Pedagogická fakulta
Faculty of Education

Jihočeská univerzita v Českých Budějovicích
University of South Bohemia in České Budějovice

JIHOČESKÁ UNIVERZITA V ČESKÝCH BUDĚJOVICÍCH

Pedagogická fakulta

Katedra informatiky

Síťové přístupové systémy se zaměřením na biometrické autentizační technologie

Network access systems with biometric authentication technology

Bakalářská práce

Vypracoval: Vlastimil Hanzal

Vedoucí práce: PaedDr. Petr Pexa, Ph.D.

České Budějovice 2015

JIHOČESKÁ UNIVERZITA V ČESKÝCH BUDĚJOVICÍCH
Fakulta pedagogická
Akademický rok: 2013/2014

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	Vlastimil HANZAL
Osobní číslo:	P12164
Studijní program:	B7507 Specializace v pedagogice
Studijní obory:	Informační technologie se zaměřením na vzdělávání
	Technická výchova se zaměřením na vzdělávání
Název tématu:	Síťové přístupové systémy se zaměřením na biometrické autentizační technologie
Zadávající katedra:	Katedra informatiky

Zásady pro vypracování:

Biometrie je odvětví vědy, pomocí které jsou lidé automaticky identifikováni nebo verifikováni díky poznatkům z medicíny, matematiky, fyziky a dalších oborů na základě svých psychických (podpis, hlas, chůze) nebo fyzických (obličej, prst, ucho, oční duhovka, sítnice, geometrie ruky) charakteristik. Biometrie se proto čím dál častěji využívá k autentizaci uživatelů a zajišťuje tak ochranu před falšováním identity. Cílem bakalářské práce bude v teoretické části podrobně popsat existující varianty biometrických autentizací a provést analýzu možných dostupných řešení biometrických autentizačních systémů v praxi, jejich porovnání a otestování. V praktické části student navrhne vlastní řešení systému pro autentizaci žáků resp. studentů v počítačové učebně, školní jídelně apod.

Rozsah grafických prací: CD ROM

Rozsah pracovní zprávy: 40

Forma zpracování bakalářské práce: tištěná

Seznam odborné literatury:

1. RAK, Roman. Biometrie a identita člověka ve forenzních a komerčních aplikacích. 1. vyd. Praha: Grada, 2008. ISBN 978-80-247-2365-5.
2. Z-WARE - identifikační systémy docházkové, stravovací, přístupové. [online]. [cit. 2014-03-30]. Dostupné z: http://www.z-ware.cz
3. JEŽEK, Vladimír. Systémy automatické identifikace: Aplikace a praktické zkušenosti. Grada Publishing, 1996. ISBN 8071692824.
4. DRAHANSKÝ, Martin a Filip ORSÁG. Biometrie. 1. vyd. [Brno: M. Drahanský], 2011. ISBN 978-80-254-8979-6.
5. TISTARELLI, M. Biometric authentication. Vyd. 1. Berlin: Springer-Verlag, 2002. ISBN 35-404-3723-1.
6. KISKU, Dakshina Ranjan, Phalguni GUPTA a Jamuna Kanta SING. Advances in biometrics for secure human authentication and recognition. Vyd. 1. Berlin: Springer-Verlag, 2002, 196 s. ISBN 978-146-6582-422.

Vedoucí bakalářské práce: **PaedDr. Petr Pexa, Ph.D.**
Katedra informatiky

Datum zadání bakalářské práce: **27. března 2014**
Termín odevzdání bakalářské práce: **30. dubna 2015**

Mgr. Michal Vančura, Ph.D.
děkan

L.S.

doc. PaedDr. Jiří Vaníček, Ph.D.
vedoucí katedry

V Českých Budějovicích dne 27. března 2014

Prohlášení

Prohlašuji, že svoji bakalářskou práci jsem vypracoval samostatně pouze s použitím pramenů a literatury uvedených v seznamu citované literatury. Prohlašuji, že v souladu s § 47b zákona č. 111/1998 Sb. v platném znění souhlasím se zveřejněním své bakalářské práce, a to v nezkrácené podobě elektronickou cestou ve veřejně přístupné části databáze STAG provozované Jihočeskou univerzitou v Českých Budějovicích na jejích internetových stránkách, a to se zachováním mého autorského práva k odevzdanému textu této kvalifikační práce. Souhlasím dále s tím, aby toutéž elektronickou cestou byly v souladu s uvedeným ustanovením zákona č. 111/1998 Sb. zveřejněny posudky školitele a oponentů práce i záznam o průběhu a výsledku obhajoby kvalifikační práce. Rovněž souhlasím s porovnáním textu mé kvalifikační práce s databází kvalifikačních prací Theses.cz provozovanou Národním registrem vysokoškolských kvalifikačních prací a systémem na odhalování plagiátů.

V Českých Budějovicích dne 24. června 2015

Vlastimil Hanzal

Abstrakt

Cílem bakalářské práce je zpracovat dostupné varianty biometrických metod, pomocí kterých jsou lidé automaticky identifikováni nebo verifikováni na základě svých anatomicko-fyziologických nebo behaviorálních charakteristik, u kterých je předpokladem, že jsou jedinečné, v průběhu času neměnné, prakticky měřitelné a technologicky zpracovatelné. Tyto metody jsou využívány již stovky let k identifikaci osob a pro různá řešení zabezpečení. Dnes jsou tyto biometrické metody zdokonalovány a propojovány s moderními informačními technologiemi. Výhoda biometrických metod se zakládá na identifikaci vlastní podstaty člověka. Vyznačují se tak vysokou mírou ochrany proti zneužití, oproti jednoduché funkci identifikačního čipu či jiného identifikačního média a k následnému falšování identity.

V teoretické části je popsáno odborné názvosloví a především jsou popsány existující varianty biometrických autentizačních metod. Dále je provedena analýza možných dostupných řešení biometrických systémů v závislosti na českém trhu. A na základě těchto informací je proveden výběr biometrické metody pro aplikaci v praktické části.

V praktické části je navrhnut vlastní projekt autentizace osob na základní škole pomocí jedné z používaných biometrických metod. A je provedeno testování této metody na dostupných zařízeních.

Klíčová slova

Biometrie, identifikace, verifikace, FAR, FRR

Abstract

The aim of this bachelor thesis is to process available variations of biometric methods which are used for an automatic identification or verification of people based on their anatomical-physiological or behavioural characteristics that are supposed to be unique, stable over time, practically measurable and technologically processable. These methods have already been used for hundreds of years for the identification of people and for various solutions of security. Today, these biometric methods are improved and connected with the modern information technology. The advantage of biometric methods is based on the identification of the basic essence of a man. Therefore, they are characterized by a high degree of protection against misuse and to following misuse of identity in comparison to a simple function of identification chip or another identification medium.

The theoretical part consists of a description of a professional terminology – primarily of a description of the biometrical authentication methods. Further on, there is an implementation of analysis of available solutions of biometrical systems in the environment of the Czech market. The choice of the biometrical system for the application in the practical part of this project has been made based on this information.

Own project of authentication people at primary school with a help of used biometrical methods is proposed in practical part. And this method will be tested on available devices.

Keywords

Biometrics, identification, verification, FAR, FRR

Poděkování

Rád bych tímto poděkoval vedoucímu mé bakalářské práce, panu PeadDr. Petru Pexovi, Ph.D. za odborné vedení práce, vstřícnost, trpělovost a cenné rady, které mi poskytl i za čas, který mi věnoval.

Dále bych rád poděkoval za spolupráci a odborné rady panu Ing. Tomáši Valerovi ze společnosti ABBAS, a.s., panu Romanu Straškovi ze společnosti IReSoft, s.r.o., panu Ing.Vladimíru Zavřelovi a panu Zdeňku Dráždilovi ze společnosti Z-WARE.

Děkuji rovněž všem osobám, které mi poskytly otisky prstů při testování biometrických snímačů.

Obsah

1 Úvod

K ověření identity osob v první řadě z důvodu bezpečí dochází již od samého počátků lidstva a každý z nás se s tímto problémem setkává ve svém každodenním životě již od svého narození. Dříve, dokud lidé žili v málo početných skupinách, postačilo k rozpoznání blízké či cizí osoby pouze zapamatování si především nejzřetelnějších charakteristik dané osoby, například její tváře nebo hlasu. Už v dávných dobách si člověk uvědomoval svojí jedinečnost, o čemž svědčí otisky dlaní u jeskynních maleb, které sloužily k určení autora malby, a mnohé další archeologické nálezy. S rozvojem doby již není možné, aby si člověk zapamatoval všechny osoby ve svém okolí. Tento problém se dnes lidstvo snaží vyřešit díky velmi rychlému rozvoji informačních technologií pomocí biometrických autentizačních systémů, které se zaměřují především na ochranu majetku a bezpečí osob. Jelikož je v dnešní době kladen velký důraz na ochranu osobních dat, ale také na ochranu osob samotných.

Biometrické systémy nejsou nijak jednoduché a zakládají se na dlouholetém zkoumání v mnoha vědních oborech. Jedním z nejdůležitějších vědních oborů při rozvoji biometrických systémů se stala věda forenzní, která slouží k vyšetřování trestních řízení před státními orgány. Dnes se však biometrické systémy používají již jako prevence před možným trestním činem, ale i pro mnohá jiná využití, například i v soukromém nebo firemním sektoru. Použití biometrických prvků má vyloučit možnosti klamání systému oproti použití jiných prostředků, např. identifikačních karet, které lze jednoduše odcizit. Biometrický vzor má zajistit spolehlivé určení osoby oprávněné pro přístup do chráněných prostor nebo k chráněným informacím.

Často dochází k obavám, či dokonce k odporu při použití identifikačních technologií podporovaných výpočetní technikou, který může být politického, náboženského, sociálního nebo dokonce právního charakteru. Není se čemu divit, když se tyto technologie dnes nachází skoro na každém kroku. Avšak tyto obavy vznikají většinou z nepochopení a hlavně z neznalosti základního principu jednotlivých identifikačních metod.

Touto prací bych chtěl biometrické systémy lidem přiblížit, aby pochopili, že slouží v první řadě pro jejich ochranu a také pro ochranu jejich majetku.

1.1 Cíle práce

Cílem této práce je v teoretické části vysvětlení obecné terminologie potřebné k pochopení biometrické autentizace a práci s biometrickými systémy. Především vymezení samotného pojmu biometrie a autentizace. Dále pak vytvoření podrobného popisu existujících variant biometrických autentizačních systémů a jejich rozdělení do jednotlivých tříd. Také provedení analýzy možných dostupných řešení biometrických systémů v závislosti na českém trhu a výběr metody aplikovatelné v praktickém návrhu autentizace osob na základní škole.

V praktické části je cílem práce vytvořit samotný návrh biometrické autentizace osob na základní škole. A biometrickou metodu použitou v návrhu otestovat na dostupných zařízeních.

1.2 Metoda práce

V teoretické části vysvětluji důležité termíny pro orientaci v dané problematice, například verifikace a identifikace, klasifikaci biometrických chyb, jako například FRR a FAR. Práce také obsahuje obrazovou dokumentaci některých používaných systémů biometrické identifikace. Popisuji existující varianty jak anatomicko-fyziologických, tak behaviorálních biometrických autentizačních systémů. Jejich význam jak z hlediska historického tak i aktuálního, dále také dělení, kritéria, využití, výhody a nevýhody těchto systémů. Podrobněji se zaměřuji na dostupné a používané technologie na českém trhu. V praktické části vytvářím návrh biometrické autentizace osob na základní škole a testuji dostupná zařízení.

Teoretická část

2 Základní pojmy

2.1 Myšlenka biometrické identifikace

Principem biometrických systémů je automatizované identifikování osob dle primárního principu identity člověka, kdy je každá osoba odlišná a tím pádem je totožná pouze sama se sebou. Je-li vědecky dokázáno, že určitá duševní či tělesná charakteristika člověka je jedinečná, pak lze tuto charakteristiku využít při jednoznačné identifikaci osoby. Pozitivní vlastností této charakteristiky tudíž bude vysoká úroveň jednoznačnosti a obtížná imitace či odcizení jinou osobou, jelikož je tato charakteristika přímo spojená s osobou, která se touto příznačnou vlastností vyznačuje. Primární myšlenka biometrické identifikace je založená na pocitu přirozenosti pro každého člověka, jelikož se s touto vlastností již narodí [1].

2.2 Definice pojmu biometrie

Biometrie (biometric) je specifický obor činnosti zkoumající a studující živé organismy. Jehož název vychází z řeckého slova „bios“ (život) a „metron“ (měření). V první řadě, a pro nás nejpodstatnější, je orientace na učení způsobů identifikace člověka dle jeho unikátních znaků, především jeho biologické (anatomické a fyziologické) vlastnosti a také jeho tzn. behaviorální charakteristiky neboli znaky chování. Případně, pokud bychom se chtěli držet doslovného znění v českém jazyce, znamenala by biometrie ”měření živého”. V přeneseném významu jde ovšem o měření a rozpoznávání určitých charakteristik člověka. V zahraničních zemích je koncept biometrie přímo interpretován jako proces automatizované metody rozpoznávání jedince opírající se o měřitelnosti biologických a behaviorálních vlastností (dle NSTC – Nation Science and Technology Council – Národní rada pro vědu a technologii USA, Výboru pro vnitrostátní a národní bezpečnost) [2].

2.3 Historie biometrické identifikace

Biometrie je využívána již od samého počátku lidstva. Mezi nejstarší dochované známky použití patří otisky dlaní v jeskyních, které se datují k období 28000 let př. n. l. [2].

Mezi první antropometrickou identifikační metodu, ze které se dochovaly památky, patřila metoda k identifikování a zaznamenávání zemědělců z údolí Nilu. Základní princip byl založen na rozpoznávání osob pomocí barvy pleti a barvy očí, dále také podle jizev a různých poranění, které během svého života utrpěli a dalších charakteristik, které usnadňovaly identifikaci zemědělce. Také sloužila k vyplácení peněz za prodej obilí do státní sýpky. Detailnější charakteristiky dělníků byly použity při vyplácení mzdy za odvedenou práci na stavbě pyramidy. Podrobně se zaznamenávaly míry, jako například délka lokte nebo vzdálenost rozpětí mezi ukazovákem a palcem ruky. Tuto metodu dále rozšířil Louis Alphonse Bertillon, který jako první na světě zajistil, aby tato metoda mohla být celosvětově použita při identifikaci zločinců a velice posunul kriminalistiku o krok vpřed. Sám nazval tuto metodu antropometrií, později však byla podle autora pojmenována Bertillonáž [3].

Stejně jako u otisků dlaní v jeskyních, tak i u prvních dochovaných záznamů o otiscích prstů se můžeme jen domnívat, zda si lidé již opravdu uvědomovali, že je každý otisk jedinečný a dokázali je rozeznat. K prvním náznakům využití metody otisku prstu patří například hliněné tabulky s otisky prstů z dob 3000 př. n. l., kterými Babyloňané stvrzovali obchodní transakce. Až v roce 1686 boloňský profesor anatomie Marcell Malpighim prvním vědecky pozoroval otisky prstů za pomoci mikroskopu. Později v roce 1788 J. C. A. Mayr zjistil, že neexistují dva jedinci se stejnými otisky. V roce 1823 vzniká první klasifikační systém otisků skládající se z devíti základních vzorů. O tento systém se postaral český profesor anatomie na Vratislavské univerzitě Jan Evangelista Purkyně. Stále to ovšem nestačilo pro jednoznačné prokázání totožnosti osoby. Až v roce 1892 sir Francis Galton obhájil svou práci i svých předchůdců, že se otisky prstů v průběhu života nemění a že neexistují dva stejné otisky. Stanovil však i pravděpodobnost výskytu stejných otisků na 1 : 64 000 000 000 a vytvořil tabulku znaků, která se s menšími změnami

používá až do dnes k identifikaci osob. Teprve v 60. let 20. století s rozvojem výpočetní techniky došlo k automatizování systému identifikace, dle otisků prstů. Jednalo se o systém AFIS (Automated Fingerprint Identification Systems) [4].

Mezi historicky nejznámější využití hlasové verifikace, kterou lze najít i ve Starém zákoně, patří vyvraždění 42000 osob. Konkrétně šlo o Izraelity, kteří prchali z Egypta. Osoby, které neprošly před vojáky testem výslovnosti slova bible, byly zavražděny [1].

2.4 Terminologie

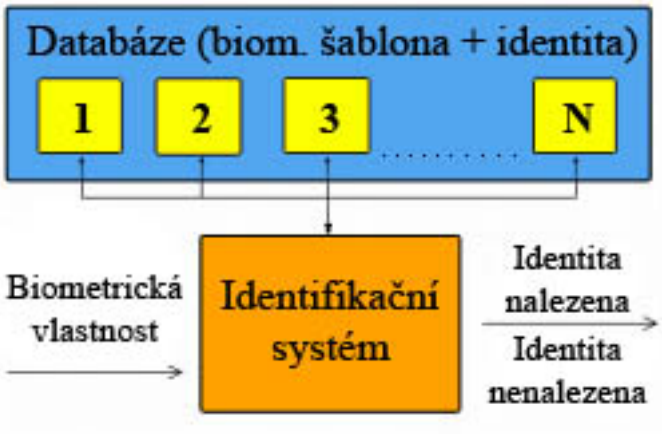
Pro kvalitní práci s biometrickými systémy je potřeba si správně vštípit základní termíny, které jsou důležité při volbě požadavků na konkrétní aplikaci.

Recognition (rozpoznávání) - je odborný výraz, pojednávající o schopnosti rozpoznávat objekty dle určitých znaků. V biometrii se jedná o vlastnost rozpoznávat osoby za pomoci dostupných metod dle jejich anatomicko-fyziologických či behaviorálních charakteristik, jedinečných a v průběhu času téměř neměnných. Avšak nemusí jít přímo o identifikaci či verifikaci [5].

Authentication (testování) - je termín, který se svým významem podobá termínu rozpoznávání s tím rozdílem, že na konci tohoto procesu rozpoznávaná osoba dostane nebo nedostane oprávnění k přístupu do systému [6].

