Návrh mechatronických systémů pro přístup do nájemních bytů

Ladislav Martinek

Bakalářská práce
2022

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav bezpečnostního inženýrství

Akademický rok: 2021/2022

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Ladislav Martinek**
Osobní číslo:	**A19668**
Studijní program:	**B3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**Prezenční**
Téma práce:	**Návrh mechatronických systémů pro přístup do nájemních bytů.**
Téma práce anglicky:	**Design of Mechatronic Systems for Access into Rental Apartments**

Zásady pro vypracování

1. Popište současné zabezpečení vstupu do nájemních bytů.
2. Zpracujte rešerši technických prostředků pro zabezpečení vstupu.
3. Proveďte analýzu mechatronických klik.
4. Zpracujte standardy pro mechatronické systémy.
5. Vyhodnoťte spolehlivost mechatronických systémů, využívajících biometrické prvky.
6. Navrhněte vlastní řešení zabezpečení vstupu.
7. Odhadněte další vývoj těchto systémů.

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

Seznam doporučené literatury:

1. RAK, Roman, Vašek MATYÁŠ a Zdeněk ŘÍHA. Biometrie a identita člověka ve forenzních a komerčních aplikacích. Praha: Grada, 2008. Profesionál. ISBN 978-80-247-2365-5./
2. LUKÁŠ, Luděk. Bezpečnostní technologie, systémy a management. Zlín: Radim Bačuvčík – VeRBuM, 2015. ISBN 978-80-87500-05-7./
3. KYNCL, Jaromír. Bezpečnost objektu ve světle moderních technologií. Praha: Komora podniků komerční bezpečnosti České republiky, 2014. ISBN 978-80-260-7115-0./
4. IVANKA, Ján. Systemizace bezpečnostního průmyslu I. Vyd. 3. Zlín: Univerzita Tomáše Bati ve Zlíně, 2009. ISBN 978-80-7318-850-4./
5. BASTIAN, Hans-Werner. Bezpečný dům a byt: ochrana před vloupáním, požárem a škodami způsobenými vodou. Praha: Beta, 2004. ISBN 80-7306-171-6./

Vedoucí bakalářské práce: **Ing. Rudolf Drga, Ph.D.**
Ústav bezpečnostního inženýrství

Datum zadání bakalářské práce: **17. ledna 2022**
Termín odevzdání bakalářské práce: **31. května 2022**

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

doc. Mgr. Milan Adámek, Ph.D. v.r.
děkan

Ing. Jan Valouch, Ph.D. v.r.
ředitel ústavu

Ve Zlíně dne 17. ledna 2022

Prohlašuji, že

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

Prohlašuji,

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

Ve Zlíně, dne 30. 05. 2022

Ladislav Martinek v. r.
podpis studenta

ABSTRAKT

Bakalářská práce se zabývá biometrií a užití v zabezpečení vstupů. Teoretická část je zaměřena na biometrii a užití biometrických prvků v komerčních bezpečnostních aplikacích, možnosti zabezpečení vstupu a jaké normy se aplikují pro mechatronické systémy v zabezpečení vstupu. Praktická část se zajímá vyhodnocením spolehlivosti biometrických systému v mechatronickém systému, současným zabezpečením vstupů nájemních bytů a budoucností biometrických a mechatronických systémů. Výsledkem je návrh zabezpečení nájemních bytů s využitím mechatronických systémů s biometrickou čtečkou.

Klíčová slova: biometrie, biometrický systém, otisk prstu, zabezpečení vstupu, mechatronický systém

ABSTRACT

Bachelor thesis deals with biometrics and use of biometrics in entrance security. The theoretical part is focused on biometrics and use of biometrics in commercial security applications, entrance security options and what standards apply to mechatronic systems for entrance security. The practical part is focused on evaluation of reliability of biometric systems used in mechatronic system, current state of entrance security for rental apartments and future of biometrical and mechatronic systems. Result is security design for entrance security of rental apartments with use of mechatronic systems with biometric reader.

Keywords: biometrics, biometrical system, fingerprint, entrance security, mechatronic system

Děkuji panu Ing. Rudolfu Drgovi, Ph. D. za poskytnuté prostředky a rady při vedení mé bakalářské práce. Chtěl bych také poděkovat svým rodičům a sestře za podporu během celého studia.

Prohlašuji, že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

OBSAH

ÚVOD **9**
I TEORETICKÁ ČÁST **10**
1 BIOMETRIE **11**
1.1 BIOMETRICKÉ PRVKY 12
1.1.1 Otisk prstu 14
1.1.2 Obličej 19
1.1.3 Oční duhovka 22
1.2 UŽITÍ V BEZPEČNOSTNÍCH APLIKACÍCH 23
1.2.1 Otisk prstu 23
1.2.2 Obličej 26
1.2.3 Oční duhovka 27
2 ZABEZPEČENÍ VSTUPU **28**
2.1 PROSTŘEDKY 28
2.1.1 Zabezpečení stavebních prvků 28
2.1.2 Mechanické zábranné systémy 29
2.1.3 Prvky plášťové ochrany 33
2.1.4 Kamery 34
3 MECHATRONICKÉ SYSTÉMY **35**
3.1 NORMY ZASTŘEŠUJÍCÍ MECHATRONICKÉ SYSTÉMY 35
II PRAKTICKÁ ČÁST **37**
4 SPOLEHLIVOST BIOMETRICKÉHO SYSTÉMU V MECHATRONICKÉM SYSTÉMU **38**
4.1 VÝSLEDKY 39
5 SOUČASNÉ ZABEZPEČENÍ VSTUPU NÁJEMNÍCH DOMŮ A BYTŮ **44**
5.1 NEDOSTATKY VSTUPŮ 44
6 NÁVRH ZABEZPEČENÍ VSTUPU BYTŮ **46**
6.2 PŘEHLED, POPIS, ZDŮVODNĚNÍ A CENA POUŽITÝCH KOMPONENTŮ 46
6.2.1 FAB 4292 47
6.2.2 Oboustranná cylindrická vložka FAB 3 48
6.2.3 Richter Czech Smart Handle H.03 48
6.2.4 Cena návrhu 58
7 BUDOUCNOST BIOMETRICKÝCH A MECHATRONICKÝCH SYSTÉMŮ **59**
7.1 BUDOUCNOST MECHATRONICKÝCH SYSTÉMŮ 59
ZÁVĚR **60**
SEZNAM POUŽITÉ LITERATURY **61**
SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK **63**

SEZNAM OBRÁZKŮ 64
SEZNAM TABULEK 65

ÚVOD

Biometrie se v dnešní době nachází všude okolo nás, pouze ji neregistrujeme. Ať už se jedná o přístup do telefonu přes otisk prstu či obličej, fotku na občanském nebo řidičském průkazu, vždy prokazujeme svoji identitu přes specifickou, unikátní součást naší osoby.

V teoretické části práce jsem se zaměřil na objasnění biometrie a biometrických systémů. V případě biometrických systémů se budu snažit objasnit výhody a nevýhody s nimi spojené a v jakých stavech pracují. Následují biometrické prvky, jež mohou být užívané při identifikaci osoby; zaměřím se hlavně na popsání nejužívanějších a nejspolehlivějších prvků. Jedním z hojně používaných identifikačních prvků je otisk prstu, kde se budu chtít zaměřit na popsání nahodilých, detailních identifikačních prvků a strojového zpracování otisku. Obličej je stále více využívaný v automatizované identifikaci. Oční duhovka je prohledávaná alternativa pro identifikaci, proto bych chtěl zjistit proč. Komerční bezpečnostní aplikace využívající otisk prstu, obličej i oční duhovka budou též probírány.

Dále jsou probírány možnosti, jak zabezpečit vstup před násilným vniknutím, či vyhlášení poplachu, když dojde k násilnému vniknutí. Kupříkladu možnosti zabezpečení stavebních otvorů, užití mechanických zábranných systémů a prvků plášťové ochrany, či kamer pro dohled. Mechatronické systémy a normy, které je zastřešují budou probírány v dalších částech.

Praktická část bakalářské práce bude zaměřena na zjištění spolehlivosti biometrické čtečky u mechatronických systémů. Cílem bude zjistit, s jakou spolehlivostí odolávají neznámým uživatelům a jak citlivé jsou. Dále bude zjišťováno, jak zabezpečené jsou vstupy nájemních domů a bytů.

V poslední části bude jeden z možných návrhů na zlepšení zabezpečení vstupu pro nájemní byty s užitím mechatronického systému v kombinaci s biometrickou čtečkou.

I. TEORETICKÁ ČÁST

1 BIOMETRIE

Biometrie je obor zabývající se zkoumáním a praktickým využitím identifikace člověka na základě měřitelnosti jedinečné biologické, či fyziologické charakteristiky. [1] V dnešní době vidíme aplikaci biometrie všude kolem sebe. Používá se k ochraně osob a majetku, zajištění vnitřní bezpečnosti, ověření identity osob na hranicích, ale i v každodenním životě, například při odemykání telefonu.

Značnou výhodou biometrických systémů, systémů využívajících biometrie pro verifikaci, identifikaci a autorizaci, je jednoduchost jejich užívání. Pokud budeme mluvit o otisku prstu, tak stačí pouze správně přiložit prst a zařízení či dveře se otevřou.

Další výhody biometrických systémů:

- nelze zapomenout či ztratit přístupový prvek:
    - Oproti heslům, či klíčům nelze biometrický prvek ztratit, jelikož osoba ho vždy má na sobě.
- těžké, téměř nemožné napodobit přístupový prvek:
    - Velice náročné vytvořit napodobeninu, která by mohla překonat biometrický systém.
- nepřenositelnost přístupového prvku:
    - Osoba ho má vždy při sobě a nemůže ho předat jinému subjektu.
- vysoká přesnost a rychlost identifikace:
    - Díky pokroku v technologii jsou biometrické systémy schopny identifikovat známou osobu téměř okamžitě. [1]

Nevýhody biometrických systémů:

- nutnost napájení:
    - Aby zůstaly funkční, musí biometrické systémy být neustále napájeny.
- nemožnost používat systém hned:
    - Biometrický systém musí mít šablonu, aby mohl porovnávat s nasnímaným biometrickým prvkem a následně určit, jestli se jedná o osobu známou, či neznámou.

- nutnost ukládání dat:
    - Vytvořené šablony musí být uloženy v paměti zařízení nebo v databázi, aby biometrický systém mohl být dlouhodobě používán.
- cena:
    - Biometrické systémy bývají dražší na pořízení než konvenční systémy.

Jak již bylo zmíněno, je nutné, aby biometrický systém měl předpřipravenou šablonu pro uživatele. Biometrické systémy pracují se šablonami ve třech stavech a to: Verifikace, Identifikace, Autentizace. [1]

Verifikace znamená, že se musí uživatel přihlásit do systému (například pomocí uživatelského jména a hesla, nebo identifikační karty), následně nasnímat daný biometrický prvek (např. otisk prstu, oční duhovka, …), ze kterého software vybere důležité prvky, a poté se šablona (data) ukládá do databáze nebo do paměti zařízení. [1]

Identifikace znamená, že uživatel nastaví biometrický prvek, který nasnímá a porovná ho se všemi záznamy v paměti zařízení či v databázi. Výsledkem je výstup z paměti zařízení nebo z databáze, že se jedná o daného uživatele, nebo oznámení, že se uživatel nenachází v systému. Oproti verifikaci se uživatel nepřihlašuje do systému. [1]

Autentizace znamená, že uživatel pouze nastaví biometrický prvek ke čtecímu zařízení, to jej naskenuje a porovná data se šablonou, jež je uložena v databázi nebo v paměti zařízení. Na základě výsledku systém uživatele autorizuje, nebo ho odepře. [10]

Autentizace uživatele nemusí vždy proběhnout hladce. Problém může nastat v čistotě snímacího pole čtecího zařízení, kdy špatně nasnímá obraz prstu, anebo v softwaru, který má nastavenou příliš vysokou citlivost a pokud uživatel přiloží prst jinak nebo má jakékoliv zranění prstu, je identifikován jako nevedený v systému.

1.1 Biometrické prvky

Biometrické prvky jsou jedinečné charakteristiky, se kterými se každý člověk rodí. Můžeme je dělit na statické, jež jsou biologické a postupem času se nemění, anebo dynamické, které jsou naučené a mění se s věkem. [1]

Statické jsou:

- oko:

  - Oční duhovka a sítnice;
- hlava:
  - Obličej, dentální obraz, tvar vnějšího ucha;
- horní a dolní končetiny:
  - Otisky prstů a dlaně, geometrie dlaně, topografie žil ruky;
- tělo:
  - DNA, pach těla, obsah soli v těle. [1]

Dynamické jsou:

- hlas,
- podpis,
- dynamika stisku kláves,
- pohyb těla. [1]

Pro využití biometrických prvků v praxi je pro nás rozhodující několik kritérií. Tato kritéria jsou:

- jedinečnost:
  - Charakteristiky musí být dostatečně unikátní, aby šlo oddělit dvě osoby od sebe. Záleží na citlivosti systému.
- neměnnost:
  - Markanty musí být v čase neměnné, alespoň od dospělosti do důchodového věku.
- měřitelnost:
  - Musí být známa teoretická i praktická chybovost.
- uchovatelnost:
  - Charakteristiky musí být možné ukládat s přijatelnými náklady.
- spolehlivost:
  - Systém musí měřit, zpracovávat, ukládat a vyhodnocovat spolehlivě, kdykoliv zopakovat se stejným výsledkem.

