Primjena alata dubokog učenja za prepoznavanje lica

Santini, Karmen

SVEUČILIŠTE U ZAGREBU
FILOZOFSKI FAKULTET
ODSJEK ZA INFORMACIJSKE I KOMUNIKACIJSKE ZNANOSTI
Ak. god. 2020./ 2021.

Karmen Santini

Primjena alata dubokog učenja za prepoznavanje lica

Završni rad

Mentor: prof.dr.sc. Sanja Seljan

Zagreb, rujan 2021.

Izjava o akademskoj čestitosti

Izjavljujem da je ovaj rad rezultat mog vlastitog rada koji se temelji na istraživanjima te objavljenoj i citiranoj literaturi. Izjavljujem da nijedan dio rada nije napisan na nedozvoljen način, odnosno da je prepisan iz necitiranog rada, te da nijedan dio rada ne krši bilo čija autorska prava. Također izjavljujem da nijedan dio rada nije korišten za bilo koji drugi rad u bilo kojoj drugoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.

potpis

_____

Karmen Santini

Ovdje možete napisati kratku zahvalu ili stranicu možete ostaviti praznom.

Sadržaj

Sadržaj ii
1. Uvod 1
2. Umjetna inteligencija 3
2.1. Definicija i opseg umjetne inteligencije 4
3. Strojno učenje 8
3.1. Vrste strojnog učenja 9
3.1.1. Nadzirano učenje (učenje s učiteljem) 11
3.1.2. Nenadzirano učenje (učenje bez učitelja) 12
3.1.3. Polunadzirano učenje 13
3.1.4. Podržano učenje 14
4. Duboko učenje 15
4.1. Neuronske mreže 17
4.1.1. Konvolucijske neuronske mreže 20
4.1.2. Primjena umjetnih neuronskih mreža 22
4.2. Aplikacije za prepoznavanje i korekciju lica 22
4.2.1. Snapchat 22
4.2.2. FaceApp 24
4.2.3. Luxand FaceSDK 25
5. ISTRAŽIVANJE 27
5.1. Duboko učenje i duboki lažnjaci 27
5.2. *FaceSwap* i zamjena lica 30
5.3. Rezultati 35
6. Etički pristupi 38
6.1. Zavaravanje javnosti i širenje panike 38
6.2. Narušavanje ugleda i kršenje privatnosti 38
6.3. Širenje dezinformacija i kriminalitet 39

6.4. Mjere za reguliranje zlouporabe programa 40
6.5. Pozitivne strane dubokih lažnjaka 41
7. Zaključak 42
8. Literatura 44
Sažetak 49

1. Uvod

Prepoznavanje lica postalo je popularna tema istraživanja u području računalnog vida, obrade slika i prepoznavanja uzoraka. Na uspješnost sustava prepoznavanja lica u velikoj mjeri utječu varijacije u uvjetima osvjetljenja, smjerovima ili pozama gledanja, izrazu lica, starenju i maskiranju. Istraživanje provedeno od Aly i Hassaballah (2015)[1] jedno je od mnogih istraživanja koja upravo opisuju sustave prepoznavanja lica i kako oni funkcioniraju. U istraživanju se raspravlja o značajnim izazovima uključenima u prilagodbu postojećih algoritama za prepoznavanje lica za izgradnju uspješnih sustava koji se mogu koristiti u stvarnom svijetu. Zatim raspravljaju o dosadašnjem postignuću, posebno se usredotočujući na najuspješnije algoritme, te preispituju uspjehe i neuspjehe navedenih algoritama na određenom subjektu ili entitetu.

Prepoznavanje lica pruža široke primjene u komercijalnim, policijskim i vojnim službama, itd., poput sigurnosti zračne luke i kontrole pristupa, nadzora i praćenja zgrada, inteligentne interakcije čovjeka i računala i perceptivnih sučelja u npr. financijskom poslovanju (Marrara i sur., 2019[2], Krstić i sur., 2019[3]), pametnih okruženja kod kuće, ureda i automobila. Kortli, Jridi, Faloun i Atri (2020)[4] u svom istraživanju razvoja biometrijskih aplikacija, poput prepoznavanja lica, iznose da su se mnogi znanstvenici i inženjeri diljem svijeta usredotočili na uspostavljanje sve robusnijih i točnijih algoritama i metoda za ove vrste sustava i njihovu primjenu u svakodnevnom životu, te da razvojem informacijskih tehnologija i sigurnosnih algoritama, mnogi sustavi počinju koristiti mnoge biometrijske čimbenike za zadatak prepoznavanja. Ovi biometrijski čimbenici omogućuju prepoznavanje identiteta ljudi prema njihovim fiziološkim ili bihevioralnim karakteristikama. Oni također

---

[1] Aly, S., Hassaballah, M. (2015). Face Recognition: Challenges, Achievements, and Future Directions*, ET Computer Vision* 9(4):614-626,

[2] Marrara, S.; Pejić Bach, M., Seljan, S.; Topalovic, A. (2019). FinTech and SMEs: the Italian case. FinTech as a Disruptive Technology for Financial Institutions. Rafay, Abdul (ur.). Hershey, Pennsylvania: IGI Global,. 14-41. doi:10.4018/978-1-5225-7805-5.ch002,

[3] Krstić, Ž.; Seljan, S.; Zoroja, J. (2019). Visualization of big data text analytics in financial industry: a case study of topic extraction for Italian banks. *Proceedings of the ENTRENOVA '19 - ENTreprise REsearch InNOVAtion Conference*, 67-75.

[4] Kortli, Y., Jridi, M., Falou, A. A., & Atri, M. (2020). Face Recognition Systems: A Survey. Sensors (Basel, Switzerland), 20(2), 342.

pružaju nekoliko prednosti, na primjer, prisutnost osobe ispred senzora je dovoljna i nema više potrebe za pamćenjem nekoliko lozinki ili povjerljivih kodova. U tom su kontekstu posljednjih godina primijenjeni mnogi sustavi prepoznavanja koji se temelje na različitim biometrijskim čimbenicima, poput šarenice, otisaka prstiju, glasa i lica.

Također, istraživanje koje su proveli Galbally, Ferrara, Haraksim, Psyllos i Beslay (2019)[5] nad Schengenskim informacijskim sustavom (*SIS*) najraširenijim i najvećim sustavom razmjene informacija za sigurnost (provođenje zakona) i upravljanja granicom u Europi, govori o implementaciji dubokog učenja i sustava za prepoznavanje lica u svrhu zaštite granica i sigurnosti. Sustavi su primjenjeni tako da identificiraju i prepoznaju lica traženih osoba ili kriminalaca te tako spriječavaju njihov ulazak u neku državu i štite je.

Da bi bolje razumjeli na koji način funkcioniraju alati za prepoznavanje lica u dubokom učenju, moramo razumjeti odakle ono zapravo dolazi i iz čega se razvilo. Stoga ovaj rad na početku daje uvid u temeljni dio u područje tzv. dubokog učenja (eng. *deep learning*), odnosno u područje umjetne inteligencije (eng. *artificial intelligence*). Umjetna inteligencija širok je pojam koji obuhvaća sve ono što računalu omogućava da radi kao čovjek i bude inteligentno. Iz razvoja umjetne inteligencije proizašlo je strojno učenje, a to je vrsta učenja u kojoj stroj ili program uči iz treniranja nad različitim podacima ili iskustva, te se to učenje dijeli na nadzirano, nenadzirano i podržano. (Slota, 2020)[6] Iz daljnjeg razvoja strojnog, nastalo je duboko učenje koje se služi dubokim umjetnim neuronskim mrežama. Takvom sustavu nije potrebna ljudska intervencija za razliku od strojnoga učenja, te je potpuno samostalno. Nadalje, primjena dubokog učenja je raznolika, te se ovaj rad u praktičnom dijelu bazira na primjeni u području prepoznavanja lica osobe, na primjeru korištenja programa *FaceSwap*, koji na temelju umjetnih neuronskih mreža prepoznaje karakteristike lica i samo lice, da bi ga naposljetku uspješno zamijenilo za drugo unaprijed definirano lice. Cilj ovog rada je demonstrirati primjenu dubokog učenja pomoću alata *FaceSwap,* te prikazati njegov način rada i rezultate. Na kraju rada slijedi poglavlje u kojem se upozorava na moguće opasnosti i nemoralne zlouporabe, na moguće načine sprječavanja, ali i na pozitivne primjere korištenja ovakve tehnologije.

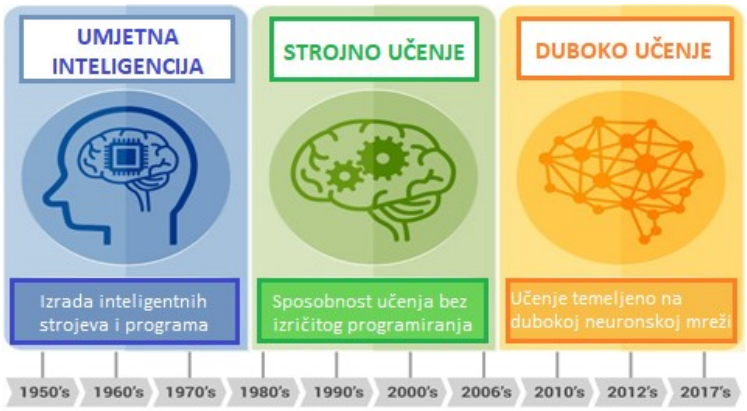
[5] Beslay, L., Galbally, J., Ferrara, P., Haraksim, R., Psyllos, A., (2019). Study on Face Identification Technology for its Implementation in the Schengen Information System, EUR 29808 EN, *Publication Office of the European Union, Luxemburg*, ISBN 978-92-76-08843-1

[6] Slota, M. (2020). Strojno učenje prepoznavanja rukopisne numeracije, Sveučilište u Zagrebu, Filozofski fakultet, završni rad, 43 str.

2. Umjetna inteligencija

Kad su računala prvi put izumljena ljudi su se pitali u kojem trenutku njihovog razvoja će ona postati inteligentna, čak više od stotinu godina prije nego što je 1946. godine prvo ENIAC računalo (Elektronički numerički integrator i računalo) i izgrađeno, kada je to sve bila samo apstraktna ideja u znanstveno-fantastičnim filmovima i serijama. Danas je umjetna inteligencija uspješno područje s mnogim praktičnim primjenama i aktivnim temama istraživanja.

Pokazalo se da je istinski izazov umjetnoj inteligenciji rješavanje zadataka koje je ljudima lako izvršiti, a teško opisati formalno, probleme koje rješavamo intuitivno, poput prepoznavanja izgovorenih riječi ili lica na slikama. Ironično, apstraktni i formalni zadaci koji su među najtežim mentalnim pothvatima za čovjeka, među najlakšima su za računalo. Računala već dugo mogu pobijediti najboljeg ljudskog šahista (1997. godine IBM Deep Blue pobjedio svjetskog prvaka u šahu Garyja Kasparova)[7], ali tek nedavno hvataju korak s nekim sposobnostima prosječnih ljudskih bića da prepoznaju predmete ili govor. Iz istraživanja i razvoja umjetne inteligencije proizašle su dvije njezine grane, strojno učenje, a potom dubinsko učenje. Slika 1 ilustrira odnos između umjetne inteligencije, strojnog učenja i dubokog učenja, gdje se prikazuje kronološki razvoj od umjetne inteligencije do dubokog učenja.



Slika 1. Kronološki prikaz razvoja umjetne inteligencije (Izvor: DanaDrivenInvestor 2018)[8]

[7] IBM, Deep Blue URL: https://www.ibm.com/ibm/history/ibm100/us/en/icons/deepblue/ [Pristupljeno:1.9.2021.]

[8] DataDrivenInvestor (2018). Deep learning URL: https://medium.datadriveninvestor.com/deep-learning-2025e8c4a50 [Pristupljeno 16.6.2021.]

2.1. Definicija i opseg umjetne inteligencije

Prema Larryju Hauseru (2020)[9], umjetna inteligencija široka je grana računalne znanosti koja se bavi izgradnjom pametnih strojeva sposobnih za izvršavanje zadataka koji obično zahtijevaju ljudsku inteligenciju. Omogućuje strojevima učenje iz iskustva, prilagođavanje novim ulazima i izvršavanje zadataka sličnih onima koje izvršava čovjek. Većina primjera umjetne inteligencije koji su danas aktualni, od računala za igranje šaha do autonomnih vozila, oslanjaju se uvelike na duboko učenje i obradu prirodnog jezika (eng. Natural Language Processing), kroz računalnu analizu teksta u različitim područjima, kao što su npr. u ekstrakciji informacija i dubinskoj analizi tekstova financijskih institucija i banaka (Pejić Bach i sur., 2019[10]), analizi informacija na web stranicama (Seljan i sur., 2020[11], Pejić Bach i sur., 2019[12]), u analizi dokumenata iz područja farmacije (Seljan i sur., 2017[13]), medicine (Selja i sur., 2014[14]), prava (Gašpar i sur., 2021[15]), itd. Korištenjem ovih tehnologija računala se mogu osposobiti za izvršavanje određenih zadataka obrađivanjem velikih količina podataka i prepoznavanjem obrazaca u podacima.

[9] Hauser, L. (2020). Artificial Intelligence, Internet Encyclopedia of Philosophy, URL: https://iep.utm.edu/art-inte/#H6 [Prostupljeno: 31.8.2021.]

[10] Pejić Bach, M.; Krstić, Ž.; Seljan, S. (2019). Big data text mining in the financial sector. Expert systems in finance: smart financial applications in big data environments. Metawa, N.; Elhoseny, M.; Hassanien, A. E.; Hassan, M. K. (ur.). London: Routledge, 80-96 doi:10.4324/9780429024061

[11] Seljan, S.; Baretić, M.; Seljan, M.; Pejić Bach, M. (2020). Information assessment of hospital websites in Croatia: how to develop accountability standards? *International journal of health planning and management*, 35 (4), 4; 970-971 doi:10.1002/hpm.2975

[12] Pejić Bach, M.; Seljan, S.; Jaković, B.; Buljan, A.; Zoroja, J. (2019). Hospital websites: from the information repository to interactive channel. *Procedia computer science*, 164 (2019), 64-71 doi:10.1016/j.procs.2019.12.155

[13] Seljan, S.; Dunđer, I.; Stančić, H. (2017). Extracting terminology by language independent methods. *Translation studies and translation practice : proceedings of the 2nd International TRANSLATA Conference* 2014. Part 1 / Zybatow, Lew N. ; Stauder, Andy ; Ustaszewski, Michael (ur.). Frankfurt am Main: Peter Lang, 141-147.

[14] Seljan, S.; Baretić, M.; Kučiš, V. (2014). Information Retrieval and Terminology Extraction In Online Resources for Patients with Diabetes. *Collegium antropologicum*, 38 (2014), 2; 705-710

[15] Gašpar, A., Seljan, S., Kučiš, V. (2021). Consistency of Translated Terminology Measured by the Herfindahl-Hirshman Index (HHI), in print.

Journal of Information Technology & Software Engineering (2011)[16] iznosi u svojoj online verziji časopisa da je umjetna inteligencija osnovana kao akademska disciplina 1955. godine, te da je imala turbulentna razdoblja popraćena pozitivnim, ali kasnije i negativnim razdobljima, te se jedno razdoblje posebno pamti te ističe od ostalih, a to je razdoblje koje se zove „UI zima“ (poznatije pod nazivom eng. *AI winter*) koje je rezultiralo ogromnim gubitkom financiranja, praćenim novim pristupima, uspjehom i obnovljenim financiranjem.

„Ono što su istraživači 60-ih i 70-ih godina pokušavali napraviti je neka vrsta monolitnog entiteta koji posjeduje vlastite module za rasuđivanje određenih ulaznih podataka i razvoja hipoteza koje su zahtijevale sve više i više apstrakcije, pa su time postajale sve udaljenije od temeljnog ulaza. Takav je pristup doveo do spektakularnog neuspjeha i dijelom postao uzrokom zime umjetne inteligencije. Taj period, a riječ je o 80-im godinama dvadesetog stoljeća, označava oskudno financiranje istraživanja i maleni napredak u umjetnoj inteligenciji. Nakon toga slijedi uspon ekspertnih sustava – odnosno tehnologija umjetne inteligencije koje su obilježene specifičnim ciljevima realiziranih sintezom velikih količina podataka iz određenog područja ljudske djelatnosti, kao što je računalni šahovski šampion Deep Blue ili MYCIN program za medicinsku dijagnostiku“ (Kovač, 2015:5)[17].

Godine 2010. Googleova DeepMind Technologies kompanija[18] razvila je program umjetne inteligencije *AlphaGo*. *AlphaGo* prvi je računalni program koji je pobijedio profesionalnog igrača Goa 2015. godine, prvi koji je pobijedio svjetskog prvaka Goa 2017. godine i vjerojatno je najjači igrač Go-a u povijesti. Ovim postignućem, umjetna inteligencija privukla je brojne svjetske medije i stekla ogromnu pažnju. Istraživanja umjetne inteligencije podijeljena su na potpolja. Ta se potpolja temelje na tehničkim razmatranjima, kao što su određeni ciljevi (npr. robotika ili strojno učenje), upotreba određenih alata (logika ili umjetne neuronske mreže), itd. Potpolja su se također temeljila na socijalnim čimbenicima (određene institucije ili rad određenih istraživača).

---

[16] Journal of Information Technology & Software Engineering (2011). Artificial-Intelligence-open-acces URL: https://www.longdom.org/peer-reviewed-journals/artificialintelligenceopenaccess-36559.html [Pristupljeno: 31.8.2021.]

[17] Kovač, L. (2015). Umjetna inteligencija danas, Sveučilište u Rijeci, Filozofski fakultet u Rijeci, diplomski rad, 82 str.

[18] DeepMind, *AlphaGo* URL: https://deepmind.com/research/case-studies/alphago-the-story-so-far [Pristupljeno: 31.8.2021]

„Dva su osnovna cilja kojima teži većina istraživanja umjetne inteligencije. Prvi, najvažniji cilj, je izgradnja inteligentnih strojeva. Drugi cilj je shvaćanje prirode inteligencije ili onoga što psiholozi nazivaju g-faktor u testovima inteligencije (pokušaj da se izmjeri generalna inteligencija koja se prostire kroz različite domene ljudskog djelovanja). Oba cilja imaju u svojoj biti potrebu za definiranjem pojma inteligencije" (Kovač, 2015:3[19]).

