Štúdia využitia biometrických metód v dochádzkových a prístupových systémoch

Radovan Potúček

Bakalářská práce
2017

Univerzita Tomáše Bati ve Zlín
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2016/2017

ZADÁNÍ BAKALÁŘSKÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Radovan Potúček**
Osobní číslo:	**A14054**
Studijní program:	**B3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**prezenční**
Téma práce:	**Studie využití biometrických metod v docházkových a přístupových systémech**
Téma anglicky:	**A Study of the Use of Biometrics in Access Control Systems**

Zásady pro vypracování:

1. **Proveďte literární rešerši na zadané téma.**
2. **Charakterizujte principy a metody měření biometrických dat a dostupné typy biometrických systémů v kontextu jejich možného využití v docházkových a přístupových systémech.**
3. **Popište způsob zpracování získaných dat, jejich uchování a nakládání s takto získanými daty.**
4. **Zpracujte a popište vybrané komerčně dostupné systémy pro kontrolu vstupu a evidence docházky.**
5. **Uveďte nové trendy v této oblasti.**

Rozsah bakalářské práce:

Rozsah příloh:

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam odborné literatury:

1. **RAK, Roman, Vašek MATYÁŠ a Zdeněk ŘÍHA. Biometrie a identita člověka ve forenzních a komerčních aplikacích. Praha: Grada, 2008. Profesionál. ISBN 978-80-247-2365-5.**
2. **LUKÁŠ, Luděk. Bezpečnostní technologie, systémy a management. Zlín: Radim Bačuvčík – VeRBuM, 2015. ISBN 978-80-87500-05-7.**
3. **KŘEČEK, Stanislav. Příručka zabezpečovací techniky. Vyd. 2. [S.l.: s.n.], 2003. ISBN 80-902938-2-4.**
4. **BOLLE, Ruud. Guide to biometrics. New York: Springer, c2004. ISBN 03-874-0089-3.**
5. **ASHBOURN, Julian. Practical biometrics: from aspiration to implementation. New York: Springer, c2004. ISBN 1852337745.**

Vedoucí bakalářské práce: **Ing. Petr Navrátil, Ph.D.**
Ústav řízení procesů

Datum zadání bakalářské práce: **3. února 2017**

Termín odevzdání bakalářské práce: **29. května 2017**

Ve Zlíně dne 3. února 2017

doc. Mgr. Milan Adámek, Ph.D.
děkan

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
L.S.

Ing. Jan Valouch, Ph.D.
ředitel ústavu

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové/bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová/bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou/bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou/bakalářskou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování diplomové/bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové/bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na diplomové/bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně, dne 22.5.2017

.....
podpis diplomanta

ABSTRAKT

Práca je zameraná na štúdiu využitia biometrických metód v dochádzkových a prístupových systémoch. Bude sa zaoberať princípmi a metódami merania biometrických dát a analýzou dostupných typov biometrických systémov v kontexte ich možného využitia v dochádzkových a prístupových systémov. Ďalej bude popisovať spôsob spracovania dát, uchovania a nakladania s takto získanými dátami. Budú uvedené nové trendy v oblasti využitia biometrických metód v dochádzkových a prístupových systémoch.

Kľúčové slová: Biometria, Biometrické metódy, Identifikácia, Prístupový systém, Dochádzkový systém

ABSTRACT

The work is focused on the study of biometric methods in access control and attendance systems. It will deal with principles and measurement methods biometric data and analysis available types of biometric systems in the context of their possible use in attendance and access control systems. Then it will describe process of data processing, stored and handled with the data thus obtained. It will stated new trends in the field of biometric methods in the attendance and access control systems.

Keywords: Biometrics, Biometric methods, Identification, Access control system, Attendance system

Chcel by som rád poďakovať vedúcemu bakalárskej práce pánovi Ing. Petrovi Navrátilovi, Ph.D. za pripomienky, poskytnuté materiály, ústretový prístup, ochotu a pomoc pri jej vypracovaní. Ďalej by som chcel ešte poďakovať celej mojej rodine za jej veľkú podporu počas celého môjho štúdia.

Prehlasujem, že som zadanú bakalársku prácu vypracoval samostatne a použitú literatúru som citoval a odovzdaná verzia bakalárskej práce a verzia elektronická nahraná do IS/STAG sú totožné.

OBSAH

ÚVOD

Biometrické metódy zastávajú nezastupiteľnú úlohu pri identifikácii a kontrole identity osôb. Dôležitosť týchto postupov a metód je zvlášť významná v tejto dobe, keď narastá hrozba regionálneho ale i globálneho ohrozenia terorizmom. Chrániť je potrebné nielen objekty, ale hlavne ľudí, ktorí pracujú v týchto objektoch. Keďže postupy na ochranu objektov, ktoré boli účinné v minulosti, sú už prekonané, je potrebné neustále zdokonaľovať už využívané bezpečnostné formy, ale hľadať i nové možnosti.

Jednou z týchto možností je biometrická metóda, ktorá vychádza z fyziologických znakov a zvykových čŕt jednotlivca. Keďže tradičné metódy identifikácie osôb už prestávajú spĺňať kritériá pre bezpečnosť, pri neustálom rozvoji počítačových technológií dochádza k častému zneužívaniu, kopírovaniu a odcudzovaniu identifikačných dát. Do popredia sa dostávajú kvalitnejšie technológie, ako sú napríklad biometrické metódy identifikácie. K identifikácii sa používajú biometrické údaje fyziologickej alebo behaviorálnej charakteristiky. Identifikačné biometrické údaje, v ktorých základ tvorí samotné ľudské telo, sú pre každého človeka jedinečné a zvyčajne sa časom nemenia. Pre dôkladné zabezpečenie sa môžu navzájom kombinovať a tým sa stávajú najspoľahlivejšími identifikačnými prostriedkami.

Biometrické identifikácie uľahčujú fyzický prístup osôb do podnikových areálov alebo tiež virtuálny prístup k vybraným podnikovým intranetom. Biometrickým systémom môžeme ľahko identifikovať prihlásenú osobu, či sledovať jej konkrétnu aktivitu.

Cieľom bakalárskej práce je poukázať na využitie biometrických metód v dochádzkových a prístupových systémoch. Analyzovať biometrické metódy na zabezpečenie kontroly priestorov a zaznamenávanie pohybu neoprávnených osôb a evidenciu dochádzky zamestnancov. Vymenovať a porovnať základné biometrické metódy. Čiastkovým cieľom je popísať spôsob spracovania dát, ich uchovanie a spôsob práce s týmito dátami. V závere práce uvádzam nové trendy využitia biometrických metód v dochádzkových a prístupových systémoch.

I. TEORETICKÁ ČASŤ

1 BIOMETRICKÉ METÓDY

„Biometriou sa označuje súbor metód určených na identifikáciu alebo verifikáciu osôb podľa jedinečných fyzických (fyziologických) znakov alebo zvykových (behaviorálnych) čŕt jedinca.“[1, s. 104]

Biometria teda umožňuje identifikovať človeka podľa jeho neopakovateľných a nenapodobiteľných znakov. Verifikovať, či je človek naozaj osobou, za ktorú sa vydáva, prostredníctvom predloženia identifikačného dokladu.

„Identifikácia je proces porovnávania rozmanitých objektov na základe ich zhody alebo rozdielov vo vlastnostiach, formách, umiestnenia, zloženia (štruktúry), funkcií, prejavoch, významu alebo v čase, s cieľom zistiť, či ide alebo nejde o zhodné (identické) objekty.“*[2, s. 40]*

Vlastný proces identifikácie je náročný a spája mnohé činnosti, ktoré nám napomáhajú čo najpresnejšie špecifikovať dané objekty. Každý objekt má svoje skupinové a individuálne vlastnosti, ktoré umožnia zaradiť objekt do určitej skupiny.

„Biometrická identifikácia/verifikácia je využitie jedinečných, merateľných, fyzikálnych alebo fyziologických znakov (tzv. markantov) alebo prejavov človeka k jednoznačnému zisteniu (identifikácie) alebo overenia (verifikácie) jeho identity.“[2, s. 104]

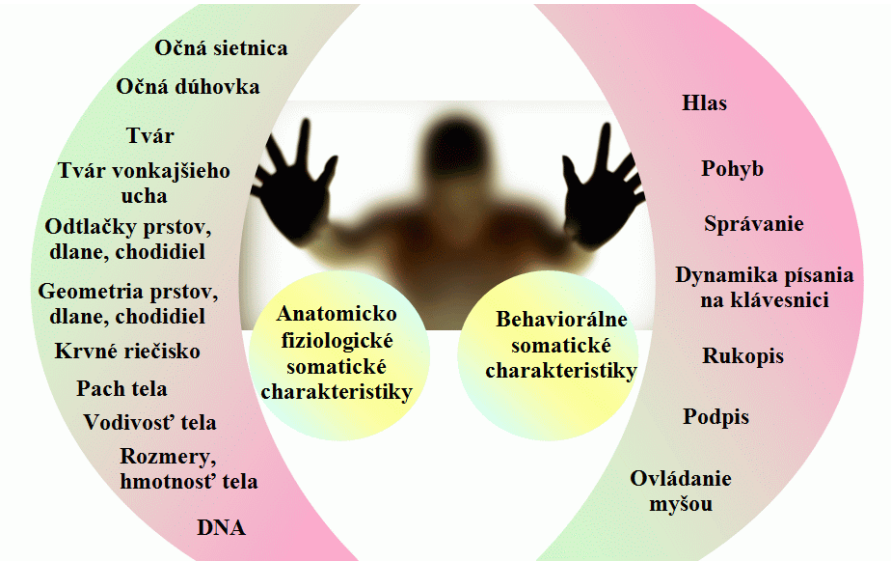
Pri verifikácii daná osoba odovzdá systému elektronickú identitu a na jej základe dôjde k overeniu fyzickej identifikácie. V databáze sú vyhľadané záznamy, ktoré obsahujú biometrické dáta. Ak záznam v systéme neexistuje, prístup je zamietnutý. Prichádza k porovnaniu vstupných dát s dátami v databáze.[3]

V praxi sa častejšie využívajú pri identifikácii osôb anatomické alebo fyziologické znaky. Zriedkavo sa využívajú behaviorálne znaky, ktoré charakterizujú vlastnosti ľudského chovania, aj povahové črty.

1.1 Základné biometrické identifikačné metódy

K základným biometrickým metódam určeným na rozpoznanie osôb na základe fyziologických a behaviorálnych znakov využívame biometrické kľúče, ktoré sa dajú ťažko falzifikovať. Biometrické znaky sú merateľné a môžu sa využívať pri identite jednotlivca. Fyziologické sú tvorené telesnými údajmi ako sú DNA, odtlačok prsta,

snímanie očnej dúhovky, sietnice, obraz tváre alebo rozmery a hmotnosť tela. K behaviorálnym znakom patria hlas, správanie, chôdza, podpis alebo rukopis. Je to základné členenie biometrickej identifikácie s požitím jednotlivých identifikačných metód a metódy, ktoré sa zatiaľ využívajú vo výskumno-vývojových laboratóriách. Biometrické identifikačné metódy znázorňuje nasledujúci obrázok.[2]



Obr. 1: Biometrické identifikačné metódy.[2]

1.2 Fyziologické biometrické metódy

Jednotlivé biometrické technológie sa líšia v spôsobe spracovania, ale ich význam je veľmi podobný. Umožňujú procesy overenia a určenia totožnosti istej osoby. Pre identifikáciu osôb sa používajú fyziologické charakteristiky, ktoré sú pre daného jedinca špecifické a predpokladá sa, že sú časovo nemenné.