- exklusivita:
    - Systém by měl používat pouze jednu metodu identifikace.
- praktičnost:
    - Uživatel by měl strávit co nejméně času se systémem a provést co nejméně úkonů, trénink uživatele pro používání systému by měl být minimální.
- přijatelnost:
    - Uživatelé by měli brát identifikační metodu systému jako přijatelnou. Nesmí diskriminovat (např. kontaktní čočky), nesmí zasahovat do lidského těla a oslabovat ho, systém musí být jednoduchý na obsluhu, používaní by mělo být důvěrné, nesmí narušovat soukromí apod.
- uživatelská přívětivost:
    - Používaní systému by mělo být nerušivé. Obdobně jako u přijatelnosti by nemělo zařízení diskriminovat, zasahovat do lidského těla a oslabovat ho, narušovat soukromí. Zároveň musí být zařízení umístěné a vybrané správně. Kupříkladu používání hlasové detekce v knihovně není uživatelsky přívětivé, ovšem otisk prstu je. [1]

Nejčastěji užívané biometrické prvky jsou právě statické. Jejich neskutečnou výhodou je jejich neměnnost v čase, tím pádem nemusíme uživatelskou šablonu upravovat každých několik měsíců či let. V komerční sféře je nejčastější snímání otisku prstu: dobrá přijatelnost, velmi dobrá jednoznačnost. Obličej: časem se měnit může, ale markanty zůstávají stejné, dobrá přijatelnost. A oční duhovka: velmi vysoká jednoznačnost, ovšem špatná přijatelnost, na rozdíl od sítnice není branná jako invazivní. V budoucnosti by mohlo dojít k analýze DNA, ovšem nyní je to spíše záležitost kriminalistiky.

1.1.1 Otisk prstu

Otisk prstu využívaný k identifikaci dokážeme datovat až do 9. století před naším letopočtem, kdy Asyřané využívali jména společně s otisky na hliněných tabulkách, aby předcházeli podvodům. Číňan Kio Kung-yen ve spisku psal, že Číňané využívali a znali otisky prstů a používali je při obchodních příležitostech. Japonsko využívalo otisky

podobně jako Čína, a to i v podobném časovém období. Zločinci museli otisknout rozsudek před nástupem trestu levým palcem, takzvaný „bo-han“, neboli pečeť palcem. [6]

Tyto civilizace je využívali pro identifikaci, ale pouze na základě toho, zda vypadají podobně. Zkoumali dva různé otisky za pomoci lupy a odhalovali možné nesrovnalosti ve dvou otiscích. Nerozdělovali otisky do tříd ani nehledali markanty, pouze se dívali na možnost, jestli jsou dva otisky stejné, či rozdílné.

V dnešní době využíváme hlavně poznatky a informace z nauky o kožních papilárních liniích, aneb daktyloskopie. Základy moderní daktyloskopie položili vědci jako Jan Evangelista Purkyně, Francis Galton, William James Herschel, Edward Richard Henry, Jean Vucetich a další. A hlavně díky těmto vědcům máme ponětí o papilárních linií a markantech. [6]

Dermatoglyfy jsou uspořádání papilárních linií. Jan Evangelista Purkyně objevil dermatoglyfy, rozdělil je do 9 vzorů a upozornil na delty – seskupení papilárních linií připomínající velké řecké písmeno delta. Nyní se místo 9 vzorů používá pouze 7 základních dermatoglyfů a daktyloskopie rozeznává 4 vzory. Tyto čtyři vzory objevil Francis Galton, a jsou založeny na počtu delt, které se na otisku nacházejí.[6]

Obrázek 1 Základní dermatoglyfy [6][7]

Základní dermatoglyfy:

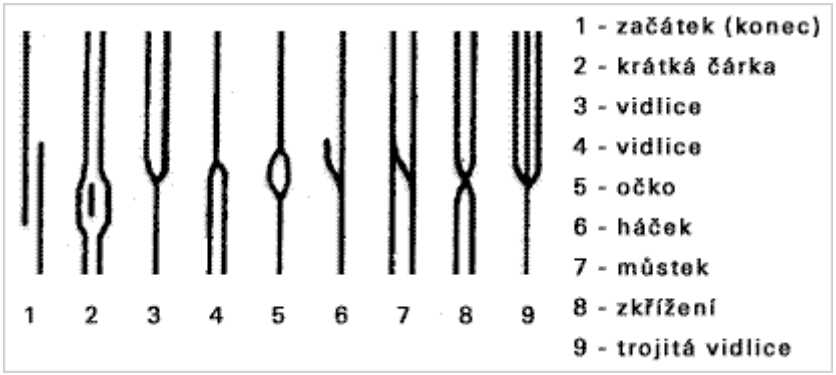
1. plochý oblouk,
2. strmý oblouk,
3. ulnární smyčka (otevřená směrem k loketní kosti),
4. radiální smyčka (otevřena směrem k vřetenní kosti),
5. dvojsmyčka,
6. spirální vír,

7. koncentrický vír. [11]

Základní daktyloskopické vzory:

1. oblouk (i strmý oblouk),
2. smyčka vlevo,
3. smyčka vpravo,
4. spirála (zahrnuje dvojsmyčku, spirální vír, koncentrický vír). [11]

Daktyloskopické markanty jsou tvořeny křížením, rozvětvováním, spojováním a přerušením papilárních linií. Podobně jako u formulování nových vzorů pro daktyloskopii, markanty částečně popsal Francis Galton, který je nazval *minutae*. Díky objevu markantů můžeme nalézt mnohem více rozdílů mezi dvěma různými otisky prstů s větší přesností. Žádné dvě osoby nemají stejné markanty, ty jsou unikátní. [1]



Obrázek 2 Markanty [8]

Markanty se vyskytují v různých počtech na otiscích. Tím pádem mají i různou identifikační hodnotu, která lze vypočítat pomocí vzorce:

$$I = -\log n$$

Rovnice 1 Identifikační hodnota markantů [1]

kde:

I – identifikační hodnota daktyloskopického markantu,

n – četnost výskytu markantu na 1 mm^2. [1]

Díky experimentům a měřením byly zjištěny hodnoty různých markantů.

Daktyloskopický markant	Hodnota
Trojitá vidlice	3,7
Zkřížení	3,1
Můstek	2,3
Háček	2,1
Očko	2,4
Krátká čárka	2,0
Vidlice	1,3
Začátek (konec)	1,0

Tabulka 1 Identifikační hodnoty daktyloskopických markantů [1]

Počet markantů nutných k identifikaci otisku s danou osob lze spočítat pomocí vzorce:

$$P = -\log\frac{1}{N} = \log N$$

Rovnice 2 Počet markantů nutných v jednoznačné identifikaci [1]

kde:

P – součet identifikačních hodnot jednotlivých charakteristických znaků ve sledované stopě,

N – počet otisků všech žijících osob. [1]

Pro výpočet, kolik je potřeba markantů z daktyloskopické stopy a kontrolního otisku, *P*musí brát v potaz, kolik je na světě lidí a kolik mohou vytvořit otisků:

$$P = \log 8 * 10^{10} = \log 8 + \log 10^{10} = 0{,}903 + 10 = 10{,}903$$

Rovnice 3 Výpočet počtu markantů pro jednoznačnou identifikaci [1]

Z výpočtu je zřejmé, že je potřeba alespoň 11 markantů pro jednoznačnou identifikaci.

Zpracovávání otisku prstu biometrickým systémem se rozděluje na tři fáze:

- předzpracování obrazu otisku prstu,
- nalezení a extrakce markantů,
- porovnání otisků. [1]

Předzpracování obrazu otisku prstu má za úkol zvýraznit papilární linie a odstranit šum z původního obrazu. Šum může představovat nekvalitní obraz, nereálný obraz, nečitelné oblasti, jizvy, falešné markanty. Následně je otisk převeden na malé, obrazové lokality. Je vytvořena síť tvořená ze směru papilárních linii procházejících těmito lokalitami. Aplikuje se filtr, jež zvýrazní všechny pixely nacházející se ve směru papilární linie v lokalitě a pixely v opačném směru jsou potlačeny. Touto operací se odstraní šum a v otisku se naleznou papilární linie. Obraz se poté převede z barevného prostředí na černobílé, kdy černá představuje papilární linie a bílá pozadí. Tato operace se nazývá *„binarizace“*, protože převádíme barevný obraz na 2 hodnoty. Jako poslední fáze předzpracování obrazu se provede *„skeletizace“*, kdy čáry papilárních linií se zúží ze své přirozené tloušťky na tloušťku jednoho pixelu. Operace má za úkol zabránit duplicitám, které mohou vzniknout ukončením či rozvětvováním tlustých papilárních linií. Po vytvoření skeletovaného obrazu se přechází na nalezení a extrakci markantů. [1]

Nalezení a extrakce markantů začíná odstraněním falešných markantů a přímočaré jizvy, které protínají papilární linie v jednom směru. Jako další jsou eliminovány hraniční a koncové body, protože se jedná o krajní body a nejsou to skutečné konce otisku prstu. Poté se hledají reálné daktyloskopické markanty, pro které definujeme:

- typ:
  - O jaký markant se jedná (začátek (konec), vidlice, očko apod.).
- souřadnice x a y:
  - Kde se markant nachází.
- směr (orientace):
  - Kam směřuje. [1]

Z nalezených a extrahovaných markantů je následně vytvořena šablona. Šablona obsahuje 10 až 100 markantních bodů. Pro datové uložení markantu je zapotřebí:

- 1-4 bitů pro uložení typu
- 18 bitů (2*9) pro uložení souřadnice x a y

- 9 bitů pro uložení směru [1]

Ovšem výše zmíněná čísla jsou pouze orientační. Po dalším zpracování může velikost jednoho markantu vzrůst na např. 10 bytů. To by představovalo velikost 1000 bytů pro jednu šablonu o 100 markantech.

Jakmile je vytvořena šablona, tak se uloží, nebo se porovnává. V případě porovnávání se vezme právě nasnímaná šablona a porovná s tou uloženou v paměti zařízení či v databázi. Porovnávají se jednotlivé markanty a sousední markanty. Sousedství lze vyjádřit právě uloženými souřadnicemi a uloženým směrem. Porovnávané markanty nemusí být identické. Ve snímání může nastat zkreslení, kde příčinou může být šum či snížená elasticita kůže. Porovnávají se všechny markanty i všechny kombinace mezi sebou. Výsledkem porovnávání dvou šablon otisků je určitá celočíselná hodnota, např. od 10 do 100. Pokud je tato celočíselná hodnota vyšší než (předem určený) práh, tak se otisky shodují. V opačné případě naskenovaný otisk nemá shodu s otisky uloženými v databázi. [1]

Díky pokrokům v technologii a poznatků z daktyloskopie se otisk prstu stal jedním z hlavních průkopníků užívání biometrie v bezpečnostních aplikacích. Jednoduchost používání a správy z otisku prstu činní jedno z nejlepších řešení pro zabezpečení vstupu i výpočetní techniky.

1.1.2 Obličej

Identifikace obličeje je metoda stará jako lidstvo samo, a tím pádem i nejpoužívanější. Každá osoba se prezentuje vlastní tváří a lidský mozek je schopen v okamžiku rozeznávat mezi rodinou, přáteli, spolupracovníky. Po celá staletí se snažili umělci zachytit co nejpřesněji lidskou tvář. Ale až ve 20. a 21. století začalo vědecké zkoumání obličeje pro identifikační účely, hlavně pro strojové vyhledávání a rozpoznávání lidské tváře. [1]

Výhody identifikace podle obličeje jsou:

- bezkontaktní snímání i na poměrně velkou vzdálenost:
    - Obličej známé osoby, lze zjistit z chodby, náměstí, města. Toto je výhoda i pro strojové vyhledávání osob;
- přirozenost:

    - Pro uživatele je přívětivá a akceptovatelná na rozdíl od jiných biometrických identifikačních metod;

- skrytost:
    - Uživatel nemusí ani vědět, že ho systém identifikuje. Opět je to výhoda i pro strojové vyhledávání. [1]

Nevýhody identifikace pomocí obličeje:

- nižší jednoznačnost oproti ostatním identifikační metodám:
    - Hlavně oproti identifikaci pomocí otisku prstů či oční duhovky. [1]

Klasifikační charakteristiky obrazu lidské tváře:

- forma,
- způsob snímání,
- nástroje zpracování,
- čas,
- spektra. [1]

Formy mohou být 2D, a 3D. 2D forma pracuje tak, že provede sken obličeje, zpracuje data z obličejových markantů, a následně porovnává s uloženou šablonou. 3D forma je přesnější a kromě pouhých markantů ze skenu obličeje bere v úvahu i hloubku daných markantů. 3D forma je oproti 2D formě přesnější, ale vyžaduje silnější hardware. Navíc u 2D formy nastává problém, že lze použít fotku osoby známé pro systém a využít ji pro přístup. [1]

Způsob snímání může být z profilu nebo „en face“. Rozdíl mezi těmito je pouze změna markantů. Profil je zaměřený na ucho, nos, bradu, koutek oka a koutek úst. „En face“ je zaměřena na oči a mezeru mezi nimi, velikost nosu, úst, délka i šířka obličeje. „En face“ je častější než z profilu. [1]

Nástroje zpracování rozdělujeme na algoritmy znalostní, algoritmy statistické, neuronové sítě, genetické algoritmy. [1]

Algoritmy znalostní jsou postaveny na znalostních metodách. Mezi znalostní metody patří:

- metody založené na rozložení odstínu šedi v obraze:
    - Pracují na principu rozložení odstínů šedé v obraze za normálních světelných podmínek. Například oblast očí je vždy tmavší než čelo.
- metody založené na rozpoznávání obličejových rysů:
    - Pracují na principu obrysu obličeje a jednotlivých objektů tváře jako jsou oči, ústa, nos apod.
- metody založené na informaci o barvách:
    - Pracují na principu rozlišování barev. Pro oblast očních důlků je typická barva stínů, nos je barevně výrazný a ohraničený stíny, ústa jsou barevně výrazná.
    - Při verifikaci/identifikaci je dobré mít snímač naproti jednobarevné zdi, aby tato metoda co nejlépe fungovala.
- metody založené na informaci o pohybu na scéně:
    - Pracují na principu, že obličeje osob pohybující se vzhledem k pozadí jsou jednoduše a efektivně detekovány na pozadí scény.
- metody založené na symetrii:
    - Pracují na základě skutečnosti, že lidský obličeje je do určité míry symetrický. [1]

Algoritmy statistické jsou postaveny na statisticky orientovaných metodách. Mezi statisticky orientované metody patří např. metoda podprostoru. Cílem metody podprostoru je nalézt v obrazu obličeje obecné markantní charakteristiky, např. nos, ústa, oči – pokud jsou nalezeny, lze konstatovat, že se jedná o obličej. [1]

Neuronové sítě mají za úkol naučit se rozeznávat mezi obrazy obličejů a obrazy, které nejsou obličeji. Na tento úkol se připravují speciální knihovny s obrazy obličejů i těmi, co obličeje nejsou. Následně nechají neuronovou síť rozeznávat mezi nimi. [1]

Čas rozdělujeme na statický a dynamický. [1] Statický označuje neměnný obraz obličeje, např. z fotky. Dynamický označuje obličej v ději, např. ve videu.

