3D rozpoznávání tváře *(face detection)*

Rozpoznávání tváře chápeme jako technologií počítačového vidění, využívající metody umělé inteligence pro rozpoznávání objektů. Trojrozměrné rozpoznávání tváře si jednoduše můžeme představit jako zachycení obličeje v prostoru a jeho následné rozpoznání. V základu jde o užití konkrétního algoritmu UI k detekci obličeje z videosnímku (který slouží jako matematický vzorec uplatněný na lidskou tvář a je součástí některé z metod UI – neuronová síť, metoda eigenface aj.). Algoritmus rovněž slouží k postupnému generování databáze s obličeji. Oproti rozpoznávání tváře z dvojrozměrného obrazu, které chápeme jako pouhou lokalizaci a rozpoznání tváře z digitálního obrazu, je 3D zachycení obličeje podstatně složitější, ale také časově úspornější. Navíc dvojrozměrné získávání dat o obličeji mnohdy selhává z důvodu změny osvětlení, změny barvy kůže (teplota, opálení, make-up) či kvůli jiné polohy hlavy, čemuž se 3D technologie vyvarovala díky používání principu morfometrie, která zajišťuje rozpoznávání tváře na základě geometrie pevných obličejových rysů, které jsou dány kostmi.

Získaný obraz se používá ve verifikačních (tj. ověřovací) nebo identifikačních (tj. jednoznačné zjištění) systémech. Verifikační systémy srovnávají detekovaný obličej s konkrétním obličejem v databázi (fotografií), pod kterým se daná osoba verifikuje a následně nachází, anebo nenachází shodu. Výsledkem verifikačních systému je pouhé ověření dané osoby. S těmito systémy se standardně setkáváme v čistě biometrických systémech (bezpečný přístup či přihlášení do určitého objektu či systému). Zatímco identifikační systémy, které využívají vládní složky, jako je FBI, NSA aj., fungují na principu jednoznačné identifikace, což znamená srovnávání detekované tváře se všemi tvářemi uloženými v databázi

Trojrozměrný model tváře můžeme získat nejčastěji dvojím způsobem, a to konverzí dvojrozměrného obrazu na 3D scénu (nejčastěji pomocí normálové mapy) anebo pomocí 3D scanneru, což je zařízení, které je schopno zachytit 3D scénu přímo.

Jak již bylo zmíněno, pro účely čistě biometrické se využívají verifikační systémy. Takovým příkladem je systém Broadway 3D, který se využívá na zajištění bezpečnosti na mezinárodním letišti v Soči. Systém využívá 3D čtečku obličeje s rozšířenou verzí metody „eigenface“. Princip je však stejný jako u původní metody „eigenface“, tzn., že se do databáze nejdříve uloží vymodelovaná standardizovaná (průměrná) tvář, která byla statisticky vytvořená z obrovského souboru obrázků s tvářemi (aby program dokázal i z dálky rozpoznat, jak lidská tvář vypadá). Standardizovaná hlava je v programu uložena jako sada vektorů (čísel), jejichž projekce je pak 3D model. V případě, že se do bezpečností databáze zařazují tváře nové (které budou do budoucna rozpoznávány), tzn. zaměstnanci letiště, či zaměstnanci leteckých společností, vychází se z této původní hlavy, u které dojde ke změně matematického vzorce (na základě odlišné geometrie obličejových rysů). Prakticky to znamená, že když se chce osoba verifikovat, program pro rozpoznávání tváře zachytí při chůzi její tvář, 3D čtečka jej načte, program poté detekuje geometrii obličejových rysů, prohledá databázi, nalezne shodu (event. nenalezne shodu) a osoba projde bezpečnostní kontrolou. Celá tato akce trvá asi 2 sekundy. Rozpoznávání obličeje v systém Broadway 3D probíhá na základě zhruba 40 000 obličejových rysů, které se v programu ukládají jako matematický vzorec, jedinečný pro každou tvář. Dříve systémy nedokázaly zachytit lidi, kteří měli na sobě čepici, šátek nebo brýle, a z tohoto důvodu bylo přísně zakázáno nosit jakoukoli pokrývku hlavy (obličeje). Toto již není současný problém.

