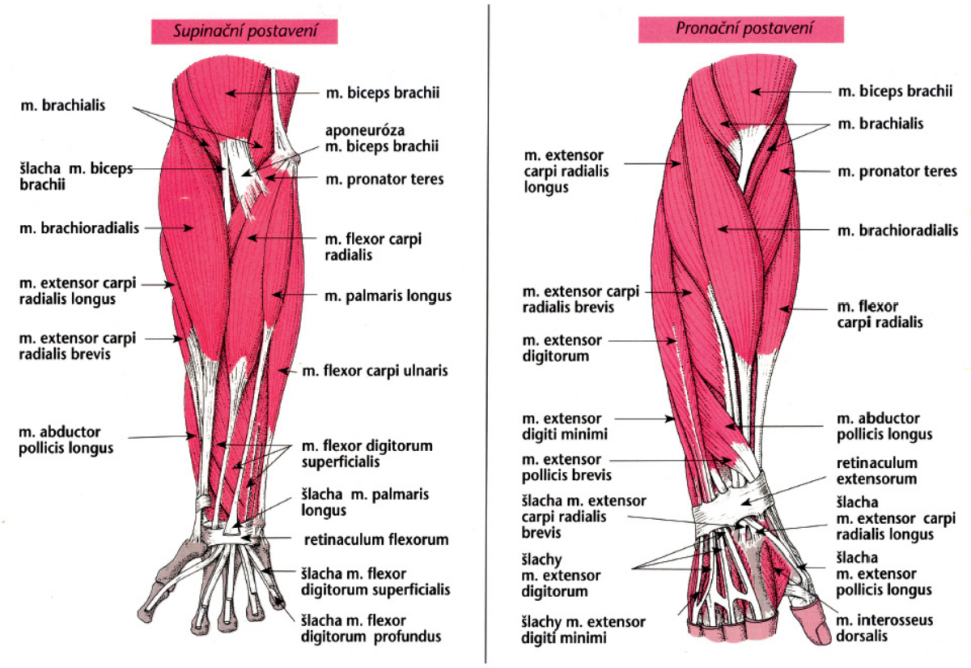
Během analýz chování psaní na klávesnici mne zaujal faktor únavy během opisování delšího textu. Tato únava je úzce spojená s přetěžováním pohybového aparátu ruky a předloktí. Jedná se zejména o přetížení z důvodu práce jednostranné a monotónní.

Z pohybového ústrojí horní končetiny bude z hlediska posouzení zátěže při psaní na klávesnici nejdůležitější částí kostra volné horní končetiny (ossa membri superioris liberi), která se skládá z kosti pažní (humerus), kosti vřetenní (radius) a kosti loketní (ulna). Dále pak kostra ruky, která se skládá z kosti zápěstní (ossa

carpi), kosti záprstní (ossa metacarpi) a z článků prstů (phalanges digitorum manus) [69] (viz obrázek 2.12).

Svaly horní končetiny (musculi extremitatis superioris) tvoří skupina svalů ramenních a lopatkových, svaly paže, skupina svalů předloktí a skupina svalů ruky. Z hlediska posouzení psaní na klávesnici je nejvíce zatížená skupina svalů předloktí a ruky.

Svaly předloktí se dělí dle funkce na přední skupinu s funkcí flexe prstů ruky a pronace předloktí, laterální skupinu s kombinovanou funkcí a dorzální skupinu rovněž s kombinovanou funkcí (viz obrázek 2.13) [69].



Obrázek 2.13: Svaly předloktí [69].

Protože výzkum v oblasti sledování charakteristik psaní textu pro účely zabezpečení dat se teprve otevírá a časově bude ještě náročný, zaujala mne aktuální možnost využití již připravených technologií a znalostí v praxi pro aktuálně řešený úkol z oblasti bezpečnosti práce pro stanovení lokální svalové zátěže. Proto následuje uvedení do této problematiky.

2.5.1 Lokální svalová zátěž

Lokální svalová zátěž je zátěž malých svalových skupin při výkonu práce končetinami. Při hodnocení lokální svalové zátěže se zjišťují a posuzují vynakládané svalové síly, počty pohybů posuzovaných pohybových struktur a pracovní polohy v závislosti na rozsahu statické a dynamické složky práce [70].

2.5.1.1 Základní pojmy

Mezi základní charakteristiky týkající se lokální svalové zátěže a jejího posuzování a hodnocení patří zejména posouzení dlouhodobosti a jednostrannosti práce, posouzení, zda je práce statická či dynamická a samozřejmě měření a hodnocení maximální svalové síly, procenta maximální svalové síly a průměrné celosměnové svalové síly [70].

Kritérium dlouhodobosti – za dlouhodobost lze považovat dobu poškozování, která vylučuje vznik postižení úrazovým dějem.

Kritéria jednostrannosti a nadměrnosti – jsou posuzována vždy ve vzájemné souvislosti. Vypovídají o poměru vynakládaných svalových sil k jejich časovému průběhu z hlediska zátěže stejných pohybových struktur.

Maximální svalová síla (Fmax) – je síla, které je vyšetřovaná osoba schopna dosáhnout při maximálním úsilí, vynakládaném konkrétními svalovými skupinami. Vyjadřuje se ve fyzikálních jednotkách (N).

Procento maximální svalové síly (%Fmax) – udává poměr vynakládané svalové síly k hodnotě Fmax, přičemž Fmax odpovídá 100 %.

Průměrná svalová síla celosměnová (v %Fmax) – vyjadřuje v relativních hodnotách průměrnou směnovou časově váženou hodnotu %Fmax v průměrné směně. Za průměrnou směnu se pokládá osmihodinová směna, která probíhá za obvyklých pracovních podmínek, při níž doba výkonu práce jednotlivých pracovních operací odpovídá skutečné míře zátěže.

Svalová práce dynamická – je práce, při níž převažuje isotonická kontrakce zapojených svalových skupin, kdy vynakládaná síla je po době kratší než 3 sekundy vystřídána relaxací.

Svalová práce statická – je práce, při níž převažuje izometrická kontrakce zapojených svalových skupin, tj. kontrakce s délkou trvání delší než 3 sekundy.

Fyzická síla žen je o třetinu menší než fyzická síla mužů. Nejvyšší sílu mají muži kolem 25 let věku, pak dochází k postupnému úbytku síly v pětiletém období o 2,5 % a to 45 let, pak je úbytek rychlejší, kolem 5 % v pětiletém období. Biologická tolerance pohybového aparátu s věkem klesá, nadměrné jednostranné přetěžování k hranici biologické tolerance může po určité době překročit toleranci tkáně.

2.5.1.2 Zásady postupu pro měření a hodnocení lokální svalové zátěže

Při měření a hodnocení musí být provedeno následující:

1. Podrobná analýza pracovních podmínek – zahrnuje popis práce a sledování časových faktorů práce, režim práce a odpočinku v průběhu průměrné směny, týdne event. roku, rozbor časových faktorů u jednotlivých prováděných pracovních operací (délka trvání úkonů, doba relaxace, apod.), podíl zátěže u jednotlivých svalových skupin, posouzení statické a dynamické složky práce, plnění norem, výskyt pracovních úkonů s vysokou silovou zátěží, výskyt podmíněně přijatelných a nepřijatelných pracovních poloh, popis pracovního místa aj.

2. Hodnocení časových faktorů práce – časový snímek pracovního dne se pořizuje k tomuto účelu metodou nepřerušovaného pozorování a zaznamenávání veškeré spotřeby pracovního času během směny. Zaznamenává se postupný čas s přesností na minuty a doba trvání jednotlivých pracovních úkonů a operací v průměrné směně.

3. Popis a posouzení pracovního místa – zaměřujeme se především na manipulační rovinu a pohybový prostor, ovládací prvky stroje nebo technického zařízení (sdělovače, ovladače), dosahové vzdálenosti, pracovní nástroje a nářadí, ručně manipulovaná břemena aj.

4. Popis a hodnocení pracovních poloh – provedeme biomechanickou analýzu výskytu podmíněně přijatelných a nepřijatelných pracovních poloh při práci, posouzení vhodnosti základní zvolené pracovní polohy, v případě použití jiné metody než integrované elektromyografie posouzení poloh horních končetin při práci.

Před měřením musí být určeny osoby, na kterých bude měření prováděno. Ty musí být zapracované (minimálně 3 měsíce hodnocenou práci rutinně provádějí) a musí být schopny spolupracovat při měření. Výběr osob se provádí v závislosti na účelu měření. Pro šetření nemoci z povolání je měření prováděno na alternující osobě věkově a konstitučně odpovídající šetřenému pacientovi. Při měření ke kategorizaci prací je třeba provádět minimálně na 2 zapracovaných osobách.

Hygienické limity jsou odlišné pro ženy a muže a jsou postaveny pro průměrného pracovníka ve věku cca 40 let.

Měření nebo hodnocení má probíhat za běžných provozních podmínek tak, aby byly proměřeny všechny pracovní úkony a operace, které pracovník v průměrné

směně provádí. Následně je provedeno časové vážení na průměrnou pracovní směnu.