1.2.1 Odtlačky prstov

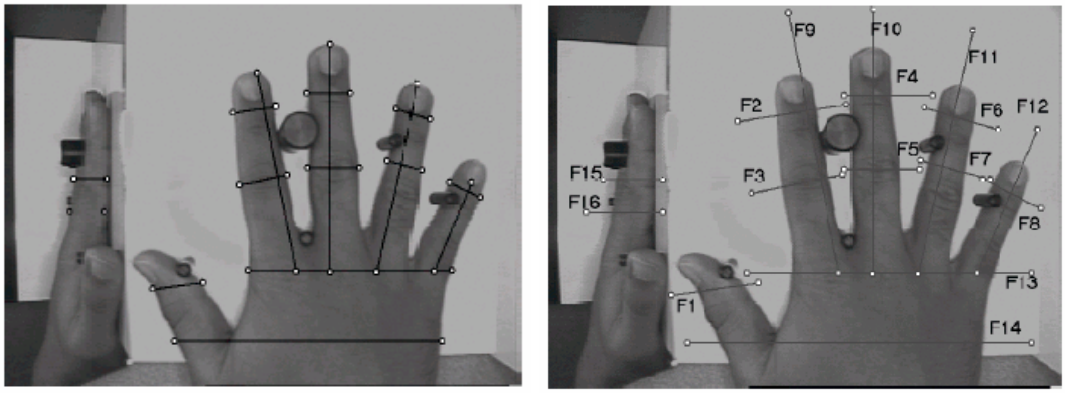
Snímanie odtlačkov prsta sa využíva najčastejšie a je jednou z najznámejších metód biometrickej identifikácie. Táto metóda je založená na snímanie povrchu prsta, ktorý obsahuje drobné brázdovité útvary, ktoré vytvárajú rôzne tvary, papilárne línie. Každý človek ich má jedinečné, a preto je to dobrý spôsob identifikácie.

Obr. 2: Extrahovanie detailov z odtlačku prsta.[4]

Snímanie odtlačkov prstov je jednou z najstarších biometrických technológií pri kriminálnom vyšetrovaní.[2]

1.2.2 Geometria ruky

Na začiatku pokusov o bezpečnostnú identifikáciu osoby bola realizácia zaznamenávania anatomicko-geometrických charakteristík ľudskej dlane a prstov, ktorú po prvýkrát použili v USA. Bolo to približne v rokoch 1970 - 1980. Základom tejto metódy bolo dvoj a trojrozmerné meranie dĺžky a šírky prstov, kĺbov a kostí.



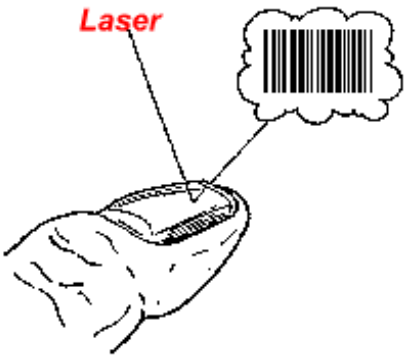
Obr. 3: Zobrazenie osí, pomocou ktorých prebieha výpočet biometrickej charakteristiky.[2]

Metóda geometrie ruky v porovnaní s inými biometrickými metódami neprodukuje veľké dátové množiny. To znamená rýchlu verifikáciu aj pri veľkom počte záznamov.[2]

1.2.3 Tvar nechta

Ďalšou biometrickou metódou identifikácie osôb je zaznamenávanie čiarových nerovností na povrchu nechta, ktoré kopírujú štruktúru lôžka nechta a sú tým jedinečné u každého človeka a na každom prste. Pri správnom osvetlení odrazom dostaneme tzv. „čiarový kód“.

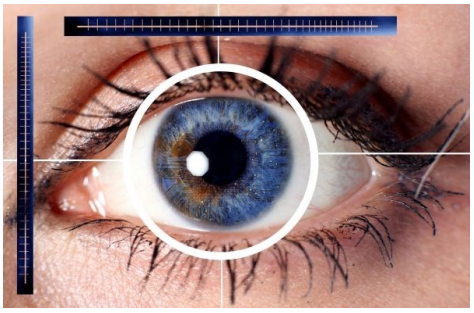
Podkožná štruktúra nachádzajúca sa pod nechtom zobrazuje rôzne široké čiary s rôzne širokými medzerami. Ak necháme pod určitým uhlom dopadať lúč polarizovaného svetla, potom môžeme zistiť fázové zmeny lúča po jeho odraze. Keď spracujeme zaznamenaný odraz, získame jednorozmernú štruktúru lôžka nechta. Tá nám pripomína čiarový kód.[5]



Obr. 4: Princíp identifikácie nechtu.[5]

1.2.4 Očná dúhovka

Aj farebný kruh okolo zreničky obsahuje špecifické a jedinečné identifikačné body, pomocou ktorých veľmi presne dokážeme identifikovať danú osobu. V prípade dúhovky existuje niekoľko odlišných foriem, ktoré sú rôzne kombinované, dokonca aj dúhovky jedného človeka sú rozdielne, sú jedinečné.

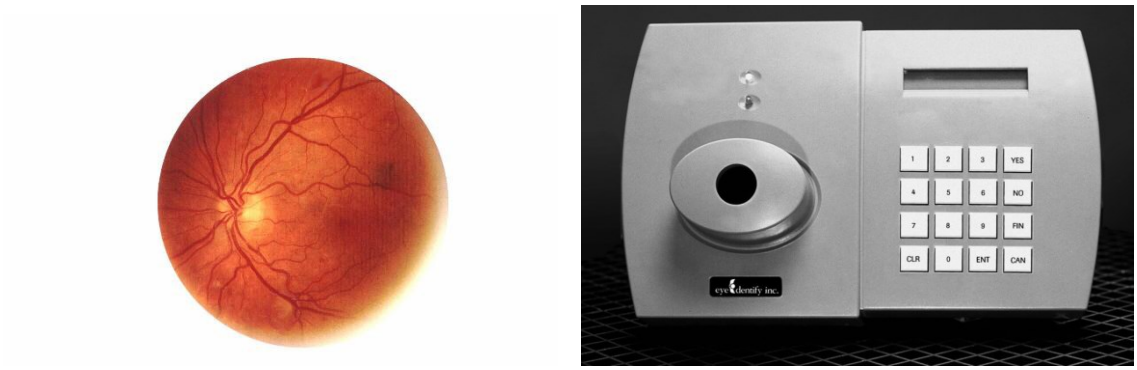


Obr. 5: Výber oblasti analýzy.[6]

Dúhovka sa skladá z náhodne rozmiestnených farebných štruktúr, ktoré sú podobné ako snehové vločky. Žiadne dve dúhovky nie sú rovnaké. Snímanie prebieha štandardnou video technológiou.[2]

1.2.5 Očná sietnica

Obsahuje dostatočné množstvo špecifických anatomických bodov, ktoré s veľkou presnosťou dokážu identifikovať osobu. Zaznamenávanie biometrickej vzorky prebieha pomocou svetelného lúča. Biela sietnica oka časť lúča pohlcuje a časť odráža. Na sietnici sa zaznamenávajú drobné žilky a cievky, tým sa stávajú nezameniteľnými. Obrázky sietnice majú rovnaké charakterizačné vlastnosti ako odtlačky prstov.

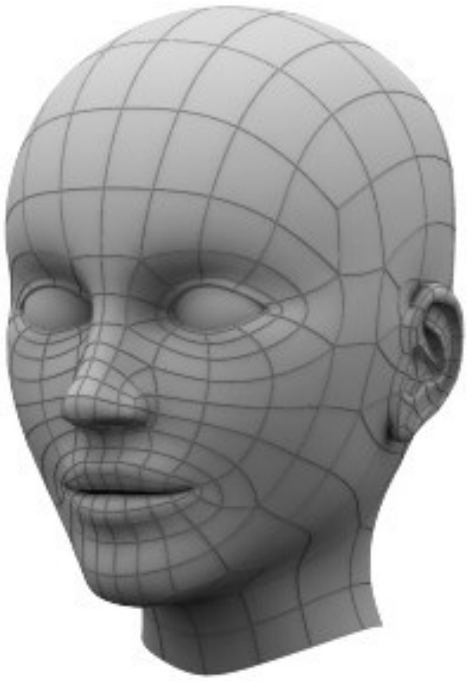


Obr. 6: Obraz sietnice a snímacie zariadenie.[2]

Metóda snímania sietnice sa javí ako najbezpečnejšia biometrická identifikačná metóda.

1.2.6 Tvár

Ďalšou mimoriadne dôležitou sférou identifikácie človeka je využitie počítačovej technológie na rozpoznávanie ľudskej tváre. Ľudská tvár totiž obsahuje identifikačné antropologické body, ktoré sú pre každú osobu špecifické a tiež časovo nemenné.



Obr. 7: Identifikačné antropologické body.[7]

K identifikácii tváre väčšinou slúži tvar a poloha opticky významných miest na tvári ako sú oči, nos, ústa, obočie. Obraz v počítači neuchováva presnú polohu očí, nosa a pier, ale ukladá sa len vzdialenosť očí, vzdialenosť pier od nosa, uhol medzi špičkou nosa a jedným okom.

1.2.7 DNA

Najväčšie predpoklady identifikácie osoby tým najpresnejším a najspoľahlivejším spôsobom má DNA. Obsahuje nesmierne veľa informácií o každej osobe, ale len malá časť z nich stačí pre identifikáciu. Tak, ako v dvadsiatom storočí bola daktyloskopia hlavným ukazovateľom identifikácie osôb, tak v dnešnej dobe bude rovnako dôležitá v identifikácii a iných oboroch DNA. V tejto súvislosti sa preto hovorí o genetickom odtlačku.

Obr. 8: Biometrická štruktúra DNA.[8]

„Využitie identifikácie človeka prostredníctvom DNA pre rýchle a spoľahlivé preverenie identity osôb, napríklad v rámci bezpečnostných systémov, je výrazne limitované zložitým technologickým spôsobom nevyhnutným pre stanovenie vlastného genetického profilu jednotlivca, kde aj tie najrýchlejšie metódy sú schopné dať odpoveď do niekoľkých hodín. Hlavné uplatnenie preto genetická identifikácia nachádza v oblastiach forenzných vied, kde časové hľadisko nie je rozhodujúce.“[2, s. 535]

Táto metóda je relatívne nová, i keď jej korene siahajú do polovice 80 rokov 20. storočia. Objektom jej skúmania je nosič genetickej informácie, molekula DNA. Približne 99,5 percent ľudského genetického materiálu je rovnaká u všetkých ľudí, no napriek tomu existuje mnoho identifikačných bodov, ktoré môžeme použiť k identifikácii.[9]

1.3 Behaviorálne biometrické metódy

Medzi najpoužívanejšie behaviorálne metódy patrí podpis a skúmanie hlasu. V miere zabezpečenia patria medzi najslabšie metódy, preto sa zvyčajne požívajú aj podporné zabezpečovacie systémy a metódy vo forme hesiel.

1.3.1 Hlas

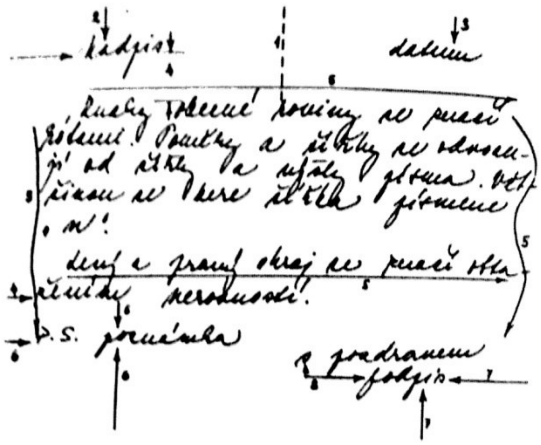
Táto identifikácia je založená na vibráciách, výslovnosti a rýchlosti reči. Do určitej miery to závisí od veľkosti hlasiviek, nosovej dutiny, úst a ďalších ukazovateľov tvorby hlasu. Vysoké frekvencie obsiahnuté v zvukovom spektre ľudskej reči sú tvorené pomocou hlasivkových pulzov, nižšie frekvencie nám udáva vokálny trakt. Identifikácia hlasu môže byť rozdelená podľa toho, či je závislá alebo nezávislá na texte. Identifikácia, ktorá je

závislá na texte, využíva základný tón reči. Technológie sa zakladajú na analýze slov alebo celých viet, ktoré poznajú len dané osoby. Nevýhodou môže byť, keď verifikácia je ovplyvnená chorobou, ako je nádcha alebo zlým psychickým stavom osoby.

