GYMNÁZIUM JÍROVCOVA 8

MATURITNÍ PRÁCE

Rozpoznávání obličeje pomocí strojového učení

Lukáš Lacina
vedoucí práce: Dr. rer. nat. Michal Kočer

V Českých Budějovicích 14. února 2025 **2024/2025**

Prohlášení

Prohlašuji, že jsem tuto práci vypracoval samostatně s vyznačením všech použitých pramenů.

V Českých Budějovicích dne ..... podpis .....

Lukáš Lacina

Abstrakt

Klíčová slova

Poděkování

Obsah

I Rozpoznávání obličeje a strojové učení **2**

1 Úvod do rozpoznávání obličeje **3**

1.1 Definice technologie rozpoznávání obličeje 3

1.2 Způsob fungování 3

1.3 Význam a využití 4

1.4 Zneužití technologie rozpoznávání obličeje 4

2 Historie a vývoj rozpoznávání obličeje **6**

2.1 Počátky technologie rozpoznávání obličeje 6

2.2 Automatizace a První algoritmy 6

2.2.1 Metoda Eigenfaces a PCA 6

2.2.2 Projekt FERET 7

2.3 Strojové učení a jeho vliv v technologii rozpoznávání obličeje 7

2.3.1 Hluboké učení a konvoluční neuronové sítě 8

2.3.2 CNN modely 8

2.4 iPhone X a FaceID 8

2.5 Technologie rozpoznávání obličeje dnes 9

3 Umělá inteligence a strojové učení) **10**

3.1 Umělá inteligence 10

3.2 Strojové učení 10

3.2.1 Učení s učitelem (Supervised learning) 11

3.2.2 Učení bez učitele (Unsupervised learning) 11

3.2.3 Učení posilováním (Reinforcement learning) 11

4 Metody pro rozpoznávání obličeje / Předzpracování dat 13

4.1 Detekce obličeje . . . 13

4.2 Extrakce rysů . . . 13

4.3 Klasifikace . . . 13

5 Algoritmy pro rozpoznávání obličeje 14

5.1 Algoritmy . . . 14

5.2 Datasety . . . 14

5.3 Trénování algoritmu . . . 14

6 Problematika a etické otázky 15

6.1 Ochrana soukromí . . . 15

6.2 Diskriminace a zaujatost . . . 15

6.3 Etické otázky... . . . 15

II Implementace programu na rozpoznávání obličeje 16

7 Cíl a záměr práce 17

8 Představa a použité nástroje 18

9 Struktura programu 19

10 Vlastní program 20

10.1 Předzpracování dat . . . 20

10.2 Vlastní algoritmus . . . 20

10.3 Předtrénování algoritmu . . . 20

10.4 Uživatelské rozhraní . . . 20

Bibliografie 23

Zkratky 24

Přílohy 27

A Fotky z pokusů 28

B Příloha další **29**

Úvod

Část I

Rozpoznávání obličeje a strojové učení

1 Úvod do rozpoznávání obličeje

1.1 Definice technologie rozpoznávání obličeje

Technologie rozpoznávání obličeje je technologií, která dokáže detekovat a extrahovat lidskou tvář z digitálního obrazu a poté porovnat tuto tvář s databází předem identifikovaných tváří. Tato technologie se obecně rozděluje na 3 formy dle její funkce: [1, 14]

- **One-to-One Identification**: Tato forma rozpoznávání obličeje porovnává obličej jedné osoby s předem identifikovanou tváří v databázi. Nejčastěji se využívá pro autentizaci uživatelů, například při odemykání mobilních zařízení. [14]
- **One-to-Many Identification**: Tato forma umožňuje technologie identifikovat konkrétní osobu mezi mnoha dalšími tím, že porovná obličej s rozsáhlou databází identit. Používá se zejména k masovému sledování. [14]
- **Emotion and Demographic Recognition**: Tato forma zpracování obličeje je nejpokročilejší a zaměřuje se na analýzu rysů obličeje tak, aby následovně odhadla demografické charakteristiky, jako je věk, pohlaví nebo emoční stav konkrétní osoby. [14]