2.5.1.3 Interpretace výsledků měření lokální svalové zátěže

Zjišťujeme, zda:

1. se jedná o práci s převahou statické nebo s převahou dynamické složky
    - práce s převažující statickou složkou zátěže – úkony, při kterých svaly ruky a předloktí setrvávají v izometrické kontrakci[4] po dobu delší než 3 s), takové úkony musí být ve směně déle než polovinu pracovní doby
    - práce s převažující dynamickou složkou zátěže – ve směně nepřevažují úkony se statickou složkou zátěže,
2. v průběhu směny nedochází k překračování limitních hodnot vynakládaných velkých svalových sil
    - limitní hodnoty pro práci dynamickou – nad 55 % Fmax (mohou být v osmihodinové směně 600krát za směnu), síly nad 70 % Fmax (nadlimitní svalové síly) se jako pravidelná součást výkonu práce nesmí vyskytovat.
    - limitní hodnoty pro práci statickou – svalové síly nad 45 % Fmax (nadlimitní svalové síly) se jako pravidelná součást výkonu práce nesmí vyskytovat,
3. hodnota celosměnového časově váženého průměru vynakládaných svalových sil nepřesahuje limitní hodnoty
    - celosměnový časově vážený průměr vynakládaných svalových sil nesmí překročit u práce s převahou dynamické složky hodnotu 30 % Fmax
    - celosměnový časově vážený průměr vynakládaných svalových sil nesmí překročit u práce s převahou statické složky hodnotu 10 % Fmax,
4. celosměnový počet pohybů rukou a předloktí nepřekračuje daný hygienický limit a to s ohledem na velikosti průměrných směnových vynakládaných svalových sil

[4]Izometrická kontrakce je svalová činnost, při které se nevykonává pohyb a vzdálenost začátků od úponů svalu se nemění. Při této činnosti se nemění délka svalu, ale mění se napětí. Dynamická kontrakce (izotonická) je svalová činnost, při které se mění vzdálenost začátků a úponů svalu a napětí ve svalu je přibližně během celé činnosti stejné. Podle změny délky svalu rozeznáváme koncentrickou (zkrácení svalu) a excentrickou (natažení svalu) kontrakci. Koncentrická kontrakce vyvolává zrychlení pohybu (akceleraci), zatímco excentrická zpomalení pohybu (deceleraci) [71].

- četnost pohybů ruky a předloktí za směnu nesmí překročit hodnotu 27 000 pohybů
- pro každou průměrnou směnovou časově váženou hodnotu vynakládaných svalových sil je dána limitní hodnota počtu pohybů za směnu, tato hodnota nesmí být překročena.[5]

Součástí protokolu z měření lokální svalové zátěže metodou iEMG jsou přílohy, které jsou tištěny z hodnotícího EMG softwaru. Obsahují průměrné časově vážené hodnoty %Fmax pro časové úseky dle časového snímku, pro jednotlivé pracovní operace a dále celosměnovou časově váženou hodnotu %Fmax pro jednotlivé hodnocené svalové skupiny. Dále obsahují tabulky s výsledky frekvenční analýzy pro jednotlivé pracovní operace a po časovém vážení na průměrnou směnu.

Při použití metody výpočtovou metodou musí být součásti protokolu i výpočty průměrné směnové časově vážené hodnoty a frekvence vynakládaných svalových sil.

[5]Pro počítání pohybů existuje obecné pravidlo uplatňované i v ostatních zemích EU. Podle tohoto pravidla pohyb nastává vždy, kdy hodnocená část těla změní směr nebo dochází ke změně zrychlení. Počet pohybů se nerovná počtu úkonů, např. na jeden zdvih jsou počítány dva pohyby.

3. Použité metody zkoumání

3.1 Klasifikační metody

Pro analýzu dat byla použita klasická klasifikační metoda – lineární diskriminační analýza (LDA) a několik moderních klasifikačních metod. Jedná se o regularizovanou diskriminační analýzu (RDA) [72], klasifikační strom [73], náhodné lesy [74], lineární metodu SVM (support vector machines), které používají funkci Gaussian radial base jako funkci jádra (nelineární SVM) [75]. Z těchto metod lze za spolehlivé pro vysokorozměrná data považovat pouze metody RDA a SVM klasifikátor [76]. Na druhou stranu SVM vyžaduje velký počet pozorování, aby se zjistily optimální hodnoty neznámých parametrů. RDA je pak jednou z nedávno navržených verzí LDA, přizpůsobených situaci s malým počtem pozorování [76].

Diskriminační analýza je jednou z nejstarších technik vícerozměrné analýzy dat. Tato metoda umožňuje umožňuje rozlišit jednotlivé případy dle měřených charakteristik do dvou a více skupin.

3.1.1 Diskriminační analýza

Diskriminační analýza je klasifikační technika, jejímž účelem je přiřadit jednotlivé vybrané objekty z určitého vzorku do jedné nebo více skupin na základě jejich charakteristických vlastností. Obecným cílem je pak nalézt a analyticky vyjádřit takovou hranici (diskriminační funkci), která by co nejvíce rozlišovala mezi jednotlivými skupinami.

Aplikaci diskriminační analýzy potom můžeme rozdělit do čtyřech obecných kroků [72]:

1. V prvním kroku určujeme základní objekty, na kterých budeme diskriminační analýzu provádět.

2. Druhým krokem je přiřazení jednotlivých objektů k vybraným skupinám. Tyto skupiny jsou vlastně nezávislé proměnné a musejí být přesně definovány před samotnou aplikací diskriminační analýzy.

3. Třetím krokem je určení charakteristických rysů společných pro všechny objekty, tzv. nezávislých proměnných, tak, aby co nejlépe určovaly prvky (objekty) v dané skupině.

4. Posledním krokem je pak, jak už bylo řečeno výše, najít a analyticky vyjádřit takovou funkci, která by co nejlépe obě skupiny oddělovala. Pokud předpokládáme, že obě skupiny jsou lineárně separovatelné, použijeme lineárně diskriminační analýzu, pomocí které vyjádříme diskriminační funkci jako lineární kombinaci jednotlivých charakteristických rysů. Pokud tedy budou rysy dva, bude diskriminační funkcí přímka, pokud budou tři, bude jí rovina, pokud více než tři, bude mezi jednotlivými subjekty rozlišovat nadrovina. Tato diskriminační funkce nám poté určí tzv. z-skóre.

Zcela zásadním úkolem při určování modelu je správná identifikace a výběr nezávislých proměnných. Toto může být obecně provedeno třemi různými způsoby.

1. První způsob je takzvaná přímá metoda, která je založena na teoretickém expertním zdůvodnění relativní významnosti jednotlivých ukazatelů. Jinými slovy jsou ukazatele vybírány a přidávány postupně.

2. Druhá metoda je postupná a je založena na postupném odebírání jednotlivých ukazatelů z původní rozsáhlé škály dle jejich relativní diskriminační síly.

3. Třetí metoda pak kombinuje dvě předcházející.

O **lineární diskriminační analýze (LDA)** hovoříme v situaci, kdy se populace dělí do dvou tříd a náhodný vektor má vícerozměrné normální rozdělení. Nejznámější je Fisherova lineární diskriminační funkce.

Regularizovaná diskriminační analýza (RDA) je diskriminační analýza založená na kombinaci lineární diskriminační analýzy (LDA) a kvadratické diskriminační analýzy, která navíc využívá regularizaci, tj. upravuje variační matice tak, aby byly regulární i v případě, že počet proměnných je velký (nebo relativně velký vůči počtu pozorování). Tato metoda byla představena J.H. Friedmanem v roce 1988 [72, 77].

3.1.2 Stromy a lesy

Rozhodovací strom tvoří sada hierarchicky uspořádaných rozhodovacích pravidel. Se stromovou strukturou se setkáváme poměrně často, neboť je přehledná a snadno interpretovatelná. U rozhodovacích stromů je zřejmá analogie s reálnými stromy v přírodě, proto byla jednoduše převzatá terminologie, která je pro stromy běžná a dobře vystihuje podstatu algoritmu. Podobně jako u reálného stromu tedy hovoříme o tom, že rozhodovací strom roste, větví se nebo jej

prořezáváme. Rozhodovací strom se skládá z kořene, který představuje celý soubor a postupně probíhá větvení do dalších uzlů – strom roste. Uzly, které se již dále nedělí, se označují jako terminální uzly nebo také listy. Stromy jsou binární nebo nebinární, podle toho, zda se větví na dvě nebo více větví [73].

Rozhodovací stromy můžeme rozdělit podle typu závisle proměnné na klasifikační a regresní. U **klasifikačního stromu** jsou pozorování kategoriální závisle proměnné zařazeny do některé z kategorií.

Náhodný les je kombinovaná učící metoda pro klasifikaci a regresi, která vytvoří více rozhodovacích stromů při učení a následně vydá modus (nejčastější hodnotu) tříd vrácených jednotlivými stromy [74].