Obr. 9: Biometrická štruktúra hlasu.[10]

1.3.2 Podpis

Ďalšou biometrickou metódou, ktorou môžeme identifikovať osobu, je podpis. Obsahuje obrovské množstvo informácií o danej osobe. Pri spracovávaní podpisu sa vyhodnocuje obraz, ale i dynamické vlastnosti pri písaní ako je smer podpisu, rýchlosť pera, tlak pera na podložku. Vyhodnocuje sa stav, kedy písomný prejav vznikol, s akým cieľom a motiváciou, psychická úroveň jednotlivca, ale aj vplyv okolia, v akom prostredí, v akej polohe sa píše a tiež aký je stav písacích potrieb. Pri analýze písma sa skúma smer podpisu, plošné usporiadanie písmen, sklon a veľkosť písmen, tiež umiestnenie diakritických znamienok, vzdialenosť slov, plynulosť pri písaní, to znamená viazanosť písmen.



Obr. 10: Identifikácia písomného prejavu.[2]

Výhodami biometrických metód je, že sa dajú ťažko falzifikovať, automaticky sa dáta spracúvajú do počítačových databáz, sú spoľahlivé a efektívne.

1.3.3 Dynamika písania na klávesnici

Nie až tak novou biometrickou technológiou je dynamika písania na klávesnici, ktorú používala počas druhej svetovej vojny britská tajná služba ako metódu k overovaniu autenticity rádiotelegrafických správ špiónov. Pre zistenie dynamiky písania na klávesnici potrebujeme hlavne nejaké programové vybavenie a klávesnicu.

„Prvým a zároveň jediným produktom je Net Nanny Software so svojou patentovanou technológiou BioPassword. Jedinou aplikáciou, ktorá je ponúkaná, je nadstavba pre prihlásenie do Windows NT. Pre zavedenie užívateľa je potrebná vzorka textu, v ktorom sa minimálne osemkrát opakuje osem znakov. Čím viac sa znaky opakujú, tým viac sa znižuje chybovosť overenia. Tento text musí užívateľ pri zavedení zopakovať minimálne pätnásťkrát.“[5]

Na vytvorenie svojho charakteristického profilu môže užívateľ zachytiť stlačenie klávesu, a následne jeho uvoľnenie. Informácie o stlačených klávesoch sa získavajú hardwarovými prerušeniami. Ten umožní zachytiť stlačenie klávesu a jeho uvoľnenie. Z týchto dvoch poznatkov môžeme vypočítať dĺžku trvania stlačenia klávesu. Meranie rozdielu stlačenia a uvoľnenia klávesu môže viesť aj k záporným hodnotám. Napríklad používanie klávesových skratiek CTRL+C alebo ALT+F4, keď stlačíme kláves ešte pred uvoľnením predchádzajúceho.

2 HISTÓRIA BIOMETRICKEJ IDENTIFIKÁCIE

Pre každého človeka je charakteristická biometrická identita, každý jedinec má fyzické a psychické charakteristické vlastnosti, ktoré sú jedinečné.

Použitie biometrických identifikačných metód sa využívalo už v období faraónskeho Egypta. Známe sú historické záznamy o biometrickej identifikácii osôb v údolí Nílu, kde roľníkov identifikovali podľa farby pleti, očí alebo iných charakteristických znakov, ako sú poranenia, či jazvy. Identifikácia slúžila na kontrolu pri výkupe obilia a slúžila k vyplácaniu mzdy. Neskôr faraónsky úradník zapisoval robotníkov, ktorí pracovali na stavbe, viedol o každom záznamy, základné identifikačné údaje, ako sú meno a vek, ale aj popis tváre a celého tela.

Už starí Číňania využívali identifikáciu osôb založenú na odtlačku prstov. V Babylone obchodné zmluvy podpisovali tým, že namiesto podpisu vložili odtlačok palca.

Veľký pokrok sa zaznamenal až pri výskumoch českého prírodovedca a lekára Jána Evangelistu Purkyně, ktorý sa zaoberal obrazcami papilárnych línii a tiež navrhol ich delenie.

„V roku 1924 Americký kongres svojim dekrétom založil identifikačnú divíziu FBI, ktorá ako základnú identifikačnú metódu zvolila odtlačky prstov. Daktyloskopická zbierka v roku 1946 obsahovala 100 miliónov kariet, v roku 1971 až 200 miliónov kariet s desiatimi odtlačkami prstov na každej z nich. V roku 1999 bolo rozhodnuté ukončiť papierové spracovanie a ďalej viesť evidenciu výhradne počítačovým spôsobom, pomocou AFIS – Automated Fingerprint Information System.“[2, s. 91]

Dnes sa odtlačky prstov pre policajné a bezpečnostné účely na celom svete spracovávajú hlavne pomocou výpočtovej techniky. Aj ostatné biometrické identifikačné metódy mali podobný historický vývoj ako odtlačky prstov. Identifikácia osôb na základe sietnice sa začala v roku 1980 a základy využitia identifikácie pomocou očnej dúhovky založil matematik Dr. Johan Daughman z Univerzity v Cambridge.[2]

Biometrická identifikácia ľudskej tváre a podpisu sú omnoho mladšie, pretože vznikli neskôr. DNA vznikla na prelome 20. a 21. storočia a jej objavenie je také významné ako boli v minulosti odtlačky prstov. Slúži predovšetkým ako identifikácia trestne stíhaných osôb. Metódy biometrickej identifikácie sa neustále zdokonaľujú a využívajú sa vo všetkých smeroch a odboroch ľudskej činnosti.

3 BEZPEČNOSŤ BIOMETRICKÝCH SYSTÉMOV

Biometrický systém musí obsahovať funkcie, ktorých cieľom je bezpečnosť, spoľahlivosť a efektívnosť.

„Každý informačný systém sa skladá z mnohých rôznych aktív (napríklad dáta, programy, technické vybavenie atď.), s ktorými sú spojené určité zraniteľné miesta. Zraniteľné miesto je slabina v systéme, ktorá môže byť využitá pre narušenie zamýšľaného využitia informačného (biometrického) systému. Možnosť využitia zraniteľného miesta predstavuje hrozbu, s ktorou je spojené riziko jej uskutočnenia.“[3, s. 71]

V rámci informačného systému sú aktíva navzájom prepojené a jedno zraniteľné miesto môže ovplyvniť viaceré, a tak porušiť integritu dát. Bezpečnosť sa netýka len biometrických zariadení, ale aj prenosu a ukladaniu dát.

Typickými možnosťami napadnutia biometrického systému je:

- Predloženie falošnej biometrie snímaču
- Ovplyvnenie extraktora rysov vírusom
- Zmena biometrických rysov
- Útok na registračné centrum
- Útok na prenosový kanál medzi registračným modulom a databázou
- Zmena biometrickej šablóny
- Ovplyvnenie porovnávacieho modulu
- Útok na prenosový kanál medzi databázou šablón a porovnávacím modulom
- Zmena finálneho rozhodnutia
- Útok na samotnú aplikáciu

Prenos biometrických dát je v dnešnej dobe zabezpečený šifrovaním, ktoré môžeme dešifrovať len so znalosťou kľúča. Biometrický systém musí odolať mnohým útokom a zároveň spĺňať základné požiadavky bezpečnosti.[3]

Biometrické overenie identity osoby má vždy bezpečnostný charakter. Jedným z kritérií zabezpečujúcich spoľahlivosť identifikácie je pravdepodobnosť chybného odmietnutia identity osoby, alebo prijatie neoprávnenej osoby. Chybné odmietnutie identity osoby je udávané pravdepodobnosťou, pri ktorej biometrický systém urobí chybu a odmietne osobu, ktorej šablónu má uloženú v databáze. Ide o nepríjemnosť vzhľadom k užívateľovi, no neohrozí bezpečnosť objektu. Opakom je chybné prijatie neoprávnenej

osoby. Systém sa domnieva, že chybné biometrické dáta sú totožné so šablónou v databáze a nesprávne potvrdí totožnosť osoby. Nastavenie biometrického systému sa nakonfiguruje aby sa spomínané chyby eliminovali.[11]

3.1 Základné princípy spracovania dát

Základom biometrickej identifikácie je overenie a porovnanie zhody nasnímaných biometrických znakov so vzorkami, ktoré máme uložené v databáze.

3.1.1 Zber biometrických dát

Biometrické spracovanie dát sa začína meraním anatomických, fyziologických, alebo behaviorálnych znakov človeka. Biometrickým snímačom môže byť kamera, mikrofón, skener odtlačku prstov, ruky alebo skener na získanie elektronického obrazu. Senzory snímania biometrických dát musia brať ohľad na spôsob, akým sa meranie uskutoční. Teda na uhol a vzdialenosť merania, vonkajšie podmienky a samotné správanie sa danej osoby. Taktiež snímanie ovplyvňujú aj technické parametre snímania, ako je rýchlosť prenosu, presnosť merania, technické parametre snímacieho senzoru.[2]

3.1.2 Prenos biometrických dát

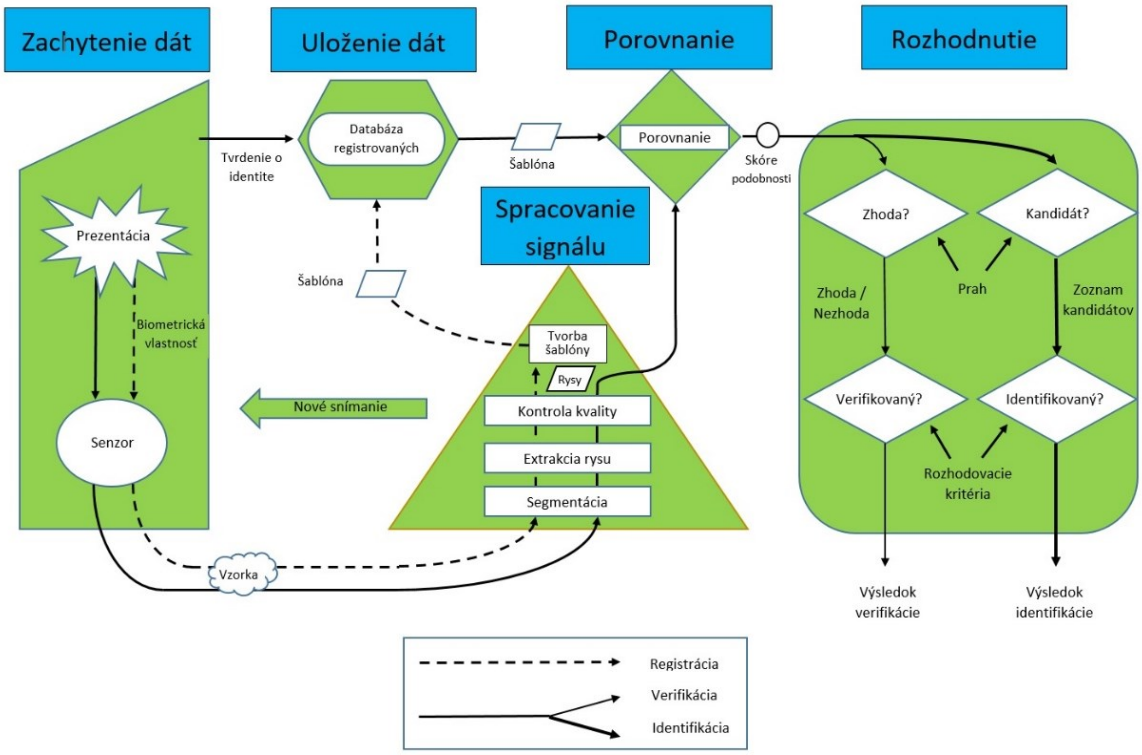
Mnohé biometrické systémy zbierajú dáta na jednom mieste a spracovávajú ich na inom mieste. Preto je dôležité zabezpečiť ochranu týchto dát. Často však sú dáta veľmi objemné a zaberajú veľa miesta, preto sa prenášajú rôznymi komprimovanými technikami. Veľký objem dát, ktoré sa prenášajú, zaťažujú prenosový kanál. Tým sa zníži rýchlosť prenášania. Komprimáciou a následnou dekomprimáciou sa znižuje kvalita prenášaných dát. V súčasnosti sa hľadajú také spôsoby komprimačných metód, aby čo najmenej ovplyvnili kvalitu dekomprimovaných dát.[2]

