Sveučilište u Rijeci
University of Rijeka
http://www.uniri.hr

Polytechnica: Journal of Technology Education, Volume 7, Number 2 (2023)
Politehnika: Časopis za tehnički odgoj i obrazovanje, Svezak 7, Broj 2 (2023)

Politehnika
Polytechnica
https://politehnika.uniri.hr
cte@uniri.hr

DOI: https://doi.org/10.36978/cte.7.2.3

Prethodno priopćenje
Preliminary note
UDK: 004.85

Strojno učenje u uvjetima manje raspoloživosti podataka

Vedran Juričić
Filozofski fakultet
Sveučilište u Zagrebu
I. Lučića 3, 10000 Zagreb
vjuricic@ffzg.unizg.hr

Sažetak

Strojno učenje je predmet istraživanja brojnih znanstvenih i stručnih projekata, i važan sastavni dio sustava koji se koriste u medicini, bankarstvu, računalnoj sigurnosti, komunikaciji i brojnim drugim domenama. Jedno je od najaktivnijih područja istraživanja, s konstantnim napretkom i razvojem novih algoritama i pristupa, te poboljšanjem postojećih metoda. Značajan utjecaj na performanse modela strojnog učenja ima skup podataka nad kojim je napravljeno treniranje, odnosno kvaliteta podataka, ravnomjerna razdioba vrijednosti i veličina skupa. To predstavlja potencijalan problem kod metoda strojnog učenja koje zahtijevaju prethodno označene podatke, jer prikupljanje podataka može biti iznimno složeno, skupo i vremenski zahtjevno. U tom slučaju klasičan model strojnog učenja vrlo vjerojatno neće imati dobre performanse. Jedan od pristupa rješavanja ovog problema je primjena učenja prijenosom, u kojem model koristi skup podataka ne samo iz promatrane domene, već i iz druge, idealno srodne domene. U radu su simulirani uvjeti manje raspoloživosti skupa podataka, na kojem su analizirane performanse tri modela temeljena na neuronskim mrežama, od kojih se jedan temelji na prethodno istreniranom modelu. Opisan je postupak kreiranja skupova za treniranje i prezentirani su rezultati analize navedena tri modela s različitim veličinama skupova.

Ključne riječi: *strojno učenje; učenje prijenosom; klasifikacija; skup za treniranje; neuronske mreže.*

1 Uvod

Strojno učenje sustavima omogućuje djelovanje na inteligentan način, odnosno daje im mogućnost učenja i unaprjeđenja na temelju prethodnog iskustva bez promjene u arhitekturi i prilagodbe programskog koda (Sarker, 2021a). Danas se primjenjuje u gotovo svim domenama, poput znanosti, financija, bankarstva, sigurnosti, prijevoza, komunikacija i osiguranja.

Metode se, prema potrebnoj količini ljudskog nadzora, dijele u 4 kategorije: nadzirano (engl. supervised), nenadzirano (engl. unsupervised), polu-nadzirano (engl. semi-supervised) učenje i učenje podrškom (engl. reinforcement) (Sarker, 2021b). Nadzirano učenje pretpostavlja postojanje prethodno označenog skupa podataka, u kojem je svakom skupu vrijednosti ulaznih varijabli pridružena vrijednost izlazne varijable, odnosno varijable cilja. Na temelju vrste varijable cilja metode se dalje mogu podijeliti u dvije glavne potkategorije: klasifikacija i regresija. Kod klasifikacije ili razvrstavanja se radi o kvalitativnoj varijabli cilja i predviđanju diskretne vrijednosti, a kod regresije o kvantitativnoj varijabli cilja i predviđanju kontinuirane vrijednosti. Primjer je analiza cijena nekretnina na temelju kvadrature, lokacije, blizine javnog prijevoza i ostalih karakteristika. Ako je cijena izražena u brojkama, tada se radi o regresiji. Ako se cijena razdijeli u razrede, tada se radi o klasifikaciji.

