ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

FAKULTA DOPRAVNÍ

Miroslav Štěrba

Zavedení biometrické autentizace do prostředí ČVUT

Bakalářská práce

2018

ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE
Fakulta dopravní
děkan
Konviktská 20, 110 00 Praha 1

K614..... Ústav aplikované informatiky v dopravě

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení studenta (včetně titulů):

Miroslav Štěrba

Kód studijního programu a studijní obor studenta:

B 3710 – LOG – Logistika a řízení dopravních procesů

Název tématu (česky): **Zavedení biometrické autentizace do prostředí ČVUT**

Název tématu (anglicky): The introduction of biometric authentication to CTU

Zásady pro vypracování

Při zpracování bakalářské práce se řiďte osnovou uvedenou v následujících bodech:

- Analýza současného stavu (ID karty ČVUT, prostory ČVUT a jejich zabezpečení)
- Biometrické identifikace (popis metody, vytipování vhodných metod)
- Architektury systému
- Multikriteriální optimalizace (analýza vybraných metod, návrh řešení v rámci ČVUT)

ČVUT FD

Rozsah grafických prací: dle vedoucího bakalářské práce

Rozsah průvodní zprávy: minimálně 35 stran textu (včetně obrázků, grafů a tabulek, které jsou součástí průvodní zprávy)

Seznam odborné literatury:
1. Ščurek R.: Biometrické metody identifikace osob v bezpečnostní praxi, 2008
2. Ščurek R.: Biometrické technologie - technické prostředky bezpečnostních služeb, 2015
3. Rak R., Matyáš V., Říha Z.: Biometrie a identita člověka ve forenzních a komerčních aplikacích, 2008

Vedoucí bakalářské práce: **Ing. Jana Kaliková, Ph.D.**

Datum zadání bakalářské práce: **27. října 2017**
(datum prvního zadání této práce, které musí být nejpozději 10 měsíců před datem prvního předpokládaného odevzdání této práce vyplývajícího ze standardní doby studia)

Datum odevzdání bakalářské práce: **27. srpna 2018**
a) datum prvního předpokládaného odevzdání práce vyplývající ze standardní doby studia a z doporučeného časového plánu studia
b) v případě odkladu odevzdání práce následující datum odevzdání práce vyplývající z doporučeného časového plánu studia

ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE Fakulta dopravní -3-
L. S.

doc. Ing. Vít Fábera, Ph.D.
vedoucí
Ústavu aplikované informatiky v dopravě

prof. Dr. Ing. Miroslav Svítek, dr. h. c.
děkan fakulty

Potvrzuji převzetí zadání bakalářské práce.

Miroslav Štěrba
jméno a podpis studenta

V Praze dne ..... 27. října 2017

Poděkování

Chtěl bych poděkovat Ing. Janě Kalikové, Ph.D. za její rady a odborné vedení mé bakalářské práce. Dále děkuji vedoucím laboratoří a vědeckých pracovišť Fakulty dopravní ČVUT za poskytnutí informací a v neposlední řadě děkuji své rodině a blízkým za jejich trpělivost, morální a materiální podporu a také shovívavost při studiu.

Prohlášení

Předkládám tímto k posouzení a obhajobě bakalářskou práci, zpracovanou na závěr studia na ČVUT v Praze Fakultě dopravní.

Prohlašuji, že jsem předloženou práci vypracoval samostatně a že jsem uvedl veškeré použité informační zdroje v souladu s Metodickým pokynem o etické přípravě vysokoškolských závěrečných prací.

Nemám závažný důvod proti užití tohoto školního díla ve smyslu § 60 Zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon).

V Praze dne 26. července 2018 ……

Miroslav Štěrba

Název práce:	**Zavedení biometrické autentizace do prostředí ČVUT**
Autor:	Miroslav Štěrba
Obor:	Logistika a řízení dopravních procesů
Druh práce:	Bakalářská práce
Vedoucí práce:	Ing. Jana Kaliková, Ph.D.

ABSTRAKT

Bakalářská práce na téma biometrický applet pro ID karty ČVUT je zaměřena na vytipování a výběr vhodné biometrické metody, která zabezpečí přístup do prostor vyžadujících vysoký stupeň bezpečnosti přístupu na celém ČVUT. Vycházím z několika kritérií, na základě kterých vyberu biometrickou metodu. Jsou to rychlost verifikace, spolehlivost, náklady, uživatelská přívětivost a stálost v čase. V první části práce je zmapování celého Českého vysokého učení technického a poté popis vytipovaných biometrických metod pro moji práci, se kterými dále pracuji v praktické části, kde na základě multikriteriální optimalizace rozhoduji, kterou biometrickou metodu zvolím. Přínosem této práce bude zvýšení bezpečnosti majetku, přičemž pilotní projekt je navržen pro Fakultu dopravní.

Klíčová slova:

Biometrie, biometrický applet, čidlo, otisk prstů, duhovka, geometrie tváře 3D, geometrie ruky, struktura žil na zápěstí

ABSTRACT

Bachelor thesis on topic of biometric applet for ID card CTU is focused on the identification and selection of suitable biometric method that ensures access to areas requiring a high degree of security of access throughout CTU. I have several criteria, on the basis of which I will choose biometric method. They are the speed of verification, reliability, cost, user friendliness and permanence in time. In the first part of the thesis is the mapping of the whole CTU and then a description of the selected biometric methods for my work, with which I continue to work in the practical part where I decide on the basis of the multi-criteria optimization which biometric method to choose. The benefit of this work will be the increased security of the property, while the pilot project is for the Faculty of Transport.

Keywords:

Biometrics, biometric applet, sensor, fingerprint, iris, face geometry 3D, hand geometry, wrist structure

Obsah

Seznam použitých zkratek

ČVUT	České vysoké učení technické
FD	Fakulta dopravní
FRR	False Rejection Rate – pravděpodobnost chybného odmítnutí autorizované osoby biometrickým zařízením
FAR	False Acceptance Rate – pravděpodobnost chybného přijetí neoprávněné osoby biometrickým zařízením
EER	Equal Error Rate – bod, ve kterém se protínají křivky FRR a FAR
ISIC	International Student Identity Card
BA	Biometrický applet
MO	Multikriteriální optimalizace
RFID	Radio Frequency IDentification
PIN	Personal Identification Number
VIC	Výpočetní a Informační centrum

1. Úvod

Ke zpracování bakalářské práce na zavedení biometrické metody celoplošně na ČVUT mě vedl požadavek na zvýšení bezpečnosti vstupu do vyhrazených prostor, a hledal jsem nejvhodnější biometrický applet.

Cílem práce bylo pomocí metody multikriteriální optimalizace zvolit nejvhodnější biometrickou metodu, která by se použila a nahrála na ID kartu ČVUT pro zajištění bezpečnosti. Zvolil jsem si k tomu 5 biometrických metod a pomocí zmíněné metody multikriteriální optimalizace zjistím, která by se dala pro Fakultu dopravní, pilotní projekt mé práce, a celé ČVUT použít.

V mé bakalářské práci se budu zabývat tím, jak zvýšit bezpečnost při ověřování identity všech akademických pracovníků a studentů, tedy všech členů akademické obce na Českém vysokém učení technickém, přičemž pilotní projekt bude pro fakultu, kterou studuji, Fakultu dopravní v Praze. K dosažení kladného výsledku bude sloužit vytipovaná biometrická metoda, kterou budu posuzovat pomocí multikriteriální optimalizace (kritéria - rychlost verifikace, spolehlivost, náklady, uživatelská přívětivost a stálost v čase). Výsledná biometrická metoda bude zavedená na vstupech do laboratoří, vědeckých pracovišť, serveroven a tiskového centra, zbytek bude zabezpečený pomocí čidla. Biometrický applet bude nahrán na dosavadní kartu ČVUT/ISIC kartu a zvýší zabezpečení majetku a drahé techniky, což je také jeden z cílů této práce, o který mi jde. Současná ID karta má digitální certifikát s PINem a po vytipování vhodné metody na ni bude nahrán i biometrický applet.

V dnešní době je zabezpečení na kartu nedostačující, protože jsou pořád lepší a lepší technologie. Tato doba vyžaduje maximální zabezpečení majetku a zejména lidí, v tomto případě lidí z akademické obce ČVUT. Nyní máme vstupy zabezpečeny pomocí čipových ID karet, kde je jméno, číslo karty, a osobní číslo při prokazování se. Ty mohou být snadno zneužity, protože oproti bankovním kartám, které jsou chráněny PIN kódem, ID karty ČVUT nebo ISIC nepoužívají k ověření žádný kód. Stačí kartu pouze přiložit k čtecímu zařízení. To znamená, že každý, kdo si vypůjčil nebo ukradl kartu, má přístup do většiny chráněných místností (PC učebny, laboratoře, posluchárny…). Je tedy potřeba, aby minimálně v některých prostorách dosahovalo zabezpečení vyšší úrovně, a já se budu v této práci zabývat tím, co by to přinášelo, kdyby se na ID kartu ČVUT zavedl biometrický applet, což je v dnešní době jedno z nejrozumnějších řešení.

2. Zmapování ČVUT

České vysoké učení technické v Praze (ČVUT) patří k největším a nejstarším technickým vysokým školám v Evropě. V roce 2014 bylo vyhlášeno nejlepší technickou univerzitou v České republice. V současné době má ČVUT osm fakult a studuje na něm přes 21 000 studentů.

ČVUT, rok 2017:

Počet lidí ke dni *5. 4. 2017*:	**27 331** (dle ID karet)
Počet budov:	**139** (některé budovy ČVUT nevlastní)
Každá fakulta:	± **3 vstupy**
Počet učeben:	**430**
Počet čidel:	**922***

*ke dni 24. 4. 2018 je v celoškolním přístupovém systému K4 (připojený k serveru VIC) 922 přístupových bodů. Jeden bod představuje buď příchozí čtečku karet, nebo příchozí a odchozí čtečku karet

Fakulta dopravní, rok 2017:

Studenti:	**1903**
Zaměstnanci:	**413**
Počet lidí:	**2316**
Počet budov:	**6**
Počet čidel:	**97**
Počet čidel BIO	**0**

.

Tabulka 1 Počty studentů a zaměstnanců v akreditovaných studijních programech (2018) [zpracováno autorem]

	Bakalářské studium	Navazující magisterské studium	Doktorské studium	Celkem	Počet zaměstnanců
Fakulta stavební (FSv)	**3420**	**1480**	**530**	**5430**	**450**
Fakulta strojní (FS)	**1580**	**633**	**289**	**2502**	**550**
Fakulta elektrotechnická (FEL)	**1641**	**871**	**374**	**2886**	**859**
Fakulta jaderná a fyzikálně inženýrská (FJFI)	**889**	**294**	**308**	**1491**	**714**
Fakulta architektury (FA)	**868**	**614**	**152**	**1634**	**199**
Fakulta dopravní (FD)	**1283**	**471**	**149**	**1903**	**413**
Fakulta biomedicínského inženýrství (FBMI)	**1135**	**424**	**102**	**1661**	**248**
Fakulta informačních technologií (FIT)	**1700**	**490**	**65**	**2255**	**210**
Kloknerův ústav (KÚ), Masarykův ústav vyšších studií (MÚVS)	**934**	**307**	**44**	**1285**	**157**
	13450	**5584**	**2013**	**21047**	**3800**

3. Biometrie a základní pojmy

Biometrie (biometric) je vědní obor zabývající se studií a zkoumáním živých organismů (bio-), především člověka, a měřením (-metric) jeho biologických (anatomických a fyziologických) vlastností a také jeho chováním, tzn. behaviorálních charakteristik. Pojem biometrika je odvozený z řeckých slov "bios" a "metron". První znamená "život", druhé pak "měřit, měření". Kdybychom se chtěli držet doslovného překladu, zněla by biometrie jako "měření živého". V přeneseném významu jde ovšem o měření a rozpoznávání určitých charakteristik člověka. Biometrika se věnuje studiu metod vedoucích k rozpoznávání člověka na základě jeho unikátních proporcí nebo vlastností. V zahraniční je pojem biometric přímo vykládán jako proces automatizované metody rozpoznávání jedince založený na 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). Rozpoznávání lidí pomocí biologických charakteristik je metoda využívaná historicky, lidé se rozpoznávají pomocí vzhledu tváře nebo jsou známy otisky dlaní v jeskyních jako jakýsi podpis autora (některé z nich jsou až 30 000 let staré). S rozvojem počítačových technologií na konci 60. let se začalo i biometrické rozpoznávání člověka stávat automatizovaným. [8, 9]

Termíny biometrická identifikace, biometrie, biometriky apod., spojované především s výpočetní a automatizační technikou, jsou okruhu úzce zaměřených specialistů známé již přes třicet let. Laická veřejnost je zná spíše z oblasti sci-fi literatury a filmů, jako jsou Hvězdné války, Star Trek, Minority Report nebo špionážních snímků typu Mission: Impossible, State Enemy, apod. V očích nezasvěcené veřejnosti vzniká proto dojem, že se jedná o „High-tech“ produkty, vzniklé pouze v představě tvůrců komerčně úspěšných žánrů.

Biometrická identifikace popřípadě verifikace je využití jedinečných, měřitelných, fyzikálních nebo fyziologických znaků (tzv. markantů) nebo projevů člověka k jednoznačnému zjištění (identifikace) nebo ověření (verifikace) jeho identity.

Základní pojmy

Biometrie – skládá se z řeckých slov “bios“, živý, a “metria“, měření. Je to tedy vědní obor zkoumající biologické organismy a jejich fyziologické a anatomické parametry a behaviorální vlastnosti.

Biometrika – věnuje se studiu metod sloužících k rozpoznávání člověka na základě jeho biologických parametrů nebo behaviorálních vlastností.

Autentizace – proces, při kterém se ověřuje totožnost uživatele. Výsledkem procesu je pak povolení nebo zamítnutí přístupu do systému.
Identifikace – při tomto procesu systém sejme biometrická data neznámého uživatele, která následně porovná s celou databází. Jedná se tedy o princip „one-to-many".
Verifikace - při tomto procesu uživatel nejdříve zadá systému svoji totožnost (např.:
pomocí karty nebo hesla), následně systém sejme biometrická data, která porovná s dříve uloženým etalonem. Jedná se tedy o princip „one-to-one". [2, 24]

3.1 Metody autentizace

Existují 3 druhy autentizace: použití hesla, předmětu nebo biometrického prvku.

Autentizace heslem – „něco vím", je nejvíce využívanou možností pro přístup osob do systému. Je to dáno především jednoduchou realizací pomocí softwaru a z toho vyplývající nízkou cenou. Při volbě nebo přidělení hesla se musí pro zvýšení bezpečnosti dodržovat několik zásad. Heslo by mělo obsahovat velká i malá písmena, číslovky, nejlépe by se mělo jednat o shluk nespojitých písmen a číslovek bez slovního významu, popřípadě bez bližšího vztahu k uživateli. Heslo by se mělo v určitých intervalech obměňovat, zároveň by měla být distribuce hesla od administrátora k uživateli dostatečně zabezpečená. I přes to může dojít s pomocí speciálních programů k dešifrování hesla, popřípadě k vysledování neoprávněnou osobou. Velkou roli má také kázeň uživatele, který by neměl mít heslo nikde napsané nebo ho dokonce vyzradit třetí osobě. Často dochází také k zapomenutí hesla.
Autentizace předmětem – „něco mám", princip autentizace uživatele spočívá ve vlastnictví určitého předmětu, jenž se obecně nazývá „token". Mezi jeho hlavní vlastnosti by měla patřit obtížná padělatelnost. Mezi jeho výhody patří žádoucí přenositelnost a vyšší bezpečnost než u autentizace pomocí hesla. Nevýhodou je pak možnost odcizení, a proto je zde žádoucí doplnění této autentizace o heslo nebo biometrickou autentizaci.
Biometrická autentizace – „něco jsem", využívá jedinečných tělesných znaků jedince k jeho identifikování. Hlavní výhodou je příznivý poměr bezpečnost/cena, dále pak rychlost a praktičnost, jelikož nelze nic zapomenout ani ztratit. Pokud použijeme vhodné lidské charakteristické znaky, je výhodou i stálost. Bezpečnost můžeme dále zvýšit kombinací několika metod, jež jsou v další části popsány. I tuto metodu autentizace je možno napadnout, ale v současnosti je to nejefektivnější způsob zabezpečení v automatických systémech kontroly vstupů, a nachází proto uplatnění ve všech sektorech a stupních zabezpečení, především pak v docházkových systémech, při celních kontrolách, na letištích, v přístupových systémech bank, na výzkumných pracovištích, ve vojenských objektech a dalších klíčových místech s vysokým stupněm zabezpečení. Ve vývoji a v experimentálním

využití jsou pak nově systémy k vyhledávání potencionálních teroristů, založených na identifikaci osob ve skupině lidí na základě výrazu obličeje a chování. Nebo na základě promítání sledu obrázků o délce cca 30 vteřin s různou tématikou (např.: fotografie Usamy Bin Ladina, teroristických činů, atd.) a následného vyhodnocení reakce dotyčného jedince. Tyto systémy jsou experimentálně zkoušeny především ve státech jako Izrael, Velká Británie a Německo. [2]

Obrázek 1 Porovnání zabezpečení identifikátorů kontroly vstupu [1]

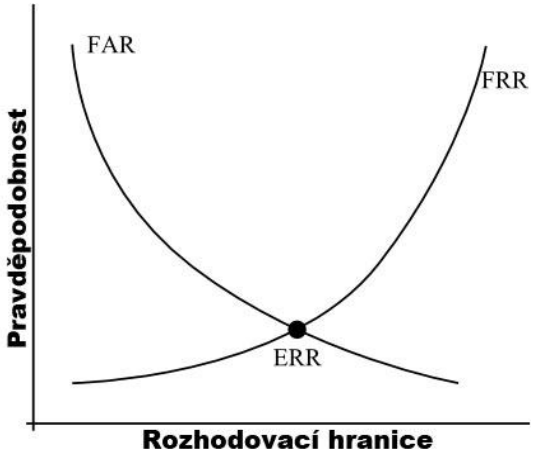
3.2 Měření výkonnosti biometrických systémů

False Acceptance Rate (FAR): koeficient míry bezpečnosti, je to chybné přijetí, které je dáno poměrem počtu biometrických předloh neregistrovaných uživatelů, kterým je chybně umožněn vstup, k počtu všech vzorků, které byly v daném rozsahu testu zkoumány.

