Univerzita Karlova

1. lékařská fakulta

UNIVERZITA KARLOVA
1. lékařská fakulta

Bezpečnost IT v biomedicíně

Autoreferát disertační práce

Ing. Anna Schlenker

3. září 2019

Doktorské studijní programy v biomedicíně
Univerzita Karlova a Akademie věd České republiky

Obor: Biomedicínská informatika
Předseda oborové rady: prof. MUDr. Štěpán Svačina, DrSc., MBA
Školitel: Ing. Milan Šárek, CSc.

Disertační práce bude nejméně pět pracovních dnů před konáním obhajoby zveřejněna k nahlížení veřejnosti v tištěné podobě na Oddělení pro vědeckou činnost a zahraniční styky Děkanátu 1. lékařské fakulty.

Obsah

Abstrakt

Název práce: Bezpečnost IT v biomedicíně

Autor: Ing. Anna Schlenker

Školitel: 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.

Abstract

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.

1 Předmluva

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.

2 Úvod

V době, kdy jsem začínala své doktorské studium, byla vzhledem k rychlému rozvoji informačních technologií velmi aktuální otázka jejich 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 několika 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 vy-

hodnocování 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.

3 Hypotézy a cíle práce

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 každý 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.

4 Materiál a metodika

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.

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.

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 [2]. Behaviorální biometrie pro autentizaci uživatelů tvoří vznikající trend ve 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 [3]. 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 [3] kvalitní bezpečnostní výsledky. Jako příklad lze uvést produkt BioPassword [4] společnosti Net Nanny.

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 [5].

Pro analýzu dat byla použita klasická klasifikační metoda – lineární diskriminační analýza (LDA) a několik moderních klasifikačních metod. Jedná se o regularizovanou diskriminační

analýzu (RDA) [6], klasifikační strom [7], náhodné lesy [8], lineární metodu SVM (support vector machines), které používají funkci Gaussian radial base jako funkci jádra (nelineární SVM) [9]. Z těchto metod lze za spolehlivé pro vysokorozměrná data považovat pouze metody RDA a SVM klasifikátor [10]. 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 [10].

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.

5 Výsledky

Hlavním **softwarovým výsledkem** 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. Druhá verze aplikace 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.

5.1 Robustní metody výběru proměnných pro mnohorozměrná data

V této studii 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 publikaci [11] 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.

5.2 Objektivizace měření a hodnocení lokální svalové zátěže

Cílem studie [12] 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.

Podle výsledků 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.

6 Diskuse

Analýza dat byla provedena na datasetu z pilotní studie [13] 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 [14], inspirovaný biometrickými autentizačními systémy pro lékařské zprávy [15, 16].

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.

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 [17]. 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.

7 Závěry

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.).

Použitá literatura

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

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

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

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

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

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

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

[9] 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.

[10] 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`

[11] 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.

[12] 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.

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

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

[15] 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`

[16] 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.

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

A Publikace

Publikace s IF, které jsou podkladem práce

1. 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. **IF=0,958**

2. 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. **IF=2,931**

Publikace bez IF, které jsou podkladem práce

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

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

3. 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)

4. Schlenker, A.: Multifactor Data Security in Information Systems in Health Care. In: International Journal on Biomedicine and Healthcare. 2014;2(1):25. ISSN 1805-8698

5. Schlenker, A., Šárek, M.: Behavioural Biometrics for Application in Biomedicine. In: International Journal on Biomedicine and Healthcare. 2013;1(1):61. ISSN 1805-8698

6. Schlenker, A., Šárek, M.: Neural Networks in Keystroke Dynamics for Multi-Factor Authentication in Biomedicine. In: Manka, J., Tyšler, M., Witkovský, V. Frollo, I.: Measurement 2013. Bratislava: Institute of Measurement Science, Slovak Academy of Science, 2013;109–112. The 9th International Conference Measurement 2013. Smolenice castle (SK), May 27-30, 2013. ISBN 978-80-969-672-5-4

7. Schlenker, A.: Keystroke Dynamics for Authentication in Biomedicine. In: Kuželová, D., Hakl, F.: Doktorandské dny '12. Praha: Ústav informatiky AV ČR, v. v. i.& MATFYZPRESS, 2012;52-55. Doktorandské dny 2012 Ústavu informatiky AV CR, v. v. i.. Jizerka (CZ), 24.09.2012-26.09.2012 ISBN 978-80-7278-217-7

8. Schlenker, A., Šárek, M.: Behavioural Biometrics for Multi-Factor Authentication in Biomedicine. In: European Journal for Biomedical Informatics. 2012;8(5):19-24. ISSN 1801-5603

9. Schlenker A., Šárek M.: Biometric Methods for Applications in Biomedicine. In: European Journal for Biomedical Informatics. 2011;7(1):37–43. ISSN 1801-5603

10. Horňáková A., Šárek M.: Biometrické zabezpečenie dát v biomedicíne. In: Sborník příspěvků MEDSOFT 2011; 29.–30. března 2011; Roztoky u Prahy. Praha: Art D; 2011.

11. Horňáková A., Šárek M.: Data Security in Biomedicine. In: Kuželová, D., Hakl, F.: Doktorandské dny '11. Praha: Ústav informatiky AV ČR, v. v. i.& MATFYZPRESS.

Publikace s IF bez vztahu k tématu práce

1. Schlenker, J., Socha, V., Riedlbauchová, L., Nedělka, T., Schlenker, A., Potočková, V., Malá, Š., Kutílek, P.: Recurrence plot of heart rate variability signal in patients with vasovagal syncopes. In: Biomedical Signal Processing and Control. 2016;25:1-11 **IF=3,063**