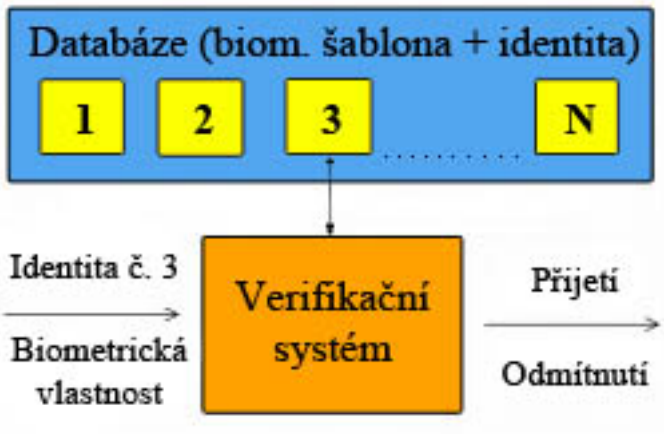
Identification (rozeznávání) - je metoda, kdy biometrický systém srovnává sejmutý biometrický údaj osoby s celou databází uložených šablon. Základní princip vychází z předpokladu, že osoba se zatím nijak neidentifikovala například pomocí karty či hesla. Tato metoda je často označována jako 1:N či „one-to-many“. Česky tuto metodu můžeme nazvat otázkou „Kdo to je?“ a odpovědí bude nalezení či nenalezení identity uživatele v databázi [7, 8].

Identifikaci lze také rozdělit na pozitivní, kdy se osoba snaží prokázat, že již je uložena v databázi a negativní, kdy se snaží prokázat, že není uložena v databázi [11].



Obrázek 1: Schéma identifikace

Verification (ověřování) - je metoda porovnání, v reálných zařízeních uživatel poskytne svojí totožnost systému přiložením identifikační karty či hesla a poté potvrdí svojí totožnost přiložením biometrického vzorku. Tuto metodu může taktéž označit poměrem, 1:1 nebo „one-to-one“ [7, 8].



Obrázek 2: Schéma verifikace

Autorizace (oprávnění) - je proces následující po kladné autentizaci, kdy jsou osobě vpuštěné do systému přiděleny určité kompetence k činnostem, které může v systému vykonávat [6].

Matching (srovnání) – jde o porovnání již uložené šablony s přijatým biometrickým otiskem do systému. Identifikující se osoba s velkou pravděpodobností nikdy nepřiloží například svůj prst vždy pod stejným úhlem jako při vytvoření šablony. Proto je identicky shodný vzorek s již uloženou šablonou brán jako ohrožení systému [9].

Score (Skóre) - je počet procent shody dvou porovnávaných biometrických vzorů [7].

Treshold (práh citlivosti) - Bezpečnostní prahová úroveň je hodnota nastavená administrátorem, kterou když vzorek překročí, je vpuštěn do systému, pokud ne, je odmítnut [10].

Biometric sample (biometrický vzorek) - je sejmutou charakteristikou jako například otiskem prstu, zvukovým záznamem či podpisem [1].

Biometric characteristics (biometrická charakteristika) - měřitelný údaj z biometrického vzorku [1].

Biometric identificator (biometrický markat) - segment biometrické charakteristiky, který lze použít k autentizaci [1].

Biometric template (biometrická šablona) - získané hodnoty z biometrického vzorku postačující k jednoznačné autentizaci [1].

2.5 Společné rysy biometrických systémů

Na první pohled se zdá, že se biometrické metody vzájemně liší, avšak základní princip zůstává stále stejný. Hlavní rozdíl spočívá v metodě sejmutí biometrického vzorku.

2.5.1 Princip autentizace

Každé zpracování biometrického vzorku se skládá z pěti kroků [1, 8]:

- Snímání dat - v této části dochází k zachycení biometrických charakteristik člověka, které jsou převedeny do podoby vzorku a odeslány dále do systému.
- Přenos dat - určité systémy zpracovávají sejmuté vzorky na jiném místě, než byly sejmuty. Je žádoucí, aby byl přenos dat bezpečný a ob-

jem odesílaných dat co nejmenší, o což se starají šifrovací a kompresní algoritmy.

- Zpracování signálu - zde dohází k vytažení markantů a odstranění nežádoucích vlivů z dekomprimovaného biometrického vzorku pomocí matematických algoritmů, ze kterých je vytvořena šablona. Z důvodu bezpečnosti je tento proces pouze jednostranný, tudíž nelze z markantů vytvořit zpětně biometrický vzorek, aby nedošlo k odcizení. Pokud nejsou data dostačující, dochází k požadavku na opětovné sejmutí vzorku. Do tohoto kroku můžeme řadit i proces porovnání, je však někdy řazen jako mezikrok či jako samostatný krok, ve kterém dochází k porovnání a určení skóre vytvořené šablony se šablonou uloženou v databázi při registraci.

- Rozhodování - jde o určení konečného rozhodnutí na základě shody šablony uložené v databázi a nově sejmuté šablony.

- Uložení dat - šablony a u některých zařízení také nezpracované sejmuté vzory jsou uloženy v databázi, ze které jsou později použity při autentizaci.

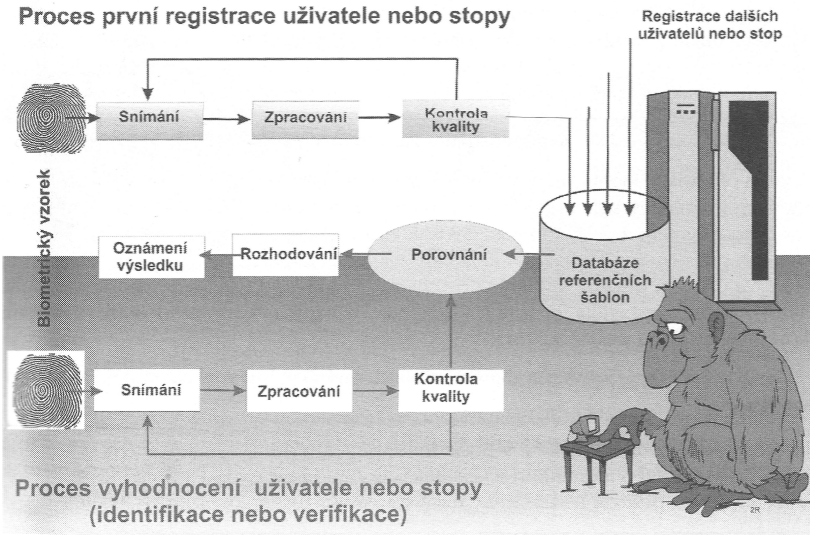
2.5.2 Provozní stavy systémů

Registrační modul

Během této fáze osoby několika opakovanými pokusy poskytnou své biometrické údaje systému. Dostatek dat je poté výsledkem vytvoření referenční šablony (etalonu), která je uložena do paměti [11].

Verifikační/identifikační modul

Osoba jedním pokusem předloží své biometrické údaje, ze kterých je opětovně vytvořena šablona, která je porovnána s původní šablonou. Zde nastává problém, jelikož vždy nelze zajistit úplně totožné předložení biometrického údaje. Proto se v systému nastavuje prahová hodnota [11].



Obrázek 3: Schéma registrace a identifikace nebo verifikace[1]

2.6 Kritéria kladená na biometrické aplikace

Na biometrické systémy je kladeno mnoho kriterií, která musí splňovat pro jednoduché, spolehlivé, rychlé a především bezpečné fungování v praxi. Mezi obecná kritéria řadíme [1]:

Operační - to jsou kritéria zaměřená především na zásadní funkčnost každé metody.

- **Jedinečnost -** každý snímaný prvek konkrétní metodou musí být ve světě dostatečně unikátní. Proto musíme volit takové charakteristiky, aby byla nejmenší pravděpodobnost, při možné identitě dvou osob, že by se tyto dvě osoby setkaly u jednoho snímacího zařízení.
- **Neměnnost -** podstatným faktorem je, aby se technologicky zpracovávaný prvek neboli markant postupem času nezměnil.
- **Měřitelnost** - veškeré charakteristiky, pomocí kterých chceme osoby autentizovat, musí být měřitelné, formulovatelné a také musí být před praktickým využitím známá výkonnost.

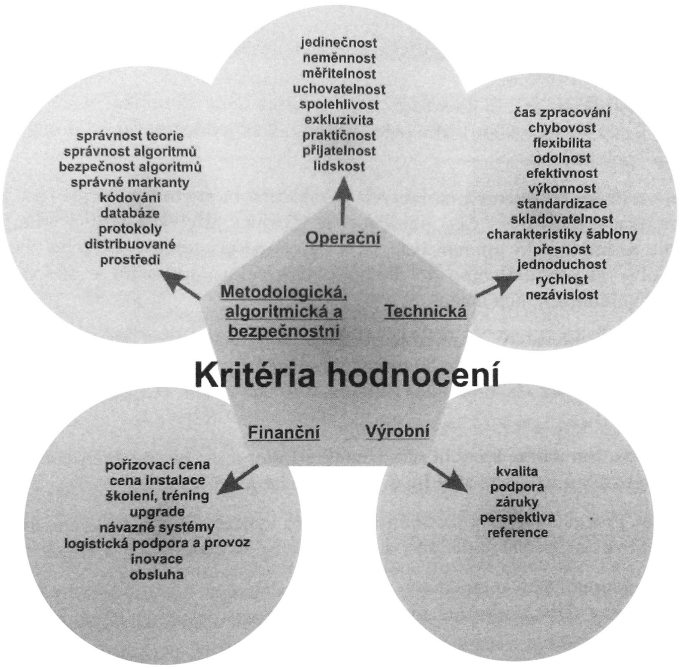
- **Uchovatelnost -** již získané charakteristiky musí být archivovány v takové cenové relaci, aby zůstaly ve stejné kvalitě jako při pořízení.
- **Spolehlivost -** možnost opětovného provedení celého procesu autentizace se stejným výsledkem.
- **Exkluzivita -** použitá metoda musí splňovat veškeré podmínky k samostatné konečné autentizaci bez podpory jiné metody.
- **Praktičnost -** jedná se především o nejjednodušší, nejrychlejší a pro uživatele nejpřívětivější.
- **Přijatelnost -** každý krok systému musí být z hlediska sociálního, náboženského, politického atd. vhodný pro všechny osoby, které mohou přijít do styku s tímto zařízením.
- **Lidskost -** osoba, která prochází procesem autentizace, se musí cítit zcela přirozeně, proto musíme zvažovat, i do jakého prostředí budeme konkrétní zařízení umist'ovat, ne každé zařízení se hodí ve všech situacích.

Technická - jsou jedny z nejčastějších kriterií kladených na biometrické autentizační technologie, které nejsou o nic méně významné než operační.

Výrobní - jsou kriteria kladená na kvalitu referencí jak výrobce, tak i dodavatele.

Matematická, algoritmická a bezpečnostní - jsou především kritéria kladená na vývojáře těchto technologií.

Finanční - cena vždy hrála a vždy bude hrát velkou roli při pořízení případného zařízení. Zákazník by si však měl uvědomit i případné náklady při obsluze zařízení.



Obrázek 4: Kritéria hodnocení biometrických technologií[1]

Mezi základní a nejdůležitější charakteristiky biometrických vlastností, podle kterých vybíráme konkrétní biometrický systém a na které se zaměřuji v tabulce 2 na straně 51 patří [12]:

- Univerzálnost - každá osoba vlastní tuto biometrickou charakteristiku.
- Jedinečnost - žádné dvě osoby nemají shodnou biometrickou charakteristiku.
- Stálost - biometrická charakteristika zůstává v průběhu času neměnná.
- Získatelnost - biometrickou charakteristiku lze změřit.
- Výkonnost - tato vlastnost zahrnuje především problematiku řešenou v kapitole 2.7 na následující straně.
- Přijatelnost - ochota lidí poskytnout svou biometrickou charakteristiku.
- Odolnost proti napadení - odolnost proti použití falsifikátu.

Mezi tyto charakteristiky také patří [13]:

- Cena - náklady na pořízení systému.

2.7 Měření výkonnosti biometrických systémů

Pokud chceme prakticky realizovat konkrétní zařízení pracující na určité biometrické autentizační metodě, nestačí, aby splňovalo jen výše zmíněná kritéria. Musí být prvně testováno, jelikož nelze docílit toho, aby byl každý otisk do detailu stejný, jako je to například u hesla. Proto je nutné si uvědomit, že každý biometrický systém pracuje se statistickým posudkem dvou prvků, a to prvotně vytvořené šablony a nového nasnímaného vzoru. Výsledkem je poté skóre, které je v procentech nebo i graficky uvedeno u každého zařízení.

Nejdůležitější metody rozhodování při určování výkonnosti biometrických systémů je možné rozdělit dle těchto kategorií [2, 8, 14]:

2.7.1 Chyby v rozhodování

Chybné odmítnutí (False Rejection Rate- FRR)

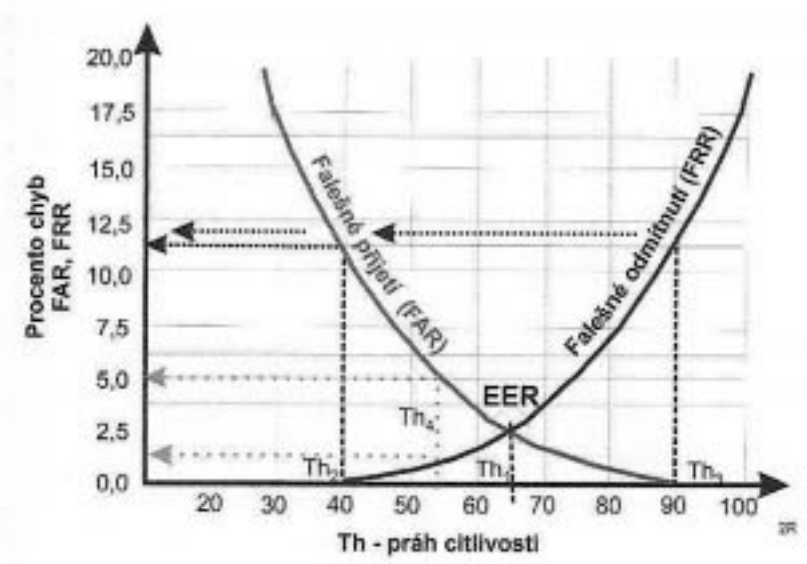
Jedná se o chybu prvního typu. Uvádí průměrný počet chybně odmítnutých osob, které by měly mít přístup. Jedná se tedy o chybu uživatelsky nepřívětivou, avšak ne příliš závažnou.

$$FRR = \frac{Počet\ nesprávných\ odmítnutí}{Počet\ všech\ autentizačních\ pokusů} * 100\ [\%]$$

Chybné přijetí (False Acceptance Rate – FAR)

Jedná se o chybu druhého typu, kdy jsou do systému chybně přijaty osoby, které by přístup mít neměly. Příklady chybného přijetí jsou uvedeny v následující sekci výhody a nevýhody biometrických systémů.

$$FAR = \frac{Počet\ nesprávných\ přijetí}{Počet\ všech\ autentizačních\ pokusů} * 100\ [\%]$$



Obrázek 5: Reálná biometrická aplikace[1]

2.7.2 Oprávnění

Přijetí oprávněné osoby (True Positive Rate - TPR)

Vyjadřuje pravděpodobnost oprávněného přístupu osoby s jíž uloženým biometrický metanolem v databázi. Pokus osoby o identifikaci je vyhodnocen algoritmem jako oprávněný s povolením k přístupu. Je možné se setkat s termínem senzitivita nebo citlivost.

Odmítnutí neoprávněné osoby (True Negative Rate - TNR)

Vyjadřuje pravděpodobnost neoprávněného přístupu osoby s neuloženým biometrickým etanolem v databázi. Identifikace osoby je vyhodnocena algoritmem jako pokus s negativním povolením k přístupu. Je také možné se setkat s termínem specificita.

2.7.3 Chyby před porovnáním

Neschopnost snímání (Failure To Enroll Rate - FTE nebo FER)

Míra neschopnosti se zaregistrovat udává procentuální podíl osob, které není možné do systému zaregistrovat. Tyto chyby vznikají při předkládání biometrické charakteristiky snímači. Mohou být způsobeny zraněním nebo vrozeným deficitem snímané charakteristiky.

$$FTE = \frac{Počet\ neúspěšných\ registrací}{Počet\ všech\ pokusů\ o\ registraci} * 100\ [\%]$$

Nedostatečná kvalita (Failure To Acquire Rate - FTA)

Míra neschopnosti systému uznat vzorek nedostatečné kvality například z důvodu malého počtu markantů.

$$FTA = \frac{Počet\ neúspěšných\ snímání}{Počet\ všech\ snímání\ biometrických\ dat} * 100\ [\%]$$

2.7.4 Chyby v porovnávání

Nesprávné přiřazení snímaného vzorku k referenčnímu neboli **False Identification Rate (FIR)** můžeme rozdělit na:

Nesprávné ztotožnění (False Match - FM)

Je míra pravděpodobnosti, že daný vzorek bude nesprávně zvolen za shodný s některým referenčním vzorkem jiné osoby. Ve forenzních aplikacích se můžeme setkat s termínem **(False Match Rate - FMR)**

$$FMR = \frac{Počet\ nesprávně\ označených\ shodných\ vzorků}{Počet\ všech\ srovnání} * 100\ [\%]$$

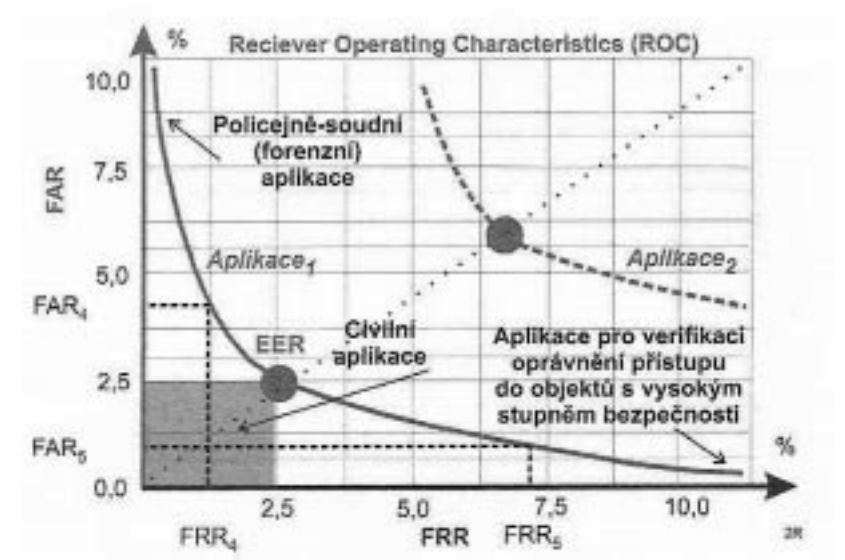
Nesprávné neztotožnění (False Non-Match - FNM)

Je míra pravděpodobnosti, že snímaný vzorek jedné osoby bude nesprávně zvolen za odlišný od svého referenčního vzorku. Ve forenzních aplikacích se můžeme setkat s termínem **(False Non-Match Rate -FNMR)**

$$FNMR = \frac{Počet\ nesprávně\ označených\ rozdílných\ vzorků}{Počet\ všech\ srovnání} * 100\ [\%]$$

2.7.5 Prostředky k určení chyb

Fungování biometrických aplikací v praxi není nikdy ideální ve smyslu stoprocentního odmítnutí či přijetí osob. K objektivnímu určení kvality a vzájemnému porovnání jednotlivých aplikací slouží křivka provozní charakteristiky přijetí **(Receiver operating characteristics - ROC**) nebo přesnější křivka k detekci chyb porovnáním **(Detection Error Trade-off - DET)**. Každá aplikace má nastavený určitý práh citlivosti (tzv. threshold). Při změně nastavení tohoto prahu se obě hodnoty mění, vždy se jedna hodnota zvyšuje a druhá snižuje.