Algoritmi nenadziranog učenja temelje se na neoznačenom skupu podataka, u kojem se pokušavaju pronaći skriveni uzorci i strukture. Najčešće rješavaju probleme grupiranja (engl. clustering), smanjenja dimenzionalnosti (engl. dimensionality reduction) i otkrivanja anomalija (engl. anomaly detection). Kod polu-nadziranog učenja se mali skup označenih podataka kombinira sa skupom neoznačenih. Može se koristiti za klasifikaciju zvučnih zapisa, tekstualnih dokumenata i sadržaja mrežnih stranica, odnosno u situacijama kada ne postoji ili se ne može dobiti velik broj označenih podataka. Učenje podrškom je, uz planiranje, jedan od pristupa slijednom donošenju odluka (Moerland, 2020), kod kojeg postoji interakcija između modela i okoline. Prijelaz iz jednog stanja u drugo se temelji na prethodno zadanom upravljanju (engl. policy) i ostalim parametrima, pri čemu se za svaki prijelaz dobiva nagrada, koja može biti pozitivna i negativna (Li, 2017).

Bez obzira na vrstu strojnog učenja i sam cilj, pristup je uglavnom jednak i sastoji se od tri koraka. Najprije se prikupljaju podaci nad kojima će se sustav učiti, odnosno nad kojima će se raditi treniranje modela. Općenito, što je više podataka dostupno, to će biti bolje performanse modela. Drugi korak je definiranje arhitekture i implementacija i treniranje modela. Zadnja faza je primjena treniranog modela nad novim podacima, kako bi oni kategorizirali ili kako bi se na temelju njih procijenile tražene vrijednosti (Molnar, 2020). Na performanse modela utječe odabir algoritma klasifikacije, gradijenta, vrijednosti hiperparametara, slojeva i niz drugih parametara, ali i skup podataka nad kojim je napravljeno treniranje. Brojni znanstveni radovi su fokusirani na poboljšanje kvalitete modela, a iznimno se malo radova orijentira na kvalitetu podataka i njezino poboljšanje (Jain i dr., 2020). Skupovi podataka imaju iznimnu važnost u strojnom učenju i predstavljali su ograničenje u razvoju algoritama i istraživanja (Paullada, 2021).

U nekim slučajevima postoje različita ograničenja, poput cijene, složenosti postupka i raspoloživog vremena, zbog kojih je vrlo teško ili skupo doći do potrebne količine kvalitetnih podataka i zbog čega model, bez obzira na arhitekturu, ne pokazuje optimalne rezultate.

U ovom se radu analizira model i metoda klasifikacije u uvjetima u kojima su dostupne iznimno male količine podataka. Analiza je najprije provedena nad najvećim mogućim skupom podataka, kako bi se utvrdile optimalne performanse modela. Nakon toga je napravljeno nekoliko analiza sa manjim skupovima podataka, kojima se broj elemenata uzastopno povećavao. U radu je opisan način dobivanja skupova podataka i korišteni modeli, a pokazuje se i mogućnost učenja prijenosom (engl. transfer learning) i njegov utjecaj na performanse.

2 Učenje prijenosom

U današnje doba velikih podataka, podatkovne znanosti, napredne analize, duboke analize itd., količina generiranih i dostupnih podataka je u stalnom porastu (Cao, 2017). Podatke ne stvaraju samo ljudi, već računala, pametni telefoni, mrežni i drugi elektronički uređaji. Postoje javno dostupni skupovi podataka koje se, uz eventualno navođenje autora ili druge uvjete i licence, mogu koristiti za analize, učenje, treniranje modela, usporedbu s vlastitim podacima itd. Npr. Kaggle (Kaggle: your machine learning and data science community, 2023) sadrži više od 250 tisuća skupova podataka, podijeljenih u nekoliko kategorija, koji se mogu pretražiti prema nazivu, ključnim riječima, veličini itd.