1.2 Způsob fungování

Rozpoznávání obličeje je složitý proces, který zahrnuje několik klíčových kroků, které lze shrnout následovně: [1, 10]

1. **Shromažďování dat:** Prvním krokem je shromáždění dat z digitálních snímků. Tyto snímky mohou pocházet z různých zdrojů, jako jsou fotografie, videa nebo bezpečnostní kamery. [1, 10]

2. **Detekce obličeje:** V této fázi dochází za pomoci složitých algoritmů k identifikaci a lokalizaci obličeje v obraze. Tento krok zahrnuje analýzu obrazu za účelem určení oblastí, kde se nacházejí obličeje. [1, 10]

3. **Extrakce rysů:** Jakmile je obličej detekován, následuje extrakce klíčových rysů obličeje, jako jsou vzdálenost mezi očima, tvar lícních kostí a délka čelisti. Tyto rysy se dále převádějí do matematické reprezentace, která umožňuje jejich snadnější analýzu a porovnání. [1, 10]

4. **Porovnání:** Extrahované rysy se poté porovnávají s uloženými daty v databázi obličejů. Tato fáze zahrnuje hodnocení podobnosti mezi jednotlivými obličeji, což je klíčové pro určení identity osob. [1, 10]

1.3 Význam a využití

Význam technologie rozpoznávání obličeje je v dnešní době větší, než si většina lidí uvědomuje. Nejčastěji se využívá **v bezpečnosti**, kdy tato technologie umí ověřovat identitu jednotlivců, například při přihlašování k různým službám či zařízením. Také však hledá pohřešované osoby nebo odhaluje osoby podezřelé. Newyorská policie například uvedla, že díky technologii rozpoznání obličeje dokázala chytit pachatele do 24 hodin od útoku. Bezpečnost je hlavní důvod, proč se technologie rozpoznávání obličeje stává populární, avšak poskytuje mnohem více přínosů. [12]

Rozpoznávání obličeje se používá **v marketingu** pro zefektivnění různých procesů. Například v obchodě Amazon Go stačí zákazníkovi k nákupu pouze projít obchodem, vzít si zboží a odejít. Dále se používá **v sociálních médií**, kde jsou platformy schopny automaticky označit uživatele na fotografiích. V posledních pár letech se však tato technologie objevuje i **ve zdravotnictví**, kde je schopna sledovat zdravotní stav pacientů a tím zvýšit efektivitu poskytování zdravotní péče. [12]

1.4 Zneužití technologie rozpoznávání obličeje

Ačkoli má technologie rozpoznávání obličeje mnoho přínosu, může být také zneužita. Jeden z nejzásadnějších problému je **nelegální sledování osob**. Například některé autoritářské

režimy využívají tuto technologii k monitorování a potlačování opozičních skupin, což je narušení základních lidských práv a svobod. [7]

Dalším velkým problémem jsou **kybernetické útoky**, kdy hackeři využívají data o obličeji, aby mohli provádět různé podvody, například odemykání zařízení nebo bankovních účtů. Jelikož změnit biometrické údaje je v podstatě nemožné, jejich odcizení může mít závažné následky. Tyto útoky často vedou k ztrátě finančních prostředku nebo ke ztrátě soukromí. [7]

Z těchto důvodu jsou technologie rozpoznávání obličeje regulovány tak, aby se co nejvíce zamezilo zmíněným problémům. Zavádí se právní rámce a etické standardy pro jejich používání. Avšak bez těchto regulací muže tato technologie způsobit více škody než užitku. [12]

2 Historie a vývoj rozpoznávání obličeje

2.1 Počátky technologie rozpoznávání obličeje

Snaha o vytvoření technologie rozpoznávání obličeje sahá již do roku **1964**, kdy americký vědec **Woodrow Wilson Bledsoe** přišel s myšlenkou vytvořit stroj, který bude rozpoznávat lidské tváře. A tak Bledsoe společně s Helen Chan Wolf a Charles Bisson **vytvořil poloautomatickou metodu na rozpoznávání obličeje**. Bledsoeova metoda rozpoznávala rysy manuálně, vědci museli identifikovat celkově 20 různých měřítek jako je vzdálenost mezi očima, délka nosu nebo šířku rtů. Tyto parametry byly poté využity k vytvoření vektorové reprezentace obličeje, kterou počítač porovnával. V roce **1977** byl systém vylepšen o dalších 21 parametrů pro zlepšení přesnosti. [5, 17]