False Rejection Rate (FRR): koeficient komfortu, chybné odmítnutí, je to poměr uživatelů, kterým biometrický snímač nepovolí přístup, přestože jsou zaregistrováni, k počtu všech vzorků, které byly v daném rozsahu testu zkoumány.

Platí nepřímá úměra těchto hodnot, tzn. čím je menší hodnota FRR, tím je naopak větší hodnota FAR a naopak. Proto obecně v biometrii hledáme hodnoty, kdy se FRR a FAR sobě co nejvíce blíží a samozřejmě jsou nejnižší.

Equal Error Rate (EER): tzv. křížový koeficient, udávající, s jakou pravděpodobností při jakém nastavení hranice rozhodování nastane jev FAR a FFR současně (tzn. FAR=FFR).

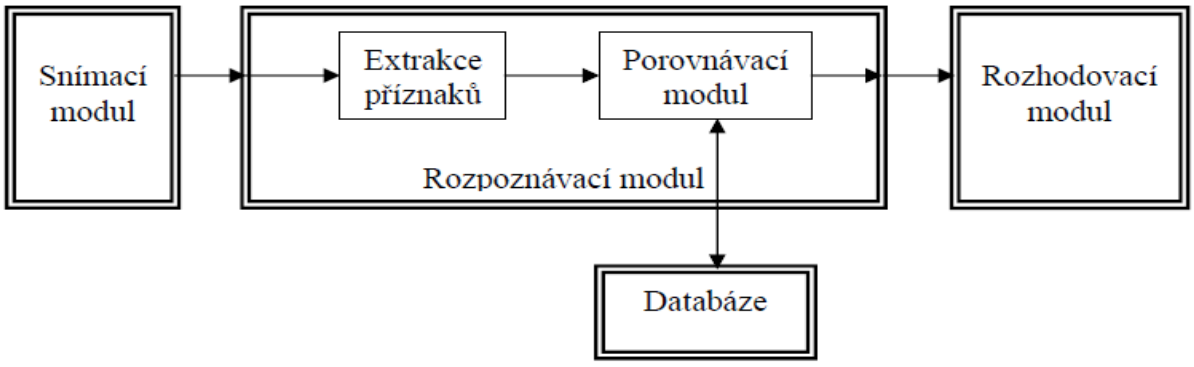


Obrázek 2 Závislost FAR a FRR na rozhodovací hranici [1, 2]

Pro ideální aplikaci platí, že křivky FAR a FRR se navzájem neprotínají a vhodným zvolením prahu citlivosti je lze bezchybně oddělit a současně dosáhnout nulové chybovosti jak chyby prvního, tak druhého druhu. Všechny osoby podstupující identifikační proces jsou tak 100% rozpoznány. [4]

3.3. Princip činnosti biometrických systémů

Tyto systémy mají přinést vyšší stupeň zabezpečení, který ale nedosahuje 100% bezpečnosti. Člověk je živý tvor a během života se mění, na což současné biometrické systémy nedokáží reagovat. [2]



Obrázek 3 Princip činnosti biometrických identifikačních systémů [2]

Snímací modul (senzor) – snímá biometrická data uživatele

Rozpoznávací modul – *modul extrakce příznaků* – extrahuje příznaky ze snímaných dat.

– *porovnávací modul* – porovnává extrahované příznaky

Databáze – slouží k uložení biometrických etalonů

Rozhodovací modul – na základě získaných dat rozhodne o shodě nebo neshodě sejmutých příznaků [2]

3.4. Rozdělení biometrických metod

Biometrické metody dělíme do dvou základních skupin:

Biologické metody – identifikují jedince na základě unikátních fyziologických a anatomických parametrů lidského těla.

Behaviorální metody – identifikují jedince na základě jeho unikátních vlastností. Ty jsou dány jednak fyzickými parametry, které člověk získává na základě DNA (pouze jednovaječná dvojčata ji mají naprosto shodnou) a také získanými zkušenostmi během života. Tyto jedinečné vlastnosti nelze napodobit. Nevýhodou je, že se mění poměrně rychle v čase. [2]

4. Popis vytipovaných biometrických metod pro použití na ČVUT

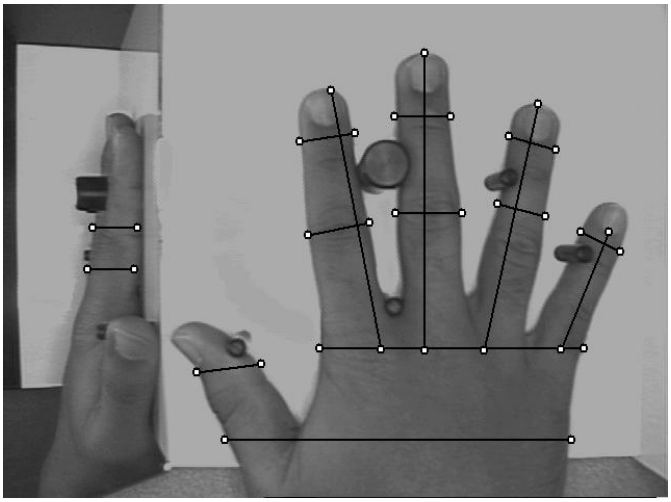
V mé práci se zabývám biologickými metodami biometrie, behaviorální metody nebudu uvažovat. Biologických metod je velké množství, ale pro mou práci jsem si vybral 5 metod, které blíže popíšu.

4.1. Geometrie ruky

Systémy rozpoznávající geometrii ruky jsou nestarším implementovaným biometrický principem. Vyvinul a nechal si jej patentovat David Sidlauskas v roce 1985 a hned v příštím roce byli již systémy rozpoznávající geometrii ruky komerčně dostupné. V roce 1996 byly tyto systémy použity pro identifikaci na Olympijských hrách v Atlantě, kde zajišťovaly bezpečnost vstupu do olympijské vesnice. Jelikož ale není geometrie ruky příliš unikátní biometrickou vlastností, je její aplikace v bezpečnostní sféře omezena právě stupněm bezpečnosti, kterého chceme dosáhnout.

Zařízení pro rozeznávání geometrie ruky využívají jednoduchého principu měření a 3 dimensionálního snímání délky, šířky, tloušťky a povrchu ruky konkrétního člověka umístěné na podložce s pěti polohovými kolíky (viz obrázek) pomocí CCD kamery.

Na obrazu ruky lze najít přes 31 000 polohových bodů a provést 90 různých měření vzdáleností. Vybrané měřené informace se ukládají do 9 bitového souboru, což činí tyto systémy velice výhodné z hlediska nízkého požadavku na paměť systému. Biometrické systémy založené na verifikaci geometrie ruky jsou používány v různorodých aplikacích docházkových systémů a přístupových systémech, kde jsou poměrně velmi rozšířené. [8, 9]



Obrázek 4 Osy měření [2]

Biometrické čtečky geometrie ruky

HandKey

HandKey je nejrozšířenější biometrická čtečka světa (cca. 100 000 instalovaných kusů). Princip čtečky funguje na snímání trojrozměrného obrazu tvaru ruky - geometrie ruky. Je uživatelsky lehce akceptovatelná, vhodná pro běžné nasazení (docházka, přístupy, atd.) [27]

Obrázek 5 Biometrická čtečka ruky HandKey [27]

PalmSecure

Bezkontaktní identifikace osob pomocí obrazu krevního řečiště. Uživatelé se mohou identifikovat přiložením ruky nad speciální senzor. Je nejen velice bezpečná, ale také praktická, tedy konkrétně že četnost připuštění neautorizované osoby je velmi nízká (< 0,00008) a zároveň četnost odmítnutí oprávněných uživatelů je také nízká – ~ 0,01 (pro srovnání u technologie využívající otisk prstu je to ~ 0,3). Stačí umístit dlaň 5 – 8 cm nad senzor a do dvou sekund by měla proběhnout identifikace, které předchází kontrola „života“ a vlastní skenování – senzor vyšle infračervené paprsky a kamera v senzoru snímá obraz krevního řečiště v dlani. Uvnitř senzoru dochází k zakódování sejmutého otisku. Otisk krevního řečiště zabere v systému asi 1–3 KB.

Technologie PalmSecure může být využita u docházkových systémů, pro přihlašování do systému a pro zajištění fyzického přístupu. Bank of Tokyo-Mitsubishi UFJ už tento systém využila například u svých bankomatů. [25]

Obrázek 6 Skenování ruky pomocí čtečky [25]

4.1.1. Tabulka 2 Rozhodující parametry metody geometrie ruky [zpracováno autorem]

cena čtečky vč. instalace	Od cca 45 000 Kč bez DPH
komfort (FRR)	0,1%
bezpečnost (FAR)	0,1%
spolehlivost	nízká (1:10 000)
uživatelská přívětivost	vysoká
rychlost verifikace	1 – 2s
stálost v čase	70%

4.2. Geometrie tváře 3D (face detection)

Verifikace obličeje je dnes nejvíce zkoumanou metodou, neboť problematika identifikace osob dle tváří je velmi obsáhlá. Rozpoznávání je založeno na srovnávání obrazu sejmutého kamerou s obrazem, který je uložen v centrální databázi. K jednoznačné identifikaci slouží většinou tvar obličeje a poloha opticky významných míst na tváři, jako jsou oči, nos, ústa či obočí. Obraz v počítači může být někdy uložen jako matice jasových úrovní, častěji je však diskriminován nějakou funkcí, která snižuje redundanci dat. Neuchovává se tedy přesná poloha očí, nosu a rtů, ale ukládá se jen vzdálenost očí, vzdálenost rtů od nosu, úhel mezi špičkou nosu a jedním okem, atd.

V současné době je známo několik technik rozpoznávání tváří. K těm významnějším a nejvíce používaným patří metoda měření geometrických vlastností a metoda porovnávání šablon. Všeobecně se věří, že po zdokonalení systému rozpoznávání obličeje, by mohli odpadnout mnohé, méně efektivní systémy (např. docházkový systém do zaměstnání). Je však pravdou, že během výzkumů se velmi často špatně specifikovaly požadavky, což vedlo k nízké funkčnosti a efektivitě systému. Jsou však známy i případy, kdy byly požadavky na systém tak přemrštěné, že bylo obtížné, respektive naprosto nemožné takový systém realizovat. Proto je nutné si uvědomit, jak vysoké nároky je nutné klást na daný identifikační systém. Je obrovský rozdíl v realizaci systémů, který porovnává dva statické obrazy a systému, který ověřuje totožnosti jednotlivce nacházejícího se ve skupině lidí.

Atraktivnost rozpoznávání obličejů je z hlediska praktického užívání pochopitelná, ovšem je nezbytné být realistický ohledně vyhlídek této technologie. Doposud neměli obličejové rozpoznávací systémy v praktických aplikacích velký úspěch. Existují dva odlišné přístupy k rozpoznávání geometrie tváře: geometrický (založený na rysech tváře) a fotometrický (založený na vzhledu obrazu tváře). Tři nejlépe prozkoumané a studované algoritmy rozpoznávání tváře jsou: Analýza hlavních částí (PCA - Principal Components Analysis), Lineární diskriminační analýza (LDA - Linear Discriminant Analysis), Elastický srovnávací diagram (EBGM - Elastic bunch graph matching).

PCA využívá vektorů tváře odvozených s kovarianční matice pravděpodobnostní distribuční funkce k vytvoření šablony vhodné pro srovnávání. Každá tvář lze rozdělit na tzv. eigenfaces (vzory tváří - matice jasových úrovní) a poté jde opět složit (viz. Obrázek 5). Každá eigenface je reprezentována pouze číslem, takže se namísto obrázku ukládá pouze číslo.

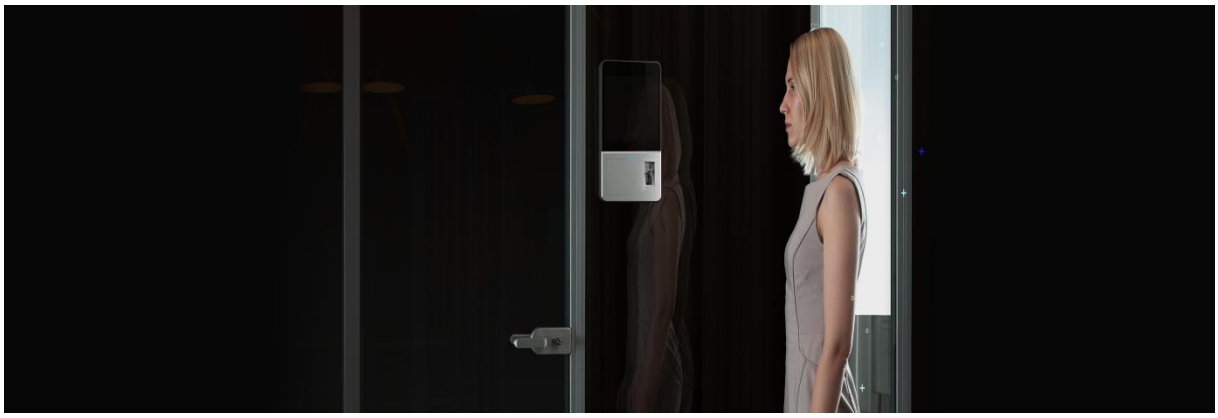
LDA je metoda, kdy se třídí pořízené obrazy tváří do skupin. Cílem je maximalizovat rozdíly mezi jednotlivými skupinami a minimalizovat rozdíly v každé skupině, každý blok snímků reprezentuje jednu třídu.

EBGM byla vyvinuta, jelikož předešlé metody nemohou uvažovat nelineární charakteristiky jako je osvětlení okolí, pozice hlavy anebo výraz tváře (úsměv, zamračení). Na obličeji se definuji uzlové body, které se poté propojí a tím definují linie tváře v prostoru, vznikne tím souřadnicová síť obličeje (viz. Obrázek 7). Samotné rozpoznávání pak probíhá tak, že systém pomocí filtru uzlových bodů reaguje na jednotlivé snímané tváře a může je pak porovnávat a vyhodnocovat. Problémem je přesnost lokalizace orientačních bodů na tváři, řešením může být kombinace s PCA nebo LDA metodou.