Dalším příkladem užití této technologie je identifikační systém OptimEyes patřící společnosti Amscreen. Jedná se o užití pro komerční účely, konkrétně pro on-line řízení reklamy. V současnosti je tato technologie využívána na všech čerpacích stanicích ve Velké Británii a rovněž v některých nákupních střediscích v této zemi. Základem je vestavená

kamera s 3D čtečkou, která je propojená s programem pro rozpoznávání obličejů. Program v reálném čase rozpoznává počet možných zákazníků, počet aktuálních zákazníků, pohlaví zákazníků a v neposlední řadě také věk (rozlišuje 4 hlavní věkové skupiny). Tyto údaje slouží jako výstupní data na monitorech manažerů reklam, kteří mohou ihned ovlivňovat běh svých reklamních kampaní (tzn. spustit vhodný typ reklamy pro konkrétní skupinu lidí). Atribut pohlaví je rozpoznáváno na základě uložených a předem naučených vizuálních prvků – například nalezení tmavé zóny vlevo od brady znamená dlouhé vlasy (což je z 97% žena). Systém je na tolik vyvinutý, že dokáže rozpoznat jedince, i v případě, že má na sobě brýle či čepici. Jsou však dva krajní případy, kdy program do určité míry selhává. Prvním případem je rozlišení pohlaví v pokročilém věku, neboť ženám se s narůstajícím věkem vytrácí typické obličejové ženské rysy a obličej se blíží spíše mužskému. Druhým případem je rozlišení atributu věku, a to u jedince (tedy ženy) s burkou (pokrývka přes celý obličej/tělo – islámské vyznání).

Identifikační systémy využívají i vládní složky, jako je FBI, NSA aj. Software pro trojrozměrné rozpoznávání tváří užívaný FBI nazývá Biometric Center of Excellence a jeho nedílnou součástí je databáze NGI. Systém pro rozpoznávání je vestavěný v bezpečnostních kamerách a nazývá se Interstate Photo System (IPS). Proces rozpoznávání se uskutečňuje pomocí neuronové sítě a aplikování algoritmu PCA, LDA a EBGM, kde rozhodující úlohu má algoritmus PCA. V současnosti systém propojuje rozpoznání tváře a diferencujících rysů (mateřská znamínka, tetování či jizvy). Základem je databáze s obličeji, kde je třeba mít minimálně 2 fotografie každé osoby (zepředu a z profilu), tak aby neuronová síť měla větší předpoklad úspěšnosti při trénování a následném testování.

Cílem je jednak najít zločince a nežádoucí osoby, které není schopna tato složka pomocí lidí najít, ale také ověření běžné sorty lidí (nově vzniklý cíl). To znamená, že finálně by databáze měla obsahovat fotografie všech lidí. Před dvěma lety obsahovala databáze něco okolo 1,6 milionu fotografií a do roku 2015 se předpokládá počet okolo 51 milionů fotografií (denně nárůst v řádech deseti tisíců). Zdrojem tváří jsou bezpečnostní kamery, snímky pořízené po zatčení, ale také soukromé fotografie. Před dvěma lety trvalo porovnání 1 tváře s více než 10 000 tvářemi 1 sekundu, nyní se za tento stejný čas porovnává 1 tvář se zhruba 56 tisíci tváři (tj. 5,6x více). Z daných faktů vyplývá, že identifikace jedné osoby trvá zhruba 10-15 min. (x 2D identifikace otisku prstů trvající zhruba 2 hodiny). Od roku 2015 program hodlá používat i státní policie, která má v plánu užívat jej asi 196x za den. V současnosti je možné zachytit obličej z délky 8 metrů, roku 2015 se očekává nárůst této délky na 52 metrů. Vzhledem k výrazné časové úspoře se do budoucna plánuje nahradit dvojrozměrné rozpoznávání otisků prstů právě za tento systém. Systém je v současné chvíli nainstalován na více než 18 tis. amerických úřadech. Vytvoření tohoto projekt trvalo 3 roky a v plně funkční verzi je od září roku 2014 (stále se však NGI databáze rozrůstá).

Z dané práce vyplývá, že původní účel, pro který byla tato technologie sestrojena, tedy na zajištění ochrany a bezpečnosti obyvatelstva, se značně liší od účelů, ke kterým se používá nyní, tzn. pro komerční účely (reklamy).