Spektrum označuje, v jakém prostředí obličej rozpoznáváme. Může být barevné, černobílé, či infračervené. Infračervené je postavené na rozložení tepla v obličeji. [1]

Obličej nalézá stále větší využití v bezpečnostních aplikacích. Největší využití obličeje jako identifikačního prvku nalézáme ve strojovém vyhledáváním, ale i rozpoznávání tváře se najde u většiny chytrých telefonů.

1.1.3 Oční duhovka

Oční duhovka, i přes svou malou velikost (11 mm), představuje jeden z nejlepších identifikačních prvků v rozsáhlých systémech, kde je potřeba procházet velké databáze v krátkém čase. Oční duhovka má složitý vzor, díky kterému obsahuje množství charakteristických znaků. [1]

Tyto charakteristické znaky se nacházejí na předním listu duhovky (takzvaná stroma). Stroma je tvořena kolagenními a elastickými vlákny, která jsou protkána hladkým svalstvem. Stroma obsahuje četné cévy, které vytvářejí právě charakteristické znaky, např. krypta je tvořena přerušovaným místem. Charakteristické znaky duhovky:

- klenuté vazy,
- rýhy,
- hřebeny,
- krypty,
- prstence,
- koróny,
- pihy,
- klikaté čáry. [12]

Nesmírné rozdíly mezi dvěma očními duhovkami představují obrovskou výhodu pro duhovku jakožto identifikační prvek. Další výhody představují:

- neměnnost:
    - Oční duhovka je z velké části dokončena již v 8. měsíci těhotenství a plně dokončena je v prvních letech života.
- 2D forma:

- Nezáleží na úhlu snímání či osvětlení.

- ochrana před vnějšími vlivy:
  - Jelikož je součástí oka, je chráněna před vnějšími vlivy. I pokud má osoba kontaktní čočky, jsou systémy schopné duhovku zpracovat.

- jednoduchost nalezení:
  - Systémy jsou schopny přesně a spolehlivě nalézt duhovky na obraze a vytvořit stálý obrazec pro identifikaci. [1]

Nevýhoda užití oční duhovky spočívá v problému, kdy ji veřejnost bere jako invazivní. Oproti oční sítnici, kde je potřeba využívat laser, se u oční duhovky využívá blízké části infračerveného spektra, které je bráno jako neinvazivní. Při použití blízké části infračerveného spektra vyvstanou stromální znaky v závislosti na cévách, jež probíhají stromou. Vyvstanou i znaky tmavě pigmentované duhovky, které by normálně mohly být neviditelné. [1]

Oční duhovka nalézá stále většího využití,ať už se jedná o rozsáhlejší komplexy jako letiště či nájemné domy, kde se oční duhovka používá obdobně jako otisk prstu.

1.2 Užití v bezpečnostních aplikacích

Biometrické prvky nalézají v bezpečnostních aplikací největší užití. Pomocí biometrických prvků lze nalézt či ověřovat identitu známé osoby. Biometrie představuje alternativu k běžný způsobům, jako jsou např. jméno a heslo, klíče, identifikační karta, PIN. Ovšem biometrické systémy bývají kombinované s těmito běžnými způsoby. Důvodem jsou případy, kdy biometrický systém nemůže z určitého důvodu autentizovat známého uživatele. Může to být zranění biometrického prvku uživatele, nebo výpadek samotného systému, který by uzamknul celý objekt.

1.2.1 Otisk prstu

Otisk prstu je nejvyužívanější biometrický prvek v bezpečnostních aplikacích určených pro ověřování identity. V kriminalistice je využívaný posledních 200 let při řešení trestných činů a odhalování pachatele. K odhalení otisku prstů na místě činu bývají používány různé způsoby např.: fyzikální, chemické, fyzikálně-chemické apod.

Zvýrazněné otisky bývají odebrané a dají se zkoumat přes automatizovaný biometrický systém, který porovnává otisk s databází otisků prstů.

V komerční sféře se s otisky prstu setkáváme hlavně u výpočetní techniky, primárně u chytrých telefonů. Kromě výpočetní techniky se ale využívají pro zabezpečení prostorů před vniknutím, nebo jakožto systémy kontroly vstupu. Při obou aplikacích nám jde hlavně o střežení věcí a prostor, které mají být přístupné jen pro ověřené uživatele (zaměstnanci, rodina apod.).

Snímače pro otisk prstu mohou být:

- optoelektrické:
    - Založeny na odrazu lomu světla.
    - Pod dotykovým povrchem je vrstva fosforu. Ta má za úkol osvítit plochu prstu, která se pak odrazí a vrací se přes luminofor.
    - Poté se přenese na CCD maticový detektor, zdigitalizuje ho a předá pro zpracování.
    - Výhodou je vysoká kvalita obrazu, odolnost proti statickým výbojům a minimální vliv okolního prostředí.
    - Nevýhodou je, že může nastat špatné vykreslení prstu v závislosti na znečištění či zranění, anebo snímání předchozího ulpělého otisku. Dále pak větší rozměry, které jsou omezující pro malá zařízení.
- kapacitní:
    - Založeny na rozdílu kapacity mezi deskou snímače a povrchem prstu. Snímač a prst představují desky kondenzátoru. Samotný snímač je osazen velkým množstvím elektrod, a díky tomu se získává obraz otisku. Papilární linie vytvářejí větší odpor díky většímu přilehnutí k desce než mezery.
    - Výhodami jsou malé rozměry, vysoká kvalita obrazu a jednoduchost principu funkčnosti.
    - Nevýhodou je nízká životnost snímače kvůli nastřádané statické elektřině.

- teplotní
    - Pracují na principu snímání rozdílu teplot mezi papilárními liniemi a mezerami. Nutné je několikrát přejíždět prstem přes snímač. Obraz otisku je pak získám formou digitálních pásů, které jsou složeny dohromady.
    - Výhodou jsou malé rozměry.
    - Nevýhodou je nízká kvalita obrazu a problémy s algoritmy zpracovávající markanty. Důvodem je nasnímání různých míst prstu kvůli způsobu snímání. Proto je obtížné vytvořit databázi otisků.
- elektroluminiscenční:
    - Pracují na využití speciální vrstvy, která reaguje na tlak způsobený luminiscenčním efektem. Obsahuje světlo eliminující vrstvu, která filtruje světlo z míst, kde tlačí papilární linie. Zpracování zajišťují fotodiody.
    - Výhodami jsou miniaturní rozměry, velmi dobré rozlišení v poměru k prodejní ceně a schopnost číst i extrémně suché otisky.
    - Nevýhodami jsou menší odolnost vůči mechanickému poškození a náchylnost ke znečištění prachem a vodou.
- radiofrekvenční:
    - Pracují na způsobu připojení generátoru střídavého signálu na 2 rovnoběžné desky, kde jedna deska je snímač a druhá je otisk prstu. Vyskytuje se zde pouze složka elektrického pole, bez pole magnetického, protože vlnová délka je mnohem větší než délka desek. Tvar pole kopíruje otisk prstu.
    - Výhodou je odolnost vůči nečistotám, kdy nečistoty v mezerách nejsou problémem, protože snímač kopíruje otisk prstu a nesnímá obraz prstu.
- multispektrální:

- Pracují způsobem osvětlení prstu; využívají více osvětlovacích soustav o různých vlnových délkách, které projdou pod kůží a umožní senzoru nasnímat více identifikační údajů z prstu.
- Výhodami jsou schopnost čtení nevýrazných, suchých, špinavých prstů, odolnost vůči útokům a odolnost vůči externím vlivům (voda, světlo, prach apod.). [13]

1.2.2 Obličej

Obličej je v bezpečnostních aplikacích používán hojně. Největší zastoupení nachází hlavně u průkazů totožnosti, jako jsou např. občanský průkaz nebo pas. Jako přístupový prvek nalézá největšího zastoupení u mobilních telefonů. Další aplikace obličeje jako přístupového prvku jsou hlavně pro státní kontroly, např. při kontrole na hranicích, ve věznicích, ve vládních objektech, ale i v bankách, kasinech, klubech.[1]

Pro užití jako přístupového prvku či k rozpoznávání osob je nutné strojové rozpoznávání obličeje. Probíhá ve dvou fázích. První fází je detekce a lokalizace tváře, kde pomocí kamery se nalezne obličej na scéně, zde se jedná o detekci. Lokalizace je prostorové umístění lidského obličeje, kdy se musíme předat i souřadnice, se kterými může systém dále pracovat. Pokud se jedná o přístupový prvek, tato metoda nezabere moc času. Zde se jedná o jednu tvář, nejčastěji v dobrém osvětlení a s jednoduchým pozadím. Situace se mění, pokud hledáme osobu v davu lidí. Zde může být problém s vyhledáním osoby z důvodu četného počtu lidí a svou úlohu hrají i emoce, které mohou zhoršit identifikaci.[1]

Druhá fáze je rozpoznání tváře. Z první fáze jsme obličej izolovali a provede se extrakce charakteristik. Zde opět záleží na typu aplikace. Pokud se jedná o přístup do místnosti, stačí pouze projít databází, zda se obličej shoduje se záznamem uloženým v databázi. Pokud se jedná o hledanou osobu či prověřujeme osobu, jež se nalézá např. na letišti, vlakovém nádraží, či rušném náměstí, musíme hledat její jméno, či jestli není podezřelá z určitého trestného činu. V závislosti na daném požadavku se může čas měnit. Ovšem všechny aplikace musí být rychle vyřešené, protože potřebují co nejrychlejší odpověď. [1]

Užití obličeje nachází velkého uplatnění jak u policie (např. při ukládání obličeje do databáze s kartou zločince či hledání nebezpečných osob), tak i u míst s velkým počtem osob najednou, např. letiště. [1]

1.2.3 Oční duhovka

Oční duhovka se už nyní využívá pro kontrolu či přístup do objektů. Jedním z hlavních využití je pro přístup do objektů s vysokým stupněm zabezpečení, jakými jsou např. bankovní trezory, věznice, jaderné elektrárny apod. I na letištích nachází obrovského využití. [1]

Letiště ve Spojených státech amerických, Nizozemí, Japonsku, Spojených arabských emirátech aj. využívají oční duhovky v několika různých případech:

- místo pasů při kontrole příjíždějících pasažérů zaregistrovaných jako *„frequent traveller“*,
- zrychlený check-in odjíždějících pasažérů,
- urychlené řízení přístupu pro piloty a členy posádek,
- pro zaměstnance letiště při přístupu na letištní plochu a do ostatních vyhrazených prostor,
- pro kontrolu přijíždějících pasažérů, jestli nebyly dříve vyhoštěni. [1]

Přístupové aplikace oční duhovky pro širokou veřejnost lze nalézt v Japonsku. Sken oční duhovky je zde používán u nájemních domů. Nájemníci jsou uloženi v databázi spravované pro daný nájemní dům. U vchodu je prověřena identita osoby, a pokud je nájemníkem, systém ji pustí a přivolá jí výtah do patra, kde má byt. [1]

Další aplikací oční duhovky bylo prověření identity afgánských uprchlíků vracejících se do Afganistánu z Pákistánu. Komise pro uprchlíky Spojených národů díky identifikaci za pomoci oční duhovky spravedlivě rozdělovala pomoc, jejíž peněžní hodnota byla pod 30$. Účelem bylo, aby tyto prostředky nepadly do rukou nesprávných lidí. [1]

Oční duhovka se stává čím dál tím více populární. Nachází zatím hlavně uplatnění pro objekty s vysokým stupněm zabezpečení, ale i uplatnění pro širokou veřejnost na letištích či v nájemních domech.

2 ZABEZPEČENÍ VSTUPU

Vstup představuje první linii zabezpečení před vloupáním. Pro zabezpečení vstupu můžeme využít mechanické zábranné systémy, dále se používají prvky plášťové ochrany, také lze použít kamery.

Užití těchto prvků může značně zpomalit, odhalit, či dokonce odradit potencionální zloděje od vniknutí do objektu, nebo je minimálně zpomalit, než se k objektu dostane vyslaná bezpečnostní zásahová jednotka.