Obrázek 6: Závislost FAR a FRR[1]

Bod určující protnutí křivek se nazývá míra rovnosti chyb **(Equal Error Rate - EER)**

2.8 Obecné výhody a nevýhody biometrických systémů

Každá autentizační metoda má své světlé i stinné stránky. Stejně je tomu tak u biometrických metod autentizace.

Výhody

Nejpodstatnější výhodou biometrické autentizace je přímá závislost na fyziologických či behaviorálních vlastnostech člověka, které jsou relativně neměnné v čase. Veškeré metody se zakládají na principu, kdy si uživatel nemusí nic pamatovat ani nosit nic u sebe, tudíž o biometrickou vlastnost nemůže přijít ani ji někomu předat. Díky tomu jsou snižovány náklady na provoz a zvyšována rychlost a bezpečnost autentizace.

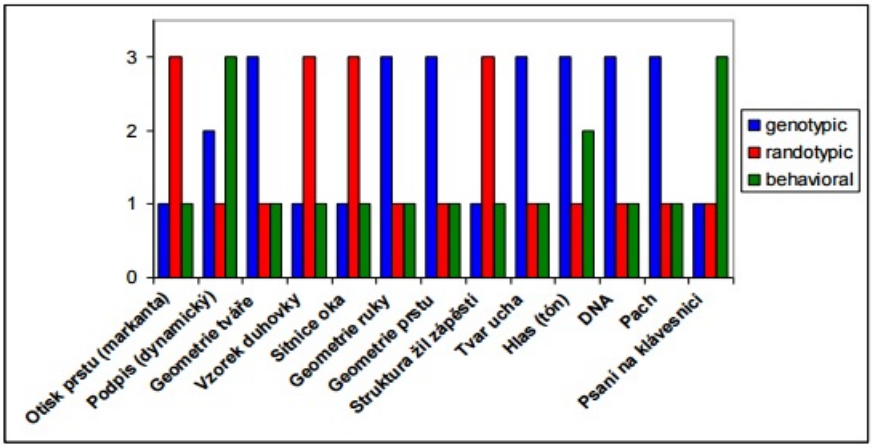
Nevýhody

Biometrické systémy jsou v celku novou metodou autentizace a jsou stále ve vývoji. Zásadním problémem všech biometrických systémů, kdy osoba nemůže být autentizována, je chybějící vlastnost osoby potřebná k autentizaci z důvodu vrozené vady či nehody. Ovšem i hendikep v jiné části těla může znesnadňovat autentizaci, kdy jsou snímací zařízení instalována mimo dosah osob na invalidním vozíku. U některých osob se také můžeme setkat s odporem při snímaní a ukládání osobních biometrických dat například z náboženských důvodů. Proto se musí při navrhování sytému brát zřetel na to v jakých podmínkách a jaké osoby budou autentizovány, každý systém musí být navrhován individuálně. Ne každá metoda se dá použít v daném prostředí i z hygienických a časových důvodů. Také nelze komerčně využít veškerých metod kvůli možnosti ztráty a zneužití osobních informací, například informace z DNA, které mohou využít pojišťovny ke svým účelům.

2.9 Rozdělení biometrických metod

Veškeré biometrické metody spočívají na základě třech vlastností [2]:

- Genotypické - vznikají při početí na základě DNA.
- Randotypické - vznikají v prenatálním období.
- Behaviorální - jsou určeny chováním.



Obrázek 7: Vliv vývojových vlastností[2]

Všechny tři typy v určité míře ovlivňují každou metodu.

Základním rozdělením biometrických autentizačních metod podle měřených charakteristik [1]:

- **Anatomicko-fyziologické** - taktéž nazývané statické. Jedná se o vlastnosti lidského těla, ze kterých lze získat biometrický vzorek za pomoci přímého snímání a měření této vlastnosti. Mají velkou míru jedinečnosti a v průběhu času neměnnosti, tudíž se více hodí k autentizaci osob.

- **Behaviorální** - taktéž nazývané dynamické. Jedná se o vlastnosti založené na chování člověka. Především je požadována od člověka určitá interakce. Za určitých předpokladů se dají tyto vlastnosti v průběhu času měnit, jsou však stále jedinečné.

Není nutnost, aby biometrické systémy fungovaly pouze jen na jedné ojedinělé metodě snímání. Sloučením více biometrických metod můžeme především dosáhnout lepšího zabezpečení, je však také možné sloučit systém s metodou autentizace heslem či předmětem (tzv. tokenem) a tím dosáhnout i rychlejšího ověření tedy verifikací.

Dalším dělením biometrických metod může být například dělení na policejně-soudní, bezpečnostně-komerční a ezoterické[1][1].

[1]Určený úzkému okruhu specialistů [1]

3 Biometrické metody

3.1 Anatomicko-fyziologické metody v oblasti hlavy

Biometrické metody založené na rozpoznávání charakteristik v oblasti hlavy můžeme řadit mezi nejvíce žádané, jelikož hlava je důležitá část těla, velmi viditelná a s poměrně velkým množstvím znaků. Není tudíž divu, že se tímto směrem ubírá mnoho biometrických výzkumů.

3.1.1 Geometrie tváře

Metoda rozpoznávání tváře je sama o sobě velmi rozsáhlou kapitolou, proto se jí pokusím shrnout a zaměřím se především na rozpoznávání tváře pomocí počítačových systémů.

Rozpoznávání osob podle tváře je jednou z nejstarších a člověku nejpřirozenějších metod. Tato metoda je nejvíce používána v oblastech s velkým počtem osob, což ve své podstatě skýtá mnoho překážek.

Základní princip funkce rozpoznávání tváře můžeme rozdělit na dvě části [1, 8, 15]:

Detekce a lokalizace

Jde o nalezení a rozeznání tváře v nasnímané scéně od ostatních objektů a vypočítání pozice. Především je potřeba vytvořit počítačový model tváře. Ten lze vytvořit pomocí různých modelů, které se mohou i prolínat. Mezi základní modely patří:

- 2D - dvourozměrný model.
- 3D - prostorový model.
- Infračervený (termosnímek) - snímání teplot v oblasti obličeje.

Podle matematického modelování lze detekci a lokalizaci rozdělit na:

- Staticky orientované metody
  - Metoda podprostoru (eigenface) - nalezení typických charakteristik pro lidskou tvář (nos, ústa, atd.).
  - Metoda neuronových sítí - je metoda založená na dvou třídách, a to třída s obrazy tváří a třída s obrazy ostatních objektů uložených v knihovnách.
- Znalostní metody
  - Metody založené na rozložení odstínů šedi v obraze - je metoda založená na základě odstínů šedi ve tváři.
  - Metody založené na rozpoznávání obličejových obrysů - jde o nalezení hran dané tváře.
  - Metody založené na informaci o barvách - je metoda odlišující tvář od okolního prostředí pomocí barev.
  - Metody založené na informaci o pohybu na scéně - pohyb osoby vůči pozadí.
  - Metody založené na symetrii - nalezení symetrického objektu, který má rysy tváře.

Rozpoznání

Jde o nalezení potřebných markantů v již detekované tváři pro porovnání se šablonou uloženou v databázi. Metody rozpoznávání lze rozdělit na:

- Metody založené na rozložení odstínů šedi v obraze - metoda je v principu stejná jako u detekce, jen s rozdílem, že již porovnáváme odstíny s obrazy v databázi.
- Metody založené na geometrických tvarech a identifikačních markantech - metoda založená především na vzdálenostech a úhlech jednotlivých markantů.

- Metoda optických toků - analýza více snímků vůči pohybu určitých bodů.
- Metoda deformačních modelů - využití síťového 3D prostorového modelu.
- Metody neuronových sítí - metoda založená na principu lidského mozku, která se sama učí.
- Metoda „Eigenhead“ - modelování 3D snímku celé hlavy.

Nejznámější algoritmy používané při rozpoznávání tváří:

PCA (Principal Component Analysis) - transformace obličeje o menší datové velikosti při nejmenší ztrátě informací.

LDA (Linear Discriminant Analysis) - stejné jako PCA ovšem zobrazovaná osoba je známá.

ASM (Active Shape Model) a AAM (Active Appearance Model) - jsou metody, které obrázek zobrazují jako obličej, až poté hledají podobnost.

3.1.2 Oční duhovka

Metody snímající oko patří mezi nejpřesnější metody, ale zároveň i k těm nejdražším. Jejich využití se hodí pro místa s vysokou bezpečnostní úrovní, jako jsou například jaderná zařízení. Duhovkou můžeme označit barevnou část oka. Struktura duhovky je jedinečná a časově neměnná. Kupodivu i jedna a ta samá osoba má v každém oku jinou strukturu duhovky [2, 8].

Ke snímání duhovky je využívána digitální kamera a infračervené osvětlení. Ze získaného snímku software vytvoří mapu za pomocí četnosti, orientace a pozice specifických charakteristik typických pro duhovku jako jsou například [11]:

- Krypty - tmavá a velice tenká místa duhovky.
- Radiální rýhy - paprsky vybíhající od zornice k okraji duhovky.

- Pigmentové skvrny - náhodné shromáždění pigmentů.
- Pigmentové záhyby - spodní vrstva duhovky v oblasti zornice.

Obrázek 8: Oční duhovka [2]

3.1.3 Oční sítnice

Sítnice je povrch oka citlivý na světlo skládající se z mnoha nervových buněk. K rozpoznávání osob je použit obraz struktury cév na zadní straně lidského oka a v okolí slepé skvrny pomocí infračerveného paprsku LED[2] diodou o nízké intenzitě [11].

Výhody a nevýhody

Výhodou je vysoká přesnost a v průběhu času relativní neměnnost. Může se změnit pouze vlivem úrazu či nemoci. Nevýhoda pak spočívá ve velké uživatelské nepřívětivosti, kdy je potřeba oko přiblížit na poměrně malou vzdálenost snímači bez brýlí nebo čoček [17].

3.1.4 Povrchová topografie rohovky

Je metodou využívající infračervené světlo malého výkonu vyzařované taktéž LED diodou, které je zaměřeno do středu zornice. Podle intenzity odraženého světla od rohovky oko reaguje. Oko každého jedince reaguje odlišně v závislosti na čase a rozšíření čočky. Proto lze také pomocí této metody rozpoznávat osoby [2].

[2] z anglického Light Emitting Diode – dioda emitující světlo [16]

Výhody a nevýhody

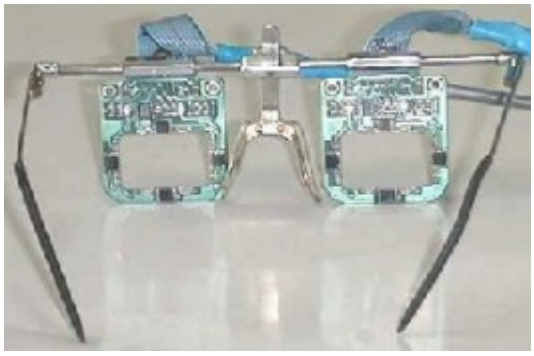
Tato metoda není běžně používanou autentizační metodou, a proto nelze porovnat její výhody a nevýhody oproti ostatním běžně používaným komerčním metodám.

3.1.5 Pohyb očí

Jedním z neobvyklých způsobů rozpoznávání je metoda zaměřující se na pohyb očí. Tato metoda za pomoci infračerveného světla snímá pohyby očí. K tomuto účelu byly vyvinuty na Slezské universitě v Gliwicích v Polsku speciální brýle [2].

Výhody a nevýhody

Tato metoda ovšem zatím nebyla ještě uplatněna při komerčním využití, tudíž není důležité pro tuto práci porovnat výhody a nevýhody oproti ostatním metodám.



Obrázek 9: Brýle pro sledování pohybu očí [2]

3.1.6 Tvar a pohyb rtů

Tuto metodu v praxi můžeme zařadit spíše mezi pomocné metody při rozpoznávání obličeje či ověřování pomocí hlasu, než jako samostatnou komerčně využívanou metodu.

Zakládá se na nasvícení a snímání opakovaného pohybu rtů při vyřčení předem stanovené fráze či během rozhovoru. Nejznámější metody se zakládají na osvětlení pomocí [8]:

FIR(Far-InfraRed) - vysoká bezpečnost, zároveň i náklady.

NIR(Near-InfraRed) - nižší bezpečnost, ovšem levnější technologie.

Výhody a nevýhody

Výhodou je možnost propojení s metodou rozpoznávání obličeje, a tím dosažení vyšší bezpečnosti. Nevýhoda spočívá v potřebě kvalitního nasvícení, čímž se zvyšuje pořizovací cena [8].

3.1.7 Tvar ucha

Rozpoznávání osob pomocí tvaru ušního boltce je známé již tisíce let. Převážně je používána při forenzních vyšetřování [1].

Obecně rozdělení této metody můžeme řadit do třech skupin [1]:

- Morfologické vztahy – 2D nebo 3D geometrii ušního boltce
- Termogram – mapování teplot na ušním boltci
- Otisku struktur - využití ve forenzní oblasti

Výhody a nevýhody

Výhodou je bezkontaktní snímání tvaru ucha ovšem je zapotřebí přesné lokalizace počátečního bodu, jinak dochází k odchylkám. Zásadní nevýhodou této metody je fakt, že ucho může být zakryto jak vlasy, tak například čepicí [8].

3.1.8 Odraz zvuku v ušním kanálku

Je jednou z méně užívaných novějších metod. Princip této metody spočívá ve vyslání zvukového signálu pomocí reproduktoru do zvukovodu. Intenzita odraženého a pohlceného zvuku je pro každou osobu individuální, tudíž se tato metoda dá také použít při rozpoznávání [2].

Výhody a nevýhody

Tento systém prozatím nemá komerční využití, do budoucna se počítá s implementací do mobilních zařízení k ochraně proti odcizení [11].

3.1.9 Odontologie

Tato metoda je využívána pouze ve forenzní sféře a soustředí se na rozpoznávání člověka pomocí informací o chrupu [18].

Výhody a nevýhody

Při forenzním vyšetřování je výhodou, že chrup povětšinou oběti zůstane a je často jednoduché najít alespoň nějaké zubařské záznamy. Pro využití autentizace osob do budov je tato metoda nevhodná.

3.2 Anatomicko-fyziologické metody končetin

Biometrické metody založené na rozpoznávání charakteristik v oblasti končetin patří mezi nejvíce používané metody v komerční sféře z důvodu nízké ceny a dlouholetých zkušeností.

3.2.1 Geometrie ruky

Metodu založenou na snímání tvaru prstů a dlaně ruky řadíme mezi nejstarší používané biometrické technologie. Základní princip spočívá ve snímání a měření fyzikálních charakteristik ruky především délek, šířek, tlouštěk, ale také se využívá celkového obrysu ruky. Určitá zařízení pracují pouze se snímkem dvou prstů. Starší zařízení snímala pouze siluetu ruky shora či zespoda pomocí přímé optické cesty, což nezajišťovalo dostatek měřitelných charakteristik. V novějších zařízeních se používají zrcadla pro úpravu optické cesty, čímž se snižuje velikost zařízení a zvyšuje možnost snímání o další rozměr. Kvalitnější zařízení poskytují i podsvícení nebo infračervené nasvícení ruky. Na podložce, která slouží k umístění ruky, se nacházejí kolíky, které zajišťují stejnou polohu ruky při opětovném přiložení. U této metody není snímán otisk ruky nebo prstů, tím se zabývá jiná metoda. CCD[3] kamera snímá siluetu ruky s přibližným rozlišením 32000 pixelů a systém zajistí až 90 měření za 1 sekundu. Sejmutý vzor poté dokáže uložit do pouze 9 bytové šablony, což snižuje požadavky na paměť [1, 8].

[3] z anglického Charge Coupled Device - zařízení s vázanými náboji citlivé na světlo [19]

Osoby lze také rozeznávat podle tvaru sevřených prstů do dlaně. Měřeny jsou určité vzdálenosti bodů na vnější straně pěsti [2].

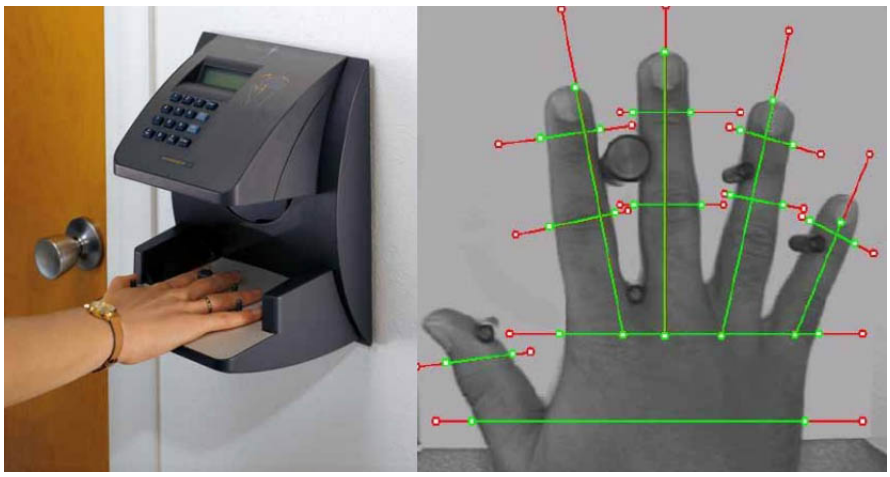
Rozpoznávání osob pomocí geometrie ruky lze rozdělit dle metod do těchto skupin [8]:

- Přímé měření - měření předem daných významných rozměrů jako je délka a šířka prstů na konkrétních místech.
- Zarovnání ruky - měření rozdílu natočené ruky do nadefinované polohy oproti vzoru.
- Analýza šířky prstů - měření vzdálenosti okrajů prstu od středové osy ruky.
- 3D geometrie - měření využívající třídimenzionální zobrazení ruky.

Výhody a nevýhody

Na tuto metodu nemá vliv zašpinění rukou. To se stává výhodou ve firmách, kde pracuje mnoho dělníků manuálně [20].

Nevýhodou je velká plocha dotyku, která není příliš uživatelsky přívětivá především z hygienické stránky. Tato metoda je také náchylná na změny způsobené například zraněním .