Umjetna inteligencija djeluje kombinirajući velike količine podataka s brzom, iterativnom obradom i inteligentnim algoritmima, omogućavajući softveru da automatski uči iz uzoraka ili značajki u podacima. Prema Tyagi (2021)[20] umjetna inteligencija široko je područje proučavanja koje uključuje brojne teorije, metode i tehnologije, kao i sljedeća glavna potpolja:

- **Strojno učenje** (eng. *machine learning*) automatizira izradu analitičkih modela. Koristi metode iz statistike, istraživanja operacija i fizike kako bi pronašao skrivene uvide u podacima, a da nije izričito programirano gdje tražiti ili što zaključiti.
- **Neuronska mreža** (eng. *neural network*) vrsta je strojnog učenja koja se sastoji od međusobno povezanih jedinica (poput neurona) koje obrađuju informacije reagirajući na vanjske ulaze, prenoseći informacije između svake jedinice. Proces zahtijeva više prolaza podataka kako bi se pronašle veze i izvuklo značenje iz nedefiniranih podataka.
- **Duboko učenje** (eng. *deep learning*) koristi ogromne neuronske mreže s mnogo slojeva procesorskih jedinica, iskorištavajući napredak u računalnoj snazi i poboljšane tehnike treninga za učenje složenih obrazaca u velikim količinama podataka. Uobičajene aplikacije uključuju prepoznavanje slike i govora.
- **Kognitivno računanje** (eng. *cognitive computing*) je potpolje umjetne inteligencije koje teži prirodnoj, ljudskoj interakciji sa strojevima. Korištenjem umjetne inteligencije i kognitivnog računanja, krajnji je cilj da stroj simulira ljudske procese kroz sposobnost interpretacije slika i govora - a zatim koherentno govori kao odgovor.

[19] Kovač, L. (2015). Umjetna inteligencija danas, Sveučilište u Rijeci, Filozofski fakultet u Rijeci, diplomski rad, 82 str.

[20] Tyagi, N. (2021). 6 Major Branches of Artificial Intelligence (AI), Artificial Intelligence, analyticSteps URL: https://www.analyticssteps.com/blogs/6-major-branches-artificial-intelligence-ai [Pristupljeno: 31.8.2021.]

- **Računalni vid** (eng. *computer vision*) oslanja se na prepoznavanje uzoraka i duboko učenje, tj. na prepoznavanja onoga što je na slici ili videozapisu. Kada strojevi mogu obrađivati, analizirati i razumjeti slike, mogu snimati slike ili videozapise u stvarnom vremenu i tumačiti svoju okolinu.
- **Obrada prirodnog jezika** (eng. *natural language processing*) sposobnost je računala da analizira, razumije i generira ljudski jezik, uključujući i govor. Sljedeća faza obrade prirodnog jezika je interakcija u prirodnom jeziku, koja omogućava ljudima da komuniciraju s računalima koristeći uobičajeni svakodnevni jezik za izvršavanje zadataka.

3. Strojno učenje

Danas se lako mogu pronaći primjeri gdje se pojmovi strojno učenje i duboko učenje koriste naizmjenično u medijima. Međutim, stručnjaci ih uglavnom razlikuju, te da bi se ovo područje uistinu moglo kvalitetno proučavati, važno je da ih i pojedinci razumiju i razlikuju kao i stručnjaci. Umjetna inteligencija vrlo je česta riječ koja može podrazumijevati mnogo različitih stvari. Može ukazivati na bilo koji oblik tehnologije koji uključuje neke inteligentne aspekte, a ne na točno određeno tehnološko područje. Suprotno tome, strojno učenje odnosi se na određeno područje. Drugim riječima, strojnim učenjem označavamo određenu tehnološku skupinu umjetne inteligencije. Samo strojno učenje uključuje i mnoge tehnologije. Jedno od njih je duboko učenje. Činjenica da je duboko učenje vrsta strojnog učenja te da je ono proizašlo iz njega ključno; stoga je potrebno proći kroz pregled povezanosti i razvoja umjetne inteligencije, strojnog učenja i dubokog učenja. Duboko učenje nedavno je u središtu pozornosti jer je vješto riješilo neke probleme koji su doveli u pitanje umjetnu inteligenciju. Njegova je izvedba zasigurno iznimna na mnogim poljima. Međutim, suočava se i s ograničenjima. Ograničenja dubokog učenja proizlaze iz njegovih temeljnih koncepata koji su naslijeđeni od njegovog prethodnika - strojnog učenja (Stewart, 2019)[21]. Kao vrsta strojnog učenja, duboko učenje ne može izbjeći temeljne probleme s kojima se strojno učenje suočava. Zbog toga bitno je dati pregled strojnog učenja prije rasprave o konceptu dubokog učenja. Prema Oppermannu (2019)[22] duboko učenje i strojno učenje razlikuju se u načinu na koji algoritam uči. Duboko učenje automatizira veći dio procesa izdvajanjem značajki, uklanjajući neke ručne ljudske intervencije i omogućujući upotrebu većih skupova podataka, dok strojno učenje više ovisi o ljudskoj intervenciji za učenje. Ljudski stručnjaci određuju skup značajki kako bi razumjeli razlike između unosa podataka, te strojno učenje obično zahtijeva strukturiranije podatke za učenje.

Najjednostavnije rečeno, strojno učenje je proučavanje računalnih algoritama koji se automatski poboljšavaju iskustvom i upotrebom podataka. Prema Bheemaiah, Esposito i Tse

[21] Stewart, M. (2019). The Limitations of Machine Learning, TowardsDataScience URL: https://towardsdatascience.com/the-limitations-of-machine-learning-a00e0c3040c6 [Pristupljeno: 3.9.2021.]

[22] Oppermann, A. (2019). Artificial Intelligence vs. Machine Learning vs. Deep Learning, TowardsDataScience URL: https://towardsdatascience.com/artificial-intelligence-vs-machine-learning-vs-deep-learning-2210ba8cc4ac [Pristupljeno: 3.9.2021.]

(2017)[23] umjesto unaprijed odabira modela i umetanja podataka u njega, u strojnom učenju podaci određuju koja analitička tehnika treba biti odabrana za najbolje izvršavanje trenutnog zadatka. Drugim riječima, računalo koristi podatke koje ima za odabir i obuku algoritma. Stoga algoritam nije statičan. Analizira podatke kojima je izložen, odlučuje o najboljem načinu djelovanja, a zatim djeluje. U biti, ono uči iz podataka i pritom znanje odnosno iskustvo može izvući iz podataka. Ova metoda učenja temelji se na ponavljanju. Algoritam nije ništa drugo do skup uputa koje računalo koristi za pretvaranje ulaza u određeni izlaz. Stoga je u strojnom učenju aspekt učenja je samo algoritam koji uvijek iznova ponavlja svoju operaciju izvođenja i vrši male prilagodbe dok se ne ispuni određeni skup uvjeta. Lakmus test algoritma za učenje je kada može predvidjeti kada će mu se dati novi podaci o kojima prethodno nije bio obučen.

Algoritmi strojnog učenja grade model zasnovan na uzorcima podataka, poznatijima kao podaci za obuku, kako bi donijeli predviđanja ili odluke, a da to nisu izričito programirani. Algoritmi strojnog učenja koriste se u širokom spektru aplikacija, poput medicine, filtriranja e-pošte, prepoznavanja govora i računalnog vida, gdje je teško ili nemoguće razviti konvencionalne algoritme za izvršavanje potrebnih zadataka.

3.1. Vrste strojnog učenja

„Strojno učenje se bazira na dizajniranju algoritama koji omogućavaju učenje. Učenje nije stvaranje svjesnosti nego je stvar pronalaska statističkih pravilnosti, podudarnosti i uzoraka među podacima. Prema Rokadu (2019)[24] strojno učenje je podijeljeno prema željenom izlazu algoritma, pa se stoga može podijeliti na:

- Nadzirano učenje (eng. *supervised learning*) - algoritam kreira funkciju koja preslikava ulaze (input) na željene izlaze (output). Rješavaju se problemi klasifikacije, potrebno je naučiti (predvidjeti ponašanje) funkciju koja

[23]Bheemaiah, K., Esposito M., Tse, T. (2017). What is machine learning? The Conversation URL: https://theconversation.com/what-is-machine-learning-76759 [Pristupljeno: 3.9.2021.]

[24]Rokad, B. (2019). Machine Learning Approaches and Its Applications, DataDrivenInvestor URL: https://medium.datadriveninvestor.com/machine-learning-approaches-and-its-applications-7bfbe782f4a8 [Pristupljeno: 3.9.2021.]

preslikava vektore u nekoliko klasa tako što prati, odnosno pregledava rad nekoliko input-output primjera te iste funkcije.

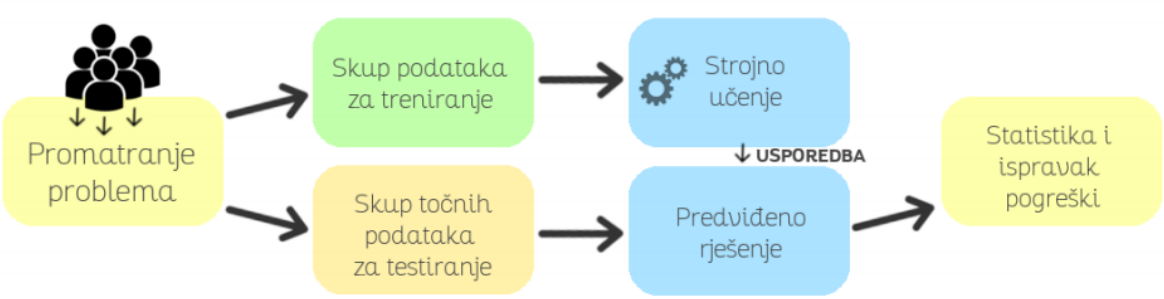
- Nenadzirano učenje (eng. *unsupervised learning*) - gdje se modelira set ulaza, a da nema početnih primjera, što znači da algoritam sam mora naučiti.
- Polunadzirano učenje (eng. *semi-supervised learning*) - kombinira se nadzirano i nenadzirano učenje kako bi se stvorila prikladna funkcija ili klasifikator.
- Podržano učenje (eng. *reinforcement learning*) - algoritam uči politiku ponašanja kada mu se prezentira zapažanje o okolini ili svijetu. Svaka akcija ima odražaj na okoliš, te isto tako okoliš povratno reagira, na osnovu čega algoritam uči“ (Subotić, 2020:10[25]).

Slika 2. Glavna podjela strojnog učenja (Izvor: Josipović, 2019) [26]

[25] Subotić, D. (2020). Primjena dubokog učenja, Strojarski fakultet Slavonski Brod, diplomski rad, 57 str.

[26] Josipović, M. (2019). Postupci strojnog učenja za popravljanje točnosti klasifikacije manjinskih klasa kod nebalansiranih skupova podataka, Sveučilište u Zagrebu, Fakultet elektrotehike i računarstva, završni rad, 24 str.

3.1.1. Nadzirano učenje (učenje s učiteljem)



Slika 3. Nadzirano učenje (Izvor: Tikvica, 2019) [27]

Nadzirani algoritmi strojnog učenja mogu primijeniti naučeno u prošlosti na nove podatke koristeći primjere s oznakom za predviđanje budućih događaja. Polazeći od analize poznatog skupa podataka za obuku, algoritam učenja proizvodi zaključenu funkciju za predviđanje izlaznih vrijednosti. Sustav je u stanju osigurati ciljeve za svaki novi unos nakon dovoljne obuke. Algoritam učenja također može usporediti svoj izlaz s ispravnim, predviđenim izlazom i pronaći pogreške kako bi prema tome promijenio model (Expert.ai Team, 2020)[28].

"Algoritmi nadziranog učenja izgrađuju model na temelju ulaznih ali i poznatih iz lažnih podataka, pri čemu skup podataka koji sadrži ulazne i izlazne podatke nazivamo podacima za treniranje. Nakon učenja na skupu podataka za treniranje model je sposoban s određenom točnošću predvidjeti rezultate obrade podataka koji nisu bili među podatcima za treniranje. Klasifikacija i regresija su dvije vrste nadziranog učenja (Khalilan i Shiva, 2019)[29], a razlikuju se po obliku izlaznih podataka, kod klasifikacije izlaz je limitirani skup vrijednosti dok je izlaz regresijskih algoritama kontinuirana vrijednost. Klasifikacijom se rješavaju problemi poput označavanja neželjene elektroničke pošte, prepoznavanja objekata kod računalnog vida te raspoznavanja govora i rukom pisanih znakova dok se regresija može koristiti za predviđanje cijena nekretnina ili cijena dionica, predviđanje opterećenja na

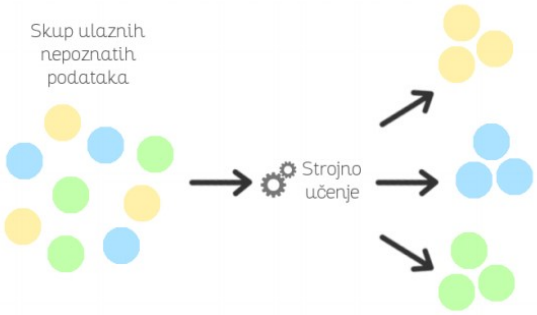
[27] Tikvica, A. (2019). Interoperabilnost servisa strojnog učenja različitih pružatelja usluga u oblacima, Sveučilište u Zagrebu, Fakultet organizacije i informatike, diplomski rad, 53 str.

[28] Expert.ai Team (2020). What is Machine Learning? A Definition., Expert.ai URL: https://www.expert.ai/blog/machine-learning-definition [Pristupljeno: 3.9.2021.]

[29] Khalilian, M., Shiva, H. (2019). Document classification methods.

sustave koji imaju više izvora opterećenja ili za predviđanje utjecaja reklamiranja na prodaju proizvoda" (Josipović, 2019:1:2[30]).

3.1.2. Nenadzirano učenje (učenje bez učitelja)



Slika 4. Nenadzirano učenje – grupiranje (Izvor: Tikvica, 2019) [31]

"Nenadzirano učenje obrađuje podatke koji nisu označeni, razvrstani ili kategorizirani i pronalazi pravilnosti u njima, a glavna primjena ove vrste učenja je u statistici kod procjena gustoća. Najčešća tehnika nenadziranog učenja je grupiranje koje nam omogućava da organiziramo skup podataka u podgrupe koje dijele određeni stupanj sličnosti ali su dovoljno drugačiji od podataka iz drugih grupa. Neki od problema koji se rješavaju grupiranjem su analiziranje sekvenci gena, prepoznavanje uzoraka i kompresija podataka" (Josipović, 2019:1:2[32]). U nenadziranom strojnom učenju, program traži uzorke u neoznačenim podacima. Strojno učenje bez nadzora može pronaći obrasce ili trendove koje ljudi eksplicitno ne traže. Na primjer, program za strojno učenje bez nadzora mogao bi pregledati podatke o online prodaji i identificirati različite vrste klijenata koji kupuju, ili se može koristiti za grupiranje vrste korisnika digitalnih usluga e-uprave (Seljan, i sur., 2020)[33].

[30] Josipović, M. (2019). Postupci strojnog učenja za popravljanje točnosti klasifikacije manjinskih klasa kod nebalansiranih skupova podataka, Sveučilište u Zagrebu, Fakultet elektrotehike i računarstva, završni rad, 24 str.

[31] Tikvica, A. (2019). Interoperabilnost servisa strojnog učenja različitih pružatelja usluga u oblacima, Sveučilište u Zagrebu, Fakultet organizacije i informatike, diplomski rad, 53 str.

[32] Josipović, M. (2019). Postupci strojnog učenja za popravljanje točnosti klasifikacije manjinskih klasa kod nebalansiranih skupova podataka,Sveučilište u Zagrebu, Fakultet elektrotehike i računarstva, završni rad, 24 str.

[33] Seljan, S.; Mikuloža, I.; Pejić Bach, M. (2020). e-Government in European countries: gender and ageing digital divide. Interdisciplinary Management Research XVI. Barković, Dražen... [et al] (ur.). Osijek: Josip Juraj Strossmayer University of Osijek, Faculty of Economics in Osijek, 2020. str. 1581-1602

Nenadzirano učenje ima prednost u mogućnosti rada s neoznačenim podacima. To znači da ljudski rad nije potreban da bi skup podataka bio strojno čitljiv, što omogućuje da program radi na mnogo većim skupovima podataka. U nadziranom učenju oznake omogućuju algoritmu da pronađe točnu prirodu odnosa između bilo koje dvije podatkovne točke. Međutim, učenje bez nadzora nema oznaka za rad, što rezultira stvaranjem skrivenih struktura. Odnos između podatkovnih točaka algoritam percipira na apstraktan način, bez unosa od ljudi. Stvaranje ovih skrivenih struktura čini algoritme učenja bez nadzora svestranim. Umjesto definirane i postavljene izjave problema, algoritmi za učenje bez nadzora mogu se prilagoditi podacima dinamičkom promjenom skrivenih struktura. To nudi više razvoja nakon implementacije od nadziranih algoritama za učenje (Anirudh, 2019)[34].

3.1.3. Polunadzirano učenje

U polunadziranom učenju ulazni skup podataka mješavina je označenih podataka i neoznačenih podataka. Obično skup podataka ima malu količinu označenih podataka i veliku količinu neoznačenih podataka. Matematički model koristi označene podatke za učenje strukture neoznačenih podataka i pokušava napraviti predviđanja. Polu-nadzirani problemi učenja također se mogu dalje grupirati u probleme klasifikacije i regresije (Rokad, 2019)[35].