3.1.3 Spracovanie a porovnávanie biometrických šablón

Spracovanie biometrických dát prebieha prostredníctvom šablón, ktoré sa vytvárajú komprimáciou biometrickej vzorky. Samotné porovnávanie a vyhodnocovanie biometrických systémov využíva prácu s týmito šablónami. Dochádza k porovnávaniu šablón, ktoré sú práve nasnímané, so šablónami uloženými v databáze. Potom nastáva rozhodovanie, kde sa vyhodnotí na základe daných charakteristík a metód, či nastáva zhoda medzi predkladanou a uloženou šablónou.[2]

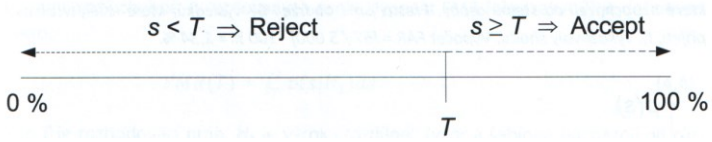
3.1.4 Uloženie biometrických dát

Poslednou etapou spracovania biometrických dát je ich uloženie. Poznáme dve základné metódy uloženia dát. Prvá metóda ukladá originálne biometrické vzorky (napríklad odtlačok prsta aj s papilárnymi líniami). Táto metóda sa využíva ako dôkazový materiál v súdnictve. V druhej metóde sa ukladajú biometrické šablóny, čo prináša značné výhody. Biometrická šablóna je menšia, a tak môžeme prenášať a uložiť väčšie množstvo dát. V praxi sa často stretávame aj s kombináciou týchto metód uloženia dát.[2]



Obr. 11: Štruktúra biometrického systému.[3, upravil Potúček 2017]

Výsledok porovnávania, či nastáva alebo nenastáva zhoda, leží v intervale <0,1>.



Obr. 12: Prijatie alebo odmietnutie zhody.[3]

Pri porovnávaní biometrickým systémom je výsledok buď prijatý – accept, alebo odmietnutý – reject. Podľa toho systém vyhodnotí identifikáciu danej osoby.

4 DOCHÁDZKOVÉ A PRÍSTUPOVÉ SYSTÉMY

V dnešnej dobe je na trhu veľa druhov dochádzkových systémov. Sledovanie dochádzky zamestnancov je často zdĺhavá práca, preto organizácie využívajú možnosti elektronických systémov, ktoré nám pomáhajú nahradiť papierovú formu zapisovania a kontrolovania dochádzky.

4.1 Dochádzkový systém

Evidenciu dochádzky zamestnancov, zabezpečenie kontroly priestorov a zaznamenávanie pohybu neoprávnených osôb nám umožňujú dochádzkové systémy. V súčasnosti sa vyznačujú vysokým technickým vybavením, ktoré riešia problematiku evidencie a kontroly. Sú schopné vyslať identifikačné údaje do snímacej jednotky na základe bezdotykovej identifikácie.

Dochádzkový systém je výnimočný vo svojej jednoduchosti. Jeho dáta sa zbierajú a ukladajú do databázy, ktoré neskôr kontroluje a potvrdzuje pracovník organizácie a vloží ich do mzdového programu. Vkladanie časov príchodov a odchodov je veľmi jednoduché. Dáta z čítačiek sú spracovávané v reálnom alebo špecifickom čase a posielané do databázy. Elektronické dochádzkové systémy sú stále žiadanejšie a populárnejšie v organizáciách.

4.1.1 Funkcie dochádzkových systémov

Dochádzkový systém zbiera a ukladá dáta do databázy, ktoré sú neskôr spracované a vložené do daného programu. Momentálne máme na trhu rôzne druhy čítačiek, ako napríklad čítačky na magnetické kartičky, bezdotykové kartičky alebo biometrické čítačky. Čítačky na magnetické kartičky musíme vložiť do čítačky, až potom ju dokáže identifikovať. Bezdotykové čítačky majú veľkú výhodu v tom, že stačí prejsť okolo čítačky v určitej vzdialenosti a danú osobu zaregistruje. Biometrické čítačky fungujú na princípe snímania častí tela, ktoré má každý človek jedinečné, ako sú odtlačok prsta, očná sietnica a dúhovka, alebo črty tváre, či hlasový prejav. Takéto čítačky sa využívajú v objektoch, ktoré si vyžadujú veľkú bezpečnosť a kde je dôležitá prísna kontrola pri vstupe daných osôb.

Obr. 13: Dochádzkový systém s biometrickým senzorom.[12]

Mnohé organizácie si zabezpečujú elektronické dochádzkové systémy vzhľadom na veľkosť organizácie.

Malé organizácie si zabezpečujú dochádzkové systémy, ktoré sledujú príchody a odchody zamestnancov a tiež kontrolu a nastavenie pracovného harmonogramu zamestnancov. Taktiež je možné nastaviť pravidlá pracovnej dochádzky, kde sú stanovené doby prestávok, dovoleniek, dokonca aj nadčasov. Takýmito systémami môžu organizácie sledovať nedochvíľnosť alebo absencie pracovníkov.

Väčšie organizácie si zabezpečujú zložitejšie a náročnejšie dochádzkové systémy. V týchto systémoch sa riadia pracovné dáta v súvislosti s výkonom práce, niektoré vedia dokonca sledovať aj produkciu vykonanej práce. Takto sa posudzuje produktivita zamestnancov a tiež predpovedá, čo bude potrebovať konkrétna pracovná sila, ak sa chce zvýšiť produkcia v blízkej, či vzdialenej budúcnosti organizácie.

Dochádzkové systémy sú zamerané na určité pracovné odvetvia ako zdravotníctvo, školstvo, či priemysel. Tieto odvetvia majú stanovené pracovné postupy a konkrétne informácie, pomocou ktorých vytvárajú dôležité hlásenia alebo plány. Musia spĺňať všetky požiadavky organizácie. Čím jasnejšie sú očakávania od dochádzkového systému, tým sa vie presnejšie zabezpečiť funkčnosť a spoľahlivosť tohto systému.

4.1.2 Kompatibilita dochádzkových systémov

Mnohé firmy sa dopúšťajú najčastejších chýb, keď pri kúpe nového dochádzkového systému nie je kompatibilný s predchádzajúcim dochádzkovým systémom. Preto nebude možné nový dochádzkový systém zosynchronizovať a jeho výstupné dáta nebudú kompatibilné so mzdovým programom predchádzajúceho dochádzkového systému. Najskôr musíme dôkladne vypracovať analýzu dochádzkového systému, ktorý momentálne používame a vybrať taký, ktorý bude spĺňať všetky aspekty požadovaného dochádzkového systému. Väčšina dochádzkových systémov má štandardné zariadenia pre vstupné dáta a mzdové aplikácie, vďaka čomu sú nové dochádzkové systémy kompatibilné so staršími dochádzkovými systémami. Organizácia musí urobiť analýzu, ktorý zo systémov bude najlepšie spĺňať podmienky dochádzky, aby bola čo najefektívnejšia. Tejto problematike sa venujú všetky dochádzkové systémy na dnešnom trhu, ktoré sa snažia prispôsobiť väčšine našich požiadaviek.

4.1.3 Časové pečiatky v dochádzkovom systéme

Časová pečiatka je údaj, ktorý má dôveryhodný zdroj času a tým garantuje použitie presného času, napríklad pri elektronickom podpise. Časový údaj nedokážeme zmeniť.

Technológia časových pečiatok je využívaná v dochádzkových systémoch, ktorá pracuje na princípe presného času, ktorý je získaný prostredníctvom certifikačnej autority časovej pečiatky. Výhodou v dochádzkovom systéme je, že zamestnanci ani správcovia si nemôžu sami zmeniť čas príchodu alebo odchodu. Nevýhodou môže byť sledovanie osôb v priestoroch organizácie, pretože dochádzkový systém zaznamenáva identifikačné číslo karty. Tým vieme zistiť vlastníka karty a zároveň dĺžku pobytu v priestoroch.

4.1.4 Dochádzkový systém s formou webového rozhrania

Na rozdiel od bežného dochádzkového systému, ktorý beží na jednom zariadení, sa môžeme stretnúť aj s dochádzkovým systémom s formou webového rozhrania. Takýto dochádzkový systém je prístupný z rôznych zariadení s internetovým pripojením. V systéme sa nachádzajú napríklad odpracované hodiny, dovolenky, ale aj iné citlivé informácie o zamestnancoch, preto by mala byť dostatočne zabezpečená sieť, na ktorej beží dochádzkový systém. V rámci organizácie môže bežať na intranetovskej sieti alebo u hostingového poskytovateľa.

Výhodami dochádzkových systémov s formou webového rozhrania je jednoduchý prístup, kde sa môžu zamestnanci prihlásiť cez svoj webový prehliadač pomocou svojich prístupových mien a hesiel. Pri použití prístupových čítačiek sú dáta hneď prenesené do dochádzkového systému.

Obr. 14: Dochádzkový systém pomocou intranetu.[13]

Ďalej systém automaticky zaznamenáva odpracované hodiny jednotlivých zamestnancov na konci mesiaca, ich nadčasy, čím sa uľahčuje administratívna práca. Takéto dáta získané z dochádzky sú ľahko spracovateľné a prenosné do mzdových programov a tak sa bez problémov vypočíta mzda zamestnancov. Veľkou výhodou je aj zálohovanie dát v prípade zlyhania systému. Aktualizácie systému automaticky zaznamenávajú zmeny a pravidlá rôznych zákonov a pracovných poriadkov, ktoré sú pre organizáciu mimoriadne dôležité.

4.2 Prístupový systém

Prístupový systém nám umožňuje sledovať presný pohyb osôb v priestore a čase, alebo povoliť vstup len v určitom čase a do určitých priestorov. Takto môžeme mať pod kontrolou spolu s návštevným systémom kompletný pohyb v priestoroch organizácie. Osoby, ktoré majú prístup do danej organizácie, môžu vstúpiť len s použitím bezkontaktnej čipovej karty alebo biometrickým overením.

Prístupové systémy nám umožňujú nepoužívať veľké množstvá kľúčov, ale ich nahradiť kartou, čipom alebo biometrickým odtlačkom prsta. Ďalej umožňujú obmedziť vstup do priestorov cudzím osobám a tým, ktorí môžu vstúpiť do priestorov, dáva možnosť využiť len určitý časový interval. Rovnako bezpečnostné prístupové systémy sú schopné

spätne kontrolovať pohyb osôb v priestoroch, okamžite zabrániť vstupovaniu cudzím osobám. Vďaka prístupovým systémom sa môžeme pripojiť k zabezpečovacím a kamerovým systémom a zároveň ovládať doplnkové zariadenia, ako sú brány alebo závory.