Bledsoeova metoda byla sice průlomová, avšak měla spousty výrazných omezení jako její **nízkou rychlost či častou nepřesnost**. Nepřesnost byla způsobována variabilitou osvětlení, úhly pohledu a individuálními rysy obličejů, což omezovalo její praktické užití. [5, 17]

2.2 Automatizace a První algoritmy

2.2.1 Metoda Eigenfaces a PCA

V roce **1988** se začala uplatňovat statistická metoda **PCA (Principal component analysis)** v oblasti počítačového vidění. Tato metoda byla schopna redukovat potřebné množství dat a extrahovat klíčové rysy v obličeji, které do této doby určovali vědci manuálně. [1, 5]

Díky metodě PCA vyvinul **Matthew Turk a Alex Pentland** v roce **1991** novou revoluční metodu rozpoznávání obličeje - **metoda Eigenfaces**. Tato metoda byla schopna detekovat obličeje na snímcích, což vedlo k **první automatické technologii rozpoznávání obličeje**. Tato metoda byla jednoduchá a měla relativně dobrou přesnost, což vedlo

k jejímu rychlému rozšíření. Nicméně tomuto průlomu bránily technologické a environmentální faktory, jako například omezený výpočetní výkon a kvalita databází, ze kterých se algoritmus učil. [2, 5]

2.2.2 Projekt FERET

V roce **1993** přišla agentura **DARPA** (Defense Advanced Research Projects Agency) s programem **FERET** (Facial Recognition Technology), který měl za cíl vyvinout **rozsáhlou standardizovanou databázi obličejů**. Tento projekt vznikl jako reakce na rostoucí zájem o technologie rozpoznávání obličeje a jejich aplikace v bezpečnosti a identifikaci. [4, 5, 18]

Databáze FERET obsahovala přes **14 000 snímků obličejů**, které byly foceny **v rozdílných podmínkách**, včetně osvětlení, úhlů a výrazů. Tato rozmanitá databáze umožnila testování a trénování různých algoritmů rozpoznávání obličejů na kvalitním datasetu, který je klíčový pro spolehlivou funkčnost algoritmu. Projekt FERET také přinesl **standardizované metodologie pro hodnocení výkonu algoritmů**, což umožnilo porovnávat efektivitu různých přístupů. [4, 18]

Díky tomuto projektu se zlepšila efektivita a přesnost technologií rozpoznávání obličeje a FERET se stal základem pro budoucí aplikace. [4]

2.3 Strojové učení a jeho vliv v technologii rozpoznávání obličeje

Strojové učení je podmnožina umělé inteligence, která má schopnost se učit nebo predikovat žádané stavy. Strojové učení se začíná v oblasti rozpoznávání obličejů uplatňovat **již v 90. letech** - poprvé se objevilo **v metodě Eigenfaces**. Strojové učení umožňovalo algoritmům učit se z velkého množství dat, což způsobovalo výrazné zlepšení přesnosti a spolehlivosti rozpoznávání obličeje. [8, 9]

Avšak k významnému pokroku došlo až **na začátku 21. století**, kdy se začíná aplikovat technika **hlubokého učení**. [8, 9]

2.3.1 Hluboké učení a konvoluční neuronové sítě

Hluboké učení je technika strojového učení, která používá **konvoluční neuronové sítě (CNN)**. CNN je umělá neuronová síť, která je navržena tak, aby efektivně zpracovávala a analyzovala obrazová data. Tato technika se začala v rozpoznávání obličejů používat **v roce 2012**, kdy **Alex Krizhevsky a jeho tým vytvořili síť AlexNet**. AlexNet vyvolal velký příliv zájmu a investic do metod hlubokého učení a díky tomu vznikají během následujících 4 let nové revoluční algoritmy - **DeepFace, VGGFace, DeepID a FaceNet**, které posunuly technologii rozpoznávání obličeje na novou úroveň. [8, 9]