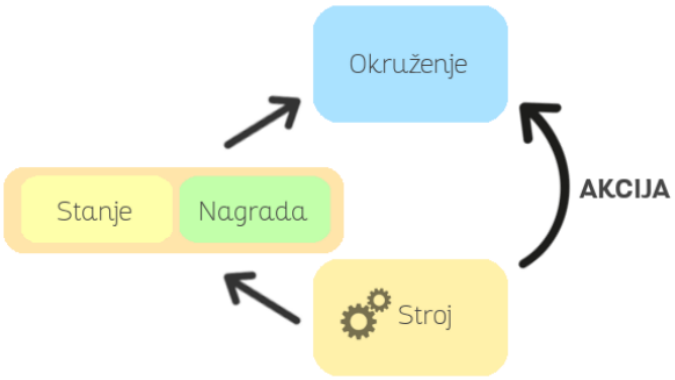
„Polu-nadzirano učenje je vrsta strojnog učenja koja koristi vrlo mali set podataka u obliku uređenih parova (y , x) = (ulazni podaci, izlazni podaci) i 8 veliki set ulaznih podataka bez pripadajuće kategorije. Tako, polu-nadzirano učenje spada između nadziranog učenja (s potpuno označenim podacima) i nenadziranog učenja (u potpunosti bez označenih ulaznih podataka). Polunadzirano učenje prvo koristi označene podatke za učenje, a potom u set za treniranje doda i neoznačene podatke. Ovaj tip učenja često se primjenjuje kada je teško klasificirati ulazne podatke. Istraživači strojnog učenja otkrili su da neoznačeni podaci, kada

[34] Anirudh, V. K. (2019). What Is Machine Learning: Definition, Types, Applications and Examples, Toolbox URL: https://www.toolbox.com/tech/artificial-intelligence/tech-101/what-is-machine-learning-definition-types-applications-and-examples [Pristupljeno: 3.9.2021.]

[35] Rokad, B. (2019). Machine Learning Approaches and Its Applications, DataDrivenInvestor URL: https://medium.datadriveninvestor.com/machine-learning-approaches-and-its-applications-7bfbe782f4a8 [Pristupljeno: 3.9.2021.]

se koriste zajedno sa malom dozom označenih podataka, mogu proizvesti mnogo preciznije učenje“ (Relić, 2019)[36].

3.1.4. Podržano učenje



Slika 5. Podržano učenje (Izvor: Tikvica, 2019) [37]

“Podržano učenje se temelji na tome da se agenta koji rješava određeni problem nagradi ako povuče dobar potez (npr. tijekom igranja šaha). Agent nastoji maksimizirati svoje nagrade i tako "uči" snalaziti se u određenoj okolini pomoću prošlih iskustava” (Josipović, 2019:1:2[38]).

Podržano strojno učenje metoda je učenja koja stupa u interakciju sa svojim okruženjem proizvodeći radnje i otkrivajući pogreške ili nagrade. Pretraživanje pokušajima i pogreškama te odgođena nagrada najvažnije su karakteristike podržanog učenja. Ova metoda omogućuje strojevima i softverskim agentima da automatski odrede idealno ponašanje u određenom kontekstu kako bi povećali njegove performanse. Jednostavna povratna informacija o nagradi potrebna je kako bi agent saznao koja je radnja najbolja; to je poznato kao signal pojačanja (Expert.ai Team, 2020)[39].

---

[36] Relić, B. (2019). Klasifikacija očitanja koristeći metode dubokog učenja, Sveučilište u Zagrebu, Fakultet elektrotehnike i računarstva, završni rad, 26 str.

[37] Tikvica, A. (2019). Interoperabilnost servisa strojnog učenja različitih pružatelja usluga u oblacima, Sveučilište u Zagrebu, Fakultet organizacije i informatike, diplomski rad, 53 str.

[38] Josipović, M. (2019). Postupci strojnog učenja za popravljanje točnosti klasifikacije manjinskih klasa kod nebalansiranih skupova podataka, Sveučilište u Zagrebu, Fakultet elektrotehike i računarstva, završni rad, 24 str.

[39] Expert.ai Team (2020). What is Machine Learning? A Definition., Expert.ai URL: https://www.expert.ai/blog/machine-learning-definition [Pristupljeno: 3.9.2021.]

4. Duboko učenje

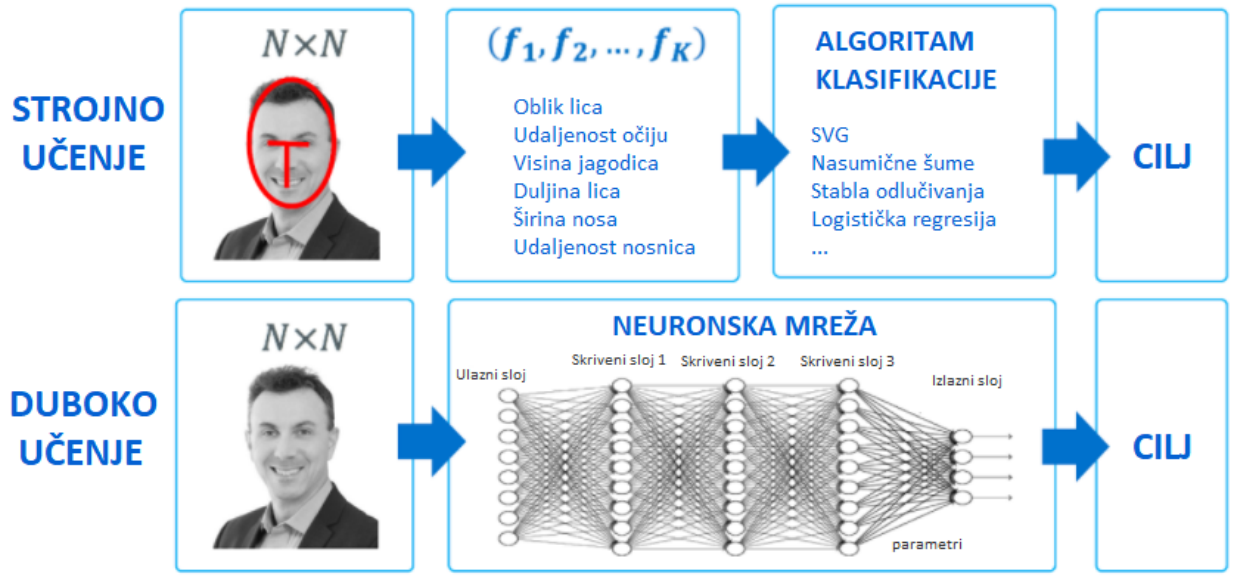
Duboko učenje proizašlo je iz istraživanja umjetne inteligencije i strojnog učenja.

Prema Bengio, Courville i Goodfellow (2016)[40] duboko učenje oblik je strojnog učenja koji omogućuje računalima da uče iz iskustva i razumiju svijet u smislu hijerarhije pojmova. Budući da računalo skuplja znanje iz iskustva, nema potrebe za ljudskom intervencijom jer algoritmu ne treba govoriti o važnim značajkama. Umjesto toga, sposoban je sam otkriti značajke iz podataka pomoću neuronske mreže. Ime je nadahnuto matematičkim objektom koji se naziva umjetni neuron koji "puca" ako kombinacija ulaza premaši neki prag, baš kao što to čini neuron u mozgu. Umjetni neuroni mogu se složiti u slojeve, a duboko učenje uključuje duboku neuronsku mrežu koja ima mnogo slojeva umjetnih neurona. Umjetni neuroni u dubokoj neuronskoj mreži međusobno su povezani snažnim vezama. Proces određivanja snaga veza naziva se treniranje duboke neuronske mreže.

Slika 6 prikazuje razlike u procesu učenja između strojnog učenja i dubokog učenja koje je proizašlo iz njega. Na primjeru prepoznavanja lica, ako želimo pomoću modela strojnog učenja utvrditi čije je lice prikazano na slici, prvo se moraju identificirati jedinstvene značajke ili obilježja lica (oblik lica, veličina, oblik očiju, usta itd.), te izdvojiti značajke i predati algoritmu kao ulazne podatke. Tako algoritam izvršava klasifikaciju uz pomoć nadzora. U slučaju modela dubokog učenja, korak izdvajanja značajki potpuno je nepotreban. Model će sam pomoću neuronske mreže prepoznati ove jedinstvene karakteristike lica i dati točan rezultat bez ljudskog interveniranja (Dwivedi, 2018)[41].

[40] Bengio, Y., Courville, A., Goodfellow, I. (2016). Deep learning, Cambridge MA: *MIT Press*, 785 str.

[41] Dwivedi, D. (2018). Face Detection For Beginners, TowardsDataScience URL: https://towardsdatascience.com/face-detection-for-beginners-e58e8f21aad9 [Pristupljeno: 3.9.2021.]



Slika 6. Razlika prepoznavanja lica između dubokog i strojnog učenja (Izvor: Robins, 2020)[42]

Kelleher (2019)[43] za duboko učenje kaže da je potpolje umjetne inteligencije koje se usredotočuje na stvaranje velikih modela neuronskih mreža koji su sposobni donijeti točne odluke na temelju podataka. Duboko učenje posebno je pogodno za kontekst u kojem su podaci složeni i gdje su dostupni veliki skupovi podataka. Danas većina internetskih tvrtki i vrhunskih potrošačkih tehnologija koristi duboko učenje. Između ostalog, *Facebook* koristi duboko učenje za analizu teksta u internetskim razgovorima, rade se različite analize tekstova na internetu u različite svrhe, npr. financijske analize (Pejić Bach, M. i sur., 2019)[44]. *Google, Baidu* i *Microsoft* koriste duboko učenje za pretraživanje slika, kao i za strojno prevođenje (Seljan i Dunđer, 2015)[45]. Svi moderni pametni telefoni imaju sustave za duboko učenje; na primjer, duboko učenje sada je standardna tehnologija za prepoznavanje govora i za otkrivanje lica na digitalnim fotoaparatima. U zdravstvenom se sektoru duboko učenje koristi za obradu medicinskih slika (rendgenske zrake ili X-zrake, CT (kompjuterizirana tomografija) i MRI (magnetska rezonanca) snimke) i dijagnosticiranje zdravstvenih stanja.

[42] Robins, M. (2020). The Difference Between Artificial Intelligence, Machine Learning and Deep Learning, Intel, URL: https://www.intel.la/content/www/xl/es/artificial-intelligence/posts/difference-between-ai-machine-learning-deep-learning.html [Pristupljeno 19.6.2021.]

[43] Kelleher, J. D. (2019). Deep Learning, London*, The Massachusetts Institute of Technology: The MIT Press*, 296 str.

[44] Pejić Bach, M., Krstić, Ž., Seljan, S. (2019). Big data text mining in the financial sector. Expert systems in finance: smart financial applications in big data environments. Metawa, N., Elhoseny, M., Hassanien, A. E., Hassan, M. K. (ur.). London: Routledge, 80-96 doi:10.4324/9780429024061

Duboko učenje također je srž samovozećih automobila, gdje se koristi za lokalizaciju i mapiranje, planiranje pokreta i upravljanje, percepciju okoliša, kao i za praćenje stanja vozača (Gupta, Anpalagan, Guan, Shaharyar Khwaja 2021.)[46].

4.1. Neuronske mreže

Ujević Andrijić (2019)[47] u članku "Umjetne neuronske mreže" objašnjava povezanost umjetne inteligencije s ljudskim mozgom, odnosno ljudskom inteligencijom te iznosi da je ono povezano s računalnom inteligencijom s nekoliko karakteristika koje su im međusobno zajedničke. Uspoređuje ih s nekoliko sličnih obilježja, za ljudsku inteligenciju iznosi karakteristike poput paralelnog odvijanja više operacija, sposobnosti učenja, sposobnosti generaliziranja, sposobnosti prilagođavanja, suvislo postupanje s informacijama, tolerancija na pogreške i nepotpune informacije, dok za umjetnu računalnu inteligenciju iznosi karakteristike poput brze provedbe numeričkih složenih proračuna te rad s velikom količinom podataka. Smatra da su upravo ta obilježja ono što je dovelo do ideje stvaranja umjetnih neuronskih mreža koje bi funkcionirale jednako ili bar, za sad približno brzo poput bioloških. Upravo zbog toga što su umjetni neuroni proizvod bioloških, ključno je razumjeti način na koji ljudski funkcioniraju da bi se umjetni mogli dalje istraživati i razvijati (Matić, 2014)[48].

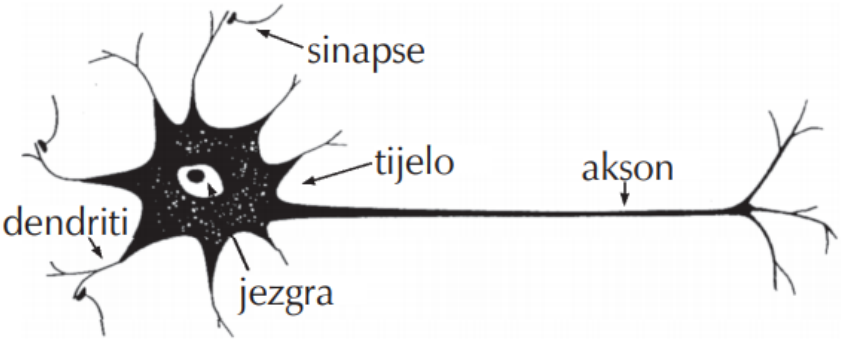
---

[45] Seljan, S.; Dunđer, I. Machine Translation and Automatic Evaluation of English/Russian-Croatian. Proceedings of the International Conference "Corpus Linguistics - 2015". Zakharov, V. P. ; Mitrofanova, O. A. ; Khokhlova, M. V. (ur.). St. Petersburg, Rusija: St. Petersburg State University, 72-79.

[46] Gupta, A., Anpalagan, A., Guan, L., Shaharyar Khwaja, A. (2021). Deep learning for object detection and scene perception in self-driving cars: Survey, challenges, and open issues, Volume 10, 100057, ISSN 2590-0056 URL: https://www.sciencedirect.com/science/article/pii/S2590005621000059#! [Pristupljeno: 3.9.2021.]

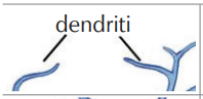
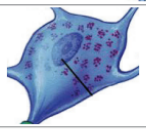
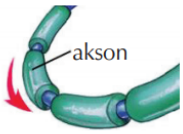
[47] Ujević, Andrijić, Ž., (2019). Umjetne neuronske mreže*, Osvježimo znanje*, Kem. Ind. 68 (5-6) 219–220 str.

[48] Matić, P., (2014). Kratkoročno predviđanje hidrološkog dotoka pomoću umjetne neuronske mreže, Sveučilište u Splitu; Fakultet elektrotehnike, strojarstva i brodogradnje, doktorska disertacija, 137 str.



Slika 7. Građa biološkog neurona (Izvor: Ujević Andrijić, 2019) [49]

Nadalje Ujević Andrijić (2019)[50] iznosi da se svaki neuron sastoji od tri dijela, tijela stanice koje sadrži jezgru s informacijama o nasljednim značajkama, dendrita koji prenose signale ili impulse s drugih neurona, te sadrže na krajevima sinapse i aksona, dugih niti koje prenose signal do drugih neurona pri čemu se grana u vlakna. Sinapse koje su na završetcima aksona prethodnog neurona i dendrita sljedećeg neurona oslobađaju neurotransmitere (materijal potreban za prijenos signala) pri čemu se odvija reakcija i impulsi se prenose preko sinapsa s jednog na drugi neuron. Tablica 1. prikazuje sličnosti građe i funkcija umjetnih i bioloških neurona.

Biološki neuron		**Umjetni neuron**
	Prima ulazni signal putem dendrida (sinaptičke veze)	Prima ulaze (*i*) koji su određeni težinskim koeficijentima (*w*)
	Obrada signala u somi	Obrada ulaza, unutarnji prag – bias (*b*)
	Pretvara obrađeni ulaz u izlaz putem aksona	Pretvara ulaze u izlaz (prijenosna funkcija)
	Šalje informacije putem sinapsi do svih neurona s kojima je neuron povezan	Šalje informaciju prema izlazu i sljedećim neuronima

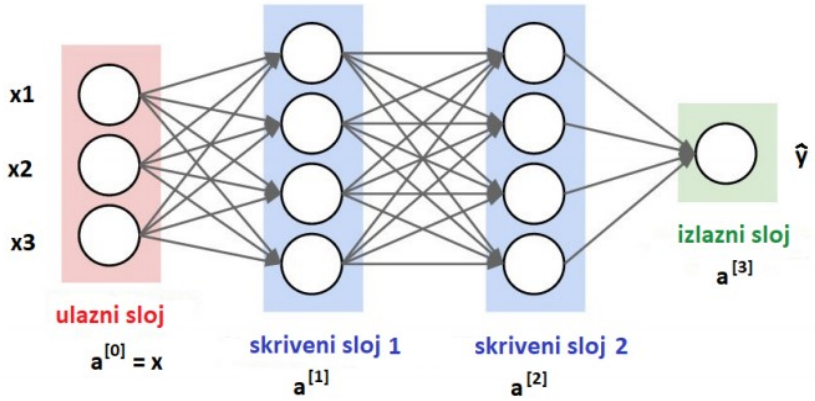
Slika 8. Usporedba biološkog i umjetnog neurona (Izvor: Ujević Andrijić, 2019)[51]

[49] Ujević, Andrijić, Ž., (2019). Umjetne neuronske mreže, *Osvježimo znanje*, Kem. Ind. 68 (5-6) 219–220 str.

[50] Ibid

[51] Ujević, Andrijić, Ž., (2019). Umjetne neuronske mreže, *Osvježimo znanje*, Kem. Ind. 68 (5-6) 219–220 str.

Subotić navodi (2020)[52] da se neuronske mreže sastoje od procesnih jedinica (neurona) koji se grupiraju u slojeve i povezani su direktno međusobnim vezama, te se težina tih veza mijenja prilikom učenja. Iznosi da duboke neuronske mreže imaju dva ili više skrivenih slojeva, kao što je prikazano na slici 6, te objašnjava „ulazni sloj prima ulazne podatke iz okoline i prosljeđuje ih u prvi skriveni sloj. Informacije putuju i procesuiraju se kroz slojeve, te dolaze do izlaznog sloja. Uspoređuje se dobiveni rezultati sa željenima, te ovisno o veličini greške, prilikom povratka informacija natrag kroz mrežu, podešavaju se težine veza. Ovaj proces se ponavlja iterativno sve dok veličina greške ne bude dovoljno mala, odnosno zadovoljavajuća. Takav proces podešavanja težina se naziva učenje“ (Subotić, 2020:34[53]).



Slika 9. Duboka neuronska mreža s dva skrivena sloja i izlaznim slojem s jednim neuronom (Izvor: Džomba, 2018) [54]

Prema Matić (2014)[55], najvažnija svojstva neuronskih mreža su paralelna obrada informacija (informacije spremljene u neuronsku mrežu raspodijeljene su na više jedinica), svojstvo redundantnosti, tj. svojstvo otpora na kvar (neuronska mreža raditi čak i ako se uništi jedan njen dio), učenje i adaptacija koje neuronsku mrežu čine sposobnom obrađivati neprecizne podatke u nestrukturiranom i neodređenom okruženju (navedeno možemo opisati kao svojstvo poopćivanja), viševarijabilni sustavi (neuronske mreže karakterizira laka primjena za modeliranje i upravljanje viševarijabilnim procesima), te univerzalni

[52] Subotić, D. (2020). Primjena dubokog učenja, Strojarski fakultet Slavonski Brod, diplomski rad, 57 str.