Identifikace osob dle geometrie tváře je dnes velice moderním a expandujícím principem. Dochází k jejímu nasazování na letištích, nádražích, rušných ulicích a náměstích a všeobecně na místech, kde by se mohli pohybovat pohřešované a hledané osoby apod. [8, 9]

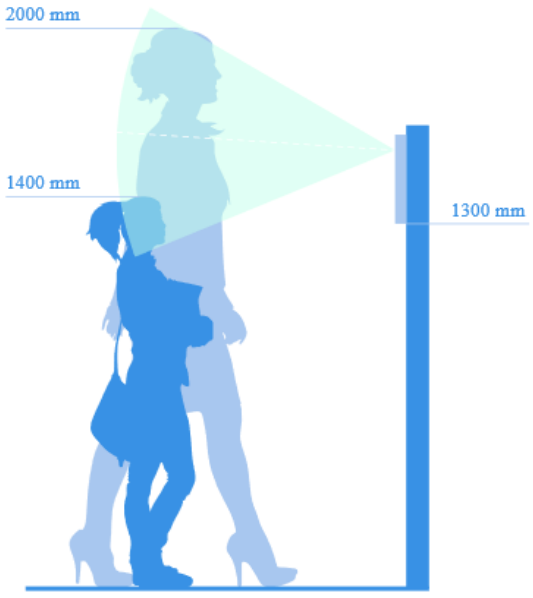
Obrázek 7 Důležité body pro geometrii tváře [9]

3D čtečky obličejů



Obrázek 8 Artec Intercom 3D [10]

- Vysoká kapacita - až 30 lidí za minutu
- Unikátní rozpoznání obličeje založené na 3D površích a struktuře
- Speciální funkce zabezpečení datového centra a podpora obnovení po havárii
- Široký rozsah výšky uživatelů od 1,4 m – 2,0 m
- Okamžité rozpoznání uživatelů s obličejem, brýlemi a klobouky
- Velká databáze v identifikačním režimu



Obrázek 9 Široký rozsah výšky čtečky Artec Intercom 3D [10]

Obrázek 10 Artec Broadway 3D BM [10]

O Broadway 3D je známo, že je prvním zařízením na světě, které dokáže vizuálně identifikovat člověka tak snadno, jak se lidé navzájem identifikují.

Identifikace trvá několik sekund. Chůze nebo dokonce běh kolem zařízení, krátký pohled na to - a bude vás identifikovat mezi desítkami tisíc registrovaných uživatelů. Na rozdíl od jiných biometrických zařízení nevyžaduje Broadway 3D přímý fyzický kontakt nebo přesné umístění před systémem rozpoznávání. Je schopen autentizovat lidi, když stojí, chodí nebo dokonce běží.

Stejně jako vnímáme jeden druhého, Broadway 3D má systém 3D vidění, který si pamatuje jedinečný trojrozměrný tvar obličeje. Na rozdíl od lidského zraku je však zařízení schopno odlišit geometrii s přesností až na několik zlomků milimetru a rozdělit i identické dvojčata, což činí z Broadway 3D jedno z nejpřesnějších biometrických zařízení na trhu. [10]

Využívá se na zajištění bezpečnosti na mezinárodním letišti v Soči.

4.2.1. Tabulka 3 Rozhodující parametry metody geometrie tváře 3D [zpracováno autorem]

cena čtečky vč. instalace	Od cca 150 000 Kč bez DPH
komfort (FRR)	0,9%
bezpečnost (FAR)	0,1%
spolehlivost	vysoká (1:1 000 000)
uživatelská přívětivost	vysoká
rychlost verifikace	2s
stálost v čase	50%

4.3. Otisk prstu

Identifikace na základě otisku prstu je jednou z nejznámějších a nejvíce publikovaných biometrických metod. Otisk prstu se používá pro identifikaci už celé století, a to hlavně pro svou vlastnost jedinečnosti a stálosti v čase. Navíc se musela tato identifikace s rozvojem počítačové techniky stát plně automatizovanou, aby si zajistila místo v dnešní době. Identifikace otisku prstu je s oblibou používaná především pro relativní jednoduchost získání srovnávacího vzorku, pro vysoké procento použitelné populace (nelze identifikovat pouze jedince, kteří přišli o obě ruce i nohy, což je málo pravděpodobné), dále pro četnost zdrojů ze kterých lze získat vzorek (10 prstů) a také protože jde již o zavedenou metodu s velkou databází u policie a s uplatněním v právní sféře a imigrační problematice.

Používání otisku prstu (přesněji obrazců papilárních linií na vnější straně prstů rukou, nohou a dlaní) jako metody pro identifikaci se začala používat už na konci 19. století, kdy Sir Francis Galton nalezl a definoval některé charakteristické body na prstu, které mohou sloužit k identifikaci člověka. Tyto „Galtonovi body“ položily základ vědnímu zkoumání otisku prstu, který byl rozvíjen po celé století. [8]

Metody zachycení otisku prstů

Otisk získaný pomocí inkoustu a papíru

Klasická metoda (rolled finger). Tato metoda se používá pouze ve forenzní sféře, policií při vyšetřování. Používá se inkoustu a papíru. Prst se po papíře roluje, aby se získal otisk celého prstu (prakticky od nehtu po nehet) s co možná nejvíce použitelnými markantami a aby se tím zvýšila i rychlost rozpoznání otisku.

Statické snímání

Jedná se o nejběžnější používanou metodu snímání otisku prstu. Uţivatel přitiskne svůj prst na senzor bez jakéhokoliv pohybování s ním. (existují desítky různých fyzikálních principů snímání, které jsou vysvětleny dále). Výhodou této metody je nesporně jednoduché ovládání (stačí pouze přiložit prst). Na druhou stranu je zde řada nevýhod: přehnanou silou tlačení prstu může uživatel rozlomit snímací čočku (obzvlášť je-li doba snímání delší, uživatel znervózní a přitlačí více), přiložení prstu a jeho současné pootočení vede k deformaci pokožky a celého otisku, senzor se lehce zašpiní (nehygieničnost) a na senzoru můžou zůstat latentní otisky. [8]

Snímače otisků prstů

Existují desítky metod snímání otisku prstu využívající nejrůznější fyzikální principy. Vědci se neustále snaží o nalézání nových a nových metod, a avšak ty nejjednodušší a nejsnadnější jsou již objeveny a používány. Jedná se především o:

Optické senzory

- Na základě odrazu (reflexní)
- Reflexní se skládáním obrazu
- Bezdotykový odraz
- Transmisní
- Křemíkové čipy a kapacitní snímač
- Kapacitní snímač a TFT

Elektro-optické snímače

Kapacitní snímače

- TFT optické

Tlakové snímače

- Vodivá membrána na silikonu
- Vodivá membrána na TFT

- Dotekové mikro-elektro-mechanické spínače

Rádiové snímače

Teplotní senzory

Ultrazvukové snímače

Fotonové krystaly

Snímače povrchové impedance [8, 9]

Při identifikaci se využívá možné rozdělení pomocí základního vzoru papilárních linií. Ty existují tři:

1. Smyčka – Alespoň jedna papilární linie tvoří smyčku mezi deltou a středem centrální oblasti. Tvoří přibližně 60% ze všech otisků.

2. Vír – Tvoří ji minimálně dvě delty, přičemž papilární linie vytvářejí oválné, kruhové nebo spirálovité obrazce s jádrem uprostřed. Tvoří přibližně 30% ze všech otisků.

3. Oblouk – Papilární linie zde vytvářejí oblouky. Tvoří přibližně 10% ze všech otisků.

Biometrické čtečky otisků prstů

Terminály ZK Finger zahrnují nejrůznější zařízení biometrické identifikace, od venkovních teplotně odolných až voděodolných přístupových čteček, přes anti-vandal přístupová zařízení až po vnitřní docházkové terminály s LCD displejem nebo v multimediálním provedení s dotykovou obrazovkou. Všechny nabízené terminály jsou v provedení se čtečkou karet EMarine. Pro snadné zadávání otisků prstů do systému slouží stolní čtečka otisků prstů, která se k počítači připojuje přes USB rozhraní. Anglický software pro přístupový systém je dodáván zdarma, stejně jako software pro docházku, který je navíc volitelně i v české jazykové mutaci. [26]

Výrobce	**ZK Finger**
Model	**ELI-TERM/OUT**
Rozměry	70 x 140 x 30 mm
FAR*	0,0001%
FFR*	1%
Max. otisků	1 500
Max. karet	10 000
Krytí krytí	IP54
Software	anglický, zdarma
Koncové ceny	10 914 Kč bez DPH
Výhody	Zadávání otisků bez SW, možnost výměny sklíčka, česká hlasová navigace

Obrázek 11 ZK Finger [26]

4.3.1. Čtečka, kterou použiji do mé bakalářské práce:

Sebury F007 EM-II :

Čtečka otisku prstu F007EM-II je jednoduché autonomní zařízení pro správu otisků prstů a přístupových karet formátu EMarine. Lze ji umístit do vnitřního i venkovního prostředí, při umístění do venkovního prostředí je vhodné zamezit kontaktu s deštěm a přímým slunečním světlem dopadajícím kolmo na snímač.

Výhody

- Ekonomicky příznivé řešení pro jednoduché aplikace
- Čtečka dokáže přečíst i ušmudlané prsty od trávy, uhlí či šmíru a hlíny, stačí jen prst lehce otřít, třeba o dlaň
- Možnost venkovního použití
- Snadné zapojení i nastavení
- Řešení zcela bez nutnosti softwaru

Čtečka obsahuje akustickou i optickou signalizaci všech svých režimů. Pro připojení k napájení, zámku, přístupovému systému a dalším periferiím slouží deset barevně odlišených vodičů délky cca 25 cm. [1]

Technické parametry:

- FAR: <0.0000256%
- FRR: <0.0198%
- Max. počet uživatelů: **celkem 3000 (2000 RFID karet a 1000 otisků prstů)**
- Doba čtení otisku/identifikace: **< 1 s**
- Rozměry: 70 x 155 x 35 mm (š x v x h)
- Hmotnost: 0,5 kg
- Cena: **2 998 Kč**

Obrázek 12 Sebury F007 EM-II [1]

<u>iEvo Micro</u>

Biometrická čtečka otisků prstů iEvo Micro pro interiéry, multispektrální snímač s vysokou úspěšností snímání i problematických prstů. Úzké provedení i pro instalaci na dveřní zárubně.

- Kapacita paměti vzorů: **8000 uživatelů**
- Data nejsou ukládána do čtečky samotné, ale putují do řídící jednotky
- Černé nebo barevné provedení
- Multispektrální metoda čtení biometrické informace (MSI) [1]

Obrázek 13 iEvo Micro [1]

Varianta Comfis

Hlavní jednotkou je terminál F702-MS od firmy Comfis, odolný proti venkovním nepříznivým vlivům.

- Kapacita otisků/záznamů: **1 500/50 000**
- doba verifikace: **≤ 2 s**
- FAR: ≤ 0,0001 %
- FRR: ≤ 1 %.

Obrázek 14 Terminál Comfis F702-MS [11]

Podřazené čtečky otisku prstů SR100 jsou kompatibilní s terminálem. Veškeré informace o uživatelích včetně záznamů o transakcích jsou ukládány do nadřazeného zařízení. [11]

Obrázek 15 SR100 [11]

Tabulka 4 Kalkulace terminálu a čtečky otisku prstu [11]

	Typ	Cena/kus
Terminál	F702-MS	18 970 Kč
Čtečka	SR100	3 076 Kč

4.3.2. Tabulka 5 Rozhodující parametry metody otisk prstu [zpracováno autorem]

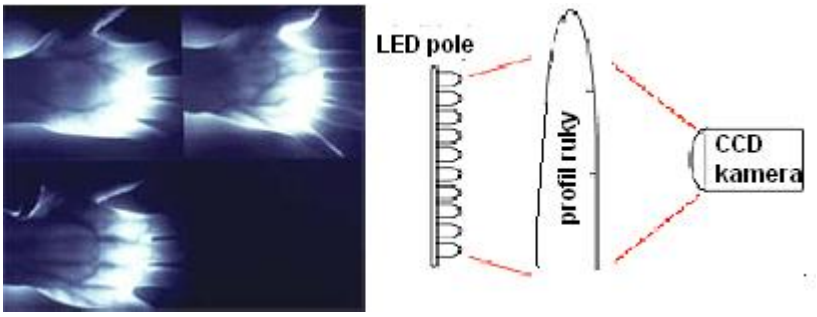
cena čtečky vč. instalace	Od 2 000 Kč bez DPH
komfort (FRR)	1,0%
bezpečnost (FAR)	0,0001%
Spolehlivost	vysoká (1:1 000 000)
uživatelská přívětivost	vysoká
rychlost verifikace	0,2-1s
stálost v čase	60%

4.4. Struktura žil na zápěstí/dlani

Jedná se o jednu z nejnovějších metod rozpoznávání jedince (první komerčně dostupné systémy jsou datovány až k roku 2000). Tato technologie se vyznačuje obtížností falšování (síť cév je obtížné napodobit, jelikož je uvnitř ruky a není tedy viditelná pro napodobení, navíc některé principy přímo vyžadují, aby byla ruka živá, tedy aby v ní tekla teplá krev).

Technologie spočívá ve snímání hřbetu ruky speciální kamerou v infračerveném světle. Tak lze získat černobílý obraz stromové struktury žil, které tvoří zřetelný vzorec. Struktura krevního řečiště se navíc v dospělém věku příliš nemění, je velice výrazná a její jedinečnost i mezi jednovaječnými dvojčaty prokázaly některé vědecké studie. Výhodou je také bezkontaktní princip (uživatel se nemusí dotýkat povrchu snímače, což zvyšuje hygienu a pravděpodobnost správného přijmutí uživatele).

Pro uplatnění této technologie existuje mnoho různých použití (např. v Japonsku jsou systémy rozmístěny na univerzitách, nemocnicích a pokladních automatech). Aplikace musí mít zajištěnu ID verifikaci, vysokou fyzickou bezpečnost kontroly přístupů, vysokou bezpečnost datových sítí a kontrolu přístupu do pokladních systémů. Další nespornou výhodou je možnost verifikace i identifikace (lze použít pro systémy 1:1, kdy se používá ID karet nebo jiných tokenů, anebo systémů 1:N, kdy je pořízený vzorek porovnáván s celou databází šablon). Snímání probíhá tak, že zdroj (pole LED diody) prosvítí ruku a na základě různé absorpce (odrazu) záření krevních cév a ostatních tkání se vytvoří obraz (viz Obrázek 16) pomocí snímací CCD kamery (charge-coupled device - zařízení s nábojovou vazbou). Obraz je dále digitalizován a zpracováván za cílem vyextrahování sítě cév. Ukládají se důležité vlastnosti jako: body a úhly větvení cév a tloušťka cév. [8]



Obrázek 16 Obraz světelné prostupnosti ruky a princip snímání [8]

Technologie žil dlaně ruky

Princip rozpoznání vzorce krevního řečiště v dlani ruky je velmi podobný technologii žil hřbetu ruky. V tomto případě se ale samozřejmě detekují žíly dlaně ruky. Používá se k tomu bezdotykový snímač, ke kterému se ruka přiloží, viz Obrázek 17. Snímač je schopen zachytit obraz dlaně bez ohledu na pozici a pohyb dlaně. [8]

Obrázek 17 Snímač dlaně [6, 8, 24]

Nejdříve se zachytí snímek dlaně infračerveným paprskem, jak je vidět dole na obrázku. Síť tmavších čar (zvýrazněná krev obsahující odkysličený hemoglobin) zde představuje vzorec žil dlaně.

Obrázek 18 IR snímek dlaně [6]

Z tohoto obrazu systém extrahuje vzorec žil dlaně do nového obrazu. Takovýto obraz se následně dle potřeby transformuje a porovná s uloženou šablonou z registrace uživatele. [6, 9]

Obrázek 19 Extrahované žíly dlaně [6, 8]

Obrázek 20 Biometrie krevního řečiště [19]

4.4.1. Tabulka 6 Rozhodující parametry metody struktura žil na zápěstí [zpracováno autorem]

cena čtečky vč. instalace	Od cca 45 000 Kč bez DPH
komfort (FRR)	0,01%
bezpečnost (FAR)	0,00008%
Spolehlivost	vysoká
uživatelská přívětivost	vysoká
rychlost verifikace	2,5s
stálost v čase	60%

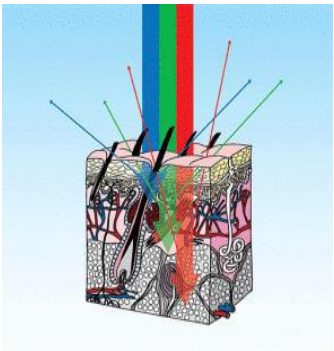
4.5. Identifikace pomocí spektroskopie kůže

Někdy je také tato metoda nazývána *Lumidigm Reads Skin Physiology*. Optické vlastnosti kůže jsou určeny jejími chemickými a strukturálními vlastnostmi, které jsou unikátní pro každého člověka.