„Najdôležitejším riadiacim faktorom prístupových systémov je prideľovanie prístupového práva, ktoré sa vystavuje konkrétnym osobám na základe stupňov oprávnenia podľa priestorových, časových, personálnych a iných dispozícií.“[14, s. 256]

Kontrola vstupu v zabezpečujúcich systémoch je rozdelená podľa tried identifikácie a tried prístupu.

Triedy identifikácie:

Trieda 0 – nevyžaduje priamu identifikáciu a prístup je možný použitím jednoduchých tlačidiel a kontaktov, pri vstupe je potrebná fyzická kontrola. Vchádzajúca osoba sa preukáže zamestnaneckým preukazom alebo návštevníckou vstupenkou.

Trieda 1 – vyžaduje pre vstup heslo, PIN kód, ktoré zariadenie porovná s údajom v pamäťovej jednotke.

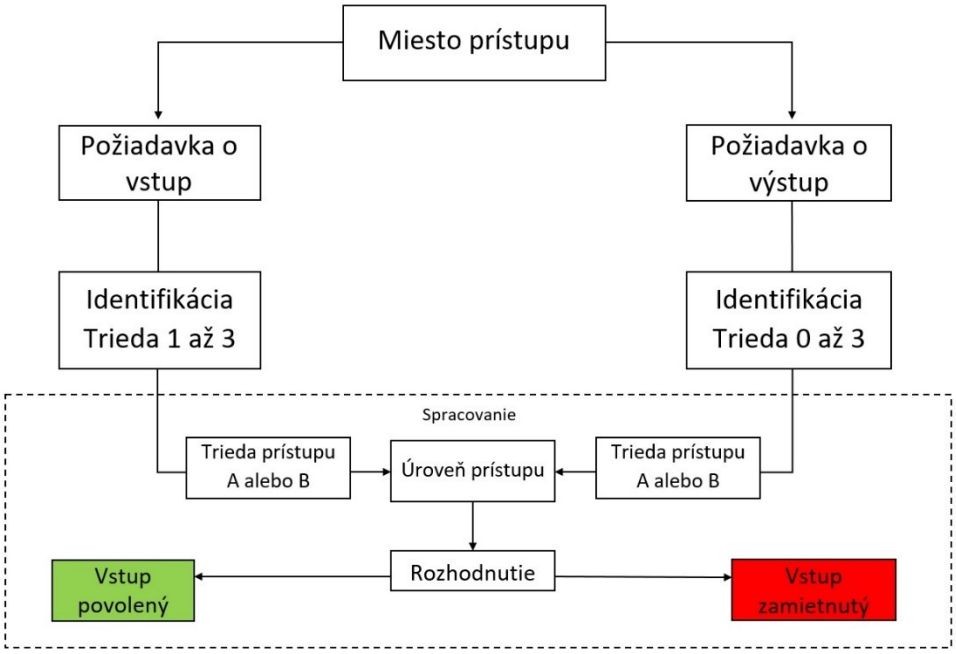
Trieda 2 – vyžaduje pevný identifikačný prvok, ako sú prístupové karty alebo biometrické prvky vstupujúcej osoby.

Trieda 3 – využíva kombináciu prvkov prvej a druhej triedy alebo kombináciu identifikačného prvku a biometrickej metódy.

Triedy prístupu:

Trieda A – systém nepoužíva časové filtre, prístup nie je časovo obmedzený.

Trieda B – systém používa časové filtre a musí ukladať prístupové informácie. Ukladá do pamäti informácie o napadnutí systému, otvorenie prístupu bez oprávnenia alebo odmietnutý prístup a tiež otvorenie prístupu po uplynutí povolenej doby.[14]



Obr. 15: Postup povolenia prístupu.[14, upravil Potúček 2017]

Elektronická forma prístupových systémov si našla svoje uplatnenie v chránených zónach, strážených parkoviskách, ale aj zaznamenávanie a evidenciu návštev v organizáciách. Všetky zmeny, pokusy o vstupy, alebo akékoľvek neštandardné postupy sa zaznamenávajú do databázy. Prístupový systém v prípade týchto podmienok umožňuje zasielanie upozornenia na mobil alebo e-mail.

4.2.1 Spôsoby a možnosti prístupového systému

Biometrická identifikácia – funguje v tomto systéme pomocou biometrického odtlačku prsta alebo ruky. Systém môže fungovať pomocou internetového pripojenia a s možnosťou zadávania príkazov o oprávnení v reálnom čase.

Automatický zabezpečovací systém – dokáže vyhodnotiť pohyb osôb a ich počet v danom objekte a po opustení zóny poslednou osobou sa automaticky zapne zabezpečovací systém.

Ovládanie výťahov – osoby sa musia identifikovať ID kartou, ktorá im umožní prístup na poschodie vopred povolené. Systém zabezpečuje evidenciu osôb cez webové rozhranie, pomocou ktorého je znemožnený nekontrolovateľný pohyb osôb po budove organizácie.

4.2.2 Rozdelenie prístupových systémov podľa typu

Podľa typu môžeme prístupové systémy rozdeliť na autonómne prístupy, ktoré sú jednoduché a spoľahlivé, sú bez pripojenia do počítačovej siete a fungujú bez užívateľského programu. Ďalším typom je prístup Lite, ktorý je tiež bez pripojenia do počítačovej siete, ale obsahuje užívateľský program pre nastavenie vstupných dát pre jednotlivé osoby. Vysoko výkonným serverovým systémom je sieťový prístupový systém s pripojením snímačov do počítačovej siete.

4.2.2.1 Autonómny prístupový systém

Je určený na riadenie a kontrolu prístupu do objektov. Vyznačuje sa ľahkou inštaláciou, jednoduchosťou ovládania a riadenia prístupu. Je navrhnutý ako krabicový systém. Pozostáva z čítacieho zariadenia, riadiacej elektroniky a referenčnej čipovej karty.

Obr. 16: Autonómny prístupový systém.[15]

Čítacie zariadenie ovláda ľubovoľné elektrické zariadenia, napríklad turniket alebo závoru a po priložení ID karty k čítaciemu zariadeniu na komunikačnú vzdialenosť do 5 cm sa povolí vstup danej osobe.

Referenčná čipová karta je jedinečná tým, že má špeciálne oprávnenia, pomocou ktorých daná osoba ovláda celý prístupový systém. Bezpečnosť používateľov je zabezpečená tým, že jednu čipovú kartu nemôžeme použiť pre iné prístupové systémy, ktoré neboli vopred povolené. Základom tohto systému je vytvorenie čipových kariet pre určitú skupinu osôb, ktoré majú prístup do tých istých priestorov, napríklad pracovníci jednej kancelárie. Ak dôjde k strate jednej z kariet z jednej kancelárie, nemusia sa rušiť prístupové práva všetkým pracovníkom, stačí zrušenie prístupových práv len tým kartám, ktoré mali rovnaké povolenia ako stratená karta.

Master karta umožňuje programovanie jednotlivých snímačov, napríklad vkladanie nových údajov, ich zmeny a vymazanie kariet. Prostredníctvom Master karty sa dajú nastaviť jednotlivé oneskorenia otvorenosti zámkov.

Autonómny prístupový systém sa používa pre vchodové dvere na obytných domoch, internátnych budovách a pracovných prevádzkach. Umožňuje jednostranné alebo obojstranné otváranie dverí, turniketov a iných vstupných elektrických zariadení.

4.2.2.2 Sieťový prístupový systém

Sieťový prístupový systém je serverová aplikácia s použitím databázového serveru. Systém sa dá ovládať z ktoréhokoľvek počítača pripojeného k internetovej sieti, nie je obmedzený počtom užívateľov. Vyznačuje sa vysokým užívateľským komfortom pri správe osôb, užívateľov a prístupových práv. Umožňuje import rôznych dát z akéhokoľvek iného prístupového systému. V prípade ak snímač nemá spojenie zo serverom, napríklad pri výpadku prúdu alebo pádu systému, prejde do stavu offline a jeho dáta a funkčnosť zostávajú zachované.

Sieťový prístupový systém je zložený z koncentrátora, dverového terminálu s čítacím zariadením a počítača so softwarom. Riadiacou jednotkou sieťového prístupového dochádzkového systému je koncentrátor EM808.1. Koncentrátor komunikuje s PC centrom a využíva pritom protokol TCP/IP, čo umožňuje komunikáciu cez internet.

Obr. 17: Koncentrátor EM 808.1.[16]

Riadiaca elektronika čítacieho terminálu predstavuje oddelenú časť umiestnenú vo vnútornom priestore objektu, čím sa zvyšuje bezpečnosť celého systému. Čítačka môže byť vybavená modulom s číselnou klávesnicou, kde je potrebné zadať vstupné heslo (PIN).

Obr. 18: Dverový prístupový terminál EM551.[16]

Sieťové prístupové systémy sa využívajú vo firmách a organizáciách s rôznym počtom zamestnancov. Môže sa využívať aj v organizáciách, ktoré majú viacposchodové budovy alebo sú od seba vzdialené.

4.2.2.3 Prístupové systémy Lite

Je to vyššia verzia prístupového systému, kde nie sú snímače pripojené k počítačovej sieti a preto fungujú autonómne. Prístupové dáta je možné nastaviť alebo nainštalovať do počítača s existujúcim užívateľským rozhraním, kedy je jednotlivým osobám povolený vstup do objektu. Nastavenia povolenia karty do snímača je realizované pomocou špeciálneho kábla, ktorý sa pripojí priamo k snímačom. To znamená, že takýmto spôsobom musíme fyzicky zapojiť všetky snímače, na ktorých chceme zmeniť nastavenie prístupových práv. Takýto program nedáva možnosť vytvárania časových zón. Karty, ktoré sa dajú nahrať do snímača sú limitované pamäťou snímača.

Medzi hlavné dôvody používania dochádzkových a prístupových systémov patrí uľahčenie a zamedzenie častých chýb pri spracovaní dát. Ďalším dôvodom je to, že výsledné údaje o dochádzke sa ľahšie kontrolujú, poprípade sa dopĺňajú chýbajúce údaje, ktoré je možné prehľadne tlačiť pomocou rôznych prehľadových zostáv alebo exportovať do nadväzujúcich systémov. Prístupové systémy umožňujú ľahší vstup do objektu na základe čipových kariet, ktoré sú použiteľné len pre určité časti objektu. Tým sa zabezpečí, že do oblasti s kontrolovaným vstupom môžu vstupovať len tie osoby, ktoré majú na to oprávnenie.

II. PRAKTICKÁ ČASŤ

5 SYSTÉMY PRE KONTROLU DOCHÁDZKY

Biometrické systémy sú zložené z čítačky odtlačkov prstov a softwaru, ktorého úlohou je porovnať pravosť odtlačkov. Čítačka s počítačom je spojená prostredníctvom paralelného portu. Pri prihlasovaní a priložení odtlačku prsta pošle čítačka odtlačkov prstov získanú bitmapu počítaču. Ten vyhľadá v databáze danú registračnú šablónu a porovná zhodu so zadaným obrazom odtlačku prsta. Ak nastáva zhoda v podobnosti obrazu, je daná osoba identifikovaná.

Biometrické dáta nebývajú obyčajne spracovávané v pôvodnom formáte. Spracovávajú sa len dôležité a pre identifikáciu podstatné a špecifické znaky. Týmto sa podstatne redukuje objem a veľkosť dát. Tie sa uložia ako registračné záznamy. Existujú štyri možnosti ako uložiť získané dáta:

- na kartu,
- do centrálnej databázy na server,
- do pracovnej stanice,
- priamo do autentizačného terminálu.

Biometrické vzorky a spracovávané údaje sú veľmi citlivé materiály, ktoré by mali byť uložené v zašifrovanej podobe bez ohľadu na aké účely sa budú používať.

Prevádzkovateľ môže spracúvať biometrické údaje len vtedy, ak to vyplýva zo zákona o ochrane osobných údajov, alebo ak mu na spracúvanie dala písomný súhlas dotknutá osoba. Biometrické údaje zasahujú do citlivých osobných údajov a súkromia človeka.