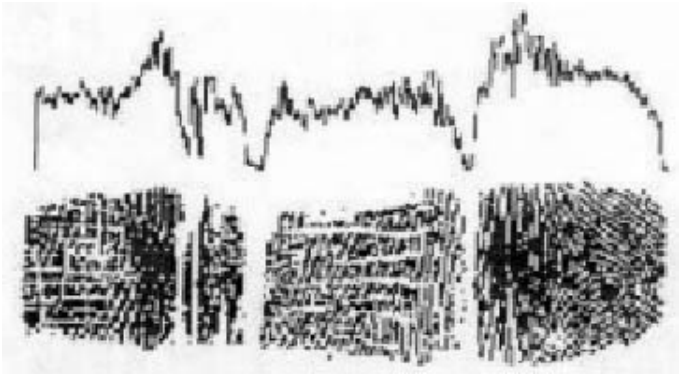


Obrázek 10: Snímání geometrie ruky [21]

3.2.2 Otisk prstu, dlaní a chodidel

Tyto metody jsou jedny z nejdéle a nejvíce používaných metod. Za svůj vznik vděčí především forenznímu vyšetřování. Méně známé metody, jako je otisk dlaně ruky či chodidla nohy a konkrétně také plantogram nohy, na jehož základě se nezkoumají pouze papilární linie, ale i rozměry, se komerčně příliš nevyužívají, především pak otisk nohy z důvodu uživatelské nepřívětivosti.

Velmi podobnou metodou je metoda měření vrásnění prstu a vzdálenosti kloubů využívající elektrostatickou kapacitní reaktanci [2].



Obrázek 11: Vrásnění článků prstu [2]

Nejznámější a nejpoužívanější je metoda otisku prstu. Jelikož se na této metodě zakládá velká část mé bakalářské práce, pokusím se jí vysvětlit podrobněji.

Každá osoba na světě, s výjimkou hendikepovaných osob jako například osob bez končetin či s poruchami kůže v této oblasti, má na povrchu dlaní, chodidel a všech prstů takzvané papilární linie neboli vyvýšené reliéfy. Tyto papilární linie graficky zobrazujeme jako otisk prstu, dlaně či chodidla.

Ovšem až 2 % populace nemá dostatečně zřetelné papilární linie v oblasti prstů pro biometrické systémy [17].

Vědním oborem zabývajícím se touto problematikou je daktyloskopie, která také určuje tři základní daktyloskopická pravidla [8]:

- Na světě nelze nalézt dvě osoby se stejnými otisky.
- Papilární linie zůstávají po celý život téměř neměnné.

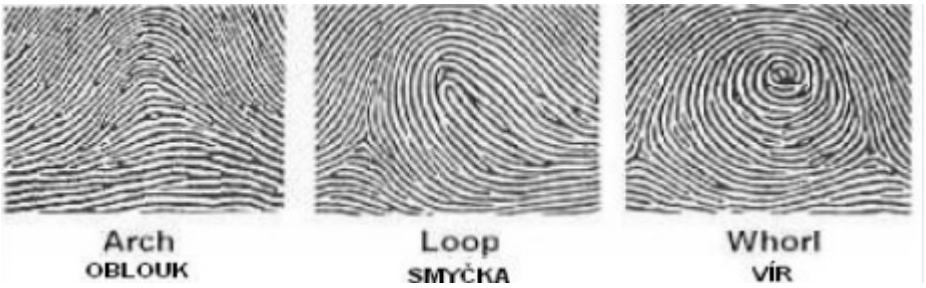
- Papilární linie jsou relativně neodstranitelné, pokud neodstraníme epidermální neboli zárodeční vrstvu kůže.

Pro rozlišení otisků rozdělujeme papilární linie do třech kategorií tzv. tříd otisků prstů dle klasifikační (Henryho) systému, vytvořeném na počátku 20. století Sirem Edwardem Henrym. Tyto kategorie jsou [11, 22, 23]:

smyčka (loop) - Papilární linie vytvářející mezi deltou a středem linii. Tento vzor se vyskytuje přibližně v 65% všech otisků.

vír (whorl) - Papilární linie tvořící kruhové, oválné čí spirálovité vzory s jádrem uprostřed. Tento vzor se vyskytuje přibližně v 30% všech otisků.

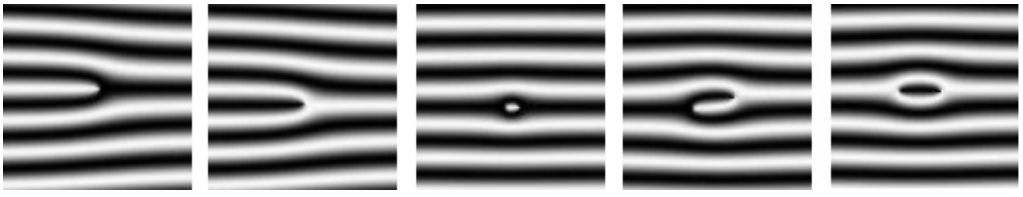
oblouk (arch) - Papilární linie vytvářející jednoduchý oblouk bez delty, nerozbíhající se. Tento vzor se vyskytuje přibližně v 5% všech otisků.



Obrázek 12: Třídy otisků prstů [2]

K přesnému určení otisku jsou používány markanty (tzv. vzory), které jsou vytvářeny papilárními liniemi. Základní vzory jsou uvedeny na obrázku 13. Tyto vzory se mohou opakovat, na jednom otisku prstu se může vyskytovat od 75 do 175 markantů. Při forenzním vyšetřování je v České republice stanoveno 10 různých markantů potřebných k identifikování osoby [1].

Ovšem v přístupových systémech je využíváno pouze dvou markantů: ukončení a vidličky [8].



Obrázek 13: Příklady markantů; ukončení, vidlička, bod, hák, očko [21]

Dělení algoritmů rozpoznávání

Algoritmy pro rozpoznávání otisků prstů mohou být různorodé, je to dáno především výrobci. Každý systém je zaměřen a aplikován na rozdílné prostředí, proto neexistuje jeden přesně ucelený princip funkce.

Pro rozpoznávání otisků můžeme určit dva základní principy [1, 11]:

- Podle globálního vzoru - systém přiřadí otisk k jedné ze tříd otisků prstů. Následně zjistí pozici vybraných markantů a počet papilárních linií. Tato metoda klade menší požadavky na rozlišení. Je to ovšem moderní metoda fungující na principu samostatného počítačového myšlení a výrobci si tuto metodu chrání, tudíž není podrobně zdokumentována.

- Podle podrobnosti - systém porovnává v několika krocích s již uloženým etalonem pozici a orientaci jednotlivých markantů otisku prstu. To klade větší nároky na senzor. Jedná se o metodu fungující na daktyloskopickém principu, která je zdokumentována, proto dále vycházím pouze z této metody.

Postup zpracování otisku

Při zpracování otisku pomocí informačních technologií můžeme celý postup rozdělit do tří fází [1]:

1. **Snímání otisků prstů**

   Tato práce je zaměřená především na automatické rozpoznávání osob pomocí komerčně dostupných systému, proto zmiňuji pouze zařízení fungující na principu live-scanning.

   Princip live-scanning je založen na snímání otisků v přítomnosti rozpoznávané osoby a k automatickému vyhodnocení [1].

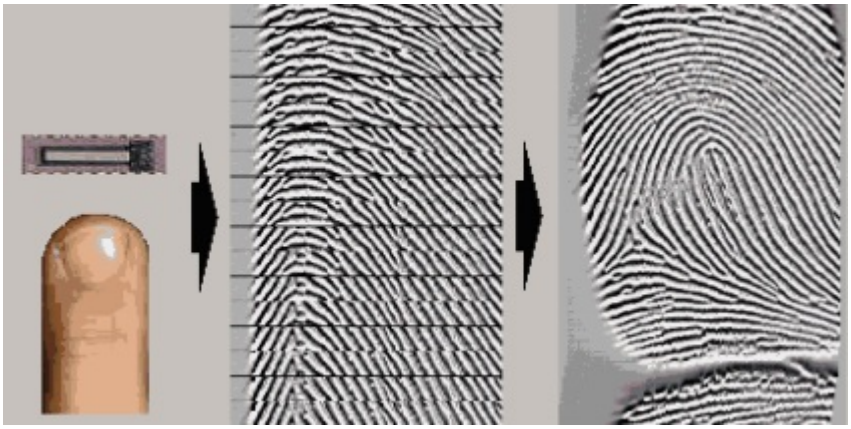
   Snímače

   Senzory snímající otisky prstů jsou založeny na mnoha technologických principech, které mají v každém prostředí, ve kterém budou používány, své výhody i nevýhody.

Existují dva základní principy snímání otisku [2]:

Statické - při kterém rozpoznávaná osoba drží prst na snímači bez jakéhokoliv pohybu. Tuto metodu dále dělíme na dotykovou a bezdotykovou.

Šablonováním - při kterém rozpoznávaná osoba přejíždí svým prstem po snímači, který je tvořen úzkým pruhem. Algoritmus poté sestaví z dílčích částí celý otisk prstu.



Obrázek 14: Snímaní šablonováním [2]

Typy snímačů[1, 2, 8, 11, 24, 25, 26, 27, 28, 29, 48]:

- Optické
  - Odrazové - jde o jeden z nejdéle používaných typů snímačů. Prst přiložený na průhlednou desku je osvětlován laserovým paprskem. Množství odraženého světla se liší podle hloubky brázd neboli mezer mezi hřebínkovitými výběžky neboli papilárními liniemi. Postupně světlo prochází přes čočku a filtr do CCD snímače.
  - Odrazové se skládáním obrazu - princip je stejný jako u předchozího snímače s tím rozdílem, že je používán ke snímání odrazový rolovací senzor, po kterém prst klouže.
  - Bezdotykové - TST[4] dochází k přímému snímání pomocí LED

[4] z anglického Touchless Technology – bezkontaktní technologie[2]

diody a odražený světelný paprsek je přijímán snímačem typu CMOS[5]

- Transmisivní - princip vychází z prosvícení prstu z horní části (od nehtu) a sejmutí obrazu snímačem (CCD nebo CMOS podle výrobce) na opačné straně.
- TFT - snímací zařízení je nahrazeno displejem TFT[6].
- Elektrooptické - tento typ je založen na vlastnostech polymerního materiálu, který při nabuzení vhodným napětím a při připojení na snímač nasvítí pouze místa, kde se přiložené papilární linie dotýkají.
- Multispektrální - tato metoda využívá prosvícení prstu pod různými vlnovými délkami, a tím poskytne více informací.

- Výhody - zajišťuje vysokou kvalitu a odolnost proti statickým výbojům.
- Nevýhody - především větší rozměr kromě elektrooptických a chybovost při znečištění. Jedním ze zásadních problémů u dotykových zařízení je otisk předešlé osoby, který zůstal na dotykové vrstvě.

- Elektronické - fungují základě vzniku elektrického pole mezi párem nabitých desek. Tvar pole se mění v závislosti na přiloženém otisku.
  - Výhody - nereaguje na špínu, proniká do hloubky papilárních linií.
  - Nevýhody - nejsou hygienické a nerozpoznají živou tkáň.

- Kapacitní - tento druh snímačů funguje na principu měření kapacitního odporu, který je rozdílný v oblasti brázd a hřebínkovitých výběžků.

[5] z anglického Complementary Metal Oxide Semiconductors - zařízení využívající doplňující se kov-oxid-polovodič odvádějící náboj z každé snímací buňky čipu zvlášť [17]

[6] z anglického Thin Film Tranzistor - průhledný film tvořený miniaturními tranzistory umožňující přepínání pixelů mezi stavy „zapnuto“ a „vypnuto“ [1]

  - Výhody - nízká cena a malá velikost.
  - Nevýhody - nízká životnost vlivem statické elektřiny a nejsou odolné vůči vlhkosti.

- Teplotní - princip spočívá na rozdílné teplotě v oblasti brázd a papilárních linií, kterou snímá pyrodetektor.
  - Výhody - možnost ochrany proti otřesu, otěru a vodě.
  - Nevýhody - nízká kvalita a nejisté algoritmy.

- Tlakové - princip tohoto snímače spočívá na dvou vrstvách vodivého materiálu oddělených izolačním gelem. Vystouplá papilární linie oproti brázdě spojí stlačením gelu vodivé vrstvy k sobě.
  - Výhody - odolný proti vlhkosti a lze jej miniaturizovat až na možnost implementace do platební karty.
  - Nevýhody - nízká citlivost.
- Ultrazvukové - fungují podobně jako optické snímače s tím rozdílem, že měří přijímaný zvuk oproti světlu.
  - Výhody - proniknutí přes nečistoty.
  - Nevýhody - větší rozměr zařízení.
- Radiofrekvenční - princip spočívá ve vyslání nízkofrekvenčního signálu směrem k prstu a měření odraženého signálu pomocí mnoha antén.
  - Výhody - odolnost vůči nečistotám.
  - Nevýhody - poněkud delší doba vyhodnocení.
- Elektroluminiscenční - princip funkce tohoto snímače funguje na vrstvě emitující světlo důsledkem tlaku vyvolaného papilárními liniemi na tuto vrstvu.
  - Výhody - malý rozměr, nízká cena.
  - Nevýhody - náchylnost na poškození a znečištění.

Kontrola živosti

Detekce živosti je důležitým krokem při rozpoznávání osob. Zajišťuje, že je osoba opravdu živou osobou a nejedná se pouze o maketu otisku. V kapitole 7.2 na straně 88 je proveden test zvoleného zařízení, zda je možné ho oklamat metodou, kterou popisuje Tsumotu Matsumota. Mezi metody kontroly živosti řadíme [8]:

Detekce potu - funguje na principu postupného ztmavení papilárních linií z důvodu výronu kapiček potu.

Spektroskopická - funguje na principu částečného pohlcení paprsků světla různých vlnových délek kůží. Tuto metodu nelze použít jako samostatnou identifikační metodu, jelikož jsou rozdíly příliš malé.

V poslední době je však této metodě věnována velká pozornost. Je snaha použít tuto metodu jako samostatnou identifikační metodu [2].

Kontrola pulsu - pomocí laseru, který dokáže rozpoznat změny objemu prstu při rozdílném tlaku průtoku krve.

Dále je možné různé metody spojit s metodami, které již ve své podstatě mají kontrolu živosti. Tyto metody jsou například: ultrazvuková, teplotní nebo tlaková.

2. **Uložení a zpracování otisků prstů**

   K ukládání nasnímaného vzoru je využívána komprimační metoda WSQ, která zajišťuje vysoký komprimační poměr s minimální ztrátou dat [30].

   - Příklad: Otisk s rozlišením 589 x 605 pixelů v černobílé 8bitové škále [1].
     - Bez komprimace: 325kB
     - JPEG: 108kB
     - WSQ: 28kB

Zpracování lze rozdělit do dvou fází [1]:

(a) Předzpracování obrazu - jde především o korekturu obrazu otisku prstu rozdělenou do tří kroků:

   i. Prostorová konvoluce - odstranění šumu.

   ii. Binarizace - převod barev na binární hodnoty.

   iii. Skeletizace - redukce čar na tloušťku jednoho pixelu.

(b) Nalezení a extrakce markantů - vyloučení falešných markantů, určení typu, souřadnic a orientace nalezených markantů pomocí algoritmů.

3. **Porovnání otisků prstů**

Určení konečného skóre systémem, které je porovnáno s prahovou hodnotou a dochází k rozhodnutí, zda je otisk schválen či zamítnut [1].

3.2.3 Podélné rýhování nehtů

Tato metoda není primárně založena na viditelném rýhování nehtů, ale na nehtovém lůžku, které se nachází pod nehtovou ploténkou [2].

Zajímavou metodou je také zápis dat do nehtové ploténky pomocí laseru [8].

Výhody a nevýhody

Nehtové lůžko je chráněno nehtovou ploténkou, proto není snadné tuto vrstvu narušit. U zápisu do nehtové ploténky dochází ke ztrátě dat při odrůstání nehtu.

3.2.4 Krevní řečiště

Jedná se o moderní metodu snímající tvar cévního řečiště v oblasti dlaně a hřbetu ruky ale také článků prstů [31].

Skenování probíhá pomocí infračerveného světla a CCD kamery na principu prosvícení. Je snímán a vyhodnocován celý obraz nikoli určené body [1].

Obrázek 15: Krevní řečiště [21]

3.2.5 Dynamika úchopu

Snímání probíhá pomocí tlakových bodů, které jsou rozloženy na pažbě zbraně. Úchyt zbraně a tlak vyvolaný na pažbu je pro každou osobu specifický. Díky tomuto poznatku lze zamezit oprávněnému užití zbraně cizí osobou [2].

Výhody a nevýhody

Použití je především k policejním účelům. Prozatím tato metoda nemá uplatnění pro autentizaci osob na základní škole.

3.3 Anatomicko-fyziologické metody v oblasti celého těla

3.3.1 Pach lidského těla

Tato metoda je prozatím používána pouze ve forenzním vyšetřování, kdy jsou pro tyto účely speciálně vycvičeni psi. Základní funkce technického snímání pachu spočívá v absorbaci molekul v okolí snímače pomocí chemických senzorů, které změní své vlastnosti. Tato změna je poté převedena na některou z elektrických veličin [2, 8].

Výhody a nevýhody

V komerční sféře zatím neexistují dostatečně citlivé senzory. Největší nevýhodou této metody je prozatím malá zkušenost se změnami pachu při hormonálních či emocionálních výkyvech [2].

3.3.2 Obsah soli v lidském těle

Jednou z nejméně známých metod je i měření obsahu soli v lidském těle, i tak lze od sebe odlišit různé osoby [1].

Výhody a nevýhody

Tato metoda nemá komerční využití na českém trhu.

3.3.3 Rozměry lidského těla (Atropometrická metoda)

Jak již zmiňuji v kapitole 2.3 na straně 14, tak Antropometrická metoda je jednou z prvotních metod biometrické autentizace, ze které se dále rozvíjely metody jako geometrie ruky či tváře. Samotná původní metoda sloužila v kriminalistice k nalezení pachatele. Bylo měřeno 11 částí těla, a to například výška těla vestoje, výška těla vsedě, šířka rozpětí paží atd. Počet 11 rozměrů zajišťoval pravděpodobnost shody dvou zločinců na 1:4 191 304. Dále pak byly osoby děleny do skupin například podle barvy očí a jiných vlastností [1].

Výhody a nevýhody

Tato metoda se dnes používá jako doplněk k různým metodám, kdy je společně s jiným snímáním použito měření výšky či dokonce váhy s určitým rozptylem pro přesnější autentizaci nebo pro rychlejší verifikaci při rozdělení osob do jednotlivých skupin.

3.3.4 DNA

Tuto metodu uvádím také jen pro úplnost výčtu metod. Je jednou z nejpřesnějších metod a je využívána pouze k identifikaci osob v kriminalistice.