Kůže se skládá z několika vrstev a má odlišnou tloušťku nejen na různých částech těla, ale liší se i u každého člověka, přičemž každá vlnová délka se láme a odráží v jiné vrstvě, což je následně vyhodnoceno fotodetektorem.

Například krátké vlnové délky jako je modré světlo se odráží od melaninu a krve, světlo delších vlnových délek pak proniká hlouběji do kůže. Tyto optické vlastnosti můžeme změřit pomocí metody rozptýlených odrazů. Biometrický senzor je tvořen 32 LED diodami šestnácti různých vlnových délek v rozmezí 395–940 nm a křemíkového fotodetektoru. Vždy dvě pro jednu vlnovou délku na protilehlé straně senzoru a pět křemíkových fotodiod. Diody emitující větší vlnovou délku jsou na vnější straně, diody kratších vlnových délek pak na vnitřní straně. Nejčastěji se senzor zaměřuje na dlaň ruky. Princip metody spočívá v tom, že vybraná část pokožky je ozářena světlem o více vlnových délkách (od viditelného až k blízkému infračervenému světlu). Každá vlnová délka světla se láme a odráží v jiné vrstvě pokožky a od jiných struktur kůže. Odraz je zachycen přijímačem složeným z fotodiod a předán k dalšímu zpracování a analyzování.

Tato metoda není prozatím využívána, ale nabízí dostatečný potenciál ke komerčnímu využití. [2]



Obrázek 21 Spektroskopie kůže [8]

Biometrické čtečky spektroskopie kůže

Obrázek 22 Lumidigm řady V V302 IP65 [8]

4.5.1. Tabulka 7 Rozhodující parametry metody spektroskopie kůže [zpracováno autorem]

cena čtečky vč. instalace	600 Kč
komfort (FRR)	3,9%
bezpečnost (FAR)	1,2%

4.6. Duhovka

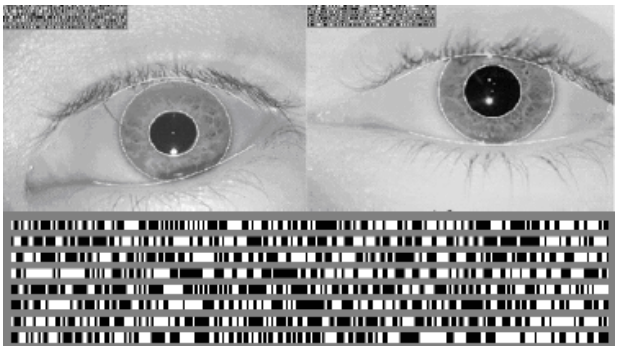
Duhovka je pigmentovaná vnitřní struktura oka obklopující zornici. Oční duhovka je u každého jedince unikátní. Liší se i u jednovaječných dvojčat, dokonce má i každý člověk odlišnou pravou a levou duhovku. Zatímco existuje 60 odlišných forem otisků, tedy markantů, jež mohou být kombinovány na jednom otisku prstu, počet různých forem vzorů duhovky je vyšší než 400. To z ní dělá matematicky nejoriginálnější část těla. Tyto vzory se vytvářejí v období nitroděložního vývoje (od třetího do osmého měsíce) a nejsou dědičné jako barva a struktura. Duhovka je v čase absolutně neměnná, což z ní dělá nejlepší identifikační metodu.

V roce 1994 si John Daugman nechal patentovat první algoritmus pro identifikaci podle obrazu oční duhovky, který je v současnosti základem většiny systémů tohoto typu. Skutečnost, že tento algoritmus je patentován, navyšuje cenu těchto systémů (např.: docházkový systém pro malou firmu vyjde cca na 150 tis. Kč).

Ke snímání oční duhovky se využívá CCD kamera s vysokým rozlišením, popřípadě doplněná o decentní infračervené osvětlení (750–1000 nm) snižující odrazy okolí od rohovky. Při identifikaci je nutná aktivní účast žadatele o přístup. Systém odhalí i brýle či kontaktní čočky, které správné identifikaci nezabrání, stejně tak neovlivňuje spolehlivost ani většina současných očních operací (včetně transplantace rohovky). Identifikace probíhá ze vzdálenosti od 7,6 cm do 1 m podle použitého přístroje a vyžaduje, aby se žadatel o přístup díval do jednoho konkrétního bodu po dobu 2–3 sekund, během nichž je vytvořena monochromatická fotografie. Následně biometrický systém lokalizuje vnitřní a vnější okraj duhovky a využije několik jasně viditelných charakteristik (např.: pigmentové skvrny, pigmentové záhyby, radiální rýhy, krypty), z nichž sestaví mapu duhovky. Její velikost je 256–512B, což například konkrétní aplikaci IrisCodeTM umožňuje porovnat mapu o velikosti 512B s 500 000 jiných map za vteřinu.

Při registrování uživatele se vytvoří několik fotografií duhovky (2–4), aby se minimalizovalo riziko nesprávného vyložení odrazů jako specifických složek duhovky a šablona byla naprosto konzistentní s reálnou skutečností. Následně se uloží pod specifický

etalon, kterému se nejvíce podobá, z důvodu urychlení identifikace v rozsáhlých databázích. [2]



Obrázek 23 Lokalizování duhovky a její piktografické znázornění [8]

Obrázek 24 Snímač duhovky [8]

Využívá se v docházkových systémech, zónách s velmi vysokými nároky na bezpečnost, komerčních organizacích všeho druhu, přístupových systémech, identifikačních systémech (vstup na hranicích do SAE od roku 2001, Liga arabských států od roku 2008, některá vězení v USA).

Biometrické čtečky duhovky

Iris ID

Obrázek 25 iCAM7 Series [2]

- Vysoká přesnost 1:N nebo 1:1 (s kartou nebo PINem)
- Vysoká rychlost
- Nekontaktní - čistý a hygienický
- Modulární verze až pro 10.000 účastníků

Funkce:

Rychlé plně automatické snímání duhovky

Jednoduché bezkontaktní uživatelské rozhraní

Integrovaná kamera pro fotografování s vysokým rozlišením

Integrovaná bezdotyková čtečka čipových karet

iCAM se aktivuje, když uživatel přistupuje nebo když je prezentována karta.

Rozsah snímání snímků je vzdálen 11-15 palců (28-38 cm).

Automatické nebo poloautomatické nastavení výšky.

Umístění bodu přes můstek nosu snadno pomáhá vyrovnání.

Oranžová se změní na zelenou, pokud je uživatel ve správné vzdálenosti.

Vizuální indikace je zesílena pomocí přátelských zvukových výzev.

Je také možné zachytit obraz obličeje.

4.6.1. Tabulka 8 Rozhodující parametry metody duhovka [zpracováno autorem]

cena instalace	od cca 70 000 Kč bez DPH
komfort (FRR)	0,00066%
bezpečnost (FAR)	0,00078%
Spolehlivost	vysoká (1:6 000 000)
uživatelská přívětivost	nízká
rychlost verifikace	3,5s
stálost v čase	90%

5. Architektura systému

Máme 3 možnosti, jak se k problematice postavit:

1. Serverový systém
- uživateli je sejmut daný biometrický znak (biom_pattern: BP) a ten je uložen v nějaké databázi na serveru.
Čtečky jsou poté pomocí počítačové sítě propojeny se serverem, a když uživatel přiloží i svůj např. prst, tak je porovnán s BP, který je uložen v dbf. na serveru. Tam také probíhá vyhodnocení, je tam uložen porovnávací algoritmus a server dává výsledek vyhodnocení. Výhody: stačí úplně "hloupé" čtečky, vše se obstarává na straně serveru, čtečka jen dostane výsledek vyhodnocení (a podle toho vpustí či nevpustí). Nevýhody: přenos dat prostřednictvím sítě (šifrování, bezpečnost)
2. Distribuovaný systém
- BP je opět uložen na serveru. Čtečka má svůj vlastní vyhodnocovací algoritmus a po sejmutí např. otisku prstu, vyrobí tzv. fingerprint_code (iris_code pro duhovku, atd.), ten posílá po netu na server, kde se porovná s fingerprint_codem uloženým v dbf. na serveru. Server pak pošle čtečce ano či ne ohledně vyhodnocení úspěšné identifikace.
3. Samostatné čtečky
- BP je opět uložen v dbf. na serveru, ale pouze pro záložní účely. Sejmutý znak je nahraný na ID kartu ve tvaru fingerprint_codu (bezpečné), čtečka obsahuje vyhodnocovací algoritmus, který porovná code na kartě s kodem, který si sama vyhodnotí po přiložení ruky a sejmutí otisku.

Nejvýhodnější pro nás i z hlediska zabezpečení je systém samostatné čtečky, aby nedocházelo k přenosu či zneužití dat, proto ho volím pro mou bakalářskou práci. Otisky nebudou nikde na síti, aby nám to někdo kradl, a když někdo ukradne ID kartu, tak z toho nezíská otisk prstu.

6. Analýza pro potřeby BA

Skoro všechny levnější čtečky mají maximální kapacitu otisku od 1000 do 1500, což znamená od 500 do 750 osob (dva otisky pro jednoho uživatele). Z tohoto důvodu by bylo komplikovanější používat biometrické snímače pro vstup do všech počítačových učeben z důvodu většího počtu studentů, kteří potřebují do nich vstup v průběhu celého studia. To ale není velký problém, protože za celou dobu fungování Fakulty dopravní v Praze nebyly kromě jedné krádeže tiskárny zaznamenány mimořádné události spojené s poškozením či krádeží fakultního majetku. [19]

Jaké prostory chci zabezpečit na FD

V mé práci budou vstupy zabezpečeny dle důležitosti a možností podle levelů:

Level 1 — zabezpečení pomocí čidla: 97*

Level 2 — zabezpečení pomocí čidla + biometrický applet: 27

*už je zabezpečeno

Navrhovaný stav bezpečnostního přístupu do prostor ČVUT

<u>3 základní stupně zabezpečení:</u>

0 *(nejnižší zabezpečení)* - vrátnice

1 *(nízké až střední zabezpečení)* – posluchárny+učebny+ústavy+děkanát+PC učebny: **čip**

2 *(střední až vysoké zabezpečení)* – serverovna 2x, tisk. centrum 2x, laboratoře: **BIO**

---

3 *(nejvyšší zabezpečení)* – pomocí karty s **PIN**em /neuvažuji, není to cílem práce/

Počet místností na FD potřebujících bezpečnostní vstup:

Místnosti na Fakultě dopravní, které by bylo potřeba zabezpečit pomocí *biometrického appletu:* („A“-ANO, „N“-NE)

- <u>unikátní vědecká pracoviště:</u>
  - Certifikační orgán pro výrobky při Fakultě dopravní – **A** (K508)
  - Zkušební laboratoř FD – **A** (K027)

- Laboratoř interaktivních vozidlových simulátorů DSRG – **A**
- Dopravní sál FD – **A**
- Laboratoř simulací v letectví – **A**
- Laboratoř bezbariérové dopravy – N
- Laboratoř navigačních a identifikačních systémů (e-Ident) – N
- Laboratoř pro dynamické zkoušení materiálů a konstrukcí DYNLAB – **A**
- Laboratoř telematiky chytrých měst – N (K620)
- Laboratoř řízení a modelování dopravy – **A (2x)** (K620)
- Laboratoř odbavovacích a informačních systémů ve veřejné osobní dopravě – **A** (K620)
- Biofeedback – **A** (K620)
- Zabezpečovací technika – **A** (K620)
- Laboratoř ATM systémů – **A** (A234-b)
- Laboratoř NDT (Non Destructive Testing) a kalibrace letových zapisovačů – **A** (A-234a)
- Specializované centrum pro aplikovanou simulaci a vizualizaci – **A** (SM8)
- Výzkumná laboratoř vozidel – N
- Společná laboratoř tunelových systémů FD, Žilinské univerzity a Eltodo a.s. - N
- Společná laboratoř spolehlivosti systémů FD ČVUT a Ústavu informatiky AV ČR – N
- Společná laboratoř elektronové mikroskopie – **A**
- Společná laboratoř biometrické identifikace a lokalizace v dopravě – **A**
- Mobilní měřící laboratoř – N
- Laboratoř speciálních projektů při ústavu bezpečnostních technologií a inženýrství – **A**
- Laboratoř měřících metod v dopravě – **A (2x)** (A-132, A-133)
- Laboratoř lidského faktoru a automatizace v letectví – **A** (A-234f)
- Laboratoř letecké bezpečnosti – **A** (A-234e)
- Laboratoř dopravní energetiky – N
- Laboratoř bezpečnosti dopravních systémů – **A** (B-130)
- Redakce časopisu Neural Network World – N
- Serverovna Praha – **A (2x)**

- <u>Tiskové centrum FD</u> - **A**
  - Na Konviktu a na Horské

⇨ Počítáme pouze s místnostmi označenými písmenem „**A**“

- Rezerva 1 čidlo pro děkanát

CELKEM: 27 místností bude zabezpečeno pomocí biometrického appletu

Místnosti na Fakultě dopravní, které jsou zabezpečeny pomocí *čidla*:

- PC učebny:

Praha:

Konvikt:

  - K104, K105, K107b, K107c

Horská:

  - B101, B102, B106, B109, SM6, A270, A271

Děčín:

  - 2 učebny

- Ústavy:
  - Ústav aplikované matematiky;
  - Ústav dopravních systémů;
  - Ústav aplikované informatiky v dopravě;
  - Ústav jazyků a společenských věd;
  - Ústav dopravních prostředků;
  - Ústav logistiky a managementu dopravy;
  - Ústav mechaniky a materiálů;
  - Ústav dopravní telematiky;
  - Ústav letecké dopravy;
  - Ústav soudního znalectví v dopravě;
  - Ústav bezpečnostních technologií a inženýrství;

- Děkanát;
- Posluchárny.

6.1 Používané technologie

6.1.1. Radio Frequency IDentification (RFID)

Bezkontaktní identifikace využívá k přenosu informace mezi transpondérem a čtecím zařízením rádiové a mikrovlnné spektrum elektromagnetické vlny. Kartou se rozumí obecný pojem pro RFID zařízení schopné nést informaci a komunikující se čtecím zařízením, transpondérem (tag, token, label), pak zařízení s integrovanou anténou, čipem a kondenzátorem, nesoucí informaci a komunikující se čtecím zařízením. V závislosti na druhu transpondéru je informace různou formou vyslána a zpracována čtecím zařízením, které informaci buď přepošle do informačního centra, nebo samovolně vykoná nějakou činnost. Základem každé instance RFID je transpondér, čtečka a programového vybavení – middleware.

Ve světě existuje několik různých standardů RFID (např. ISO/IEC 10536, ISO/IEC 14443, ISO/IEC 15693 aj.), jednotný všeobjímající standard neexistuje. Dílčí řešení se liší podle použité frekvence, kódování, množství přenášené informace, způsobu šifrování či tvaru transpondéru.
Na ČVUT v Praze je několik druhů přístupových karet – transpondérů. Liší se nejen svým provedením – ISO karty či různé klíčenky, ale také použitým standardem. Studenti mají možnost vybrat si svou studentskou kartu ze dvou variant – studentská karta ČVUT a studentská mezinárodní karta ISIC s logem ČVUT. Studentská i zaměstnanecká karta ČVUT používá stejnou technologii. Na bázi RFID čipů funguje i Národní technická knihovna (NTK) - od vstupu, přes samopůjčování a vracení knih. [14]

6.1.2. Mifare DESFire EV1

Podobně jako má každý systém svoji hierarchii, tak i u RFID najdeme jednodušší i sofistikovanější technologie. DESFire EV1, pracující na frekvenci 13,56 MHz, patří ke špičce v RFID, proto jej dnes můžeme najít hlavně v platebních systémech, veřejné dopravě a dalších oblastech, kde je požadavkem rychlé čtení i zápis na kartu, různé aplikace na kartě a hlavně vysoká bezpečnost komunikace. Výhodou systému je i antikoliznost - důležitá v případě, pokud je v dosahu čtečky více RFID karet. Poměrně velká paměť karet (2, 4 nebo 8 kB) umožňuje uložit značné množství dat v různých souborech. O bezpečnou komunikaci se starají kryptovací algoritmy DES/2K3DES a zejména 3K3DES a AES. [20]

Biometrický applet bude uložen na ID kartě ČVUT

6.2 ID karta ČVUT

Funguje na principu elektromagnetických vln pomocí RFID. Tato bezkontaktní identifikace plně nahrazuje čárové kódy z důvodu snazší manipulace a většího prostoru pro přenášená data.

