Prednosti tehnologije za prepoznavanje lica

Seminarski rad u okviru kursa
Računarstvo i društvo
Matematički fakultet

Vuk Stefanović
mi19066@alas.matf.bg.ac.rs

Jun 2023.

Sažetak

Tema ovog rada je tehnologija za prepoznavanje lica. Rad objašnjava šta predstavlja tehnologija za prepoznavanje lica, njene prednosti, način na koji funkcioniše i gde se primenjuje.

Sadržaj

1 Uvod

Tehnologija za prepoznavanje lica je vrsta biometrijske tehnologije koja koristi algoritme i mašinsko učenje za identifikaciju i verifikaciju identiteta osobe na osnovu njenih crta lica. Poslednjih godina postaje sve popularniji zbog potencijalne primene u različitim industrijama, uključujuci bezbednost, marketing i zdravstvenu zaštitu. Softver identifikuje 80 čvornih tačaka na ljudskom licu. U ovom kontekstu, čvorne tačke su krajnje tačke koje se koriste za merenje varijabli lica osobe, kao što su dužina ili širina nosa, dubina očnih duplji i oblik jagodičnih kostiju. Sistem radi tako što hvata podatke za čvorne tačke na digitalnoj slici lica pojedinca i čuva rezultujuce podatke kao otisak lica. Otisak lica se zatim koristi kao osnova za poređenje sa podacima snimljenim sa lica na slici ili video snimku. Iako sistem za prepoznavanje lica koristi samo 80 čvornih tačaka, može brzo i precizno identifikovati ciljne osobe kada su uslovi povoljni

Slika 1: Prikaz na koji način tehnologija za prepoznavanje lica skenira osobu

2 Bezbednost na internetu

Tehnologija za prepoznavanje lica koristi jedinstvene matematičke obrasce za čuvanje biometrijskih podataka. Stoga je ona među najsigurnijim i najefikasnijim metodama identifikacije u biometrijskoj tehnologiji. Podaci o licu mogu biti anonimizovani i čuvani kao privatni da bi se smanjio rizik od neovlašcenog pristupa. Tehnologija detekcije živosti razlikuje žive korisnike od njihovih slika lica. Ovo sprečava sistem da bude prevaren fotografijom živog korisnika. Tehnologija prepoznavanja lica može se smatrati bezbednom zbog nekoliko mehanizama i praksi koje su postavljene da zaštite tačnost, privatnost i pouzdanost sistema. Evo kako se postiže sigurnost:

- Jedinstvene biometrijske osobine - Lice svake osobe je jedinstveno. Sistemi za prepoznavanje lica koriste specifične karakteristike lica i mere da bi napravili „otisak lica“ koji je teško duplirati.
- Šifrovanje - Podaci o licu su često šifrovani, što znači da su šifrovani tako da samo ovlašcene strane mogu da ih razumeju. To otežava hakerima pristup i zloupotrebu podataka
- Zaštita skladištenja podataka - Sačuvani podaci o licu čuvaju se u sigurnim bazama podataka, često uz strogu kontrolu pristupa. Ovo sprečava neovlašceni pristup osetljivim informacijama

- Kontinuirana poboljšanja - Programeri uvek rade na poboljšanju algoritama za prepoznavanje lica. Oni koriste velike skupove podataka i napredne tehnike za poboljšanje tačnosti i bezbednosti
- Višefaktorska autentifikacija - Za dodatnu sigurnost, prepoznavanje lica se može koristiti zajedno sa drugim metodama, kao što su lozinke ili otisci prstiju. Ovo otežava pristup neovlašcenim korisnicima
- Monitoring i revizija - Organizacije koje koriste prepoznavanje lica često prate i revidiraju svoje sisteme za bilo kakve sumnjive aktivnosti. Ovo pomaže u otkrivanju i sprečavanju kršenja bezbednosti