2.1 Prostředky

Vstup lze zabezpečit několika způsoby. Zabezpečení stavebních prvků zabraňuje vytržení celého dveřního systém. Mechanické zábranné systémy (dále jen MZS) přímo zabraňující nebo zpomalující možného útočníka. Prvky plášťové ochrany informují bezpečnostní agenturu o vstupu nepovolené osoby do objektu či na pozemek. V neposlední řadě kamery a dohledové videosystémy, jež poskytují záznam o útočníkovi, a bezpečnostní agentura tak může pozorovat, jestli se jedná skutečně o útočníka, nebo o planý poplach.

2.1.1 Zabezpečení stavebních prvků

Zabezpečení stavebních prvků má hlavní úkol zabezpečit dveřní systém před úplným vytrhnutím útočníky. Stavební prvky, které lze vyztužit a zabezpečit:

- ostění,
- upevnění zárubně. [2]

Ostění je část stavebního prvku, kde jsou umístěné zárubně pro vstupní dveře. Podle konstrukce a použitého materiálu se může jednat o nosný, příčný nebo dřevěný panel, zděnou příčkou, nosnou zeď apod. [2]

Upevnění zárubně v ostění má také různé možnosti. Nejběžnějším upevněním je cementová malta, nebo betonová výplň s ocelovými výztuhami. Velmi časté je i vyplnění mezery v ostění a zárubní pomocí pěny s ocelovými výztuhy umístěnými v horní a dolní části zárubně. U objektů s vyšším stupněm zabezpečení se používá zpevnění pomocí ocelové sítě. [2]

2.1.2 Mechanické zábranné systémy

Dveře by měli představovat první a poslední překážku pro útočníka. Zabezpečení dveří může přímo odradit útočníka. Dveře lze zabezpečit různými způsoby MZS před možnými útoky. Toto zabezpečení za pomoci MZS přímo souvisí s jednotlivými prvky dveří a jejich usazením. Mezi prvky dveří, které lze zabezpečit, patří:

- zárubeň,
- závěsy,
- dveřní křídlo,
- zadlabací systém,
- zámková vložka,
- bezpečnostní kování. [2]

Zárubeň neboli rám dveří je vytvořený ze dřeva, nejčastěji u starších objektů, či oceli, která je bezpečnější. Zárubně slouží pro zavěšení dveřního křídla. Důležitým prvek je zapadající plech, tzv. protiplech, který musí být umístěný na jedné stojně. Protiplech je přišroubovaný díl, v případě ocelových zárubní je vyřezaný do stojny, sloužící pro zasouvání závory se střelkou uzamykacího zámku při zamykání či zavírání. Zárubně mohou být jednokřídlé nebo dvoukřídlé. [2]

Závěsy slouží pro uchycení dveří a pro jejich otáčení a snadnou manipulaci. Taktéž jako ochrana před vysazením či vylomením. Jsou spojeny pevně se zárubní avytvořeny z plechových dílů a otočných komponentů. Pro složitější provedení jsou vytvořeny z oceli. Při zajištění pro vyšší bezpečnost jsou vytvořeny z odlitků, nebo kované z kvalitních materiálů s pojištěním vůči vysazení. Obvykle používané ve třech kusech, ale používají se i 2 a více kusů podle váhy dveří. [2]

Dveřní prostor je stavební prostor tvořený dvěma celky s doplňky, zárubní a dveřním křídlem.

Dveřní křídlo je tvořeno pevnou dřevěnou deskou, dřevěným rámem a překližkovým vnitřkem, nebo s kazetovou výplní. Vnitřní mohou být prosklené a sklepní či dílenské mohou být oplechované, či celokovové. Opatřeno zadlabávaným zámkem, jež se nachází uvnitř dveřního křídla a nepřesahuje ven, s bezpečnou klíčovou sestavou a chráněným kováním. Usazené na nejlépe třech závěsech. Hlavní vlastností je, že křídlo

nesmí být prokopnutelné či vyvratitelné. Také musí být zajištěné vůči vysazení a vyháčkování. [2]

Alternativu k běžnému dveřnímu křídlu představují bezpečnostní dveře. Bezpečnostní dveře obsahují řadu prvků se zvýšenou odolností vůči páčení, prořezání či proražení. Často představují celý dveřní systém s celokovovou, zesílenou zárubní a bezpečnostními výplněmi, např. protipožární. Dveřní křídlo je většinou sendvičové (vícevrstvové). Zárubeň má nejméně tři robustní závěsy s pojistkou proti vypáčení. Po celém obvodu má dveřní křídlo zvýšený počet uzamykatelných a zajišťujících míst pomocí rozvoru. [2][5]

Zadlabávané zámky jsou nejčastěji opatřeny cylindrickou vložkou sloužící pro zamykání dveří. Podle vložky se zasouvá klíč, nejčastěji plochý opatřený bezpečnostním drážkováním pro zajištění, že stavítka zapadnou do správné polohy. Klíč se zasouvá špičkou do cylindrické vložky, kde posouvá závoru zámku. Tímto dojde ke správnému srovnání různých délek stavítek, přesně na hranici otáčivého válce a neotáčivého pouzdra. Po otoční klíče se otáčí i válec a zámek se odemyká. [2]

Dělení cylindrických vložek:

- podle délky:
  - Oboustranná – lze odemykat cylindrickou vložku z obou stran;
  - Jednostranná – lze odemykat cylindrickou vložku z jedné strany;
- podle tvaru:
  - Profilované, oválné, kruhové apod.;
- podle symetrie:
  - Symetrické – obě strany jsou stejně dlouhé;
  - Asymetrické – jedna strana je delší/kratší;
- podle stavítek:
  - Podle počtu stavítek v řadě – 5, 6, 7, 8, …;
  - Počet řad stavítek – jednořadé, dvouřadé, … [2]

Části cylindrické vložky:

- těleso:

  - Všechny části cylindrického zámku drží pohromadě. Svým tvarem odpovídá otvoru v zámku, do kterého se zasouvá.

- zub:
  - Svým pohybem posouvá odemykající mechanismus, jež zatahuje závoru.
- cylindr:
  - V uvolněném stavu za pomoci klíče otáčí, či pootáčí zub cylindrické vložky.
- spojka:
  - Umožňuje spojení cylindru a zubu na straně zasunutého klíče. Nachází se pouze u oboustranné cylindrické vložky.
- blokovací kolík:
  - Nachází se mezi stavítkem a pružinou. Mají různé tvary, ale zanechává se rotační plocha. Základní tvary jsou svazek prstenců, soudeček, odstupňovaný válec. Složitější tvary znesnadňují vyhmatání pomocí planžety.
  - Blokovací kolík i stavítka jsou vyrobeny většinou z tvrzeného bronzu, či tvrzené oceli, protože měkké slitiny by nevydržely a brzo by se opotřebovaly. Z tvrzené oceli nejčastěji bývá první sloupek z důvodu ochrany proti odvrtání.
- stavítko:
  - V přímém kontaktu s klíčem a pohybuje se podle jeho tvaru.
- pružiny:
  - Posouvají, či stlačují stavítka a blokovací kolík.
  - Nejčastěji vyrobené z mosazi. [2]

Bezpečnostní kování je ochrana zámku proti rozlomení. Musí se nainstalovat zevnitř, aby tento štít cylindrické vložky nešlo zvenčí odmontovat. [5]

Alternativami k cylindrické vložce a zadlabávanému zámku jsou elektronický zámkový systém a mechatronické systémy.

Elektromotorický zámkový systém je připojený na ústřednu PZTS a otevírá se za pomoci identifikačního čipu (RFID). Celý systém je ovládán motoricky, uživatel pouze přikládá čip. Systém posílá řadu hlášení o svém stavu na ústřednu, představuje jeden z ideální komponentů systému kontroly vstupu. Samotný elektromotorický zámkový systém má řadou funkcí např.:

- Po přiložení čipu, či poslání aktivačního signálu se zatáhne závora a uvolní se střelka, stačí pouze otevřít dveře.
- Jakmile se střelka zatlačí do protiplechu, automaticky se vysune závora a zablokuje se střelka.
- Při výpadku napájení zůstává systém v uzamčeném stavu. Zámek je vždy možné otevřít z vnitřní strany stiskem kliky. Nazývá se to funkce antipanic. [2]

Mechatronika kombinuje poznatky z oboru elektroniky, mechaniky, softwarového inženýrství. Mechatronika otevřela prostor pro další alternativy ke klíči či kombinaci s klíčem. [20] Příkladem je FAB +CLIQ, který využíval klíč s čipem, pomocí něhož lze programovat přístup. FAB +CLIQ se již nevyrábí, ale byl nahrazen FAB ENTR, motorický systém, který nevyužívá klíče, ale lze otevírat pomocí telefonu, dálkového ovládání, otiskem prstu či PIN kódem.

Ovšem mechatronické systémy nemusí nutně být celé zámky – viz Richter Czech Smart Handle H.02/H.03. Jedná se o mechatronické kliky, které v případě H.02 lze otevřít pomocí předem nastaveného PIN kódu v rozsahu čísel od 1 do 4. V případě H.03 lze otevřít i za pomocí otisku prstu a taktéž PIN kódu v rozsahu čísel od 1 do 7. V obou případech lze otevírat za pomocí telefonu.

Dveřní křídlo může být ještě osazeno doplňkovými bezpečnostními prvky. Přídavný zámek může zvýšit bezpečnost vstupu a nenarušuje tloušťku dveří. Instaluje se zevnitř dveří, a to buď přímo na dveře, nebo do zdi hned vedle dveří. Mnohé přídavné zámky obsahují blokující ramínko. Blokující ramínko dovoluje pootevřít dveře o 10 cm, tím si může obyvatel prověřit, o koho se jedná. Také je mnohem bezpečnější než bezpečnostní řetízek, který nevydrží, pokud útočník kopne či vrazí ramenem do dveří. [5]

Dalším přídavným bezpečnostním prvek je kukátko. Díky kukátku můžeme provit, kdo stojí za dveřmi. Obyvatelé mohou předejít možnému útočníkovi, který se snaží dostat

do domu či bytu díky překvapení místo fyzického prolomení dveřního systému. Moderní kukátka využívají kamery a lze pomocí nich i natáčet možného útočníka. [5]

Balkonové dveře mohou také sloužit jako vstup a při vloupání do bytu představují pro útočníka lákavou alternativu. Lze je zabezpečit obdobně jako dveře s přídavným zámkem, či kompletním zámkovým systémem. Ovšem nejslabší místo je samozřejmě sklo.

Standardní tloušťka skla upevňovaného do dřevěného či plastového rámu jsou 3 mm. Sklo představuje nejslabší místo jak pro okno, tak i pro samotné balkonové dveře. Pro zvýšení bezpečnosti skleněných ploch lze použít skla:

- tvrzená:
  - Vhodná pro interiér.
  - Po úderu se tříští, čímž předchází zranění, ale činí z něj nevhodný prvek pro vnější použití.
- vrstvená (sendvičová):
  - Sendvičová technologie lepení skla.
  - Sklo-fólie-sklo, tloušťka 3-0,8-3, cca 6,8 mm.

    Dvouvrstvé, třívrstvé, …
- s drátěným pletivem:
  - Zamezuje snadné rozbití a proniknutí plochou skla.
- s bezpečnostní fólií:
  - Jedná se skla s tloušťkou 4-6 mm opatřená vrstvami polyesterového filmu o tloušťce 50-400 µm.
  - Polyesterový film je téměř čirý a poskytuje dobré vlastnosti ve zpomalení pachatele i proti poranění. [3]

2.1.3 Prvky plášťové ochrany

Prvky plášťové ochrany hlídají otevření pláště budovy, a to destruktivní i nedestruktivní. Specificky vstup přes dveře, okna, vrata. Prvky plášťové ochrany zabezpečující dveře jsou:

- Magnetické kontakty

- Tvořeno dvojící dílů. Jazýčkový kontakt (relé), tvořený zatavenou trubičkou s dvěma ferromagnetickými kontakty v ochranné atmosféře, a permanentní magnet, tvořen nejčastěji zmagnetizovaný válečkem z feritu. Oba díly se nacházejí v ochranném pouzdře z nemagnetických materiálů, nejčastěji plastu.
- Jeden z kontaktů se nachází v rámu, nebo na rámu, a druhý je na pohyblivé části, např. křídlo dveří, balónové dveře apod.
- V klidovém stavu se kontakty nacházejí jen pár milimetrů od sebe. Samotný kontakt jazýčkového relé je sepnut magnetickým polem permanentního magnetu.
- Jakmile se dveře otevřou, kontakty se od sebe vzdálí, kontrakt jazýčkového relé se sepne a jestli je objekt střežený, vyhlásí se poplach.