3.1.3 Support vector machines

Support vector machines (SVM) je metoda strojového učení s učitelem, sloužící zejména pro klasifikaci a také pro regresní analýzu [53]. Je to klasifikační metoda, která explicitně formalizuje to, co neuronové sítě řeší implicitně [55]. Od neuronových sítí se liší, mimo jiné, metodou pro nalezení optimálních hodnot parametrů. Na rozdíl od heuristicky založených neuronových sítí stojí SVM klasifikátor na pevném matematickém základě a dosahuje lepší výsledky.

Základem metody SVM je lineární klasifikátor do dvou tříd. Cílem úlohy je nalézt nadrovinu, která prostor příznaků optimálně rozděluje tak, že trénovací data náležející odlišným třídám leží v opačných poloprostorech. Optimální nadrovina je taková, že hodnota minima vzdáleností bodů od roviny je co největší. Jinými slovy, okolo nadroviny je na obě strany co nejširší pruh bez bodů. Na popis nadroviny stačí pouze body ležící na okraji tohoto pásma a těch je obvykle málo - tyto body se nazývají podpůrné vektory (angl. support vectors).

Důležitou součástí techniky Support vector machines je jádrová transformace prostoru příznaků dat do prostoru transformovaných příznaků typicky vyšší dimenze. Tato jádrová transformace umožňuje převést původně lineárně neseparovatelnou úlohu na úlohu lineárně separovatelnou, na kterou lze dále aplikovat optimalizační algoritmus pro nalezení rozdělující nadroviny.

Používají se různé jádrové transformace, které intuitivně vyjadřují podobnost dat pomocí dvou vstupních argumentů. Výhodou této metody (a jiných metod založených na jádrové transformaci) je, že transformace se dá definovat pro různé typy objektů.

Lineární SVM je jednodušší varianta SVM metody, při které zůstáváme v původním prostoru příznaků a nedochází k žádné jádrové transformaci. Výsledkem potom je čistě lineární klasifikátor.

Základní myšlenkou **nelineární SVM** je použití tzv. jádrového triku (anglicky kernel trick), s jehož pomocí se provádí transformace dat z původního prostoru příznaků do prostoru vyšší dimenze, ve kterém jsou data lineárně separabilní.

Jinými slovy, provádíme zobrazení trénovacích dat z původního prostoru do jiného eukleidovského prostoru.

Protože je SVM klasifikátor ve své obvyklé podobě příliš citlivý vůči přítomnosti odlehlých hodnot v datech [78], byly navrženy i některé pokusy o jeho robustnější verzi. Zde pracujeme s **lineárním robustním SVM klasifikátorem**, který byl navržen v práci [79].

3.2 Metody pro měření lokální svalové zátěže

3.2.1 Integrovaná elektromyografie

Integrovaná elektromyografie (iEMG) je v současné době nejpřesnější dostupná metoda, při které lze monitorovat u měřených pracovníků odezvu funkce nervosvalového systému na pracovní zátěž. V průběhu měření dochází ke snímání elektrofyziologických biopotenciálů z vyšetřovaných svalových skupin rukou a předloktí. K měření se používá speciální měřící zařízení EMG Holter. Zjištěné údaje jsou následně zpracovávány pomocí speciálního softwaru dodávaného k těmto přístrojům. Výsledky měření jsou relativní hodnoty vynakládaných svalových sil v tzv. %Fmax.

Integrace je matematický proces, který vypočítává plochu opsanou křivkou. Pro integraci EMG signálů je použit celovlnný usměrňovač a elektronický integrátor. Integrovaný elektromyogram představuje celkovou svalovou aktivitu a je funkcí amplitudy, trvání a frekvence průběhu jednotlivých EMG potenciálů. Pro měření byl použit přenosný osmi-kanálový polygraf pro záznam fyziologických veličin EMG Holter se 4 EMG moduly. EMG modul slouží ke sledování činnosti svalů metodou měření a záznamu elektrických potenciálů provázejících svalovou aktivitu. EMG potenciály jsou snímány speciálními povrchovými elektrodami.

Snímaný signál je zesílen diferenciálním zesilovačem, filtrován (potlačeny složky s frekvencí 50 Hz indukované z elektrorozvodné sítě), celovlnně usměrněn, integrován, digitalizován a průběžně ukládán do paměti. EMG signály jsou vzorkovány 20-krát za sekundu, následně je vypočtena jejich průměrná hodnota, která je ukládána do paměti přístroje.

Pro měření lokální svalové zátěže byl použit přístroj EMG Holter společnosti GETA Centrum s.r.o. [80].

3.2.2 Technická data EMG Holteru

- Vstupní diferenciální odpor EMG/EKG vstupů: > 35 MΩ
- CMR, potlačení souhlasného napětí mezi EMG vstupy: > 60 dB
- Typický odstup signálu vůči šumu: > 40 dB
- Zesílení EMG/EKG modulů: 38 dB (80 x) $\pm$ 2 %
- Zesílení kanálů (za moduly): 1–256 v 1 + 8 stupních $\pm$ 5
- Integrační konstanta: 125 ms $\pm$ 5 %

- Vstupní napětí: stupeň zesílení 1–20 mV; max. rozsah ± 5 %; stupeň zesílení 9–80 μV; max. rozsah ± 5 %
- Frekvenční rozsah: 240 ÷ 60 Hz ; - 1dB, 60 ÷ 30 Hz ; - 3 dB; 30 ÷ 20 Hz ; - 6dB, pod 20 Hz ; - 12 dB
- Pásmová zádrž: útlum při 50 Hz: min. – 10 dB

3.2.3 Tenzometrická a výpočtová metoda

Pomocí tenzometrických přístrojů jsou proměřeny vynakládané svalové síly, ty jsou pak vztaženy na hodnoty maximálních svalových sil obsažené v Metodickém materiálu Národního referenčního pracoviště pro fyziologii a psychofyziologii práce [81]. Následně je prováděn výpočet průměrných směnových časově vážených svalových sil a vyhodnocení dalších kritérií.

Při použití metody tenzometrie a výpočtu je třeba vyhodnotit i postavení horních končetin při práci dle použité metodiky.

- Úhel α – vyjadřuje polohu vzhledem ke středovému bodu ramenního kloubu, resp. k rovině proložené tímto bodem a kolmé k sagitální[6] rovině těla. (0° má při předpažení).
- Úhel β – pomocí tohoto úhlu je určena poloha vzhledem k sagitální rovině těla, která dělí tělo shora dolů na pravou a levou polovinu. Při pozici končetiny, kdy předmět úchopu se nachází v rovnoběžné rovině s touto sagitální rovinou je úhel β roven 0°.
- Úhel γ vyjadřuje pozici předloktí vzhledem k nadloktí, tedy stupeň ohybu v loketním kloubu. Má hodnoty 30° až 180°.

[6]Sagitální jsou všechny roviny rovnoběžné s rovinou mediánní. Mediánní (střední) rovina prochází předozadně středem těla a dělí ho na dvě souměrné poloviny.

4. Vlastní výsledky a přínosy

Hlavním **softwarovým výsledkem** této disertační práce je funkční aplikace, která snímá a vyhodnocuje dynamiku stisku počítačových kláves. Tato aplikace má několik funkčních verzí, z nichž každá je upravená na míru konkrétnímu řešení, resp. nasazení v praxi.

První (pilotní) verze aplikace byla použita primárně pro otestování funkčnosti aplikace a nasbírání první sady dat. Experiment a výsledky této pilotní studie jsou podrobně popsány v kapitolách 4.3 a 4.4 této práce.

Druhá verze aplikace, popsaná podrobněji v kapitole 4.2, má rozšířené hlavně uživatelské rozhraní a umožňuje, mimo jiné, načtení už uložených záznamů, jejich vzájemné porovnání anebo porovnávání načteného záznamu s aktuálním průběhem psaní.

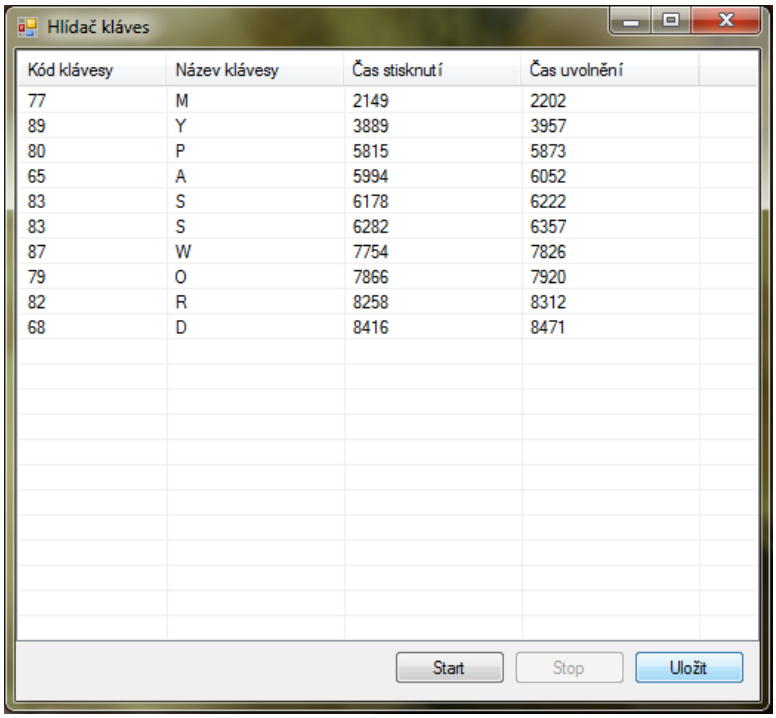
Třetí verze aplikace je uzpůsobena sběru dat při objektivizaci hodnocení lokální svalové zátěže při pracích na počítači, a to zejména při psaní na klávesnici.