3 Face ID

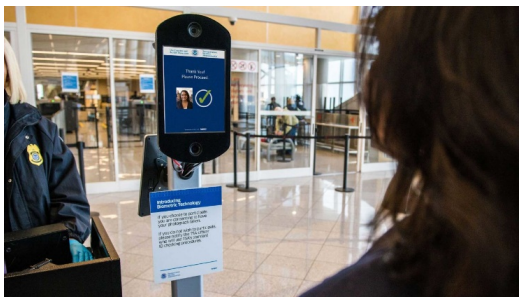
Face ID omogućava korisnicima da otključavaju svoje uređaje, kupuju i pristupaju sigurnim aplikacijama samo jednim pogledom. Koristi poseban sistem kamera, „TrueDepth", koji projektuje preko 30.000 nevidljivih tačaka na vaše lice kako bi napravio preciznu mapu vaših karakteristika. Ova mapa se zatim upoređuje sa onom uskladištenom u memoriji vašeg uređaja, da bi se potvrdio vaš identitet. Razni telefoni, uključujuci najnovije iPhone, koriste Face ID za otključavanje uređaja. Tehnologija nudi mocan način zaštite ličnih podataka i osigurava da osetljivi podaci ostanu nedostupni ako je telefon ukraden. Apple tvrdi da je šansa da slučajno lice otključa vaš telefon otprilike jedan prema milion. Face ID tehnologija menja igru u svetu bezbednosti i pogodnosti. Korišcenjem naprednih algoritama za prepoznavanje lica, omogucava korisnicima da otključaju svoje uređaje samo jednim pogledom, čineci proces bržim i lakšim nego ikada ranije. Štaviše, Face ID-a takođe pruža visok nivo bezbednosti, uz mere za zaštitu privatnosti i podataka korisnika. A kako tehnologija nastavlja da se razvija, možemo očekivati još uzbudljiviji napredak u buducnosti.

Slika 2: Prikaz kako Face ID funkcionise

4 Ilegalna migracija na granicama

Prepoznavanje lica postalo je uobičajen prizor na mnogim aerodromima širom sveta. Sve veci broj putnika ima biometrijske pasoše, koji im omogucavaju da preskoče uobičajeno dugačke redove i umesto toga prođu kroz automatizovanu kontrolu e-pasoša kako bi brže stigli do kapije. Gledanje nije uvek viđenje, a razlika između to dvoje može biti problematična za zaposlene na carini i graničnoj zaštiti. Zbog toga je granična služba

primenila tehnologiju za prepoznavanje lica gde softver za pracenje očiju meri performanse vizuelnog pretraživanja polaznika. Dok upoređuju slike lica Radne stanice prate kretanje očiju preko slika, podučavajuci učenike najboljim praksama i veštinama kritičkog vizuelnog prosuđivanja. Prepoznavanje lica na granici se može takođe koristiti za pronalaženje nestalih osoba i žrtava trgovine ljudima. Pretpostavimo da se nestali pojedinci dodaju u bazu podataka. U tom slučaju, organi za sprovođenje zakona mogu biti upozoreni čim budu prepoznati pomocu prepoznavanja lica. Od postavljanja, otprilike u prve tri godine, pre svega u vazduhoplovnom okruženju i donekle u pomorstvu, identifikovali smo oko 300 krijumčara koji koriste ovu tehnologiju. U poslednjih godinu dana na pešačkim kopnenim prelazima na južnoj kopnenoj granici uhvatio je oko 1.000 do 1.100.



Slika 3: Korisćenje tehnologije za prepoznavanje lica na graničnim prelazima

5 Smanjenje prevara

Dokle god postoje mehanizmi verifikacije identiteta, prevaranti ce uvek pronaci načine da zaobiđu ove barijere. Među tim tehnikama je lažiranje lica (poznato i kao napadi lažiranja lica), u kojem prevarant pokušava da zaobiđe sistem za prepoznavanje lica i da ga pogrešno identifikuje tako što predstavi lažno lice (npr. fotografiju, 3D modele, 3D štampanu masku) Kamera. Prevaranti takođe mogu da koriste metode potpomognute veštačkom inteligencijom kao što su „deepfakes", što predstavlja najvece izazove za dobavljače rešenja za prepoznavanje lica. Da bi se zaštitili od ovakvih pretnji, evoluirali su sistemi za otkrivanje lažiranja lica, kao što su provere životnosti, kako bi se umanjili rizici koji se pojavljuju. Na primer, gledanje teksture lica, gustine crta i odnosa između karakteristika može pomoci da se utvrdi da li je lice stvarno ili ne. Takve tehnologije omogucavaju operaterima da dobiju na vremenu tokom procesa uključivanja tako što imaju vece poverenje u pravi identitet svojih korisnika.