Iako postojeći skupovi vrlo vjerojatno nisu idealni za određeno istraživanje ili problem, mogu se iskoristiti kako bi se poboljšala učinkovitost modela strojnog učenja. Učenje prijenosom nastoji iskoristiti naučeno u jednoj (ishodišnoj) domeni za poboljšanje performansi sustava ili smanjenje potrebne veličine skupa podataka u ciljnoj domeni (Zhuang, 2020). Učenje prijenosom nije nužno uspješno, pogotovo ako se navedene dvije domene previše razlikuju i nemaju dovoljno zajedničkih karakteristika. Štoviše, korištenje podataka iz druge domene se čak može i negativno odraziti na model i smanjiti njegove performanse. Ovakva vrsta prijenosa se naziva negativan prijenos (Wang, 2019).

Učenje prijenosom može biti homogeno i heterogeno (Weiss, Khoshgoftaar, Wang, 2016). Kod homogenog učenja je prostor značajki ishodišne domene jednak prostoru značajki ciljne. Dakle, prostori imaju jednaku dimenzionalnost i vrijednosti atributa i oznaka, a mogu se razlikovati u razdiobama vrijednosti atributa. Razlika u razdiobama se negativno odražava na performanse modela, tako da se ova vrsta učenja fokusira na njezino smanjivanje (Shimodaira, 2000). Kod heterogenog učenja prostori značajki ishodišne i ciljne domene nije jednak, a moguće je da se uopće ne preklapaju. Metode kojima se rješava ovaj problem dijele se na simetrične (transformacije), kod kojih se oba prostora značajki preslikavaju u treći, zajednički prostor, i asimetrične, kod kojih se transformira ili prostor značajki ishodišne ili prostor značajki ciljne domene.

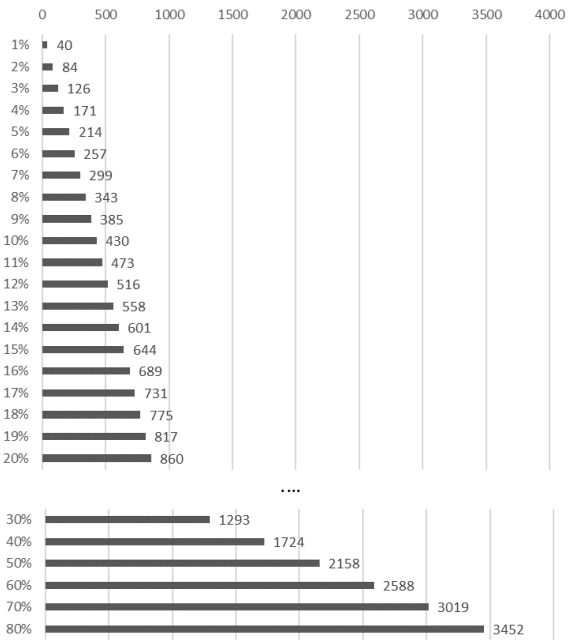
3 Istraživanje i analiza rada modela

Istraživanje u ovom radu je provedeno nad Flowers Recognition (Mamaev, 2021) skupom podataka, dostupnom na Kaggle mrežnom sjedištu, a sastoji se od 4317 slika cvjetova podijeljenih u 5 kategorija, dakle u prosjeku sadrži 850 slika po kategoriji. Slike su različitih veličina i niske kvalitete, rezolucije otprilike

320x240 piksela, zbog čega je ukupna veličina seta otprilike 230 MB.