Díky sbírání dat přímo z operačního systému je velkou výhodou všech verzí této aplikace vyloučení zpoždění, ke kterému může docházet „mezi klávesnicí a obrazovkou“. K tomuto účelu jsou snímány položky jako kód klávesy, název klávesy, doba stisknutí klávesy a doba uvolnění klávesy, které umožňují automatickou analýzu dat. Analýza spočívá ve výpočtu *časového vektoru*, který sestává z hodnot délek trvání jednotlivých stisků a délek mezer mezi jednotlivými stisky (viz kapitola 2.2.2.1).

Součástí této kapitoly je stručný popis dvou nejvýznamnějších publikací, které vznikli v rámci této disertační práce. Jde konkrétně o robustní metody výběru proměnných pro data získaná z analýzy dynamiky stisku počítačových kláves v kapitole 4.5, a o objektivizaci měření a hodnocení lokální svalové zátěže pomocí snímání dynamiky stisku počítačových kláves v kapitole 4.6. Obě publikace se nacházejí v příloze A a jejich výsledky zde již nejsou znova podrobně popisovány a diskutovány.

4.1 Pilotní aplikace „Hlídač kláves“

„Hlídač kláves“ je aplikace, která zachycuje dynamiku stisku počítačových kláves při zadávání uživatelského jména, hesla nebo i průběžně při psaní textu. Aplikace zaznamenává kód klávesy, její název, čas stisknutí a čas uvolnění tlačítka. Nahrávání se spouští stiskem tlačítka „Start“ a ukončuje stiskem tlačítka „Stop“ (viz obrázek 4.1). Po ukončení nahrávání a stisknutí tlačítka „Uložit“ se všechna data exportují do souboru CSV (viz obrázek 4.3). Všechny parametry potřebné pro dynamiku stisku počítačových kláves lze z těchto údajů vypočítat. Aplikace je naprogramována v jazyce C♯ a funguje na libovolném počítači s operačním systémem Windows a .NET Framework verze 4.0 [82].



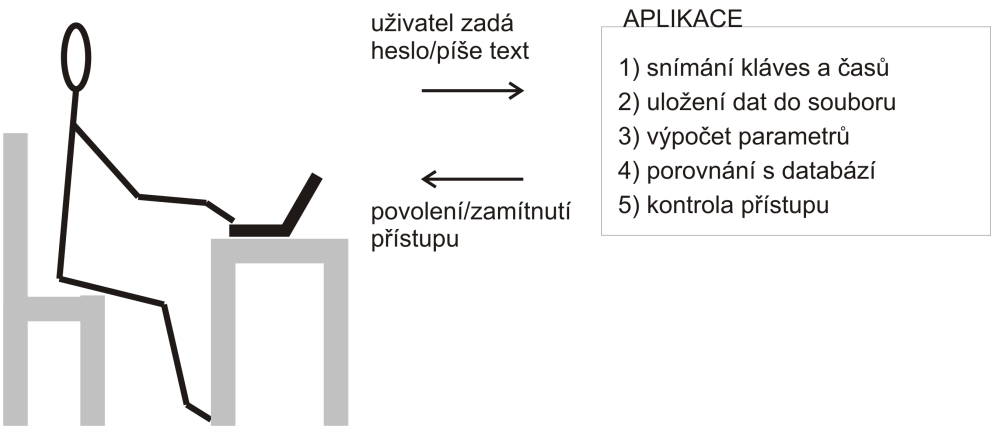
Obrázek 4.1: Aplikace zaznamenává parametry pro dynamiku stisku počítačových kláves.

4.1.1 Struktura aplikace

Obrázek 4.2 demonstruje základní strukturu aplikace. Aplikaci lze rozdělit na pět základních částí:

1. Snímání stlačených kláves a časů jejích stisknutí a uvolnění.
2. Uložení dat do souboru.
3. Výpočet potřebných parametrů.
4. Analýza dat, porovnání s databází.

5. Povolení/zamítnutí přístupu uživatele k aplikaci.



Obrázek 4.2: Struktura aplikace.

4.1.2 Implementace v jazyce C♯

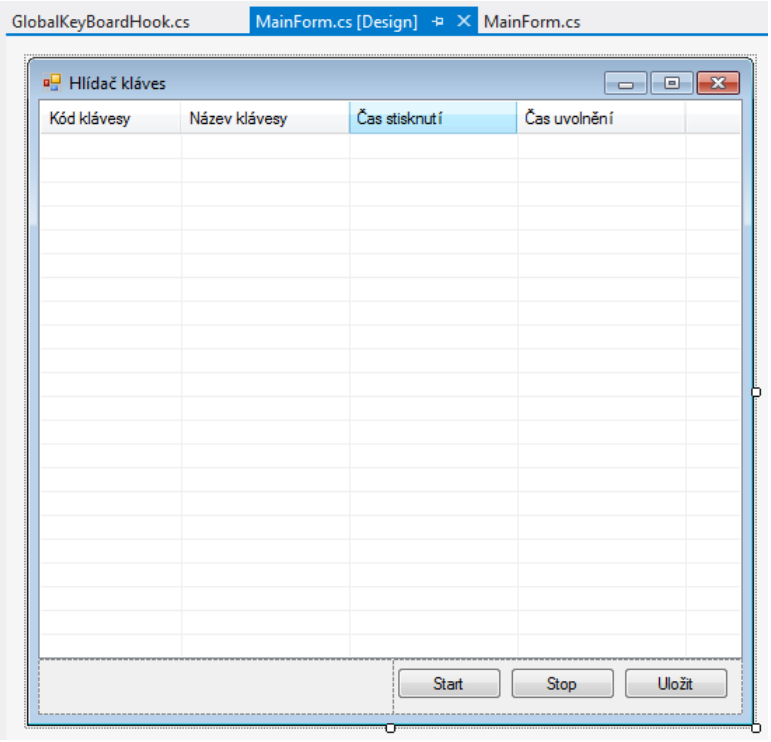
Aplikace byla vyvinuta ve vývojovém prostředí Microsoft Visual Studio Express 2012. Při tvorbě aplikace byla použita třída globalKeyboardHook.cs [83], která řeší globální odposlech kláves. Je možné ji získat jako kód podléhající The Code Project Open License (CPOL) [84]. Díky použití této třídy lze ukládat přesné časy stlačení a uvolnění jednotlivých kláves. Samozřejmostí je snímaní všech kláves na klávesnici, a také možnost snímání více kláves současně (viz obrázek 4.3).

	A	B	C	D	E	F	G
1	75	K	7229	7832			
2	76	L	7471	7833			
3	160	LShiftKey	6431	7948			
4	65	A	7677	7966			
5	68	D	9482	9572			
6	82	R	9828	9857			
7	85	U	9922	9978			
8	66	B	10235	10300			
9	89	Y	10477	10528			
10	48	D0	13415	13466			
11	57	D9	13588	13635			
12	187	Oemplus	15199	15237			
13	221	Oem6	15376	15414			
14	113	F2	18093	18180			
15	114	F3	18309	18374			
16	91	LWin	19351	19407			
17							

Obrázek 4.3: Data exportována do souboru CSV.

4.1.3 Popis pilotní aplikace

Na začátku souboru je zavedena třída StisknuteKlavesy, která obsahuje proměnné Kod (typ Keys (specifikuje kódy kláves a modifikátorů)), Stisknuto (typ long) a Uvolneno (typ long). Následně jsou všechny proměnné (včetně stopek) vynulované. Pak se po stisku tlačítka „Start“ povolí snímání kláves a hodnoty se ukládají do příslušných proměnných. Po stisku tlačítka „Stop“ se snímání zastaví a povolí se možnost uložit nasnímaná data do souboru pomocí tlačítka „Uložit“.



Obrázek 4.4: Návrh uživatelského rozhraní v programu Microsoft Visual Studio Express 2012.

4.1.4 Uživatelské rozhraní aplikace

Uživatelské rozhraní pozůstává ze čtyř sloupců. V prvním sloupci se zobrazuje kód klávesy, ve druhém její název, ve třetím čas stisknutí a ve čtvrtém čas uvolnění. Rozhraní disponuje vpravo nahoře standardními tlačítky pro minimalizaci a maximalizaci okna a také tlačítkem pro zavření aplikace. Toto tlačítko zároveň zastaví i snímání kláves.

Vpravo dole jsou pak tři tlačítka:

1. Tlačítko „Start“ zahájí snímání kláves (jejích kódů a časů stisknutí a uvolnění). Po opětovném stlačení tlačítka „Start“ (je opět aktivní až po

stlačení tlačítka „Stop“) se paměť aplikace vyprázdní (tj. nahrávání začíná od začátku).