6 Uspesnost brzine pretrage

Tehnologija prepoznavanja lica je napravila značajan napredak tokom godina i sada može da radi impresivnim brzinama. Brzina tehnologije prepoznavanja lica može da varira na osnovu nekoliko faktora, uključujuci hardver koji se koristi, korišcene algoritme i specifičan slučaj upotrebe. Evo nekih opštih smernica:

- Prepoznavanje u realnom vremenu - Mnogi moderni sistemi za prepoznavanje lica su sposobni za obradu u realnom vremenu, što znači da mogu analizirati i prepoznati lica u delicu sekunde. Ovo je ključno za aplikacije kao što su nadzor, kontrola pristupa i autentifikacija korisnika
- Okviri u sekundi (FPS) - Brzina prepoznavanja lica se često meri u frejmovima u sekundi (FPS), što pokazuje koliko pojedinačnih okvira (slika) sistem može da obradi i analizira u jednoj sekundi. Sistemi visokih performansi mogu postici stope FPS-a u rasponu od 30 do 60 FPS-a ili čak više
- Hardversko ubrzanje - Specijalizovani hardver, kao što su GPU-ovi (Jedinice za grafičku obradu) i TPU-i (Tenzorske procesorske jedinice), može značajno da ubrza zadatke prepoznavanja lica
- Modeli dubokog učenja - Moderne tehnike prepoznavanja lica često se oslanjaju na modele dubokog učenja, kao što su konvolucione neuronske mreže (CNN), koje su optimizovane za brzinu i tačnost. Ovi modeli mogu efikasno da obrađuju velike količine podataka, omogucavajuci brže prepoznavanje
- Ekstrakcija karakteristika - Brzina prepoznavanja lica takođe može zavisiti od toga koliko efikasno sistem izdvaja i obrađuje crte lica. Neki sistemi koriste tehnike za izdvajanje osnovnih crta lica pre pokretanja stvarnog algoritma za prepoznavanje, poboljšavajuci brzinu obrade
- Veličina baze podataka - Broj lica u bazi podataka koja se pretražuju takođe utiče na brzinu prepoznavanja. Vece baze podataka zahtevaju više računarskih resursa za uparivanje, što može uticati na ukupne performanse
- Faktori životne sredine - Kvalitet ulaznih slika, uslovi osvetljenja i složenost pozadine mogu uticati na brzinu i tačnost prepoznavanja lica. Slike lošeg kvaliteta mogu zahtevati više vremena obrade da bi se postigli tačni rezultati.

Sve u svemu, tehnologija prepoznavanja lica je napredovala do tačke u kojoj može da izvrši prepoznavanje velike brzine u različitim praktičnim scenarijima. Međutim, važno je napomenuti da stvarna brzina može da varira u zavisnosti od specifične tehnologije koja se koristi i uslova u kojima se primenjuje.

7 Zaključak

Ukratko, tehnologija prepoznavanja lica je postala bolja zahvaljujuci pametnijim algoritmima i bržem hardveru. Odličan je u tome što je precizan i brz, koristi se svuda, od bezbednosti do zabavnih stvari. Ali, to je takođe izazvalo zabrinutost za privatnost i pravičnost, tako da su pravila važna. Dok nastavljamo da ga proučavamo, prepoznavanje lica bi

moglo da olakša upotrebu uređaja i da nam pruži više ličnih iskustava – ali moramo da budemo oprezni i da ga pravilno koristimo.

Literatura

[1] Definition of Facial recognition

[2] The benefits of facial recognition technology

[3] Face ID advanced technology Apple

[4] Border protection systems

[5] Anti-spoofing facial recognition

[6] Wikipedia Facial recognition system