Výhody a nevýhody

Pro využití v komerčních aplikacích zatím není dostatečně přijatelná především ze stránky ochrany soukromí a uživatelské nepřívětivosti. Informace nesoucí struktura DNA mohou být zneužity.

3.3.5 Bioelektrické pole

Bioelektrické pole je okem neviditelné pole kolem každé osoby a nejen osoby. Snímačem tohoto pole lze osoby autentizovat, jelikož je pro každou osobu jedinečné [2].

Výhody a nevýhody

Velkou výhodou této metody je možnost zjištění bioelektrického pole osoby, která je v pohybu. Nevýhoda pak spočívá v nemožnosti rozeznat dvě osoby, které se nacházejí ve své blízkosti [2, 32].

3.3.6 Biodynamický podpis

Metoda biodynamického podpisu je založena na rozdílných EKG křivkách každé osoby. Autentizace osob probíhá pomocí dotyku se zařízením k tomu určenému. Jde o zařízení, které obsahuje dva vodivé kontakty, na které osoby přikládají dva prsty [2, 33].

Velmi podobnou metodou je metoda založená na křivce EEG. Opět je ze zařízení generován signál do autentizované osoby a po následném vyhodnocení je nebo není osoba autentizována [34, 35, 36].

Výhody a nevýhody

Tyto metody se převážně používají v medicínské praxi a běžně nejsou používané.

3.4 Behaviorální metody

3.4.1 Analýza hlasu

Biometrická informace získaná pomocí mikrofonu, založená na vlastnostech hlasu (výšce, hlasitosti či délce trvání tónu) daných hlasovým ústrojím člověka. Charakteristickou informací může být také styl vyjadřování a z tohoto důvodu řadíme analýzu hlasu mezi behaviorální charakteristiky [22].

Při komerčním nasazení se používá metoda založená na verifikaci, jelikož samotná identifikace je příliš náročná [8].

Výhody a nevýhody

Velká výhoda spočívá v možnosti autentizovat osobu na značnou vzdálenost a především v uživatelské přívětivosti, kdy je řeč přirozeným stylem vyjadřování. Nevýhodou je nemožnost autentizovat osoby, které jsou němé či pokud je ve snímaném prostoru velký hluk [1, 8].

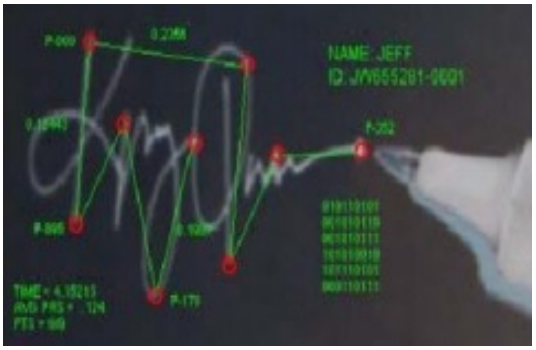
Obrázek 16: Zobrazení hlasového signálu

3.4.2 Dynamika podpisu

Tato metoda je založená na měření rychlosti, tlaku a stylu jednotlivých tahů při psaní podpisu perem na tablet umožňující toto snímání. Celý záznam se ukládá ve čtyřech rozměrech, tudíž je minimální pravděpodobnost plagiátorství [11].

Výhody a nevýhody

Výhodou se stává uživatelská přívětivost z důvodu zvyklosti na využívání podpisu. Nevýhodou se stává nižší přesnost [17].



Obrázek 17: Princip měření dynamiky podpisu [2]

3.4.3 Dynamika stisku kláves

Jednou z nejlevnějších metod je právě metoda dynamiky stisku kláves, a to z důvodu, že není potřeba speciálních zařízení pro snímání. Oproti psaní hesla se nesleduje pouze psaný text, ale časová prodleva mezi jednotlivými stisky kláves, délka trvání jednotlivého stisku, celková rychlost psaní a pokud to klávesnice umožňuje, tak i polohu prstu na klávese a tlak vyvinutý na tuto klávesu [2, 37].

Výhody a nevýhody

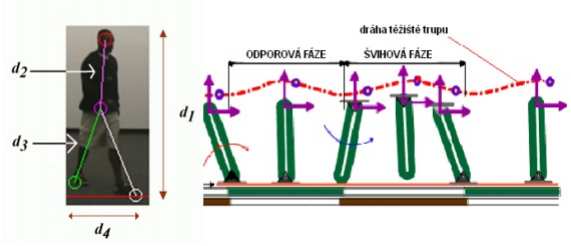
Výhoda spočívá v možnosti autentizovat osobu na velkou vzdálenost a i uživatelsky je tato metoda vcelku přívětivá. Mezi výhody lze také zařadit možnost, kdy aplikace autentizující osoby běží na pozadí a stále kontroluje. Nevýhody však v této metodě převažují. Nejzávažnější chybou je nízké procento správné autentizace osob z důvodu změny stylu psaní při fyzickém úrazu či jiných okolnostech [2, 37].

3.4.4 Dynamika chůze

Pohyb při chůzi je pro každou osobu jedinečný a lze tak porovnávat stereotypní pohyby znázorněné křivkami opisujícími určité body, především těžiště těla. Tato metoda je uplatněna hlavně ve forenzní sféře, kdy pachateli nepomůže ani maskovací převlek. S rozvojem moderní techniky se tato metoda uplatňuje na rušných místech, jako jsou letiště či nádraží [2].

Výhody a nevýhody

Velký vliv na tuto metodu má fyzický stav identifikované osoby, ovšem i oblečení, osvětlení místnosti či vlivy okolního prostředí [8].



Obrázek 18: Jeden z postupů měření dynamiky chůze [21]

4 Analýza dostupných řešení

Cílem této části práce je provést analýzu metod biometrických systémů dostupných na českém trhu použitelných k optimálnímu a komplexnímu řešení biometrické autentizace žáků na základní škole. Analýza je založena na dostupné literatuře a na informacích, které mi poskytly firmy uvedené v kapitole 6.1 na straně 59.

Tabulka porovnání obsahuje výhody a nevýhody jednotlivých metod, které lze použít v komerční sféře, tedy i pro účely této práce. Ostatní metody, které pro využití při autentizaci na základní škole nelze použít nebo nejsou dostupné, jsou již rozebrány v předchozím výčtu metod.

Biometrická charakteristika	Výhody	Nevýhody
Geometrie tváře	• uživatelská přijatelnost • možnost snímání v pohybu • bezkontaktnost	• snížení přesnosti osvětlením, natočením hlavy, předměty jako brýle a další • s přesností roste cena a velikost šablony • vysoká chybovost
Oční duhovská	• vysoká přesnost a míra jedinečnosti • bezkontaktnost • nízká náchylnost k poškození	• nepřijatelné v některých kulturách • vysoká pořizovací cena • možnost zneužití • v některých případech nutnost sundání brýlí nebo kontaktních čoček
Otisk prstu	• přijatelná cena • malá velikost snímače	• fyzický kontakt
Krevní řečiště	• existuje i bezkontaktní forma • není ovlivněno špínou či světelnými podmínkami • neměnnost a vysoká míra jedinečnosti	• u kontaktních forem fyzický kontakt a velká plocha dotyku

Tabulka 1: Porovnání výhod a nevýhod biometrických metod [17, 38, 39]

Pro porovnání je použito kromě výčtu výhod a nevýhod také několik kritérií zmíněných v tabulce 2.

Biometrická charakteristika	Geometrie tváře	Oční duhovská	Otisk prstu	Krevní řečiště
Univerzalita	1	1	2	2
Jedinečnost	3	1	1	2
Stálost	2	1	1	2
Získatelnost	1	2	2	2
Výkonnost???	3	1	1	2
Akceptovatelnost	1	2	2	2
Odolnost	3	1	2	*
Cena	2	3	1	2

1 - nejlépe splněná vlastnosti; 2 - středně; 3 - nejhůře

Tabulka 2: Porovnání kritérií biometrických metod [1, 2, 8, 11, 40]

Z předchozí tabulky nejlépe vychází metoda snímání oční duhovky a metoda snímání otisku prstu. Jako jedno z nejdůležitějších kriterií považuji cenu systému, a proto je pro praktickou část vybrána metoda otisku prstu. Metoda otisku prstu je také nejrozšířenější metodou biometrické autentizace, jak ve světě, tak i na českém trhu. S tímto tvrzením souhlasí čeští poskytovatelé uvedení v kapitole 6.1 na straně 59. Pokud se zaměřím i na zbylé nabízené metody, tak metoda snímání obličeje je využívána především v oblastech s pohybem osob, jako jsou například herny. Metoda snímání oční duhovky je upřednostňována ve specializovaných centrech s vysokou bezpečností a metoda snímání krevního řečiště prozatím nemá velké uplatnění, ale také se používá k podobným účelům.

Praktická část

5 Návrh biometrického systému

Jedním z hlavních cílů mé práce je navrhnout vhodný systém použitelný pro autentizaci žáků na základní škole. Proč vůbec kontrolovat docházku dětí do základní školy? Tak především je školní docházka dle zákona povinná. A jako druhá možnost je využití okamžitého kontaktování zákonných zástupců, pokud žák nedorazí do budovy školy včas na výuku a škola nebude obeznámena s jeho pozdním příchodem. Tato druhá možnost je již jen systémovým problémem, běžné přístupové systémy toto neumožňují.

Osobně si myslím, že kontrola vstupu do budovy je to krok správným směrem, pokud beru v potaz události, kdy byly napadeny cizí osobou děti nebo personál školy jak v České republice, tak i v jiných státech. Je potřeba zajistit co nejdříve a co nejbezpečněji vstup do budov škol.

Každý systém musí být přesně nastaven dle konkrétních podmínek daného prostředí. Nelze zvolit jeden globální systém, který by vyhovoval všem podmínkám.

Při samotném návrhu je třeba brát zřetel na všechny situace, které mohou při samotném návrhu nebo při běhu systému nastat. Základní otázkou je, zda je vůbec možné tento typ autentizace použít. Pokud je v budově velký počet osob, které nezávisle na čase vstupují a opouští budovu, jako například na vysoké škole, kdy žáci nemají souvislý rozvrh, klesá výkonnost těchto systémů a zvyšují se nároky především ze strany správy dat. Proto jsem zvolit počet žáků dle statistiky Ministerstva školství, mládeže a tělovýchovy v České republice. Statistika uvádí, že maximálně jedna základní škola v běžném školním roce za posledních 5 let převýšila hranici počtu 1000 žáků. Pokud chceme docílit co nejnižší možnosti odmítnutí přístupu žáka do školy, je vhodné použít nejméně dva otisky. Jeden z pravé a druhý z levé ruky, proto je potřeba, aby systém dokázal pojmout 2000 otisků, tím se však zvyšují i nároky na systém. Jedna ze tří firem, se kterými jsem tuto práci konzultoval, neposkytuje zařízení s takovou kapacitou šablon. Ovšem tato

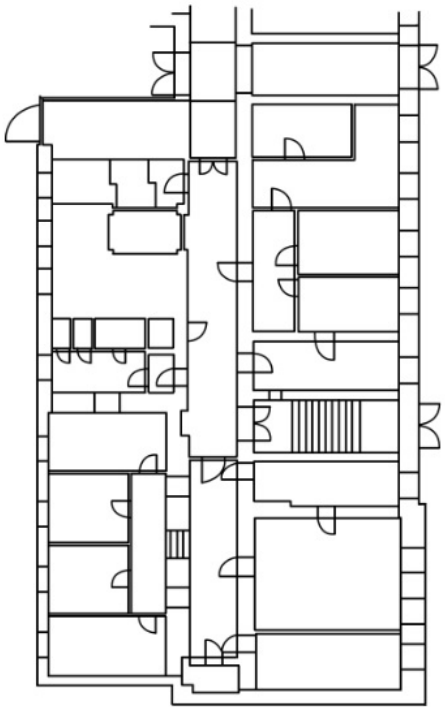
firma poskytuje nejvyšší bezpečnost a pokud vycházím z maximálního možného počtu, který poskytuje, a to 1500 otisků tedy 750 žáků, tak toto číslo stále zahrnuje 99,44% počtu základních škol za posledních 5 let [42].

Snímače mají především potíže rozeznat otisk, pokud je prst zašpiněný. Například pokud žáci opustí budovu školy při tělesné výchově nebo technických pracích, kde se mohou ušpinit, tak později při návratu jim nemusí být povolen přístup. O tento problém se může postarat učitelský dozor, který žáky vpustí do budovy a zajistí, aby se mezí žáky nevmísila cizí osoba.

Z druhé stránky není vhodné použít dotykový snímač otisků prstu u výdejního okénka v prostorách jídelny. I když je ploška bříška prstu velmi malá, nevyhovuje hygienickým podmínkám. Proto je v tomto případě vhodné používat čipy nebo karty pro potvrzení, že byl oběd objednán a řádně zaplacen. I přes možnost ztráty či odcizení předmětu pro autentizaci.

5.1 Budova

Jelikož se mi nepodařilo sehnat reálnou školu, která by vyžadovala nebo alespoň uvažovala o implementaci biometrického autentizačního systému, zvolil jsem pro návrh budovu Pedagogické fakulty Jihočeské univerzity v Českých Budějovicích nacházející se v ulici Jeronýmova 10. Tuto variantu jsem zvolil z důvodu, že je možné implementovat více různých zařízení na tři vchody nacházející se v této budově, které mohou studenti využít, a také z důvodu možnosti použití vnitřních i vnějších biometrických snímačů.



Obrázek 19: Schéma budovy

Jak je z plánu budovy zřejmé, je potřeba instalovat tři čtečky otisků prstů. Jeden vchod je totiž nepřístupný.

5.2 Účel systému

Biometrické autentizační systémy je možné rozdělit podle funkce do dvou skupin:

5.2.1 Přístupové

První skupinou jsou systémy přístupové, které jsou založeny na funkci povolení či zamítnutí vstupu osoby do objektu dle jeho oprávnění. V zásadě jde o náhradu místo klíče nebo čipu. Tento systém nemusí být oproti docházkovému systému tolik společensky přijatelný, neboť jde o bezpečnost objektu a osob.

5.2.2 Docházkové

Druhou variantou systému je systém docházkový, který má za účel automatickou evidenci osob, které vstoupily nebo opustily objekt a tyto informace ukládat do databáze k následnému použití. Zjednodušeně se dá říci, že jde o „píchačky“, které se využívají ve firmách pro kontrolu docházky a výpočtu mzdy zaměstnanců, nebot' to vyžaduje stát. U těchto zařízení je možné nastavit více funkcí než pouhý vstup a výstup, například odchod k lékaři a další. Důležité je, aby se jednalo o biometrický autentizační systém, který je dobře akceptovatelný lidmi z důvodu každodenního používání, systém by také měl být rychlý, aby se u vchodu do budovy netvořily fronty.

5.2.3 Výběr

Dle těchto informací je třeba zvolit správný systém použitelný pro školní účely. I když teoreticky obě tyto varianty souhlasí, v praxi tomu tak vždy být nemusí, záleží na požadavcích pro konkrétní systém. Lze využít i čtečky určené pro přistup a v jednoduchém spojení se systémem lze zaznamenávat příchody osob. Na základních školách je potřeba zajistit především neoprávněný přístup cizích osob. Docházkový systém prozatím nemá uplatnění, kromě kontroly docházky učitelského sboru. Pro kontrolu docházky žáků by musela být v každé třídě čtečka, jelikož se zaznamenává docházka na každou hodinu zvlášt' do třídní knihy, proto tuto variantu mohu rovnou vyřadit a dále se zabývat pouze přístupem do budovy školy.

5.3 Právní náležitosti

V souvislosti s pořizováním a ukládáním biometrických informací je třeba řešit otázku právních záležitostí, především ochranu před zneužitím.

Systém je třeba registrovat na Úřadu pro ochranu osobních údajů, pokud je biometrický údaj v systému spjat s osobními údaji [51]. Pro funkci systému není důležité znát osobní informace osob. Každá osoba přidělená do systému může dostat svůj zvláštní identifikační kód, a tím se eliminuje nutnost registrace systému na Úřadu pro ochranu osobních údajů. Ovšem vždy je určitá

možnost spojitosti, proto je vhodným řešením systém registrovat.

Správce systému nemusí požadovat od osob povolení pro snímání biometrických dat. Pokud, je v prostorách školy tento systém provozován je tato informace zanesena do školního řádu a je na každém, zda poskytne svůj biometrický údaj či nebude tuto školu navštěvovat. Pokud nemůže poskytnout svůj biometrický údaj, musí mu být poskytnuta jiná možnost přístupu do budovy.

5.4 Bezpečnost

Jedním z nejdůležitějších faktorů výběru systému je především bezpečnost.

5.4.1 Možné útoky

V podstatě na každý prvek systému je možné vyvolat útok. Jedná se o útoky jako na každé jiné technologie, proto není důvod hned podceňovat tyto systémy. Mezi nejběžnější útoky patří [8]:

Falešný vzorek - jde o nejčastější možnou variantu napadení, kdy je přiložen na snímač falešný či dokonce amputovaný článek prstu. Tuto variantu demonstruji v kapitole 7.2 na straně 88. Ochranou proti tomu druhu útoku je kontrola živosti, která je popsaná v kapitole 1 na straně 42.

Opětovné použití údaje - signál v digitální podobě, který již byl aplikován, je znova předložen do cesty mezi senzor a extraktor rysů. Pro tento způsob útoku je potřeba systém dostatečně znát. Ochranou je důkladné zabezpečení přenosové cesty.

Ovlivnění extrakčního algoritmu - napadení trojským koněm může být jednou z metod pro vygenerování nežádoucí šablony.

Změna rysů - opětovně jako mezi senzorem a extraktorem rysů, je také možné mezi extraktorem rysů a porovnávacím modulem zaměnit data.

Změna porovnání - virem je také možné napadnout porovnávací modul, který upraví skóre pro porovnávání, a tím zjednodušit proniknutí.

Modifikace šablony - samotnou šablonu lze v databázi nahradit jinou.

Útok na přenosový kanál šablony - při přenosu šablony z databáze lze napadnout cestu, a tím pozměnit šablonu.

Změna výsledku - lze ovlivnit i konečný výsledek rozhodnutí tím, že bude zamítnut.

5.5 Společné funkce systému

Veškeré systémy využívají určité stejné funkce, které není potřeba zmiňovat pro každý systém zvlášť, proto jim věnuji tuto kapitolu.

5.5.1 Způsob připojení

On-line – stálé kabelové propojení snímače s řídícím počítačem. Lze jednoduše spravovat data uložená ve snímači. Data jsou oboustranně zasílána ke zpracování. Výhodné pro systémy s velkým počtem uživatelů, u kterých je potřeba spravovat informace.