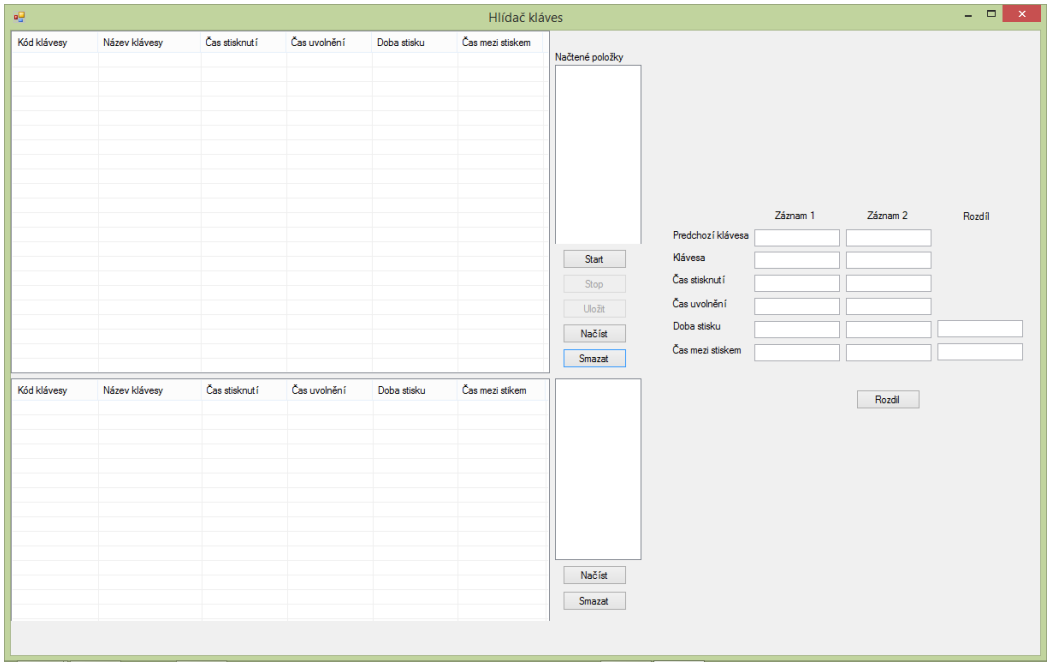
2. Tlačítko „Stop“ ukončí snímání kláves. Tlačítko je aktivní pouze při spuštěné aplikaci (nemá smysl zastavovat něco, co neběží).

3. Tlačítko „Uložit“ uloží nahraná data do souboru s příponou CSV. V případě, že v průběhu běhu aplikace nebyly zmáčknuté žádné klávesy na klávesnici, toto tlačítko není aktivní. Zabraňuje se tak možnosti uložení prázdného souboru.

4.2 Rozšířená aplikace „Hlídač kláves“

Rozšířená verze aplikace „Hlídač kláves“ může být komfortně použita dvěma způsoby [85]:

1. Jako aplikace pro *statické ověření* (uživatelské jméno + heslo + dynamika stisku počítačových klávesy při zadávání uživatelského jména a hesla).
2. Jako aplikace pro *kontinuální ověřování* (ověřuje, zda uživatel, který pracuje s informačním systémem, je stejný uživatel, jako ten, který je přihlášen).



Obrázek 4.5: Rozšířená verze aplikace pro snímání dynamiky stisku počítačových kláves.

4.2.1 Popis rozšířené aplikace

V této „rozšířené“ verzi aplikace bylo provedeno několik významných změn oproti pilotní verzi [85] (viz obrázek 4.5):

1. Jsou přidány výpočty *doby trvání stisku* a *doby mezi jednotlivými stisky* přímo do okna aplikace.
2. Je přidána funkce načtení již uloženého záznamu.
3. Je přidáno druhé okno pro záznam dynamiky stisku počítačových kláves. Díky tomuto vylepšení je možné přímo porovnat dva záznamy mezi sebou.

4. Je přidaná možnost vybrat si konkrétní část záznamu, označit ji v obou porovnávaných záznamech v oknech nalevo a napravo je vidět přímo rozdíly jednotlivých charakteristik.

Rozšířená aplikace je také implementována v C♯ pomocí Microsoft Visual Studio Express 2012 a snímána data jsou exportována do souboru CSV.

4.3 Sběr dat a analýza v pilotní studii

Pilotní studie se zúčastnilo 32 probandů, 10 mužů a 22 žen. Každý z nich byl požádán, aby napsal slovo *kladruby*, název města v České republice. Nejdřív bylo každému probandu řečeno, aby slovo napsal pomalu a bylo mu umožněno si psaní tohoto slova nejdřív několikrát vyzkoušet za účelem tréninku. Pak byl požádán, aby slovo napsal přibližně desetkrát pomalu. Následně bylo probandu řečeno, aby slovo napsal rychle a bylo mu opět dovoleno několikrát si to vyzkoušet. Poté byl požádán, aby slovo napsal přibližně desetkrát rychlým tempem. Pokud některé z měření obsahovalo překlep, bylo celé jedno pozorování, tj. jedno napsané slovo, z další analýzy vyřazeno.

Data obsahují 15 proměnných, jmenovitě dobu trvání 8 stisků kláves pro písmena (K, L, A, D, R, U, B, Y) a 7 odpovídajících latencí kláves (K-L, L-A, ..., B-Y). Získali jsme tedy data ve formě tabulky s 663 řádky a 17 sloupci. Nicméně, protože existuje 15 proměnných pozorovaných pro každého jednotlivce a pro každý typ psaní (pomalé, rychlé), považujeme data za mnohorozměrná [51].

Provedli jsme několik analýz s cílem naučit se klasifikačnímu pravidlu umožňujícímu přiřazení datového vektoru 15 proměnným neznámé osoby konkrétní osobě z databáze 32 probandů. V této souvislosti jsme srovnávali lineární diskriminační analýzu (LDA), regularizovanou diskriminační analýzu (RDA) [72], klasifikační strom, vícevrstvý perceptron a metodu SVM (support vector machines). Mezi těmito metodami lze považovat za spolehlivé také pro mnohorozměrná data pouze metody RDA, neuronové sítě a SVM [76].

RDA je jednou z nedávno navrhovaných regularizovaných verzí LDA, šitých na míru situaci s malým počtem pozorování. Na druhé straně, jak neuronové sítě, tak SVM vyžadují velký počet pozorování, aby bylo možní nalézt optimální hodnoty jejich parametrů.

Výpočty jsme provedli v softwaru R. Použité balíčky a funkce jsou uvedené v tabulce 4.1. Ve všech případech používáme výchozí nastavení parametrů.

4.4 Výsledky pilotní studie

Nejprve jsme použili klasifikační metody, abychom se naučili klasifikačnímu pravidlu, které umožňuje přiřadit nový datový vektor jednomu z 32 probandů. Následně jsme provedli autovalidaci, tj. použili jsme klasifikační pravidlo pro přiřazení každého z datových vektorů jednomu z 32 jedinců. Výsledky jsou uvedeny v tabulce 4.1. Nejlepší ověřovací výsledek jsme získali pomocí metody SVM, a to 91 % datových vektorů. Na druhou stranu, vícevrstvý perceptron nepřinesl žádný výsledek, pravděpodobně proto, že je zde malý počet pozorování ve srovnání s velkým počtem pozorovaných proměnných.

Tabulka 4.1: Výsledky pilotní studie na 32 probandech se 2 režimy psaní (pomalejší, rychlejší).

Klasifikační metoda	Správná klasifikace (%)			
	syrová data	upravená data*	balíček R	funkce
LDA	73	82	MASS	lda
RDA	79	86	rda	rda
Klasifikační strom	51	51	tree	tree
SVM	91	93	e1071	svm

* data bez odlehlých hodnot

Dále jsme učili klasifikační pravidlo na 64 skupinách, rozlišujeme mezi jednotlivci i režimem psaní. Nejlepším výsledkem je SVM. Autentizace však klesne na 83 %, u LDA klesne na 72 %.

Později jsme provedli analogickou studii s ohledem pouze na data získaná v režimu pomalého psaní. Zde je nejlepší výsledek dosažen u SVM, a to konkrétně 92 %. Ve studii, která zvažuje pouze režim rychlého psaní, SVM opět získá správné ověření v 92 % pozorování.

Pokud cílem je klasifikovat pozorování pouze do režimu psaní, SVM poskytuje správný výsledek klasifikace v 83 % a LDA v 60 % případů. Neexistuje tedy žádná výhoda v rozlišování mezi dvěma režimy psaní.

Nakonec se pokusíme naučit robustní klasifikační pravidlo. V sadě tréninkových dat ignorujeme všechna měření nad 500 milisekund, což se zdá být rozumným předběžným zpracováním dat, které zajistí robustní výsledky (viz [47]). To snižuje původní počet 663 pozorování na 534. Takto je 19 % pozorování ze studie odstraněno jako odlehlé hodnoty. Autovalidaci provádíme s 534 neodlehlými pozorováními a výsledky jsou uvedeny v tabulce č. 4.1. Je zřejmé, že měření s upravenými daty umožňují přesnější a spolehlivější ověřování s nejlepším výsledkem 93% získaným pomocí SVM.