2.3.2 CNN modely

Tyto modely byly trénovány na několika milionech snímků, měli vysokou rychlost zpracování a také vysokou úspěšnost. Například model **DeepFace** od společnosti Meta měl úspěšnost správného rozpoznání obličeje **přes 97 %**, což je stejná přesnost, jakou má člověk. [9, 16]

2.4 iPhone X a FaceID

Technologie rozpoznávání obličeje se začala používáním hlubokého učení rychle zdokonalovat a **12. září 2017 představila společnost Apple iPhone X, první iPhone s funkcí FaceID**. Zařízení bylo uvedeno na trh 3. listopadu téhož roku. **FaceID** je biometrická metoda, která pomocí **3D skenování** obličeje umožňuje odemknout iPhone a nabízí tak vysokou úroveň bezpečnosti. Poprvé v historii přineslo FaceID pokročilou technologii 3D rozpoznávání obličeje přímo do spotřebitelského zařízení, což nastavilo nový standard v oblasti zabezpečení. Před FaceID bylo rozpoznávání obličeje u spotřebitelských zařízení převážně pouze 2D, a tedy ne moc bezpečné, protože bylo možné ho oklamat například fotografií. [5, 13]

V dnešní době je FaceID tak dokonalé, že rozpozná obličej přes čepici, šátky, optické brýle, kontaktní čočky, roušku či růst vousů. **Úspěšnost FaceID je 99,99 %** a kromě odemykání zařízení umí také ověřovat platby, přihlašovat uživatele do aplikací nebo vytvářet animované emoji (Animoji a Memoji) na základě pohybů obličeje. [13]

2.5 Technologie rozpoznávání obličeje dnes

Dnes se technologie rozpoznávání obličeje stále více opírá o pokroky v hlubokém učení a konvolučních neuronových sítích. Moderní algoritmy, jako jsou DeepFace, FaceNet a FaceID, dosahují vysoké přesnosti rozpoznávání obličeje i v extrémních podmínkách, což posunulo technologii na novou úroveň. Tyto modely jsou schopny v některých aspektech překonávat lidské schopnosti, avšak stále narážejí na problémy, jako je variabilita osvětlení, úhly pohledu a odlišnosti v obličejových výrazech. [14]

3 Umělá inteligence a strojové učení)

Předtím než se podrobně zaměříme na technologii rozpoznávání obličeje, je klíčové si vysvětlit základní principy umělé inteligence a strojového učení, na kterých tato technologie staví a které jí umožňují dosahovat vysoké přesnosti a spolehlivosti při identifikaci obličejů.

3.1 Umělá inteligence

Umělá inteligence (AI, artificial intelligence) je oblast informatiky, která se zabývá vytvářením systémů, které mají napodobovat lidský mozek a být tedy schopné vykonávat úkoly, které vyžadují lidskou inteligenci. Tyto úkoly zahrnují rozpoznávání a používání řeči, plánování tras, řešení problému, rozpoznávání obrazů atd. Umělá inteligence se dělí na několik podkategorií, z nichž strojové učení je jednou z nejvýznamnějších. [8]

Hlavním cílem umělé inteligence je vyvinout systémy, které se dokážou samostatně učit a adaptovat na nové situace. To zahrnuje schopnost analyzovat velké množství dat, vyvozovat z nich závěry a zrychlovat se. V kontextu rozpoznávání obličeje se umělá inteligence využívá k trénování modelů, které dokážou efektivně rozpoznávat vzory v obličejích. [8]