3.1 Izrada skupa podataka

Iz gore opisanog skupa je najprije izdvojeno 20% (860) slika koje čine skup za provjeru (engl. test set) modela, pri čemu je korišten stratificirani slučajni uzorak pa je broj elemenata u pojedinoj klasi razmjeran njihovom broju u originalnom skupu. Preostalih 80% (3452) elementa čini skup za treniranje (engl. training set), odnosno model se u najboljem slučaju može trenirati s otprilike 700 elemenata po klasi, što je dovoljan broj da bi se postigli zadovoljavajući rezultati i relativno visoka točnost. Budući da je cilj rada promotriti ponašanje modela u uvjetima nedovoljne raspoloživosti podataka, model je treniran više puta nad mnogo manjim uzorcima. Prva serija je trenirana s 1% (40) elemenata, odnosno u prosjeku 8 elemenata po klasi. Druga serija je trenirana s 2%, odnosno 84 elementa. Broj elemenata se na taj način povećavao do ukupno 20%, a zatim se do 80% povećavao za 10%. Slika 1 prikazuje postotak elemenata u pojedinoj seriji.



Slika 1. Veličina pojedine serije treniranja modela

Model je treniran nad ukupno 26 serija, a treniranje je za svaku seriju provedeno 10 puta, odnosno uzorak nad kojem će se raditi je kreiran 10 puta, kako bi se umanjili eventualni efekti nastali zbog različitog formiranja slučajnog uzorka. U ostatku rada su korištene i prikazane aritmetičke sredine vrijednosti dobivenih u navedenih 10 ponavljanja.

Slike su minimalno pretprocesirane i nije korištena nijedna metoda osim skaliranja, kojom su sve slike svedene na istu veličinu, uz zadržavanje vizualnih značajki i semantike. Skaliranje je uobičajena metoda prilikom rada s neuronskim mrežama i uglavnom se uzima stalna veličina, radi jednostavnosti i efikasnosti (Hu, Shi, 2022). Slike su svedene na veličinu 224x224 piksela jer je s tom veličinom trenirana postojeća neuronska mreža koja će se koristiti u istraživanju i koja je opisana u ostatku rada.

3.2 Arhitektura modela

U sklopu rada su definirana i implementirana tri modela, koji su zasebno trenirani i evaluirani nad prethodno opisanim skupovima podataka.

Model A je realiziran na temelju dva jednostavnija modela koji su na Kaggle stranici pokazali vrlo dobre rezultate prilikom rada s Flowers Recognition skupom podataka. Arhitektura modela, odnosno neuronske mreže prikazana je u tablici 1, iz koje je vidljivo da se sastoji od 9 slojeva i sadrži više od 5.5 milijuna parametara koji se mogu trenirati (engl. trainable parameters). U prvih šest slojeva izmjenjuju se konvolucija (engl. convolution) i sažimanje maksimalnom vrijednošću (engl. max pooling) s različitim izlaznim oblicima. Slijede sloj ravnanja (engl. flatten) i dva sloja potpunog povezivanja (engl. dense).

Broj	Naziv	Izlazni oblik	Broj parametara
1	Konvolucija	222x222x16	448
2	Sažimanje maksimumom	111x111x16	0
3	Konvolucija	109x109x32	4640
4	Sažimanje maksimumom	52x52x32	0
5	Konvolucija	52x52x64	18496
6	Sažimanje maksimumom	26x26x64	0
7	Ravnanje	43264	0
8	Potpuno povezivanje	128	5537920
9	Potpuno povezivanje	5	645

Tablica 1. Arhitektura modela A

Model B je implementacija postojeće neuronske mreže MobileNet v2, čija je arhitektura detaljno opisana u radu Sandler i dr. (2018), a ovdje su navedena osnovna obilježja. Sastoji se od inicijalnog sloja pune konvolucije (224x224) nakon čega slijedi 19 slojeva rezidualnog uskog grla (engl. residual bottleneck), kojima se smanjuje broj parametara i kompleksnost izračuna, ali se zadržavaju slične karakteristike i performanse (He i dr., 2016). Nakon navedenih slojeva slijede sloj konvolucije, sažimanja prosječnom vrijednošću (engl. average pooling) i dodatan sloj konvolucije. Iako ima više slojeva od modela A, ovaj model ima 2.1 milijun parametara za treniranje.