4.5 Robustní metody výběru proměnných pro mnohorozměrná data

V této publikaci byl použitý přístup MRMR (*Minimum Redundancy Maximum Relevance*) pro výběr proměnných, který představuje úspěšnou metodologii pro redukci rozměrů, která je vhodná pro mnohorozměrná data pozorovaná ve dvou nebo více různých skupinách. Různé dostupné verze přístupu MRMR byly navrženy tak, aby hledaly proměnné s největší relevancí pro klasifikační úlohu při řízení redundance vybrané sady proměnných. Obvyklá kritéria relevance a redundance však mají nevýhody v tom, že jsou příliš citlivá na přítomnost odlehlých měření a/nebo jsou neefektivní.

V tomto článku navrhujeme nový přístup nazvaný *Minimum Regularized Redundancy Maximum Robust Relevance* (MRRMRR), vhodný pro všechna data o vysoké dimensionalitě pozorovaná ve dvou skupinách, která nemohou být stroji chápána a správně interpretována (jako například nestrukturovaný text).

Metoda kombinuje principy regularizace a robustní statistiky. Zejména je redundance měřena novou regularizovanou verzí součinitele součinitele součtu a relevance je měřena vysoce robustním korelačním koeficientem založeným na nejméně vážených čtvercových regresích s váhami adaptivními na data. Porovnáváme různé metody redukce rozměrů na třech reálných datových sadách. Pro zkoumání vlivu šumu nebo výstupů na data provádíme výpočty také pro data uměle znečištěná silným hlukem různých forem. Experimentální výsledky potvrzují robustnost metody s ohledem na extrémní hodnoty.

4.5.1 Data získaná z analýzy dynamiky stisku počítačových kláves

Analýza dat byla provedena na datasetu z pilotní studie [86] zaměřené na autentizaci osob na základě charakteristiky psaní lékařských zpráv ve zdravotnických zařízeních. Navrhli jsme a implementovali softwarový systém založený na měření dynamiky stisku počítačových kláves [87], inspirovaný biometrickými autentizačními systémy pro lékařské zprávy [88, 89].

Tréninková data obsahují tzv. časový vektor složený z trvání stisknutí jednotlivých kláves a z latencí mezi jednotlivými stisknutími naměřené v milisekundách na 32 probandech, kteří desetkrát zadali krátké heslo („kladruby“) svou obvyklou rychlostí psaní. Navzdory nízké hodnotě proměnných $p = 15$ jsou data mnohorozměrná, protože p převyšuje počet měření pro každého jednotlivce. V praktické aplikaci jeden z 32 jednotlivců identifikuje sebe (řekněme jako XY)

a zadává heslo. Cílem analýzy je ověřit, zda konkrétní jedno psaní na klávesnici patří nebo nepatří osobě XY. Úkolem ověřování je tedy klasifikační problém, a to přiřazení jednotlivce k jedné ze skupin.

Výsledky klasifikační úlohy ve studii s křížovou validací jsou uvedeny v Tabulce 4.2. Pokud je klasifikace prováděna se surovými daty, SVM překonává jiné metody. Mezi jeho nevýhody však patří neschopnost nalézt optimální hodnoty jejich parametrů a velký počet vektorů [51]. Pokud se MRRMRR používá k volbě 4 proměnných s $|r^A_{LWS}|$ jako měřítko relevance a $|\tilde{r}^*|$ jako měřítko redundance, zdá se, že zde není významnější ztráta důležitých informací pro klasifikační úkol.

Tabulka 4.2: Výsledky leave-one-out křížové validace vyhodnocené s přesností klasifikace pro data ze studie dynamiky stisku počítačových kláves, kde MRRMRR používá $|r^A_{LWS}|$ jako měřítko relevance a $|\tilde{r}^*|$ jako měřítko redundance.

Redukce dimenzionality	Klasifikační metoda	Přesnost klasifikace (%)
—	SVM	93
—	Klasifikační strom	55
—	LDA	Neproveditelné
—	PAM	75
—	SCRDA	79
Počet hlavních komponent		4
PCA	SVM	90
PCA	Klasifikační strom	59
PCA	LDA	79
PCA	PAM	77
PCA	SCRDA	79
Počet proměnných pro MRRMRR		4
MRRMRR	SVM	93
MRRMRR	Klasifikační strom	55
MRRMRR	LDA	79
MRRMRR	PAM	75
MRRMRR	SCRDA	79

4.6 Objektivizace měření a hodnocení lokální svalové zátěže pomocí snímání dynamiky stisku počítačových kláves

Cílem této studie bylo zhodnotit přínos použití dynamiky stisku počítačových kláves v kombinaci s integrovanou elektromyografií (iEMG) pro objektivní vyhodnocení lokální svalové zátěže rukou a předloktí při psaní na klávesnici počítače a porovnání této metody s výsledky běžně používaných metod.

Studie byla provedena na 12 subjektech. Data byla shromážděna pomocí vlastní aplikace pro zachycení dynamiky stisku počítačových kláves a pomocí EMG Holteru pro detekci elektromyografických potenciálů pro stanovení lokální svalové zátěže.

Výsledky studie ukázaly, že v současné době používané metody objektivního vytížení při psaní na klávesnici počítače nejsou zcela přesné. Zejména bylo prokázáno, že skutečný celkový počet stisknutí kláves při tvorbě textu je podstatně vyšší než počet znaků, z nichž se text skládá. Kromě tohoto počtu je třeba vzít v úvahu i tzv. neviditelné klávesy, klávesové zkratky a zejména korekce v psaném textu.

Výsledky ukázaly, že všichni probandi v naší studii překročili platné hygienické limity pro celkový počet malých opakovaných pohybů rukou a předloktí a celkový počet pohybů na klávesnici. Většina probandů v naší studii také překročila platný hygienický limit pro nejvyšší průměrnou časově váženou hodnotu % Fmax (procento maximální svalové síly). To znamená, že metoda dynamiky stisku počítačových kláves má velký potenciál ke zvýšení přesnosti hodnocení lokální svalové zátěže při používání klávesnice a tím ke zlepšení stávající metodiky využitelné při diagnostice poškození zdraví z práce z možného přetížení při práci na počítači.

Závěr

Cílem předložené disertační práce bylo vyřešit problém výběru správné bezpečnostní strategie a následně ji implementovat v oblasti biomedicíny a zdravotnictví. Nejvhodnější metodou pro řešení bezpečnosti se ukázala být biometrická charakteristika, dynamika stisku počítačových kláves. Tato behaviorální biometrická charakteristika byla vybrána hlavně z důvodu úspory času pro uživatele (zdravotnický personál) protože se snímá v průběhu psaní textu a uživatele nezatěžuje žádnou činností navíc. Lze ji snímat za použití stávajícího hardwaru (klávesnice) a to také kontinuálně (v průběhu práce s počítačem) a také pro uživatele využívající vzdálené připojení (počítačovou síť).

V rámci práce byla vytvořena aplikace pro snímání této charakteristiky a na základě matematické analýzy bylo potvrzeno, že tato aplikace je schopna klasifikovat jednotlivé uživatele. Cílem analýzy dat bylo naučit se klasifikační pravidlo, které umožňuje identifikaci jednotlivce pouze na základě dynamiky stisku počítačových kláves. Nejlepší ověřovací výsledek jsme získali pomocí metody SVM (Support Vector Machines).

Nad rámec původního záměru byly na datových vektorech z dynamiky stisku počítačových kláves testovány také nové robustní klasifikační metody, například robustní SVM (Support Vector Machines) nebo MRMR (Minimum Redundancy Maximum Relevance).

Dále byla tato aplikace použita pro objektivizaci měření a hodnocení lokální svalové zátěže při práci s počítačem, resp. při psaní na klávesnici. Zde bylo prokázáno, že díky této metodě je možné lépe posoudit náročnost prací, které zatěžují zejména ruce a předloktí pracovníků, kteří část své pracovní doby tráví psaním textů na počítači.

Největším přínosem práce je úspěšné nasazení softwarového řešení v oblasti biomedicíny a zdravotnictví. Do budoucna se plánuje jednak rozšíření i o snímání dynamiky pohybů myší pro ještě komplexnější posouzení lokální svalové zátěže při práci s počítačem a jednak vytvoření aplikace, kterou bude možné použít i na dotykových zařízeních (tablety, chytré telefony, atd.).

Seznam použité literatury

[1] Akila M., Kumar S.S.: Improving feature extraction in keystroke dynamics using optimization techniques and neural network. In: Proceedings of International Conference on Sustainable Energy and Intelligent Systems; 2011 Jul 20-22; Chennai, India. 2011:891-898.