3.2 Strojové učení

Strojové učení (ML, machine learning) je podmnožina umělé inteligence, která se zabývá návrhem metod a algoritmů, které umožňují systémům se učit z předchozích zkušeností, tedy z dat, Data jsou základem správného fungování strojového učení a je nutné, aby byly správně zvolené a předzpracované, aby algoritmy mohly efektivně fungovat. Například při analýze počasí je potřeba mít dostatek dat, které obsahují minimální a maximální teploty, rychlost větru, objem srážek atd. Na základě takto zpracovaných dat algoritmus identifikuje vzorce a vztahy, podle kterých predikuje výsledky. [8]

Hlavní výhodou strojového učení je, že algoritmy mohou postupně zlepšovat svou přesnost

bez toho, aby bylo nutné je ručně upravovat. Tento proces zlepšování je možný díky adaptivnímu učení, kdy model zohledňuje své chyby v dalších predikcích. S rostoucím množstvím dat a trénováním modelu tedy strojové učení dosahuje stále vyšší přesnosti. [8]

Strojové učení je díky svému autonomnímu zlepšování zásadní v mnoha moderních aplikací, jako je rozpoznávání obrazu, zpracování přirozeného jazyka, automatizované rozhodovací systémy, diagnostika onemocnění nebo personalizaci obsahu na internetu. [8]

Strojové učení lze rozdělit na tři základní typy, z nichž každý má své specifické fungování a algoritmy:

3.2.1 Učení s učitelem (Supervised learning)

Učení s učitelem je metoda, při které je algoritmus trénován na datech obsahujících jak vstupy, tak i odpovídající výstupy. Během trénování model porovnává své predikce s reálnými výstupy a na základě rozdílu upravují své parametry tak, aby se zvýšila přesnosti predikce. Tento typ učení se využívá v úlohách **regrese** (kdy je cílová proměnná spojitého typu, například při odhadování tržních ceny domu) a **klasifikace** (kdy je cílová proměnná kategoriálního typu, například přiřazení obličeje z fotografie ke konkrétní osobě). Tento typ učení se využívá právě u technologie rozpoznávání obličeje, kde se často používají konvoluční neuronové sítě (CNN). [8]

3.2.2 Učení bez učitele (Unsupervised learning)

Učení bez učitele, oproti učení s učitelem, neobsahuje žádné informace o struktuře dat. Cílem těchto metod je právě strukturu v datech identifikovat. Struktura se identifikuje především pomocí **shlukování** (kdy se dělí data podle jejich podobnosti) nebo **redukce dimenzionality** (kdy se data přetransformují tak, aby byla zachována jejich nejdůležitější struktura a vzory, což zjednodušuje jejich reprezentaci). Algoritmy učené bez učitele se uplatňují tam, kde nejsou dostupná označená data, například analýza chování zákazníků nebo v doporučovacích systémech, kde se identifikují skupiny s podobnými preferencemi. [8]

3.2.3 Učení posilováním (Reinforcement learning)

Učení posilováním je metoda, při které se algoritmus učí **pomocí zpětné vazby (odměny)**. Algoritmus přijímá pouze dvě formy zpětné vazby - kladné odměny a záporné odměny. Učí

se průběžně a upravuje své parametry, díky využívání zpětných vazeb z okolí, a postupně se optimalizuje jeho chování. Algoritmus využívá **Q-učení** (vyhledává optimálnípredikci tím, že maximalizuje očekávanou hodnotu odměny v dalších krocích) a **TD-učení** (stroj se učí tak, že zkouší určité akce a upravuje predikce podle dat z minulosti). Učení posilováním se využívá v situacích, kde je klíčová schopnost rozhodování, například hraní her (šachy nebo Go) či autonomní ovládání systémů. [8]