5.1 Dochádzkový systém

Dochádzkové systémy sú určené na evidenciu dochádzky a následné spracovanie dát, ktoré sa spracovávajú priamo v mzdových systémoch. Samotné registrovanie dochádzky na biometrických termináloch je automatizované spracovanie údajov zo snímačov do spracovania dochádzky.

Dochádzkový systém má moderný program, kde:

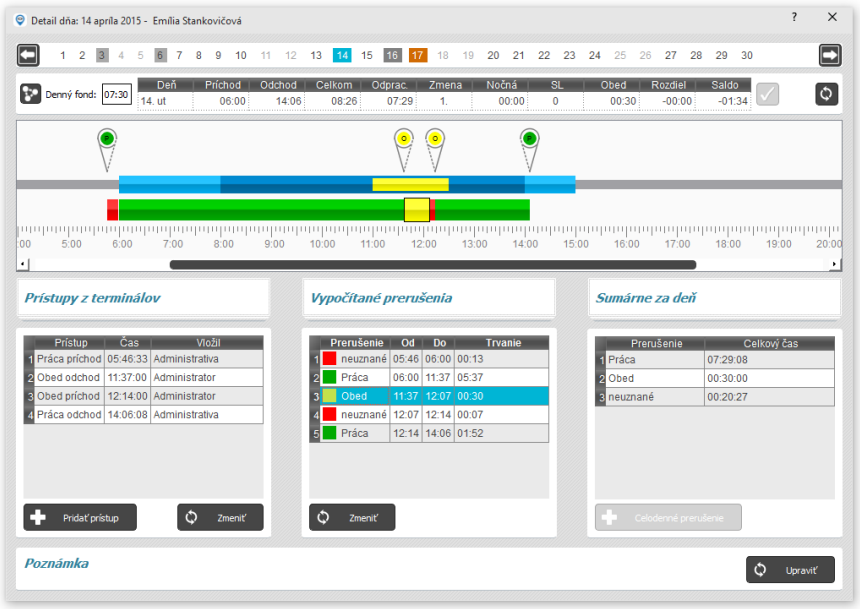
- Každý zamestnanec má nastavovaný individuálny záznam.
- Obsahuje podporu monitorovania jeho aktivít.
- Obsahuje podporu dovoleniek, sviatkov, voľna.
- Zaznamenáva skoršie príchody, skoršie odchody, meškania a celkový odpracovaný pracovný čas.

- Systém automaticky generuje mesačné dochádzkové reporty s presnou dochádzkou jednotlivých zamestnancov, s presnou dochádzkou všetkých zamestnancov, celkový odpracovaný čas jedného zamestnanca, celkové meškanie zamestnanca a tiež celkovú mesačnú štatistiku dochádzky.
- Je možné zadávať základné a tiež osobné údaje zamestnancov denne, mesačne a tiež je možné zadávať individuálne reporty.

Dochádzkovými systémami zamedzíme podvodom pri evidencii príchodov. Tiež redukuje pracovné vyťaženie nadriadených a zároveň obmedzí chybnosť pri spracovávaní dát. Ďalším podstatným dôvodom pre zavedenie dochádzkového systému je zjednodušenie spracovania dochádzky pre personálne a mzdové oddelenie. No základom a podstatou dochádzkových systémov je prehľad dochádzky.

5.1.1 Biometrické dochádzkové systémy

Dochádzkový systém **SYSTEM-IS AMS** umožňuje prehľad dochádzky zamestnancov. Zaujímavosťou tohto systému je nastavenie denného grafu v detaile dňa, jeho koncepcia je nastavená na vizualizáciu výpočtov. Môžeme nastaviť pevnú a pohyblivú pracovnú dobu konkrétneho dňa, príchody a odchody zamestnancov a iných vlastností skupiny.



Obr. 19: Denný graf a úprava dochádzky – System-IS AMS.[17]

Prostredníctvom grafu môžeme vidieť jednotlivé časové úseky prerušenia dochádzky. Vypočítané úseky môžeme dopĺňať a aktualizovať.[17]

Ďalším dochádzkovým systémom na trhu je **ATTENDANCE PRO W**. Taktiež umožňuje evidenciu dochádzky a spracovanie výstupov z tejto dochádzky priamo v mzdových systémoch. Evidencia dochádzky je vykonávaná prostredníctvom biometrických terminálov alebo formou bezkontaktných terminálov RFID. V programe je možné vytvoriť zoznam oddelení a zároveň nastaviť každé oddelenie samostatne.[18]

5.2 Prístupové systémy

Zabezpečenie pracovísk, kancelárií, laboratórií a iných priestorov uskutočňujú prístupové systémy, ktoré spoľahlivo riešia kontrolu a ochranu hmotného a nehmotného majetku. Zabezpečujú kontrolu prístupu k informáciám v daných spoločnostiach a pracoviskách.

Hlavnou úlohou prístupového systému býva zabezpečiť kontrolu pri vstupe do objektov, umožňuje sledovať pohyb osôb v priestore a čase. To znamená, že umožní povoliť vstup zamestnancov do povolených objektov len v presne určenom čase. Umožňuje mať pod kontrolou pohyb všetkých osôb v daných priestoroch. Systém presne eviduje, kto danými dverami prešiel a aký čas bol v danom priestore. V systéme je možné zadefinovať určité pravidlá, napríklad vedúci pracovník má povolený vstup všade, zamestnanec len do určitých miestností. Programy v prístupových systémoch zhodnotia koľko ľudí sa nachádza v priestore, ich zoznam aj dĺžku pobytu v objekte. Prístupový systém môže tiež slúžiť ako evidenčný systém pre vstup a výstup zamestnancov. V systéme sa môžu robiť zmeny aj v priebehu roka, kde nastavenie podmienok a daných parametrov prispôsobujeme daným požiadavkám. Komponenty sa môžu dodatočne nainštalovať.

5.2.1 Biometrické prístupové systémy

Prístupový systém **ARBE** eviduje ľudí v určitých objektoch. Môže byť navzájom prepojený aj so zabezpečovacím systémom a po opustení miestnosti poslednou osobou sa automaticky aktivuje. V tomto systéme sa namiesto bezkontaktnej identifikačnej karty používa biometrický odtlačok prsta ruky. Systém má možnosť pridávať a odoberať oprávnenia, pracuje on-line.[19]

Biometrický prístupový systém **ALVENO** využíva najnovšie technológie pri zabezpečovaní ochrany daných objektov. Identifikačný systém spozná zamestnanca po priložení čipu alebo odtlačku prsta.

Obr. 20: Prístupový systém ALVENO.[20]

Systém Alveno po identifikácii zamestnanca prostredníctvom určitého identifikačného prvku umožní jeho vstup do objektu. Program Alveno Access zabezpečí prehľad o pohybe zamestnancov v priestoroch objektov a zároveň obmedzenie prístupu do určitých miestností. Pri čítačkách je možné vytlačiť prehľad zamestnancov, ktorí ju v daný deň použili.[20]

Profesionálny prístupový systém **PATROL** zabezpečuje spoľahlivé sledovanie, evidenciu a riadenie prechodov osôb do objektov a priestorov čítačiek. Systém je vysoko spoľahlivý a bezpečný, spravuje biometrické a tiež bezkontaktné čítačky. Identifikačné údaje sa prenášajú do všetkých čítačiek v sieti. Je možné importovať dáta z iných informačných systémov a tiež umožňuje export prístupových transakcií do rôznych systémov, vrátane dochádzkových.[21]

6 KOMERČNE DOSTUPNÉ SYSTÉMY

V 21. storočí máme nové trendy v práci aj v pracovnom prostredí. Jedným z prvkov je flexibilná pracovná doba. Kontrola a evidencia dochádzky zamestnancov by v minulosti bola náročná. Dnes máme na evidenciu dochádzky prístupové a dochádzkové systémy, ktoré nám umožňujú kontrolovať dochádzku zamestnancov. Obmedzujú výskyt chybných údajov pri spracovaní dát o dochádzke, zvyšujú efektívne využívanie pracovného času a celkovej pracovnej morálky. Flexibilná pracovná doba zvyšuje pracovitosť zamestnancov a zároveň je menej stresujúca.

Dochádzkovým systémom môžeme sledovať zamestnancov počas celej pracovnej doby na základe podkladov, ktoré sa prostredníctvom biometrických terminálov dostávajú do programov, ktoré vedia ukázať do akej miery zamestnanec, ale aj celá firma využíva svoj pracovný čas. Informácie z biometrických terminálov sa automaticky prepočítavajú a vytvárajú sa pre zamestnancov dochádzkové listy, ktoré sa prenesú do mzdových systémov, kde sa následne spracúvajú. Najväčšou výhodou týchto terminálov je, že ich nemožno zneužiť. Pri verifikácii porovnávajú počet bodov na prste, alebo používajú identifikáciu osôb podľa ich jedinečných fyzických znakov. V súčasnosti máme na trhu množstvo nových inovatívnych terminálov, ktoré majú multifunkčné vlastnosti.

6.1 Typy biometrických terminálov

Veľkou výhodou biometrických terminálov je rýchla a jednoznačná identifikácia užívateľa. Terminály obsahujú čítačku kontaktných čipov alebo snímačov bezkontaktných technológií. Konfigurácia a nastavenie terminálov sa uskutočňuje pomocou pridaného softwaru, ktorý umožňuje komunikáciu a úpravu priamo na mieste.

Biometrické terminály sú vo väčšine prípadov kombinované. Využívajú dve alebo viac biometrických metód na identifikáciu osôb. Najčastejšie sa používa prepojenie identifikácie pomocou odtlačkov prstov a tváre. Do popredia sa dostávajú terminály s väčším LCD displejom, poprípade dotykovým displejom a komunikáciou prostredníctvom WiFi.

Jednou z inovatívnych biometrických čítačiek odtlačkov prstov pre riadenie a kontrolu prístupových a dochádzkových systémov je **MA300**. Je bezkonkurenčne výkonný a maximálne spoľahlivý, zamedzí vstupu neoprávneným osobám do objektu vďaka biometrickému snímaniu odtlačkov prstov.

Obr. 21: Biometrická čítačka MA300.[22]

Môže byť inštalovaný samostatne alebo ako súčasť systému. Je nastaviteľný ľahko a pohodlne cez Bluetooth, či mobilnou aplikáciou ovládanou administrátorom. Jeho kovový obal zvyšuje odolnosť proti mechanickému poškodeniu a je odolný voči vode, prachu a inému vonkajšiemu poškodeniu s certifikáciou IP65.

Tab. 1: Technické parametre biometrickej čítačky MA300

Kapacita odtlačkov prstov	1500
Kapacita ID kariet	10000
Senzor	Optický ZK
Komunikácia	RS485, TCP/IP, USB-host, Bluetooth
Pracovná teplota	-10 °C- 60 °C
IP ochrana	IP65
Rozmery	73x148x34,5mm
Hmotnosť	1,15kg

Ďalším typom z radu biometrických čítačiek odtlačkov prstov pre prístupové dochádzkové systémy je **X8-BT**. Má vynikajúcu spoľahlivosť, presnosť a rýchlosť. Môže pracovať v samostatnom režime s rozhraním tretích strán, napríklad s elektrickým zámkom, alarmom, zvončekom a senzorom otvorenia dverí.

Obr. 22: Biometrická čítačka X8-BT.[23]

Dotyková klávesnica zabezpečuje jednoduché a pohodlné použitie. Podporuje komunikáciu cez Bluetooth alebo pomocou mobilnej aplikácie, s možnosťou meniť nastavenia a prehľad dát.

Tab. 2: Technické parametre biometrickej čítačky X8-BT

Kapacita odtlačkov prstov	500
Kapacita ID kariet	500
Senzor	SilkID
Komunikácia	Bluetooth
Pracovná teplota	-10 až 60°C
Rozmery	101,5x101,5x37mm

Inovatívny výrobok **MB360** pozostáva z pokročilých ZK overovacích technológii. Podporuje viac overovacích metód vrátane tváre, odtlačkov prstov, karty, hesiel alebo kombináciu medzi nimi. Je vybavený numerickou klávesnicou a farebným displejom.

