POLICEJNÍ AKADEMIE ČESKÉ REPUBLIKY V PRAZE
Fakulta bezpečnostně právní

Katedra kriminalistiky

Využití biometrických systémů v bezpečnostní praxi

Diplomová práce

Use of biometric systems in security practice

Diploma thesis

Vedoucí práce:

doc. Ing. Jonák Jiří Ph.D.

Autor:

Bc. Dominik Melč

Praha 2024

Čestné prohlášení

Prohlašuji, že předložená práce je mým původním autorským dílem, které jsem vypracoval samostatně. Veškerou literaturu a další zdroje, z nichž jsem čerpal, v práci řádně cituji a jsou uvedeny v seznamu použité literatury.

V Praze, dne 27. 2. 2024

……

Bc. Dominik Melč

Poděkování

Děkuji svému vedoucímu diplomové práce doc. Ing. Jiřímu Jonákovi Ph.D. za odbornou pomoc, rady a vedení při konzultacích a vypracování této práce.

Anotace:

Biometrie je vědní obor, který se zabývá studiem a zkoumáním jedinečných biologických a behaviorálních charakteristik člověka. Biometrické systémy se v bezpečnostní praxi využívají k různým účelům, například k řízení přístupu do objektů nebo systémů, k autentizaci uživatelů nebo k identifikaci osob. Tato diplomová práce se zabývá využitím biometrických systémů v bezpečnostní praxi a výzkum byl zaměřen na nástroje vyhledávání obličejů v internetovém prostředí pro policejní účely.

Klíčová slova:

biometrie, bezpečnost, identifikace, autentizace, biometrické systémy, rozpoznání obličeje

Annotation:

Biometrics is a discipline that deals with the study and investigation of the unique biological and behavioral characteristics of humans. Biometric systems are used in security practice for a variety of purposes, such as controlling access to facilities or systems, authenticating users, or identifying people. This thesis examines the use of biometric systems in security practice and the research focused on face retrieval tools in the internet environment for police purposes.

Keywords:

biometrics, security, identification, authentication, biometric systems, face recognition

Seznam použitých zkratek

AFIS	Automated fingerprint identification
FAR	False Acceptance Rate
FRR	False Rejection Rate
EKG	Elektrokardiografie
IT	Informační technologie
GDPR	General Data Protection Regulation

Obsah

Úvod

Bezpečnost je jednou z nejdůležitějších priorit moderního světa. V posledních letech dochází k neustálému vývoji nových technologií, které mají za cíl zvýšit bezpečnost osob a majetku. Jednou z těchto technologií je biometrie, nebo také biometrika.

Biometrika je obor zabývající se měřením a vyhodnocováním kvantitativních znaků živých organismů, biologických charakteristik a charakteristik chování lidí. Jde o měření a analýzu specifických fyzických nebo i behaviorálních charakteristik, které jsou jedinečné pro každou osobu. Může jít právě o otisky prstů, ale také sken duhovky, rysy v obličeji, hlas anebo i chování.

V bezpečnostní praxi se biometrické systémy využívají k různým účelům, například k řízení přístupu do objektů nebo systémů, k autentizaci uživatelů nebo k identifikaci osob.

Samotná biometrika má velký přínos i pro samotnou Policii České republiky, a to nejenom ve smyslu typické identifikace osob, ale i jiné formy využití.

V rámci bezpečnostní praxe má biometrie velký potenciál. Biometrické systémy mohou policii pomoci v identifikaci osob, autentizaci osob anebo v řízení přístupů oprávněných osob do objektů apod.

Tato práce seznamuje se základními pojmy, kategorizací a příklady biometrie.

Cíle práce

Cílem této diplomové práce je analyzovat využití biometrických systémů v bezpečnostní praxi, zejména u Policie České republiky.

V první části práce bude proveden teoretický úvod do problematiky biometrie. V druhé části práce budou popsány některé konkrétní biometrické technologie, které Policie ČR a jejich využití v bezpečnostní praxi. V třetí části práce budou prezentovány výsledky průzkumu, který se zaměřil na využití

komerčních nástrojů na vyhledávání obličejů v internetovém prostředí pro účely policejní činnosti.

Metodika

Práce je členěna do kapitol a podkapitol, které jsou ve vzájemné návaznosti. Kapitola č. 1 „První část“ vysvětluje v podkapitolách pojem biometrie, provází historií vzniku biometrie a principem, jakým biometrie funguje. Její podkapitoly se detailněji zabývají výše uvedeným. Kapitola č. 2 „Druhá část“ se poté zabývá přímo způsoby, jakými Policie České republiky využívá některé biometrické systémy. Kapitola č. 3 „Třetí část“ se zabývá provedeným výzkumem ve využití komerčním nástrojem dostupným na internetu pro vyhledávání obličejů pro účely policejní činnosti.

Všechny informace autorem využité při zpracování této diplomové práce byly získány z odborné literatury, interních aktů, zákonů a dostupných internetových zdrojů.

1. První část

První část diplomové práce seznamuje s teoretickým úvodem do problematiky biometrie, dělení biometrik, historií a základními pojmy.

1.1. Biometrie

Slovo biometrie, které je původem z řečtiny, se skládá ze slovního spojení slov „bio“, znamenající život, a „metric“, které znamená měření. V minulosti byla biometrie vymezována jako souhrn matematických metod, využívaných v lékařství a biologických vědách. Nyní lze biometrii popsat jako vědní obor, který se zabývá měřením určitých charakteristik člověka. Termín biometrie využívá v praxi více oborů, jako je biomedicína, kriminalistika nebo IT. V biomedicíně se biometrie používá k provádění statistických výpočtů v biologii nebo medicíně. Tyto výpočty mohou být použity například pro výzkum genetických oborů. Biometrické systémy se v oboru kriminalistiky používají k identifikaci a autentizaci osob v rámci prověřování trestné činnosti. Tyto systémy využívají jedinečné, měřitelné fyziologické a behaviorální vlastnosti člověka k automatické identifikaci nebo ověření jeho identity. V IT se biometrie používá k identifikaci a ověření identity člověka. Biometrické systémy využívají jedinečné, měřitelné fyziologické a behaviorální vlastnosti člověka k automatické identifikaci a ověření jeho identity.

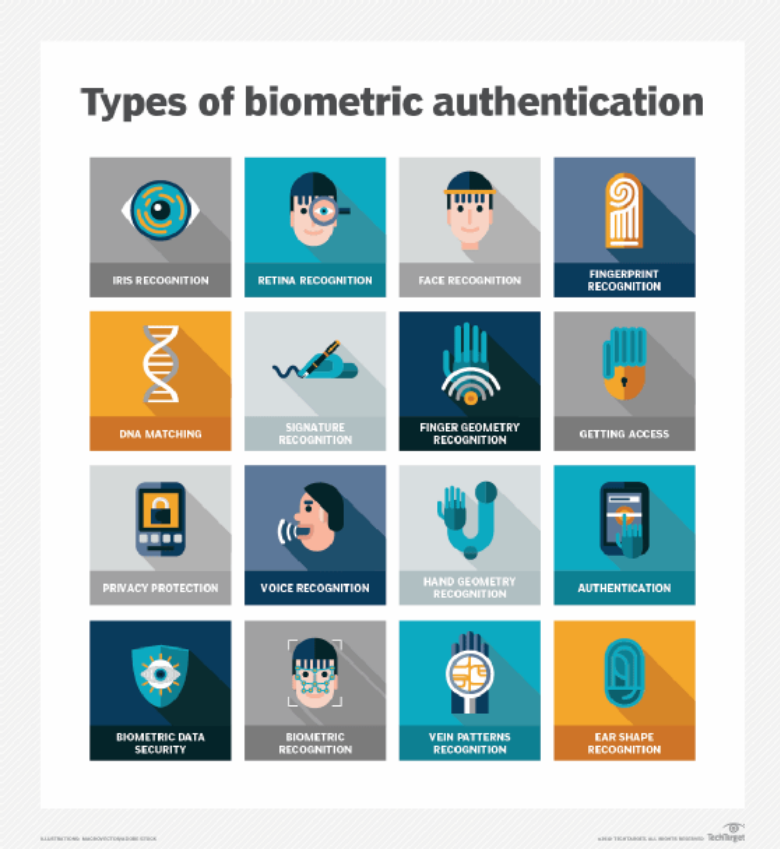
Jako každý způsob identifikace osob má i biometrie své výhody a nevýhody. Největší výhodou je jednoduchost, neboť biometrickou vlastnost nelze zapomenout, ztratit či přenést na jinou osobu. Dále také odrazení útočníka od podvodů a eliminace pokusů o popření identity osoby. Užití biometrie také zvyšuje stupeň zabezpečení a snadnost použití zvyšuje úroveň pohodlí identifikovaných osob.[1]

1 DRAHANSKÝ, Martin a Filip ORSÁG a kolektiv. Biometrie. Brno: Computer Press, 2011. ISBN 978-80-254-8979-6.

1.2. Dělení biometrik

Biometrické systémy se rozdělují na dvě hlavní kategorie: anatomicko-fyziologické a behaviorální nebo také dle způsobu využití (obrázek č. 1). Tyto systémy využívají biometrické charakteristiky, které jsou u každého jedince jedinečné a měřitelné. Tyto charakteristiky se shromažďují, zpracovávají, vyhodnocují a ukládají během procesů identifikace a verifikace. Behaviorální charakteristiky, jež souvisí s lidským chováním, se v praxi používají méně často kvůli jejich nižší objektivitě.

Pro využití biometrické charakteristiky je nezbytná její jedinečnost, stálost, měřitelnost, výkonnost a akceptace uživatelů, tedy ochota osob nechat si svou charakteristiku nasnímat. Dále je důležitá odolnost proti padělání a schopnost charakteristiky podrobit dalšímu zpracování pro vyhodnocení a porovnání.[2]



Obrázek č. 1 – Typy biometrických systémů

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

Anatomicko-fyziologické biometrické charakteristiky

Anatomicko-fyziologické biometrické charakteristiky odkazují na ty aspekty biometrie, které se týkají fyzických a fyziologických vlastností jedince. Tyto charakteristiky jsou obvykle jedinečné pro každou osobu a zahrnují:

- Otisky prstů: Jedna z nejznámějších a nejpoužívanějších biometrických charakteristik. Otisky prstů mají jedinečný vzor hřebenů a údolí, který je specifický pro každého člověka.
- Rozpoznání obličeje: Tato technologie analyzuje různé rysy obličeje, jako jsou vzdálenost mezi očima, tvar nosu a kontura čelisti, aby identifikovala jedince.
- Skenování sítnice: Tato metoda zahrnuje zaznamenání vzoru krevních cév umístěných na zadní části oka, který je také unikátní pro každou osobu.
- DNA profilování: DNA, nositel genetických informací, nabízí extrémně přesný způsob identifikace, ale je méně běžný kvůli složitosti a nákladům spojeným se sběrem a analýzou vzorků.
- Geometrie ruky a prstů: Tato metoda měří a analyzuje fyzické rozměry ruky a prstů, včetně délky, šířky a tvaru.
- Skenování žil: Podobně jako sítnice a iris, i vzor žil v ruce nebo prstu je jedinečný pro každou osobu a může být použit pro identifikaci.

Tyto anatomicko-fyziologické charakteristiky jsou obvykle velmi spolehlivé pro identifikaci a verifikaci identity, protože jsou jedinečné pro každého jedince a nejsou snadno měnitelné.[3]

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

Behaviorální biometrické charakteristiky

Behaviorální biometrické charakteristiky se zaměřují na měření a analýzu vzorců chování jednotlivce, které jsou jedinečné a odlišné. Tyto charakteristiky jsou založeny na tom, jak osoba něco dělá, což se může lišit v čase a může být ovlivněno řadou externích faktorů. Mezi hlavní behaviorální biometrické charakteristiky patří:

- Dynamika psaní na klávesnici: Tato metoda analyzuje způsob, jakým uživatel píše na klávesnici, včetně rychlosti a rytmu úderů, tlaku a doby mezi stisky kláves. Každý má svůj unikátní styl psaní.
- Analýza hlasu: Hlasová biometrie identifikuje a ověřuje jedince na základě jejich hlasových charakteristik, jako jsou tón, výška, rytmus a intonace. Hlas je ovlivněn jedinečnými fyzickými vlastnostmi hlasového traktu a může se měnit v závislosti na emocionálním stavu nebo zdraví.
- Chůze: Rozpoznání chůze analyzuje způsob, jakým osoba chodí, včetně rytmu, rychlosti, délky kroku a vzorců pohybu těla. Tento typ biometrie je stále ve výzkumné fázi.
- Gesty a pohyby rukou: Tato technika se zaměřuje na rozpoznávání a analýzu gest a pohybů rukou, které mohou být použity k identifikaci a ověření identity.

Behaviorální biometrie je často používána jako doplňková metoda k tradičnějším anatomicko-fyziologickým formám biometrie, protože může poskytovat dodatečnou úroveň bezpečnosti a ověřování. Je však důležité poznamenat, že behaviorální charakteristiky mohou být náchylnější k variabilitě v čase a mohou být ovlivněny různými vnějšími faktory, jako je únava, nemoc nebo emocionální stav.[4]

[4] DRAHANSKÝ, Martin a Filip ORSÁG a kolektiv. Biometrie. Brno: Computer Press, 2011. ISBN 978-80-254-8979-6.

1.3. Výhody a nevýhody biometrie

Biometrické systémy využívají fyzické nebo behaviorální charakteristiky jednotlivce k identifikaci nebo ověření totožnosti. Mohou mít různé výhody a nevýhody:

Výhody biometrických systémů:

- Vysoká spolehlivost: Biometrické charakteristiky jsou jedinečné u každého jednotlivce, což zvyšuje spolehlivost systému.
- Nepřenositelnost: Biometrické údaje jako otisky prstů nebo obličejové rysy jsou nesnadno napodobitelné nebo přenositelné.
- Rychlost a pohodlí: Ověření nebo identifikace může proběhnout rychle a pohodlně, bez nutnosti pamatovat si hesla nebo PIN kódy.
- Omezení možnosti ztráty nebo zneužití: Nelze zapomenout nebo ztratit biometrické údaje, jak tomu může být u karet či hesel.
- Využití ve více oblastech: Biometrické systémy mohou být využity v různých odvětvích, jako jsou bezpečnost, cestování, zdravotnictví a další.

Nevýhody biometrických systémů:

- Náklady: Implementace biometrických systémů může být nákladná, zejména pokud jde o vývoj a nasazení speciální infrastruktury.
- Ochrana soukromí: Sběr a uchování biometrických údajů může vyvolávat obavy ohledně ochrany soukromí. Je důležité, aby byly tyto údaje správně zabezpečeny.
- Chybovost: Přes vysokou spolehlivost může docházet k chybám při identifikaci, například kvůli špatným podmínkám (špatné osvětlení, nevhodný úhel atd.).
- Změny biometrických charakteristik: Určité biometrické charakteristiky mohou být ovlivněny faktory jako stárnutí, nemoci nebo úrazy, což může ztížit identifikaci.

- Nesouznění: Někteří lidé mohou mít z důvodu náboženských nebo etických důvodů výhrady proti používání biometrických systémů.

Celkově lze říci, že biometrické systémy mají mnoho výhod, ale také s sebou nesou určitá rizika a výzvy, které je třeba zvážit při jejich implementaci. Je důležité brát v úvahu potřeby a obavy uživatelů a zajišťovat správnou ochranu a správu biometrických údajů.[5]

1.4. Historie

Biometrické systémy, využívající fyzické nebo behaviorální charakteristiky jednotlivce k identifikaci nebo ověření totožnosti, mají kořeny sahající až do starověku. První známky využití biometrie se objevily ve starověké Číně, kde byly otisky prstů využívány pro autentizaci dokumentů již před tisíci lety.

Pomocí biometrie se lidé identifikují již od dob počátku lidstva, kdy dítě rozpoznalo své rodiče dle hlasu, někdo známý mohl být identifikován podle lokomoce nebo vzhledu tváře. Použití biometrických identifikačních metod, o kterém jsou záznamy, se datují až po faraonské dynastie v Egyptě. Mnoho dochovaných materiálů se zmiňují o využití biometrické identifikace v údolí Nilu, kdy byli rolníci při výkupu obilí a vyplácení mzdy identifikováni podle unikátních jizev, barvy pleti a očí, rozměrů a vah těla. Dochovaly se také záznamy o faraonovi Khafre, který, aby vyloučil neoprávněné nebo násobné vydání mezd na stavbě pyramid, přikázal vést záznamy o všech, kteří se na stavbě podíleli. Vždy před vyplacením byl každý zaměstnanec zkontrolován podle vedených záznamů. O zaměstnancích zaznamenával, mimo základních osobních údajů a popisu obličeje a těla, i některé tělesné rozměry (např. délku lokte) a všechna viditelná zranění.

V moderní době lze za významný milník považovat rok 1891, kdy byl argentinským policejním inspektorem Juanem Vucetichem úspěšně využit otisk

[5] PEREZ, Jose Luis. RECORDIA. Understanding Biometric Authentication: Advantages and Disadvantages [online]. [cit. 2024-02-25]. Dostupné z: https://recordia.net/en/understanding-biometric-authentication-advantages-and-disadvantages/

prstu jako důkaz při vyřešení vraždy (obrázek č. 2). Tato událost otevřela cestu pro systematické využívání otisků prstů v kriminalistice.