[2] Citlivé osobní údaje. Obecné nařízení o ochraně osobních údajů prakticky [online]. [cit. 2019-04-11]. Dostupné z: `https://www.gdpr.cz/gdpr/heslo/citlive-osobni-udaje/`

[3] RSA SecurID [online]. 2012 [cit. 2012-09-15]. Dostupné z: `http://www.rsa.com/node.aspx?id=1159`

[4] Rak R., Matyáš V., Říha Z.: Biometrie a identita člověka: ve forenzních a komerčních aplikacích. Grada, Praha: 2008.

[5] Švenda P.: Keystroke Dynamics [online]. 2001 [cit. 2012-06-28]. Dostupné z: `http://www.svenda.com/petr/docs/KeystrokeDynamics2001.pdf`

[6] Identity Assurance as a Service: AdmitOne Security [online]. 2010 [cit. 2012-08-04]. Dostupné z: `http://www.biopassword.com/`

[7] Monrose F., Rubin D.: Keystroke dynamics as a biometric for authentication. Future Generation Computer Systems. 2002;16(4):351-359.

[8] Zimmermann P.: PGP Source Code and Internals. MIT Press; 1995.

[9] Zvárová J.: Biomedicínská informatika I: Základy informatiky pro biomedicínu a zdravotnictví. 1.vydání. Praha: Karolinum, 2002. ISBN 80-246-0609-7.

[10] Boechat G.C., Ferreira J.C., Carvalho E.C.B.: Using the Keystrokes Dynamic for Systems of Personal Security. In: Proceedings Of World Academy Of Science, Engineering And Technology. 2006;24(18):61-66.

[11] Ježek V.: Systémy automatické identifikace. Praha: Grada, 1996.

[12] Matyas S.M., Stapleton J.: A Biometric Standard for Information Management and Security. Computers & Security. 2000;19(2):428-441.

[13] Rouse M.: Multifactor authentication (MFA) [online]. 2007 [cit. 2012-08-10]. Dostupné z: `http://searchsecurity.techtarget.com/definition/multifactor-authentication-MFA`

[14] Jorgensen Z., Yu T.: On Mouse Dynamics as a Behavioral Biometric for Authentication. In: Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security; 2011. New York: ACM; 2011:476-482.

[15] Schlenker A., Šárek M.: Biometric Methods for Applications in Biomedicine. In: European Journal for Biomedical Informatics. 2011;7(1):37–43.

[16] Ščurek R.: Biometrické metody identifikace osob v bezpečnostní praxi [online]. 2008 [cit. 2019-04-09]. Dostupné z: http://www.rucnepsanypodpis.cz/PDF/biometricke_metody.pdf

[17] RSA Data Loss Prevention (DLP) Suite. RSA, The Security Division of EMC: Security Solutions for Business Acceleration [online]. 2010 [cit. 2010-10-28]. Dostupné z: http://www.rsa.com/node.aspx?id=3426

[18] Cravotta N.: Looking under the surface of fingerprint scanners. EDN [online]. 2000 [cit. 2013-08-28]. Dostupné z: http://www.edn.com/article/507025-Looking_under_the_surface_of_finger_print_scanners.php

[19] Bicz W., et al.: Fingerprint structure imaging based on an ultrasound camera. NDTnet [online]. 1998 [cit. 2013-08-28]. Dostupné z: http://www.ndt.net/article/0598/optel/optel.htm

[20] Jain A., Bolle R., Pankarti S.: Biometrics: personal identification in networked society. New York: Springer; 2010.

[21] Zhang D.: Automated biometrics: technologies and systems. Norwell, Massachusetts: Kluwer Academic Publishers; 2000.

[22] Olzak T.: Reduce multi-factor authentication costs with behavioral biometrics. TechRepublic [online]. 2007 [cit. 2012-08-05]. Dostupné z: http://www.techrepublic.com/article/reduce-multi-factor-authentication-costs-with-behavioral-biometrics/6150761

[23] Joyce R., Gupta G.: Identity authentication based on keystroke latencies. In: Communications of the ACM. 1990 Feb;33(2):168-176.

[24] Ilonen J.: Keystroke Dynamics. In: Advanced Topics in Information Processing. Lappeenranta University of Technology [online]. 2003 [cit. 2011-08-22]. Dostupné z: http://www2.it.lut.fi/kurssit/03-04/010970000/seminars/Ilonen.pdf

[25] Bergadano F., Gunetti D., Picardi C.: User authentication through Keystroke Dynamics. In: ACM Transactions on Information and System Security. 2002;5(4):367-397.

[26] Gunetti D., Pikardi C.: Keystroke analysis of free text. In: ACM Transactions on Information and System Security. 2005;8(3):312-347.

[27] Barghouthi H.: Keystroke Dynamics. How typing characteristics differ from one application to another. [Master's thesis]. Gjovik, Norway: Gjovik University College; 2009.

[28] Cho S., Han C.H., Han D.H., Kim H.: Web based keystroke dynamics identity verification using neural network. In: Journal of Organizational Computing and Electronic Commerce, 10(4):295-307, 2000.

[29] Schlenker A, Šárek M.: Behavioural biometrics for multi-factor authentication in biomedicine. In: European Journal for Biomedical Informatics, 8(5): 19-24, 2012.

[30] Senathipathi K., Batri K.: Keystroke Dynamics Based Human Authentication System using Genetic Algorithm. In: European Journal of Scientific Research. 2012;28(3):446-459.

[31] Raj S.B.E., Santhosh A.T.: A Behavioral Biometric Approach Based on Standardized Resolution in Mouse Dynamics. In: International Journal of Computer Science and Network Security. 2009;9(4):370-377.

[32] Ahmed A.A.E., Traore I.: A New Biometrics Technology based on Mouse Dynamics. In: IEEE Transactions on Dependable and Secure Computing. 2007;4(3):165-179.

[33] Nazar A., Traore I., Ahmed A.A.E.: Inverse Biometrics for Mouse Dynamics. In: International Journal of Pattern Recognition and Artificial Intelligence. 2008;22(3):461-495.

[34] Brown M., Rogers S.J.: User identification via keystroke characteristics of typed names using neural networks. In: International Journal of Man-Machine Studies. 1993;39:999-1014.

[35] Lin D.T.: Computer-access authentication with neural network based keystroke identity verification. In: Proceedings of International Conference on Neural Networks; 1997 Jun 9-12; Houston, TX. IEEE; 1997:174-178.

[36] Loy C.C., Lai W.K., Lim C.P.: Keystroke patterns classification using the ARTMAP-FD Neural Network. In: Proceedings of International Conference on Intelligent Information Hiding and Multimedia Signal Processing; 2007 Nov 26-28; Kaohsiung. IEEE; 2007. P.61-64

[37] Araujo L.C.F., Sucupira Jr. L.H.R., Lizarraga M.G., Ling L.L., Yabu-Uti J.B.T.: User authentication through typing biometrics features. In: IEEE Transactions on Signal Processing, 2005;53(2):851–855.

[38] Bleha S., Slivinsky C., Hussein B.: Computer-access security systems using keystroke dynamics. In: IEEE Trans. Patt. Anal. Mach. Int. 1990;12(12):1217–1222.

[39] Furnell S.M., Sanders P., Stockel CT.: The use of keystroke analysis for continuous user identity verification and supervision. In: Proceedings of MEDIACOMM 95 – International Conference on Multimedia Communications, 1995.:189–193.

[40] Garcia J.: Personal Identification Apparatus, US patent number 4,621,334, Washington, DC, 1986.

[41] Hocquet S., Ramel J.Y., Cardot H.: Fusion of methods for keystroke dynamic authentication. In: Fourth IEEE Workshop on Automatic Identification Advanced Technologies, 2005:224–229.

[42] Leggett J., Williams G., Usnick M.: Dynamic identity verification via keystroke characteristics. In: Int. J. Man-Mach. Stud. 1991; 35:859–870.

[43] Obaidat M.S., Sadoun B.: Verification of computer users using keystroke dynamics. In: IEEE Transactions on Systems, Man, and Cybernetics – Part B: Cybernetics; 1997:27(2):261-269.

[44] Rundhaug F.E.N.: Keystroke dynamics – Can attackers learn someone's typing characteristics. Master's thesis, Gjovik University College; 2006.

[45] Shimshon T., Moskovitch R., Rokach L., Elovici Y.: Continuous Verification Using Keystroke Dynamics. In: International Conference on Computational Intelligence and Security (CIS), 2010:411-415.

[46] Šebesta V., Straka L.: Determination of markers by GUHA method for neural network training. In: Neural Network World; 1998:8(3):255-268.

[47] Zhou C.: A study of keystroke dynamics as a practical form of authentication. Bachelor thesis. Pomona College, Claremont; 2008.

[48] Dowland P.S., Furnell S.M.: A long-term trial of keystroke profiling using digraph, trigraph and keyword latencies. In: Security and Protection in Information Processing Systems. IFIP International Federation for Information Processing. 2004; 147:275-289.

[49] Šíma J., Neruda R.: Teoretické otázky neuronových sítí. Matfyzpress, 1996.

[50] Veselý A.: Neuronové sítě. In: Zvárová J., Svačina Š., Valenta Z. (eds.): Systémy pro podporu lékařského rozhodování. Praha. Karolinum; 2009.