Obr. 23: Biometrický terminál MB360.[24]

Overovanie užívateľov trvá menej ako jednu sekundu. Má elegantný vzhľad a dokonalú spoľahlivosť pri komunikácii s počítačovým riadiacim systémom. Dokonale zapadá do akéhokoľvek prostredia.

Tab. 3: Technické parametre biometrického terminálu MB360

Kapacita tvárí	1 200
Kapacita odtlačkov prstov	1 500
Kapacita ID kariet	2 000
Displej	2,8 palcový
Komunikácia	TCP/IP, USB-Host, Wi-Fi
Pracovná teplota	0 až 45°C
Rozmery	167,5x148,8x32,2mm
Hmotnosť	380g

SFace900 je prvý terminál, ktorý je vybavený vysoko výkonným fotoaparátom, ktorý umožňuje inštaláciu vonku, v polokrytom vonkajšom prostredí a je odolný poveternostným podmienkam. Poskytuje rýchle snímanie suchých, drsných, ale aj mokrých odtlačkov prstov.

Obr. 24: Biometrický terminál SFace900.[25]

Biometrický terminál SFace900 má vstavanú batériu, ktorá poskytuje 4 hodiny nepretržitej prevádzky. Zariadenie umožňuje uložiť 1200 šablón tvárí, 2000 odtlačkov prstov a dokáže obsiahnuť až 10 000 ID kariet. Jeho veľká úroveň zabezpečenia je dosiahnutá multifunkčnými biometrickými overovacími technológiami.

Tab. 4: Technické parametre biometrického terminálu SFace900

Kapacita tvárí	1 200
Kapacita odtlačkov prstov	2 000
Kapacita ID kariet	10 000
Displej	4,3 palcový, dotykový
Komunikácia	TCP/IP, RS232/485, USB-Host
Pracovná teplota	0 až 45°C
Rozmery	195,5x166,5x120mm
Hmotnosť	1,6kg

Multibiometrický dochádzkový a prístupový systém **P160** používa najnovšiu technológiu snímania geometrie dlane a odtlačkov prstov. Dokáže uchovať 600 snímok dlane a 20 000 odtlačkov prstov bez rozdeľovania do skupín.

Obr. 25: Biometrický terminál P160.[26]

Využíva 2,8 palcový farebný displej, ktorý je doplnený klávesnicou. Vyznačuje sa elegantným dizajnom a jednoduchou inštaláciou. Rýchlosť overovania trvá menej ako 1 sekundu.

Tab. 5: Technické parametre biometrického terminálu P160

Kapacita geometrie dlane	600
Kapacita odtlačkov prstov	20 000
Kapacita ID kariet	10 000
Displej	2,8 palcový
Komunikácia	TCP/IP, USB-Host, Wi-Fi
Pracovná teplota	0 až 45°C
Rozmery	179,95x134,94x38,5mm
Hmotnosť	1,2kg

Dochádzkový systém **BioSmart-Zpad** je kombináciou biometrického systému a operačného systému android, vďaka ktorému je pohodlnejší pre užívateľov. Má zabudovanú čítačku prstov a ID kariet. Obsahuje viac ako 10 profesionálnych dochádzkových aplikácií, ku ktorým môžete pridať vlastne vytvorené aplikácie v systéme android.

Obr. 26: Biometrický terminál BioSmart-Zpad.[27]

Jeho hlavnou výhodou je 7 palcový multi-dotykový LCD displej, na ktorom si môžete upravovať témy svojho užívateľského prostredia a umožňuje priblížiť zobrazený text pre lepšiu čitateľnosť.

Tab. 6: Technické parametre biometrického terminálu BioSmart-Zpad

Rozlíšenie displeja	800x480 Pixel
Systém	Android 4.1
CPU	1 Ghz Dual-core
Ram	1 GB
Pamäť	4 GB
Maximum používateľov	10 000
Komunikácia	TCP/ IP, Wi-Fi, USB-Host a Client
Pracovná teplota	0 až 45°C
Rozmery	222x135x51,4mm
Hmotnosť	620g

7 NOVÉ TRENDY BIOMETRICKÝCH SYSTÉMOV

Množstvo inovatívnych aplikácií s biometrickými prvkami sa stále viac využívajú v každodennom živote. Kamery sú k dispozícií na bezdrôtové snímanie odtlačkov prstov, očí, tváre. Mikrofón sa používa na rozpoznanie hlasu a ďalšie prvky, ktoré využívame v biometrických zariadeniach.

Model biometrickej karty zahŕňa integráciu biometrického snímača do karty s cieľom nahradiť heslá a PIN kódy. Karta bude fungovať až potom, keď ju užívateľ biometricky aktivuje. Jedným z kľúčových cieľov je umožniť používanie karty v bankovníctve a aktivovať ju odtlačkom prsta alebo skenerom dúhovky. Novým trendom je aktivácia prostredníctvom EKG frekvenciou srdca. **Nymi** je nositeľný náramok, ktorý overí identitu užívateľa prostredníctvom EKG a je biometricky jedinečný. Náramok sa bude využívať pri platbe a pri prístupových systémoch.[28]

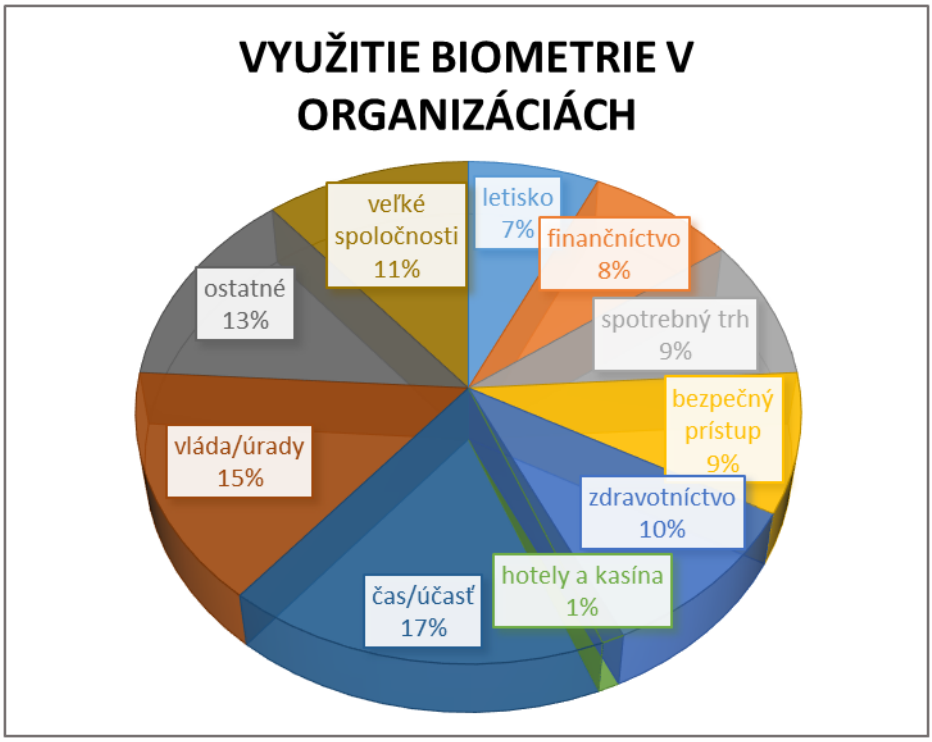
Obr. 27: Platba prostredníctvom náramku Nymi.[29]

Svet technológií sa neustále vyvíja a potreba biometrickej identifikácie sa stáva takmer nevyhnutnou záležitosťou. Používanie jednej fyziologickej alebo behaviorálnej charakteristiky pre zápis, overovanie a identifikáciu, pre dôkladné zabezpečenie sa stane nevyhovujúcim. A preto sa do popredia dostáva multimodálna biometrická technológia, ktorá kombinuje dve alebo viac biometrických údajov k identifikácii. Biometrické vlastnosti sú navzájom nezávislé, nedochádza k matematickým kombináciám, čo vedie k vyššej presnosti identifikácie.

7.1 Využitie biometrických systémov v praxi

Biometria si v spoločnosti našla svoje výrazné miesto a tento trend sa bude v budúcnosti ešte zvyšovať. Jednotlivé biometrické technológie identifikácie sa líšia, ale ich podstata je rovnaká. V súčasnosti sa stretávame s biometrickými technológiami v bežnom živote, napríklad nové mobilné telefóny a notebooky, ale najmä v organizáciách v dochádzkových a prístupových systémoch. Biometrické aplikácie využívame hlavne pri identifikácii osôb a ochrane dát.

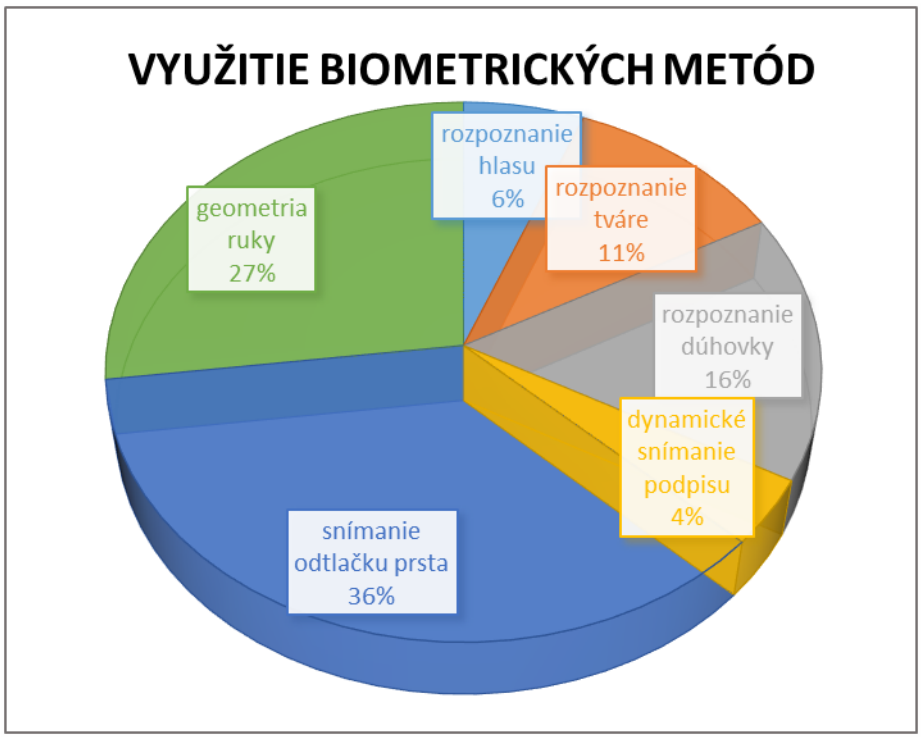
Biometrické systémy sa uplatňujú v mnohých organizáciách a veľkých spoločnostiach. Používajú sa pri kontrole totožnosti osôb a ochrane citlivých informácií vo vláde, na úradoch, na letiskách, v zdravotníctve a v iných dôležitých oblastiach.



Obr. 28: Využitie biometrie v organizáciách.[30, upravil Potúček 2017]

Bezpečné biometrické systémy v identifikácii odtlačkov prstov alebo očnej dúhovky nahrádzajú heslá alebo PIN kódy, ktoré sa používali v organizáciách. Kvalitnejšia ochrana sa docieli kombináciou týchto biometrických metód. Dochádzkové a prístupové systémy majú pre kontrolu osôb alebo ochranu dát multifunkčné biometrické terminály, ktoré využívajú viaceré biometrické metódy identifikácie.