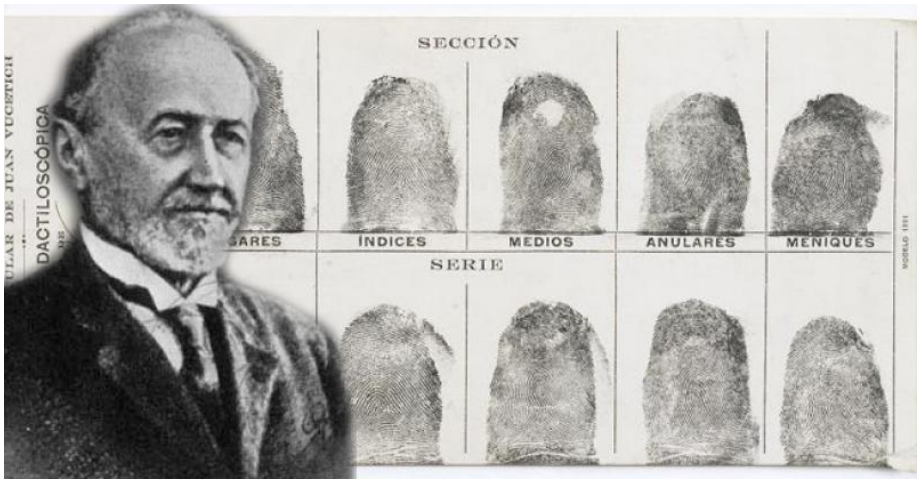
Dalším významný krok nastal v roce 1901, kdy britský antropolog Edward Henry vyvinul systém klasifikace otisků prstů, který posloužil jako základ pro moderní metody analýzy otisků. Tento systém se stal klíčovým nástrojem pro soudní a kriminalistickou identifikaci.

V 60. letech 20. století začaly vznikat výzkumné práce v oblasti rozpoznávání obličejových rysů, což vedlo k rozvoji technologií pro rozpoznávání obličejů. Tím byla položena základní kámen pro vývoj moderních systémů pro rozpoznávání tváře.

V následujících desetiletích se biometrické technologie začaly rychle rozvíjet. V 70. letech byly vyvíjeny první systémy pro rozpoznávání hlasu, využívající akustické vlastnosti řeči. Postupně se objevily další biometrické metody, jako například rozpoznávání duhovky, očního pozadí, chování nebo termální obrazovky.

V průběhu 90. let a v 21. století začaly biometrické technologie pronikat do komerčního sektoru. Využití biometrie se rozšířilo do různých odvětví, jako je bankovnictví, bezpečnost, zdravotnictví a cestovní ruch.

Dnes jsou biometrické systémy běžně využívány v každodenním životě. Skenery otisků prstů jsou integrovány do chytrých telefonů a tabletů, obličejové rozpoznávání se využívá pro odemykání zařízení a rozpoznávání hlasu umožňuje zapnout hlasové asistenty. Biometrické technologie jsou tak nedílnou součástí moderního digitálního světa a jejich vývoj stále pokračuje. Výzkumníci se zaměřují na nové metody a technologie, které budou schopny poskytovat ještě spolehlivější a bezpečnější způsoby identifikace a ověření totožnosti.



Obrázek č. 2 – Juan Vucetich a inventář otisků prstů

1.5. Základní pojmy

Pro pochopení pojednávané problematiky je třeba si definovat některé základní pojmy, které jsou úzce spojeny se samotnými biometrickými systémy.

Identita

Pojem „identita“ pocházející z latinského „identitas“ a odvozený od slova „idem“ znamenající „stejný“ se vztahuje na totožnost něčeho s jiným nebo sám se sebou. Používá se pro porovnávání, kdy lze mezi porovnávanými entitami, jako jsou pojmy nebo objekty, postavit znaménko rovnosti. Identita je utvářena kombinací faktorů včetně znalostí (to, co vím), vlastnictví (to, co vlastním) a biometrie (to, co jsem). Existují dva základní typy identity: fyzická a elektronická. Fyzická identita jedince je určena jeho vzhledem a chováním, jedná se o unikátní soubor charakteristik, kde každý má pouze jednu takovou identitu. Tuto identitu nelze zcela kopírovat mezi dvěma osobami. Na druhou stranu, elektronická identita umožňuje jednotlivci prezentovat se různými způsoby, například jako osoba, kterou by chtěl být. Jedinec si může vytvořit mnoho takových identit,

například různé účty na sociálních sítích nebo e-mailové platformy, které mohou reflektovat různé aspekty jeho osobnosti nebo zájmů.[6]

Autentizace

Autentizace je klíčovým pojmem hlavně v oblasti přístupových systémů a bezpečnosti. Proces autentizace spočívá v ověřování identity uživatele nebo entity. Tento pojem je běžně používán jak při identifikaci, tak při verifikaci, přičemž v kontextu verifikace je jeho použití častější. Autentizace je zásadní pro zajištění, že uživatelé jsou skutečně těmi, za koho se vydávají, a že mají oprávnění přistupovat k daným systémům nebo informacím. V praxi se autentizace může provádět různými způsoby, od tradičních hesel a PIN kódů až po pokročilejší metody, jako jsou biometrické technologie (například otisky prstů nebo rozpoznání obličeje) a vícefaktorová autentizace, která kombinuje několik metod pro zvýšení bezpečnosti. Rozvoj technologií, jako je kryptografie a blockchain, dále rozšiřuje možnosti a metody autentizace, poskytujíc větší ochranu a bezpečnost v digitálním světě.[7]

Identifikace

Identifikace slouží k určení identity osoby pomocí biometrického vzorku. Tato metoda, známá jako „One-To-Many Matching“ (jeden k mnoha), 1:N nebo rekognice, probíhá tak, že uživatel poskytne biometrický vzorek, aniž by předem specifikoval svou identitu. Vzorek je poté porovnán se všemi šablonami uloženými v databázi, aby se zjistilo, zda některá šablona vzorku odpovídá. Tento proces může být časově náročnější než verifikace, jelikož databáze obsahují často rozsáhlé množství šablon. Typickým příkladem systému, který

[6] DRAHANSKÝ, Martin a Filip ORSÁG a kolektiv. Biometrie. Brno: Computer Press, 2011. ISBN 978-80-254-8979-6.

[7] DRAHANSKÝ, Martin a Filip ORSÁG a kolektiv. Biometrie. Brno: Computer Press, 2011. ISBN 978-80-254-8979-6.

využívá metodu identifikace, je Automatický systém identifikace otisků prstů (AFIS).[8]

Verifikace

Verifikace se používá k ověření, zda je osoba, která se pokouší o přístup, skutečně tou, za kterou se vydává. Tento postup ověřování identity je známý jako „One-To-One Matching“ (jeden ku jednomu), 1:1 nebo autentizace, jelikož dochází k porovnání jednoho vzorku s jednou konkrétní šablonou v databázi, která náleží ověřované osobě. Na rozdíl od identifikace, kde se biometrický vzorek porovnává s mnoha šablonami, v případě verifikace osoba nejprve sdělí svou elektronickou identitu. Na základě této informace je v databázi vyhledán příslušný záznam, s nímž jsou poté porovnána předložená data. Pokud odpovídající záznam neexistuje, přístup je automaticky odmítnut. Výsledkem procesu verifikace je buď potvrzení, nebo vyvrácení deklarované identity osoby. [9]

1.6. Druhy biometrických identifikací

Biometrické identifikace lze klasifikovat do několika hlavních typů podle fyzických nebo behaviorálních charakteristik, které používají k ověření identity osoby. Zde jsou některé z nejběžnějších typů:

Biometrická identifikace na základě otisku prstu

Biometrická identifikace na základě otisku prstu je jednou z nejrozšířenějších a nejpoužívanějších forem biometrického ověřování (obrázek č. 3). Spočívá v analýze jedinečných vzorů na prstech jedince. Tato metoda začíná získáním obrazu otisku prstu, obvykle pomocí snímače, který může být optický, kapacitní, ultrazvukový nebo tepelný. Po získání obrazu systém analyzuje jedinečné rysy otisku prstu, jako jsou hřebeny, bifurkace a smyčky.

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

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

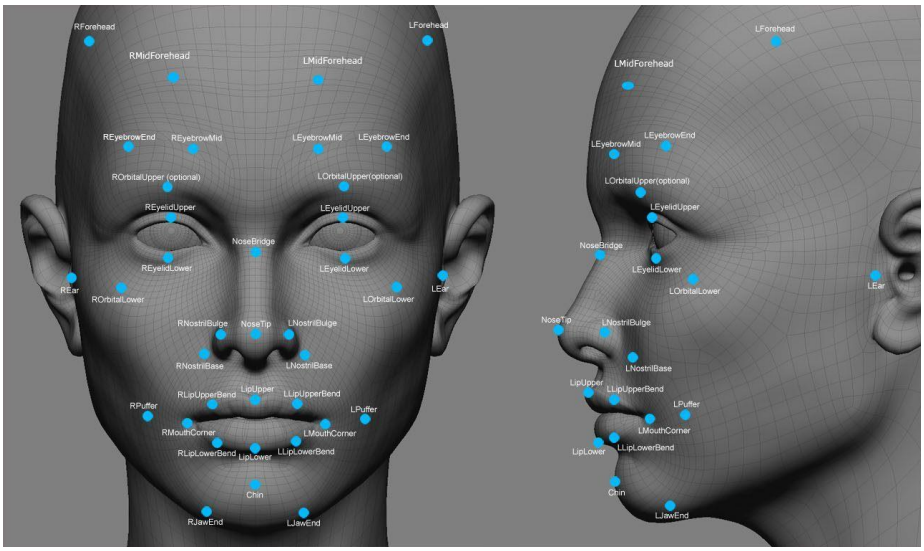
Tyto rysy jsou následně převedeny na digitální formát a uloženy pro budoucí porovnání. Když je potřeba ověřit identitu, nově získaný otisk se porovná s uloženými daty. Tato technologie se běžně používá v mnoha aplikacích, včetně zabezpečení mobilních telefonů, přístupu do budov, kontrolních systémů na hranicích a v bankovnictví. Je ceněna pro svou jednoduchost, rychlost a přesnost. Nicméně, otázky týkající se soukromí a bezpečnosti, jakož i možnost falešného přijetí nebo odmítnutí, jsou stále předmětem diskuse a výzkumu. S rozvojem technologií se vylepšují i metody pro zvýšení bezpečnosti a spolehlivosti biometrické identifikace otiskem prstu.

Obrázek č. 3 – Biometrická identifikace na základě otisku prstu

Biometrická identifikace na základě rozpoznání obličeje

Biometrická identifikace na základě rozpoznání obličeje je technologie, která identifikuje nebo ověřuje osobu pomocí jejích fyzických rysů obličeje (obrázek č. 4). Tato metoda se stala populární díky své nenáročnosti na uživatele a širokému uplatnění v různých oblastech. Princip spočívá v získání digitálního obrazu obličeje, který se může provést pomocí fotoaparátu nebo kamery. Následně dochází k analýze obrazu, kde se pomocí algoritmů rozpoznají klíčové rysy obličeje, jako jsou vzdálenosti mezi očima, nosu a ústy, tvar čelisti a další anatomické charakteristiky. Tyto rysy se převádějí na digitální

data, která se porovnávají s databází uložených obrazů obličejů pro identifikaci nebo ověření identity. Biometrická identifikace obličeje je široce používána v bezpečnostních systémech, při odemykání mobilních zařízení, v systémech pro sledování docházky a v mnoha dalších aplikacích. Tato technologie je ceněna pro svou schopnost rychlého a pohodlného ověřování, ale současně vyvolává otázky ohledně soukromí a ochrany osobních údajů. Vyvíjí se také metody pro zlepšení přesnosti a odolnosti proti falšování, jako jsou 3D skenování a analýza živých rysů.[10]



Obrázek č. 4 – Biometrická identifikace na základě rozpoznání obličeje

Biometrická identifikace na základě rozpoznání hlasu

Biometrická identifikace na základě rozpoznání hlasu je proces, který umožňuje identifikovat nebo ověřit identitu jedince na základě jedinečných charakteristik jeho hlasu. Tato technologie funguje tak, že nejprve zachytí vzorek hlasu, obvykle prostřednictvím mikrofonu nebo telefonu, poté dochází k analýze hlasového vzorku, při které se zjišťují specifické rysy, jako je tón, intenzita, výška a rytmus hlasu. Tyto charakteristiky se následně převádějí do digitální formy a porovnávají s uloženými hlasovými vzory pro identifikaci nebo ověření. Biometrická identifikace hlasem se často používá v telefonních bankovních

[10] BIOMETRICS INSTITUTE. Types of Biometrics [online]. [cit. 2024-02-17]. Dostupné z: https://www.biometricsinstitute.org/what-is-biometrics/types-of-biometrics/

službách, zákaznických centrech, při ověřování přístupu do zabezpečených systémů a v interakci s hlasově ovládanými zařízeními a digitálními asistenty. Výhodou této metody je její nenáročnost na uživatele a možnost vzdáleného použití. Nicméně, výzvami jsou citlivost na změny hlasu způsobené například nemocí nebo stárnutím a potenciál pro falšování hlasu. Proto se neustále vyvíjejí technologie pro zlepšení přesnosti a bezpečnosti rozpoznávání hlasu, včetně pokročilých algoritmů strojového učení a analýzy.[11]

Biometrická identifikace na základě oční sítnice

Biometrická identifikace na základě oční sítnice je metoda, která využívá jedinečné vzory krevních cév na sítnici oka k identifikaci jednotlivce (obrázek č. 5). Sítnice nacházející se na zadní straně oka má komplexní a jedinečnou strukturu, která se během života člověka nemění. Proces identifikace začíná skenováním oka pomocí speciálního zařízení, jež zachytí detailní obraz sítnice. Tento obraz je pak analyzován za účelem identifikace charakteristických bodů a vzorů v sítnici. Tyto informace jsou převedeny do digitálního formátu a porovnány s databází uložených vzorů sítnice pro ověření identity. Identifikace sítnice je považována za jednu z nejpřesnějších biometrických technologií díky vysoké úrovni detailů a jedinečnosti vzorů sítnice. Používá se v bezpečnostních aplikacích jako jsou přístupy do vysoko zabezpečených oblastí, v bankovnictví a v některých vládních systémech. Výzvou pro tuto technologii je potřeba spolupráce subjektu při skenování a potenciální problémy s ochranou soukromí spojené s ukládáním citlivých biometrických dat. Přes tyto výzvy je biometrická identifikace sítnice stále více využívána díky její vysoké úrovni bezpečnosti a přesnosti.[12]

[11] BIOMETRICS INSTITUTE. Types of Biometrics [online]. [cit. 2024-02-17]. Dostupné z: https://www.biometricsinstitute.org/what-is-biometrics/types-of-biometrics/

[12] BIOMETRICS INSTITUTE. Types of Biometrics [online]. [cit. 2024-02-17]. Dostupné z: https://www.biometricsinstitute.org/what-is-biometrics/types-of-biometrics/

Obrázek č. 5 – Biometrická identifikace na základě oční sítnice

Biometrická identifikace na základě chůze

Biometrická identifikace na základě chůze je relativně nová metoda, která rozpoznává a identifikuje jednotlivce podle jejich způsobu chůze. Tato metoda vychází z předpokladu, že každý člověk má jedinečný způsob chůze, který lze použít k jeho identifikaci. Proces identifikace začíná sběrem dat o chůzi jedince, což se obvykle provádí pomocí senzorů nebo videokamer. Data zahrnují různé aspekty chůze, jako je délka kroku, rytmus, rychlost a celkový vzorec pohybu. Tyto informace jsou pak analyzovány a porovnávány s databází uložených vzorců chůze, aby se určila identita osoby. Identifikace na základě chůze může být užitečná v bezpečnostních aplikacích, kde není možné nebo vhodné použít jiné biometrické metody, například v situacích, kde je potřeba identifikovat osoby na dálku nebo v pohybu. Jedná se o méně invazivní formu biometrie, která umožňuje identifikaci bez potřeby bezprostřední fyzické interakce. Nicméně, výzvou pro tuto technologii je zajištění přesné identifikace, protože chůze může být ovlivněna mnoha faktory, včetně zdravotního stavu, obuvi a únavy. Vývoj v oblasti analýzy pohybu a strojového učení však umožňuje postupné zlepšování přesnosti a spolehlivosti této metody.

Další druhy biometrických identifikací, které mohou být méně tradiční jsou například geometrie ruky, podpis, skenování žil, dynamika psaní na klávesnici,

rozpoznání ušního boltce, termografie obličeje, rozpoznání vůně, analýza elektrokardiogramu (EKG), cévní vzory na očním bělmu.[13]

1.7. Technické aspekty biometrických systémů

Biometrické systémy spojují pokročilou technologii a unikátní fyzické nebo behaviorální charakteristiky jednotlivců, aby poskytly bezpečný a efektivní způsob identifikace nebo ověření identity. Tyto systémy jsou složité a zahrnují několik klíčových technických aspektů:

- Snímače a akvizice dat: Biometrické systémy začínají shromažďováním dat pomocí snímačů, které zachytávají biometrické charakteristiky, jako jsou otisky prstů, obraz obličeje, vzor duhovky, hlas a další. Kvalita snímače a procesu akvizice dat je zásadní pro celkovou přesnost systému.

- Zpracování dat: Po získání surových dat následuje jejich předzpracování, což může zahrnovat filtraci šumu, normalizaci a další techniky pro zlepšení kvality obrazu nebo vzorku.

- Extrakce identifikačních rysů: Klíčovým krokem je extrakce charakteristických rysů z biometrických dat. Tento proces transformuje surová data do formy, která umožňuje efektivní porovnání.