ID karta ČVUT se dělí podle typu osoby:

- průkaz typu osobní – zahrnuje dříve používaný „průkaz zaměstnance“ a „průkaz hosta“. Je to průkaz vázaný na identitu nositele, která je evidována v systému EGJE nebo CRI. Průkaz Student je taky osobní, přičemž pro studenty je ve dvou variantách: ČVUT karta či ISIC karta a má jiný design a funkce.

Průkaz OSOBNÍ je vydáván ve dvou variantách:

a) **S KONTAKTNÍM ČIPEM** – pro osoby s platným pracovně právním vztahem typu hlavní pracovní poměr nebo dohoda o pracovní činnosti

- Na tento průkaz bude nahrán BA

- Na kontaktní čip obdrží osoba nahraný osobní certifikát pro elektronický podpis a vytisknutý PIN kód. [28]

Obrázek 26 Vzor Průkazu ČVUT s kontaktním čipem [12]

b) **BEZ KONTAKTNÍHO ČIPU** – pro zaměstnance a nestudenty (DPČ, DPP, účastníci kurzu celoživotního vzdělávání, externí osoby) [28]

Obrázek 27 Vzor Průkazu ČVUT bez kontaktního čipu [12]

- průkaz typu přenosný - není vázaný na identitu nositele a slouží hlavně k dočasnému umožnění přístupu do prostor ČVUT osobám, které nejsou evidovány v EGJE ani CRI.

Průkaz je možno vydat pouze zmocněné osobě na základě písemné žádosti vedoucího součásti nebo vedoucího pracoviště ČVUT. Zástupce součásti žádost předá Vydavatelství průkazů. Pracovníci Vydavatelství průkazů zkontrolují úplnost vyplněných údajů a dohodnou se zástupcem předání zhotovených přenosných průkazů. Následně zástupce převzetí průkazů stvrdí podpisem a předá je na pracovišti.

Obrázek 28 Vzor Průkazu ČVUT přenosného [12]

Průkaz typu STUDENT – ČVUT karta nebo mezinárodní ISIC karta

Obrázek 29 Vzor Průkazu ČVUT [12]

Obrázek 30 Vzor Průkazu ISIC [12]

Použití:

Průkaz studenta ČVUT

- Na tento průkaz bude nahrán BA

- k identifikaci při vstupu do prostor ČVUT
- v knihovnách ČVUT a v Národní technické knihovně
- ke stravování v provozovnách Správy účelových zařízení ČVUT (menzy)
- k identifikaci v zabezpečovacích systémech ČVUT
- k identifikaci mimo ČVUT jako potvrzení o studiu pro mimoškolní aktivity studenta, pokud byly s externími organizacemi (s dopravními podniky, finančními institucemi apod.) uzavřeny smlouvy nebo pokud tyto organizace poskytují volné vstupy a slevy na studentské průkazy dle svých vnitřních pravidel
- jako průkazka pro koupi kupónu na městskou hromadnou dopravu (pouze občané ČR)
- pro platby v Transakčním zúčtovacím systému (tisk, parkování) [28]

Průkaz ČVUT s licencí ISIC

- Na tento průkaz bude nahrán BA

- jediný mezinárodně akceptovaný doklad studenta ve 130-ti zemích
- cestovní služby: letenky, autobusové jízdenky, cestovní pojištění ISIC
- slevy u dopravců mimo rámec žákovského jízdného
- slevy ve vybraných lyžařských střediscích
- slevy v kinech, divadlech a dalších kulturních institucích
- slevy na festivalech
- slevy ve vybraných obchodech a restauracích
- každoroční bonus při předložení průkazu ISIC a zřízení studentského účtu u vybraných bank [28]

KLÍČENKA - vydává se jako doplněk ke kartě. Přívěsek s čipem použitelný pouze na vstupy do budov, případně pro vjezd do garáží provozovaných ČVUT. Je vydávána pouze pro zaměstnance. [28]

- Na tento průkaz bude nahrán BA

6.3 Technické řešení

Biometrický applet (BA) bude umístěn:

- *na kontaktní čipové kartě pro zaměstnance*
- *na bezkontaktní čipové kartě pro studenty*
- *na klíčence*

BA bude vždy uložen na bezkontaktním čipu s použitou technologií: MIFARE DESFire 4K EV1: kapacita ve velikosti cca 4KB, je zde prostor pro nahrání až 8 aplikací, např. uložená jízdenka na MHD, studium, elektronická peněženka, možnost platit ve skriptárně, menze apod.

6.3.1. Pilotní projekt – fakulta dopravní

Stávající stav		**Rozšířený stav o:**
Počet lidí:	1684 /dle ID karet/	1190 pro BA viz Tabulka 9
Počet budov:	6	
Počet čidel:	97	
Počet čidel BIO:	0	+27

Cena čidel BIO: 27*2998=80 946 Kč

Čtečka, kterou použiji pro pilotní projekt:

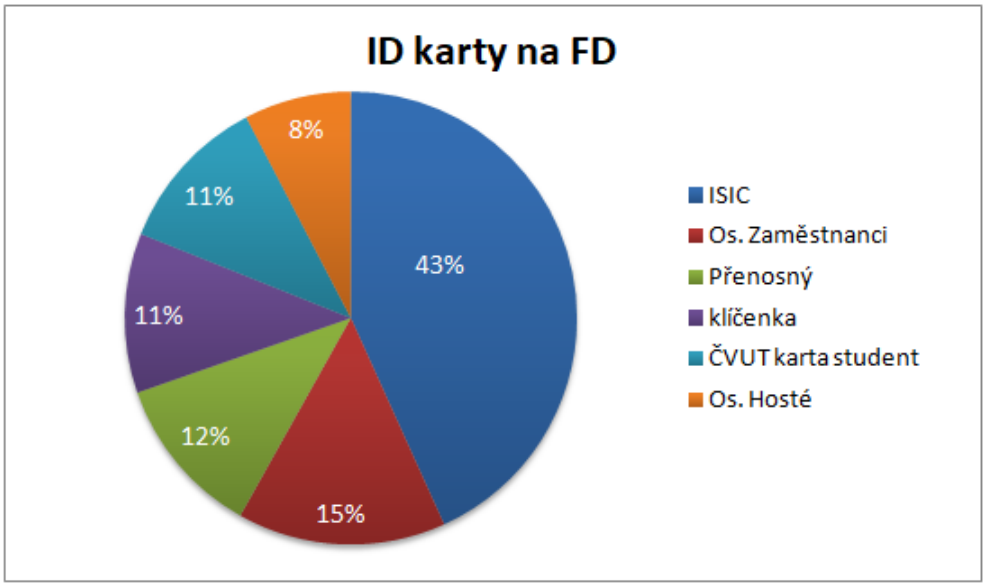
Sebury F007 EM-II

- Max. počet uživatelů: **celkem 3000 (2000 RFID karet a 1000 otisků prstů)**
- Doba čtení otisku/identifikace: **< 1 s**
- Cena: **2 998 Kč**

Tabulka 9 Počet ID karet na FD [zpracováno autorem]

Typ průkazu	Celkem (k 18. 6. 2018)	Použitá technologie		
Student	918	**ISIC**	DESFIRE MIFARE a mg. pruh	696 32
		ČVUT karta	DESFIRE ~~MIFARE a mg. pruh~~	182 ~~8~~
Zaměstnanec	251		DESFIRE ~~MIFARE a mg. pruh~~ Kontaktní a DESFIRE	4 ~~6~~ 241
Klíčenka	192		DESFIRE ~~MIFARE~~	67 125
Průkaz ČVUT (host) *	129		DESFIRE ~~MIFARE a mg. pruh~~ Kontaktní a DESFIRE	86 ~~3~~ 40
Přenosný *	194		DESFIRE ~~MIFARE a mg. pruh~~	153 ~~41~~
∑	1684			1190
* neuvažuji při práci, ~~BA není možné nahrát~~				

Který z našich průkazů splňuje technologii a je vhodný pro BA? Viz červená barva

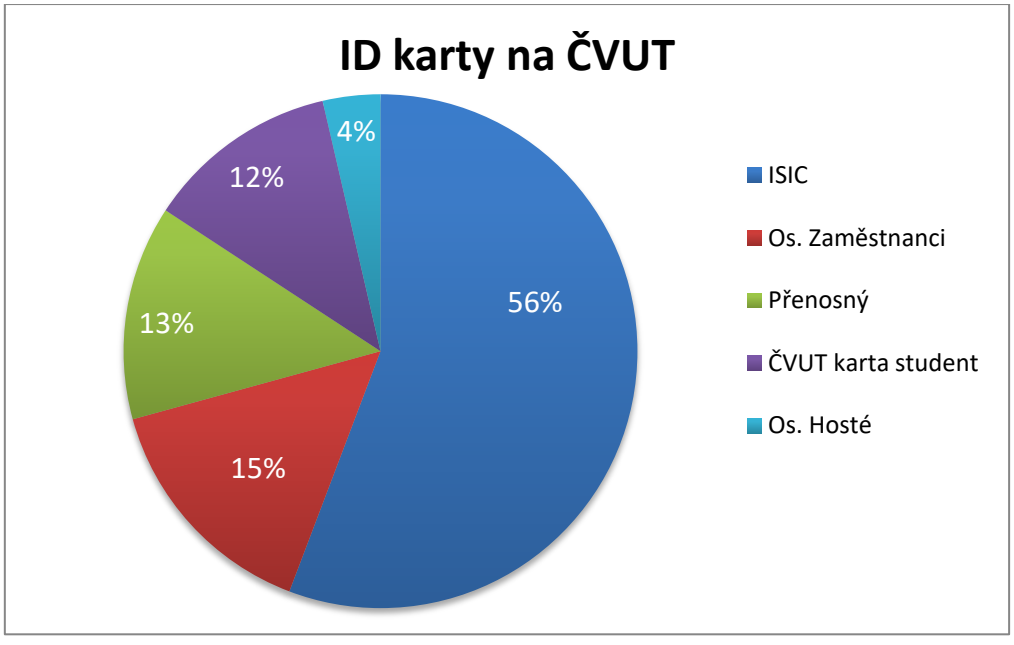


Graf 1 Počet ID karet na FD [zpracováno autorem]

Fakulta dopravní je pilotní projekt, ale protože v plánech je řešení problematiky celého ČVUT, tak pro přehled uvádím informace počtu karet také pro ČVUT, počty zaměstnanců, apod. viz tabulka:

Tabulka 10 Počet ID karet na ČVUT [zpracováno autorem]

Průkaz		CELKEM (ke dni 2. 11. 2017)
Student • **ČVUT karta** • **ISIC**	 3 235 14 854	**18 089**
Osobní • **zaměstnanci** • **hosté** *	 3 984 964	**4 948**
Přenosný *	3 596	**3 596**
∑		**26 633**
* neuvažuji při práci pozn.: zjednodušená tabulka		



Graf 2 Počet ID karet na ČVUT [zpracováno autorem]

7. Multikriteriální optimalizace (MO)

Multikriteriální optimalizace je optimalizace více funkcí najednou. Je zapotřebí další matematický aparát. [29]

Při řešení problému se rozhoduji na základě více kritérií. Cílem je dát doporučení pro volbu tzv. kompromisního rozhodnutí, které se snaží respektovat všechna uvažovaná kritéria.

MO v našem případě znamená, že budeme pomocí vah *w* (náklady, uživatelská přívětivost, rychlost verifikace, bezpečnost, stálost v čase, komfort, míra spolehlivosti) optimalizovat stávající zařízení (ID karta ČVUT – studenti i zaměstnanci).

Praktická část

7.1. Návrh řešení

Jak jsem poznamenal výše, tak jsem si vybral 5 biometrických metod, které jsou popsány v teoretické části práce. Abych zjistil, která z metod je pro Fakultu dopravní potažmo ČVUT nejpřívětivější, porovnal jsem tyto metody dvěma způsoby: pomocí vzorce a pomocí vah.

Pro naše využití na ČVUT počítám se *spolehlivostí, uživatelskou přívětivostí, rychlostí verifikace, stálostí metody v čase* a *náklady*.

biometrické vlastnosti:

- otisk prstu – měří se struktura papilárních linií a jejich detailů
- duhovka oka – obrazový vzorec duhovky
- geometrie tváře – vzdálenosti očí, nosu a úst
- geometrie ruky – rozměry dlaně a prstů
- struktura žil na zápěstí – struktura žil [8]

7.2. Analýza vybraných metod

1. Pomocí vzorce,
2. Pomocí přiřazení vah *w*

Porovnání biometrických metod pomocí vzorce

7.2.1. Vzorec

Vytvořil jsem vzorec, podle kterého se dá zjistit, jaká metoda je pro zavedení na FD potažmo ČVUT nejlepší. Vycházel jsem při jeho tvoření z matematické analýzy a dalších matematických předmětů na naší škole.

$$F = 1 - \log_{10}\left(\frac{N}{UP} \times \left(\sqrt{RV^2 + MS^2 + S^2} \times \frac{1}{\sqrt{2}}\right) + (FRR + FAR)^2\right)$$

7.2.2. Vysvětlení významu koeficientů použitých ve vzorci pro porovnání biometrických metod

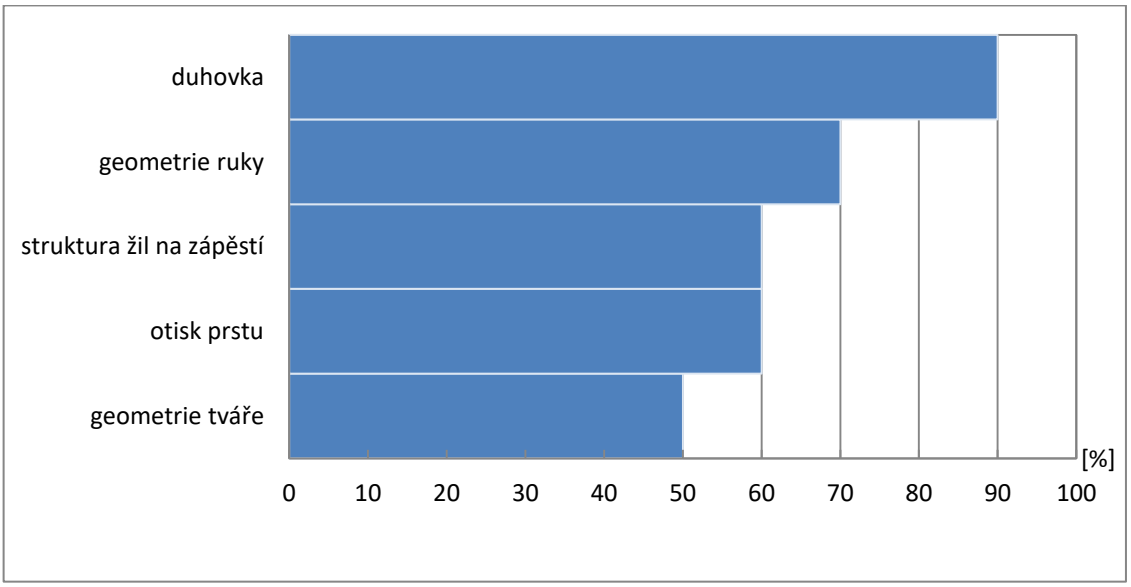
- **F** – koeficient, který vyjadřuje nejvhodnější biometrickou metodu, $F \in (0; 1>$.

- **FRR (False Rejection Rate)** – Chybné odmítnutí žadatele: Koeficient chybného odmítnutí žadatele je označován jako chyba I. druhu. Udává, s jakou pravděpodobností zařízení nerozpozná oprávněnou osobu, která má uloženou svou referenční biometrickou šablonu. Nerozpoznání uživatele způsobuje zamezení přístupu osoby, která je oprávněná, v systému registrovaná a přístup má mít povolen. Chybné odmítnutí je nežádoucí, ale tato chyba pouze snižuje komfort verifikace/identifikace a neohrožuje bezpečnost chráněného objektu.