[53] Ibid

[54] Džomba, K. (2018). Konvolucijske neuronske mreže, Sveučilište u Zagrebu, Prirodoslovno-matematički fakultet, diplomski rad, 78 str.

[55] Matić, P., (2014). Kratkoročno predviđanje hidrološkog dotoka pomoću umjetne neuronske mreže, Sveučilište u Splitu; Fakultet elektrotehnike, strojarstva i brodogradnje, doktorska disertacija, 137 str.

aproksimator (neuronske mreže imaju mogućnost aproksimiranja proizvoljne kontinuirane nelinearne funkcije do željene točnosti).

4.1.1. Konvolucijske neuronske mreže

Konvolucijske neuronske mreže dio su umjetne neuronske mreže koje su specijalizirane za prepoznavanje (klasificiranje) slika, zvuka, govora i videozapisa. Osnovna pretpostavka iza konvolucijske neuronske mreže je korištenje unaprijed definiranih filtara za identificiranje uzoraka na rubovima slike, dijelovima predmeta i nadovezivanje na to znanje za otkrivanje cjelovitih objekata poput životinja, ljudi, automobila itd (Džomba, 2018)[56].

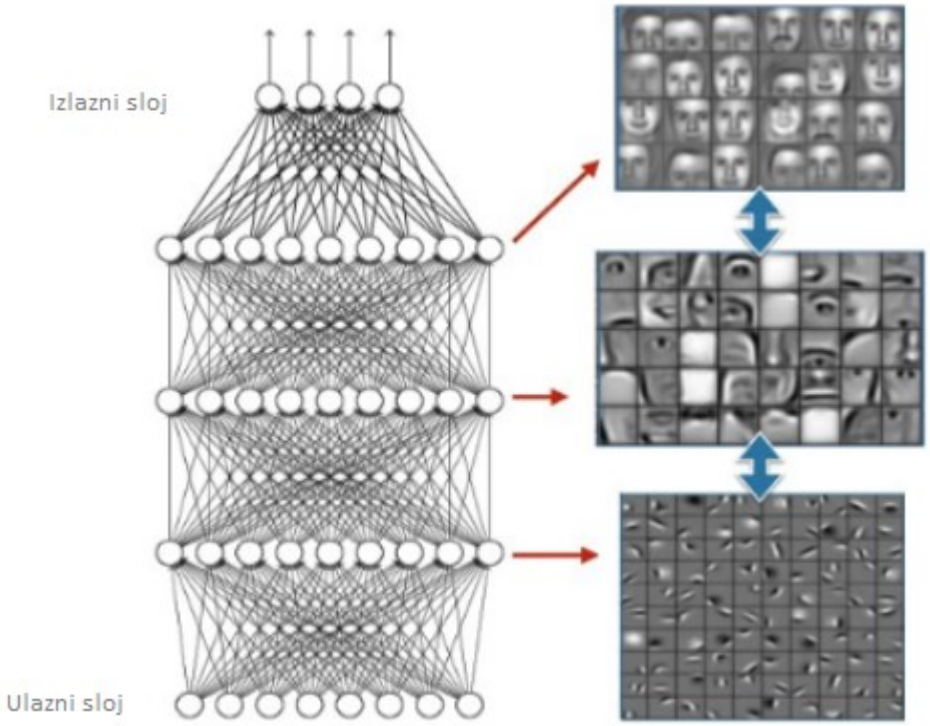
Kelleher (2019)[57] smatra da su konvolucijske neuronske mreže dizajnirane za zadatke prepoznavanja slika. Osnovni cilj dizajna neuronskih mreža u konvoluciji bio je stvoriti mrežu u kojoj bi neuroni u ranom sloju mreže izvlačili lokalne vizualne značajke, a neuroni u kasnijim slojevima kombinirali bi te značajke u značajke višeg reda. Lokalna vizualna značajka je značajka čiji je opseg ograničen na malu zakrpu, skup susjednih piksela, na slici. Na primjer, kada se primijene na zadatak prepoznavanja lica, neuroni u ranim slojevima neuronske mreže konvolucije nauče aktivirati kao odgovor na jednostavne lokalne značajke (poput linija pod određenim kutom ili segmenata krivulja), neurone dublje u mreži kombiniraju ove značajke niske razine u značajke koje predstavljaju dijelove tijela (poput očiju ili buke), a neuroni u završnim slojevima mreže kombiniraju aktivacije dijelova tijela kako bi mogli identificirati cijela lica na slici. Korištenjem ovog pristupa, temeljni zadatak prepoznavanja slike je učenje funkcija otkrivanja značajki koje mogu robusno identificirati prisutnost ili odsutnost lokalnih vizualnih obilježja na slici. Proces učenja funkcija u osnovi je neuronskih mreža, a postiže se učenjem odgovarajućeg skupa utega za veze u mreži. Konvolucijske neuronske mreže tako uče funkcije otkrivanja značajki za lokalne vizualne značajke. Međutim, Kelleher (2019)[58] također govori da je povezan izazov dizajniranje arhitekture mreže tako da će mreža prepoznati prisutnost lokalne vizualne značajke na slici,

[56] Džomba, K. (2018.) Konvolucijske neuronske mreže, Sveučilište u Zagrebu, Prirodoslovno-matematički fakultet, diplomski rad, 78 str.

[57] Kelleher, J. D. (2019.) Deep Learning, London, *The Massachusetts Institute of Technology: The MIT Press*, 296 str.

[58] Ibid.

bez obzira gdje se na slici pojavljuje. Drugim riječima, funkcije otkrivanja značajki moraju moći raditi na nepromjenjiv prijevod. Na primjer, sustav prepoznavanja lica trebao bi moći prepoznati oblik oka na slici bez obzira nalazi li se oko u središtu slike ili u gornjem desnom kutu slike. Ova potreba za neovisnošću pri prevođenju primarni je princip dizajna konvolucijskih neuronskih mreža za obradu slike.



Slika 10. Klasifikacija i identifikacija obilježja lica pomoću konvolucijske neuronske mreže (Izvor: cnnetss.com) [59]

Slika 10 prikazuje kako na svojoj najnižoj razini, slojevi neuronske mreže prvo nauče otkrivati rubove i uglove slike. Na sljedećem sloju uče otkrivati dijelove lica, a na posljednjem sloju otkrivaju cijelo lice.

[59] URL: www.cnnetss.com

4.1.2. Primjena umjetnih neuronskih mreža

„Primjenjuju se kod modeliranja procesa za predviđanje budućeg vladanja procesa i u sklopu naprednog vođenja procesa, te u dijagnostici stanja pri radu procesa i strojeva. U metodama strojnog učenja neuronske mreže se dosta primjenjuju za klasifikaciju: prepoznavanje slika, govora, prevođenje, analiza društvenih mreža, inteligentno internetsko pretraživanje, ciljani marketing i sl. I na kraju važno je naglasiti da je s obzirom na strukturu crne kutije (eng. *black-box*) neuronskih mreža izrazito važno razumjeti i interpretirati dobivene rezultate u skladu s domenskim znanjem“ (Ujević Andrijić, 2019:220[60]).

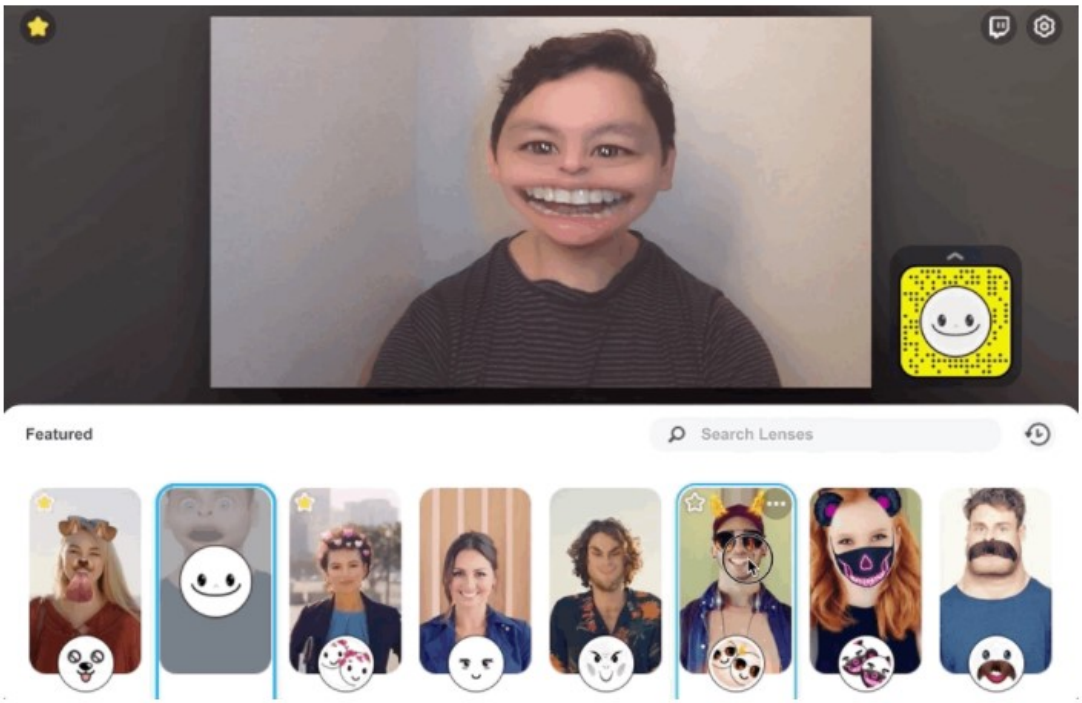
4.2. Aplikacije za prepoznavanje i korekciju lica

Duboko učenje nova je i najsuvremenija tehnologija koja se danas koristi za velike primjene. To je vrhunska tehnologija koja se koristi za mnoštvo različitih novih područja istraživanja. Primjenjuje se u vojsci, u kibernetičkoj zaštiti (eng. *cybersecurity*), u raznim kompjuterskim igricama i robotici, za autonomna vozila, za prepoznavanja lica, slika, govora, teksta, u detektiranju prevara, automatskom strojnom prevođenju, označavanju slika, itd. Kroz primjere *Snapchat*-a, *FaceApp*-a i *Luxand*-a, objasnit će se primjene dubokog učenja koje su najraširenije.

4.2.1. Snapchat

Jedna od najpopularnijih aplikacija koju koristi današnja mladež u svrhu zabave, slanja slika i korištenja različiti filtera koje na korisnikovo lice stavljaju mačje karakteristike poput ušiju, razne životinjske maske ili šminku ili u potpunosti preoblikuju lice je *Snapchat*.

[60] Ujević, Andrijić, Ž., (2019). Umjetne neuronske mreže, Osvježimo znanje, Kem. Ind. 68 (5-6) 219–220 str.

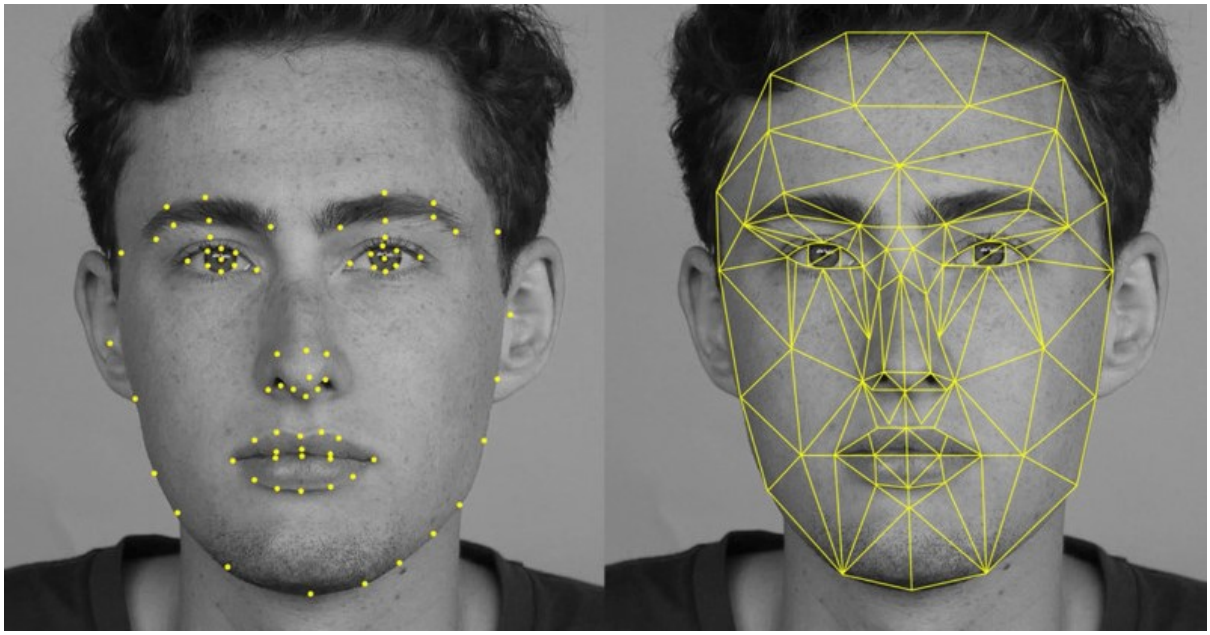


Slika 11. Snapchat filteri (Izvor: lensstudio.snapchat.com) [61]

Filteri aplikacije *Snapchat* koriste računalni vid kako bi uočili razna obilježja ljudskog lica (nos, usta, oči..). Da bi došao do te razine prepoznavanja, *Snapchat* je trenirao sustav koristeći stotine (vrlo vjerojatno tisuće) lica koja su ručno označena točkama kako bi se pokazalo gdje su granice usana, očiju, nosa i lica. Trenirana aplikacija tada uzima tu točkovnu masku i pomiče ju tako da odgovara pojedinačnom licu na temelju podataka koje dobiva s korisnikovog fotoaparata brzinom od 24 kadra u sekundi. Posljednji korak je stvaranje mreže od te točkaste maske, te se naposljetku ta mreža stavlja na lice korisnika i pomiče s korisnikom, te na njegovo lice aktivira filtere (PetaPixel, 2016)[62].

[61] URL: www.lensstudio.snapchat.com

[62]PetaPixel (2016). A Look at How Snapchat's Powerful Facial Recognition Tech Works URL: https://petapixel.com/2016/06/30/snapchats-powerful-facial-recognition-technology-works/ [Pristupljeno: 3.9.2021.]



Slika 12. Mreža koju Snapchat koristi u prepoznavanju obilježja lica (Izvor: PetaPixel.com) [63]

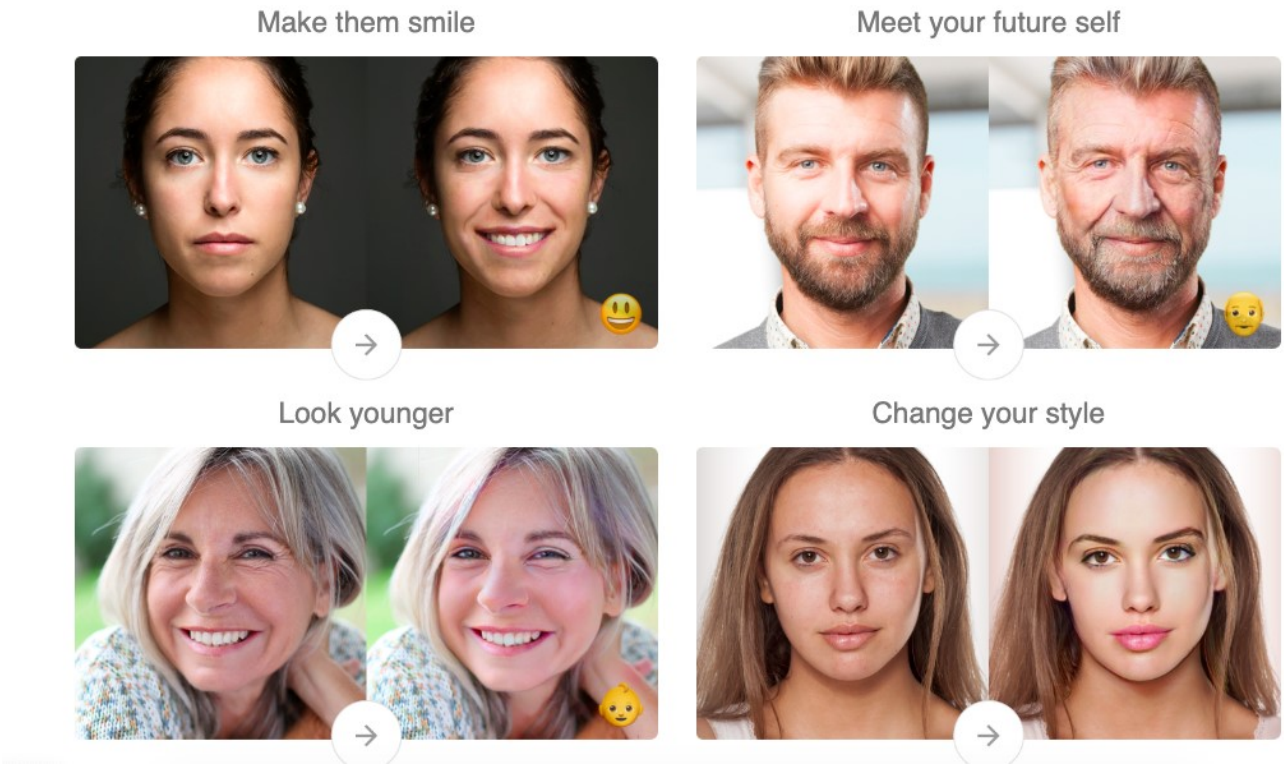
4.2.2. FaceApp

Aplikacija za manipulaciju slikama koja svojim korisnicima omogućuje izmjenu i transformaciju slika pomoću filtera naziva se *FaceApp*. Aplikacija funkcionira na tehnologiji prepoznavanja slika, koja je ključna za sustave prepoznavanja lica i koristi duboko učenje za prepoznavanje ključnih značajki (kapci, jagodične kosti, linija čeljusti, most na nosu, itd.) ljudskog lica kako bi stvorila te transformacije (Das, 2020)[64].