- Mikrospínače
  - Zabudované do rámů proti západce zámku.
  - V případě střežení, pokud se se západkou zámku pohne, vyhlásí se poplach. [4]

2.1.4 Kamery

V zabezpečení vstupu hrají kamery roli dohledovou. Obyvatelé, bezpečnostní firma, či vrátný mohou kontrolovat, kdo se před dveřmi nachází, a podle informace patřičně reagovat. Kamery nacházejí uplatnění i jako videotelefon u vstupu či kukátko. [5]

3 MECHATRONICKÉ SYSTÉMY

Mechatronika je mezioborový inženýrský obor. Kombinuje a čerpá z oborů elektroniky, mechaniky, výpočetní techniky a řízení. Výhodou oproti standardním elektromotorickým zařízení je flexibilita chodu. Mechatronické systémy se dají naprogramovat přesně, podle možností systému, k uspokojení uživatele. Také se oproti elektromotorickým zařízením zvyšuje rychlost a přesnost. [20]

3.1 Normy zastřešující mechatronické systémy

Mechatronické systémy jsou elektrická zařízení, musí splňovat nařízení vlády č. 118/2016 *„Nařízení vlády o posuzování shody elektrických zařízení určených pro používání v určitých mezích napětí při jejich dodávání na trh“*. Nařízení stanovuje, že výrobek musí být ve shodě se zněním nařízení, např. stanovuje, že všechna elektrická zařízení musí projít zkouškami, které zajišťují bezpečné zařízení neohrožující lidské zdraví. Musí též splňovat nařízení vlády č. 117/2016 *„Nařízení vlády o posuzování shody výrobků z hlediska elektromagnetické kompatibility při jejich dodávání na trh“*. Zařízení nesmí během svého provozu rušit jiná záření nepřístupným elektromagnetickým rušením. Zároveň musí mít zařízení schopnost odolávat elektromagnetickému rušení bez zhoršení kvality. Pokud obsahují prvky bezdrátového spojení, např. Bluetooth, musí splňovat nařízení vlády č. 426/2016 *„Nařízení vlády o posuzování shody rádiových zařízení při jejich dodávání na trh“*. Zajišťuje, že zařízení dodávané na trh je v souladu s předpisy stanovenými v nařízení, např. musí využívat kmitočtového pásma účelně, musí být zajištěny základní bezpečnostní zásady, musí být zajištěna úroveň elektromagnetické kompatibility v rozsahu požadavků.

Mechatronické dveřní kování a cylindrické vložky mají také své vlastní normy. Požadavky a zkušební metody pro mechatronické cylindrické vložky upravuje ČSN EN 15684 *„Stavební kování – Mechatronické cylindrické vložky – Požadavky a zkušební metody“*. Obsahuje kategorie použití postavených na výkonnostních testech a bezpečnostní třídy postavené na konstrukčních požadavcích a výkonových testech simulující útok. Norma je zaměřena pouze na cylindrickou vložku a přídavné funkce, pouze pokud se týkají konstrukce nebo chodu cylindrické vložky.

Požadavky a zkušební metody pro mechatronické dveřní kování upravuje ČSN EN 16867 *„Stavební kování – Mechatronické dveřní kování – Požadavky a zkušební metody“*. Klasifikuje mechatronické dveřní kování v několika charakteristikách podle kategorie

použití, životnosti, bezpečnosti, typu ovládacího zařízení. Také specifikuje vhodnost zkouškami pro použití na požárně odolných, či protikouřových dveřních sestavách. Normě ČSN EN 16867 končí platnost 01. 06. 2022 platnost a je nahrazena ČSN EN 16867 +A1.

.

II. PRAKTICKÁ ČÁST

4 SPOLEHLIVOST BIOMETRICKÉHO SYSTÉMU V MECHATRONICKÉM SYSTÉMU

Spolehlivost biometrických systémů jde určit pomocí FRR a FAR. FRR, False Rejection Rate, česky Pravděpodobnost chybného odmítnutí, je kritérium ukazující na bezpečnostní i uživatelskou spolehlivost. Udává chybovost a nerozpoznání uživatele s uloženou šablonou biometrického prvku. Uživatel je biometrickým systémem odmítnut či nenalezen a musí se znovu prokazovat. [1]

Výpočet FRR:

$$FRR = \frac{N_O}{N_{VZ}}$$

Rovnice 4 Vzorec pro výpočet chybného odmítnutí [1]

kde:

N_O – počet chybných odmítnutí známého uživatele

N_{VZ} – počet všech pokusů o verifikaci, identifikaci, autorizace známého uživatele

Oproti policejně-soudním aplikacím se v komerčních aplikacích nejedná o závažnou bezpečnostní chybu. Nežádoucí je z pohledu uživatelské přívětivosti a spolehlivosti biometrického systému. Známý uživatel při několika chybných odmítnutích může mít pocit, že systém je „velmi přísný“, a klesá jeho důvěra ve spolehlivost systému. Není žádoucí, aby existoval velký počet známých uživatelé, jež byli odmítnuti. [1]

FAR, False Acceptance Rate, česky Pravděpodobnost chybného přijetí, je kritérium zaměřené na bezpečnost biometrického zařízení. Útočník se snaží dostat do objektu střeženého biometrického systémem či systémy napodobením identity známého uživatele. Útočník, jež se snaží použít tento způsob o překonání biometrického zabezpečení, musí být rozpoznán a okamžitě odmítnut jako osoba neznámá či neoprávněná. Pro aplikace střežící přístup do objektu se chybné přijetí neznámé osoby musí brát jako bezpečnostní incident, ve kterém může dojít k nežádoucím aktivitám. [1]

Výpočet FAR:

$$FAR = \frac{N_P}{N_{VN}}$$

Rovnice 5 Vzorec pro výpočet pravděpodobnosti chybného přijetí [1]

kde:

N_P – počet chybných přijetí neznámého uživatele

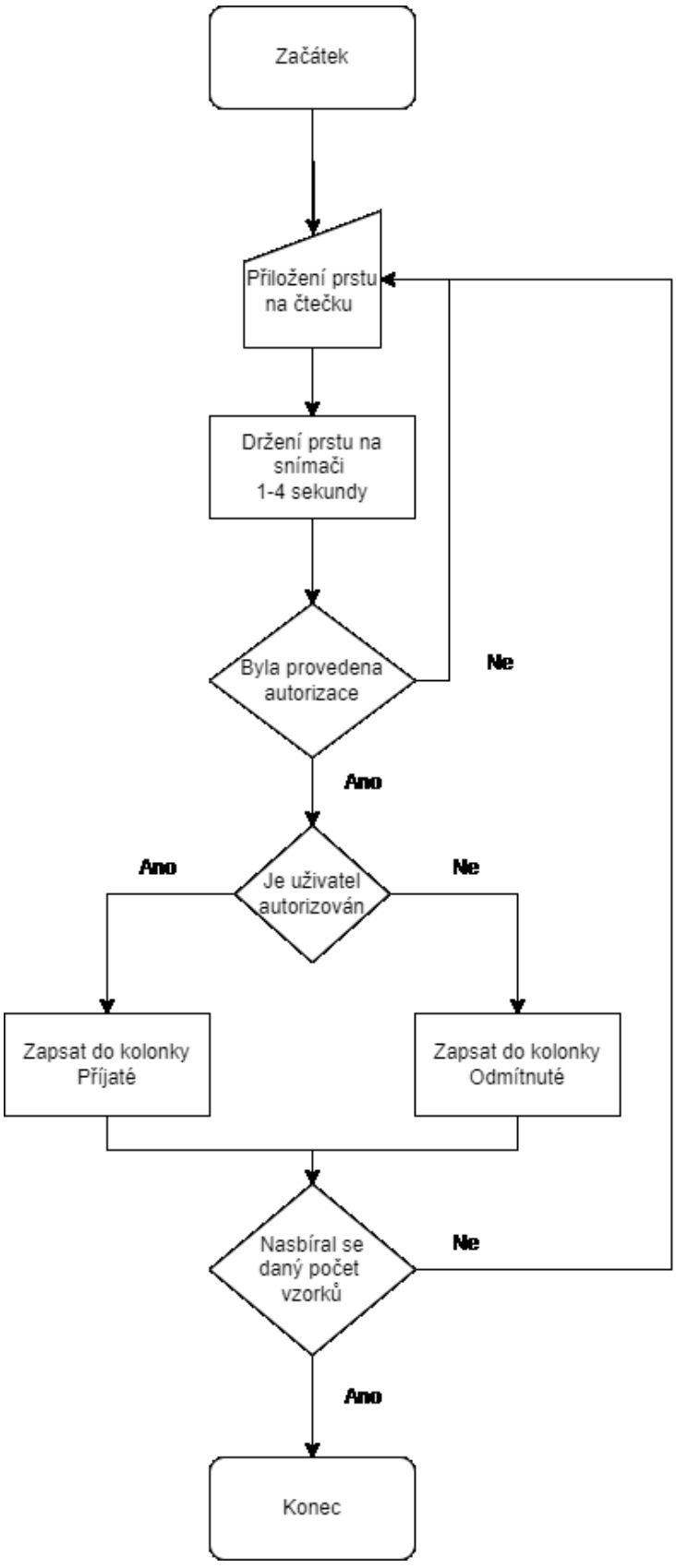
N_{VN} – počet všech pokusů o verifikaci, identifikaci, autorizaci neznámého uživatele

4.1 Výsledky

Sbírání vzorků pro metody FRR a FAR probíhali na Richter Czech Smart Handle H.03. Jedná se o rozetové dveřní kování, klika je mechatronická s otevíráním pomocí otisku prstu, telefonu, či PIN kódu. Testování proběhlo na instalované Richter Czech Smart Handle H.03 ve výřezu dveří. Proběhlo nasnímání otisku 500x pro každou metodu.

Obrázek 3 Nainstalovaná Richter Czech Smart Handle H.03 [vlastní zdroj]

Testování:



Obrázek 4 Sběr hodnot pro výpočet FRR a FAR

[vlastní zdroj]

Naměřené hodnoty pro pravděpodobnost chybného odmítnutí:

Přijaté	480
Odmítnuté	20
Celkem	500

Tabulka 2 Naměřené hodnoty FRR [vlastní zdroj]

Hodnota pravděpodobnosti chybného odmítnutí:

$$FRR = \frac{20}{500} = 0{,}04 = 4\%$$

Rovnice 6 Výpočet pravděpodobnosti chybného odmítnutí [vlastní zdroj]

Naměřené hodnoty pro pravděpodobnost chybného přijmutí:

Odmítnuté	500
Přijaté	0
Celkem	500

Tabulka 3 Naměřené hodnoty FAR [vlastní zdroj]

Hodnota pravděpodobnosti chybného přijmutí:

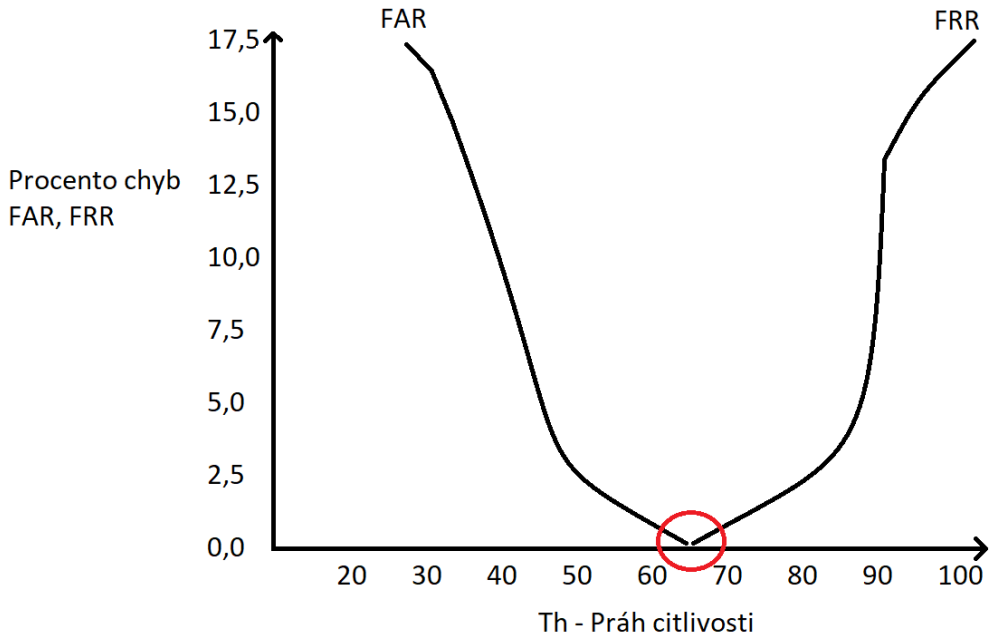
$$FAR = \frac{0}{500} = 0 = 0\%$$

Rovnice 7 Výpočet pravděpodobnosti chybného přijmutí [vlastní zdroj]

Sběru dat pro pravděpodobnost chybného přijmutí bylo náročnější než pro pravděpodobnost chybného odmítnutí. Největší překážkou představovalo dočasné vypnutí čtečky otisku prstu každých přibližně 50 vzorků uživatele neznámého pro systém.

Jedním z možných důvodů pro nulové přijetí neznámého uživatele byl nízký počet otisků, přibližně 5, v systému mechatronické kliky.

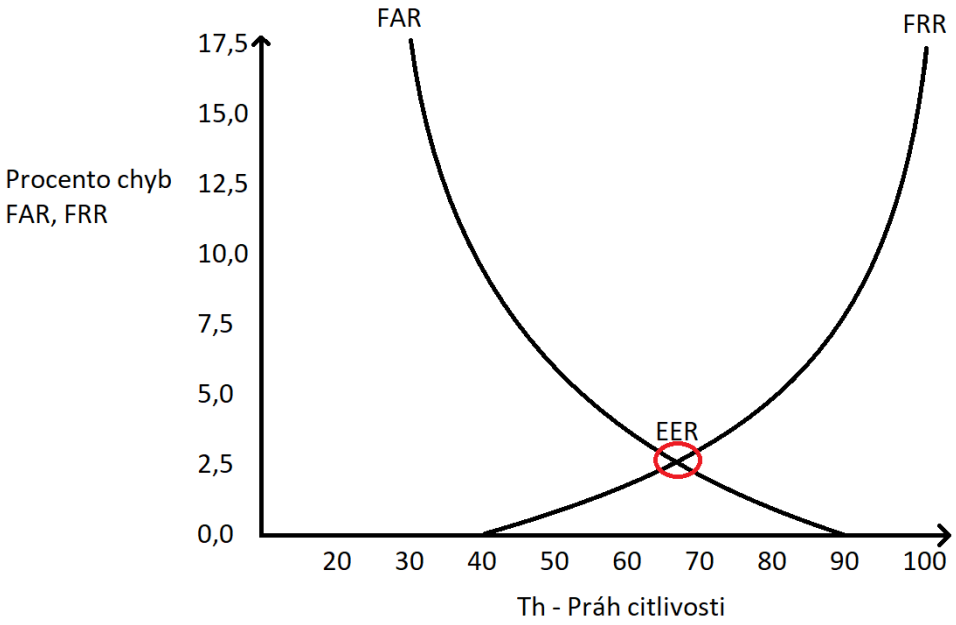
Číselné hodnoty mají nulovou vypovídající hodnotu bez kontextu. Hodnoty pravděpodobnosti chybného odmítnutí i chybného přijmutí odpovídají prahu citlivosti. V ideálním biometrickém systému by korelace hodnot FAR a FRR vypadaly:



Obrázek 5 Ideální biometrický systém [1]

Z grafu můžeme vyčíst, že čím vyšší práh citlivosti, tím menší hodnota FAR a tím větší hodnota FRR. FAR hodnota dokonce dosahuje záporných hodnot, jakmile začne růst FRR.