- Vytváření šablon: Extrahované identifikační rysy jsou poté převedeny do digitální šablony, která reprezentuje biometrické charakteristiky jedince. Tyto šablony jsou uloženy v databázi pro budoucí porovnání.

[13] BIOMETRICS INSTITUTE. Types of Biometrics [online]. [cit. 2024-02-17]. Dostupné z: https://www.biometricsinstitute.org/what-is-biometrics/types-of-biometrics/

- Porovnání a shoda: Když systém obdrží nový biometrický vzorek, porovná jej se šablonami v databázi. Tento proces může být buď 1:1 (verifikace) nebo 1:N (identifikace).

- Rozhodovací proces: Systém určuje, zda došlo k shodě na základě předem nastavených prahových hodnot. Pokud je shoda nad tímto prahem, identifikace/verifikace je považována za úspěšnou.

- Bezpečnost a ochrana dat: Zabezpečení biometrických dat je kritické, protože se jedná o citlivé informace. Systémy musí zahrnovat silná bezpečnostní opatření, aby chránily data před neoprávněným přístupem nebo útoky.

- Výkon a metriky: Výkon biometrického systému je hodnocen pomocí různých metrik, jako jsou míra falešného přijetí (FAR), míra falešného odmítnutí (FRR) a celková přesnost.

- Integrace: Biometrické systémy musí být často integrovány s dalšími systémy, jako jsou kontrolní systémy přístupu nebo databáze, a musí být schopné spolupracovat s různými technologickými platformami.

- Uživatelské rozhraní a zkušenosti: Design uživatelského rozhraní a celková uživatelská zkušenost jsou důležité pro zajištění, že systém je přátelský a snadno použitelný pro koncové uživatele.

Tyto technické aspekty hrají zásadní roli ve vývoji, implementaci a účinnosti biometrických systémů v různých aplikacích a prostředích.[14]

[14] WAYMAN, James. Biometric systems: technology, design, and performance evaluation. London: Springer, c2005. ISBN 1852335963.

1.8. Hardware a software biometrických systémů

Biometrické systémy se skládají z dvou hlavních komponentů: hardware a software. Hardware zahrnuje fyzická zařízení a senzory, které získávají biometrická data, jako jsou skenery otisků prstů, kamery pro rozpoznávání obličeje, snímače oční duhovky nebo mikrofony pro analýzu hlasu. Tyto zařízení musí být přesná a spolehlivá, aby zajistila efektivní sběr dat.

Software biometrických systémů je zodpovědný za zpracování a analýzu získaných dat. To zahrnuje algoritmy pro detekci a extrakci biometrických rysů, tvorbu biometrických šablon a jejich porovnání pro identifikaci nebo verifikaci identity. Software také zahrnuje rozhraní pro integraci s dalšími systémy, jako jsou systémy kontroly přístupu nebo databáze identifikačních údajů.

Významnými úlohami softwarových komponentů jsou také zajištění bezpečnosti a ochrany soukromí. Biometrická data jsou citlivá a software musí zahrnovat silné šifrovací a bezpečnostní protokoly, aby zabránil úniku nebo zneužití těchto dat.

Společně hardware a software biometrických systémů umožňují automatizované rozpoznávání jednotlivců na základě jedinečných fyzických nebo behaviorálních charakteristik, což nachází uplatnění v řadě aplikací od zabezpečení až po personalizované služby.[15]

Hardware biometrický systémů

Hardware biometrických systémů se specializuje na fyzické komponenty potřebné pro sběr a detekci biometrických dat. Tento hardware zahrnuje širokou škálu zařízení a senzorů, které jsou navrženy tak, aby zachytily specifické biometrické informace. Mezi hlavní typy hardwaru biometrických systémů patří:

- Skenery otisků prstů: Tyto zařízení zaznamenávají obraz otisků prstů pomocí různých technologií jako jsou kapacitní, optické nebo ultrazvukové senzory.

[15] WAYMAN, James. Biometric systems: technology, design, and performance evaluation. London: Springer, c2005. ISBN 1852335963.

- Snímače oční duhovky a sítnice: Tyto zařízení používají kameru k zaznamenání unikátních vzorů na duhovce nebo sítnici oka. Duhovka je osvětlena pro lepší viditelnost vzoru.

- Systémy rozpoznávání obličeje: Využívají kamery, často s podporou infračerveného záření, k zachycení obrazu obličeje a identifikaci unikátních rysů.

- Zařízení pro rozpoznání hlasu: Tyto systémy využívají mikrofony k zachycení a analýze hlasových vzorů.

- Snímače otisků prstů nebo dlaní: Podobně jako skenery otisků prstů, ale na větší ploše, pro detailnější rozpoznání.

- Behaviorální biometrické senzory: Například zařízení sledující dynamiku psaní na klávesnici nebo pohyb myši, která mohou identifikovat uživatele podle jejich interakce s zařízením.

- Mobilní zařízení: Mnoho moderních mobilních telefonů a tabletů má integrované biometrické senzory, jako jsou čtečky otisků prstů nebo technologie rozpoznávání obličeje.

- Specializovaný hardware pro další typy biometrie: Například zařízení pro rozpoznávání chůze nebo unikátních srdečních rytmů.

Tento hardware musí být vysoce přesný a spolehlivý, aby zajistil efektivní a bezpečný sběr biometrických dat. Kromě toho je důležitá integrace s ostatními

systémy a zajištění, aby data byla zpracována a uložena bezpečně a v souladu s příslušnými právními normami.[16]

Software biometrických systémů

Software biometrických systémů je navržen tak, aby pracoval s biometrickými údaji a technologiemi, které identifikují a ověřují jednotlivce na základě jejich biometrických charakteristik. Biometrické charakteristiky zahrnují například otisky prstů, rozpoznávání obličeje, hlasovou identifikaci, skenování duhovky, geometrii rukou, dynamiku klávesnice a další. Tyto systémy mají širokou škálu aplikací, včetně zabezpečení, správy přístupu, identifikace osob, občanských průkazů, platebních systémů a mnoha dalších.

Zde je několik klíčových aspektů a funkcí software biometrických systémů:

- Sběr dat: Software biometrických systémů musí být schopen sbírat biometrická data od uživatelů. To může zahrnovat snímání otisků prstů, fotografie obličeje, nahrávání hlasu a další.

- Extrakce a zpracování dat: Po sběru dat software extrahuje relevantní biometrické charakteristiky a provádí jejich zpracování, aby byly připraveny k další analýze.

- Porovnávání a ověřování: Software biometrických systémů porovnává biometrické vzory uživatele s uloženými vzory v databázi a určuje, zda se jedná o platného uživatele.

- Správa uživatelů: Software umožňuje správu uživatelů, vytváření a aktualizaci biometrických profilů, revokaci přístupu a další administrativní úkoly.

[16] Biometric Devices 101: Definition and Examples. Online. Dostupné z: https://www.aratek.co/news/biometric-devices-definition-and-examples. [cit. 2024-01-25].

- Zabezpečení dat: Vzhledem k citlivosti biometrických dat musí software biometrických systémů zajistit jejich bezpečnost. To zahrnuje šifrování, bezpečný přenos dat a kontrolu přístupu.

- Integrace: Software biometrických systémů často musí být integrován do existujících systémů, jako jsou řídicí systémy přístupu, platební brány nebo software pro správu identit.

- Výkonnost a spolehlivost: Důležitým faktorem je rychlost a spolehlivost systému, zejména pokud jde o rychlou identifikaci nebo ověření osob.

- Monitorování a audit: Software biometrických systémů by měl umožňovat monitorování aktivit a auditování přístupu k biometrickým datům pro sledování neoprávněného použití.

- Aktualizace a údržba: Jelikož technologie biometrických systémů a hrozby se mohou měnit, je důležité, aby software umožňoval aktualizace a údržbu.

Software biometrických systémů je součástí vývoje biometrických technologií a má široké využití ve všech oblastech, kde je potřeba jednoznačně identifikovat nebo ověřit jednotlivce.[17]

1.9. Bezpečnost biometrických systémů

Bezpečnost biometrických systémů je kritickým faktorem, protože tyto systémy se spoléhají na jedinečné biometrické charakteristiky jednotlivců pro identifikaci a ověřování. Pokud by byl biometrický systém zranitelný vůči útokům nebo podvodům, mohlo by to ohrozit celý systém a způsobit potenciální škody.

[17] What is Biometrics? How is it used in security? [online]. [cit. 2024-01-25]. Dostupné z: https://www.kaspersky.com/resource-center/definitions/biometrics

Zde jsou klíčové aspekty a metody, které přispívají k bezpečnosti biometrických systémů:

- Šifrování dat: Biometrická data musí být uložena a přenášena v šifrované formě. To zajišťuje, že data nejsou snadno čitelná ani při případném úniku.

- Správa klíčů: Pro šifrování a dešifrování biometrických dat je nezbytná správa klíčů. Klíče by měly být uloženy v bezpečném prostředí a chráněny před neoprávněným přístupem.

- Fyzická ochrana: Fyzická zařízení, která používají biometrické technologie, by měla být fyzicky chráněna před neoprávněným přístupem. To může zahrnovat použití bezpečnostních kamer, kontrolu přístupu a další opatření.

- Detekce podvodů: Biometrické systémy by měly být vybaveny mechanismy pro detekci podvodů, jako jsou falešné otisky prstů, masky obličeje nebo hlasové nahrávky. Toto se obvykle nazývá „antispoofing“ a je kritické pro ochranu systému.

- Správa identit: Uchovávání a správa biometrických dat by měla být provedena s ohledem na zásady správy identit. To zahrnuje zabezpečení dat v databázích a zajištění správného přidělování práv přístupu.

- Dvojí ověření: Pro vyšší bezpečnost může být použito dvojí ověření, kde se kombinují biometrické charakteristiky s dalšími faktory, jako je heslo nebo karta.

- Aktualizace a opravy: Biometrické systémy by měly pravidelně aktualizovat svůj software a algoritmy, aby byly chráněny před novými hrozbami a zranitelnostmi. Opravy chyb by měly být prováděny okamžitě.

- Auditování a sledování: Zaznamenávání aktivit a auditování přístupu k biometrickým datům je důležité pro identifikaci potenciálních hrozeb a neoprávněných pokusů o přístup.

- Ochrana proti útokům na komunikaci: Při přenosu biometrických dat mezi zařízením a serverem je nutné zajistit, aby byla komunikace zabezpečena proti útokům, jako je odposlech nebo útoky typu „man-in-the-middle“.

- Školení uživatelů: Uživatelé biometrických systémů by měli být informováni o bezpečnostních postupech a vědomi si potenciálních rizik.

Bezpečnost biometrických systémů vyžaduje komplexní přístup a trvalou pozornost, protože hrozby a techniky útoků se neustále vyvíjejí. Je důležité, aby organizace, které používají biometrické systémy, měly pečlivý bezpečnostní plán a pravidelně prováděly audit bezpečnosti.[18]

Hodnocení spolehlivosti a výkonnosti biometrických systémů

Biometrický systém má jako primární cíl zajistit, že oprávněná osoba má přístup k určitým právům, jako je například vstup do objektu, zatímco osoba, která tato práva nemá, je odmítnuta. V praxi se používají dva klíčové pojmy, jež se týkají potenciálních situací, kdy tento proces může selhat.

Prvním z těchto pojmů je tzv. „False Rejection Rate“ (FRR), což je pravděpodobnost chybného odmítnutí. Tento ukazatel popisuje podíl osob, které byly biometrickým systémem odmítnuty, i když by jim to nemělo být. Z hlediska bezpečnosti v civilních aplikacích to nemusí být zásadní problém, ale v policejně-soudních aplikacích je to závažná záležitost, například při potvrzování identity pachatele.

[18] RISKS & BENEFITS OF BIOMETRICS IN SECURITY [online]. [cit. 2024-01-25]. Dostupné z: https://www.softwaresecured.com/post/risks-and-benefits-of-biometrics-in-security

Příklad: bylo provedeno porovnání 1 000 otisků prstů. Byly porovnány páry, které patří stejnému uživateli a stejný prst. Přesto 285x došlo k odmítnutí a vykazovaly neshodu. Výpočet FRR = (285/1000) x 100 = 28,5 %

Tím druhým způsobem je pojem tzv. False Acceptance Rate (FAR) neboli pravděpodobnost chybného přijetí. Popisuje podíl osob, které byly systémem přijaty, ale přijaty být neměly.

Příklad: bylo provedeno porovnání 1 000 vzorků duhovek. Byly porovnány páry, které nepocházejí od stejné osoby. Přesto bylo přijato 12 výsledků. Výpočet FAR = (12/1000) x 100 % = 1,2 %

Biometrické systémy zatím nejsou schopny zaznamenat každého jednotlivce, například osoby s omezenou schopností otevřít oči nebo jednotlivce s chybějícími prsty. Bylo empiricky odhadnuto, že až 4 % populace má otisky prstů nízké kvality, které jsou obtížné zaznamenat s použitím současných snímačů otisků prstů. Tato míra chybovosti je známá jako „Failure to Enroll“ (FTE) nebo také míra neschopnosti zaznamenat.

V případě, že je uživatel již registrován, může se stát, že získaná biometrická data nejsou dostatečně kvalitní pro další zpracování. Je proto třeba znovu získat biometrická data. Tato míra chybovosti je určována pomocí ukazatele nazývaného „Failure to Acquire“ (FTA), což je míra neschopnosti získat potřebná biometrická data.

V případě, že kvalita vstupních dat je dostatečná, dochází k provedení biometrického srovnání s uloženou šablonou. Pokud během tohoto srovnání nastane nesprávné ztotožnění, tato situace je označována jako „False Match Rate“ (FMR), což představuje míru chybné shody. Tato hodnota vyjadřuje procento osob, které byly chybně akceptovány. Naopak, pokud k nesprávnému ztotožnění nedojde, mluvíme o „False Non-Match Rate“ (FNMR), což je procentuální podíl situací, kdy nedojde k úspěšnému ztotožnění.

Pro ilustraci uvažujme příklad, kdy letištní bezpečnostní orgány hledají mezi 100 FBI nejhledanějšími zločinci (databáze obsahuje 100 vzorků).

Nejmodernější systém ověřování otisků prstů pracuje s FNMR na úrovni 1 % a FMR na úrovni 0,001 %. To znamená, že tento systém má šanci nesprávně identifikovat osobu jako nežádoucího subjektu v 1 % případů a nesprávně identifikovat osobu jako žádoucího subjektu v 0,001 % případů. Tento systém má tedy velkou pravděpodobnost identifikace hledaného zločince na 99 %. Nicméně produkuje vysoký počet falešných poplachů, například pokud 200 000 lidí projde biometrickým systémem během jednoho dne, systém vytvoří 200 falešných poplachů.

Dále můžeme narazit na termín „Failure to Match“ (FTM), což představuje míru neschopnosti provést srovnání. Tento ukazatel udává procentuální podíl biometrických charakteristik, které nelze porovnat s uloženou šablonou nebo jiným způsobem zpracovat po procesu registrace.

1.10. Způsoby ukládání a zpracování biometrických dat

Ukládání a zpracování biometrických dat je klíčovým aspektem moderních technologií zabezpečení a identifikace. Biometrická data mohou zahrnovat otisky prstů, obličejové rozpoznání, skenování sítnice nebo duhovky, rozpoznání hlasu a další unikátní charakteristiky těla nebo chování jedince.

Lokální ukládání znamená, že biometrická data jsou uložena přímo na zařízení uživatele, například na smartphonech nebo počítačích. Tato metoda nabízí větší kontrolu uživatele nad svými daty a snižuje riziko úniku dat z centrálního úložiště. Na druhé straně, centralizované databáze jsou často spravovány vládami nebo velkými organizacemi, což umožňuje efektivní přístup a sdílení dat mezi různými entitami, ale zvyšuje riziko úniku nebo zneužití dat. Hybridní modely kombinují lokální a centrální ukládání, kde jsou základní biometrické informace uloženy centrálně, ale klíčová ověřovací data jsou uchovávána lokálně.

Zpracování biometrických dat zahrnuje několik kroků. Kolekce a digitalizace zahrnuje sběr fyzických biometrických vzorků, například otisku prstu, a jejich převod do digitální formy. V procesu extrakce vlastností softwarové algoritmy identifikují a extrahují unikátní biometrické rysy z digitálního vzorku. Systémy pak porovnávají extrahované vlastnosti s uloženými vzory pro ověření

identity. Dále, biometrická data jsou často šifrována pro ochranu soukromí a zajištění bezpečnosti dat, využívají se metody jako hashování nebo bezpečné protokoly pro přenos dat.

Etické a právní aspekty zahrnují otázky týkající se souhlasu uživatelů a transparentnosti ve sběru a užití biometrických dat, riziko hackování a zneužití biometrických dat, zejména v případě úniků z centrálních databází, a právní rámce, jako je GDPR v Evropě, které stanovují pravidla pro sběr, ukládání a zpracování osobních a biometrických dat.[19]

Biometrické technologie se neustále vyvíjejí, a s nimi i metody jejich zabezpečení a etické normy. Je důležité udržovat rovnováhu mezi inovacemi v oblasti bezpečnosti a ochranou osobních údajů a soukromí jednotlivců.

1.11. Použití biometrických systémů

Použití biometrických systémů je rozšířené v různých oblastech, od zabezpečení až po osobní identifikaci, a to díky jejich schopnosti poskytovat unikátní a spolehlivé ověření identity.