Model C oslanja se na prethodno trenirani MobileNet v2 model, dostupan na TensorFlow Hub (TensorFlow Hub, 2023) mrežnom sjedištu. Model je treniran na ImageNet (ImageNet, 2021) skupu

podataka i sastoji se od više od 10 milijuna slika podijeljenih u 1000 razreda. Kako bi se dobila potrebna arhitektura i omogućila klasifikacija slika za istraživanje, na navedenu neuronsku mrežu je dodan sloj potpunog povezivanja s 5 izlaza. Model se, dakle, sastoji od dva sloja i sadrži velik broj parametara, od kojih je moguće trenirati samo 5010.

Tablica 2 prikazuje osnovne informacije o modelima. Zadnji sloj u sva tri modela je potpuno povezivanje i sastoji se od 5 neurona, a kao aktivacijska funkcija je korišten Softmax.

Model	Broj slojeva	Broj parametara
A	9	5.5 milijuna
B	23	2.1 milijuna
C	2	5010

Tablica 2. Osnovne informacije o modelima korištenima u istraživanju

4 Rezultati

Svaki od navedenih modela treniran je na ukupno 26 prethodno opisanih skupova podataka, a kroz svaki skup napravljeno je 50 prolaza (epoha). Korištena funkcija gubitka je kategorična unakrsna entropija (engl. categorical crossentropy), a optimizator Adam, adaptivna procjena momenta (engl. ADAptive Moment estimation). Kao mjera uspješnosti modela uzeta je točnost (engl. accuracy), dakle omjer ispravno klasificiranih elemenata u ukupnom broju elemenata.

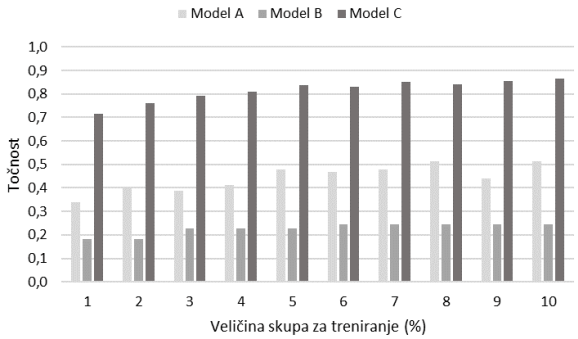
Tablica 3. prikazuje točnost i vrijeme treniranja modela nad cijelim skupom za treniranje (80%). Prikazana je najveća vrijednost točnosti u bilo kojoj od 50 etapa, a vrijeme treniranja je vrijeme potrebno za prolaz svih etapa.

Model	Točnost	Vrijeme treniranja (min)
A	0.71	3.75
B	0.74	321.34
C	0.89	6.17

Tablica 3. Rezultati prilikom testiranja nad cijelim skupom

Iz tablice je vidljivo da je točnost modela A gotovo jednaka točnosti modela B i razlika je otprilike 4%. Modeli imaju, kao što je prethodno opisano, vrlo različitu strukturu i kompleksnost. Unatoč gotovo jednakoj točnosti, za treniranje modela B je potrebno gotovo 10 puta više vremena nego za treniranje modela A. Model C pokazuje najveću točnost, 0.89, što je 25% veća vrijednost od modela A., dok je za njegovo treniranje bilo potrebno 65% više vremena. Rezultati u tablici 3. predstavljaju najbolje rezultate modela u optimalnim uvjetima, odnosno slučaj u kojem je za treniranje iskorišten sav skup za treniranje.