V reálném biometrickém systému to ovšem vypadá jinak:



Obrázek 6 Reálný biometrický systém [1]

Z grafu lze vyčíst, že čím menší práh citlivosti, tím nižší FRR, menší chybné odmítnutí, ale tím vyšší FAR, chybné přijmutí a opačně. Připodobnit to lze ke dveřím. Pokud jsou otevřené, tak vlastník má mnohem jednodušší přístup do objektu, ale i každý má přístup do objektu. Pokud jsou dveře zavřené na tři zámky a za mřížemi, tak vlastníkovi trvá mnohem déle, než se dostane do objektu, ale i ostatním trvá mnohem déle, nebo je dokonce nemožné se dostat do objektu.

Stav rovnosti je v bodu EER, Equal Error Rate, česky Stejná chybovost, kdy FAR je v rovnosti s FRR, okolo 2,5 % v prahu citlivosti cca 65.

Pro naše výsledky na Richter Czech Smart Handle H.03 vychází z výsledků pravděpodobnosti chybného odmítnutí (4 %) práh citlivosti okolo cca 75. Z hodnoty prahu citlivosti se můžeme dozvědět, že pravděpodobnost chybného přijmutí se pohybuje okolo l,25 %. Hodnoty při testování pro FAR vyšly 0 %, důvodem je opět nízký počet uložených šablon v systému mechatronické kliky. Biometrická čtečka ve dveřní kování Richter Czech Smart Handle H.03 lze označit pro užití v běžném prostředí (např. kanceláře, nájemní byty, sklepy…) jako spolehlivá. Ovšem pro objekty s vyšším a vysokým stupněm zabezpečení je práh citlivosti 75 nedostačující.

5 SOUČASNÉ ZABEZPEČENÍ VSTUPU NÁJEMNÍCH DOMŮ A BYTŮ

Zabezpečení nájemních domů a bytů se za poslední léta značně zlepšilo, avšak dle statistik kriminality je procento vykradených bytů stále vysoké. Pokud porovnáme rok 2017 až rok 2021 (viz Tabulka 4 Statistika kriminality vloupání do bytu), počet vloupání do bytu se snížil o 2 %, ale stále se pohybujeme okolo 10 %.

Rok	Krádeže vloupáním do bytů	Krádeže vloupání celkem	Poměr
2017	2518	24 127	10,44
2018	2171	21 151	10,26
2019	2144	22 161	9,67
2020	1861	20 661	9,01
2021	1553	18 812	8,26

Tabulka 4 Statistika kriminality vloupání do bytu [15]

Jedním z faktorů snížení počtu krádeží vloupáním do bytu je zvýšené zabezpečení vstupů, a to jak vstupu do nájemního domu, tak i do jednotlivých bytů. Ovšem stále je zde značný počet nezabezpečených nebo nedostatečně zabezpečených bytů i nájemních domů. Vstupy do nájemních domů bývají často dobře zabezpečeny na rozdíl od vstupu do jednotlivých bytů, které často jsou zabezpečeny pouze klasickou cylindrickou vložkou.

5.1 Nedostatky vstupů

Vstupy nájemních bytů v některých případech trpí značnými nedostatky. Nájemní domy mívají velice dobře zabezpečené vstupy s bezpečnostním zámkem, kováním. Pachatelé se dostávají do nájemních domů vynalézavostí, zazvoněním na libovolný byt a předstíráním, že jsou nájemníci, návštěva, či řemeslníci, nebo využijí nájemníka procházejícího dveřmi, také využívají anonymitu.

Nájemní byty pak se svým nedostatečně zabezpečeným vstupem představují pouze malou překážku. Hlavními nedostatky vstupů nájemních domů, jež byly odpozorovány, jsou:

- nedostačující, v mnoha případech zastaralé cylindrické vložky:

    - Pro pachatele nepředstavuje žádný problém vyháčkování zámku.
- odhalená cylindrická vložka:
    - Lze ji rozlomit.
- z dodatečných bezpečnostních prvků se nachází pouze bezpečnostní řetízek:
    - Bezpečnostní řetízek lze prolomit pouhým úderem ramenem na dveře.
- nájemníci často nezamykají, pouze zavřou dveře:
    - Netýká se zabezpečení dveří, pouze nepozornosti nájemníků.

Všechny tyto nedostatky se dají vyřešit výměnou či přidáním nových bezpečnostních prvků, jakými jsou např.:

- nové dveřní kování,
- nová cylindrická vložka,
- přídavný zámek,
- přidání mechatronických prvků,
- výměna standardních dveří za bezpečnostní,
- apod.

Vše opět záleží na vlastníkovi(vlastnících/nájemnících), kolik jsou ochotni investovat do zabezpečení majetku nájemního domu či bytu.

6 NÁVRH ZABEZPEČENÍ VSTUPU BYTŮ

6.1 Bezpečnostní posouzení objektu

Uvažujme nájemní dům se třemi nadzemními patry, bez sklepní jednotky a podzemní garáže. V přízemí a na každém patře se nacházejí čtyři byty. Dům se nachází v hustě zabydlené oblasti. Jedná se o starší budovu, po rekonstrukci fasády a vnitřních prostor. Rekonstrukce zahrnovala výměnu starých oken za nová plastová s vícevrstvou okenní tabulí a výměnu starého nábytku za nový v nájemních bytech.

Zabezpečení zahrnovalo pouze vstup nájemního domu a byt správce, kvůli zabezpečení náhradních klíčů a dokumentů. Vstup nájemního domu byl opatřen bezpečnostními dveřmi s ocelovou konstrukcí, hliníkovým rámem a ocelovým opláštěním s tříbodovým bezpečnostní zámkem, třemi závěsy s pojistkou vůči vysazení a s dveřním madlem. Otevření je nastaveno na klíč, nebo na vzdálené otevření přes tlačítko v bytech. Vstup do bytu správce byl opatřen novým protipožární zadlabávaným zámkem, novou cylindrickou vložkou s bezpečnostní třídou 3 a s bezpečnostním kováním.

Průměrná hodnota majetku v bytech se odhaduje na cca 150 tisíc korun českých. Hodnota se odvozuje od nového nábytku a elektroniky, vzhledem k vlastnímu majetku nájemníků.

6.2 Přehled, popis, zdůvodnění a cena použitých komponentů

Vstupy nájemních domů jsou tvořeny dřevěnými dveřmi o šířce 50 mm se zadlabávaným zámek a cylindrickou vložkou se standardním kováním, usazenými na 3 závěsech. Z doplňkových bezpečnostních prvků obsahují vstupy bezpečnostní řetízek a kukátko. Pro zabezpečení vstupu bytů se použijí následující komponenty:

Komponent	Název použitého zabezpečení
Zadlabávaný zámek	FAB 4292
Cylindrická vložka	Oboustranná cylindrická vložka FAB 3
Pojistky proti vysazení	Pojistky dveřních závěsů
Dveřní kování	Richter Smart Czech Handle H.03

Tabulka 5 Komponenty zabezpečení vstupu [vlastní zdroj]

6.2.1 FAB 4292

Jedná se o protipožární zadlabávaný zámek určený pro vstupní dveře pro byty. Obsahuje otvor pro cylindrickou vložku a otvory v bočních deskách pro rozetové dveřní kování. Rozměry zámku jsou:

- rozteč, rozměr mezi ořechem kliky a cylindrické vložky, 72 mm,
- backset, vzdálenost mezi středem kliky a čelem zámku, 55 mm,
- hloubka zádlabu 80 mm,
- šířka čela 20 mm,
- ořech, pro usazení kliky, 8 mm. [16]

Důvodem zvolení FAB 4292 je výměna stávajícího starého zadlabaného zámku. Protipožární vlastnosti jsou výhodou pro budoucí výměnu stávajících dveří za protipožární. Vybrán byl také pro otvory v bočních deskách pro rozetové kování. Alternativou k FAB 4292 je FAB 190/140, ovšem bez protipožárních vlastností a o cca 200,- Kč levnější.

Obrázek 7 FAB 4292 [16]

6.2.2 Oboustranná cylindrická vložka FAB 3

Oboustranná cylindrická vložka FAB 3 je tvořena z mosazi, uzamykací systém je 5tistavítkový. Obsahuje ochranu proti odvrtání (určena mimo jiné pro vstupní dveře bytu). Vybraný rozměr bude 35+35 mm, jelikož dveře budou mít s rozetovým kováním šířku 70 mm. [17]

Důvodem zvolením cylindrické vložky FAB 3 je zvýšená ochrana proti odvrtání, zabrání lépe připraveným pachatelům.

6.2.3 Richter Czech Smart Handle H.03

Richter Czech Smart Handle H.03 je rozetové dveřní kování s mechatronickou klikou určené pro dveře s tloušťkou 38-56 mm. Rozměr rozet je 60 mm průměr, rozteč šroubů a závitů 40 mm, výška 10 mm. Mechatronická klika je z vnitřní strany vždy aktivní, pokaždé se dá otevřít, a z vnější strany je uzamčena a lze otevřít pomocí otisku prstu, PIN kódu, či chytrým telefonem. Spravovat ji lze za pomoci chytrého telefonu. Po zavření dveří je střelka jištěna. Aplikaci „Janus Lock“ určena pro správu lze stáhnout z Google Play na Android zařízeních, či App Store na Apple zařízeních. [18]

6.2.3.1 Popis aplikace

Uživatel se nejdříve musí zaregistrovat pomocí e-mailové účtu, kde zadá e-mail, jméno a příjmení, poté zadá heslo o alespoň 6 znacích a na uvedenou e-mailou adresu přijde aktivační e-mail. Může se též zaregistrovat pomocí Google, Facebook či WeChat účtu. Aplikaci lze poté zabezpečit 4místným PIN kódem. Aplikace poté přejde na výpis všech spárovaných klik.

Obrázek 8 Aplikace Janus Lock [vlastní zdroj]

Ikona ozubeného kola v levém horním rohu otevírá nastavení účtu. Zde lze najít jméno vlastníka účtu, hashovaný email/účet, zdali je zapnuté zabezpečení aplikace pomocí PIN kódu, jazyk aplikace a možnost odhlášení.

Ikona plus v pravém horním rohu odkazuje na spárování s klikou. Nejdříve bude aplikace vyhledávat v okolí zařízení, poté, co najde, se zoobrazí upozornění, že se má zmáčknout jakékoliv tlačítko, aby se mohlo spárovat s mobilem. Poté stačí vybrat danou kliku.

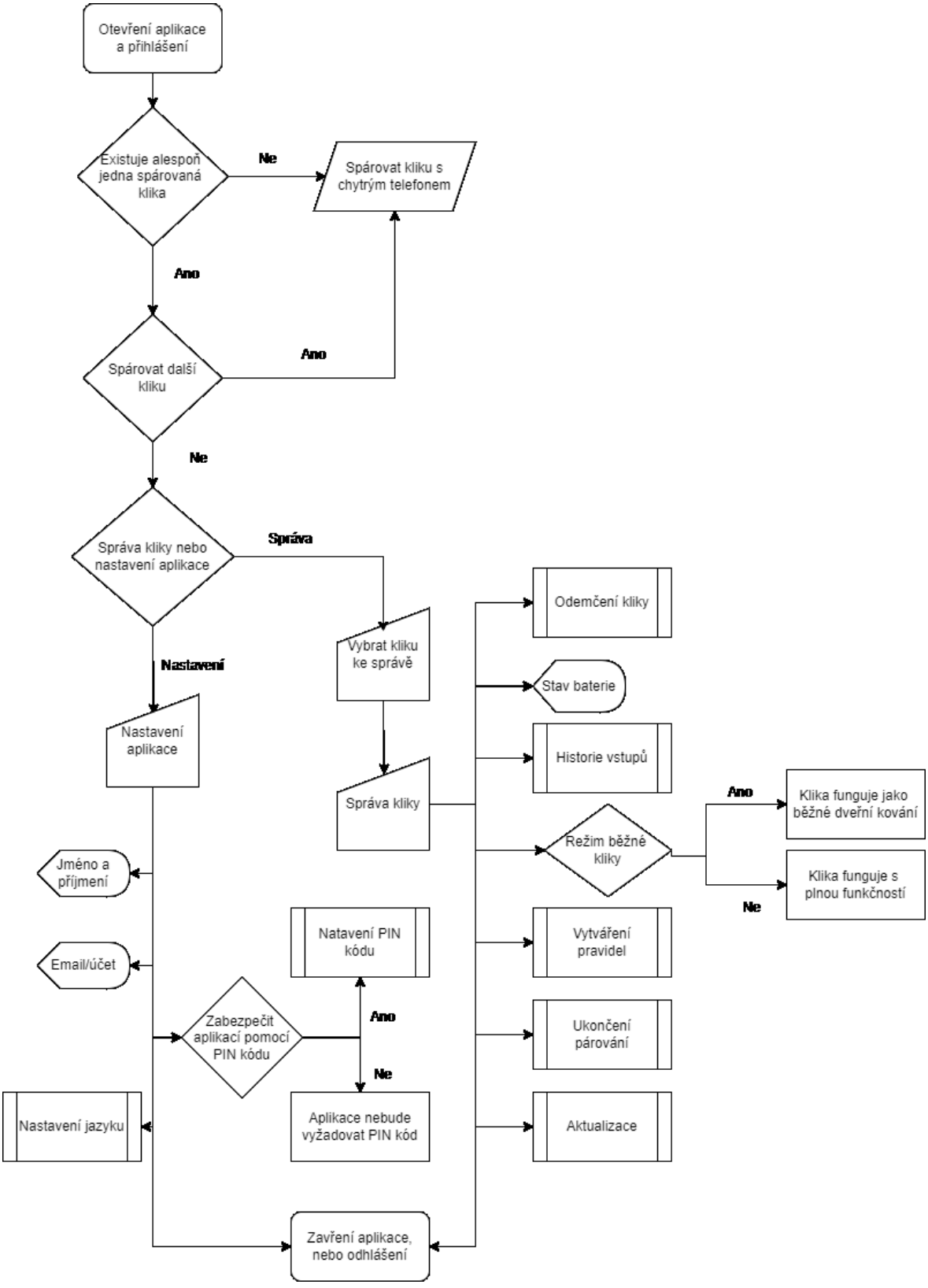
Obrázek 9 Párovaní kliky s mobilem v aplikaci [vlastní zdroj]