V oblasti bezpečnosti a trestního řízení

Biometrické systémy hrají klíčovou roli v oblasti bezpečnosti a trestního řízení, poskytují unikátní a spolehlivé metody identifikace a sledování jednotlivců. Tyto systémy jsou používány k identifikaci podezřelých a pachatelů trestných činů, kde rozpoznání otisků prstů (obrázek č. 6), DNA analýzy a rozpoznání obličeje mohou rychle porovnat biometrické údaje z místa činu s databázemi podezřelých nebo již známých zločinců.

V oblasti monitorování a dohledu nad odsouzenými se využívají biometrické technologie, jako je elektronický dohled s využitím GPS a biometrických senzorů, které umožňují sledování pohybu a aktivity odsouzených

[19] JAIN, A.K., A. ROSS a S. PRABHAKAR. An Introduction to Biometric Recognition. IEEE Transactions on Circuits and Systems for Video Technology [online]. 2004, 14(1), 4-20 [cit. 2024-01-25]. DOI: 10.1109/TCSVT.2003.818349. ISSN 1051-8215. Dostupné z: http://ieeexplore.ieee.org/document/1262027/

osob podmíněně propuštěných nebo těch, kteří jsou pod domácím vězením. Vládní budovy, vojenská zařízení a další citlivé lokality často používají biometrické systémy pro kontrolu přístupu zajišťující, že pouze autorizované osoby mají přístup do zabezpečených oblastí.

Forenzní analýza v trestním řízení také využívá biometrické technologie, jako jsou srovnání otisků prstů, DNA nebo rozpoznání obličeje z místa činu. V mezinárodní bezpečnosti a protiteroristických operacích hrají biometrické údaje důležitou roli, kde hraniční kontroly zahrnují biometrické pasy a rozpoznání obličeje pro identifikaci a sledování cestujících.

Policie, hasiči a zdravotnické služby mohou používat biometrické technologie pro rychlou a bezpečnou identifikaci zaměstnanců a zajištění přístupu k citlivým informacím a zařízením. Kromě toho, vytváření a správa rozsáhlých biometrických databází umožňuje rychlé sdílení informací mezi různými bezpečnostními agenturami na národní i mezinárodní úrovni. Použití biometrických systémů v oblasti bezpečnosti a trestního řízení přináší významné výhody v podobě přesnější identifikace a sledování, což vede ke zvýšení bezpečnosti a efektivity. Je však nutné dbát na ochranu soukromí a zákonná omezení při sběru a zpracování těchto citlivých dat.

Obrázek č. 6 – Využití otisků prstů u bezpečnostních složek

V oblasti bankovnictví a financích

Biometrické systémy hrají stále důležitější roli v oblasti bankovnictví a financí, a to z několika důležitých důvodů. Prvním z těchto důvodů je bezpečnost. Biometrické systémy poskytují vyšší úroveň bezpečnosti než tradiční metody ověřování, jako jsou hesla a PIN kódy, protože biometrické

údaje, jako je otisk prstu, duhovka oka nebo obličej, jsou obtížně zfalšovatelné a nelze je zapomenout nebo ztratit (obrázek č. 7).

Druhým důležitým faktorem je pohodlí a rychlost. Biometrické systémy umožňují rychlé a pohodlné ověření totožnosti uživatele, což eliminuje potřebu pamatovat si složité heslo nebo ho opakovaně zadávat.

Třetím důležitým důvodem je prevence podvodu. Biometrie může snižovat riziko podvodu a identity theft, protože je obtížněji napodobitelná než tradiční ověřovací metody.

Některé z biometrických systémů používaných v bankovnictví a financích zahrnují rozpoznání obličeje, otisk prstu, rozpoznání duhovky oka, rozpoznání hlasu, dynamické otisky prstů a systémy kombinující více biometrických metod, známé jako biomatrici.

Použití biometrických systémů v bankovnictví a financích může zlepšit bezpečnost a pohodlí pro uživatele, ale je důležité zajistit ochranu biometrických dat a dodržování přísných zásad ochrany soukromí.[20]

Obrázek č. 7 – Využití otisků prstů u bankovního terminálu (ATM)

Ve veřejné správě a občanském životě

Samotný vývoj biometrických systémů v oblasti veřejné správy a občanského života má velký potenciál zlepšit různé aspekty každodenního

[20] GUENNOUNI, Souhail, Anass MANSOURI a Ali AHAITOUF. Biometric Systems and Their Applications. Visual Impairment and Blindness - What We Know and What We Have to Know [online]. IntechOpen, 2020, 2020-9-9 [cit. 2024-02-17]. ISBN 978-1-83880-257-8. Dostupné z: doi:10.5772/intechopen.84845

života. Následující rozšířený text poskytuje více informací o tom, jak biometrické technologie ovlivňují tyto oblasti:

- Identifikace občanů: Biometrické systémy umožňují jednoznačnou identifikaci občanů a vydání oficiálních identifikačních dokladů, jako jsou občanské průkazy nebo pasy, s větší přesností a bezpečností. Otisky prstů, rozpoznání obličeje a duhovky oka se staly běžnými metodami pro ověření totožnosti občanů. To má klíčový význam pro prevenci podvodů spojených s falešnou identitou a pro zabezpečení práv a výhod spojených s občanstvím.

- Kontrola hranic: Biometrické technologie jsou důležitou součástí bezpečnosti na hraničních přechodech a v mezinárodním letectví. Cestující jsou identifikováni pomocí otisků prstů nebo rozpoznání obličeje, což zvyšuje bezpečnost a urychluje procesy při vstupu do země. To pomáhá zabránit nelegálnímu přistěhovalectví a zlepšuje bezpečnostní opatření v souvislosti s terorismem a organizovaným zločinem.

- Volební systémy: Biometrické systémy mohou být využity k zajištění bezpečných a spravedlivých voleb. Identifikace voličů pomocí biometrických údajů, jako jsou otisky prstů, snižuje riziko podvodu a falešných hlasů. To je zvláště důležité v zemích, kde jsou volby vystaveny výzvám týkajícím se integrity a bezpečnosti.

- Přístup k veřejným službám: Biometrické systémy mohou zefektivnit procesy přístupu k veřejným službám, jako je zdravotní péče, sociální dávky nebo vydávání důležitých dokumentů. Identifikace občana pomocí biometrických údajů umožňuje rychlý a spolehlivý přístup k těmto službám, což zlepšuje efektivitu a omezuje riziko podvodů.

- Bezpečnostní opatření v občanském životě: Biometrické systémy se staly součástí každodenního života, protože jsou používány pro zabezpečení

osobních zařízení, jako jsou chytré telefony, tablety a počítače. Rozpoznání obličeje, otisků prstů nebo rozpoznání hlasu zajišťuje, že pouze oprávnění uživatelé mají přístup k svým zařízením a osobním datům.

- Ochrana soukromí a regulace: S rozšířením biometrických systémů roste také důležitost ochrany soukromí a transparentního používání těchto technologií. Zákony a regulace týkající se biometrických dat musí být jasně definovány a dodržovány, aby se zabránilo zneužití a zneužívání těchto citlivých informací.

Celkově lze říci, že biometrické systémy hrají klíčovou roli ve veřejné správě a občanském životě přinášející zvýšenou bezpečnost, efektivitu a pohodlí. Nicméně je nezbytné, aby byly tyto technologie správně regulovány a používány s ohledem na ochranu soukromí jednotlivců.[21]

Ve vojenském a obranném sektoru

Biometrické technologie mají význačné využití ve vojenském a obranném sektoru. Následující text podrobněji rozebírá způsoby, jakými jsou biometrické systémy uplatňovány v těchto oblastech:

- Přístupová kontrola: Vojenské zařízení a bezpečnostně citlivé lokality využívají biometrické systémy k ověření totožnosti a k regulaci přístupu osob. Otisky prstů, rozpoznání obličeje a duhovky oka slouží k zabezpečení těchto oblastí před neautorizovaným vstupem.

- Identifikace vojenského personálu: Biometrické systémy umožňují jednoznačnou identifikaci a ověření totožnosti vojenských členů, což je

[21] GUENNOUNI, Souhail, Anass MANSOURI a Ali AHAITOUF. Biometric Systems and Their Applications. Visual Impairment and Blindness - What We Know and What We Have to Know [online]. IntechOpen, 2020, 2020-9-9 [cit. 2024-02-17]. ISBN 978-1-83880-257-8. Dostupné z: doi:10.5772/intechopen.84845

zásadní pro zajištění bezpečnosti a řádného fungování vojenských operací.

- Bezpečnostní průchody a kontrolní body: Biometrické technologie jsou nasazovány na kontrolních bodech na vojenských základnách a jiných strategických místech pro kontrolu osob a vozidel, což výrazně zvyšuje bezpečnost těchto lokalit.

- Zabezpečení zbraní a zařízení: Některé vojenské zbraně a vybavení jsou vybaveny biometrickými systémy pro zamezení neoprávněného použití. Například pouze ověření vojenského personálu umožní aktivaci určitých zařízení.

- Ochrana vojenských informací: Biometrické systémy jsou používány pro ochranu vojenských dat, tajných informací a komunikačních sítí, což zajišťuje vysokou úroveň bezpečnosti a brání neautorizovanému přístupu.

- Vojenské mise a humanitární operace: Biometrické technologie umožňují identifikaci civilistů a humanitárního personálu v rámci vojenských misí a humanitárních operací, což zlepšuje kontrolu a bezpečnost těchto operací.

- Výzkum a vývoj: Vojenský výzkum a vývoj se zabývají zkoumáním nových biometrických technologií a metod s cílem zlepšit bezpečnost a efektivitu vojenských operací.

Využití biometrických systémů ve vojenském a obranném sektoru zvyšuje úroveň bezpečnosti a efektivity. Nicméně je nezbytné zajistit, aby byly tyto

technologie řádně chráněny a používány v souladu s etickými a právními normami, s důrazem na ochranu soukromí a osobních údajů.[22]

1.12. Etické a právní aspekty biometrických systémů

Etické a právní aspekty biometrických systémů jsou nesmírně důležité, protože tyto technologie mají velký dopad na soukromí, bezpečnost a práva jednotlivců. Následující text se zaměřuje na klíčové etické a právní otázky týkající se biometrických systémů:

Etické aspekty

1. Ochrana soukromí: Biometrické systémy získávají a uchovávají citlivé biometrické údaje, jako jsou otisky prstů nebo rozpoznání obličeje. Je důležité zajistit, aby byla tato data řádně chráněna a nepoužívána k neoprávněným účelům, což zahrnuje prodej či zneužití těchto údajů třetími stranami.

2. Transparentnost: Operátoři biometrických systémů by měli být transparentní v tom, jaké údaje sbírají, jak jsou tyto údaje uchovávány a jak jsou využívány. Uživatelé by měli mít možnost vědět, jakým způsobem jsou jejich biometrické údaje zpracovávány.

3. Důvěra a spolehlivost: Biometrické systémy by měly být spolehlivé a přesné. Chyby v identifikaci mohou mít závažné následky, a proto je důležité, aby byly tyto systémy co nejpřesnější.

[22] GUENNOUNI, Souhail, Anass MANSOURI a Ali AHAITOUF. Biometric Systems and Their Applications. Visual Impairment and Blindness - What We Know and What We Have to Know [online]. IntechOpen, 2020, 2020-9-9 [cit. 2024-02-17]. ISBN 978-1-83880-257-8. Dostupné z: doi:10.5772/intechopen.84845

4. Diskriminace a předsudky: Biometrické systémy mohou být náchylné k diskriminaci a předsudkům, zejména pokud nejsou správně nastaveny nebo pokud jsou trénovány na omezeném množství dat. Je třeba zajistit, aby tyto systémy nebyly diskriminační a nevyčleňovaly určité skupiny lidí na základě rasového, etnického nebo jiného kritéria.

5. Zneužití údajů: Existuje riziko, že biometrické údaje mohou být zneužity pro účely sledování, špehování nebo identifikaci jednotlivců bez jejich souhlasu. To je zásadní etická otázka, kterou je třeba řešit.[23]

Právní aspekty

1. Ochrana osobních údajů: Mnoho zemí má zákony a regulace ochrany osobních údajů, které se týkají i biometrických údajů. Tyto zákony stanovují pravidla pro sběr, zpracování a uchovávání biometrických dat.

2. Regulace biometrických systémů: Některé země mají specifické zákony a regulace, které se týkají biometrických systémů, a stanovují požadavky pro jejich používání ve veřejných i soukromých organizacích.

3. Smlouvy a dohody: Při využívání biometrických systémů ve veřejném a komerčním sektoru jsou uzavírány smlouvy a dohody, které stanovují podmínky pro používání těchto systémů, včetně záruk týkajících se soukromí a bezpečnosti údajů.

4. Práva jednotlivců: Jednotlivci mají právo na přístup k svým biometrickým údajům, opravu nepřesných údajů a právo na vymazání svých údajů v určitých případech.

[23] LINKEDIN. The Ethics of Using Facial Recognition and Fingerprint Technology [online]. , ArkEvo Group. [cit. 2024-02-17]. Dostupné z: https://www.linkedin.com/pulse/ethics-using-facial-recognition-fingerprint-technology-arkevo-group

5. Zákaz používání v určitých oblastech: V některých zemích jsou biometrické systémy zakázány v určitých oblastech nebo pro určité účely, například pro sledování občanů bez jejich vědomí a souhlasu.

Celkově je důležité, aby etické a právní aspekty biometrických systémů byly pečlivě zvažovány a dodržovány, aby bylo zajištěno, že tyto technologie budou používány způsobem, který respektuje práva a soukromí jednotlivců. Regulace a dohled jsou klíčovými nástroji pro dosažení tohoto cíle.[24]

1.13. Možnosti dalšího vývoje a rozvoje biometrických systémů

Biometrické systémy jsou stále aktivních oblastí výzkumu a vývoje a existuje mnoho směrů, které by mohly tuto technologii posunout dále. V následující textu jsem se zaměřil na některé možnosti dalšího vývoje a rozvoje biometrických systémů:

- Multimodální biometrie: Kombinování více biometrických modalit může zvýšit spolehlivost a bezpečnost systému. Například spojení otisků prstů, obličeje a hlasu může vytvořit silnější autentizační mechanismus.
- Pokročilé senzory: Rozvoj pokročilých senzorů může zvýšit přesnost biometrických systémů. Například senzory pro skenování duhovky nebo žil na ruce mohou poskytovat lepší výsledky než tradiční metody.

- Vylepšená anti-false opatření: Zlepšení technologií pro detekci falešných biometrických dat může zvýšit bezpečnost biometrických systémů a snížit riziko podvodů.

- Výzkum v oblasti biometrického spojení: Biometrický spojení je koncept, který umožňuje sdílení biometrických dat mezi různými organizacemi

[24] LINKEDIN. The Ethics of Using Facial Recognition and Fingerprint Technology [online]. , ArkEvo Group. [cit. 2024-02-17]. Dostupné z: https://www.linkedin.com/pulse/ethics-using-facial-recognition-fingerprint-technology-arkevo-group

nebo zařízeními. Tento směr může mít potenciál zlepšit bezpečnost a pohodlí při používání biometrických systémů v různých situacích.

- Standardizace: Standardizace biometrických systémů může usnadnit interoperabilitu mezi různými zařízeními a aplikacemi a zvýšit jejich širokou akceptaci.

- Ochrana soukromí: Růst biometrických systémů si vyžaduje zvýšenou pozornost k ochraně soukromí uživatelů. Vývoj nových technologií pro ochranu biometrických dat a dodržování přísných zásad ochrany soukromí je klíčovým směrem.

- Využití umělé inteligence a strojového učení: Strojové učení a umělá inteligence mohou pomoci zlepšit rozpoznávání a autentizaci v biometrických systémech. Pokroky v těchto oblastech mohou zvýšit rychlost a přesnost biometrických systémů.

- Biometrické systémy v mobilních zařízeních: Využití biometrických technologií, jako jsou otisky prstů nebo rozpoznávání obličeje, v mobilních zařízeních a platebních aplikacích může zvýšit jejich bezpečnost a pohodlí.

- Vývoj ve zdravotní péči: Biometrické systémy mohou být využity pro zabezpečení a správu přístupu k zdravotním záznamům a zařízením, což může zlepšit péči o pacienty a ochranu jejich dat.

- Vývoj veřejných a bezpečnostních systémů: Biometrické technologie mohou být použity pro zlepšení bezpečnosti veřejných prostor a v rámci větších bezpečnostních projektů, jako jsou pasy, víza a kontroly na hranicích.

Závěrem, biometrické systémy mají stále velký potenciál pro rozvoj a vývoj v mnoha různých oblastech. Tyto směry mohou zlepšit bezpečnost, pohodlí a efektivitu biometrických systémů a jejich širokou akceptaci ve společnosti. Je však důležité, aby byla zachována rovnováha mezi bezpečností a ochranou soukromí uživatelů.

2. Druhá část

Tato část diplomové práce seznamuje se dvěma hlavními druhy biometrických identifikací a systémů, které již Policie ČR bezpečně používá a jsou nedílnou součástí jejich každodenní služby.

2.1. Daktyloskopie – Otisky prstů

Název daktyloskopie vychází z řeckých slov daktylos – prst a skopein – viděti. Obecně se charakterizuje jako nauka o obrazcích papilárních linií na vnitřní straně článků prstů rukou, dlaní a na prstech nohou a chodidel.