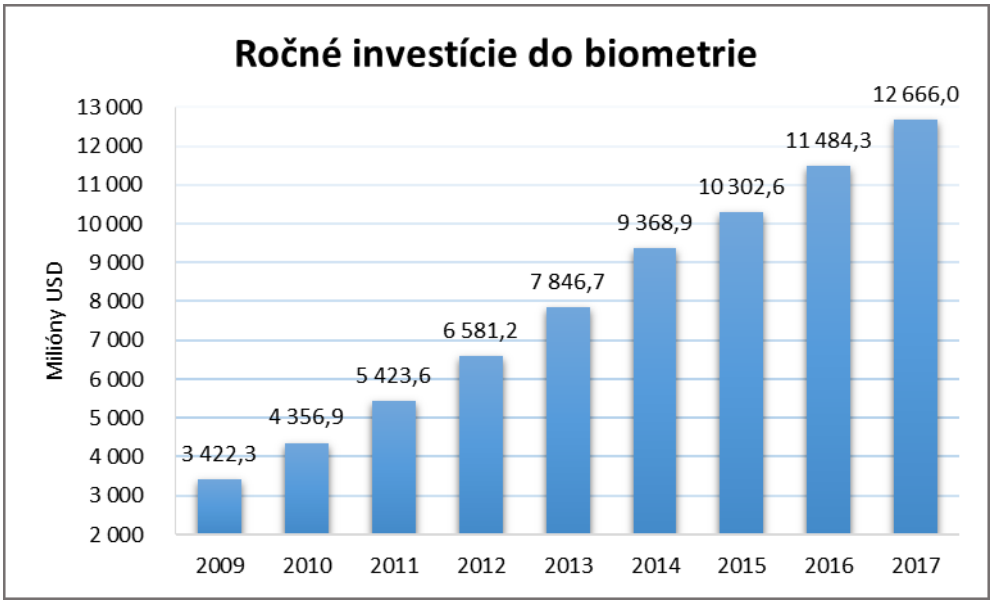
Porovnanie biometrických technológií v systémoch na súčasnom trhu naznačuje obrázok č. 29.



Obr. 29: Využitie biometrických metód.[30, upravil Potúček 2017]

Najčastejšie sa stretávame s používaním biometrie, ktorá sníma odtlačky prstov. Ďalšou veľmi rozšírenou technológiou je geometria snímania ruky. Organizácie si musia určiť aké zabezpečenie chcú v danom podniku zaviesť a vybrať najvhodnejší typ. Pomocou identifikačných čipových kariet sa porovnáva identita so skutočnými fyzickými charakteristikami a dátami uvedenými na karte. Pomocou kombinácie odtlačkov prstov a fotografie sa dá vylúčiť zneužitie a tak zvýšiť bezpečnosť.[30]

V poslednej dobe sa investuje do biometrie a do biometrických systémov dosť finančných prostriedkov, čo znázorňuje aj nasledujúci graf.



Obr. 30: Ročné investície do biometrie.[3, upravil Potúček 2017]

Dôvodom je stále rastúci dopyt po prístupových systémoch, ktoré zabezpečia dané objekty a cenné predmety. Taktiež je možné využívať biometrické systémy v boji s terorizmom, kde systém hľadá nebezpečné osoby na zoznamoch alebo pomocou kamerových systémov. V dochádzkových systémoch zaznamenávajú príchody a odchody zamestnancov a tiež evidenciu a kontrolu dochádzky. Biometrické systémy sa stále vyvíjajú a dosahujú dokonalejšie produkty.[3]

ZÁVER

Biometrické systémy sú v našej spoločnosti stále viac rozšírenejšie v rôznych odvetviach. Vhodné biometrické prostriedky nám umožňujú zabezpečiť a ochrániť objekty, prístroje, cenné predmety, rôzne štátne inštitúcie, ale tiež ľudí, ktorí sa nachádzajú v týchto objektoch.

Prínos tejto práce spočíva v popísaní využitia biometrických metód v dochádzkových a prístupových systémoch, ktoré zastávajú nezastupiteľnú úlohu pri kontrole identity osôb pri ich vstupe do objektov, sledovanie ich pohybu a času strávenom v tomto objekte. Tieto systémy uľahčujú evidenciu a kontrolu zamestnancov, prehľad dochádzky a následné spracovanie dát v mzdovom systéme.

V závere práce som uviedol nové trendy využitia biometrických metód v dochádzkových a prístupových systémoch. Keďže tradičné bezpečnostné metódy prestávajú spĺňať kritériá pre bezpečnosť, pri neustálom rozvoji počítačových technológií dochádza k ich častému zneužívaniu, kopírovaniu a odcudzovaniu. Na základe analýzy dostupných typov biometrických systémov som poukázal na nové inovatívne terminály, ktoré majú multifunkčné vlastnosti a tým nám znásobia bezpečnosť.

V tejto bakalárskej práci sa mi podarilo poukázať na nové trendy biometrických systémov, ktoré v budúcnosti zabezpečia ľahší a bezpečnejší život.

ZOZNAM POUŽITEJ LITERATÚRY

[1] Čo je biometria? *biometria.sk* [online]. Banská Bystrica, Lazovná 12, PSČ 974 01 [cit. 2016-12-10]. Dostupné z: http://www.biometria.sk/co-je-biometria.html

[2] Rak, Roman, Vašek MATYÁŠ a Zdeněk ŘÍHA. *Biometrie a identita člověka ve forenzních a komerčních aplikacích.* Praha: Grada, 2008. ISBN 978-80-247-2365-5.

[3] DRAHANSKÝ, Martin a Filip ORSÁG. Biometrie. [Brno: M. Drahanský], 2011. ISBN 978-80-254-8979-6.

[4] Uwierzytelnianiebiometryczne i skimmery. *trybawaryjny.pl* [online]. [cit. 2016-12-12]. Dostupné z: http://trybawaryjny.pl/uwierzytelnianie-biometryczne-i-skimmery/

[5] Ďásek, M. Biometrika. *akela.mendelu.cz* [online]. 2003 [cit. 2016-12-13]. Dostupné z: https://akela.mendelu.cz/~lidak/bif/dasek.html

[6] Otevírame vchodové dveře biometricky. *ceskestavby.cz* [online]. České Budějovice, Kostelní 942/46, PSČ 370 04, 2011 [cit. 2016-12-13]. Dostupné z: http://www.ceskestavby.cz/clanky/otevirame-vchodove-dvere-biometricky-20498.html

[7] Biometrie obličeje. *Biometricke-ctecky.cz* [online]. Brno, Edisonova 5, PSČ 612 00 [cit. 2016-12-12]. Dostupné z: http://www.biometricke-ctecky.cz/biometriky/oblicej/

[8] Structureof DNA. *Openwalls.com* [online]. [cit. 2016-12-12]. Dostupné z: http://openwalls.com/image?id=4587

[9] BOLLE, Ruud. *Guide to biometrics*. New York: Springer, c2004. ISBN 03-874-0089-3.

[10] Dithering – z teorie zpracování digitálního záznamu. *Muziku.cz* [online]. [cit.2016-12-13]. Dostupné z: http://www.muzikus.cz/pro-muzikanty-testy/Dithering-z-teorie-zpracovani-digitalniho-zaznamu~15~cervenec~2004/

[11] ASHBOURN, Julian. *Practical biometrics: from aspiration to implementation.* New York: Springer, c2004. ISBN 1852337745.

[12] Dochádzkové systémy. *variaflex.sk*[online]. [cit. 2016-12-13]. Dostupné z: https://variaflex.sk/dochadzkove-systemy

[13] Dochádzkový systém. *vema.sk* [online]. Bratislava, Plynárensa 7, PSČ 821 09 [cit. 2016-12-13]. Dostupné z: http://www.vema.sk/dochadzkovy-system/

[14] KŘEČEK, Stanislav. *Příručka zabezpečovací techniky.* Vyd. 2. [S.l.: s.n.], 2003. ISBN 80-902938-2-4.

[15] EM3161 FR. *EMware.*com [online]. [cit. 2016-12-13]. Dostupné z: http://www.emware.com/page16.html

[16] Prístupový systém. *TransData.sk* [online]. Bratislava, Jašíkova 2, PSČ 821 03 [cit. 2016-12-13]. Dostupné z: http://www.transdata.sk/sk/pristupovy-system-1

[17] Denný graf v detaile dňa a úprava dochádzky. *dochadzkovy.system-is.com* [online]. Banská Bystrica, Lazovná 56, PSČ 974 01 [cit. 2017-03-19]. Dostupné z: http://dochadzkovy.system-is.com/denny-graf-v-detaile-dna-uprava-dochadzky

[18] Docházkový systém AttendanceProW. *biometric.sk*[online]. Bratislava, Rovniakova 2, PSČ 851 01 [cit. 2017-03-11]. Dostupné z: https://biometric.sk/dochadzkovy-system/

[19] Prístupový systém. *arbe.sk* [online]. Bratislava, Pekná cesta 19, PSČ 831 52 [cit. 2017-03-20]. Dostupné z:http://www.arbe.sk/index.php/pristupovy-system.html

[20] Alveno přístupový systém. *trollcomputers.cz* [online]. Česká Lípa, U Vodního hradu 1394/28, PSČ 472 01 [cit. 2017-03-20]. Dostupné z: http://trollcomputers.cz/dochazkove-systemy-alveno/alveno-pristupovy-system/

[21] Prístupový systém Patrol. *biometria.sk* [online]. Basnká Bystrica, Lazovná 12, PSČ 974 01 [cit. 2017-03-20]. Dostupné z: http://www.biometria.sk/pristupovy-system.html

[22] MA300-BT (New). *zkteco.com* [online]. [cit. 2017-04-03]. Dostupné z: http://www.zkteco.com/product/MA300-BT_(New)_505.html

[23] X8-BT (New). *zkteco.com* [online]. [cit. 2017-04-03]. Dostupné z: http://www.zkteco.com/product/X8-BT_(New)_504.html

[24] MB360 (New). *zkteco.com* [online]. [cit. 2017-04-03]. Dostupné z: http://www.zkteco.com/product/MB360_(New)_500.html

[25] SFace900 (New). *zkteco.com* [online]. [cit. 2017-04-03]. Dostupné z: http://www.zkteco.com/product/SFace900_(New)_512.html

[26] P160 (New). *zkteco.com* [online]. [cit. 2017-04-03]. Dostupné z: http://www.zkteco.com/product/P160_(New)_524.html

[27] BioSmart-Zpad. *zkteco.com* [online]. [cit. 2017-04-03]. Dostupné z: http://www.zkteco.com/product/BioSmart-Zpad_237.html

[28] Biometric Trends for 2017. *veridiumid.com* [online]. Boston, Quincy, MA 02171, USA [cit. 2017-04-30]. Dostupné z: https://www.veridiumid.com/blog/biometric-trends-for-2017/

[29] Putting Nymi´s biometric wearable payments through its paces. *betakit.com* [online]. [cit. 2017-05-02]. Dostupné z: http://betakit.com/putting-nymis-biometric-wearable-payments-through-its-paces/

[30] Biometrické systémy v praxi. *systemonline.*cz [online]. Brno, Okružní 19, PSČ 638 00 [cit. 2017-05-03]. Dostupné z: https://www.systemonline.cz/clanky/biometricke-systemy-v-praxi.htm

ZOZNAM POUŽITÝCH SYMBOLOV A SKRATIEK

DNA	Deoxyribonukleová kyselina
FBI	Federálny vyšetrovací úrad
PIN	Osobné identifikačné číslo
ID karta	Identifikačná karta
PC	Osobný počítač
TCP/IP	Protokoly pre komunikáciu v počítačovej sieti
RFID	Identifikácia na rádiovej frekvencii
LCD	Displej z tekutých kryštálov
RS485	Komunikačná zbernica
WiFi	Bezdrôtová sieť
IP	Stupeň ochrany
EKG	Elektrokardiografia

ZOZNAM OBRÁZKOV

ZOZNAM TABULIEK