- **FAR (False Acceptance Rate)** - Chybné přijetí žadatele: Koeficient chybného přijetí žadatele je označován jako chyba II. druhu. Udává, s jakou pravděpodobností zařízení povolí přístup osobě, která nemá v systému uloženou svou referenční biometrickou šablonu. Důvodem může být, že osoba, u níž má dojít k potvrzení identity, je mylně ztotožněna s jinou osobou, nebo je to úspěšné cílené oklamání systému pachatelem. Chybné přijetí žadatele vytváří vážné bezpečnostní riziko. [19]

- **S (Stálost biometrické vlastnosti v čase)**

  Jeden z nejdůležitějších požadavků na biometrickou vlastnost. V potřebách biometrických systémů potřebujeme také, aby sejmuté a uložené vzorky do databáze byly co nejdéle (nejlépe stále) co nejvíce aktuální. Mluvíme tedy o stálosti biometrických vlastností. Důvodů, proč se může tato vlastnost změnit je několik a to například opotřebení tkáně, vliv růstu živé tkáně, biologické stárnutí, popřípadě špína a nečistoty, zranění nebo následující hojící se rány. Nejméně ovlivnitelné biometrické vlastnosti jsou znázorněné v následujícím grafuGraf 3, z kterého lze vyčíst, že největší stálost v čase má vzorek duhovky, dosahuje 90% stálosti v čase. Z hlediska školy si zaměstnanec musí každých 10 let jít pro novou kartu. Karta platí 10 let. Proto je pro nás důležité, aby byl parametr stálý po desetiletí. [9]



Graf 3 Stálost biometrické vlastnosti v čase [8, 9]

- **N (Náklady)**

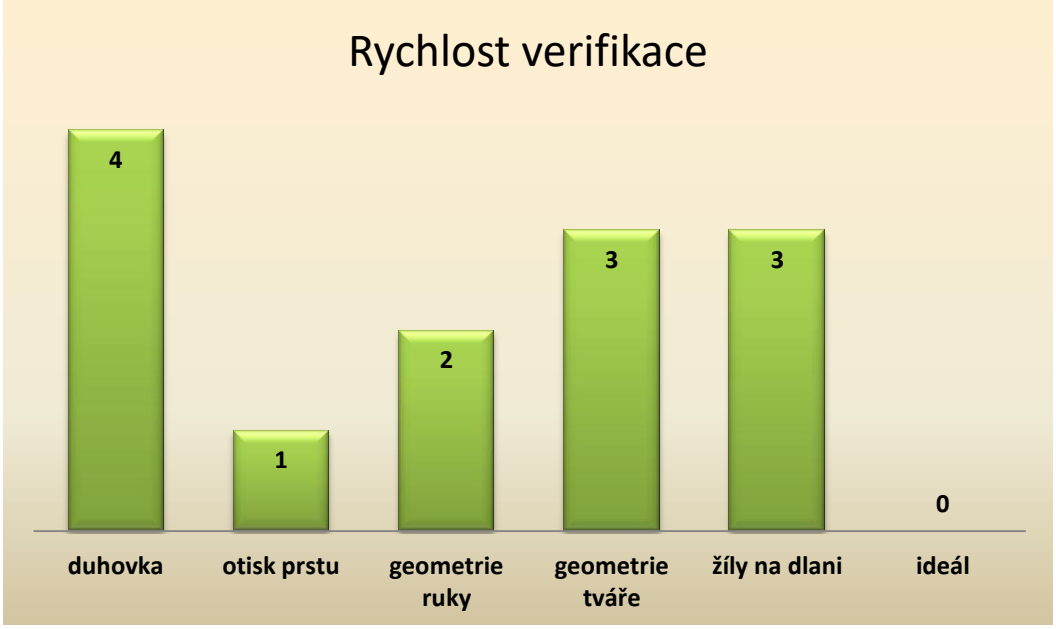
  To, co mě zajímá, je cena instalace respektive pořizovací náklady na jednu čtečku. Neuvažuji náklady na provoz, údržbu, protože jsou u jednotlivých metod srovnatelné. Instalaci také neuvažuji. Jedná se o zjednodušený model.

- **RV (Rychlost verifikace)** – Koeficient vyjádřený v sekundách. Tento koeficient ukazuje dobu potřebnou k povolení otevření dveří. Doba začíná od kontaktu člověka s biometrickou čtečkou, dále sleduje ověření identity člověka a povolení otevření dveří. [19]

Význam jednotlivých koeficientů:

- *RV = 0:* doba identifikace je rovna 0 s;
- *RV= 1:* doba identifikace je v rozmezí <0 - 1> s;
- *RV = 2:* doba identifikace je v rozmezí <1 - 2> s;
- *RV = 3:* doba identifikace je v rozmezí <2 - 3> s;
- *RV = 4:* doba identifikace převyšuje 3 s.

Na následujícím grafuGraf 4 je vidět, jak se liší koeficienty rychlosti jednotlivých metod.



Graf 4 Koeficienty rychlosti biometrických metod [zpracováno autorem]

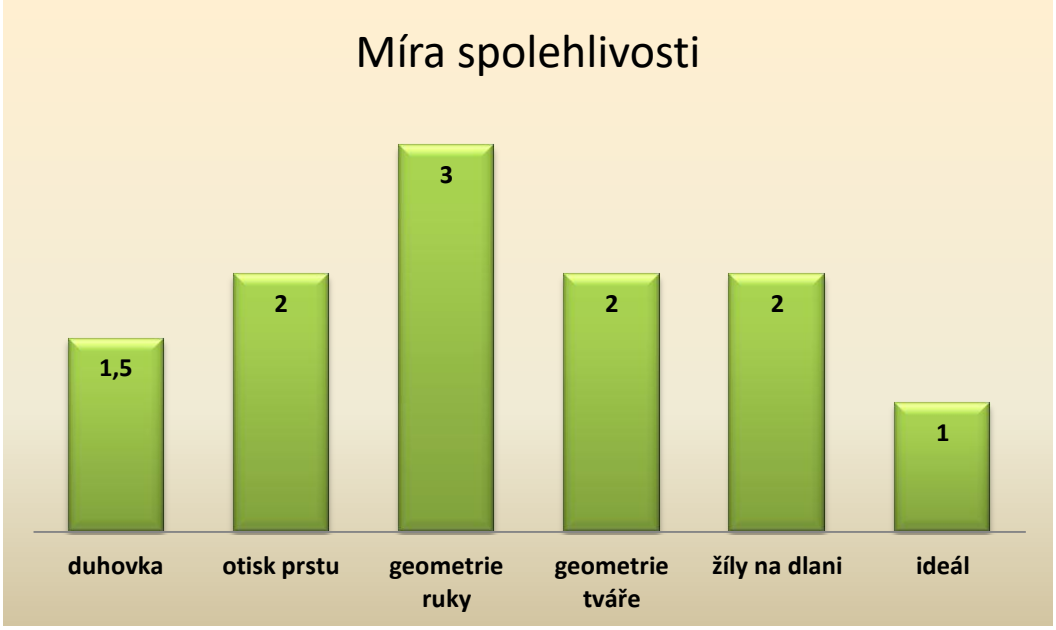
- **MS (Míra spolehlivosti)** – Koeficient založený na bezpečnosti při ověření osoby pomocí vybrané biometrické identifikační metody. Je závislý na FRR a FAR a na možnosti obejít systém. [19]

Význam jednotlivých koeficientů:

- *MS* = 1:
  - úroveň spolehlivosti vybrané metody – nejvyšší (ideální);
  - metoda – ideální.
- *MS* = 1,5:
  - úroveň spolehlivosti vybrané metody – velmi vysoká;
  - metoda – duhovka.
- *MS* = 2:
  - úroveň spolehlivosti vybrané metody – vysoká;
  - metoda – geometrie tváře, otisk prstu, žíly na dlani.
- *MS* = 3:
  - úroveň spolehlivosti vybrané metody – nízká;

- metoda – geometrie ruky.

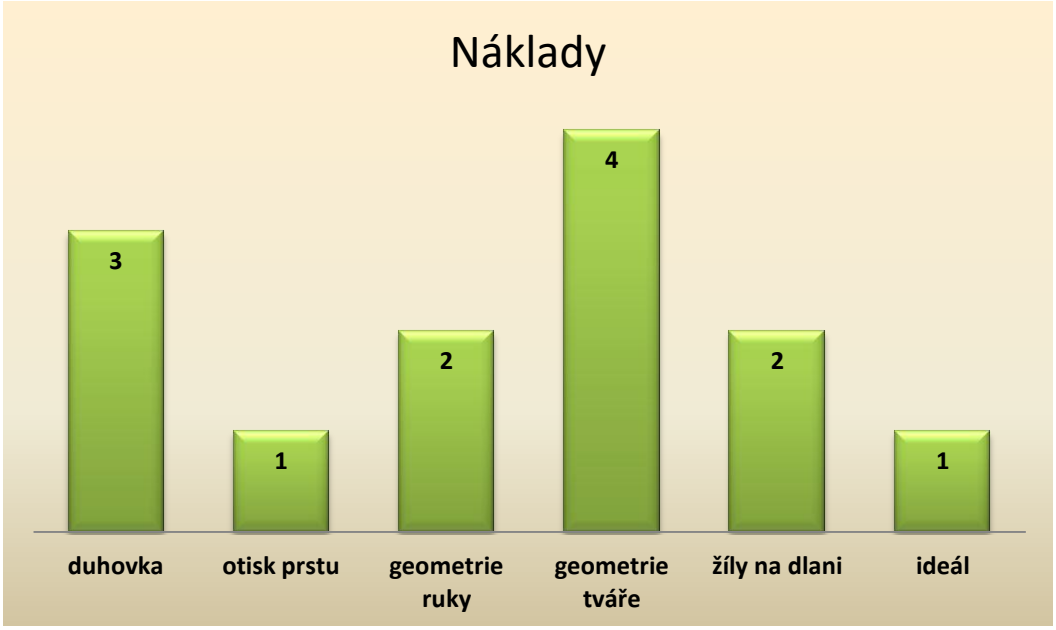
Na následujícím grafuGraf 5 je vidět, jak se liší koeficienty míry spolehlivosti jednotlivých metod.



Graf 5 Koeficienty míry spolehlivosti biometrických metod [zpracováno autorem]

- **N (Náklady) –** Pořizovací náklady na jednu čtečku, vyjádřené z aritmetického průměru několika biometrických čteček vhodných pro mou práci:
  - *N = 1:* cenová kategorie biometrických čteček dané identifikační metody je v rozmezí <0 - 15 000> Kč, metoda: otisk prstu;
  - *N = 2:* cenová kategorie biometrických čteček dané identifikační metody je v rozmezí <30 000 - 45 000> Kč, metoda: geometrie ruky, žíly na dlani;
  - *N = 3:* cenová kategorie biometrických čteček dané identifikační metody je v rozmezí <60 000 - 75 000> Kč, metoda: duhovka;
  - *N = 4:* cenová kategorie biometrických čteček dané identifikační metody převyšuje 75 000 Kč, metoda: geometrie tváře 3D.

Na následujícím grafuGraf 6 je vidět, jak se liší koeficienty nákladů jednotlivých metod.



Graf 6 Koeficienty nákladů biometrických metod [zpracováno autorem]

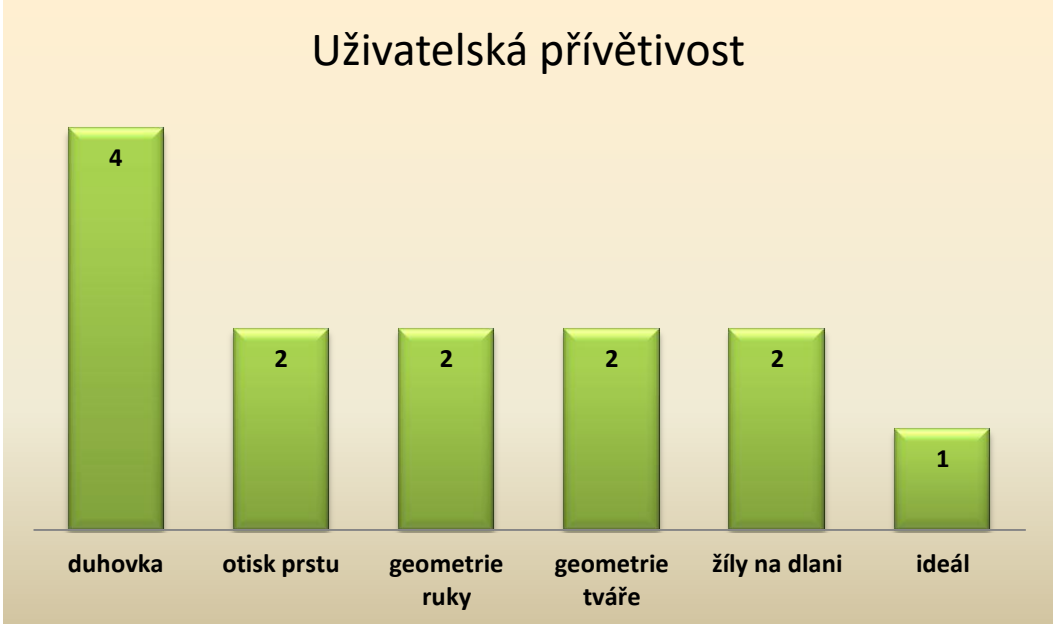
- **UP (Uživatelská přívětivost) –** Uživatelskou přívětivost posuzuji z hlediska klidné, bezbolestné a příjemné manipulace s biometrickou čtečkou

Význam jednotlivých koeficientů:

- *UP* = 1:
  - úroveň přívětivosti vybrané metody – nejvyšší (ideální);
  - metoda – ideální.

- *UP* = 2:
  - úroveň přívětivosti vybrané metody – vysoká;
  - metoda – otisk prstu, geometrie tváře 3D, geometrie ruky, žíly na dlani (nevyvolává nepříjemné pocity, nedochází k diskriminaci)

- *UP* = 4:
  - úroveň přívětivosti vybrané metody – nízká;
  - metoda – duhovka (může vyvolávat nepříjemné pocity, nutno sejmout brýle nebo kontaktní čočky)



Graf 7 Koeficienty přívětivosti biometrických metod [zpracováno autorem]

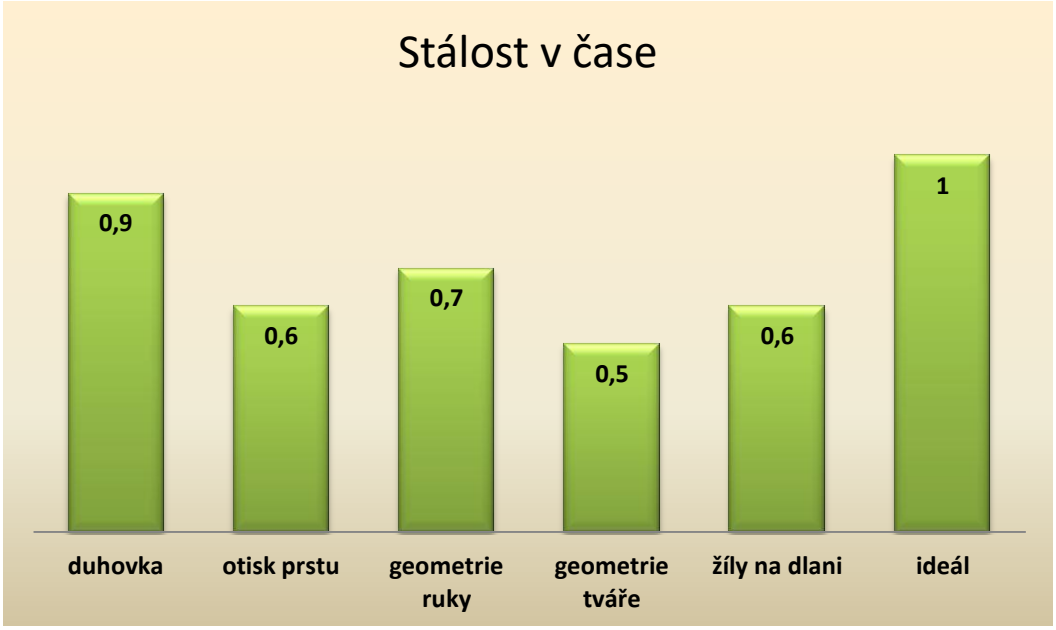
- **S (stálost v čase)**

Význam jednotlivých koeficientů:

- *S* = 0:
  - stálost vybrané metody – nejvyšší (ideální) 100%;
  - metoda – ideální

- *S* = 1:
  - stálost vybrané metody – vysoká 61-99%;
  - metoda – geometrie ruky, duhovka

- *S* = 2:
  - stálost vybrané metody – střední 30-60%;
  - metoda – geometrie tváře 3D, struktura žil, otisk prstu



Graf 8 Koeficienty stálosti v čase biometrických metod [zpracováno autorem]

V tabulce č. Tabulka 11 jsou všechny koeficienty, které jsem využil k porovnání biometrických metod pomocí vzorce.