4 Metody pro rozpoznávání obličeje / Předzpracování dat

4.1 Detekce obličeje

4.2 Extrakce rysů

4.3 Klasifikace

5 Algoritmy pro rozpoznávání obličeje

5.1 Algoritmy

5.2 Datasety

5.3 Trénování algoritmu

6 Problematika a etické otázky

6.1 Ochrana soukromí

6.2 Diskriminace a zaujatost

6.3 Etické otázky...

Část II

Implementace programu na rozpoznávání obličeje

7 Cíl a záměr práce

8 Představa a použité nástroje

9 Struktura programu

10 Vlastní program

10.1 Předzpracování dat

10.2 Vlastní algoritmus

10.3 Předtrénování algoritmu

10.4 Uživatelské rozhraní

Závěr

Bibliografie

1. ADJABI, Insaf; OUAHABI, Abdeldjalil; BENZAOUI, Amir; TALEB-AHMED, Abdelmalik. Past, Present, and Future of Face Recognition: A Review. *Electronics*. 2020, roč. 9, č. 8. Dostupné také z: `https://www.mdpi.com/2079-9292/9/8/1188`.
2. ANTONIADIS, Panagiotis. *How Do Eigenfaces Work?* 2024. Dostupné také z: `https://www.baeldung.com/cs/cv-eigenfaces`.
3. AUTORŮ, kolekriv. *JEDNODUŠE: Umělá inteligence*. Universum, 2023.
4. CONTIBUTORS, NIST. *Face Recognition Technology (FERET)*. 2011. Dostupné také z: `https://www.nist.gov/programs-projects/face-recognition-technology-feret`.
5. CONTRIBUTORS, NEC. *A brief history of Facial Recognition*. 2022. Dostupné také z: `https://www.nec.co.nz/market-leadership/publications-media/a-brief-history-of-facial-recognition/`.
6. FRANÇOIS, CHOLLET. *Deep learning v jazyku Python: knihovny Keras, Tensorflow. Knihovna programátora*. Grada, 2019.
7. GARGARO, David. *The pros and cons of facial recognition technology*. 2024. Dostupné také z: `https://www.itpro.com/security/privacy/356882/the-pros-and-cons-of-facial-recognition-technology`.
8. HENDL, Jan. *Big data - Věda o datech, základy a aplikace*. GRADA, 2021.
9. LYTVYNENKO, Oleksandr. *Machine Learning Algorithms for Face Recognition*. 2022. Dostupné také z: `https://codeit.us/blog/machine-learning-face-recognition#what-is-face-recognition`.
10. QINJUN, Li; CUI TIANWEI, Zhao Yan; YUYING, Wu. Facial Recognition Technology: A Comprehensive Overview. *Academic Journal of Computing Information Science*. 2023.

11. RUDOLF, Pecinovský. *Python - Kompletní příručka jazyka pro verzi 3.11*. Grada, 2022.

12. SOUKUPOVÁ, Jana. *Možnosti využití technologie rozpoznávání obličejů v kontextu ochrany osobních údajů v EU*. Praha, 2022. Rigorózní práce. Univerzita Karlova, Právnická fakulta, Katedra evropského práva.

13. SUPPORT, Apple. *Informace o vyspělé technologii Face ID*. 2023. Dostupné také z: `https://support.apple.com/cs-cz/102381`.

14. *The Cambridge Handbook of Facial Recognition in the Modern State*. Cambridge University Press, 2024. Cambridge Law Handbooks.

15. VALLA, Tomáš. *Průvodce labyrintem algoritmů*. CZ.NIC, 2022.

16. WIKIPEDIA CONTRIBUTORS. *DeepFace — Wikipedia, The Free Encyclopedia*. 2024. Dostupné také z: `https://en.wikipedia.org/w/index.php?title=DeepFace&oldid=1240075590`. [Online; accessed 29-October-2024].

17. WIKIPEDIA CONTRIBUTORS. *Facial recognition system — Wikipedia, The Free Encyclopedia*. 2024. Dostupné také z: `https://en.wikipedia.org/w/index.php?title=Facial_recognition_system&oldid=1250429409`. [Online; accessed 28-October-2024].

18. WIKIPEDIA CONTRIBUTORS. *FERET (facial recognition technology) — Wikipedia, The Free Encyclopedia*. 2024. Dostupné také z: `https://en.wikipedia.org/w/index.php?title=FERET_(facial_recognition_technology)&oldid=1232099360`.

Zkratky

atd. a tak dále. 10

Seznam obrázků

Seznam tabulek

Přílohy

A Fotky z pokusů

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

B Příloha další