Off-line – dočasné kabelové propojení snímače s řídícím počítačem. Data se ze snímače stahují manuálně. Vhodné pro systémy s malým počtem osob, kde není potřeba měnit informace o osobách. V případě změny je nutné snímač odmontovat z místa, kde je nainstalován, jelikož se zdířky nacházejí z důvodu bezpečnosti na zadní straně snímače.

5.5.2 Způsob zadávání otisků - registrace

Existuje více možností registrace osob do systému, které záleží především na počtu registrovaných osob. Při malém počtu osob je jednoduché nahrát otisky přímo pomocí zařízení, které je instalované u vchodu do budovy. Toto řešení není vhodné, pokud se takto musí registrovat velký počet osob. V mém případě počítám s registrací až 1000 osob, proto využiji kromě běžných snímačů otisků i stolní snímač umístěný v kanceláři pro jednodušší a komfortnější registraci žáků. Šablony jsou poté rozšířeny do všech zařízení.

Různá zařízení také používají různý druh registrace nových osob. Registrace je především založená na opakovaném přiložení prstu na dotykový povrch snímače a z těchto pokusů je vybrán ten nejlepší, jak je uvedeno v kapitole 2.5.2 na straně 18. Osobně jsem se setkal se zařízením, které požadovalo, aby registrovaná osoba přiložila prst třikrát, ale také se zařízením, které pro registraci využívalo dva čipy - jeden pro spuštění módu registrace

a druhý pro spuštění módu mazání. Obě tato zařízení zmiňuji v kapitole 7 na straně 85.

Samotná registrace je časově velmi náročná, jelikož je systém aplikován do prostředí, kde se nacházejí malé děti, kterým ještě rostou ruce, tím se i mění šablona a je potřeba registraci opakovat alespoň jednou ročně.

6 Konečná řešení

Jako návrh biometrické autentizace žáků na základní škole jsou vytvořeny dva projekty rozdělené podle bezpečnosti.

6.1 Poskytovatelé

Pro svou práci jsem oslovil několik firem fungujících na českém trhu zabývajících se touto problematikou. Pouze tři firmy mi poskytly informace potřebné k vypracování této práce. Jedná se o firmy ABBAS, a.s., IReSoft, s.r.o. a Z-WARE.

První návrh od společnosti ABBAS sice nesplňuje kritérium 1000 osob, ale zajišťuje nejvyšší stupeň bezpečnosti. Druhý návrh od společnosti IReSoft již splňuje kritérium počtu osob, ale s využitím jednoho turniketu je méně bezpečný. Třetí návrh již nebyl realizován z důvodu nejnižší bezpečnosti. Pro zajištění bezpečnosti by u vchodu při vysokém počtu vcházejících osob před začátkem výuky musel hlídat učitelský dozor a systém by se tímto minul účinkem.

6.2 Řešení s využitím zařízení firmy ABBAS, a.s.

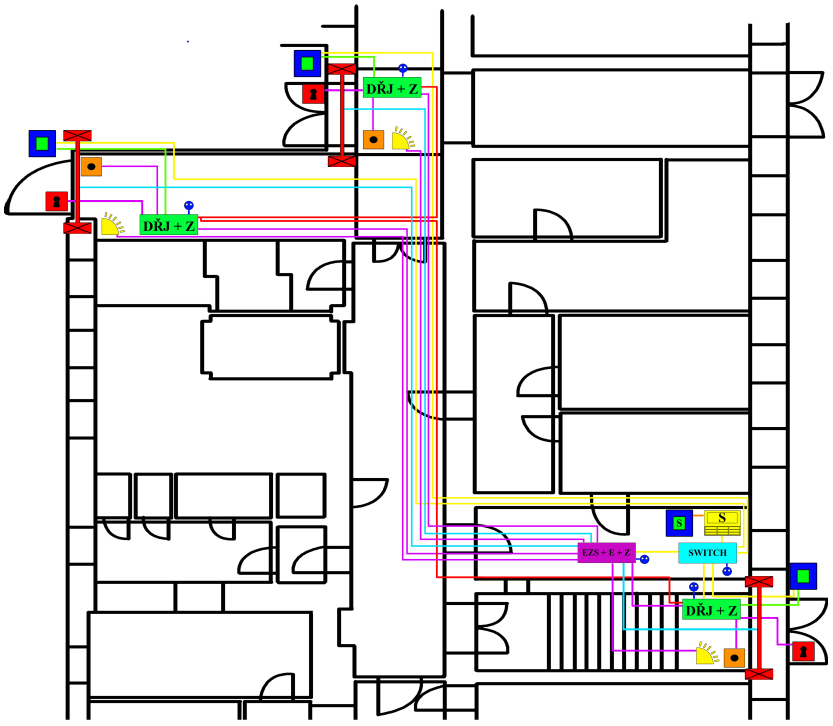
6.2.1 Popis firmy

Společnost ABBAS je česká firma fungující na trhu již od roku 1995. Tato firma je především dodavatelem bezpečnostních technologií, ale také kvalifikovaným poradcem v této oblasti.

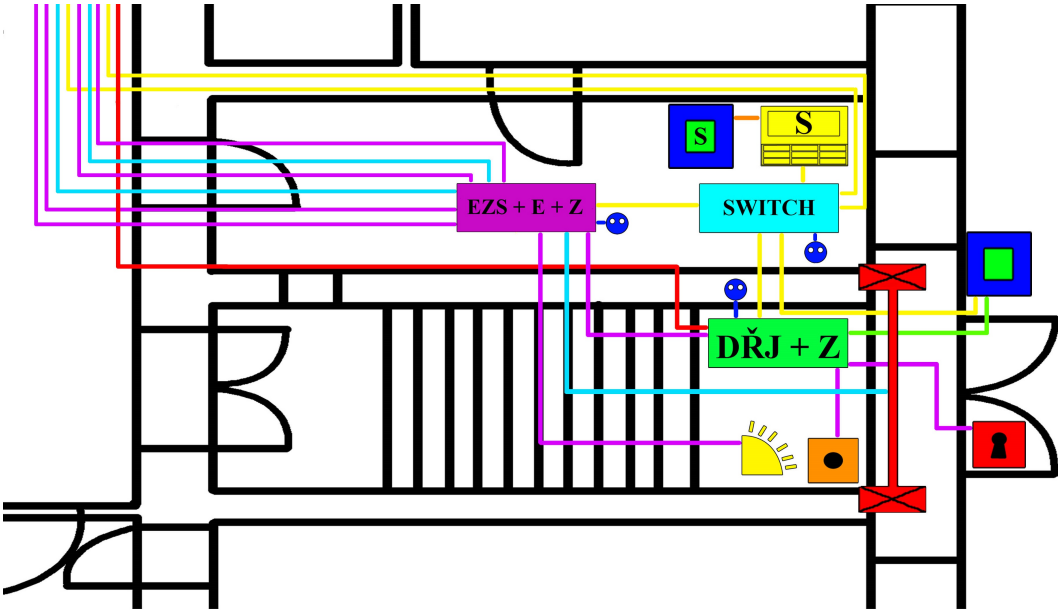
6.2.2 Hardwarové řešení

Komplexní systém se skládá z jednotlivých samostatných prvků, které zajišťují celkovou funkci systému. Návrh lze rozdělit na přístupovou část a bezpečnostní. Přístupovou část je možné dále specifikovat na oblast dveří, tyto oblasti jsou v návrhu tři a každá obsahuje jedno snímací zařízení z vnější strany dveří, jedno odchodové tlačítko z vnitřní strany dveří, jednu řídící jednotku v boxu společně se záložním akumulátorem a jeden otevírač dveří.

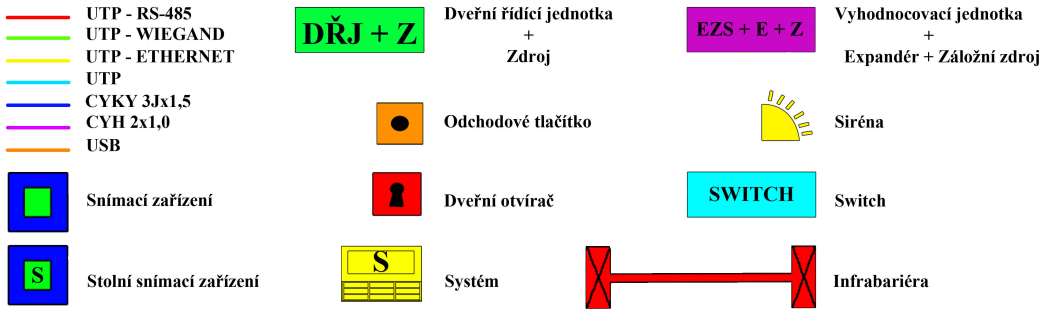
Dále k přístupové části patří samostatné stolní snímací zařízení a systém spravující přístupovou část. Bezpečnostní část v oblasti dveří obsahuje jednu infrabariéru a jedno výstražné zařízení - sirénu. Dále k bezpečnostní části patří vyhodnocovací jednotka v boxu společně s expandérem pro připojení sirének a také se záložním akumulátorem. Bezpečnostní část spravuje samostatný bezpečnostní systém. Společným prvkem celého systému je switch, který je připojen k počítači, na kterém běží systémy. Do návrhu nezapočítávám počítačovou sestavu, předpokládám, že se již v budově nachází.



Obrázek 20: Schéma zapojení ABBAS



Obrázek 21: Výřez schéma zapojení ABBAS



Obrázek 22: Legenda ABBAS

Přenosová média

Pro každou část systému je vhodné používat různé druhy přenosových médií. Mezi nejpoužívanější se řadí:

- **UTP** - Nestíněné kroucené dvojlinky

Využívající technologii:

  - **Wiegand -** toto rozhraní se používá především pro komunikaci mezi snímačem otisků prstů a dveřní řídící jednotkou. Tato komunikace je pouze jednosměrná, a to ze čtečky do řídící jednotky. Fyzická vrstva Wiegandu se skládá ze tří vodičů označovaných - GND, DATA0 a DATA1. Po tomto rozhraní putuje pouze osmimístný kód označující šablonu, nikoli samotné šablony. Délka vedení se pohybuje v desítkách metrů, proto se řídící jednotky umísťují v blízkosti čtecích zařízení.
  - **RS485 -** dříve používané sběrnice RS232 dnes nahrazované RS485 slouží ke sběrnicovému zapojení až 32 řídících jednotek. Komunikace probíhá po čtyřech vodičích a výhodou je délka jedné větve až 1200 m.
  - **Ethernet -** používající se k oboustranné komunikaci se snímacím zařízením, pomocí běžné kroucené dvoulinky a konektoru RJ-45. Převážně slouží k administraci šablon ve snímacím zařízení, jak v režimu on-line, tak off-line.

- **USB -** Univerzální sériová sběrnice

  Některé čtečky disponují usb rozhraním pro off-line administraci dat. V tomto návrhu je technologie USB využita především pro spojení pc a stolního snímacího zařízení.

- **CYH 2x1,0 -** Dvojlinka

  Obyčejná dvojlinka slouží v návrhu pro spínání určitých prvků, a to dveřního otvírače, odchodového tlačítka a sirény.

- **CYKY 3Jx1,5 -** Síťový kabel

  Síťový kabel slouží pro napájení dveřní řídící jednotky a vyhodnocovací jednotky bezpečnostního systému.

Snímací zařízení

Nejdůležitějším prvkem systému je samozřejmě samotné snímací zařízení.

Vnější snímací zařízení

V tomto návrhu bylo použito vnější snímací zařízení s pamětí pro šablony otisků prstů. Pro jednodušší správu šablon je toto zařízení v režimu on-line, tudíž je stále připojené pomocí UTP využívající technologii Ethernet ke společnému switchy. Snímací zařízení je také připojené pomocí druhé kabelové linky UTP k dveřní řídící jednotce. Na této lince je využíváno technologie Wiegand a také je po této lince snímací zařízení napájeno.

Obrázek 23: Biometrická čtečka MA 300 [43]

Technické parametry [43, 44]:

- Název: Biometrická čtečka MA 300
- Výrobce: ZK Teco
- Typ senzoru: Optoelektronický
- Komunikace: USB, TCP/IP, Wiegand, RS-485
- Napájecí napětí: 12 V DC
- Provozní teplota: -10 až +60 °C

- Maximální počet otisků prstů: 1500
- Stupeň krytí: IP54
- Rozměry: 120 x 65 x 35 mm
- Hmotnost: 1,5 kg

Vnitřní snímací zařízení

Pro jednodušší registraci osob je využito vnitřního neboli stolního snímacího zařízení. Toto zařízení je umístěno v kanceláři a slouží k nasnímání všech otisků prstů a ty jsou dále distribuovány do vnějších snímacích zařízení.

Obrázek 24: Stolní snímací zařízení ZK6000 [43]

Technické parametry [46]:

- Název: Stolní snímací zařízení ZK6000
- Výrobce: ZK Teco
- Rozlišení: 500 DPI[7]
- Komunikace: USB 2.0

[7] z anglického Dot Per Inch - počet bodů na palec [47]

- Rozměry: 81 x 50 x 21 mm
- Hmotnost: 0,095 kg

Řídící jednotka

Dveřní řídící jednotka slouží v systému jako prvek, který má za úkol porovnat přijatý kód od snímacího zařízení s kódy uloženými ve své databázi. Pokud přijatý kód souhlasí, řídící jednotka odešle impulz k sepnutí dveřního otevírače. V návrhu jsou použity tři řídící jednotky, ty jsou propojena pomocí UTP a komunikují na základě technologie RS-485. Poslední řídící jednotka, která je nejblíže switchy, je připojeny také pomocí UTP ovšem komunikace probíhá pomocí technologie Ethernet. K řídící jednotce je připojeno odchodové tlačítko pro odemčení dveří z vnitřní strany. Jednotka je umístěna na bezpečné místo uvnitř budovy, aby nebylo možné se do jednotky dostat a pomocí připojeného napětí na dveřní otvírač otevřít dveře. Z důvodu komunikační vzdálenosti technologie Wiegand. Je nutné řídící jednotku umístit do blízkosti snímacího zařízení.

Obrázek 25: Řídící jednotka Net2 plus [43]

Technické parametry [43]:

- Název: Řídící jednotka Net2 plus
- Výrobce: Paxton
- Napájecí napětí: 11-15 V DC
- Komunikace: Wiegand, Ethernet, RS-485
- Teplota provozní: 0 až +55 °C
- Max. počet kódů: 50000
- Další vlastnosti: možnost integrace EZS
- Rozměry: 320 x 236 x 80 mm
- Hmotnost: 1,538 kg

Záložní zdroj

Záložní akumulátor je do systému integrován z důvodu možnosti přístupu do budovy a odchodu z budovy při výpadku proudu. Záložní akumulátor se nachází v boxu s každou řídící jednotkou a také s vyhodnocovací jednotkou EZS.

Obrázek 26: Olověný akumulátor CT 12-7[43]

Technické parametry [43]:

- Název: Olověný akumulátor CT 12-7
- Výrobce: CTM Components
- Napětí: 12 V
- Kapacita: 7 Ah
- Rozměry: 94 x 151 x 65 mm
- Hmotnost: 2,54 kg

Odchodové tlačítko

Z důvodu snížení ceny je umístěno z vnitřní strany dveří pouze odchodové tlačítko. Proto není problém, pokud by došlo k ohrožení osob v budově pouze stisknout toto tlačítko a dojde k otevření dveří. Pokud by došlo k vybití záložního akumulátoru, dveře je možné odemknout běžným klíčem.

Obrázek 27: Odchodové tlačítko E50 [43]

Technické parametry [43]:

- Název: Odchodové tlačítko E50
- Výrobce: Paxton

- Rozměry: 58 x 50 x 14 mm
- Hmotnost: 0,238 kg

Dveřní otvírač

Je důležité, jaký druh otvírače volíme, konkrétně jakou formu napájení. Z bezpečnostních důvodů je použít otvírač, který není pod stalým napětím. Pokud bychom použili opačný, došlo by při ztrátě napějtí k otevření dveří.

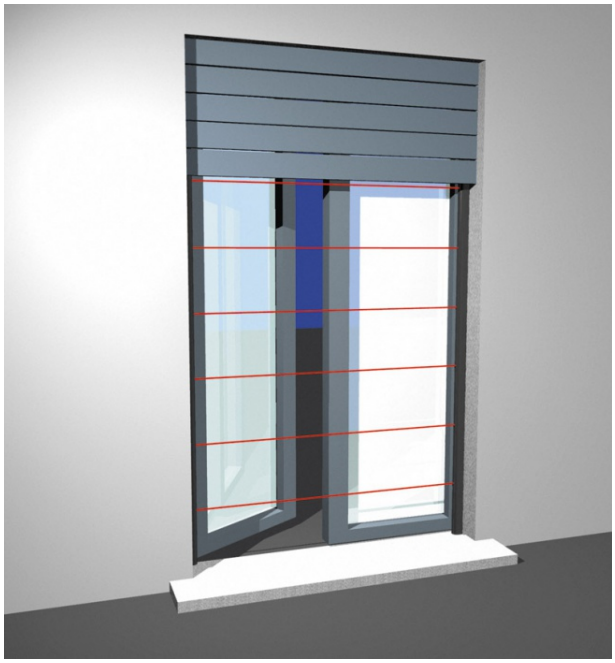
Obrázek 28: Elektromagnetický otvírač FAB BeFo Profi 11211 [43]

Technické parametry [43]:

- Název: Elektromagnetický otvírač FAB BeFo Profi 11211
- Výrobce: ASSA ABLOY Czech & Slovakia s.r.o.
- Pevnost proti vylomení: 285 kg
- Napájecí napětí: 12 V DC
- Teplota provozní: -15 až +50 °C
- Hmotnost: 0,4 kg

Infrabariéra

Infrabariéra je prvním prvkem bezpečnostní části. V návrhu je umístěna hned na vnitřní rám dveří, jelikož se dveře otevírají ven. Pokud se osoba autentizuje na vstupu, tedy na vnějším snímacím zařízení potažmo i na výstupu stiskem odchodového tlačítka, je infrabariéra po dobu průchodu autentizované osoby vypnuta. Pokud se se neautentizovaná osoba pokusí projít ihned za autentizovanou osobou, infrabariéra tento průchod zaznamená a záznam odešle do vyhodnocovací jednotky.