Spárování kliky s chytrým telefom probíhá přes Bluetooth. Vývojový diagram průběhu spárování kliky:

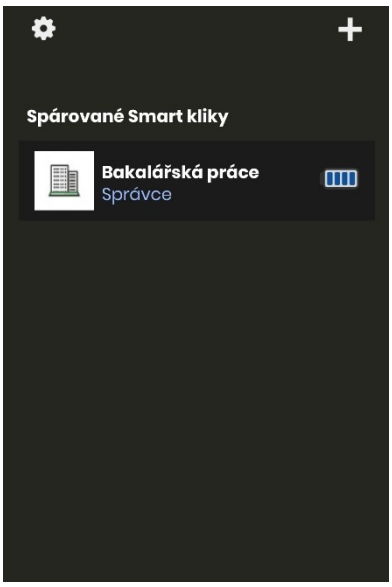
Obrázek 10 Průběh spárování

[vlastní zdroj]

Používání aplikace:

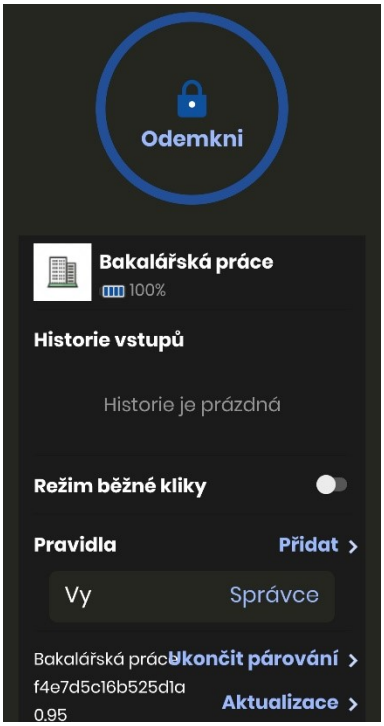


Obrázek 11 Správa Aplikace [vlastní zdroj]



Obrázek 12 Přehled v aplikaci [vlastní zdroj]

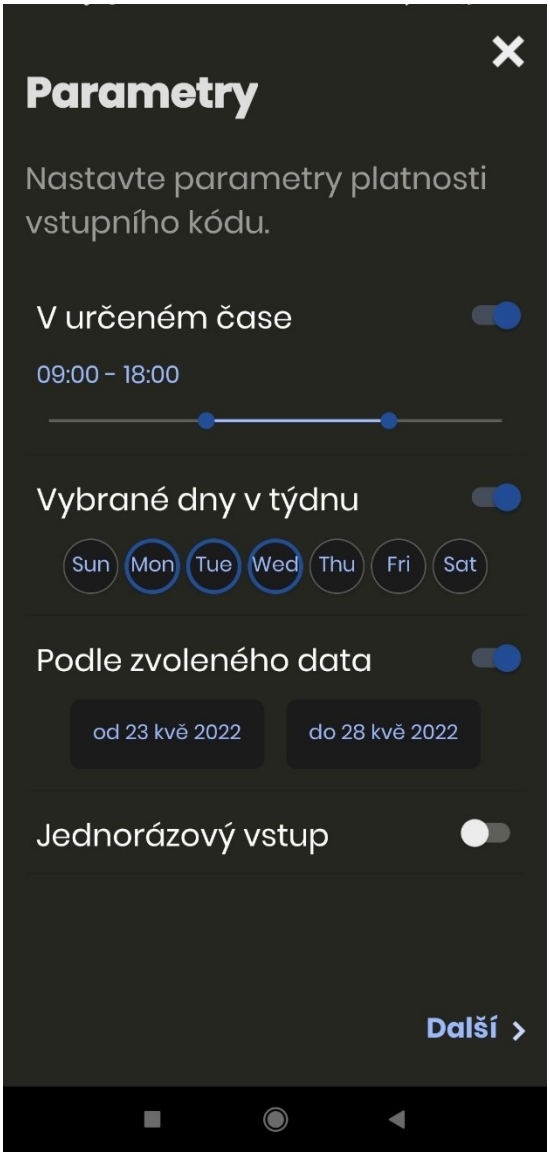
Po rozkliknutí jedné z ikon se otevře samotné nastavení kliky, kde lze odemknout kliku, vidět historii vstupů, přepnutí na režim běžné kliky, kdy se přestane jistit střelka, a pravidla, kde lze nastavit otevírání.



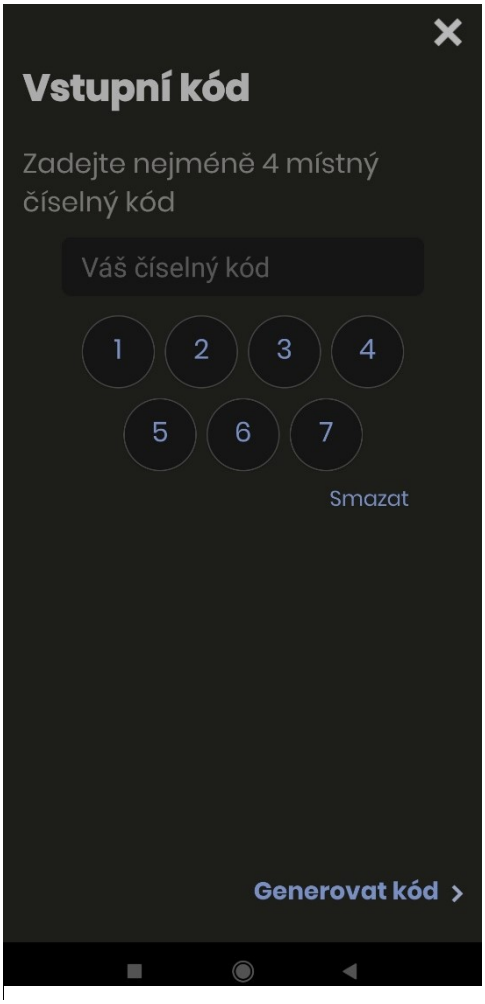
Obrázek 13 Správa kliky v aplikaci [vlastní zdroj]

Při vytváření pravidla lze nastavit:

- záslání přístupu na registrovaný účet:
    - Odešlou se přístupová pravidla jinému uživateli.
- vytvoření vstupního kódu:

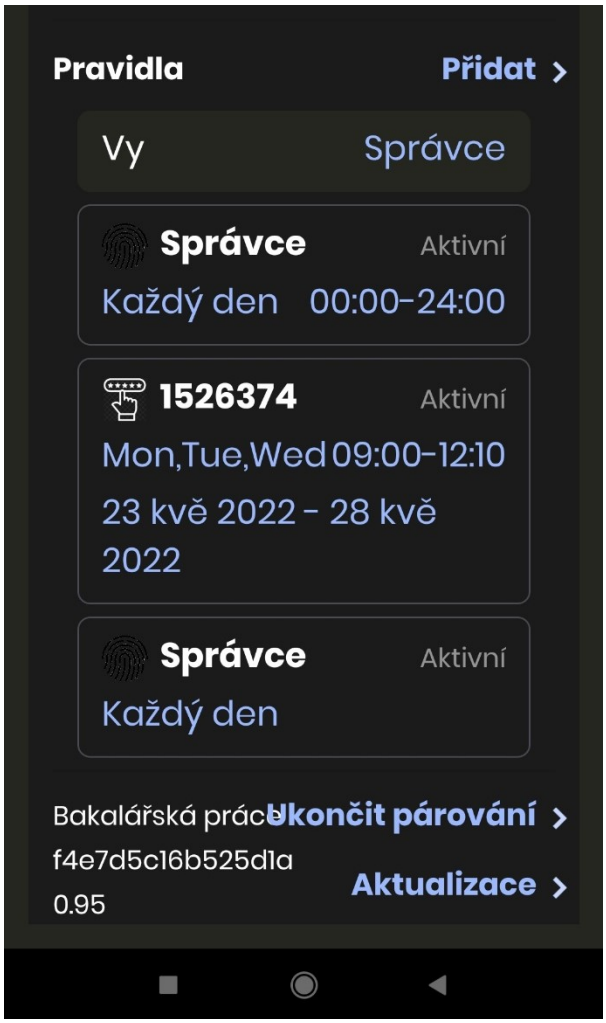


Obrázek 14 Nastavení parametrů pro vstupního PIN kódu [vlastní zdroj]



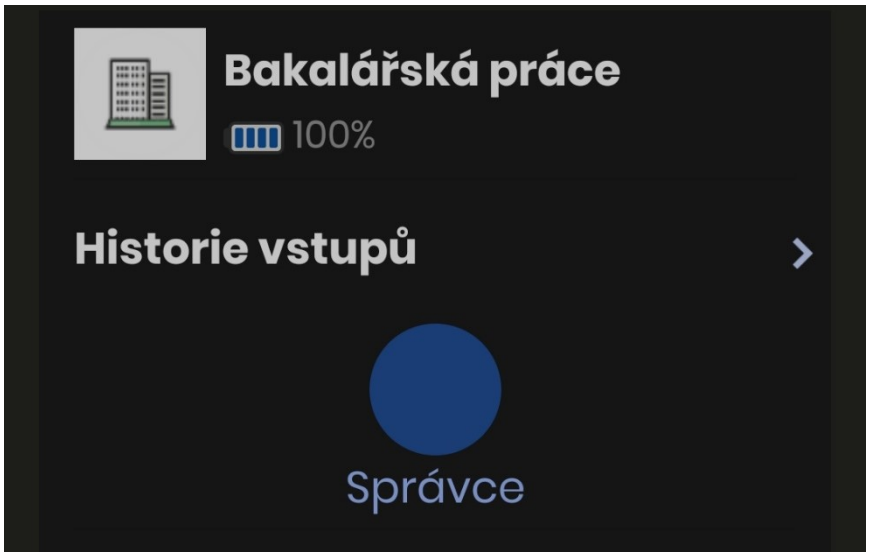
Obrázek 15 Nastavení PIN kódu
[vlastní zdroj]

- 1-denní:
    - Vytvoří se PIN kód pouze na vybraný den.
- uložit nový otisk prstu:
    - Při vytváření musí být mobil blízko kliky, při vytváření otisku se rozsvítí čtečka otisku prstu a třikrát se nasnímá otisk, poté se nastaví jméno pro otisk a uloží se do pravidel.



Obrázek 16 Vytvořená pravidla [vlastní zdroj]

V aplikaci lze sledovat i historii vstupů, která se ukládá při užití otisku prstu na otevření.



Obrázek 17 Historie vstupů v aplikaci [vlastní zdroj]

Obrázek 18 Výpis historie vstupů za poslední 180 dnů
[vlastní zdroj]

6.2.3.2 Zhodnocení a důvod použití

Přednostmi dveřního kování Richter Czech Handle H.03 jsou:

- zadržení střelky:
  - Střelkou nejde zatáhnout pouhým klíčem, uživatel se musí autorizovat.
- více možností zajištění:
  - Kliku lze zajistit nasnímáním otisku prstu, natavením PIN kódu, či otevírání chytrým telefonem.
- decentralizované řízení:
  - Pouze uživatel, který spároval svůj telefon s klikou jí může nastavovat a spravovat.
- jednouchá správa v aplikaci,
- jednoduchá instalace:
  - Stačí pouze aku vrtačka s 5 mm vrtákem, šroubovák je dodáván v balení, anebo jde použít šroubovák s křížovou hlavou PH1.

- nemusí se spárovat v nastavení Bluetooth:
    - Aplikace si kliku/kliky vyhledává sama.
- na jednu kliku nemůže být zaregistrováno více telefonů:
    - Klika je zaregistrovaná pro telefon, který se s ním pároval. Přístupová práva, ale lze odeslat.