Kao i bilo koji drugi model strojnog učenja i ova aplikacija radi na uzorcima podataka koji se obično prikupljaju s mobitela korisnika. Jednom kada se prikupe uzorci podataka, koji uključuju slike korisnika, članova obitelji, prijatelja i svega ostalog, sustav zatim podatke daje dubokim neuronskim mrežama aplikacije što pomaže sustavu da nauči obilježja ljudskog lica. Za stvaranje takvih slika, aplikacija koristi duboke generativne konvolucijske neuronske mreže. Aplikacija tada licu na slici dodaje bore, pomlađuje ga, stavlja razne frizure, šminku, mijenja spol, itd.

[63] URL: www.petapixel.com

[64] Das, S. (2020). The AI Behind FaceApp, Analyticsindiamag URL: https://analyticsindiamag.com/the-ai-behind-faceapp/ [Pristupljeno: 3.9.2021.]



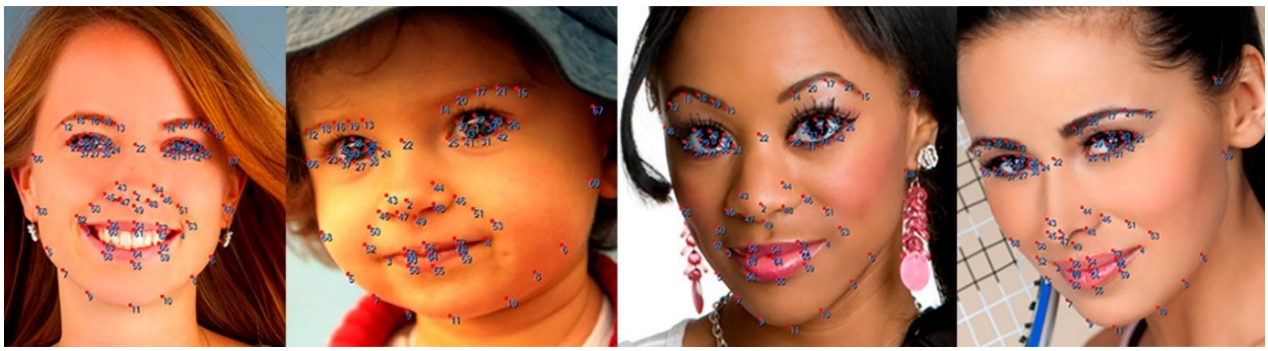
Slika 13. Razne mogućnosti manipulacije lika pomoću *FaceAppa* (Izvor: technologyreview.com) [65]

4.2.3. Luxand FaceSDK

Aplikacija *Luxand FaceSDK* koristi se za biometrijsku identifikaciju na temelju lica i prepoznavanje lica. Uglavnom se koristi za prepoznavanje i provjeru autentičnosti korisnika uz pomoć web-kamera, tražeći odgovarajuća lica u bazama podataka s fotografijama. Aplikacija također može automatski otkriti značajke lica u grafičkim uređivačima i koristiti fotografije i video tokove za otkrivanje lica u stvarnom vremenu. *Luxand FaceSDK* pruža nadzor, pomaže u kontroli sustava za evidentiranje radnog vremena i izgradnju sigurne identifikacije. *Luxand FaceSDK* koristi sofisticirane algoritme za brzo i pouzdano otkrivanje i praćenje značajki lica. SDK vraća koordinate 70 točaka značajki lica, uključujući oči, konture oka, obrve, konture usana, vrh nosa i tako dalje. Otkrivanje djeluje u stvarnom vremenu na

[65] URL: www.technologyreview.com

radnoj površini i mobilnom uređaju, što omogućuje izvođenje glatkog praćenja u stvarnom vremenu i transformacije crta lica u video zapisima uživo. Baza podataka *Luxand FaceSDK*-a može uspoređivati različita lica, vraćajući stupanj sličnosti. To omogućuje identificiranje ljudskih lica koja se pojavljuju na fotografijama ili video streamovima pretraživanjem baza podataka o licima. Prepoznavanje i identificiranje statičnih slika omogućuje pronalaženje sličnih lica u bazama podataka vozačkih dozvola, a istovremeno pomaže u otkrivanju duplikata. Sustav provodi indeksiranje slika, stvarajući kompaktne predloške za brže pretraživanje. To zauzvrat omogućuje izgradnju niza sigurnosnih aplikacija kao što su video nadzor i sustavi za kontrolu pristupa u stvarnom vremenu (Luxand.com)[66].



Slika 14. Prepoznavanje lica pomoću Luxand FaceSDK (Izvor: Luxand.com) [67]

[66] Luxand URL: https://www.luxand.com/facesdk/
[67] URL: www.luxand.com

5. ISTRAŽIVANJE

U praktičnom djelu rada kao primjer primjene dubokog učenja za prepoznavanje lica koristit će se jedan od aktualnih alata za zamjenu lica – naziva *FaceSwap*. *FaceSwap* je aplikacija koja se koristi za izradu dubokih lažnjaka (eng. *deepfakes*) odnosno koristi se u svrhe zamjene lica osobe u videozapisu s licem neke druge osobe, a da to izgleda realno i stvarno. Ovaj dio rada objasnit će pobliže proces izrade tzv. „dubokih lažnjaka", kako nastaju i naposljetku primjerom prikazati kako radi sama aplikacija.

5.1. Duboko učenje i duboki lažnjaci

Deepfakes ili „duboki lažnjaci" su lažni videozapisi stvoreni pomoću digitalnog softvera, strojnog učenja ili u ovom slučaju, dubokog učenja i zamjene lica. Deepfakes su računalno stvoreni umjetni videozapisi u kojima se slike kombiniraju kako bi se stvorile nove snimke koje prikazuju događaje, izjave ili radnje koje se zapravo nikada nisu dogodile i pripisane osobama koje ih nikad nisu ni izrekle ili napravile. Rezultati koji se kreiraju zamjenama lica mogu biti prilično uvjerljivi, stoga su danas, ako su korišteni u krive svrhe, poprilično opasni (Sample, 2020)[68].

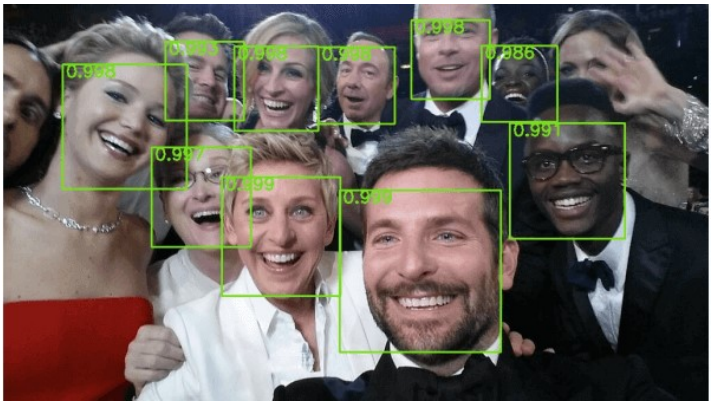
Subotić (2020)[69] navodi da prilikom učenja sustava da prepoznaju lice, treniranja neuronskih mreža i kreiranja dubokih lažnjaka, potrebno je poduzeti nekoliko koraka.

Prvi korak je detekcija lica. Program prije svega mora detektirati poziciju na kojoj se lice nalazi i okvir, te to čini pomoću koordinata na kojima se lice nalazi u određenom

[68] Sample, I. (2020). What are deepfakes – and how can you spot them, *The Guardian* URL: https://www.theguardian.com/technology/2020/jan/13/what-are-deepfakes-and-how-can-you-spot-them [Pristupjeno 3.9.2021.]

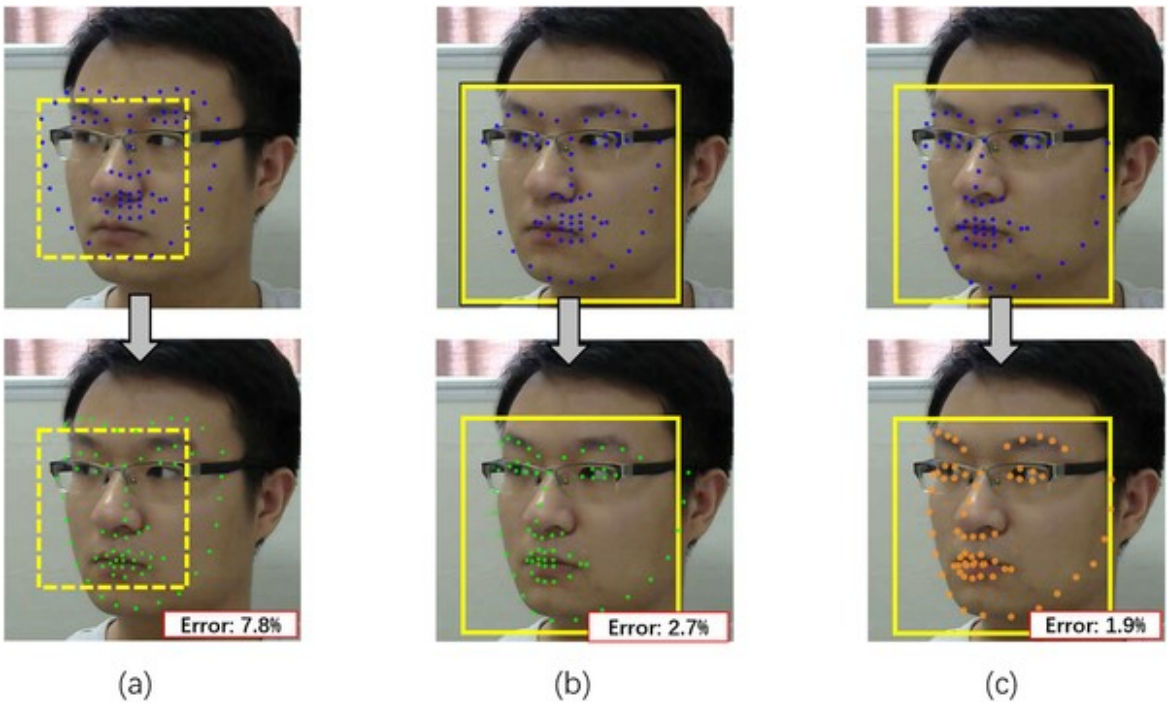
[69] Subotić, D. (2020). Primjena dubokog učenja, Strojarski fakultet Slavonski Brod, diplomski rad, 57 str.

videozapisu ili slici. Modeli koji se koriste u te svrhe su Resenet (Cv2-dnn), Mtcnn i S3Fd (Subotić, 2020)[70].



Slika 15. Detekcija lica na slici (Izvor: mantra.ai) [71]

Sljedeći korak je poravnanje lica na videozapisu ili slici. S obzirom na to da su lica na videozapisu ili slici rijetko kad poravnata tako da gledaju cijelo vrijeme ravno u kameru, često su manja ili veća, okrenuta u jednu ili drugu stranu, potrebno je poravnati sliku tako da pruža dosljedan i konstantan primjer podataka za treniranje umjetnih neuronskih mreža. Taj se problem rješava tako da se lice podijeli na glavna obilježja poput nosa, očiju, usna, brade koji čine mrežu točaka ili masku pomoću koje se lica poravnavaju u jedan isti format.

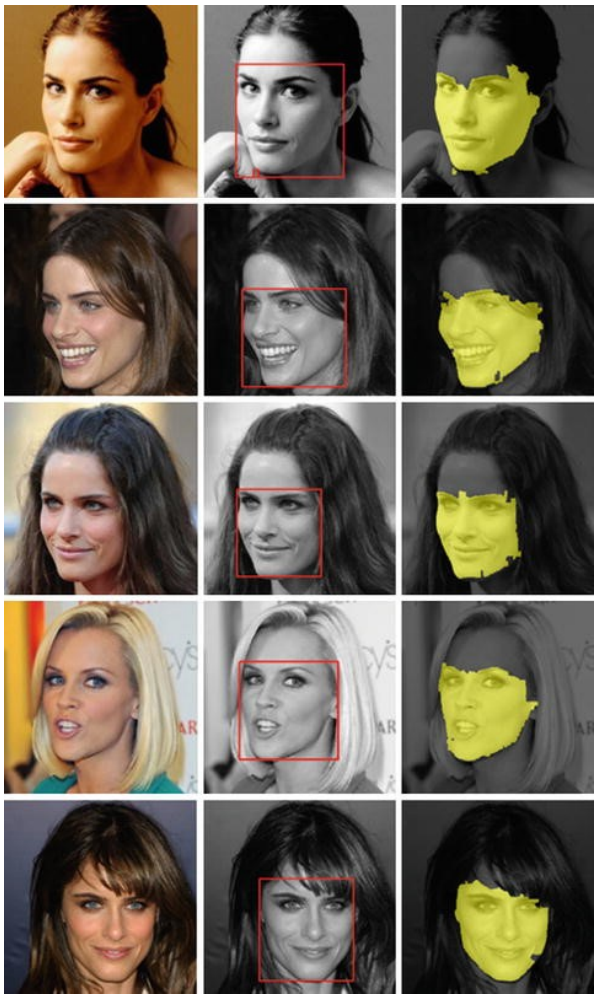


[70] *Ibid.*
[71] URL: www.mantra.ai

Slika 16. Prikaz poravnanja lica pomoću točkaste maske koja se stavlja na lice (Izvor: journals.plos.org) [72]

Zatim sustav mora prepoznati lice. Može se dogoditi da se u željenom videozapisu ili slici pojavljuje više ljudi te to stvara problem kada želimo izdvojiti samo jednu osobu. Taj problem se rješava umjetnim neuronskim mrežama koje na temelju osebujnih karakteristika pojedinca, pronalaze ga i izdvajaju iz mase. Te karakteristike duboke neuronske mreže primjenjuju na druga lica na videozapisu te ona koja nemaju te značajke preskaču dok ne identificiraju traženu osobu.

Posljednji korak je segmentacija lica koja u videozapisu ili slici traži samo ono što nam je u interesu odnosno, služi za prepoznavanje potrebnih dijelova te nepotrebne ignorira. U praksi, segmentacija će izdvojiti samo lice u cijelom videozapisu, a sve ostalo odbaciti kao na slici 17.



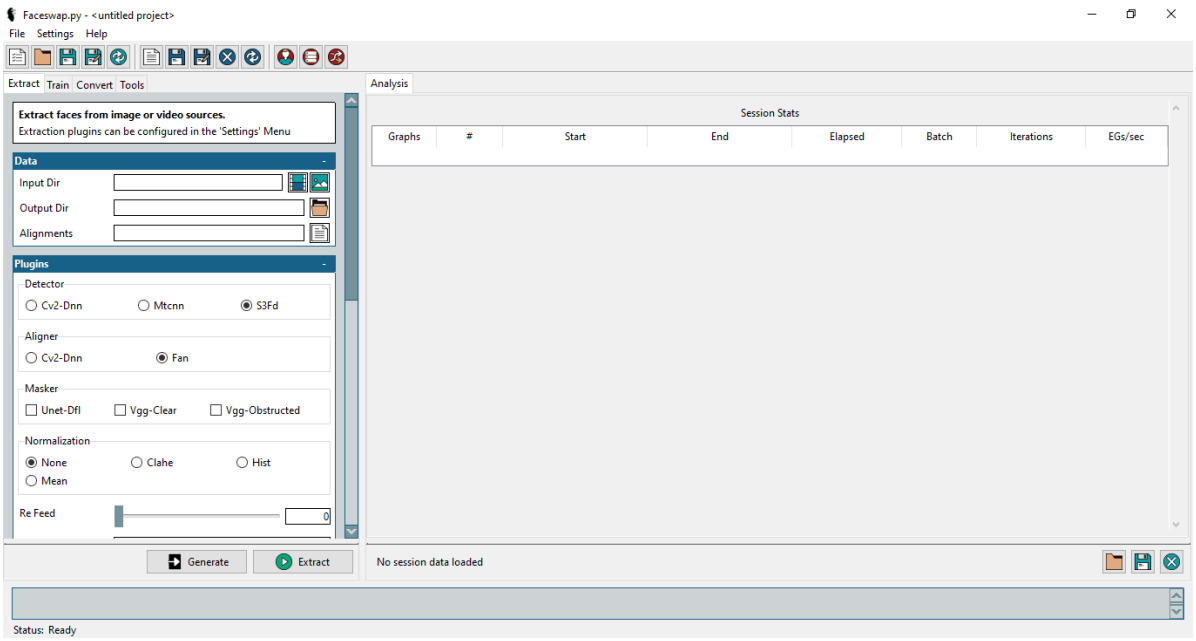
Slika 17. Segmentacija lica (Izvor: link.springer.com) [73]

[72] URL: www.journals.plos.org

[73] URL: link.springer.com

5.2. *FaceSwap* i zamjena lica

Za zamjenu lica koristit će se isječci iz intervjua dvojice poznatih glumaca, Jareda Leta i Nicolasa Cagea, te će se lice Jareda Leta iz originalnog videoisječka zamijeniti s licem Nicolasa Cagea. Za zamjenu potrebno je otvoriti program u kojem će se zamjena izvršiti. Prilikom pokretanja programa *FaceSwap* otvara se početno sučelje. Sučelje ima prozor s opcijama za izvući lice (eng. *extract*), za treniranje umjetnih neuronskih mreža (eng. *train*) i na kraju za zamijenu (eng. *convert*).