Obrázek 29: Infrabariéra DARWIN 02 [43]

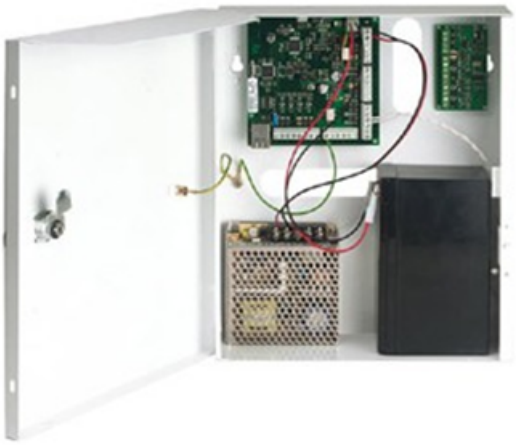
Technické parametry [43]:

- Název: Infrabariéra DARWIN 02
- Výrobce: CIAS
- Prostředí: venkovní, vnitřní
- Typ bariéry: sloupová

- Dosah: 12 m
- Počet paprsků: 2
- Stupeň krytí: IP44
- Teplota provozní: -25 až +55 °C
- Napájecí napětí: 13.8 V DC
- Hmotnost: 0,545 kg

Vyhodnocovací jednotka

Vyhodnocovací jednotka bezpečnostního systému v návrhu pod zkratkou EZS neboli Elektronický zabezpečovací systém. Tento prvek, pokud přijme podnět od infrabariéry, že se do budovy dostala neautentizovaná osoba, spouští sirénu pro upozornění osob, které mají za úkol hlídat bezpečnost vstupu do budovy. Box vyhodnocovací jednotky obsahuje ústřednu Lares 48, expandér pro sirény, klávesnici pro ovládání a záložní akumulátor. Záložní akumulátor je použit stejný jako ve dveřních řídících jednotkách.



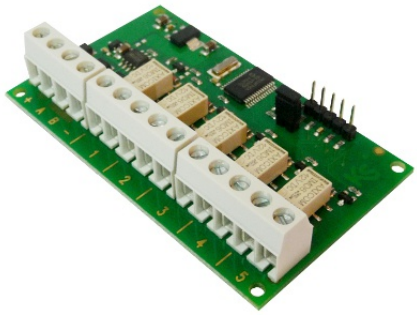
Obrázek 30: Ústředna Lares 48 [43]

Technické parametry [43]:

- Název: Ústředna Lares 48
- Výrobce: Ksenia
- Napájecí napětí: 13,8 V DC
- USB rozhraní: ano
- Počet událostí v deníku min.: 1500
- Max. počet telefonních čísel: 50
- Hmotnost: 1,5 kg

Expandér pro sirény

Expandér je umístěn v boxu společně vyhodnocovací jednotky. Slouží k sepnutí sirén při neoprávněném průchodu neautentizované osoby.



Obrázek 31: Expandér AUXI [43]

Technické parametry [43]:

- Název: Expandér AUXI
- Výrobce: Ksenia
- Napájecí napětí: 10-14V DC
- Počet vstupů na desce: 5

- Teplota provozní: +5 až +40 °C
- Rozměry: 45 x 75 x 20 mm
- Hmotnost: 0,05 kg

Siréna

Siréna je spuštěna, pokud tak vyhodnotí vyhodnocovací jednotka bezpečnostního systému. Ovšem siréna nemusí být jediným varovným signálem. Systém umí odesílat také varovné sms zprávy na mobilní telefon nebo je možné instalovat kameru, která zaznamená průchod neautentizované osoby.

Obrázek 32: Vnitřní výstražné signalizační zařízení SA 913F [43]

Technické parametry [43]:

- Název: Vnitřní výstražné signalizační zařízení SA 913F
- Výrobce: Jablotron
- Napájecí napětí: 10-14 V DC
- Akustický tlak: 110 dB
- Rozměry: 113 x 74 x 46 mm
- Hmotnost: 0,13 kg

Switch

Pro datové spojení komponent je do návrhu integrován switch.

Obrázek 33: Switch DSW-3008G [43]

Technické parametry [43]:

- Název: Switch DSW-3008G
- Výrobce: DINOX
- Přenosová rychlost: 1000 Mbps
- Počet portů: 8
- Rozměry: 33 x 215 x 106 mm
- Hmotnost: 0,6 kg

Software

Pro celkovou funkci návrhu slouží tři důležité programy. První ZKSoftware slouží pro správu osob, jak jejich biometrických dat, tak doplňujících informací. Druhým programem je Net2 Access Control sloužící pro kontrolu přístupu. Tím je myšleno přidělování přístupových práv jednotlivým osobám a ovládání jednotlivých dveří. Oba tyto programy jsou instalovány na počítač, který je v budově a slouží k podobným účelům. Posledním programem je Basis, který spravuje informace pořízené z jednotlivých čidel.

Obrázek 34: Ukázka ZKSoftware [43]

6.2.3 Cenová relace

Cenová relace je sestavena ze všeho potřebného hardwaru pro kompletní funkci systému. Délka kabeláže je odhadnuta, jelikož neznám veškeré průchody ve zdech, které by se daly využít. Cena kabeláže pochází od společnosti GES-ELECTRONICS, a.s [52]. Cenová relace také neobsahuje montáž ani cenu počítačové sestavy, na které běží systémy. Samotná montáž se v navrhovaných prostorách nepředpokládá.

Produkt	Počet ks	Cena bez DPH
Čtečka otisků	3	10 914 Kč
Stolní čtečka otisků	1	3 924 Kč
Dveřní řídící jednotka	3	10 470 Kč
Záložní zdroj	4	399 Kč
Dveřní otvírač	3	990 Kč
Odchodové tlačítko	3	860 Kč
Infrabariéra	3	1 975 Kč
Vyhodnocovací jednotka	1	7 990 Kč
Expandér pro sirény	1	1 290 Kč
Siréna	3	246 Kč
Switch	1	1 450 Kč
UTP	125	6,05 Kč/m
CYH 2X1,0	100	7,44 Kč/m
Cyky 3Jx1,5	15	16,60 Kč/m
Software	3	zdarma
Celkem		94 364,25 Kč

Tabulka 3: Cenová relace ABBAS

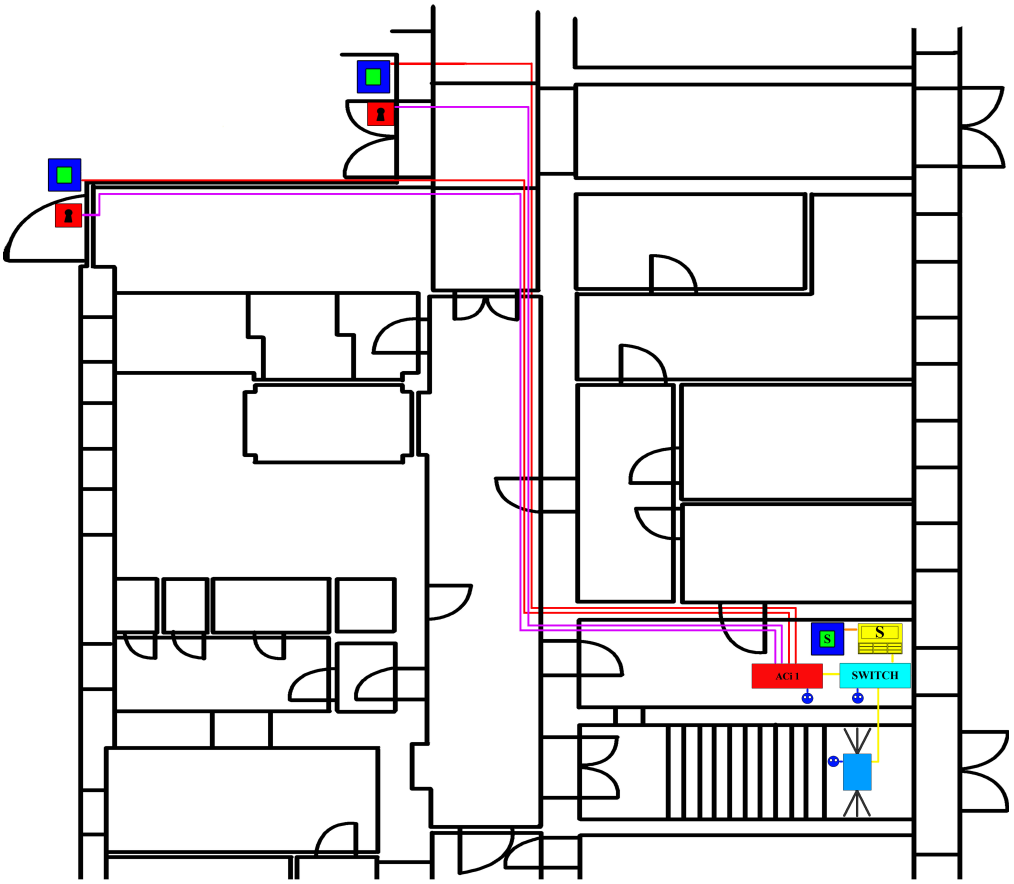
6.3 Řešení s využitím zařízení firmy IReSoft, s.r.o.

6.3.1 Popis firmy

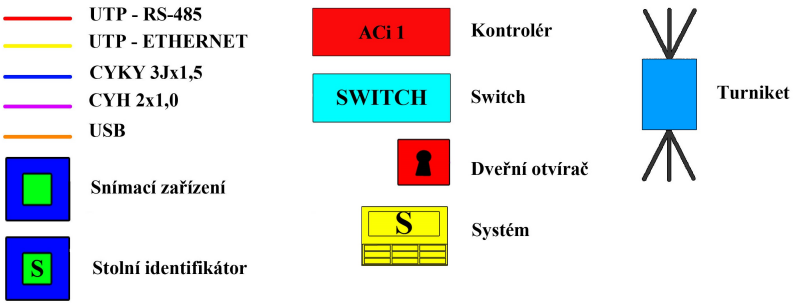
Společnost IReSoft, s.r.o. funguje od roku 2002 na českém trhu. Jedním z produktů této firmy jsou biometrické systémy Alveno, které poskytují již 10 let.

6.3.2 Hardwarové řešení

Jako druhé méně bezpečné řešení je v návrhu použit jeden turniket v hlavním vchodu. Ostatní dva vchody disponují pouze externím čidlem a dveřním otvíračem. Tyto dveře budou po dobu největšího návalu vypnuty, aby nedošlo k vniknutí nepovolené osoby. Dále návrh obsahuje jeden stolní identifikátor, jeden kontrolér pro správu externích čidel a zámků, switch a samozřejmě přístupový systém.



Obrázek 35: Schéma zapojení IReSoft



Obrázek 36: Legenda IReSoft

Turniket

Oboustranný přístupový turniket je umístěn do hlavního vchodu, kde zajistí bezpečný a plynulý průchod při největším návalu před začátkem výuky. Je totiž schopen autentizovat nezávisle na sobě dvě osoby. Toto zařízení není možné zálohovat proti výpadku proudu, je to tudíž méně bezpečná varianta. Při urychleném opouštění budovy, například při požáru, lze turniket vypnout tím se spustí otočné rameno a je možné plynule procházet. Turniket funguje na stejném principu jako ostatní dveře, v návrhu obsahuje externí čidla a kontrolér. Turniket lze umístit na jakékoli místo a zbylý prostor lze doplnit různými zábranami.

Obrázek 37: Turniket ACTi 52 (TS1200 Series) [45]

Technické parametry [44, 45]:

- Název: Turniket ACTi 52 (TS1200 Series)
- Výrobce: ZK Teco
- Senzor: Optický
- Rozlišení: 500 dpi
- Kapacita paměti: 3000 otisků prstů
- Komunikace: TCP/IP

- Napájecí napětí: 230 V AC
- Rozměry + Délka ramene: 600 x 330 x 980 + 500 mm
- Hmotnost: 55 kg
- Krytí: IP 54

Externí čidlo

U vedlejších vchodů jsou v návrhu umístěny pouze externí čidla na otisky prstů. Tato čidla mají za úkol sejmout otisk a poslat jej do kontroléru. Z důvodu snížení ceny návrhu je umístěno čidlo jen z vnější strany dveří.

Obrázek 38: Externí čidlo ZK1200 [45]

Technické parametry [44, 45]:

- Název: Externí čidlo ZK1200
- Výrobce: ZK Teco
- Komunikace: RS 485
- Napájení: 12 V po UTP
- Rozměry: 102 x 50 x 37,3 mm
- Krytí: IP65

Stolní identifikátor

Stejně jako v prvním návrhu, je i v druhém návrhu použit stolní identifikátor po usnadnění registrace.

Obrázek 39: Stolní identifikátor ZK4000 [45]

Technické parametry [44, 45]:

- Název: Stolní identifikátor ZK4000
- Výrobce: ZK Teco
- Komunikace: USB
- Hmotnost: 0,2 Kg
- Rozměry: 49 x 79,8 x 65,5 mm

Kontrolér

Kontrolér je umístěn na bezpečném místě uvnitř budovy. Pokud nejsou potřeba záznamy o jednotlivých dveřích, může být použita levnější varianta kontroléru pro jedny dveře, kdy je použito čidlo, které by mělo být umístěno z vnitřní strany dveří na vnější stranu jiných dveří. Kontrolér má za úkol zpracovat přijatý otisk od externího čidla a povolit či zamítnout přístup do budovy.

Obrázek 40: Kontrolér ACi 1 (inBio-160) [45]

Technické parametry [44, 45]:

- Název: Kontrolér ACi 1 (inBio-160)
- Výrobce: ZKTeco
- Napájecí napětí: 12 V
- Komunikace: RS485, Wiegand, Ethernet
- Kapacita paměti: 3000 otisků prstů
- Teplota provozní: 0 až +55 °C
- Rozměry: 90 x 350 x 300 mm
- Hmotnost: 3,6 kg

Záložní zdroj, dveřní otvírač, kabeláž

Tyto prvky jsou použity z prvního návrhu, jelikož firma Alveno záložní zdroj pro kontrolér ACi 1 (inBio-160), dveřní otvírač ani kabeláž neposkytuje, řešení nechává na zákazníkovi.

Switch

Do návrhu je také potřeba integrovat switch, který je použit opět od firmy ABBAS, ovšem menší a levnější verze.

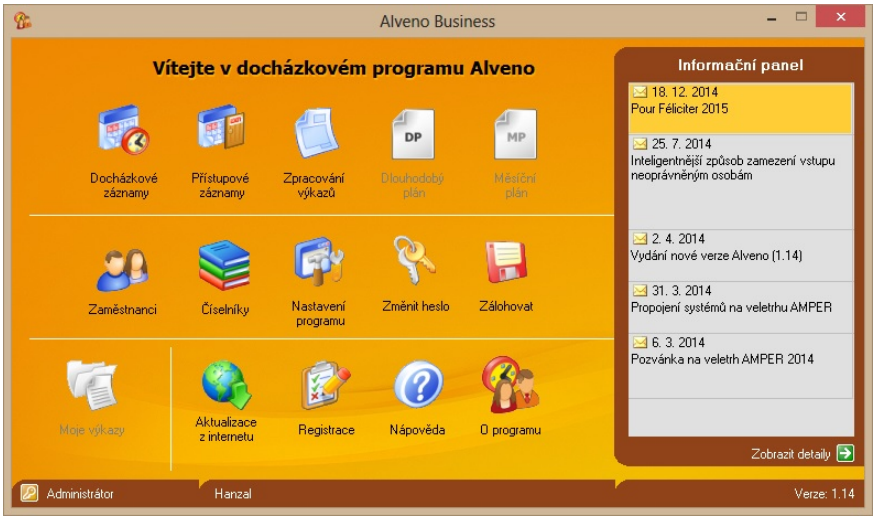
Obrázek 41: Switch DSW-3005 [43]

Technické parametry [43]:

- Název: Switch DSW-3005
- Výrobce: DINOX
- Přenosová rychlost: 1000 Mbps
- Počet portů: 5
- Rozměry: 28 x 117 x 85 mm
- Hmotnost: 0,3 kg

Přístupový systém

Systém je pojmenován Alveno Access a slouží pro správu všech osob a evidenci přístupů. Tento systém je instalován opět na stolní počítač.



Obrázek 42: Systém Alveno [45]

6.3.3 Cenová relace

Cenová relace obsahuje veškerá potřebná zařízení i s předpokládanou délkou kabeláže. Cena kabeláže pochází opět od společnosti GES-ELECTRONICS, a.s [52].

Produkt	Počet ks	Cena bez DPH
Turniket	1	104 990Kč
Externí čidlo	2	4 500 Kč
Stolní identifikátor otisků	1	5 000 Kč
Kontrolér	3	6 000Kč
Přístupový systém	1	4 000 Kč
Záložní zdroj	4	399 Kč
Dveřní otvírač	3	990 Kč
Switch	1	1 050 Kč
UTP	45	6,05 Kč/m
CYH 2X1,0	40	7,44 Kč/m
Cyky 3Jx1,5	10	16,60 Kč/m
Celkem		147 341,85 Kč

Tabulka 4: Cenová relace IReSoft

7 Testy

7.1 Testování zařízení

Následující kapitola se věnuje testování zapůjčených zařízení od společností IReSoft a Z-WARE. Zaměřuje se především na reálnou chybovost těchto zařízení. Testováno bylo 10 osob ve věku od 10 do 70 let. Každá osoba byla seznámena s jednotlivými zařízeními a s jejich funkcí. Následně bylo všech 10 osob poučeno o správné prezentaci svých biometrických dat snímači pro snížení odmítnutí z důvodu špatného přiložení prstu na plochu snímače.

Před samotnou registrací bylo provedeno každou osobou 15 pokusů o neoprávněnou autentizaci pro získání procentuální hodnoty nesprávných přijetí FAR.

V rámci registrace osob bylo původním záměrem do systému uložit všech 10 možných otisků prstů každé osoby. Ani jedna osoba netrpěla žádným hendikepem v oblasti rukou, který by bránil snímání otisku. I přesto se nepodařilo u jedné osoby registrovat 3 otisky prstů pomocí zařízení DSi200 a jednoho prstu u zařízení T5. Při registraci bylo dbáno na co největší kvalitu registračního vzorku, pokud neodpovídal dostatečné kvalitě vyžadující systémem byla registrace opakována. Zaznamenáván byl i počet opakování registrace jednotlivých prstů.

Dále bylo testováno procento nesprávných odmítnutí FRR. Autentizace byla prováděna po registraci všech otisků osoby. Osoby měly možnost nahodile používat kterékoli prsty během 15 pokusů o autentizaci. Testování bylo prováděno při nastavení jedné prahové hodnoty. Obě testovaná zařízení nenabízejí možnost změny prahové hodnoty.

7.1.1 Zařízení docházková čtečka DSi 200

Toto zařízení bylo zapůjčeno firmou IReSoft. Jedná se o zařízení určené pro menší firmy do 50 zaměstnanců, využívající senzor s rozlišením 500 dpi. Společnost u tohoto zařízení neuvádí procentuální hodnotu FAR a FRR. [45].