Tabulka 11 Ohodnocení koeficientů [zpracováno autorem]

	duhovka	otisk prstu	geometrie ruky	tvář 3D	žíly na dlani	ideální metoda
FRR	0,00066	1	0,1	0,9	0,01	0
FAR	0,00078	0,0001	0,1	0,1	0,00008	0
Rychlost verifikace (RV)	3	1	2	3	3	0
Míra spolehlivosti (MS)	1,5	2	3	2	2	1
Náklady (N)	3	1	2	4	2	1
Uživatelská přívětivost (UP)	4	2	2	2	2	1
Stálost v čase (S)	0,9	0,6	0,7	0,5	0,6	1

Vyhodnocení výsledků

Viz vzorec:

$$F = 1 - \log_{10}\left(\frac{N}{UP} \times \left(\sqrt{RV^2 + MS^2 + S^2} \times \frac{1}{\sqrt{2}}\right) + (FRR + FAR)^2\right)$$

Ideální metoda:

$F = 1 - \log_{10}\left(\frac{1}{1} \times \left(\sqrt{0^2 + 1^2 + 1^2} \times \frac{1}{\sqrt{2}}\right) + (0 + 0)^2\right)$ = **1**

Duhovka:

$F = 1 - \log_{10}\left(\frac{3}{4} \times \left(\sqrt{3^2 + 1{,}5^2 + 0{,}9^2} \times \frac{1}{\sqrt{2}}\right) + (0{,}00066 + 0{,}00078)^2\right)$ = **0,73**

Otisk prstu:

$F = 1 - \log_{10}\left(\frac{1}{2} \times \left(\sqrt{1^2 + 2^2 + 0{,}6^2} \times \frac{1}{\sqrt{2}}\right) + (1 + 0{,}0001)^2\right)$ = **0,74**

Geometrie ruky:

$F = 1 - \log_{10}\left(\frac{2}{2} \times \left(\sqrt{2^2 + 3^2 + 0{,}7^2} \times \frac{1}{\sqrt{2}}\right) + (0{,}1 + 0{,}1)^2\right)$ = **0,58**

Geometrie tváře 3D:

$F = 1 - \log_{10}\left(\frac{4}{2} \times \left(\sqrt{3^2 + 2^2 + 0{,}5^2} \times \frac{1}{\sqrt{2}}\right) + (0{,}9 + 0{,}1)^2\right)$ = **0,21***

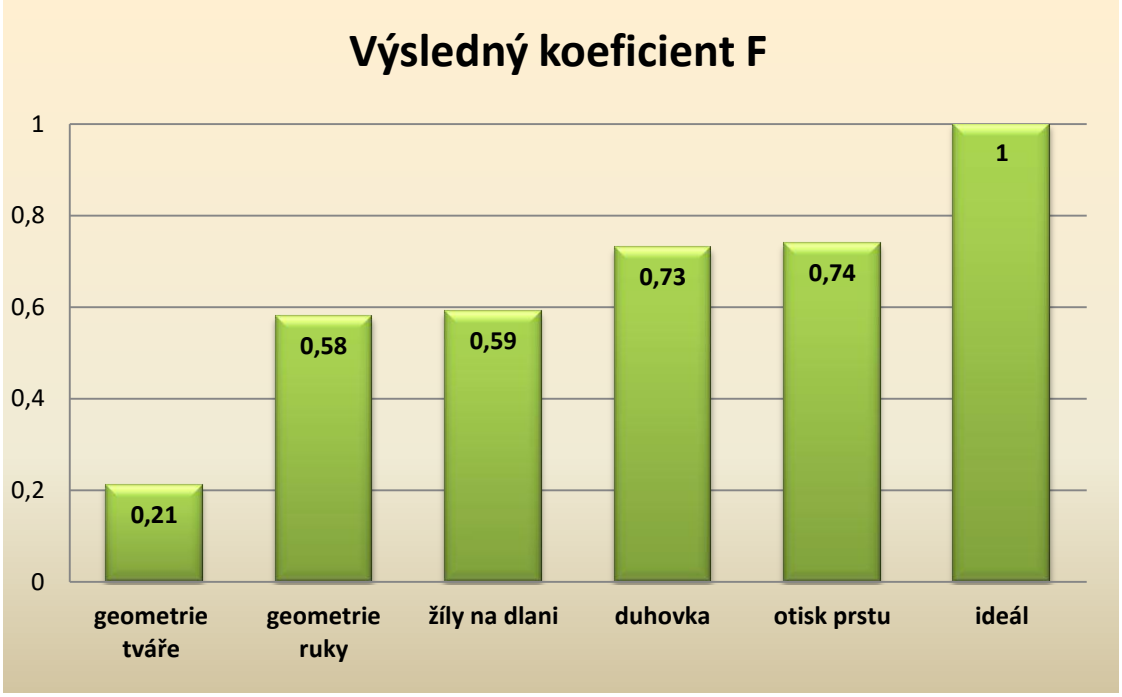
*I když je to metoda dost často používaná (letiště), navíc 3D – přesná a dobrá metoda, ale jelikož má vysoké náklady s delší dobou ověřování, tak nám vyšla nejhůře při takto stanoveném vzorci.

Žíly na dlani:

$F = 1 - \log_{10}\left(\frac{2}{2} \times \left(\sqrt{3^2 + 2^2 + 0{,}6^2} \times \frac{1}{\sqrt{2}}\right) + (0{,}01 + 0{,}00008)^2\right)$ = **0,59**

Tabulka 12 Hodnoty F pro jednotlivé biometrické metody [zpracováno autorem]

Vybraná biometrická metoda	Koeficient F
duhovka	0,73
otisk prstu	0,74
geometrie ruky	0,58
geometrie tváře 3D	0,21
žíly na dlani	0,59
ideál	1



Graf 9 Hodnoty F biometrických metod [zpracováno autorem]

Podle vzorce vychází, že nejvhodnější biometrickou identifikační metodou pro zavedení na Fakultu dopravní (případně na celé ČVUT) je metoda založená na snímání otisků prstů. Verifikace podle otisků prstů je v současnosti nejpopulárnější.

Porovnání biometrických metod pomocí přiřazení vah *w*

7.2.3. Váhy *w*

Druhou metodou, kterou budu vyhodnocovat ideální biometrickou metodu, bude přiřazení vah, viz tabulka č. Tabulka 13.

Největší váhu jsem přiřadil **rychlosti verifikace (RV)**, která je zásadní pro pohodlné a rychlé ověřování velkého množství lidí a stejnou váhu přikládám také pro **náklady (N)**, jelikož si škola nemůže dovolit nejdražší technologie, tudíž hledáme kompromis mezi přijatelnou cenou a kvalitou.

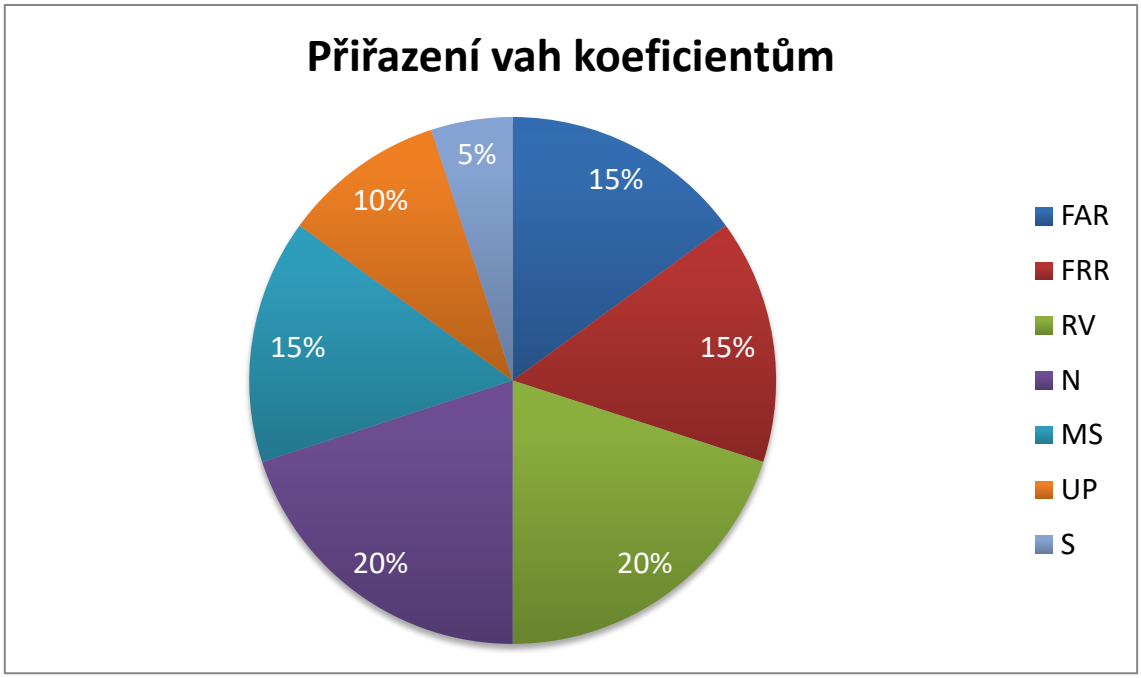
O něco nižší váhu, která je ale neméně důležitá než předešlé dávám pro **míru spolehlivosti (MS)**, která je důležitá z hlediska bezpečnosti i správnému porovnávání lidí a předpokládám, že nikdo z akademických pracovníků nebude chtít systém nějakým způsobem obejít.

Čtvrté místo patří **uživatelské přívětivosti (UP)**, jelikož chci, aby se uživatel při verifikaci cítil bezpečně a pohodlně. Každý také není zvyklý si denně přikládat a skenovat prst, či duhovku…

Na poslední místo přikládám vlastnost **stálost v čase (S)**. Vycházím z pohledu studenta, který chce školu dokončit a pak si najít práci, proto už jeho biometrické údaje nebude třeba uchovávat. Časový horizont je kolem 6 let.

Tabulka 13 Hodnoty vah pro jednotlivé koeficienty [zpracováno autorem]

Koeficient	Váha w
FAR	15%
FRR	15%
RV	20%
N	20%
MS	15%
UP	10%
S	5%



Graf 10 Váhy jednotlivých koeficientů [zpracováno autorem]

Pro ideál zvolím 100%. Právě pro zjištění % podílu každého koeficientu pro danou metodu musím stanovit 100%. V tabulce č.Tabulka 11 se u ideální metody vyskytují také nuly, abych zamezil tomu, aby byla váha nulová, tak jsem nahradil nulu vhodnou malou kladnou konstantou ε. Přičítám číslo 1. Po přičtení tohoto koeficientu se tabulka změní na:

Tabulka 14 Přepočet koeficientů [zpracováno autorem]

	duhovka	otisk prstu	geometrie ruky	tvář 3D	žíly na dlani	ideální metoda
FRR	1,00066	2	1,1	1,9	1,01	1
FAR	1,00078	1,0001	1,1	1,1	1,00008	1
Rychlost verifikace (RV)	4	2	3	4	4	1
Míra spolehlivosti (MS)	2,5	3	4	3	3	2
Náklady (N)	4	2	3	5	3	2
Uživatelská přívětivost (UP)	5	3	3	3	3	2
Stálost v čase (S)	1,9	1,6	1,7	1,5	1,6	2

Výpočet F‘:

$$FRR' = \frac{FRR_{ideál}}{FRR},\ FAR' = \frac{FAR_{ideál}}{FAR},\ RV' = \frac{RV_{ideál}}{RV},\ MS' = \frac{MS_{ideál}}{MS},\ N' = \frac{N_{ideál}}{N},\ UP' = \frac{UP_{ideál}}{UP},\ S' = \frac{S_{ideál}}{S}$$

Dále budu násobit F‘ váhami, které jsem si určil.

$$F' = FRR' * w(FRR) + FAR' * w(FAR) + RV' * w(RV) + MS' * w(MS) + N' * w(N) + UP' * w(UP) + S' * w(S)$$

Duhovka:

$$FRR' = \frac{FRR_{ideál}}{FRR} = \frac{1}{1{,}00066} \cong 1$$

$$FAR' = \frac{FAR_{ideál}}{FAR} = \frac{1}{1{,}00078} \cong 1$$

$$RV' = \frac{RV_{ideál}}{RV} = \frac{1}{4} = 0{,}25$$

$$MS' = \frac{MS_{ideál}}{MS} = \frac{2}{2{,}5} = 0{,}8$$

$$N' = \frac{N_{ideál}}{N} = \frac{2}{4} = 0{,}5$$

$$UP' = \frac{UP_{ideál}}{UP} = \frac{2}{5} = 0{,}4$$

$$S' = \frac{S_{ideál}}{S} = \frac{2}{1{,}9} \cong 1{,}05$$

Vyhodnocení:

F_D' *= 1*15+1*15+0,25*20+0,8*20+0,5*15+0,4*10+1,05*5 = 67,75 =* ***0,68***

Otisk prstu:

$$FRR' = \frac{FRR_{ideál}}{FRR} = \frac{1}{2} = 0{,}5$$

$$FAR' = \frac{FAR_{ideál}}{FAR} = \frac{1}{1{,}0001} \cong 1$$

$$RV' = \frac{RV_{ideál}}{RV} = \frac{1}{2} = 0{,}5$$

$$MS' = \frac{MS_{ideál}}{MS} = \frac{2}{3} \cong 0{,}67$$

$$N' = \frac{N_{ideál}}{N} = \frac{2}{2} = 1$$

$$UP' = \frac{UP_{ideál}}{UP} = \frac{2}{3} \cong 0{,}67$$

$$S' = \frac{S_{ideál}}{S} = \frac{2}{1{,}6} \cong 1{,}25$$

Vyhodnocení:

F_O' *= 0,5*15+1*15+0,5*20+0,67*20+1*15+0,67*10+1,25*5 = 73,85 =* ***0,74***

Geometrie ruky:

$$FRR' = \frac{FRR_{ideál}}{FRR} = \frac{1}{1{,}1} \cong 0{,}91$$

$$FAR' = \frac{FAR_{ideál}}{FAR} = \frac{1}{1{,}1} \cong 0{,}91$$

$$RV' = \frac{RV_{ideál}}{RV} = \frac{1}{3} \cong 0{,}33$$

$$MS' = \frac{MS_{ideál}}{MS} = \frac{2}{4} = 0{,}5$$

$$N' = \frac{N_{ideál}}{N} = \frac{2}{3} \cong 0{,}67$$

$$UP' = \frac{UP_{ideál}}{UP} = \frac{2}{3} \cong 0{,}67$$

$$S' = \frac{S_{ideál}}{S} = \frac{2}{1{,}7} \cong 1{,}18$$

Vyhodnocení:

*F_G' = 0,91*15+0,91*15+0,33*20+0,5*20+0,67*15+0,67*10+1,18*5 = 66,55=* ***0,67***

Tvář 3D:

$$FRR' = \frac{FRR_{ideál}}{FRR} = \frac{1}{1{,}9} \cong 0{,}53$$

$$FAR' = \frac{FAR_{ideál}}{FAR} = \frac{1}{1{,}1} \cong 0{,}91$$

$$RV' = \frac{RV_{ideál}}{RV} = \frac{1}{4} = 0{,}25$$

$$MS' = \frac{MS_{ideál}}{MS} = \frac{2}{3} \cong 0{,}67$$

$$N' = \frac{N_{ideál}}{N} = \frac{2}{5} = 0{,}4$$

$$UP' = \frac{UP_{ideál}}{UP} = \frac{2}{3} \cong 0{,}67$$

$$S' = \frac{S_{ideál}}{S} = \frac{2}{1{,}5} \cong 1{,}33$$

Vyhodnocení:

*F_T' = 0,53*15+0,91*15+0,25*20+0,67*20+0,4*15+0,67*10+1,33*5 = 59,35=* ***0,59***

Žíly na dlani:

$$FRR' = \frac{FRR_{ideál}}{FRR} = \frac{1}{1{,}01} \cong 0{,}99$$

$$FAR' = \frac{FAR_{ideál}}{FAR} = \frac{1}{1{,}00008} \cong 1$$

$$RV' = \frac{RV_{ideál}}{RV} = \frac{1}{4} = 0{,}25$$

$$MS' = \frac{MS_{ideál}}{MS} = \frac{2}{3} \cong 0{,}67$$

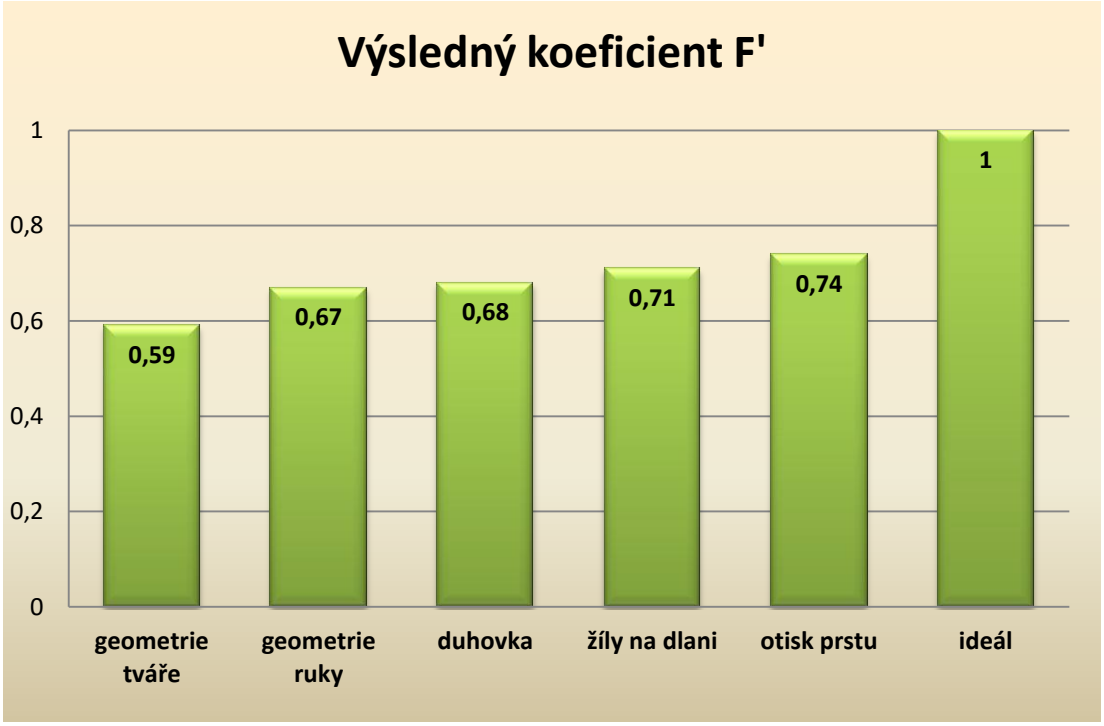
$$N' = \frac{N_{ideál}}{N} = \frac{2}{3} \cong 0{,}67$$

$$UP' = \frac{UP_{ideál}}{UP} = \frac{2}{3} \cong 0{,}67$$

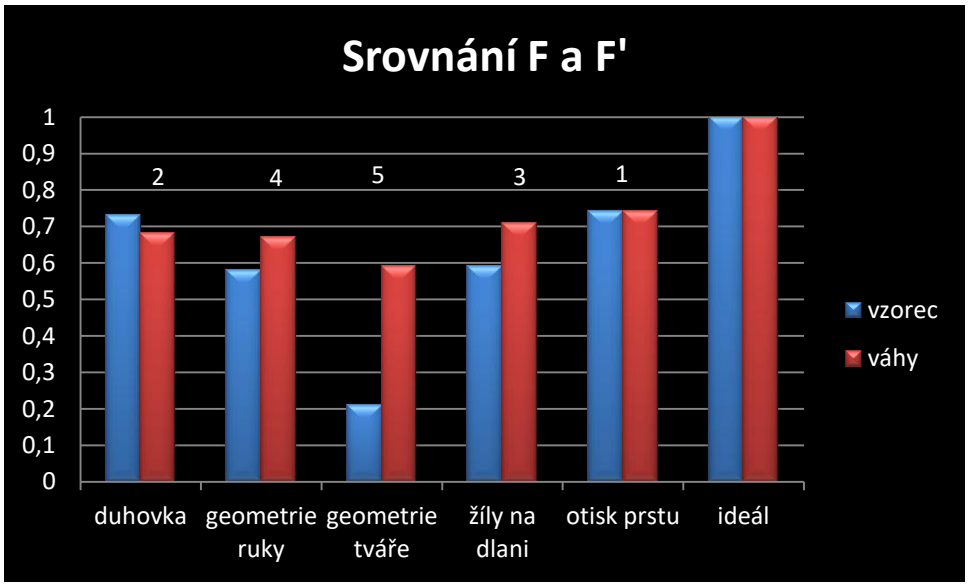
$$S' = \frac{S_{ideál}}{S} = \frac{2}{1{,}6} = 1{,}25$$

Vyhodnocení:

$F_Ž'$ = *0,99*15+1*15+0,25*20+0,67*20+0,67*15+0,67*10+1,25*5 = 71,25 =* ***0,71***



Graf 11 Hodnoty F‘ biometrických metod [zpracováno autorem]



Graf 12 Srovnání výsledků dle vzorce a dle vah [zpracováno autorem]

7.3. Výběr optimální varianty

Podle toho, co mi vyšlo z pohledu vzorce a vah, bych pro Fakultu dopravní potažmo celé ČVUT zvolil biometrickou metodu otisku prstu, kde je nejnižší pořizovací cena čtečky a celkově se tato metoda nejvíce blíží ideálu, který hledám (viz graf 12). Také je to metoda, která zajistí požadovanou bezpečnost, a rychlost verifikace je ideální pro akademické prostředí.

Samozřejmě je těžké definovat optimální biometrickou metodu. V poměru cena a přesnost vychází nejlépe otisk prstu. Na druhém místě vyšla duhovka oka, která má vysoké hodnocení ve všech kategoriích v případě, že cena nehraje roli. Tato biometrická metoda je na tom velmi dobře co se do přesnosti a stupně zabezpečení týče. V případě tváře je tu do značné míry patrná ještě jistá neschopnost absolutního stanovení markantních bodů, které by se v čase neměnily a byly pokud možno absolutní. Geometrie ruky nevyšla dobře, protože je vysoce nespolehlivá, má nízkou úroveň miniaturizace a malý rozsah potenciálního nasazení v praxi. Na posledním místě se umístila geometrie tváře 3D, o které jsem se již zmiňoval.

8. Závěr

Na základě vyhodnocení praktické části bakalářské práce navrhuji pro fakultu dopravní a celé ČVUT biometrickou metodu otisk prstu, která vyšla při testování jako nejpřívětivější. Myslím si, že je v dnešní době důležité mít zabezpečeny místnosti pomocí biometrie, což je jakási přidaná bezpečnostní hodnota pro vstup do laboratoří a podobných místností na škole. Dále je důležité říci, že bylo potřeba zjistit, do kterých laboratoří a výzkumných pracovišť biometrickou metodu zavedu. Kvůli tomu jsem potřeboval znát laboratoře a výzkumná pracoviště, která skutečně fyzicky sídlí na fakultě. Tuto informaci mi poskytli vedoucí těchto místností.

Na začátku práce jsem vytipoval, popsal a analyzoval 5 vybraných biometrických metod, se kterými jsem v další části pracoval.

Porovnal jsem je pomocí vzorce a vah. Vzorec jsem vymyslel díky matematickým znalostem a také mnoha pokusy. Ve vzorci se pracuje se 7 koeficienty pro každou z biometrických metod. Tyto koeficienty byly zjištěny pomocí ověřených zdrojů literatury. Pomocí vzorce bylo zjištěno, že nejpřívětivější metodou je metoda otisku prstu.

Pro druhé porovnání jsem si vybral přiřazení vah. Vycházel jsem ze stejných koeficientů jako při práci se vzorcem, ale potom jsem je musel přepočítat. Koeficientům jsem přidělil důležitost – váhy. Dále jsem zjistil procentuální podíl koeficientů pro danou metodu v závislosti na koeficientech ideální metody. F‘ jsem zjistil tak, že jsem sečetl všechny přepočtené koeficienty vynásobené váhami. Dospěl jsem ke stejnému výsledku jako při pomocí vzorce, což jsem ani nepředpokládal.

Jak to bude celé řešeno? Na ID kartě nebude přímo otisk prstu, bude tam fingerprint_cod. Po přiložení prstu ke čtečce čtečka také vypočítá kód, podívá se, jaký kód je na kartě a algoritmem porovná tyto dva kódy. Poté dá rozhodnutí – vstup povolen/nepovolen. Nebude to tedy zneužitelné, otisk bude pouze v databázi ČVUT (ale ani tam být nemusí).

Také je důležité říci, že v dnešní době už je zcela běžné mít dvoufaktorové ověřování. I na sociálních sítích je kromě hesla i ověření pomocí tel. čísla. Ať to jsou sociální sítě, bankomaty, vstupy do smartphonů na základě biometrie a kódu.

Analýza společnosti IHS Markit předpovídá, že příští rok masivně stoupne počet zařízení, které budou disponovat čtečkou otisků prstů v displeji. Zatímco dnes jde stále o rarity, příští rok budou takové mobily celkem běžnou záležitostí. [23]

Jelikož se spousta věcí automatizuje a lidé se stávají samostatnými jednotkami, které se chtějí pohybovat samostatně, a aby jim to bylo umožněno, tak je vhodná právě zmíněná dvoufaktorová autentizace, která nabývá na významu. Nechceme šikanovat studenty, chceme, aby se mohli pohybovat samostatně a i z hlediska ochrany majetku je zmíněná autentizace ideální. V našem případě biometrický applet + čip.

Věřím, že tyto poznatky a navržená řešení použiji i ve své další práci.

9. Seznam použité literatury

[1] Biometrie otisku prstu. *Biometric Line* [online], [cit. 2017-09-03]. Dostupný z: http://www.biometricke-ctecky.cz/produkty/ctecky-otisku-prstu/

[2] FLÍDR, Jakub. *Biometrické autentizační metody*: *bakalářská práce*. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, 2009. 50. Vedoucí bakalářské práce Ing. Jiří Sobotka

[3] Skenery oční duhovky v CERNu [online], Dostupný z: http://www.biometricke-ctecky.cz/aktuality/skenery-ocni-duhovky-v-cernu/

[4] Posterus. Portál pre odborné publikovanie. *Sulovská, Kateřina* [online]. [cit. 2017-09-03]. Dostupný z: http://www.posterus.sk/?p=11511

[5] Biometrické systémy v praxi. *Pužmanová, Rita.* [online]. [cit. 2017-09-07]. Dostupný z: https://www.systemonline.cz/clanky/biometricke-systemy-v-praxi.htm

[6] Technologie žil hřbetu / dlaně ruky. *Dobiáš, Richard, Hirš, Petr.* [online]. [cit. 2018-02-28]. Dostupný z: http://www.biometricke-systemy.cz/

[7] ŠTĚDROŇ, Bohumír, Petr MOOS, Marcela PALÍŠKOVÁ, Otto PASTOR, Miroslav SVÍTEK a Libor SVOBODA. *Manažerské rozhodování v praxi*. Přeložil Jiří HANDLÍŘ. V Praze: C.H. Beck, 2015. Beckova edice ekonomie. ISBN 978-80-7400-587-9.

[8] ŠČUREK, R. *Biometrické technologie - technické prostředky bezpečnostních služeb.* VŠB TU Ostrava, Fakulta bezpečnostního inženýrství, Katedra bezpečnostních služeb. Ostrava: VŠB TU Ostrava, 2015, 1. vydání. 115 stran. ISBN 978-80-248-3786-4. Dostupný z: https://www.fbi.vsb.cz/export/sites/fbi/060/.content/sys-cs/resource/PDF/BiometrickeTechnologie.pdf

[9] ŠČUREK, R. *Biometrické metody identifikace osob v bezpečnostní praxi*. VŠB TU Ostrava, Fakulta bezpečnostního inženýrství, Katedra bezpečnostního managementu, Oddělení bezpečnosti osob a majetku [online]. 2008 [cit. 2017-03-08]. Dostupný z: http://www.fbi.vsb.cz/shared/uploadedfiles/fbi/biometricke_metody.pdf

[10] Artec ID. Dostupný z: https://www.artecid.com/

[11] VYORAL, Pavel. *Identifikační biometrické systémy*: *bakalářská práce*. Zlín: Univerzita Tomáše Bati ve Zlíně, Fakulta aplikované informatiky, 2011. 66. Vedoucí bakalářské práce

Ing. Milan Navrátil, Ph.D. [online]. Dostupný z: http://docplayer.cz/39469507-Identifikacni-biometricke-systemy.html

[12] Průkazy ČVUT. Dostupný z: https://portal.cvut.cz/

[13] RAK, R.; MATYÁŠ, V.; ŘÍHA, Z., a kol. *Biometrie a identita člověka ve forenzních a komerčních aplikacích*. Praha: GRADA, 2008, ISBN 978-80-247-2365-5.

[14] HOLENDA, M., VANĚK, T., ROHLÍK M. *Klonování RFID čipů na přístupových kartách* [online]. [cit. 2018-03-30]. Dostupný z: http://access.feld.cvut.cz/view.php?cisloclanku=2012070003

[15] KUČEROVÁ, VLADIMÍRA, VONDRÁKOVÁ, ANDREA. *My jsme ČVUT* [online]. Praha: České vysoké učení technické, 2017, s. 60 [cit. 2018-04-30]. Dostupný z: https://www.media.cvut.cz/cs/publikace/20171017-my-jsme-cvut-2017#page/62. ISBN 978-80-01-06334-7.

[16] KUBÁT, Zbyšek. *Čipový přístupový systém*: *středoškolská práce*. Praha: Střední průmyslová škola elektrotechnická, 2013. 59. Vedoucí práce Ing. Vladimír Beránek. [online]. Dostupný z: http://www1.fs.cvut.cz/stretech/2013/sbornik_2013/84.pdf

[17] iCAM7 series. Dostupný z: http://www.irisid.com/productssolutions/hardwareproducts/icam7-series/

[18] ZEMAN, Tomáš. *Aplikace biometrických systémů*: *bakalářská práce*. Praha: Bankovní institut vysoká škola Praha, Katedra matematiky, statistiky a informačních systémů, 2011. 52. Vedoucí bakalářské práce Mgr. Miroslav Široký, DiS. [online]. Dostupný z: http://docplayer.cz/5456127-Aplikace-biometrickych-systemu.html

[19] AUSHEV, Murad. *Návrh implementace identifikačního systému pro přístupové systémy ČVUT*: *bakalářská práce*. Praha: České vysoké učení technické, Fakulta dopravní v Praze, 2016. 70. Vedoucí bakalářské práce Ing. Jana Kaliková, Ph.D.

[20] *RFID DESFire EV1 - jedna karta pro více aplikací*. [online]. 2012, [cit. 2018-06-18]. Dostupný z: http://www.soselectronic.cz/articles/no-name/rfid-desfire-ev1-jedna-karta-pro-vice-aplikaci-1192

[21] VALER Tomáš. *Biometrická bezpečnost* [online]. Dostupný z: http://www.abbas.cz/clanky/recenze-technika/biometricka-bezpecnost/

[22] Lumidigm V-Series V302 IP65. Dostupný z: https://www.fulcrumbiometrics.com/Lumidigm-V-Series-V302-p/101170.htm

[23] Příští rok už budete odemykat smartphony otiskem prstu přes displej. [online]. 2018, [cit. 2018-06-18]. Dostupný z: https://mobil.idnes.cz/100-milionu-smartphonu-2019-ctecka-v-displeji-displej-fvq-/mob_tech.aspx?c=A180427_131325_mob_tech_oma

[24] PODIVÍN Milan. *PalmSecure – Biometric Technology Vaše ruka je klíčem.* [online]. 2013, [cit. 2018-06-18]. Dostupný z: https://www.isss.cz/archiv/2014/download/prezentace/fujitsu_podivin.pdf

[25] TROUSIL Pavel. *PalmSecure – identifikace osob pomocí obrazu krevního řečiště* [online]. 2014, [cit. 2018-06-19]. Dostupný z: https://www.chip.cz/novinky/palmsecure-identifikace-osob-pomoci-obrazu-krevniho-reciste/

[26] VALER Tomáš. *Biometrie na dosah* [online]. Dostupný z: http://www.abbas.cz/clanky/recenze-technika/biometrie-na-dosah/

[27] Granus s.r.o., *Biometrická čtečka ruky* [online]. Dostupný z: https://dodavatele.epoptavka.cz/70421-granus-s-r-o/nabidka/31845-biometricka-ctecka-ruky

[28] Vydavatelství průkazů ČVUT. Dostupný z: https://portal.cvut.cz/pristup-do-is/uzivatele-a-pristup-do-is-cvut/vydavatelstvi-prukazu/

[29] Moderní metody optimalizace. *Multikriteriální optimalizace*. [online], [cit. 2018-07-18]. Dostupný z: http://mech.fsv.cvut.cz/~leps/teaching/mmo/prednasky/prednaska10_MO.pdf

Seznam obrázků

Seznam tabulek

Seznam grafů