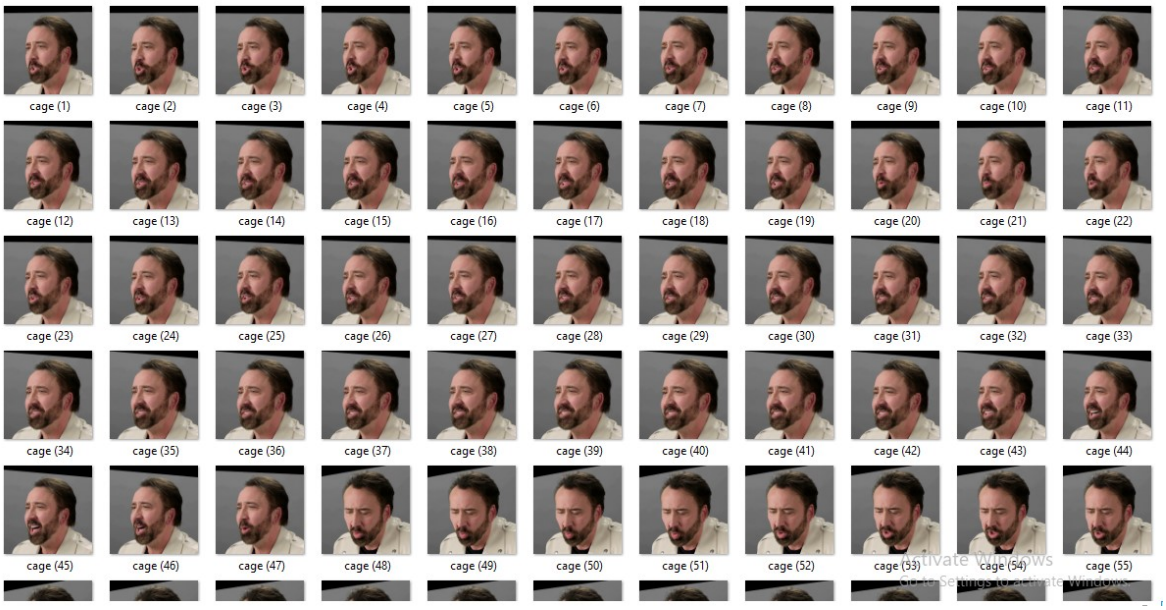


Slika 18. Početni zaslon programa FaceSwap[74] (Izvor: FaceSwap)

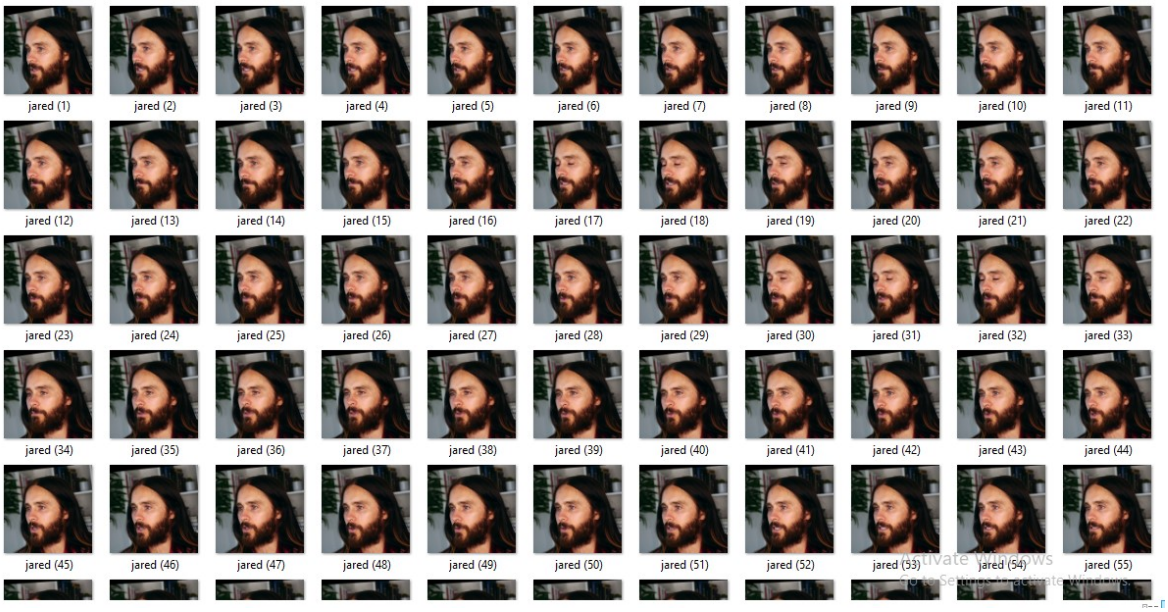
Prije same zamjene potrebno je izvući lica iz videozapisa na temelju kojih će se program trenirati. To se vrši pomoću naredbe `extract`, gdje se odabire videozapis s licem koje želimo izvući te aplikacija prvo detektira lice, zatim poravnava, te segmentira. Na slici 19 prikazane su segmentirane odnosno izdvojene slike lica glumca Nicolasa Cagea. Iz odabranog videa koji je korišten za segmentaciju izvučeno je 1440 slika lica Nicolasa Cagea iz isječka koji traje tri minute i 13 sekundi, a iz isječka intervjua Jareda Leta koji traje 38 sekundi izvučeno je 980 slika lica. Prije samog treniranja programa, potrebno je ručno

[74] FaceSwap program

pregledati mapu u koju su pohranjene slike i izbrisati one koje nemaju izraze lica ili je lice prekriveno s nekim objektom ili rukom. Ta opcija nije nužna, ali radi bolje kvalitete je preporučljiva.



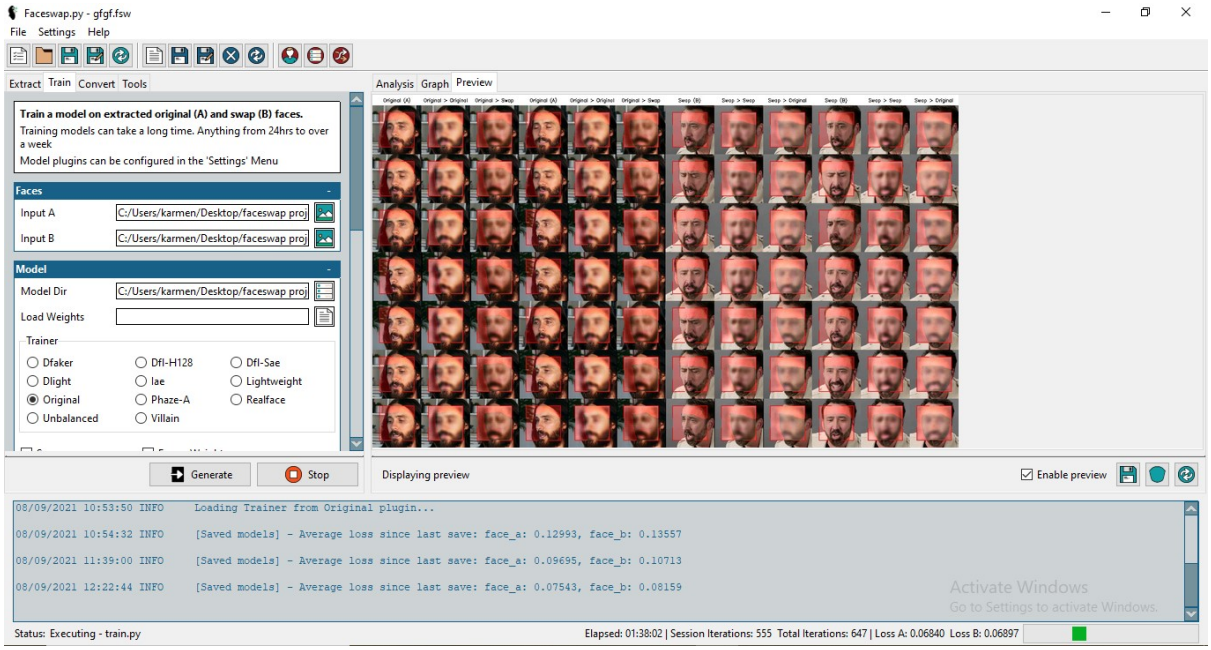
Slika 19. Mapa s izdvojenim slikama lica Nicolasa Cagea (Izvor: vlastita izrada)



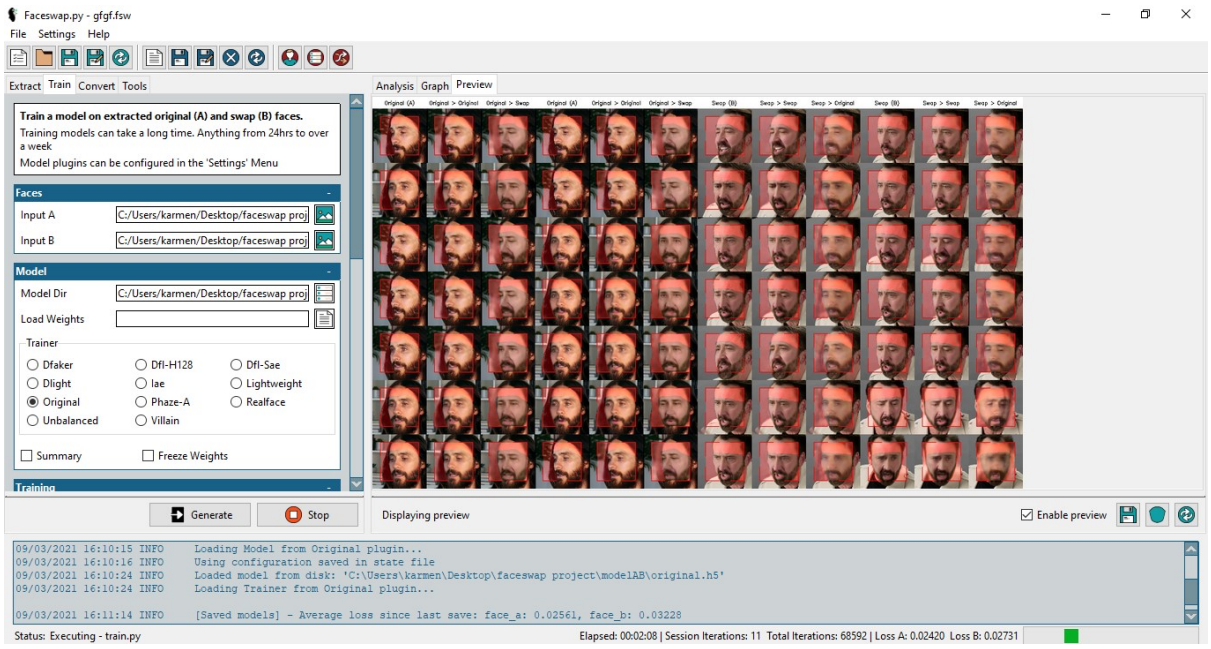
Slika 20. Mapa s izdvojenim slikama lica Jareda Leta (Izvor: vlastita izrada)

Nakon što su lica oba glumca segmentirana i odvojena, program pokreće treniranje ili učenje svojih umjetnih neurona. U prozoru se odabere opcija `train`, te se odabire za input A

datoteka sa slikama Jareda Leta, te za input B datoteka sa slikama Nicolasa Cagea. Odabiru se dodatne mape gdje će biti pohranjeni modeli, te se klikne dolje u podnožju prozora na treniranje odnosno `train` za početak učenja. Ovaj proces može trajati od 24 sata pa sve do tjedan dana, ovisno o računalu na kojem radite i njegovim specifikacijama. Idealno je trenirati program minimalno 40,000 iteracija za pristojnu kvalitetu izlaznog produkta.

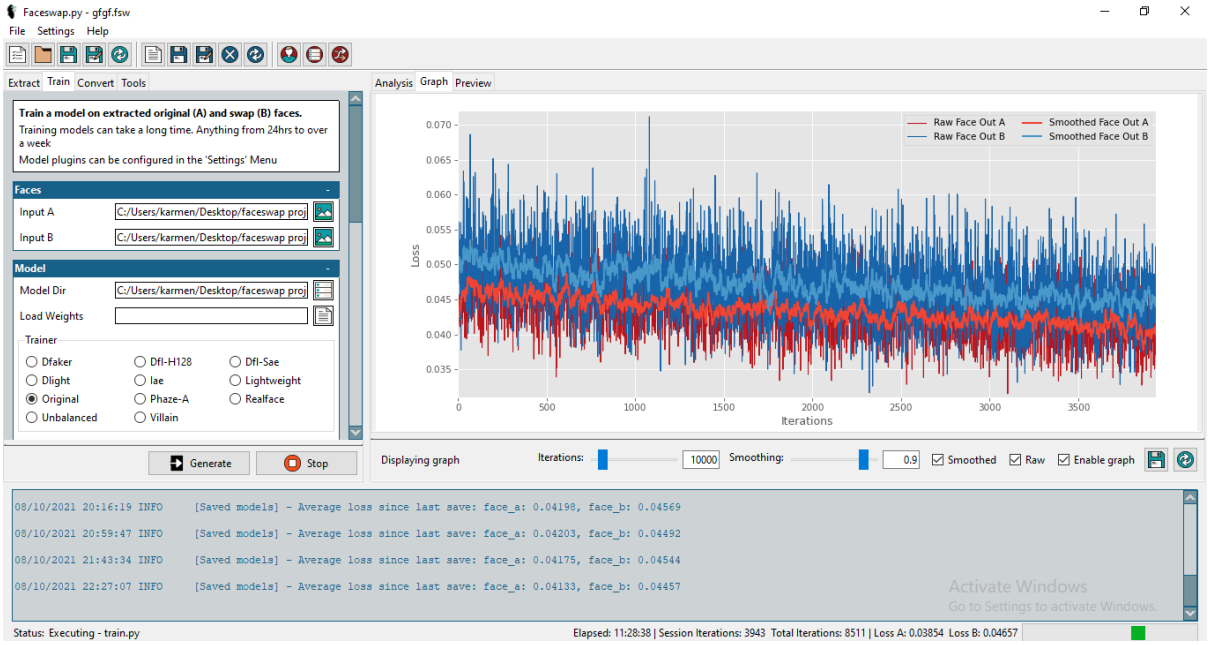


Slika 21. Treniranje aplikacije koja ima 647 iteracija (Izvor: vlastita izrada)

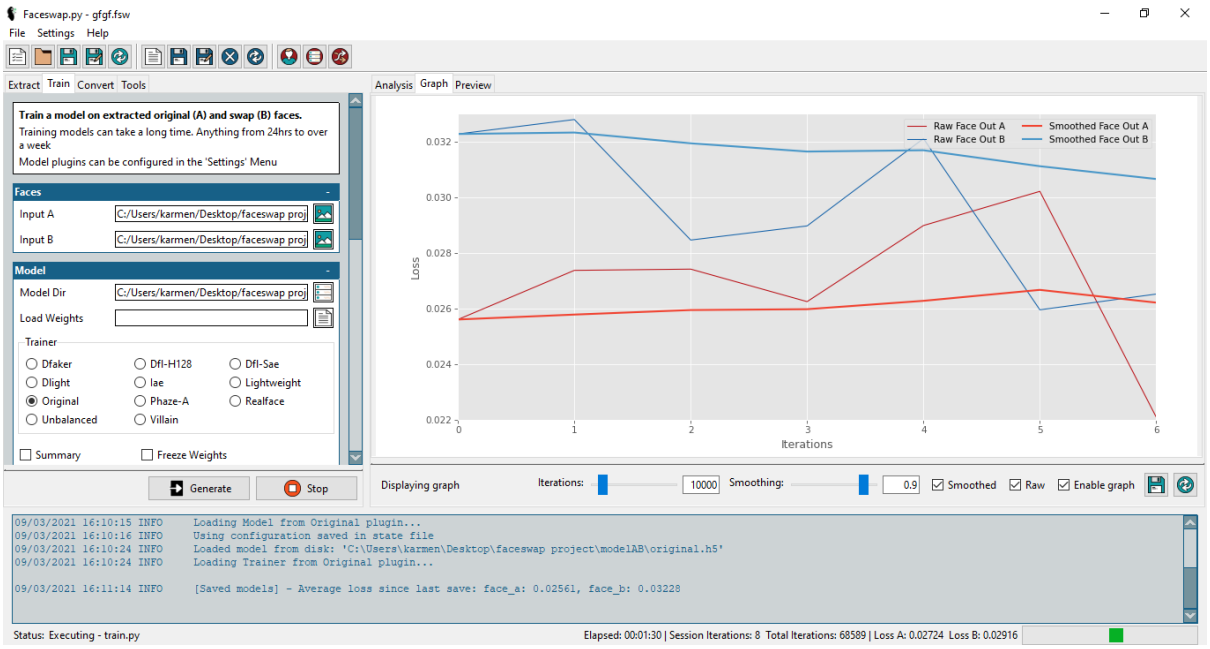


Slika 22. Treniranje aplikacije s 68 581 iteracija (Izvor: vlastita izrada)

Program također prikazuje i prati iteracije te njihove vrijednosti gubitka prilikom treniranja kao što je prikazano na slici 23 s početka treniranja i 24 na kraju treniranja.

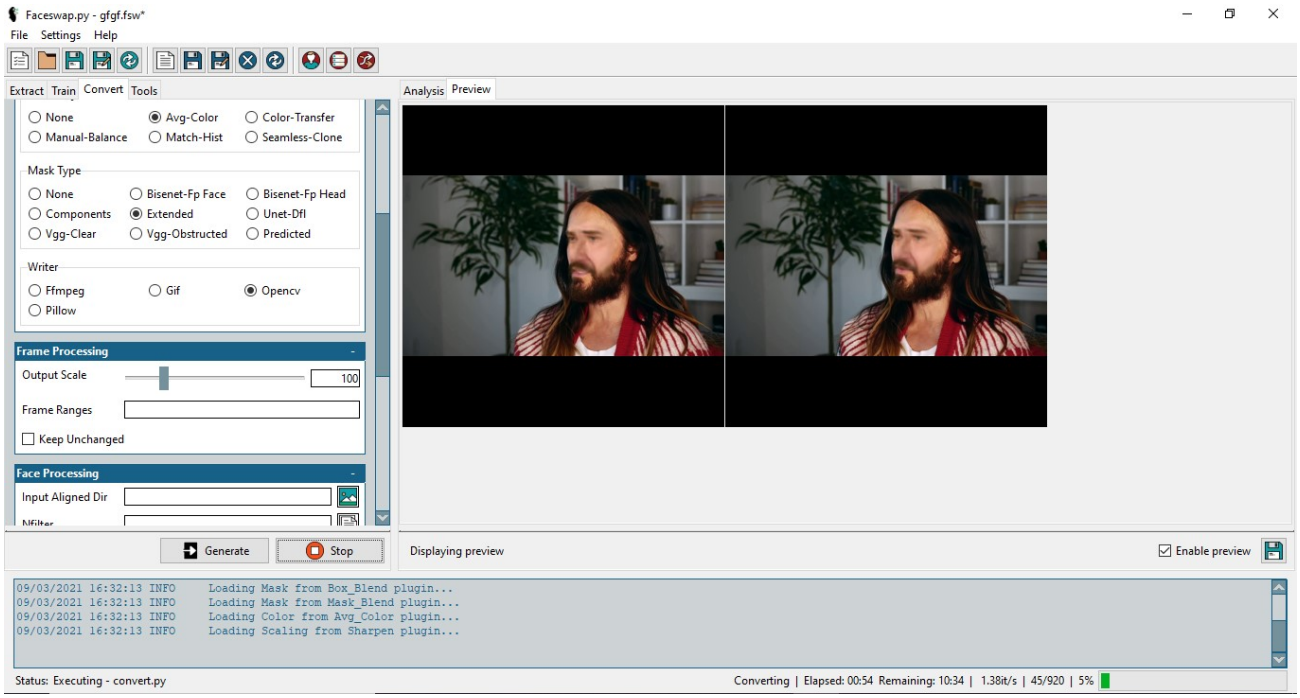


Slika 23. Graf s vrijednostima gubitka s 8511 sveukupnih iteracija (Izvor: vlastita izrada)



Slika 24. Graf s vrijednostima gubitka s 68 581 iteracija (Izvor: vlastita izrada)

Nakon treniranja potrebno je ta dva lica spojiti u jedan videozapis kao što je prikazano na slici 25, odnosno zamijeniti što je ujedno i posljednji korak u ovom praktičnom radu. U snimci iz intervjua Jareda Leta njegovo lice je zamijenjeno s licem Nicolasa Cagea. Na ovaj način se vrši zamjena lica u programu *FaceSwap*.