Z hlediska kriminalistické techniky je daktyloskopie obor, který zkoumá obrazce papilárních linií na vnitřní straně posledních článků prstů rukou a na dalších článcích prstů rukou, na dlaních a prstech nohou a chodidel z hlediska zákonitostí jejich vzniku, vyhledávání, zajišťování a zkoumání s cílem identifikovat osobu, která otisky vytvořila.

V policejní praxi se daktyloskopie začala využívat zhruba od poloviny 90. let 19. století. Než bylo možné využít daktyloskopii pro účely identifikace osob, bylo třeba prokázat individuálnost, neměnnost a neodstranitelnost obrazců papilárních linií. Autorem tří fyziologických zákonů byl anglický přírodovědec Francois Galton (1822-1911).

Základní pojmy kriminalistické daktyloskopie

Vymezení zkoumání

1. Daktyloskopickým zkoumáním se pro potřeby objasňování trestní věci zjišťuje, na podkladě zvláštností tvarů otisků papilárních linií na prstech, dlaních a chodidlech, shoda dvou a více otisků. K tomu se využívají a rozvíjejí poznatky obecné dermatologie.

2. Daktyloskopie vychází z poznání, že
    a. nejsou na světě dva lidé, kteří by měli stejné obrazce papilárních linií,
    b. obrazce papilárních linií u lidí zůstávají po celý život relativně neměnné,
    c. papilární linie jsou neodstranitelné, není-li odstraněna zárodečná vrstva kůže.

3. Daktyloskopické zkoumání je vzájemné porovnávání objektů zajištěných v souvislosti s objasňovanou trestní věcí se srovnávacím materiálem, při kterém se zjišťuje vzájemná shodnost charakteristických znaků v jejich detailech a rozmístění.

4. Zkoumání se provádí ve stejném měřítku za využití optických přístrojů a pomůcek.

Objekty zkoumání

1. Objektem zkoumání jsou daktyloskopické otisky a daktyloskopické stopy.

2. Daktyloskopický otisk je otisk papilárního terénu prstů (obrázek č. 8), dlaní nebo chodidel konkrétní osoby.

3. Daktyloskopická stopa je každý otisk nebo vtisk prstu, dlaně nebo bosého chodidla, který vznikl dotykem s předmětem schopným jeho vzniklý obraz nebo tvar přijmout, po určitou dobu uchovat, a je zjistitelná, zajistitelná a využitelná.

4. Rozlišuje se taktická (důkazní) a technická hodnota daktyloskopické stopy. Taktická (důkazní) hodnota představuje míru pravděpodobnosti, že stopa pochází od určité osoby. Technickou hodnotou se označuje míra možnosti jejího zajištění a upotřebitelnosti pro zkoumání.

5. Daktyloskopické stopy se z hlediska možnosti zkoumání člení na upotřebitelné, částečně upotřebitelné a neupotřebitelné. Upotřebitelnost stopy se stanoví na základě počtu charakteristických znaků nutných k identifikaci. Charakteristickým znakem je jakékoliv utváření papilárních linií, které se odlišuje od ostatních (např. začátek, konec, vidlice, očko).

6. Upotřebitelné daktyloskopické stopy vykazují 10 a více charakteristických znaků papilárních linií. Stopy se využívají pro stanovení individuální identifikace.

7. Částečně upotřebitelné daktyloskopické stopy vykazují 7 až 9 charakteristických znaků. Stopy lze využít pro vyloučení shody nebo k určení skupinové příslušnosti.

8. Neupotřebitelné daktyloskopické stopy vykazují méně jak 7 charakteristických znaků.

9. Daktyloskopické stopy mohou být

    a. viditelné, které se dále člení na plastické a plošné,
    b. neviditelné (latentní).

10. Viditelné plastické stopy (vtisky) vznikají tlakem prstu, dlaně nebo chodidla na tvárný materiál, kterým může být měkká hlína, jíl, čerstvý lak, modelovací hmota, tmel, vosk, čokoláda, sýry, tuky apod.

11. Viditelné plošné stopy (otisky) mohou být barevné, krvavé, mastné, lepkavé, prašné a v prachu.

12. Neviditelné (latentní) stopy jsou pouhým okem téměř neviditelné nebo nejsou viditelné vůbec. Na hladkých a lesklých předmětech mohou být spatřeny s použitím lupy a šikmého osvětlení.

Obrázek č. 8 – Markanty

Druhy zkoumání

Daktyloskopické zkoumání provádí srovnání a zjišťuje shodu:

1. zajištěných daktyloskopických stop s otisky prstů (dlaní) osob registrovaných v daktyloskopických sbírkách,

2. zajištěných daktyloskopických stop z místa činu s kontrolními otisky prstů, dlaní a bosých chodidel osob vytypovaných, podezřelých, domácích apod.,

3. otisků prstů (dlaní) určité osoby s otisky uloženými v daktyloskopických sbírkách,

4. otisků prstů (dlaní) neznámých osob a mrtvol s otisky uloženými v daktyloskopických sbírkách,

5. zajištěných daktyloskopických stop se stopami uloženými ve sbírce stop z neobjasněných trestných činů,

6. otisků prstů (dlaní) zakládaných do daktyloskopické sbírky se stopami uloženými ve sbírce stop z neobjasněných trestných činů.

Daktyloskopování osob

Dle čl. 36 ZP PP č. 275/2016, kterým se upravuje provozování informačních systémů AFIS 2000, C-AFIS a některé podmínky provozování daktyloskopických sbírek.

Policejní orgán odpovídá za to, která osoba je daktyloskopována a proč. Daktyloskopování je prováděno:

- osobám podezřelým či obviněným z úmyslných trestných činů, včetně těch, které nejsou trestně odpovědné pro nedostatek věku nebo nepříčetnost, pokud policejní orgán nerozhodne s ohledem na charakter a provedení trestného činu jinak,

- osobám nalezeným, po nichž bylo vyhlášeno pátrání a které nemají právní způsobilost v plném rozsahu,

- osobám, které odmítly nebo nemohou prokázat svoji totožnost

- tzv. domácím osobám, u nich není daktyloskopování prováděno na daktyloskopickou kartu, ale např. na čistý list papíru, jejich otisk nejsou

vkládány do systému AFIS ani do daktyloskopických sbírek, slouží jen k porovnání a vyloučení stop a poté jsou vráceny zpět policejnímu orgánu,

- cizincům, pokud tak stanoví právní předpisy.

Právní úprava daktyloskopování osob

Oprávněnost takového zásahu do práv osob je upravena právními předpisy, a to zejména trestním řádem a zákonem o policii:

- § 114 odst. 3 trestního řádu, který říká, že je-li k důkazu třeba zjistit totožnost osoby, která se zdržovala na místě činu, je osoba, o kterou jde, povinna strpět úkony potřebné pro takové zjištění.

- § 63 odst. 4 zákona o Policii ČR, kdy pokud nelze totožnost předvedené osoby zjistit na základě sdělených údajů ani v dostupných evidencích, je policista oprávněn získat informace potřebné k jejímu ztotožnění snímáním daktyloskopických otisků a dalších úkonů.

- § 65 je pojednání o získávání osobních údajů pro účely budoucí identifikace, kdy policie může při plnění svých úkolů pro účely budoucí identifikace u a) osoby obviněné ze spáchání úmyslného trestného činu nebo osoby, které bylo sděleno podezření pro spáchání takového trestného činu, b) osoby ve výkonu trestu odnětí svobody za spáchání úmyslného trestného činu, c) osoby, jíž bylo uloženo ochranné léčení, nebo d) osoby nalezené, po níž bylo vyhlášeno pátrání a která nemá způsobilost k právním úkonům v plném rozsahu, snímat daktyloskopické otisky, zjišťovat tělesné znaky, provádět měření těla, pořizovat obrazové, zvukové a obdobné záznamy a odebírat biologické vzorky umožňující získání informací o genetickém vybavení.

Daktyloskopická identifikace

Po zajištění daktyloskopických otisků následuje vyhledávání vzájemně shodných skupin charakteristických znaků. V kriminalistické expertizní praxi se provádí porovnávání daktyloskopických markantů v daktyloskopické stopě se srovnávacím materiálem v komparátoru. Poté se vyvozují závěry o shodnosti nebo rozdílnosti zkoumaných objektů.

V dalším stádiu znalec na základě kvality a kvantity charakteristických znaků stanoví, zda se jedná o shodu nebo neshodu zkoumaných objektů. S využitím formální a dialektické logiky může vyslovit čtyři druhy kategorických soudů:

- kategoricky kladný soud (stopa z místa činu i srovnávací otisk byly vytvořeny jednou osobou)

- kategoricky záporný soud (stopa a srovnávací otisk byly vytvořeny dvěma osobami)

- částečně kladný a částečně záporný soud (ve stopě a srovnávacím vzorku byly zjištěny odlišnosti, které musí znalec vysvětlit, než se rozhodne o celkovém závěru zkoumání).

Daktyloskopické sbírky

Dle čl. 54 ZP PP č. 275/2016, který upravuje členění daktyloskopických sbírek a jejich využití, a to následovně:

1. K účelu identifikace osob a stop se vedou:
    a. Ústřední daktyloskopická sbírka v Kriminalistickém ústavu Praha,
    b. Krajské daktyloskopické sbírky u odborů kriminalistické techniky a expertiz.

2. Daktyloskopické sbírky uvedené v odstavci 1 zahrnují:

a. sbírku otisků prstů a dlaní osob,
b. sbírku stop z neobjasněných případů,
c. sbírku stop z objasněných případů.

3. Daktyloskopických sbírek se využívá zejména k
   a. zjišťování a prověřování totožnosti osob a mrtvol neznámé totožnosti,
   b. vyhledání shodných daktyloskopických otisků prstů (dlaní) se stopami zejména z místa činu,
   c. srovnání otisků prstů osob obviněných z určité trestné činnosti s daktyloskopickými stopami z neobjasněných trestných činů,

   d. sledování směru pohybu hledaného pachatele podle daktyloskopických stop, které zanechal na místech činů,
   e. srovnání daktyloskopických stop zajištěných na předmětech pohřešované osoby s otisky mrtvoly k možnému zjištění její totožnosti.

4. Ke srovnávání dat v daktyloskopických sbírkách se využívá automatizovaný daktyloskopický identifikační systém (Automated Fingerprint Identification System - AFIS).

AFIS BIS

V roce 1975 byl systém AFIS zaveden v USA. V roce 1994 byl nainstalován americkou společností Printrak MorphoTrak na Kriminalistickém ústavu Praha s označením AFIS 2000.

V roce 2010 došlo k velké aktualizaci tohoto systému. Kromě skutečnosti, že byl nově označen názvem AFIS BIS (Biometric Identification System), byly nainstalovány nové zmodernizované stanice. Taktéž systém získal nové funkce, mezi kterými je porovnávání jak otisků prstů, tak nově i dlaní. Obsluhu systému a nahrávání daktyloskopických karet osob do systému provádí pracovníci Kriminalistického ústavu Praha ve spolupráci s pracovníky OKTE.

2.2. Rozpoznání obličeje

Tento způsob identifikace je pro samotnou Policii České republiky novinka, koneckonců o tom vypovídá i dosud neucelený názor, co se týče právní úpravy. Dnes již takovýto biometrický systém funguje, a to zejména na mezinárodním letišti Václava Havla, který disponuje velkým počtem kamerových a záznamových zařízení, které jsou pro tento způsob automatizovaného porovnávání nezbytné.

V roce 2011 došlo k rozšíření technologie rozpoznávání obličejů díky sociální síti Facebook, která ji začlenila pro svých 900 milionů uživatelů. Díky obrovskému množství dat bylo možné algoritmy tohoto systému zefektivnit. Tato technologie se celosvětově využívá především pro bezpečnostní účely, jako je identifikace hledaných osob nebo nebezpečných individuí či skupin. S rostoucím počtem moderních kamer s vysokým rozlišením lze obličej rozpoznat i na velké vzdálenosti, a dokonce i v případě, že je obličej částečně skrytý nebo maskovaný. Metody rozpoznávání obličejů zahrnují různé techniky, přičemž nejznámější jsou 2D a 3D rozpoznávání. Základní 2D geometrie analyzuje vzdálenosti mezi nosním, ústy, očima a dalšími rysy obličeje. Tato metoda však nebyla považována za dostatečně přesnou, a proto byla rozšířena o 2D statistické metody pro detailnější analýzu. Tyto metody vytvářejí abstraktní model obličeje pro srovnání s referenčními daty. 2,5D metoda přidává k těmto technikám prostorový efekt, což pomáhá odhalit podvody jako například použití fotografie. Nejpokročilejší je 3D rozpoznávání, které s využitím laserových snímačů dokáže zachytit obličej nezávisle na osvětlení a poloze. Pro dosažení

maximální úrovně bezpečnosti je doporučeno kombinovat 3D rozpoznávání s jinými metodami, jako jsou snímání duhovky nebo tepelné mapování obličeje.[25]

Normy

Identifikace tváří podléhá normám ISO/IEC 19794-5:2011 Face Image Data a ANSI/INCITS 385-2004[R2014] Face Recognition Format For Data Interchange.

ISO/IEC 19794-5:2011 specifikuje formát záznamu pro ukládání, nahrávání a přenos informací z jednoho nebo více obrazů obličeje nebo krátkého videa. Určuje také omezení scény obrazu obličeje, jeho fotografické vlastnosti, vlastnosti digitálního obrazu a poskytuje nejlepší postupy pro fotografování tváří.

ANSI/INCITS 385-2004[R2014] určuje definice vlastností fotografií (pozadí, postoj, ohnisko aj.), vlastnosti digitálního obrazu a formát pro výměnu dat.[26]

Současné využití rozpoznávání obličejů Policií České republiky

Policie České republiky využívá systém rozpoznávání obličeje pro zlepšení své schopnosti identifikovat osoby na základě obrazového materiálu (obrázek č. 9). Tento systém může být použit v různých kontextech, včetně vyšetřování trestných činů, hledání pohřešovaných osob nebo identifikaci osob v rámci monitorování veřejných prostor.

- Vyšetřování trestných činů: Systém rozpoznávání obličeje umožňuje policistům rychle a efektivně porovnávat obrazový materiál získaný během vyšetřování, jako jsou záznamy z bezpečnostních kamer, s databázemi fotografií osob, které jsou již v policejních evidencích. To může pomoci rychle identifikovat podezřelé nebo svědky.

[25] MITRA, Sinjini; GOFMAN, Mikhail (ed.). Biometrics in a data driven world: trends, technologies, and challenges. CRC Press, 2016.

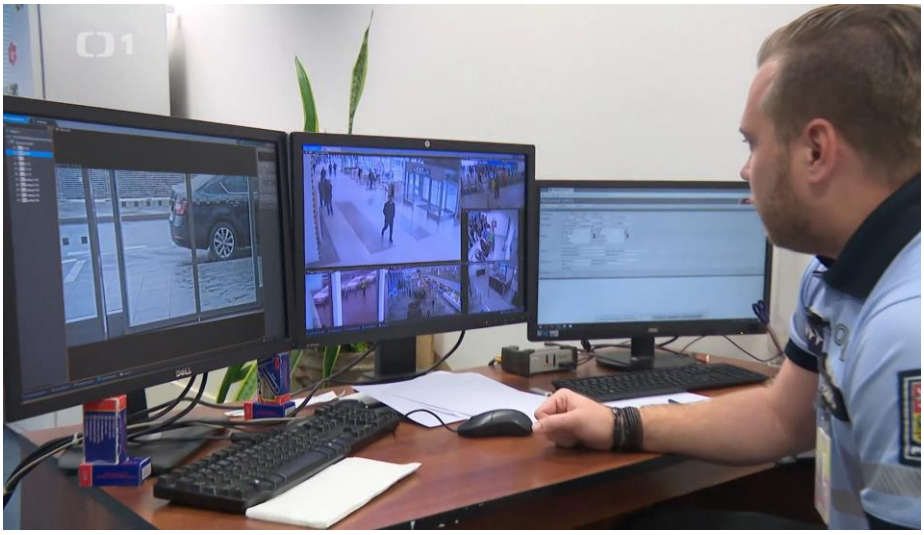
[26] INCITS 385-2004[R2014]: Information Technology - Face Recognition Format For Data Interchange. ANSI Webstore [online]. [cit. 2024-01-05]. Dostupné z: https://webstore.ansi.org/Standards/INCITS/INCITS3852004R2014

- Hledání pohřešovaných osob: Systém může být také využit k identifikaci pohřešovaných osob, pokud jsou k dispozici jejich fotografie. To může zahrnovat porovnávání fotografií pohřešovaných s obrazy získanými z míst, kde by mohli být, například z nádraží, letišť nebo jiných veřejných prostor.

- Monitorování veřejných prostor: V některých případech může policie využívat systémy rozpoznávání obličeje k monitorování veřejných prostor s cílem identifikovat osoby, které jsou hledány kvůli trestným činům nebo jsou považovány za bezpečnostní riziko. Toto využití je obvykle předmětem veřejné debaty a diskuse o ochraně soukromí.

Použití technologie rozpoznávání obličeje policií musí být v souladu s právními předpisy a normami pro ochranu osobních údajů a soukromí. V České republice je toto použití regulováno zákony o ochraně osobních údajů a specifickými pravidly pro práci policie. Kritici použití technologie rozpoznávání obličeje poukazují na potenciální rizika pro soukromí a obavy z možného zneužití.

Je důležité, aby byla technologie rozpoznávání obličeje využívána transparentně a s náležitou péčí o ochranu práv a svobod jednotlivců, včetně zavedení mechanismů pro dohled a zpětnou vazbu.