Obrázek 43: Docházková čtečka DSi 200 [45]

Prováděno bylo 150 autentizačních pokusů o nesprávné přijetí. Nesprávně nebyl přijat ani jeden otisk.

$$FAR = \frac{Počet\ nesprávných\ přijetí}{Počet\ všech\ autentizačních\ pokusů} * 100 = \frac{0}{150} * 100 = 0[\%]$$

Prováděno bylo 150 autentizačních pokusů o nesprávné odmítnutí po schválené registraci. Nesprávně bylo odmítnuto 41 pokusů o autentizaci.

$$FRR = \frac{Počet\ nesprávných\ odmítnutí}{Počet\ všech\ autentizačních\ pokusů} * 100 = \frac{41}{150} * 100 = 27,3[\%]$$

7.1.2 Zařízení přístupová čtečka ITouch T5 Fingerprint

Toto zařízení bylo zapůjčeno firmou Z-WARE. Jedná se o zařízení určené až pro 512 zaměstnanců, využívající senzor s rozlišením 500 dpi. Společnost u tohoto zařízení uvádí procentuální hodnotu FAR 0.00001% a FRR 0.001% [53].

Obrázek 44: Přístupová čtečka ITouch T5 Fingerprint [49]

Prováděno bylo 150 autentizačních pokusů o nesprávné přijetí. Nesprávně nebyl přijat ani jeden otisk.

$$FAR = \frac{Počet\ nesprávných\ přijetí}{Počet\ všech\ autentizačních\ pokusů} * 100 \frac{0}{150} * 100 = 0[\%]$$

Prováděno bylo 150 autentizačních pokusů o nesprávné odmítnutí po schválené registraci. Nesprávně bylo odmítnuto 83 pokusů o autentizaci.

$$FRR = \frac{Počet\ nesprávných\ odmítnutí}{Počet\ všech\ autentizačních\ pokusů} * 100 \frac{83}{150} * 100 = 55,3[\%]$$

7.2 Pokus o neoprávněný vstup

Poslední kapitolou praktické části je otestování bezpečnosti biometrických snímačů. Praktický test byl stejně jako v předchozí kapitole prováděn na docházkové čtečce DSi 200 a přístupové čtečce ITouch T5 Fingerprint. Dostupné biometrické snímače byly testovány proti padělanému otisku prstu. Test se zakládá na předložení falešného biometrického otisku snímači.

Existují dvě metody, jak oklamat biometrické systémy:

První, poněkud nákladnější, ovšem při skutečném pokusu o překonání systému bez prozrazení osoby pokoušející se o toto překonání, je metoda založená na forenzním vyšetřování. Otisk je zviditelněn pomocí zvýrazňujícího jemného prášku. Poté je pořízena fotografie otisku, která je vytištěna na průhlednou fólii. Tato fólie je přiložena fotocitlivé desce a prosvícena a následně vyvolána. Vytvořený předmět slouží jako forma pro odlitek.

Druhá metoda se zakládá na výzkumu japonského vědce Tsumotu Matsumota z Jokohamské univerzity, který v roce 2002 dokázal snadnost překonání biometrických zařízení. Tato metoda se zakládá na vytvoření formy z plastické hmoty rozehřáté za pomoci tepla, do které je vtlačen prst, a do takto vzniklé formy je nalita tekutá želatina, která po zatuhnutí vytvoří umělý otisk prstu [50].

Od té doby šly biometrické technologie prudce kupředu, především byly instalovány mnohé kontroly živosti, které mají těmto pokusům o neoprávněný vstup zamezit. Proto opakuji tento pokus, zda je dnes stále možnost takto překonat biometrický systém.

Obrázek 45: Postup tvorby želatinového prstu [50]

Pro zhotovení formy bylo použito lepidlo z tavné pistole, do kterého byl před vychladnutím vtlačen prst, který již byl registrován do systému. Po vychladnutí tvořilo lepidlo kvalitní formu pro zhotovení želatinového prstu. Pro želatinový prst byla použita potravinářská želatina, která byla připravena podle návodu. Tato ještě rozehřátá želatina byla vlita to studené formy z lepidla a byla uložena do lednice na pár minut. Po vychladnutí tvořila želatina kvalitní odlitek, který byl použit na neoprávněný přistup do systému.

Obě zapůjčená zařízení povolila takto zhotovenému odlitku přístup. Přelstít zařízení nebylo až tak jednoduché, bylo potřeba želatinový prst přiložit nejpřesněji na stejné místo, jako byl přiložen skutečný prst. Manipulaci s želatinovým prstem stěžovala také teplota, kdy se vlivem teploty želatinový prst roztékal a papilární linie tak zanikaly.

Firmy, které testovaná zařízení zapůjčily, nebyly s tímto rizikem obeznámeny. Firma IReSoft dokonce uváděla, že zařízení disponuje kontrolou živosti.

8 Závěr

Biometrie je odvětví vědy, které má velké předpoklady k dalšímu růstu. Biometrické autentizační systémy mají velké množství uplatnění a je jisté, že mnohé způsoby ještě nebyly objeveny. Vždy je ovšem důležité, aby byla přesně stanovena pravidla užití biometrických systémů a nedocházelo k jejich zneužití.

Cílem této práce bylo v teoretické části vysvětlit obecnou terminologii potřebnou k pochopení biometrické autentizace a práci s biometrickými systémy. V této části práce byly objasněny nejdůležitější termíny a to především samotný pojem biometrie, ale také autentizace a její princip. Dále byly vysvětleny termíny jako identifikace a verifikace a mnohé další. Nebylo zapomenuto ani na stručnou historii biometrické autentizace. Byla objasněna kritéria kladená na biometrické autentizační systémy a bylo podrobně vysvětleno měření výkonnosti biometrických systémů. Poskytovatelé uvádějí nejnižší možnou chybovost při ideálních podmínkách, která ovšem neodpovídá skutečnosti, proto je v praktické části proveden test skutečné chybovosti na zapůjčených zařízeních. Tento test výkonnosti biometrického systému na zapůjčených zařízeních byl proveden na základě procentuální chybovosti FAR a FRR za pomoci několika osob.

Dalším nejrozsáhlejším bodem této práce bylo vytvoření podrobného popisu existujících variant biometrických autentizačních systémů a jejich rozdělení do jednotlivých tříd. V této části byly popsány metody, které lze najít v dostupné literatuře a byly vysvětleny výhody a nevýhody těchto metod pro využití v praxi. Nejsou zmíněny některé nekonvenční metody, které nejsou zdokumentovány nebo jsou ve stádiu, kdy by jejich využití bylo příliš nákladné nebo pro autentizaci osob nevhodné, jako například otisk jazyka. Toto téma je velmi obsáhlé, jelikož každá metoda využívá různé funkce, které závisí na tvůrcích té určité metody. Tato práce je především zaměřená na systémy, které lze získat na českém trhu.

Následně byla provedena analýza možných dostupných řešení biometrických systémů použitelných pro autentizaci žáků na základní škole a výběr metody aplikovatelné v praktickém návrhu autentizace osob na základní škole.

Pro tento účel byla zvolena pouze jedna metoda a to metoda otisku prstu. Ostatní metody nebyly vhodné či dostupné.

V praktické části bylo cílem této práce vytvořit samotný návrh biometrické autentizace osob na základní škole. Byl kladen důraz na nejvyšší bezpečnost a nejnižší cenu celkového systému. Pro ukázku byly zvoleny dva návrhy od dvou různých poskytovatelů. Jako poslední bod této práce byl proveden pokus o překonání zabezpečení systému proti použití padělaného otisku na zapůjčených zařízeních.

Veškeré stanovené cíle práce byly splněny.

Seznam doporučené literatury a zdrojů

[1] RAK, Roman. Biometrie a identita člověka ve forenzních a komerčních aplikacích. 1. vyd. Praha: Grada, 2008. ISBN 978-80-247-2365-5.

[2] ŠČUREK, PH.D., Mgr. Ing. Radomír. Biometrické metody identifikace osob v bezpečnostní praxi: Studijní text. In: [online]. 2008 [cit. 2015-02-05]. Dostupné z: http://www.biometrickypodpis.cz/PDF/biometricke_metody.pdf

[3] SULOVSKÁ, Kateřina. Biometrické systémy zaměřené na rozpoznávání tváře, jejich spolehlivost a základní metody pro jejich tvorbu [online]. 2011 [cit. 2015-06-21]. Dostupné z: http://www.posterus.sk/?p=11511

[4] Otisky prstů..stručná historie [online]. 2009 [cit. 2015-06-21]. Dostupné z: http://zadny.blog.cz/0907/otisky-prstu-strucna-historie

[5] PATO, Joseph N a Lynette I MILLETT. Biometric recognition: challenges and opportunities. Washington, D.C.: National Academies Press, 2010, xv, 165 p. ISBN 03-091-4207-5.

[6] ROUSE, Margaret. What is authentication, authorization, and accounting (AAA)? - Definition from WhatIs.com [online]. 2010 [cit. 2015-06-22]. Dostupné z: http://searchsecurity.techtarget.com/definition/authentication-authorization-and-accounting

[7] Biometrie. [online]. © 2011–2015 [cit. 2015-02-05]. Dostupné z: http://www.biometricke-ctecky.cz

[8] DRAHANSKÝ, Martin a Filip ORSÁG. Biometrie. 1. vyd. [Brno: M. Drahanský], 2011. ISBN 978-80-254-8979-6

[9] Biometric Match [online]. [cit. 2015-06-22]. Dostupné z: http://www.technovelgy.com/ct/Technology-Article.asp?ArtNum=82

[10] Biometric Match Threshold [online]. [cit. 2015-06-22]. Dostupné z: http://www.technovelgy.com/ct/Technology-Article.asp?ArtNum=98

[11] BITTO, Ondřej. Šifrování a biometrika aneb tajemné bity a dotyky. Vyd. 1. Kralice na Hané: Computer Media, 2005, 168 s. ISBN 80-866-8648-5.

[12] JAIN, Anil K, Ruud BOLLE a Sharath PANKANTI. Biometrics: personal identification in networked society. Boston: Kluwer, 1999, x, 411 p. ISBN 07-923-8345-1.

[13] Bolle, R. M. et al. Guide to Biometrics. New York: Springer-Verlag, 2014. ISBN 0-387-40059-3.

[14] MARTIN, A., T. KAMM, M. ORDOWSKI, M PRZYBOCKI a G. DODDINGTON. The DET curve in assessment of detection task performance [online]. 1997 [cit. 2015-06-22]. Dostupné z: http://www.itl.nist.gov/iad/mig/publications/storage_paper/det.pdf

[15] SULOVSKÁ, Kateřina. Sledování vlivu teploty na termogram lidské tváře - část 1 [online]. 2012 [cit. 2015-06-22]. Dostupné z: http://www.posterus.sk/?p=13335

[16] LED - základní pojmy [online]. [cit. 2015-06-22]. Dostupné z: http://www.ledtip.cz/cz-clanky-6.html

[17] PUŽMANOVÁ, Rita. Biometrické systémy v praxi [online]. 2004 [cit. 2015-06-22]. Dostupné z: http://www.systemonline.cz/clanky/biometricke-systemy-v-praxi.htm

[18] Forensic Odontology [online]. [cit. 2015-06-22]. Dostupné z: https://theiai.org/disciplines/odontology/index.php

[19] Digitální zaznamenávání obrazu, zachytávání videa [online]. [cit. 2015-06-22]. Dostupné z: http://www.gjszlin.cz/ivt/esf/premiere/zaznam-zabery-esf.php

[20] BITTO, Ondřej. Naše kompletní biometrické identity – Živě.cz [online]. 2007 [cit. 2015-06-22]. Dostupné z: http://www.zive.cz/clanky/nase-kompletni-biometricke-identity/sc-3-a-137647/default.aspx

[21] DRAHANSKÝ, Martin. Přehled biometrických systémů a testování jejich spolehlivosti [online]. 2007 [cit. 2015-06-22]. Dostupné z: http://data.security-portal.cz/clanky/113/odborne_prednasky/Prezentace.pdf

[22] WOODWARD, John D., Nicholas M. ORLANS a Peter T. HIGGINS. Biometrics identity assurance in the information age. Vyd. 1. New York: McGraw-Hill, 2003, 432 s. ISBN 00-722-2227-1.

[23] WAYMAN, James L., Anil K. JAIN, Davide MALTONI a Dario MAIO. Biometric systems: technology, design and performance. London: Springer-Verlag, 2005, xiv, 370 s. ISBN 18-523-3596-3.

[24] Biometrie otisku prstu [online]. 2015 [cit. 2015-06-22]. Dostupné z: http://www.biometricke-ctecky.cz/biometriky/otisk-prstu

[25] COUFAL, Tomáš. Co je to FingerChip® | HW.cz [online]. 2007 [cit. 2015-06-22]. Dostupné z: http://www.hw.cz/teorie-a-praxe/co-je-to-fingerchipr.html

[26] Biometrics: fingerprint sensing techniques [online]. 2015 [cit. 2015-06-22]. Dostupné z: http://fingerchip.pagesperso-orange.fr/biometrics/types/fingerprint_sensors_physics.htm

[27] Biometrics: fingerprint sensing techniques [online]. 2015 [cit. 2015-06-22]. Dostupné z: http://fingerchip.pagesperso-orange.fr/biometrics/types/fingerprint_sensors_physics.htm

[28] Otisk prstu | COMFIS s.r.o. [online]. 2014 [cit. 2015-06-22]. Dostupné z: http://www.comfis.cz/technologie/biometrika

[29] ĎÁSEK, Milan. Biometrika [online]. 2003 [cit. 2015-06-22]. Dostupné z: https://akela.mendelu.cz/~lidak/bif/dasek.html

[30] JAIN, Anil a Sharath PANKANTI. Automated Fingerprint Identification and Imaging Systems [online]. [cit. 2015-06-22]. Dostupné z: `http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.21.380&rep=rep1&type=pdf`

[31] Biometrie krevního řečiště [online]. 2015 [cit. 2015-06-22]. Dostupné z: http://www.biometricke-ctecky.cz/biometriky/krevni-reciste

[32] Tajemný mozek a jeho frekvence [online]. [cit. 2015-06-23]. Dostupné z: http://www.propator.websnadno.cz/VSE–vibrace.html

[33] Bromba GmbH - Press Release 07 [online]. 2006 [cit. 2015-06-22]. Dostupné z: http://www.bromba.com/press07e.htm

[34] BENEŠ, R. Autentizační metody založené na biometrických informacích [online]. 2010 [cit. 2015-06-22]. Dostupné z: http://access.feld.cvut.cz/view.php?cisloclanku=2010110002

[35] ODOM, J. Vernon, Colin BARBER, Mitchell BRIGELL, Michael F. MARMOR, Alma Patrizia TORMENE, Graham E. HOLDER, VAEGAN a Michael BACH. Visual evoked potentials standard (2004)∗ [online]. 2004 [cit. 2015-06-22]. Dostupné z: http://www.fil.ion.ucl.ac.uk/∼jdaunize/docs/vep-standard-2004.pdf

[36] MALINKA, K. STUDENT EEICT 2010: proceedings of the 16th conference. Vyd. 1. Brno: Brno university of technology, 2010, 260 s. ISBN 978-80-214-4080-7.

[37] ILONEN, Jarmo. Keystroke Dynamics [online]. [cit. 2015-06-22]. Dostupné z: http://www.it.lut.fi/kurssit/03-04/010970000/seminars/Ilonen.pdf

[38] ČERMÁK, Miroslav. Autentizace: biometrické metody - CleverAndSmart [online]. 2009, 2013 [cit. 2015-06-22]. Dostupné z: http://www.cleverandsmart.cz/autentizace-biometricke-metody

[39] TROUSIL, Pavel. PalmSecure – identifikace osob pomocí obrazu krevního řečiště | Chip.cz - recenze a testy [online]. 2014 [cit. 2015-06-22]. Dostupné z: http://www.chip.cz/novinky/palmsecure-identifikace-osob-pomoci-obrazu-krevniho-reciste

[40] ČSN EN 50133-1. Poplachové systémy - Systémy kontroly vstupů pro použití v bezpečnostních aplikacích : Část 1: Systémové požadavky. Praha : Český normalizační institut, 2001.

[41] RYAN, Mark Dermot. Biometric authenticatio [online]. 2008 [cit. 2015-06-22]. Dostupné z: http://www.cs.bham.ac.uk/~mdr/teaching/modules/security/lectures/biometric.html

[42] MŠMT ČR [online]. [cit. 2015-06-23]. Dostupné z: http://www.msmt.cz/

[43] ABBAS, a.s. [online]. 2015 [cit. 2015-06-22]. Dostupné z: http://katalog.abbas.cz

[44] ZKTeco [online]. 2014 [cit. 2015-06-22]. Dostupné z: http://www.zkteco.com

[45] Docházkový a přístupový systém - Alveno.cz [online]. 2015 [cit. 2015-06-22]. Dostupné z: https://www.alveno.cz

[46] ZKSoftware ZK6000 Fingerprint Reader [online]. 2015 [cit. 2015-06-22]. Dostupné z: http://www.neurotechnology.com/fingerprint-scanner-zksoftware-zk6000.html

[47] Co znamená jednotka DPI a kde se s ní můžeme setkat? - Grafika.cz - vše o počítačové grafice [online]. 2002 [cit. 2015-06-22]. Dostupné z: http://www.grafika.cz/rubriky/photoshop/co-znamena-jednotka-dpi-a-kde-se-s-ni-muzeme-setkat–130235cz

[48] SCHLENKER, Anna a Milan ŠÁREK. Biometrické metody pro aplikace v biomedicíně [online]. 2011 [cit. 2015-06-23]. Dostupné z: http://www.ejbi.org/img/ejbi/2011/1/Schlenker_cs.pdf

[49] Z-WARE – identifikační systémy docházkové, stravovací, přístupové. [online]. [cit. 2014-03-30]. Dostupné z: http://www.z-ware.cz

[50] HOLČÍK, Tomáš. Čtečku prstů překoná gumový medvídek – Živě.cz [online]. 2002 [cit. 2015-06-23]. Dostupné z: http://www.zive.cz/clanky/ctecku-prstu-prekona-gumovy-medvidek/sc-3-a-106728

[51] Stanovisko č. 3/2009 - Biometrická identifikace nebo autentizace zaměstnanců. In: [online]. [cit. 2015-01-20]. Dostupné z: https://www.uoou.cz/VismoOnline_ActionScripts/File.ashx?id_org=200144&id_dokumenty=9709.

[52] GES-ELECTRONICS – Internetový obchod s elektronickými součástkami [online]. 2015 [cit. 2015-06-24]. Dostupné z: http://www.ges.cz/cz

[53] Čtečky čipových karet, zabezpečovací a šifrovací software | RAS, spol. s r.o. [online]. 2015 [cit. 2015-06-24]. Dostupné z: http://www.rassro.cz

Seznam obrázků

Seznam tabulek

Přílohy

1. CD - na přiloženém CD se nachází plné znění bakalářské práce pod názvem Hanzal_BP.pdf.