Slika 25. Izmjena lica (Izvor: vlastita izrada)

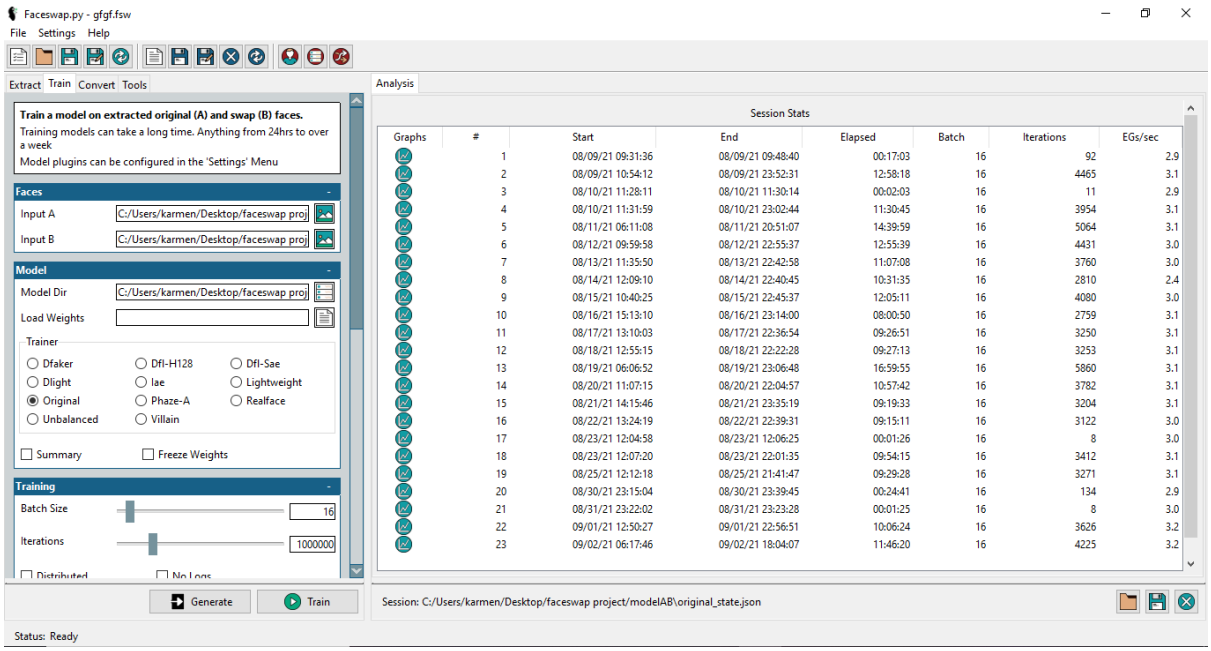
5.3. Rezultati

Rezultati procesa istraživanja su prikazani na slici 26 koja prikazuje konačnu izmjenu lica u videozapisu.

Slika 26. Originalni i zamijenjeni videozapis (Izvor: vlastita izrada)

Postupak zamjene je trajao otprilike 16 minuta te su se lica zamijenila veoma brzo u usporedbi sa dugotrajnim procesom treniranja.

Kao što se može vidjeti iz priložene slike 27, razdoblje treniranja je od 9.8.2021. do 2.9.2021., sveukupno 20 dana s prosječno 11 sati treniranja dnevno (najviše 17 sati 19.8. i najmanje 8 sati 16.8.) i otprilike 3000 iteracija prilikom svakog treniranja. Sveukupno 201 sati treniranja.



Slika 27. Razdoblje trajanja treniranja i broj iteracija za svako (Izvor: vlastita izrada)

Za izvlačenje lica glumca Nicolasa Cagea programu je bilo potrebno više od 6 sati rada na videoisječku koji je trajao tek nešto više od 3 minute s odličnom kvalitetom slike od 1920/1080 piksela, te je originalno izvučeno preko 6000 slika različitih izraza lica od kojih su nakon ručne selekcije i brisanja mutnih i nekvalitetnih uzoraka, preostalo tek 1440. Dok je kod videoisječka Jareda Leta koji je trajao samo 38 sekundi s istom kvalitetom slike, izvučeno originalno otprilike 1000 slika u periodu od manje od 2 sata te selektirano naposljetku 908 slika. Videozapis u kojem se mijenja lice (u ovom slučaju Jareda Leta) trebao bi biti kraći od zapisa koji ga mijenja (Nicolas Cage) jer se program treba trenirati na izrazima lica one osobe s kojom se vrši izmjena radi bolje zamjene. Potrebno je više slika Nicolasa Cagea na kojima se program trenira da bi zamijenio lice Jareda Leta u njegovom videozapisu. Prosječan gubitak prilikom treniranja je 0.02561 za Jareda Leta i 0.03228 za Nicolasa Cagea.

Može se zaključiti da što je dulji video i veća kvaliteta slike to je programu potrebno više vremena za izvlačenje i potrebno je također ručno odvajanje kvalitetnih od nekvalitetnih

uzoraka. Ručno odvajanje je nužno da bi konačni rezultat rada programa bio oštar i jasno vidljiv jer da su se koristile i mutne nejasne slike, program bi ih teže obradio te bi koruptirale krajnji cilj.

Također, uz kvalitetu slike i trajanje videoisječka potrebno je obratiti pozornost na cjelokupan videozapis odnosno na osvjetljenje, radnju u zapisu, sjene, postoji li više osoba, itd. Previše tamno osvjetljenje uzrokuje probleme prilikom treniranja odnosno zamjene jer određeni detalji koji su potrebni nisu dovoljno jasni ili su zatamnjeni te ih program ne može jasno odrediti ili pak su prevelike razlike između dvaju videozapisa pa izmijenjeno tamno lice na svjetlom izgleda na kraju neprirodno. Radnja je bitna jer je velika razlika ako je osoba u nekom naglom pokretu ili mirno sjedi zbog potrebnog vremena treniranja i zamjene, puno brže izmjenjuje kada su osobe u mirnom pokretu ili u mirovanju nego kada su aktivne. Više osoba u videozapisu rezultira pogrešnom zamjenom ili pak nasumične letimične neželjene zamjene u konačnom videozapisu.

Ovim alatom moguće je prepoznati lice i zamijeniti ga bez da se naruši identitet izvornog lica i njegovih izraza i osvjetljenja. No, praktični dio je rađen na video isječku koji traje 20 sekundi, te za sve iznad toga proces je uvelike kompliciraniji i iziskuje jako puno vremena koje će biti utrošeno u njega. To je jedan od najvećih problema s kojima se duboko učenje i duboke umjetne neuronske mreže susreću.

Drugi problem ovako zahtjevnijih alata su specifikacije korisnikovog računala. Računalo na kojem je rađeno istraživanje puno je slabije i sporije od računala koja su namijenjena ovakvim alatima. U prosjeku, jačem računalu bilo bi potrebno 16 sati sveukupnog treniranja da dostigne 75 000 iteracija, dok je računalu na kojem je rađena izmjena sveukupno treniranje trajalo 201 sati i rezultiralo s 68 581 iteracija.

6. Etički pristupi

Pojavom mnogih sličnih programa poput aplikacije *FaceSwap,* koji su dostupni svima koji posjeduju dovoljno snažna računala koja su u mogućnosti pokrenuti jednostavan proces izmjene lica bilo koje osobe koju žele, bilo od slavnih, političkih ikona sve do običnih ljudi, pojavljuju se paralelno i razni problemi oko zlouporabe. Ti problemi koji se javljaju mogu varirati od nemoralnih zloupotreba, zavaravanja javnosti i širenja panike, blaćenja javnih osoba, narušavanja ugleda, pa sve do kršenja privatnosti i nanošenja psihičkih trauma.

6.1. Zavaravanje javnosti i širenje panike

Jedan od primjera zavaravanja javnosti i narušavanja ugleda javne osobe jest kada je 2019. godine objavljen duboki lažni videozapis Marka Zuckerberga koji govori o tome koliko je sretan što ima podatke tisuća ljudi, što je navelo javnost u privid da je njihova privatnost narušena i podaci ukradeni. Videozapis je kreiran od *Instagram* korisnika bill_posters_uk[75] koji je kreirao *Spektar* u kojem objavljuje izmijenjene videozapise kako bi upozorio na njihovo korištenje i manipulaciju. Od tada pa nadalje, popularnost dubokih lažnjaka se od tada samo povećala, te postoji cijeli popis za reprodukciju *YouTube* s dubokim lažnim videozapisima posvećenim predsjedniku Trumpu.

6.2. Narušavanje ugleda i kršenje privatnosti

Prema Kiari Goodwine (2020)[76] jedan problem s dubokim lažnjacima jest taj što oponašaju čovjekovo lice bez njihovog dopuštenja. Prvi duboki lažnjaci koristili su fotografije ili videozapise određene osobe pomiješane s pornografijom. Takvo korištenje lica neke osobe ne bi moglo osobno utjecati na nju, ali bi se ipak moglo smatrati pogrešnim,

[75] Instagram, bill_posters_uk URL: https://www.instagram.com/bill_posters_uk/ [Prostupljeno: 1.9.2021.]

[76] Goodwine, K. (2020). Ethical Considerations of Deepfakes*, The Prindle Post* URL: https://www.prindlepost.org/2020/12/ethical-considerations-of-deepfakes/ [Pristupljeno: 1.9.2021.]

budući da se koristi kao izvor užitka i zabave, bez pristanka. Iako zvuči dosta napregnuto, od 2019., sada već nepostojeća aplikacija pod nazivom *DeepNude*, nastojala je učiniti upravo to. Ova se aplikacija koristila da bi se ponizila osoba u pitanju i narušio njihov ugled tzv. pornografija iz osvete (eng. *revenge porn*). Ovo je pitanje iznimno bitno i moglo bi biti rasprostranjenije od ostalih potencijalnih šteta dubokih krivotvorina. Istraživanje tvrtke za kibernetičku sigurnost *Sensity*[77] usredotočena na vizualne prijetnje, tvrdi da je velika većina dubokih lažnih videozapisa pornografskih (96%) i da tehnologija tek treba ući u značajnije kampanje dezinformacija.

6.3. Širenje dezinformacija i kriminalitet

Također, Goodwine (2020)[78] iznosi da je veliki dio moralne zabrinutosti zbog dubokih krivotvorina utemeljen u njihovoj mogućnosti lakog širenja dezinformacija. Kritike vezane za duboke laži posljednjih godina uglavnom se odnose na njihov potencijal manipuliranja javnošću radi postizanja političkih ciljeva. Postaje sve lakše širiti lažni video zapis koji prikazuje političara koji je očito nesposoban ili širi upitnu poruku, što bi moglo umanjiti njihovu bazu. Na lokalnoj razini, duboki lažni zapisi mogli bi se koristiti za diskreditaciju pojedinaca. Moglo bi se zamisliti svijet u kojem se duboki lažnjaci koriste za namještanje nekoga kako bi se narušio njegov ugled ili čak za sugeriranje da je počinio zločin. Video i foto dokazi uobičajeno se koriste u našem građanskom i kaznenom pravosudnom sustavu, a mogućnost manipuliranja videozapisima ili slikama neke osobe, neotkrivena, vjerojatno predstavlja ozbiljnu opasnost za pravosudni sustav koji se oslanja na naše osjetilo vida i opažanje za utvrđivanje cilja činjenica. Možda čak i gore od namještanja nedužnog može biti neuspjeh da se osude krivci.

Zapravo, nedavno istraživanje objavljeno u časopisu „Crime Science“ pokazalo je da duboke lažne prijetnje predstavljaju ozbiljnu prijetnju kriminalom kada su u pitanju audio i

[77] *Sensity* URL: https://sensity.ai/reports/ [Pristupljeno: 1.9.2020.]

[78]Goodwine, K. (2020). Ethical Considerations of Deepfakes*, The Prindle Post* URL: https://www.prindlepost.org/2020/12/ethical-considerations-of-deepfakes/ [Pristupljeno: 1.9.2021.]

[78] *Sensity* URL: https://sensity.ai/reports/ [Pristupljeno: 1.9.2020.]

video lažno predstavljanje i ucjena. U tom članku pod nazivom *AI-enabled future crime*[79] skupina autora provodi pregled kako bi se utvrdile moguće primjene umjetne inteligencije i srodnih tehnologija u počinjenju zločina. Prikupljeni primjeri korišteni su za izradu približne taksonomije kaznenih prijava u svrhu procjene njihovih relativnih razina prijetnje. Vježba je kulminirala dvodnevnom radionicom na temu „AI i budući kriminal" s predstavnicima akademske zajednice, policije, obrane, vlade i privatnog sektora. Zadaća radionice bila je (i) katalogizirati potencijalne kriminalne i terorističke prijetnje koje proizlaze iz sve većeg usvajanja i moći umjetne inteligencije, i (ii) rangirati ove prijetnje u smislu očekivane štete žrtve, kriminalne dobiti, ostvarivosti kriminala i težine poraza. Identificirano je i ocijenjeno osamnaest kategorija prijetnji. Pet od šest najbolje ocijenjenih imalo je širok društveni utjecaj, poput onih koje uključuju lažni sadržaj generiran umjetnom inteligencijom (eng. *AI*) ili su mogle djelovati opsežno korištenjem automatizacije umjetne inteligencije; šesti je bio zlouporaba tehnologije vozila bez vozača za teroristički napad.

6.4. Mjere za reguliranje zlouporabe programa

Zbog takvih zlouporaba potrebno je bilo provesti mjere pomoću kojih bi se reguliralo nemoralno korištenje takvih programa. Jim Brunner (2019)[80] u svome članku govori da kako se približavaju izbori 2020., nova inicijativa Sveučilišta Washington nastoji se boriti protiv vala sve sofisticiranijeg digitalnog krivotvorenja i dezinformacija koje se šire društvenim medijima i dati javnim alatima mogućnost za razvrstavanje stvarnih činjenica od lažnog. Istraživači sa Sveučilišta Washington razvili su duboke lažnjake koristeći algoritme kako bi suzbili njihovo širenje. Centar za informiranu javnost (CIP) dobio je 5 milijuna dolara iz Zaklade John S. i James L. Knight, kao dio bespovratnih sredstava u iznosu od 50 milijuna dolara dodijeljenih ove godine 11 američkih sveučilišta i istraživačkih institucija za proučavanje kako tehnologija dubokih lažnjaka transformira demokraciju. Misija je iskoristiti novo istraživanje kako bi pomogla svima ugroženima od zavaravanja online manipulacijama

[79] Andrews, J.T.A., Caldwell, M., Tanay, T. et al. (2020). AI-enabled future crime, *Crime Science* 9, br. 14. URL: https://crimesciencejournal.biomedcentral.com/articles/10.1186/s40163-020-00123-8#citeas [Pristupljeno: 1.9.2021.]

[80] Brunner, J. (2019). Can you tell which face is real? UW and WSU plan to fight digital 'deepfakes', *The Seattle Times* URL: https://www.seattletimes.com/seattle-news/politics/maybe-we-can-get-this-right-for-the-rest-of-the-country-how-uw-and-wsu-plan-to-fight-the-digital-deepfakes/ [Pristupljeno: 1.9.2021.]

- bilo da se radi o učenicima koji nisu sigurni koja su vijest pouzdana ili osoba koje nekritički dijele lažne vijesti na *Facebooku.*

6.5. Pozitivne strane dubokih lažnjaka

Unatoč negativnim stavovima koji su najčešće percipirani idejom dubokih lažnjaka, *Deepfake* tehnologija upotrijebljena je u pozitivne svrhe za oživljavanje umjetnosti, ponovno stvaranje glasova povijesnih ličnosti i korištenje sličnosti slavnih za prenošenje snažnih poruka javnog zdravlja.

The Dalí Museum na Floridi pokrenuo je izložbu nazvanu Dalí Lives, nastalu u suradnji s oglasnom agencijom Goodby, Silverstein & Partners (GS&P) koja je napravila realan prikaz umjetnika Salvadora Dalíja u prirodnoj veličini tehnikom uređivanja videa pomoću strojnog učenja. Koristeći arhivske snimke iz intervjua, GS&P je izvukao više od 6.000 kadrova i iskoristio 1.000 sati strojnog učenja za vježbanje AI algoritma na Dalíjevu licu. Njegov izraz lica tada je nametnut glumcu s Dalijevim tjelesnim proporcijama, a citati iz njegovih intervjua i pisama sinkronizirani su s glasovitim glumcem koji je mogao oponašati njegov jedinstveni naglasak, mješavinu francuskog, španjolskog i engleskog. Dalí se pojavljuje pred posjetiteljima kada pritisnu zvono na kiosku u kojem živi i priča im priče o svom životu. S 45 minuta novonastalih snimaka i tisućama kombinacija, svaki posjetitelj dobiva drugačije iskustvo (Lee, 2019)[81]. Slika 28 prikazuje dubokog lažnjaka Salvadora Dalíja u svom kiosku u muzeju.

Slika 28. Duboki lažnjak umjetnika Salvadora Dalíja korišten u svrhe izložbe (Izvor: Lee, 2019)[82]

[81] Lee, D. (2019.) Deepfake Salvador Dalí takes selfies with museum visitors*, The Verge* URL: https://www.theverge.com/2019/5/10/18540953/salvador-dali-lives-deepfake-museum [Pristupljeno: 1.9.2021.]