Obrázek č. 9 – Využití rozpoznávání obličejů Policií České republiky

Systém rozpoznání obličejů na Letišti Václava Havla

V současné době z důvodu vývoje bezpečnostní situace byl na Letišti Václava Havla zřízen biometrický systém, který je schopný z kamerového systému získávat věrohodná data, která může porovnávat s dostupnými databázemi. Konkrétním výsledkem tedy může být identifikování nebezpečného pachatele, jenž spáchal trestný čin, a který pro tyto účely byl vložen do databáze hledaných osob a díky porovnání jeho obličeje z kamerového systému letiště byl zadržen.

Základním aspektem pro fungování takového systému je technologická úroveň systému. Pro kvalitní porovnání obličejů a věrohodné výsledky je zapotřebí, aby porovnávací materiál byl v co možná nejlepší kvalitě, tudíž je zde velký důraz na kvalitní záznamové zařízení – kamery.

Systém posléze po získání dat z kamerových zařízení musí vyhodnotit, získaná data pro účely porovnání s pátracíma databázemi Policie ČR.

Velikou výhodou takového systému je jeho integrace do již fungujícího kamerového systému. Jedná se v podstatě o software, který porovnává výstup z kamerových systémů s porovnávacím materiálem z databází. Jedním ze systémů, který Policie ČR využívá na Letišti Václava Havla, je systém NeoFace od společnosti NEC Corporation.

NeoFace

NeoFace od společnosti NEC je pokročilá technologie rozpoznávání obličeje (obrázek č. 10), která je považována za jednu z nejpřesnějších a nejrychlejších na trhu. Tato technologie využívá algoritmy umělé inteligence a strojového učení k analýze obličejových rysů z digitálních obrazů nebo video záznamů. Je schopná identifikovat a ověřit osoby i v náročných podmínkách, jako jsou nízká kvalita obrazu, různé úhly pohledu, změny výrazu obličeje nebo částečné zakrytí obličeje.

NeoFace od NEC se využívá v široké škále aplikací, od bezpečnostních systémů přes monitorování na veřejných místech až po personalizované marketingové kampaně a automatizované systémy pro kontrolu přístupu. Její schopnost rychle a přesně identifikovat osoby ji činí užitečnou pro vládní agentury, letiště, finanční instituce a mnoho dalších odvětví.

Jednou z klíčových výhod technologie NeoFace je její vysoká úroveň přesnosti, která byla potvrzena v několika nezávislých testech a srovnáních. NEC tvrdí, že jejich technologie rozpoznávání obličeje překonává konkurenci v rychlosti, přesnosti a schopnosti adaptace na různé scénáře použití.

Bezpečnost a ochrana soukromí jsou však v oblasti rozpoznávání obličeje vždy předmětem diskuse. NEC zdůrazňuje, že klade velký důraz na etické aspekty využívání své technologie a dodržuje přísné normy pro ochranu dat a soukromí uživatelů. Přesto použití technologie rozpoznávání obličeje vyvolává otázky týkající se soukromí, etiky a potenciálního zneužití.

NeoFace je tedy předním příkladem toho, jak pokročilá technologie může přinést značné výhody pro společnost, ale zároveň představuje výzvy, které je třeba řešit z hlediska etiky a ochrany soukromí.

Jeho technické fungování se dá popsat v několika klíčových krocích a konceptech:

1) Akvizice obrazu
    - Systém nejprve získá obrazový materiál, který může pocházet z různých zdrojů, jako jsou videokamery, fotografie nebo digitální soubory.

- Obraz je předzpracován, aby se zlepšila jeho kvalita a zvýšila šance na úspěšné rozpoznání. Tento proces může zahrnovat korekci osvětlení, zarovnání obličeje a odstranění šumu.

2) Detekce obličeje
    - Software identifikuje přítomnost obličeje v obrazovém materiálu. To zahrnuje lokalizaci obličejů a možná i dalších charakteristických bodů, jako jsou oči, nos a ústa.
    - Pro detekci obličeje se často používají algoritmy, které mohou rozpoznat obličejové rysy i v různých podmínkách, jako jsou různé úhly pohledu, výrazy nebo částečné zakrytí.

3) Extrakce rysů
    - Po detekci obličeje systém analyzuje obraz a extrahuje z něj jedinečné obličejové rysy, které tvoří „obličejovou signaturu“ osoby. Tento proces zahrnuje rozpoznání a kvantifikaci různých aspektů obličeje, jako jsou vzdálenosti mezi důležitými body (oči, nos, ústa atd.), tvary částí obličeje a textura kůže.
    - Využívají se pokročilé techniky strojového učení, aby se z obličejových rysů vytvořil kompaktní a výrazný digitální otisk.

4) Porovnávání a identifikace
    - Obličejová signatura získaná z aktuálně analyzovaného obrazu se porovnává s databází uložených obličejových signatur.
    - Systém využívá algoritmy pro porovnávání, aby určil, zda se aktuální obličejová signatura shoduje s nějakou v databázi. Tento proces zahrnuje hodnocení podobnosti a určení pravděpodobnosti shody.

5) Rozhodnutí

- Na základě výsledků porovnávání systém rozhodne, zda došlo k identifikaci nebo verifikaci osoby. Výsledky mohou být prezentovány s určitou mírou jistoty nebo pravděpodobnosti.

NeoFace využívá nejnovější pokroky v oblasti umělé inteligence, hlubokého učení a neuronových sítí k optimalizaci svého výkonu. Hluboké neuronové sítě, zejména konvoluční neuronové sítě (CNN), jsou základem pro extrakci a učení se více dimenzionálních obličejových rysů.

Obrázek č. 10 – Použití systému NeoFace

3. Třetí část

Tato je část diplomové práce je zaměřena na výzkum, kterým se pokusím zjistit, zdali je možné využít komerční biometrický systémy vyhledávající obličeje v internetovém prostředí pro účely policejního operativního šetření, jako například ztotožnění neznámých osob a podobně.

3.1. Vymezení výzkumného problému

V současné době se celosvětově rozmáhá využívání biometrických technologií, zvláště systémů rozpoznávání obličejů, které představují významný nástroj pro zlepšení veřejné bezpečnosti a efektivity policejní práce. Tyto

systémy, původně vyvinuté pro komerční využití, nacházejí stále širší uplatnění i ve veřejném sektoru, včetně použití policií pro identifikaci osob, vyšetřování trestných činů a monitorování veřejných prostor. Přestože potenciál těchto technologií pro boj proti kriminalitě je obrovský, jejich nasazení vyvolává značné etické, právní a sociální otázky, zejména co se týče ochrany soukromí, práva na osobní integritu a možnosti zneužití.

Výzkumný problém této diplomové práce spočívá v analýze a hodnocení, jak mohou být komerční biometrické systémy na rozpoznávání obličejů efektivně a eticky využívány policií pro zvýšení veřejné bezpečnosti, aniž by byla ohrožena práva a svobody jednotlivců. Tento problém zahrnuje zkoumání technologických kapacit a omezení současných systémů rozpoznávání obličejů. Výzkum se zaměří na identifikaci a praktickou využitelnost těchto komerčních nástrojů pro policejní účely.

Cílem je poskytnout komplexní přehled o současném stavu využití biometrických systémů na rozpoznávání obličejů v policejní praxi, identifikovat nejlepší praxe a vyvinout doporučení pro jejich zodpovědné využívání, s ohledem na ochranu základních lidských práv a svobod. Tento výzkumný problém je vysoce relevantní v kontextu rostoucí digitalizace společnosti a potřeby řešit bezpečnostní výzvy 21. století, přičemž zajišťuje, že technologický pokrok slouží společnosti způsobem, který je eticky a právně udržitelný.

3.2. Metoda výzkumu

Výzkum bude spočívat v uměle vytvořené situaci, kdy budu mít pro výzkum fotografie lidí různých vlastností, které by mohly výsledky porovnání ovlivnit a tím získat co nejrelevantnější výsledek zkoumání.

Pro účely výzkumu budu mít k dispozici fotografie existujících lidí se známou identitou a jednu fotografii neexistujícího člověka, která byla vygenerována umělou inteligencí pro účely zkoumání. Všechny fotografie osob budou takzvaná portrétní fotografie, tzn. obličejem dopředu, kdy se fotografovaná osoba dívá do objektivu.

Nástroje pro vyhledávání obličejů budou služby PimEyes, Google Images a Social Catfish.

3.3. Předměty výzkumu

Pro účely výzkumu mám k dispozici tři portrétní fotografie osob, z nichž jsou dvě osoby skutečné a je známa jejich totožnost a jedna fotografie z fotobanky neexistujících osob, jež byla vygenerována umělou inteligencí.

Osoba číslo 1

Osoba číslo 1 je existující osoba ve věku 27 let v době pořízení níže doložené fotografie (obrázek č. 11).

Obrázek č. 11 – Osoba číslo 1

Osoba číslo 2

Osoba číslo 2 je existující žena ve věku 24 let v době pořízení níže doložené fotografie (obrázek č. 12).

Obrázek č. 12 – Osoba číslo 2

Osoba číslo 3

Osoba číslo 3 je neexistující osoba, která byla vygenerována umělou inteligencí v nezjištěné době, která byla stažena ze stránky: https://www.lidovky.cz/orientace/veda/tenhle-clovek-neexistuje-pocitac-generuje-neexistujici-obliceje-uci-se-od-sebe-sameho.A190218_091910_ln-zajimavosti_form/foto/FOR7979b3_fajn1.jpg (obrázek č. 13).

Obrázek č. 13 – Osoba číslo 3

3.4. Vyhledávací nástroje pro účely výzkumu

PimEyes

PimEyes je pokročilý vyhledávač obličejů, který funguje jako nástroj pro reverzní vyhledávání obrázků a mechanismus pro vyhledávání fotografií. Umožňuje uživatelům najít, na jakých webových stránkách jsou jejich fotografie publikovány online. PimEyes byl vytvořen jako víceúčelový nástroj, který umožňuje sledovat vaši tvář na internetu, nárokovat si práva na obrázky a monitorovat vaši online přítomnost.[27]

PimEyes používá pro hledání podobných tváří na více než 10 milionech webových stránek pokročilé technologie jako strojové učení, reverzní

[27] PIMEYES. More than a reverse image search [online]. [cit. 2024-02-13]. Dostupné z: https://pimeyes.com/en

vyhledávání obrázků a umělou inteligenci. Tento nástroj nabízí jak verzi zdarma, tak i placené. Zatímco bezplatná verze umožňuje pouze zjistit, zda je určitá tvář na internetu, placená služba poskytuje přístup ke všem dalším službám, včetně hlubokého vyhledávání, generování PDF a odesílání.[28]

Jedná se o technologii, která integruje mechanismus rozpoznávání obličeje s vyhledávačem a byla navržena v roce 2017. Nyní se vyvíjí jako pokročilý nástroj pro sebe-monitorování, sebe-ochranu a správu obrazu sebe sama.[29]

Uživatelé mohou jednoduše nahrát obrázek tváře, aby zahájili své vyhledávání. Jakmile je obrázek nahrán na webové stránky PimEyes, nástroji trvá méně než sekundu, aby prohledal internet a našel odpovídající obrázky.

Google Images

Google Images je vyhledávač obrázků společnosti Google, který umožňuje uživatelům hledat na webu obrázky související s různými tématy. Tento nástroj byl spuštěn v červenci 2001 a od té doby se stal jedním z nejpopulárnějších nástrojů pro vyhledávání obrázků na internetu. Google Images umožňuje uživatelům snadno najít obrázky, fotografie, grafiku a další vizuální obsah tím, že do vyhledávacího pole zadají klíčová slova nebo fráze související s hledaným obsahem.

Jednou z významných funkcí Google Images je možnost provádět vyhledávání obrázků pomocí obrázku, což je známé jako reverzní vyhledávání obrázků. Uživatelé mohou nahrát obrázek nebo zadat URL adresu obrázku, aby našli podobné obrázky, zjistili více informací o obrázku nebo identifikovali původ obrázku. Tato funkce je užitečná pro zjištění zdroje obrázku, identifikaci objektů, míst, osob, nebo dokonce pro ověření pravosti obrázku.

Google neustále vylepšuje Google Images zavedením nových technologií a funkcí, jako jsou pokročilé algoritmy pro rozpoznávání obrázků, filtry pro

[28] SHOTKIT. HOW TO USE FACIAL RECOGNITION SEARCH [online]. [cit. 2024-02-13]. Dostupné z: https://shotkit.com/facial-recognition/

[29] PIMEYES. More than a reverse image search [online]. [cit. 2024-02-13]. Dostupné z: https://pimeyes.com/en

upřesnění vyhledávání (např. podle barvy, typu obrázku, velikosti, práv k použití) a integraci s dalšími produkty Google, jako je Google Lens. Google Lens umožňuje uživatelům používat kameru svého mobilního telefonu pro interaktivní hledání a získávání informací o objektech v reálném světě prostřednictvím rozpoznávání obrázků.

S rozvojem umělé inteligence a strojového učení Google Images stále více zlepšuje schopnost poskytovat relevantní a přesné výsledky vyhledávání, což uživatelům usnadňuje objevování a prohlížení vizuálního obsahu na internetu.

Social Catfish

Social Catfish je specializovaný vyhledávací nástroj zaměřený na ověřování identity a reverzní vyhledávání obrázků, který pomáhá uživatelům identifikovat a ověřit osobní údaje lidí, se kterými komunikují online. Tento nástroj je široce využíván pro boj proti podvodům na internetu, jako jsou romantické podvody, catfishing (vytváření falešných online identit) a další formy online podvodů. Social Catfish umožňuje uživatelům nahrát fotografie a provádět rozsáhlá vyhledávání, aby zjistili, zda byly tyto obrázky použity jinde na internetu, a identifikovat původní zdroj obrázků.

Vedle reverzního vyhledávání obrázků Social Catfish nabízí i další služby, jako jsou vyhledávání podle jména, e-mailové adresy, telefonního čísla nebo sociálních médií, což uživatelům umožňuje získat širší kontext o osobách, s nimiž se setkávají online. Tímto způsobem mohou uživatelé zjistit, zda jsou informace poskytované danou osobou pravdivé, nebo zda existují nějaké rozpory, které by mohly naznačovat podvod.

Tento nástroj je zvláště užitečný pro osoby, které se snaží ověřit identitu někoho, koho poznaly přes online seznamky, sociální sítě nebo jiné platformy pro virtuální komunikaci. Pomocí technologií pro rozpoznávání obličejů a rozsáhlých databází obrázků Social Catfish pomáhá odhalit falešné profily a chránit uživatele před potenciálními hrozbami a zklamáními.

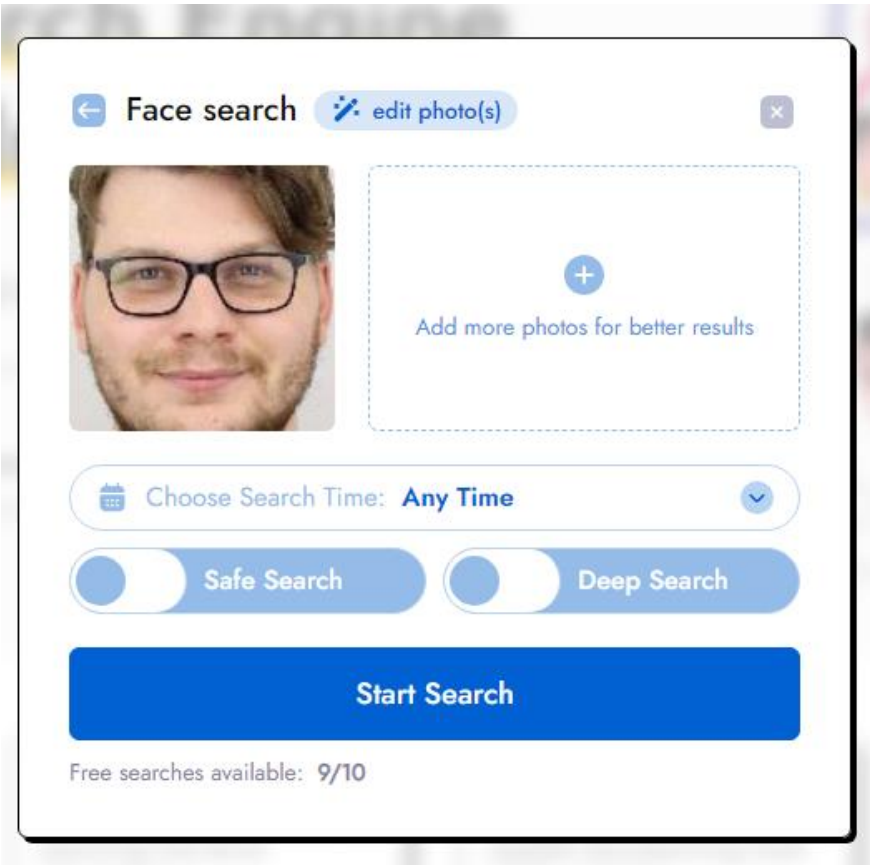
Kromě služeb ověřování identit nabízí Social Catfish také zdroje a informace týkající se online bezpečnosti a prevence podvodů, poskytuje rady, jak

se chránit před různými typy online podvodů, a vzdělává uživatele o tom, jak se bezpečně pohybovat v digitálním světě.

3.5. Průběh výzkumu

PimEyes

Vyhledávání pomocí služby PimEyes je velice jednoduché a intuitivní. Vložíte pouze již vyfocený obrázek z paměti vašeho zařízení, nebo můžete popřípadě vyfotit novou fotografii pomocí fotoaparátu, například mobilu (obrázek č. 14).