[51] Hastie T., Tibshirani R., Friedman J.: The elements of statistical learning. Data mining, inference, and prediction. Springer, New York; 2009.

[52] Lawrence S., Giles C.L., Tsoi A.C.: Lessons in neural network training: Overfitting may be harder than expected. In: Proceedings of the Fourteenth National Conference on Artificial Intelligence AAAI-97, AAAI Press, Menlo Park, 1997:540–545.

[53] Vapnik V.N.: The nature of statistical learning theory. Springer, New York; 1995.

[54] Mosteller F., Tukey J.W.: Data analysis, including statistics. In: Lindzey G., Aronson E. (eds.): Handbook of Social Psychology, Vol. 2, Addison-Wesley, New York, 1968:80–203.

[55] Berka P.: Dobývání znalostí z databází. Academia, Praha; 2003.

[56] Rowley H., Baluja S., Kanade S.: Neural network-based face detection. In: IEEE Transactions on Pattern Analysis and Machine Intelligence 1998:20(1):23-38.

[57] Rowley H., Baluja S., Kanade S.: Rotation invariant neural network-based face detection. In: Proceedings IEEE Computer Society Conference on Computer Vision and Pattern Recognition CVPR 1998, IEEE Computer Society Press, Los Alamitos, 1998:38-44.

[58] Beliakov G., Kelarev A., Yearwood J.: Robust artificial neural networks and outlier detection. Technical report [online]. 2012 [cit. 2013-02-01]. Dostupné z: `arxiv.org/pdf/1110.1069.pdf`

[59] Vondrák I.: Umělá inteligence a neuronové sítě. VŠB - Technická univerzita Ostrava, 2009.

[60] Zvárová J., Svačina Š., Valenta Z., Berka P., Buchtela D., Jiroušek R., Malý M., Papíková V., Peleška J., Rauch J., Vajda I., Veselý A., Zvára K., Zvolský M.: Systémy pro podporu lékařského rozhodování. Karolinum, Praha; 2009.

[61] Nisbet R., Elder J., Miner G.: Handbook of statistical analysis and data mining applications. Elsevier, Burlington; 2009.

[62] Kohonen T.: Self-organized formation of topologically correct feature maps. In: Biological Cybernetics 1982;43:59-69.

[63] Martinez W.L., Martinez A.R., Solka J.L.: Exploratory data analysis with MATLAB. Second edition. Chapman & Hall/CRC, London; 2011.

[64] Řezanková H., Húsek D., Snášel V.: Shluková analýza dat. Professional Publishing, Praha; 2007.

[65] Novák M. a kol.: Umělé neuronové sítě: teorie a aplikace. C.H. Beck; 1998.

[66] Hájek P, Havránek T. Mechanizing Hypothesis Formation: Mathematical Foundations for a General Theory. Berlin, Heidelberg, New York: Springer-Verlag; 1978.

[67] Tučková J, Šebesta V.: Prosody Optimisation of a Czech Language Synthesizer. In: Neural Network World. 2008:18(4):291-308.

[68] Sinělnikov R.D. a kol.: Atlas anatomie člověka. Svazek III. Praha: Státní zdravotnické nakladatelství; 1965.

[69] Hanzlová J., Hemza J.: Základy anatomie pohybového ústrojí [online]. Brno: Masarykova univerzita, 2012 [cit. 2019-04-25]. Dostupné z: https://is.muni.cz/do/fsps/e-learning/zaklady_anatomie/zakl_anatomie_I/index.html

[70] Posuzování lokální svalové zátěže [online]. [cit. 2019-04-11]. Dostupné z: http://www.khshk.cz/e-learning/kurs5/222_posuzovn_lokln_svalov_zte.html

[71] Bernaciková M., Kalichová M., Beránková L.: Základy sportovní kineziologie [online]. Brno: Masarykova univerzit, 2010 [cit. 2019-04-25]. Dostupné z: https://is.muni.cz/do/1451/e-learning/kineziologie/elportal/index.html

[72] Guo Y., Hastie T., Tibshirani R.: Regularized discriminant analysis and its application in microarrays. In: Biostatistics. 2007;8:86-100.

[73] Breiman L., Friedman J.H., Olshen R.A., Stone C.J.: Classification and regression trees. Wadsworth, Belmont, CA; 1984.

[74] Breiman L.: Random forests. In: Machine Learning. 2001;45(1):5-32.

[75] Boser B.E., Guyon I.M., Vapnik V.N.: A training algorithm for optimal margin classifiers. In: Proceedings of the 5th Annual ACM Workshop on Computational Learning Theory. 1992:144–152.

[76] Kalina J.: Classification analysis methods for high-dimensional genetic data. In: Biocybernetics and Biomedical Engineering. 2014;34:10-18. DOI: https://doi.org/10.1016/j.bbe.2013.09.007

[77] Friedman J.H.: Regularized Discriminant Analysis. In: Journal of the American Statistical Association, 1989;84(405):165-175.

[78] Hable R., Christmann A.: On qualitative robustness of support vector machines; 2011.

[79] Xanthopoulos P., Pardalos P.M., Trafalis T.B.: Robust Data Mining. Springer, New York; 2013.

[80] GETA Centrum s.r.o. EMG Holter. Fyziologie práce [online]. 2018 [cit. 2019-04-11]. Dostupné z: http://fyziologie.getacentrum.cz/emg-holter/

[81] Podlešák K., Lebedová I.: Maximální svalové síly končetin a trupu – shrnutí poznatků z měření na populaci průmyslových dělník a dělnic ČSR. Praha: Referenční laboratoř fyziologie práce; 1980.

[82] Schlenker A., Bohunčák A.: Keystroke Dynamics for Security Enhancement in Hospital Information Systems. In: International Journal on Biomedicine and Healthcare 2015;3(1):41-44. ISSN 1805-8698

[83] A Simple C♯ Global Low Level Keyboard Hook [online]. 2007 [cit. 2013-08-28]. Dostupné z: http://www.codeproject.com/Articles/19004/A-Simple-C-Global-Low-Level-Keyboard-Hook

[84] The Code Project Open License (CPOL) 1.02 [online]. 2008 [cit. 2013-08-28]. Dostupné z: http://www.codeproject.com/info/cpol10.aspx

[85] Schlenker A., Reimer M.: Big Data in Hospital Information Systems in the terms of Security. In: Svačina Š., Zvárová J. (eds.): Semantic Interoperability in Biomedicine and Healthcare 2015:39-41.

[86] Schlenker A.: Keystroke Dynamics Data, 2015, http://www2.cs.cas.cz/?kalina/keystrokedyn.html.

[87] Kalina J., Schlenker A., Kutilek P.: Highly Robust Analysis of Keystroke Dynamics Measurements. In: Applied Machine Intelligence and Informatics. 2015;133-138.

[88] Ozdemir M.K.: A framework for authentication of medical reports based on keystroke dynamics [M.S. thesis], Middle East TechnicalUniversity, 2010, http://etd.lib.metu.edu.tr/upload/12612081/index.pdf

[89] Bhatt S., Santhanam T.: Keystroke dynamics for biometric authentication-a survey. In: Proceedings of the International Conference on Pattern Recognition, Informatics and Mobile Engineering (PRIME '13), IEEE, February 2013:17-23.

Seznam tabulek

Seznam obrázků

A. Publikace

První publikace *A Robust Supervised Variable Selection for Noisy High-Dimensional Data*, autorů Jan Kalina a Anna Schlenker, vyšla v roce 2015 v časopise *BioMed Research International*. V této publikaci jsme v rámci jednoho z experimentů testovali robustní matematické metody analýzy dat na biometrických datech nasnímaných pomocí aplikace popsané v kapitole 4.2.

Druhá přiložená publikace *A New Approach to the Evaluation of Local Muscular Load while Typing on a Keyboard*, autorů Anna Schlenker a Tomáš Tichý, vyšla v roce 2017 v časopise *Central European Journal of Public Health* a věnuje se objektivizaci meření a hodnocení lokální svalové zátěže při psaní na klávesnici.

Níže jsou uvedené hlavní publikace týkající se tématu disertační práce.

1. Kalina, J., Schlenker, A.: Dimensionality reduction methods for biomedical data. In: Lékař a Technika. 2018;48:29-35.

2. Schlenker, A., Tichý, T.: A new approach to the evaluation of local muscular load while typing on a keyboard. In: Central European Journal of Public Health. 2017;25(4):255-260.

3. Kalina, J., Schlenker, A.: Robust image analysis of BeadChip microarrays. In: Proceedings of the International Conference on Bioimaging (BIOIMAGING 2015); 2015:89-94.

4. Kalina, J., Schlenker, A.: A Robust Supervised Variable Selection for Noisy High-Dimensional Data. In: BioMed Research International. Volume 2015, Article ID 320385, 10 pages.

5. Kalina, J., Schlenker, A., Kutílek, P.: Highly robust analysis of keystroke dynamics measurements. In: 2015 IEEE 13th International Symposium on Applied Machine Intelligence and Informatics (SAMI)