[82] Lee, D. (2019.) Deepfake Salvador Dalí takes selfies with museum visitors, *The Verge* URL: https://www.theverge.com/2019/5/10/18540953/salvador-dali-lives-deepfake-museum [Pristupljeno: 1.9.2021.]

7. Zaključak

Glavni cilj ovog rada bio je prikazati postupak treniranja, prepoznavanja i zamjene lica primjenom alata za duboko učenje, koje predstavljaju najsuvremeniji pristup u području umjetne inteligencije i primjene neuronskih mreža prilikom učenja i definiranja lica, te ukazati na potencijalne stvarne prijetnje korištenja takve tehnologije, ali i pozitivne strane.

U teorijskom djelu rada prikazana je struktura i opis umjetne inteligencije te njeno grananje na potpolja strojno učenje i duboko učenje. Strojno učenje je oblik učenja prilikom kojega je potrebna ljudska intervencija da bi rezultat bio uspješan, dok kod dubokog učenja se koriste umjetne neuronske mreže koje funkcioniraju u principu slično kao stvarni biološki neuroni u mozgu. Opisani su primjeri korištenja dubokog učenja i istraživanja u tom području.

U istraživanju je korišten program *FaceSwap* pomoću kojeg su demonstrirane primjene jednog od brojnih alata dubokog učenja za prepoznavanja lica, te u ovom slučaju i zamjene lica. Rezultati koji su proizašli iz istraživanja programa i rada *FaceSwapa,* daju uvid u proces stvaranja dubokih lažnjaka i njihovu manipulaciju. Programu je bilo potrebno 17 dana treniranja po otprilike 11 sati dnevno na dva videozapisa u trajanju od 3 minute i 15 sekundi i drugom u trajanju od 38 sekundi prilikom čega je izvučeno više od 60.000 iteracija koje su potrebne da bi rezultat bio kvalitetan. Broj slika iz zapisa od 1440 i 908 su ključne u treniranju programa jer veći broj slika lica osobe osigurava bolju kvalitetu i jasnoću finalnog videozapisa zamjene lica. Problemi koji mogu ugroziti rezultat su osvjetljenje, sjene i pojava drugih lica u zapisu te loša kvaliteta i oštrina, što u ovom istraživanju nije slučaj jer su videozapisi pomno izabrani.

Iako zasigurno još ima problema koje treba prevladati u ovom području, smatra se da je postignut značajan napredak u području prepoznavanja lica temeljenog na umjetnoj neuronskoj mreži. Mnogo je prednosti korištenja umjetnih neuronskih mreža poput jednostavne implementacije, jednostavnog dodavanja novih identiteta, sposobnost upravljanja jačinom učinka ili potencijala postizanja rezultata puno prirodnijeg izgleda nego što je to prethodno bilo moguće.

Unatoč mnogim prednostima, važno je istaknuti da prilikom manipulacije u ovakvom obliku potrebno je obratiti pozornost na etičke principe i moguću zlouporabu. Pristup ovakvim programima imaju svi, ali ih ne koriste svi u moralno dobre svrhe (osveta, narušavanje ugleda, dezinformiranje…) te je potrebno regulirati njihovo stvaranje i širenje.

Duboko učenje kao podskup strojnog učenja, postala je iznimno popularna tema proteklih godina zahvaljujući mnoštvu podataka te povećane snage i mogućnostima računala. Iako nedavno razvijena, ova se je tehnologija danas rasprostranila i primjenjivana u raznovrsnim programima, aplikacijama i uređajima koje svakodnevno koristimo. S daljnjim razvojem vrlo je vjerojatno da će sami alati napredovati daleko više od prognoziranog te imati ogroman utjecaj na komercijalne i svakodnevne primjene.

8. Literatura

1. Aly, S., Hassaballah, M. (2015). Face Recognition: Challenges, Achievements, and Future Directions*, ET Computer Vision* 9(4):614-626
2. Andrews, J.T.A., Caldwell, M., Tanay, T. et al. (2020.) AI-enabled future crime*, Crime Science* 9, br. 14. URL: https://crimesciencejournal.biomedcentral.com/articles/10.1186/s40163-020-00123-8#citeas [Pristupljeno: 1.9.2021.]
3. Anirudh, V. K. (2019). What Is Machine Learning: Definition, Types, Applications and Examples, Toolbox URL: https://www.toolbox.com/tech/artificial-intelligence/tech-101/what-is-machine-learning-definition-types-applications-and-examples [Pristupljeno: 3.9.2021.]
4. Bengio, Y., Courville, A., Goodfellow, I. (2016). Deep learning*, Cambridge MA: MIT Press*, 785 str.
5. Beslay, L., Galbally, J., Ferrara, P., Haraksim, R., Psyllos, A., (2019). Study on Face Identification Technology for its Implementation in the Schengen Information System, EUR 29808 EN, Publication Office of the European Union, Luxemburg, ISBN 978-92-76-08843-1
6. Bheemaiah, K., Esposito M., Tse, T. (2017). What is machine learning*?* The Conversation URL: https://theconversation.com/what-is-machine-learning-76759 [Pristupljeno: 3.9.2021.]
7. Brunner, J. (2019). Can you tell which face is real? UW and WSU plan to fight digital 'deepfakes', *The Seattle Times* URL: https://www.seattletimes.com/seattle-news/politics/maybe-we-can-get-this-right-for-the-rest-of-the-country-how-uw-and-wsu-plan-to-fight-the-digital-deepfakes/ [Pristupljeno: 1.9.2021.]
8. Das, S. (2020). The AI Behind FaceApp, Analyticsindiamag URL: https://analyticsindiamag.com/the-ai-behind-faceapp/ [Pristupljeno: 3.9.2021.]
9. DataDrivenInvestor (2018). Deep learning URL: https://medium.datadriveninvestor.com/deep-learning-2025e8c4a50 [Pristupljeno 16.6.2021.]

10. DeepMind, AlphaGo URL: https://deepmind.com/research/case-studies/alphago-the-story-so-far [Pristupljeno: 31.8.2021]
11. Dwivedi, D. (2018). Face Detection For Beginners, TowardsDataScience URL: https://towardsdatascience.com/face-detection-for-beginners-e58e8f21aad9 [Pristupljeno: 3.9.2021.]
12. Džomba, K. (2018). Konvolucijske neuronske mreže, Sveučilište u Zagrebu, Prirodoslovno-matematički fakultet, diplomski rad, 78 str.
13. Expert.ai Team (2020). What is Machine Learning? A Definition., Expert.ai URL: https://www.expert.ai/blog/machine-learning-definition [Pristupljeno: 3.9.2021.]
14. Gašpar, A., Seljan, S., Kučiš, V. (2021). Consistency of Translated Terminology Measured by the Herfindahl-Hirshman Index (HHI), in print.
15. Goodwine, K. (2020). Ethical Considerations of Deepfakes, The Prindle Post URL: https://www.prindlepost.org/2020/12/ethical-considerations-of-deepfakes/ [Pristupljeno: 1.9.2021.]
16. Gupta, A., Anpalagan, A., Guan, L., Shaharyar Khwaja, A. (2021). Deep learning for object detection and scene perception in self-driving cars: Survey, challenges, and open issues, Volume 10, 100057, ISSN 2590-0056 URL: https://www.sciencedirect.com/science/article/pii/S2590005621000059#! [Pristupljeno: 3.9.2021.]
17. Hauser, L. (2020). Artificial Intelligence, *Internet Encyclopedia of Philosophy*, URL: https://iep.utm.edu/art-inte/#H6 [Prostupljeno: 31.8.2021.]
18. IBM, Deep Blue URL: https://www.ibm.com/ibm/history/ibm100/us/en/icons/deepblue/ [Pristupljeno:1.9.2021.]
19. Instagram, bill_posters_uk URL: https://www.instagram.com/bill_posters_uk/ [Pristupljeno: 1.9.2021.]
20. Josipović, M. (2019). Postupci strojnog učenja za popravljanje točnosti klasifikacije manjinskih klasa kod nebalansiranih skupova podataka,Sveučilište u Zagrebu, Fakultet elektrotehike i računarstva, završni rad, 24 str.
21. Jun-Bao L., Shu-Chuan C., Jeng-Shyang Pan (2014). Kernel Learning Algorithms for Face Recognition, *Springer Science+Business Media*, 232 str.
22. Journal of Information Technology & Software Engineering (2011). Artificial-Intelligence-open-acces URL: https://www.longdom.org/peer-reviewed-journals/artificialintelligenceopenaccess-36559.html [Pristupljeno: 31.8.2021.]

23. Kelleher, J. D. (2019). Deep Learning, London, *The Massachusetts Institute of Technology: The MIT Press*, 296 str.
24. Kim, P. (2017). MATLAB Deep Learning: With Machine Learning, Neural Networks and Artificial Intelligence, Seoul, *Apress*, 158 str.
25. Khalilan, M., Shiva, H. (2019). Document classification methods.
26. Kortli, Y., Jridi, M., Falou, A. A., & Atri, M. (2020). Face Recognition Systems: A Survey. Sensors (Basel, Switzerland), 20(2), 342.
27. Kovač, L. (2015). Umjetna inteligencija danas, Sveučilište u Rijeci, Filozofski fakultet u Rijeci, diplomski rad, 82 str.
28. Krstić, Ž.; Seljan, S.; Zoroja, J. (2019). Visualization of big data text analytics in financial industry: a case study of topic extraction for Italian banks. Proceedings of the ENTRENOVA '19 - ENTreprise REsearch InNOVAtion Conference, 67-75.
29. Lee, D. (2019). Deepfake Salvador Dalí takes selfies with museum visitors, *The Verge* URL: https://www.theverge.com/2019/5/10/18540953/salvador-dali-lives-deepfake-museum [Pristupljeno: 1.9.2021.]
30. Marrara, S.; Pejić Bach, M., Seljan, S.; Topalovic, A. (2019). FinTech and SMEs: the Italian case. FinTech as a Disruptive Technology for Financial Institutions. Rafay, Abdul (ur.). Hershey, Pennsylvania: IGI Global,. 14-41. doi:10.4018/978-1-5225-7805-5.ch002
31. Matić, P., (2014). Kratkoročno predviđanje hidrološkog dotoka pomoću umjetne neuronske mreže, Sveučilište u Splitu; Fakultet elektrotehnike, strojarstva i brodogradnje, doktorska disertacija, 137 str.
32. Murphy, K. P. (2012). Machine Learning: A Probabilistic Perspective, Cambridge Mass, *The MIT Press*, 1067 str. (2-30)
33. Oppermann, A. (2019). Artificial Intelligence vs. Machine Learning vs. Deep Learning, TowardsDataScience URL: https://towardsdatascience.com/artificial-intelligence-vs-machine-learning-vs-deep-learning-2210ba8cc4ac [Pristupljeno: 3.9.2021.]
34. Pejić Bach, M., Krstić, Ž., Seljan, S. (2019a). Big data text mining in the financial sector. Expert systems in finance: smart financial applications in big data environments. Metawa, N., Elhoseny, M., Hassanien, A. E., Hassan, M. K. (ur.). London: Routledge, 80-96 doi:10.4324/9780429024061
35. Pejić Bach, M.; Seljan, S.; Jaković, B.; Buljan, A.; Zoroja, J. (2019b). Hospital websites: from the information repository to interactive channel. Procedia computer science, 164 (2019), 64-71 doi:10.1016/j.procs.2019.12.155

36. PetaPixel (2016). A Look at How Snapchat's Powerful Facial Recognition Tech Works URL: https://petapixel.com/2016/06/30/snapchats-powerful-facial-recognition-technology-works/ [Pristupljeno: 3.9.2021.]
37. Relić, B. (2019). Klasifikacija očitanja koristeći metode dubokog, Sveučilište u Zagrebu, Fakultet elektrotehnike i računarstva, završni rad, 26 str.
38. Robins, M. (2020). The Difference Between Artificial Intelligence, Machine Learning and Deep Learning, Intel, URL: https://www.intel.la/content/www/xl/es/artificial-intelligence/posts/difference-between-ai-machine-learning-deep-learning.html [Pristupljeno 19.6.2021.]
39. Rokad, B. (2019). Machine Learning Approaches and Its Applications, DataDrivenInvestor URL: https://medium.datadriveninvestor.com/machine-learning-approaches-and-its-applications-7bfbe782f4a8 [Pristupljeno: 3.9.2021.]
40. Sample, I. (2020). What are deepfakes – and how can you spot them, *The Guardian* URL: https://www.theguardian.com/technology/2020/jan/13/what-are-deepfakes-and-how-can-you-spot-them [Pristupjeno 3.9.2021.]
41. Seljan, S.; Miloloža, I.; Pejić Bach, M. (2020). e-Government in European countries: gender and ageing digital divide. Interdisciplinary Management Research XVI. Barković, Dražen... [et al] (ur.). Osijek: Josip Juraj Strossmayer University of Osijek, Faculty of Economics in Osijek, 2020. str. 1581-1602
42. Seljan, S.; Dunđer, I. Machine Translation and Automatic Evaluation of English/Russian-Croatian. Proceedings of the International Conference "Corpus Linguistics - 2015". Zakharov, V. P. ; Mitrofanova, O. A. ; Khokhlova, M. V. (ur.). St. Petersburg, Rusija: St. Petersburg State University, 72-79.
43. Seljan, S.; Baretić, M.; Seljan, M.; Pejić Bach, M. (2020). Information assessment of hospital websites in Croatia: how to develop accountability standards? International journal of health planning and management, 35 (4), 4; 970-971 doi:10.1002/hpm.2975
44. Seljan, S.; Dunđer, I.; Stančić, H. (2017). Extracting terminology by language independent methods. Translation studies and translation practice : proceedings of the 2nd International TRANSLATA Conference 2014. Part 1 / Zybatow, Lew N. ; Stauder, Andy ; Ustaszewski, Michael (ur.). Frankfurt am Main: Peter Lang, 141-147.
45. Seljan, S.; Baretić, M.; Kučiš, V. (2014). Information Retrieval and Terminology Extraction In Online Resources for Patients with Diabetes. Collegium antropologicum, 38 (2014), 2; 705-710

46. Schmidhuber, J. (2015). Deep Learning, Scholarpedia, 10(11):32832 URL: http://www.scholarpedia.org/article/Deep_Learning [Pristupljeno 15.6.2021.]
47. *Sensity* URL: https://sensity.ai/reports/ [Pristupljeno: 1.9.2020.]
48. Slota, M. (2020). Strojno učenje prepoznavanja rukopisne numeracije, Sveučilište u Zagrebu, Filozofski fakultet, završni rad, 43 str.
49. Stewart, M. (2019). The Limitations of Machine Learning, TowardsDataScience URL: https://towardsdatascience.com/the-limitations-of-machine-learning-a00e0c3040c6 [Pristupljeno: 3.9.2021.]
50. Subotić, D. (2020). Primjena dubokog učenja, Strojarski fakultet Slavonski Brod, diplomski rad, 57 str.
51. Tikvica, A. (2019). Interoperabilnost servisa strojnog učenja različitih pružatelja usluga u oblacima, Sveučilište u Zagrebu, Fakultet organizacije i informatike, diplomski rad, 53 str.
52. Tyagi, N. (2021). 6 Major Branches of Artificial Intelligence (AI), Artificial Intelligence, analyticSteps URL: https://www.analyticssteps.com/blogs/6-major-branches-artificial-intelligence-ai [Pristupljeno 31.8.2021.]
53. Ujević, Andrijić, Ž., (2019). Umjetne neuronske mreže, *Osvježimo znanje*, Kem. Ind. 68 (5-6) 219–220 str.
54. *FaceSwap*, verzija 2.0 URL: https://faceswap.dev/ [Pristupljeno 25.6.2021.]
55. Luxand URL: https://www.luxand.com/facesdk/ [Pristupljeno 3.9.2021.]

Primjena alata dubokog učenja za prepoznavanje lica

Sažetak

Cilj ovog rada bio je prikazati postupak treniranja, prepoznavanja i zamjene lica primjenom alata za duboko učenje, koje predstavljaju najsuvremeniji pristup u području umjetne inteligencije i primjena neuronskih mreža prilikom učenja i definiranja lica, te ukazati na potencijalne stvarne prijetnje korištenja takve tehnologije, ali i pozitivne strane.

Rad se sastoji od teorijskog i praktičnog dijela. U teorijskom dijelu definirani su pojmovi strojno učenje i duboko učenje i ključni elementi i razlike. Prikazana je struktura i način rada neuronske mreže, te osnovni principi rada koji se koriste za duboko učenje. Naglasak rada je na primjenama dubokog učenja te su prikazane tehnike koje koriste razne aplikacije u kojima je implementirano duboko učenje za prepoznavanje lica.

U praktičnom dijelu rada provedeno je istraživanje primjenom alata za prepoznavanje lica. Računalni program *FaceSwap* primjenjuje princip dubokog učenja za stvaranje „dubokih lažnjaka“ (eng. *deepfakes*) u kojima algoritam uči glavne značajke lica te izvorna lica na slikama ili videozapisima zamjenjuje željenim licem neke druge osobe. Nakon prikaza sustava i analize načina rada, prikazan je praktičan dio zamjene lica u videozapisu te su na kraju prikazani rezultati. Posljednje poglavlje odnosi se na etičke principe i ukazuje na opasnosti i moguću zlouporabu te zaštitu od neprimjerene upotrebe.

Ključne riječi: duboko učenje, primjena, neuronske mreže, strojno učenje, učenje, prepoznavanje lica

Application of deep learning tools for face recognition

Abstract

The aim of this paper was to present the process of training, recognizing and replacing faces using deep learning tools, which represent the most modern approach in the field of artificial intelligence and neural networks in learning and defining faces, and point out potential real threats of using such technology. sides.

The paper consists of a theoretical and a practical part. In the theoretical part, the terms machine learning and deep learning and key elements and differences are defined. The structure and mode of operation of the neural network are presented, as well as the basic principles of operation used for deep learning. The emphasis of the paper is on the applications of deep learning and the techniques used by various applications in which deep learning for facial recognition is implemented are presented.

In the practical part of the paper, research was conducted using facial recognition tools. The computer program *FaceSwap* applies the principle of deep learning to create "*deep fakes*" in which the algorithm learns the main features of the face and replaces the original faces in pictures or videos with the desired face of another person. After showing the system and analyzing the mode, the practical part of the face replacement in the video is shown and finally the results are shown. The last chapter deals with ethical principles and points out the dangers and possible abuse and protection against inappropriate use.

Keywords: deep learning, application, neural networks, machine learning, learning, facial recognition