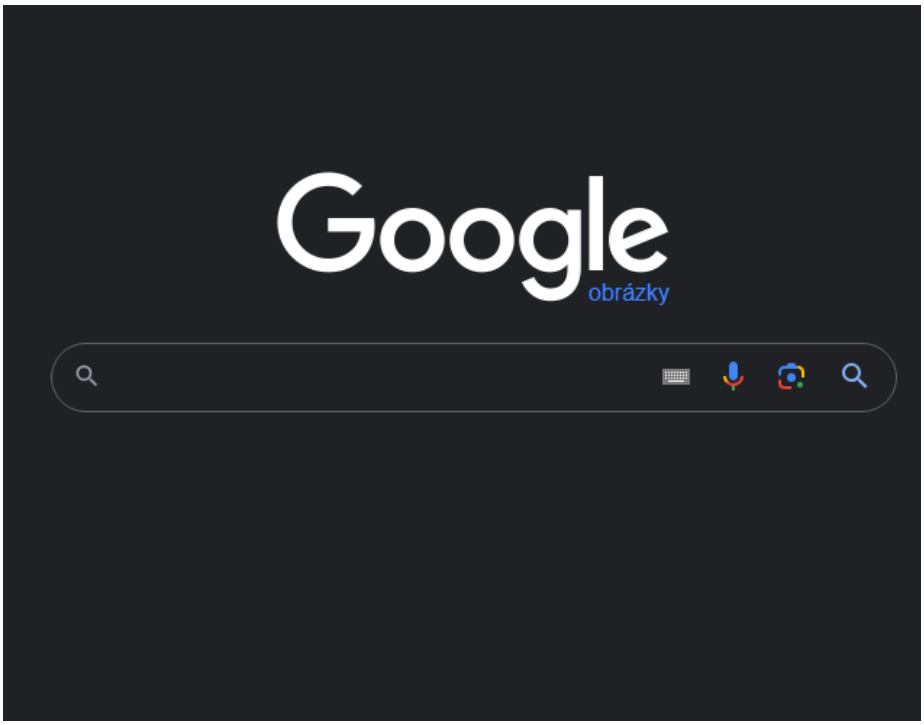
Obrázek č. 14 – Vyhledávací okénko u PimEyes

Poté jen odsouhlasíte nutná pravidla, která jsou s využívaním této služby povinná dodržet a proces vyhledávání začne. Samotné vyhledávání trvá pouze několik vteřin. Nutno podotknout, že využívám pouze verzi, která je zadarmo.

Následně se zobrazí tři výsledky vyhledávání po řadách, které můžete porovnat a případně se podívat na část zdroje, z něhož obrázek pochází.

Google Images

Obdobným způsobem jako u předchozí služby postačí pouze vložit obrázek do vyhledávacího řádku a okamžitě jsou nám známy výsledky vyhledávání. Je třeba podotknout, že u této služby není nutností vyhledávání pouze osob, ale lze pomocí ní vyhledávat i předměty, či dokonce místa (obrázek č. 15).



Obrázek č. 15 – Vzhled stránky Google Images

Social Catfish

Taktéž jako u předchozích vyhledávačů je celý proces jednoduchý a intuitivní. Pouze vložíte obrázek do vyhledávacího řádku a poté začne proces vyhledávání. V tomto případě trval zdaleka nejdéle oproti předchozím případům, ale celý proces vyhledávání byl znázorněn ikonami, ve kterých služba zrovna

vyhledává jako například sociální služby Facebook, Instagram či LinkedIn. Vyhledávání pomocí této služby, ale oproti předchozí není zdarma a celá služba je výhradně určená pro americký kontinent, avšak jedná se jeden z nejlepší vyhledávačů na internetu.

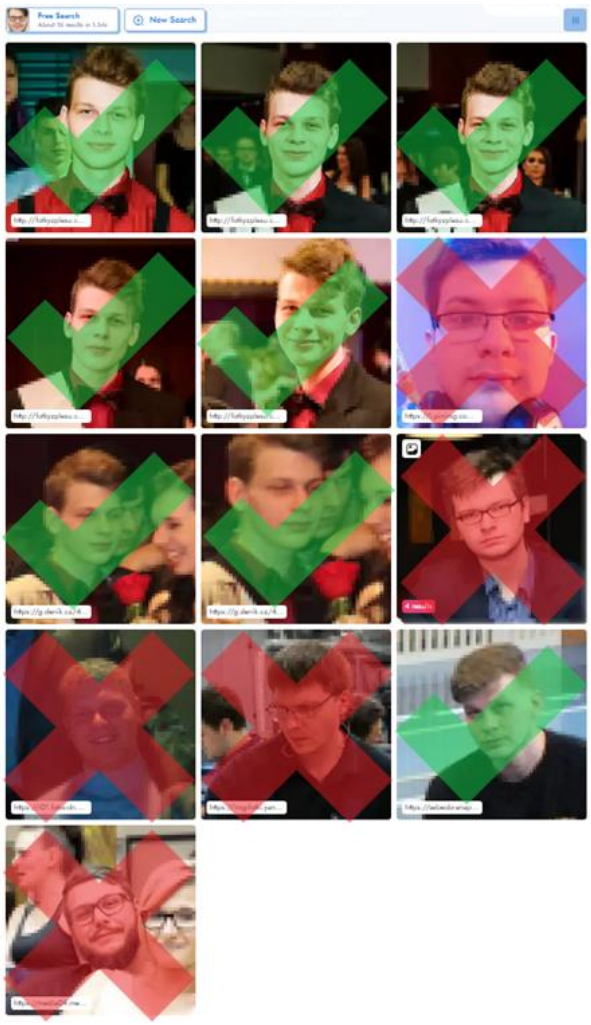
3.6. Výsledky výzkumu

PimEyes

Osoba číslo 1

Vyhledávání osoby číslo 1 pomocí služby PimEyes bylo v několika případech úspěšné (obrázek č. 16 – zeleně označena shoda, červeně označena neshoda).

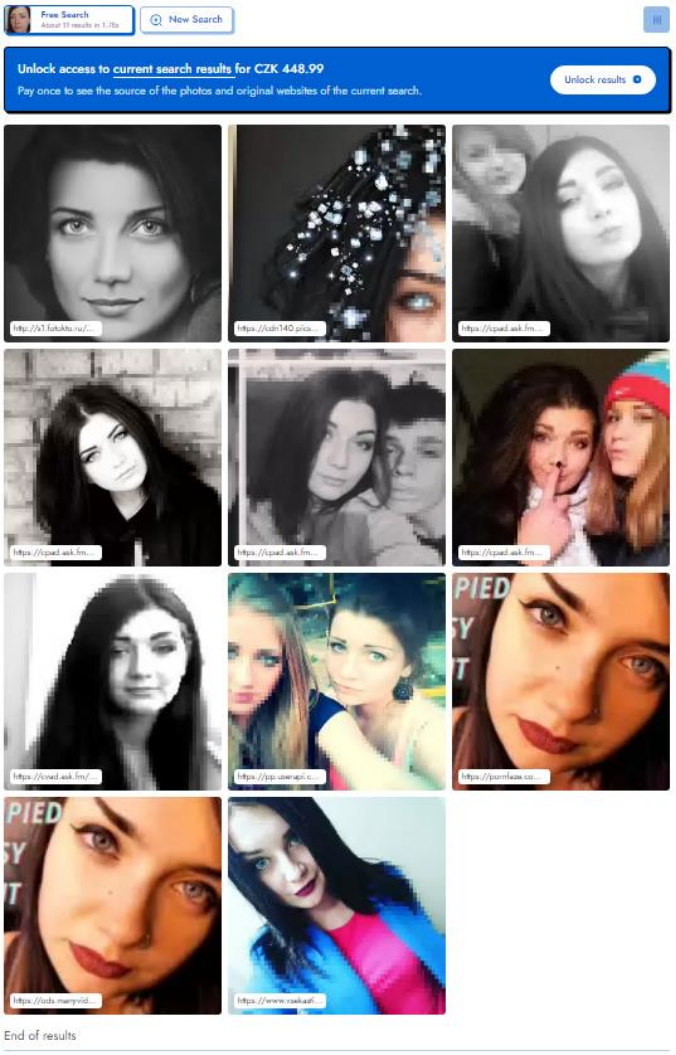
Z 15 výsledků se osobu číslo 1 podařilo skutečně najít v 10 případech z 15 vyhledaných výsledků, jednalo zejména o fotografie z maturitního plesu, což lze usoudit snadno z části url zdroje, ze které fotografie pochází.



Obrázek č. 16 – Výsledek vyhledávání osoby číslo 1 na PimEyes

Osoba číslo 2

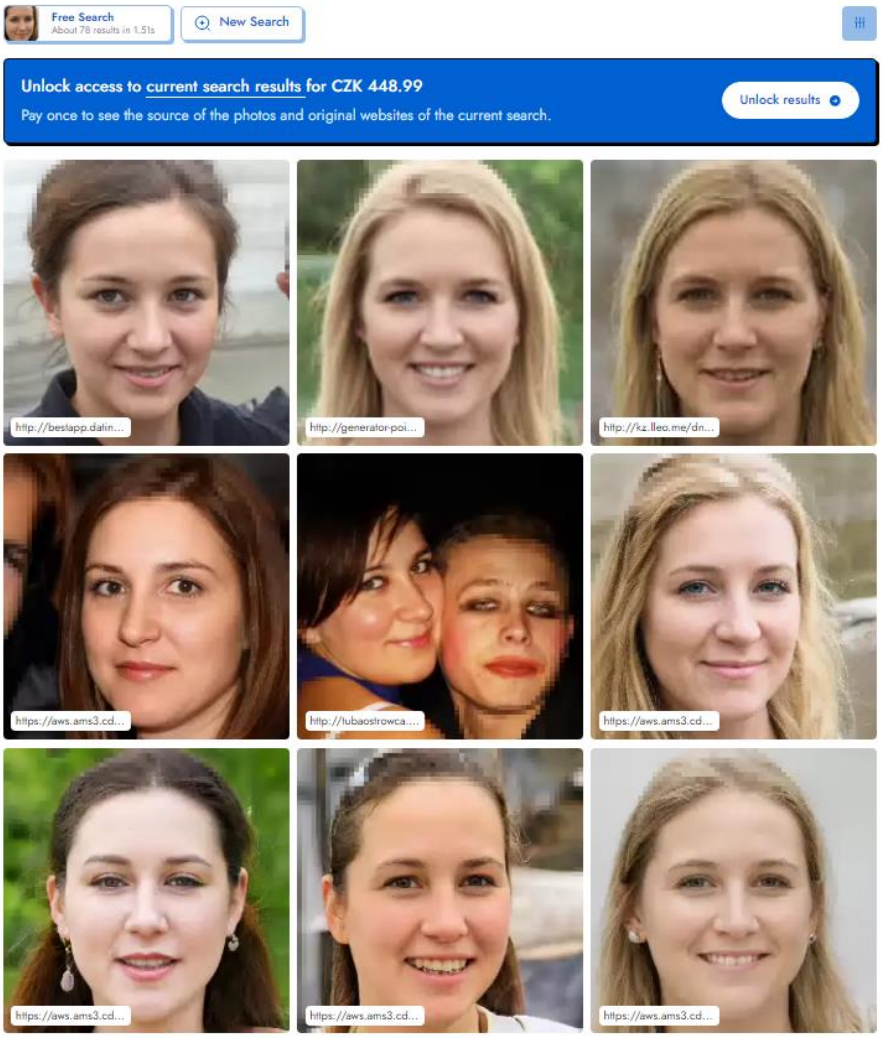
Osobu číslo 2 vyhledala služba PimEyes s celkem 11 výsledky, které se však se skutečnou osobou číslo 2 neshodovaly. (obrázek č. 17)



Obrázek č. 17 – Výsledek vyhledávání osoby číslo 2 na PimEyes

Osoba číslo 3

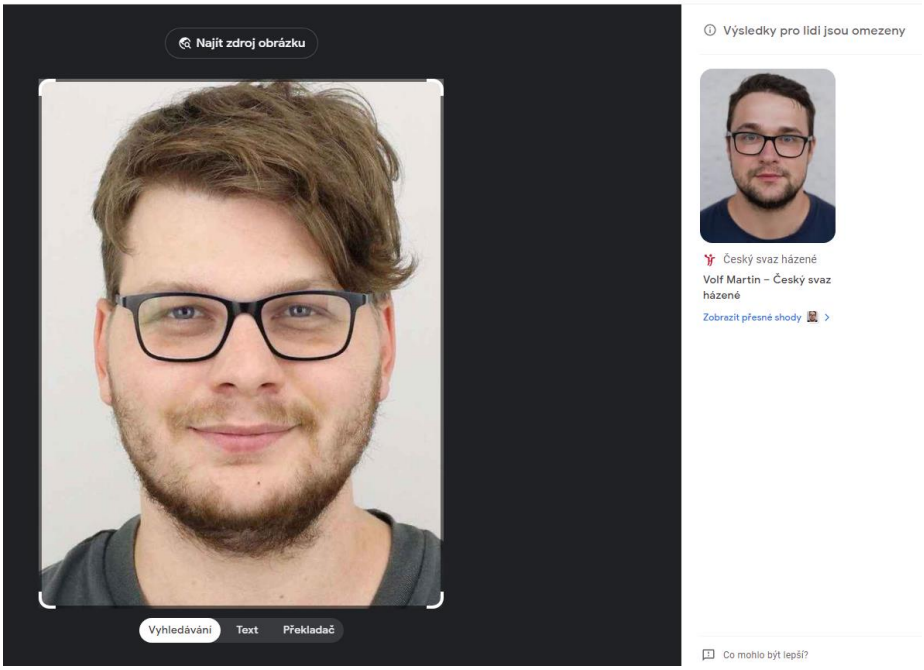
Osoba číslo 3 byla na službě PimEyes vyhledána celkem se 78 výsledky, avšak totožný obrázek se vyhledat nepodařilo (obrázek č. 18). S vědomím, že byla vyhledána neexistující osoba, je jasné, že se jedná o skutečně neshodná vyhledávání.



Obrázek č. 18 – Výsledek vyhledávání osoby číslo 3 na PimEyes

Google Images

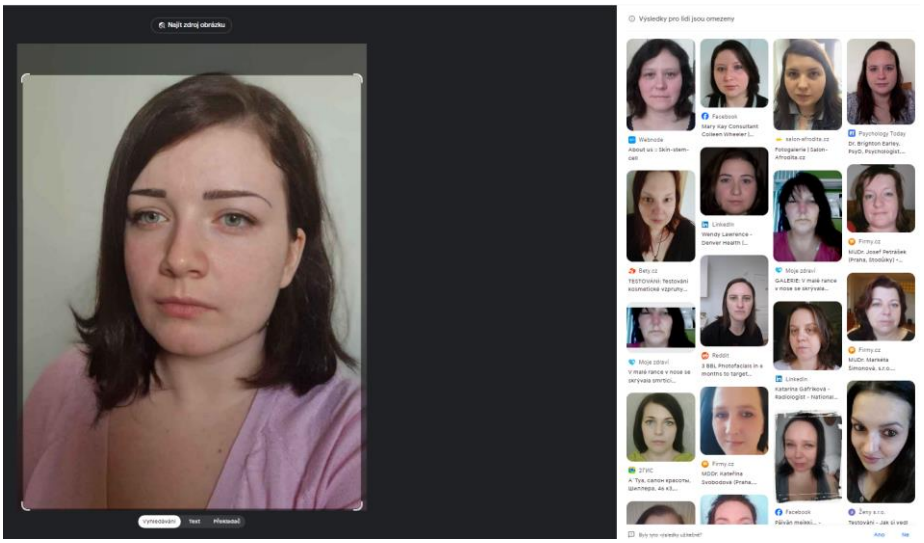
Osoba číslo 1 se pomocí nástroje Google Images nepodařila vyhledat. Výsledkem vyhledání byl pouze jeden výsledek, který odkazoval na jinou osobu než skutečně osoba číslo 1 je. (obrázek č. 19)



Obrázek č. 19 – Výsledek vyhledávání osoby číslo 1 na Google Images

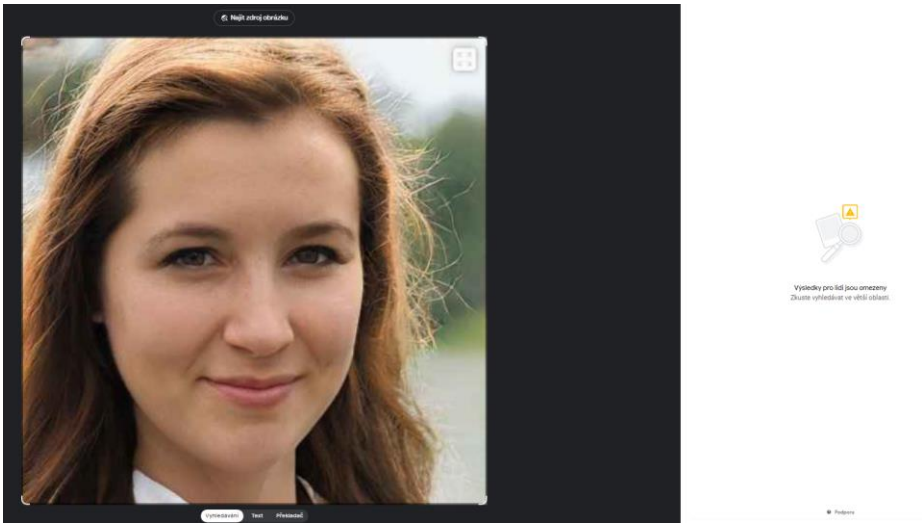
Osoba číslo 2

Výsledkem vyhledání osoby číslo 2 bylo několik osob či obrázku z různých webových stránek, ale o skutečnou osobu číslo 2 se nejednalo v žádném případě. (obrázek č. 20)