Nevýhody dveřního kování Richter Czech Handle H.03 jsou:

- horší připojení:
    - Aplikace má občas horší spojení s klikou, kdy aktualizace pravidel a operace s klikou trvají delší čas. Nejrychlejší spojení bývá v těsné blízkosti kliky.
- nutnost chytrého telefonu:
    - Pro správu kliky je nutný chytrý telefon. Může představovat problém pro starší generaci.
- neexistuje možnost centralizace:
    - Nelze vytvořit správce, který by mohl vytvářet pravidla pro obyvatele a neviděl by zadaný PIN kód pro otevírání, či odemykat pomocí telefonu.
- nemá certifikaci Národního bezpečnostního úřadu.

Důvodem zvolení Richter Czech Smart Handle H.03 je multifunkčnost zařízení a dobrý poměr cena/výkon. Uživatel si může zvolit z několika možností zajištení kliky. Při ceně na trhu v rozmezí 3 200,- Kč až 4 000,- Kč se jedná o cenově dostupější mechatronickou (kliku).

6.2.4 Cena návrhu

Cena jednotlivých komponent:

Komponent	Cena za jednotlivý kus (s DPH)	Cena za jednotlivý kus (bez DPH)
FAB 4292	360,- Kč	298,- Kč [16]
Oboustranná cylindrická vložka FAB 3	395-843,- Kč (podle rozměru)	327-697,- Kč (podle rozměru) [17]
Oboustranná cylindrická vložka FAB 3 35x35	459,- Kč	380,- Kč
Pojistky dveřních závěsů	235,- Kč	195,- Kč [19]
Richter Smart Czech Handle H.03	3 252,- Kč	2 688,- Kč [18]
Celkem	4 306,- Kč	3 561,- Kč

Tabulka 6 Ceník komponent [vlastní zdroj]

Cena zabezpečení jednoho vstupu bytu by byla 4 306,- Kč s DPH, 3 561,- Kč bez DPH. Pro všechny byty, kromě bytu správce, by zabezpečení vstupu stálo 64 590,- Kč s DPH, 53 415,- Kč bez DPH.

7 BUDOUCNOST BIOMETRICKÝCH A MECHATRONICKÝCH SYSTÉMŮ

Moderní technologie stále zlepšují a jedním z nezanedbatelných faktorů, který přispěl k rychlému technologického pokroku, je výpočetní technika. Biometrii pomohl tento technologický pokrok. Miniaturizace pomohla aplikovat jiné biometrické prvky, jako je např. oční duhovka. Ovšem pokrok v biometrii nebyl jen díky miniaturizaci. Zrychlení procesů i zefektivnění chodu vytvořilo prostor pro rychlejší a přesnější čtečky otisků prstů, kvalitnější rozpoznávání obličeje a rozšiřování využití ostatních biometrických prvků, kupříkladu dříve zmíněné oční duhovky.

Identifikace podle otisku prstu je stále nejpoužívanější a veřejností velice oblíbená. Důvod její oblíbenosti je v její spolehlivosti v systémech a jasné jedinečnosti. Užití nalézá v chytrých telefonech, čtečkách pro přístupové systémy i systémech kontroly vstupu.

Identifikace podle obličeje nalézá též užití v chytrých telefonech, ale i při kontrole nastupujících pasažérů, či vyhledávání osoby v davech. Efektivita se zlepšila díky lepšímu rozlišení kamer a rychlejšímu vyhledávání v databázích pomocí lepšího hardwaru.

Identifikace podle oční duhovky je využívaná hlavně v prostorech s vyšším a vysokým stupněm zabezpečení, nebo zastřežení prostor pro zaměstnance, v místech s velkým počet osob.

Biometrie přináší vysokou míru bezpečnosti a jednoduchá a pohodlná obsluha biometrických systémů je pro uživatele více než přívětivá. Budoucnost biometrie je jasná, stále se budou rozvíjet nové metody a automatizace stávajících metod pro komerční užití, kupříkladu DNA či tvar vnějšího ucha. Ovšem stále zůstane ověřování a identifikace pomocí otisku prstu, obličeje či oční duhovky.

7.1 Budoucnost mechatronických systémů

Mechatronické systémy mají nesmírnou výhodu v realizování dosud nerealizovatelných funkcí zařízení, snížení ekonomických nákladů a multifunkčností. [20]

Díky těmto přednostem mají mechatronické systémy před sebou slibnou budoucnost. Systémy se budou vylepšovat. Zpřesní a zrychlí se vyhodnocování, přibydou nové možnosti řízení i nové možnosti aplikací. Běžné elektromechanické i elektromotorické systémy, neelektronické cylindrické vložky i dveřní kování budou mít stále místo pro své zlepšování i místo na trhu jako dostupnější alternativa pro mechatronické zařízení.

ZÁVĚR

Biometrické systémy prošly během posledních let značným vývojem. Kombinací s mechatronickým dveřním kováním, či zámkovým systémem se vytvořilo kvalitní zabezpečení vstupu. Jedny z možných metod, jak posuzovat spolehlivost biometrické čtečky je podle metod FRR (Pravděpodobnost chybného odmítnutí) a FAR (Pravděpodobnost chybného přijmutí).

Výsledky metody FRR pro Richter Czech Smart Handle H.03 vycházely 4 %. Pro metodu FAR vycházely 0 %. To odpovídá prahu citlivosti okolo 75 ze 100, kdy porovnávaný otisk se musí shodovat alespoň ze 75 %. Příjemně mě překvapilo, že systém má takto nastavený práh citlivosti, očekával jsem, že bude blíž k 60-65.

I přes snižující se počet vloupání do bytu není dobré podceňovat zabezpečení bytu. Pro zabezpečení vstupu jsem zvolil kombinaci nového zadlabávaného zámku FAB 4292, cylindrické vložky FAB 3***, pojistky proti vysazení dveří, a právě Richter Czech Smart Handle H.03. Prvky byly zvoleny tak, aby se zamezilo vyháčkování, vyvrtání cylindrické vložky a vysazení dveří.

Práce s Richter Czech Smart Handle H.03 byla z mé strany pozitivní. Montáž proběhla rychle, správa s aplikací je intuitivní a otevírání otiskem prstu je přirozené. Jedna z výtek je občas horší připojení přes Bluetooth, kdy se aplikace nemohla spojit s klikou, aktualizace pravidel či otevíraní přes chytrý telefon trvalo déle nebo neproběhlo vůbec. Další nevýhodou je nutnost chytrého telefonu pro nastavení a správu.

Mým názorem je, že obdobné mechatronické systémy uvidíme i nadále. Ať už se jedná o systémy podobné Richter Czech Smart Handle H.03, nebo FAB ENTR. Na trhu mají místo a je to hlavně pro usnadnění přístupu oprávněných uživatelů do rodinného domu, bytu nebo jiného objektu a odrazení potencionálních útočníků.

SEZNAM POUŽITÉ LITERATURY

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

[2] LUKÁŠ, Luděk. Bezpečnostní technologie, systémy a management. Zlín: Radim Bačuvčík – VeRBuM, 2015. ISBN 978-80-87500-05-7.

[3] KYNCL, Jaromír. Bezpečnost objektu ve světle moderních technologií. Praha: Komora podniků komerční bezpečnosti České republiky, 2014. ISBN 978-80-260-7115-0.

[4] IVANKA, Ján. Systemizace bezpečnostního průmyslu I. Vyd. 3. Zlín: Univerzita Tomáše Bati ve Zlíně, 2009. ISBN 978-80-7318-850-4.

[5] BASTIAN, Hans-Werner. Bezpečný dům a byt: ochrana před vloupáním, požárem a škodami způsobenými vodou. Praha: Beta, 2004. ISBN 80-7306-171-6

Elektronické zdroje

[6] *Kriminalistická Daktyloskopie* [online]. [cit. 2021-5-15]. Dostupné z: https://kriminalistika.eu/daktyl/daktyl.html

[7] ROTREKOVA, Olga. *Dermatoglyfy* [online]. [cit. 2022-05-15]. Dostupné z: https://www.sci.muni.cz/botany/rotreklova/pokusy/Dermatoglyfy.PDF

[8] Obrazce a znaky kůže [online]. [cit. 2022-05-15]. Dostupné z: http://krimispk.sweb.cz/02_exper/expertiz/02a_dakt/02a_kuze.htm

[9] *Duhovka* [online]. [cit. 2022-05-18]. Dostupné z: https://cs.wikipedia.org/wiki/Duhovka

[10] *Proč identifikace není autorizace* [online]. Optaglio, 2017 [cit. 2022-05-17]. Dostupné z: https://optaglioblog.wordpress.com/2017/07/11/proc-identifikace-neni-autentizace/

[11] *Papilární linie* [online]. 2021 [cit. 2022-05-17]. Dostupné z: https://cs.wikipedia.org/wiki/Papil%C3%A1rn%C3%AD_linie

[12] *Oční duhovka* [online]. 2021 [cit. 2022-05-17]. Dostupné z: https://cs.wikipedia.org/wiki/Duhovka

[13] *Druhy snímačů otisků prstů* [online]. ABBAS [cit. 2022-05-17]. Dostupné z: http://www.biometricke-ctecky.cz/biometriky/otisk-prstu/

[14] Jednovaječná dvojčata mají stejnou DNA, ale policii se už neschovají. *IDnes* [online]. MAFRA, 2015 [cit. 2022-05-17]. Dostupné z: https://www.idnes.cz/technet/veda/dna-analyza-jednovajecna-dvojcata.A150429_210744_veda_pka

[15] *Statistiky kriminality* [online]. Policie ČR [cit. 2022-05-25]. Dostupné z: https://www.policie.cz/statistiky-kriminalita.aspx

[16] *FAB 4292* [online]. FAB-SHOP [cit. 2022-05-25]. Dostupné z: https://www.fab-shop.cz/fab-4292-zadl-zamek-protipozarni-pravolevy.htm

[17] *Oboustranná cylindrická vložka FAB 3**** [online]. FAB-SHOP [cit. 2022-05-25]. Dostupné z: https://www.fab-shop.cz/oboustranna-cylindricka-vlozka-fab-3.htm

[18] *Richter Czech Smart Handle H.03* [online]. Alza [cit. 2022-05-25]. Dostupné z: https://www.alza.cz/smart-touch-handle-h-03-d6255266.htm

[19] *Pojistka dveřních závěsů* [online]. Bauhaus [cit. 2022-05-25]. Dostupné z: https://www.bauhaus.cz/pojistka-dverniho-zavesu-21484711

[20] Jaký je rozdíl mezi mechatronikou a elektromechanikou. *E-konstruktér* [online]. 2017 [cit. 2022-05-17]. Dostupné z: https://e-konstrukter.cz/novinka/jaky-je-rozdil-mezi-mechatronikou-a-elektromechanikou

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

2D	Dvourozměrné
3D	Třírozměrné
apod.	a podobně
např.	například
MZS	Mechanické Zábranné Systémy
RFID	Radio-frequency identification, česky Identifikace na rádiové frekvenci
FRR	False Rejection Rate, česky Pravděpodobnost chybného odmítnutí
FAR	False Acceptance Rate, česky Pravděpodobnost chybného příjmutí
EER	Equal Error Rate, česky Stejná chybovost
mm	milimetry
Kč	Koruny české
PIN	Personal Identification Number, česky Osobní identifikační číslo
DPH	Daň z přidané hodnoty

SEZNAM OBRÁZKŮ

Obrázek 1 Základní dermatoglyfy [6][7] 15
Obrázek 2 Markanty [8] 16
Obrázek 3 Nainstalovaná Richter Czech Smart Handle H.03 [vlastní zdroj] 39
Obrázek 4 Sběr hodnot pro výpočet FRR a FAR [vlastní zdroj] 40
Obrázek 5 Ideální biometrický systém [1] 42
Obrázek 6 Reálný biometrický systém [1] 43
Obrázek 7 FAB 4292 [16] 47
Obrázek 8 Aplikace Janus Lock [vlastní zdroj] 48
Obrázek 9 Párovaní kliky s mobilem v aplikaci [vlastní zdroj] 49
Obrázek 10 Průběh spárování [vlastní zdroj] 50
Obrázek 11 Správa Aplikace [vlastní zdroj] 51
Obrázek 12 Přehled v aplikaci [vlastní zdroj] 52
Obrázek 13 Správa kliky v aplikaci [vlastní zdroj] 52
Obrázek 14 Nastavení parametrů pro vstupního PIN kódu [vlastní zdroj] 53
Obrázek 15 Nastavení PIN kódu [vlastní zdroj] 54
Obrázek 16 Vytvořená pravidla [vlastní zdroj] 55
Obrázek 17 Historie vstupů v aplikaci [vlastní zdroj] 55
Obrázek 18 Výpis historie vstupů za poslední 180 dnů [vlastní zdroj] 56

SEZNAM TABULEK

Tabulka 1 Identifikační hodnoty daktyloskopických markantů [1] 17
Tabulka 2 Naměřené hodnoty FRR [vlastní zdroj] 41
Tabulka 3 Naměřené hodnoty FAR [vlastní zdroj] 41
Tabulka 4 Statistika kriminality vloupání do bytu [15] 44
Tabulka 5 Komponenty zabezpečení vstupu [vlastní zdroj] 46
Tabulka 6 Ceník komponent [vlastní zdroj] 58

SEZNAM ROVNIC

Rovnice 1 Identifikační hodnota markantů [1] 16
Rovnice 2 Počet markantů nutných v jednoznačné identifikaci [1] 17
Rovnice 3 Výpočet počtu markantů pro jednoznačnou identifikaci [1] 17
Rovnice 4 Vzorec pro výpočet chybného odmítnutí [1] 38
Rovnice 5 Vzorec pro výpočet pravděpodobnosti chybného přijetí [1] 38
Rovnice 6 Výpočet pravděpodobnosti chybného odmítnutí [vlastní zdroj] 41
Rovnice 7 Výpočet pravděpodobnosti chybného přijmutí [vlastní zdroj] 41