Obrázek č. 20 – Výsledek vyhledávání osoby číslo 2 na Google Images

Osoba číslo 3

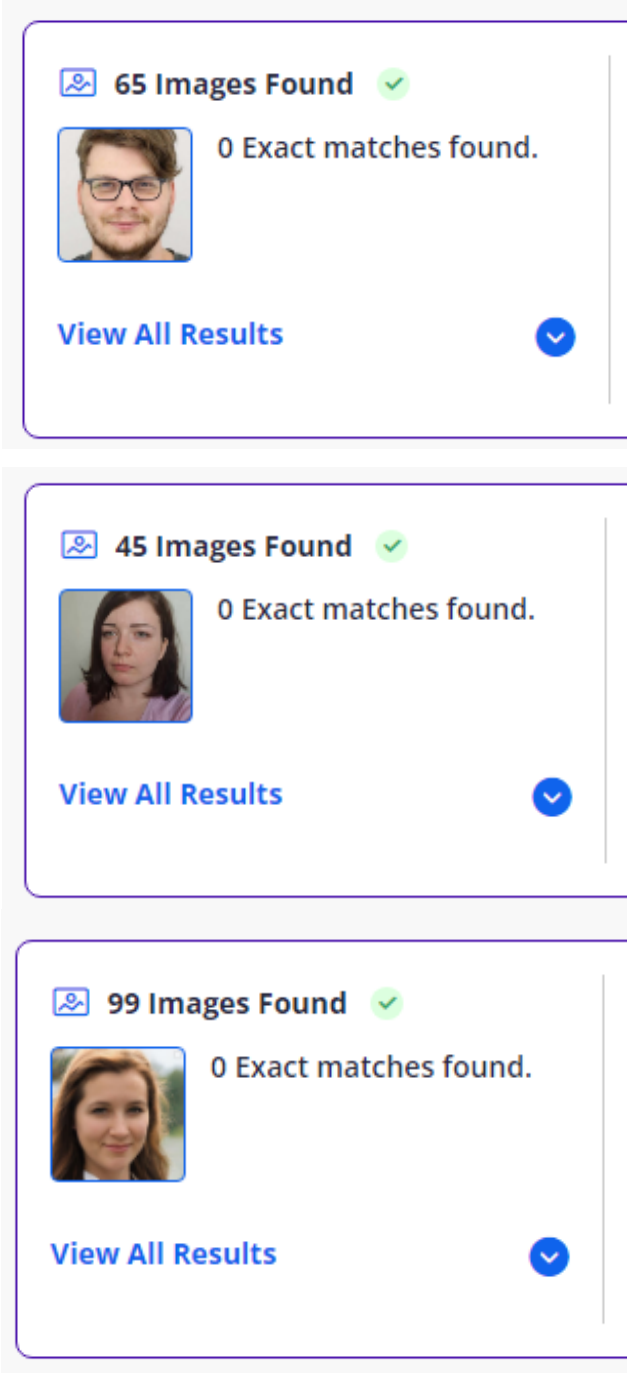
Vyhledáním osoby číslo 3 nebyly nalezeny žádné výsledky. (obrázek č. 21)



Obrázek č. 21 – Výsledek vyhledávání osoby číslo 3 na Google Images

Social Catfish

Pomocí tohoto vyhledávače se nepodařila v žádném případě u tří vyhledávaných osob najít skutečně shoda. Služba nabízela několik desítek obdobných obrázků, avšak žádný z nich nevytvářel skutečnou shodu. (obrázek č. 22)



Obrázek č. 22 – Výsledek vyhledávání osoby číslo 1,2 a 3 na Social Catfish

3.7. Závěr výzkumu

Závěr výzkumu zaměřeného na možnost využití komerčních nástrojů na vyhledávání obličejů na internetu pro policejní účely, s využitím vyhledávačů

PimEye, Google Images a Social Catfish, ukazuje smíšené výsledky, které reflektují jak potenciál, tak omezení těchto nástrojů.

Výzkum prokázal, že PimEye dokázal úspěšně identifikovat existující osobu číslo 1, což naznačuje, že pro konkrétní případy a za předpokladu dostupnosti kvalitních obrazových dat mohou být nástroje na vyhledávání obličejů účinné. Tento úspěch ilustruje potenciál těchto nástrojů pomoci policejním složkám v rychlé identifikaci osob, což může být klíčové pro řešení trestných činů, pátrání po pohřešovaných osobách nebo identifikaci podezřelých.

Nicméně, neschopnost vyhledávačů nalézt osobu číslo 2 a neexistující osobu číslo 3 poukazuje na významné omezení a výzvy spojené s používáním těchto technologií. Tyto výsledky poukazují na možnou omezenou účinnost v situacích, kde jsou dostupná data omezená, nekvalitní nebo zcela absentují. To zdůrazňuje, že spolehlivost a přesnost těchto nástrojů může být výrazně ovlivněna dostupností a kvalitou obrazových databází, na kterých vyhledávání závisí.

Dalším důležitým zjištěním je, že úspěšnost vyhledávání může být silně variabilní mezi různými platformami, což naznačuje potřebu pečlivého výběru nástrojů v závislosti na konkrétním využití. Tento fakt podtrhuje význam adaptability a flexibility při výběru technologických řešení pro policejní účely.

Závěrem, ačkoliv existuje potenciál využití komerčních vyhledávačů obličejů v policejní praxi, je nezbytné pečlivě zvážit jejich omezení a výzvy. Pro maximální efektivitu a etické využití je důležité další zkoumání a vývoj těchto technologií s důrazem na zlepšení přesnosti, rozšíření databází a zajištění souladu s právními a etickými normami. Tento výzkum také poukazuje na nutnost pokračující evaluace a validace nástrojů pro konkrétní policejní aplikace, aby se zajistilo jejich efektivní a spravedlivé využití.

3.8. Navrhované řešení

Na základě zjištění z výzkumu týkajícího se využití komerčních nástrojů na vyhledávání obličejů pro policejní účely, které ukázaly smíšené výsledky, lze navrhnout následující řešení problému:

1. Vylepšení a rozšíření databází
    - Spolupráce s komerčními poskytovateli, jako jsou PimEye, Google Images a Social Catfish, na rozšíření a aktualizaci jejich obrazových databází s cílem zvýšit přesnost a spolehlivost vyhledávání.
    - Integrace policejních databází s komerčními nástroji, pokud je to možné a právně přípustné, aby se zvýšila účinnost identifikace osob.

2. Vývoj a adaptace technologií
    - Investovat do vývoje vlastních, specializovaných vyhledávacích nástrojů na obličej, které by byly přímo navrženy pro potřeby bezpečnostních složek, s důrazem na zlepšení přesnosti a minimalizaci falešně pozitivních výsledků.
    - Adaptovat existující nástroje pro specifické policejní aplikace, včetně vývoje algoritmů schopných lépe rozlišovat mezi existujícími a neexistujícími osobami.

3. Právní a etické zabezpečení
    - Vypracovat a implementovat jasné právní a etické směrnice pro používání nástrojů na vyhledávání obličejů, zahrnující ochranu soukromí, ochranu údajů a zásady nezasahování do osobních práv.
    - Provádět pravidelné revize a evaluace používání těchto nástrojů s cílem zabezpečit jejich zodpovědné využití a soulad s právními normami.

4. Vzdělávání a školení
    - Organizovat školení a vzdělávací programy pro policejní pracovníky na téma používání nástrojů na vyhledávání obličejů, včetně aspektů právních, etických a technických.
    - Poskytnout policistům návody a nejlepší postupy pro efektivní a etické využívání těchto nástrojů.

5. Spolupráce a partnerství

- Navázat partnerství s akademickými institucemi, výzkumnými organizacemi a technologickými společnostmi na společných projektech zaměřených na vývoj a zlepšení nástrojů na vyhledávání obličejů.
- Podporovat mezinárodní spolupráci a výměnu osvědčených postupů mezi bezpečnostními složkami různých zemí.

Implementací těchto řešení mohou policejní složky využít potenciál nástrojů na vyhledávání obličejů, zatímco minimalizují rizika a omezení spojená s jejich používáním. To umožní efektivnější a etičtější využití těchto technologií v boji proti kriminalitě a při ochraně veřejnosti.

Závěr

V diplomové práci byla dopodrobna zkoumána rostoucí role biometrických technologií v kontextu zajištění veřejné bezpečnosti s konkrétním zaměřením na jejich aplikaci u Policie České republiky. Práce systematicky pokrývá teoretické základy biometrie, detailní analýzu dvou klíčových biometrických technologií daktyloskopie a rozpoznávání obličejů a jejich využití u Policie České republiky a empirický výzkum využití komerčních nástrojů pro vyhledávání obličejů na internetu v policejní praxi.

V první části byl poskytnut hloubkový teoretický úvod do problematiky biometrie, kde byly vysvětleny klíčové koncepty, historický vývoj a různé metody a technologie využívané v biometrických systémech. Byla zdůrazněna unikátnost biometrických dat a jejich potenciál pro identifikaci a autentizaci jednotlivců, což je zásadní pro bezpečnostní aplikace. Tento úvod také nastínil etické a právní otázky spojené s používáním biometrie, včetně ochrany soukromí a rizik nesprávné identifikace.

Ve druhé části práce byla podrobně prozkoumána specifická využití daktyloskopie a rozpoznávání obličejů u Policie České republiky. Byla zde popsána současná situace jak z technického hlediska, tak i z metodického či právního. Byl zde prezentován i případ úspěšného využití systému rozpoznávání obličejů na Letišti Václava Havla a jeho potenciál a přínos pro společnost.

Analýza zdůraznila význam těchto technologií pro zlepšení operativních schopností policie a jejich přínos k celkovému zvýšení bezpečnosti společnosti.

Třetí část práce se zaměřila na empirický výzkum, který zkoumal možnosti využití komerčních nástrojů na vyhledávání obličejů na internetu pro policejní účely. Přestože výzkum ukázal, že nástroje, jako PimEye, mohou být úspěšné v identifikaci určitých osob, také odhalil omezení těchto systémů, včetně problémů s přesností a spolehlivostí, a zdůraznil význam pečlivého zvážení právních a etických aspektů jejich použití. Bylo jasné, že i přes potenciál těchto technologií je nutné další výzkum a vývoj, aby bylo možné překonat existující výzvy a maximalizovat jejich přínos pro policejní praxi.

V závěrečné části práce jsou shrnuty klíčové poznatky a navržena doporučení pro budoucí vývoj a využití biometrických systémů v bezpečnostní praxi. Zdůrazňuje se potřeba pokračujícího výzkumu, vývoje a testování biometrických technologií s cílem zlepšit jejich přesnost, spolehlivost a etické využití. Je navrženo, aby byla věnována zvláštní pozornost vývoji směrnic a regulací, které by řešily právní a etické otázky spojené s biometrií, a zároveň podporovaly inovace a spolupráci mezi veřejným a soukromým sektorem. Práce zdůrazňuje, že s přihlédnutím k rychlému technologickému pokroku a rostoucímu významu biometrie pro bezpečnostní aplikace je nezbytné, aby se policie adaptovala na tyto změny a využívala nové technologie zodpovědně a efektivně, s plným respektem k právům a soukromí jednotlivců.

Seznam použité literatury

Monografie:

DRAHANSKÝ, Martin a Filip ORSÁG a kolektiv. Biometrie. Brno: Computer Press, 2011. ISBN 978-80-254-8979-6.

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

WAYMAN, James. Biometric systems: technology, design, and performance evaluation. London: Springer, c2005. ISBN 1852335963.

VÁCHOVÁ, Ivona. Biometrie a její využití v kriminalistice. Bakalářská práce. České Budějovice: Jihočeská univerzita v Českých Budějovicích, 2019.

MITRA, Sinjini; GOFMAN, Mikhail (ed.). Biometrics in a data driven world: trends, technologies, and challenges. CRC Press, 2016.

Internetové zdroje:

PEREZ, Jose Luis. RECORDIA. Understanding Biometric Authentication: Advantages and Disadvantages [online]. [cit. 2024-02-25]. Dostupné z: https://recordia.net/en/understanding-biometric-authentication-advantages-and-disadvantages/

Biometric Devices 101: Definition and Examples. Online. Dostupné z: https://www.aratek.co/news/biometric-devices-definition-and-examples. [cit. 2024-01-25].

What is Biometrics? How is it used in security? [online]. [cit. 2024-01-25]. Dostupné z: https://www.kaspersky.com/resource-center/definitions/biometrics

RISKS & BENEFITS OF BIOMETRICS IN SECURITY [online]. [cit. 2024-01-25]. Dostupné z: https://www.softwaresecured.com/post/risks-and-benefits-of-biometrics-in-security

GUENNOUNI, Souhail, Anass MANSOURI a Ali AHAITOUF. Biometric Systems and Their Applications. Visual Impairment and Blindness - What We Know and What We Have to Know [online]. IntechOpen, 2020, 2020-9-9 [cit. 2024-02-17]. ISBN 978-1-83880-257-8. Dostupné z: doi:10.5772/intechopen.84845

BIOMETRICS INSTITUTE. Types of Biometrics [online]. [cit. 2024-02-17]. Dostupné z: https://www.biometricsinstitute.org/what-is-biometrics/types-of-biometrics/

JAIN, A.K., A. ROSS a S. PRABHAKAR. An Introduction to Biometric Recognition. IEEE Transactions on Circuits and Systems for Video Technology [online]. 2004, 14(1), 4-20 [cit. 2024-01-25]. DOI: 10.1109/TCSVT.2003.818349. ISSN 1051-8215. Dostupné z: http://ieeexplore.ieee.org/document/1262027/

LINKEDIN. The Ethics of Using Facial Recognition and Fingerprint Technology [online]. , ArkEvo Group. [cit. 2024-02-17]. Dostupné z: https://www.linkedin.com/pulse/ethics-using-facial-recognition-fingerprint-technology-arkevo-group

INCITS 385-2004[R2014]: Information Technology - Face Recognition Format For Data Interchange. ANSI Webstore [online]. [cit. 2024-01-05]. Dostupné z: https://webstore.ansi.org/Standards/INCITS/INCITS3852004R2014

PIMEYES. More than a reverse image search [online]. [cit. 2024-02-13]. Dostupné z: https://pimeyes.com/en

SHOTKIT. HOW TO USE FACIAL RECOGNITION SEARCH [online]. [cit. 2024-02-13]. Dostupné z: https://shotkit.com/facial-recognition/

Seznam použitých obrázků

Obrázek č. 1 – Typy biometrických systémů
https://cdn.ttgtmedia.com/rms/onlineimages/security-biometric_authentication_types_mobile.png

Obrázek č. 2 – Juan Vucetich a inventář otisků prstů
https://www.expatincroatia.com/wp-content/uploads/2021/04/ivan-vucetic-fingerprinting.jpg

Obrázek č. 3 – Biometrická identifikace na základě otisku prstu
https://assets-global.website-files.com/61845f7929f5aa517ebab941/6359ec34f715910b3cf6515f_Biometric%20fingerprint%20scanners%20by%20Aratek.jpg

Obrázek č. 4 – Biometrická identifikace na základě rozpoznání obličeje
https://eforensicsmag.com/wp-content/uploads/2014/05/facial-recognition-data-points.jpg

Obrázek č. 5 – Biometrická identifikace na základě oční sítnice
https://d1sr9z1pdl3mb7.cloudfront.net/wp-content/uploads/2019/12/05172231/biometric-iris-recognition-for-healthcare.png

Obrázek č. 6 – Využití otisků prstů u bezpečnostních složek
https://www.thalesgroup.com/sites/default/files/gemalto/AFIS-history.jpg

Obrázek č. 7 – Využití otisků prstů u bankovního terminálu (ATM)
https://i.cdn.turner.com/cnn/2010/WORLD/europe/07/05/first.biometric.atm.europe/t1larg.jpg

Obrázek č. 8 – Markanty
https://slideplayer.cz/slide/3342891/11/images/7/MARKANTY+za%C4%8D%C3%A1tek+%28ukon%C4%8Den%C3%AD%29+kr%C3%A1tk%C3%A1+%C4%8D%C3%A1rka+vidlice+o%C4%8Dko+h%C3%A1%C4%8Dek+m%C5%AFstek.jpg

Obrázek č. 9 – Využití rozpoznávání obličejů Policií České republiky
https://edu.ceskatelevize.cz/video/13944-rozpoznavani-obliceju-pomoci-umele-inteligence

Obrázek č. 10 – Použití systému NeoFace
https://s.yimg.com/ny/api/res/1.2/IIfPVHqU4miKDq5UWO7Qdg--/YXBwaWQ9aGlnaGxhbmRlcjt3PTY0MDtoPTM2MA--/https://media.zenfs.com/en-SG/homerun/vulcanpost.com/2807c9d4e353086cafc1c9c23e21c749

Obrázek č. 11 – Osoba číslo 1
vlastní tvorba

Obrázek č. 12 – Osoba číslo 2
vlastní tvorba

Obrázek č. 13 – Osoba číslo 3
vlastní tvorba

Obrázek č. 14 – Vyhledávací okénko u PimEyes
vlastní tvorba