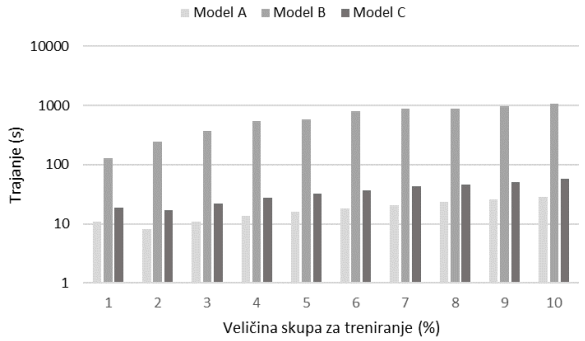
Cilj rada je promotriti rad modela u situacijama kada je veličina skupa za treniranje puno manja. Slika 2. prikazuje performanse modela s različitim veličinama skupa za treniranje. Vertikalna os prikazuje točnost, a horizontalna veličinu skupa za testiranje (od 1 do 10%). Iz grafa je vidljivo da na manjim skupovima za testiranje najslabije performanse ima model B. Prosječna točnost je 0.22 i neznatno se mijenja s povećavanjem skupa za testiranje. Točnost se od 1% do 10% povećala s 0.18 na samo 0.24.



Slika 2. Točnost modela u odnosu na veličinu skupa za treniranje (prvih 10 serija)

Performanse modela A su dvostruko bolje, odnosno prosječna točnost u prvih 10 serija je 0.44. Najveća točnost, 0.51, je zabilježena za 10. seriju. Model C je pokazao najbolje performanse. Njegova točnost je već u 1. seriji, kada je treniranje napravljeno samo s 1% (40) slika, bila 0.71, a u 10. seriji čak 0.87.

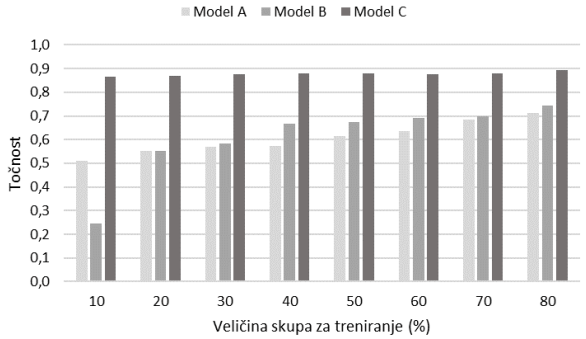
Slika 3. prikazuje vrijeme potrebno za treniranje navedenih modela. Horizontalna os prikazuje veličinu skupa za treniranje u postocima, a vertikalna trajanje treniranja u sekundama, u logaritamskom mjerilu.



Slika 3. Vrijeme potrebno za treniranje modela (prvih 10 serija)

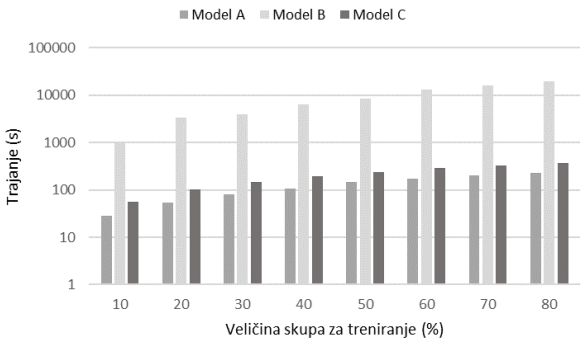
Iz grafa na slici 3. je vidljivo da vrijeme potrebno za treniranje raste s povećanjem skupa podataka, što je očekivano, ali i da model B zahtijeva najviše vremena za treniranje. Trajanje treniranja modela B je u 1. seriji gotovo 10 puta veće nego za druga dva modela. Za treniranje nad 10% (430) slika i u 50 epoha je bilo potrebno 17.5 minuta.

Slika 4. prikazuje točnost modela nad većim skupovima za treniranje, odnosno od 10% do 80%. Iz grafa je vidljivo da je točnost modela C najveća i da u cijelom promatranom intervalu neznatno raste (od 0.87 do 0.89). Točnost ostalih modela također raste, a najveći je rast vidljiv za model B (od 0.24 do 0.74). Točnost modela A i B je otprilike jednaka kad je treniranje provedeno nad 20% skupa, a nakon tog postotka model B pokazuje bolje rezultate.



Slika 4. Točnost modela u odnosu na veličinu skupa za treniranje (zadnjih 8 serija)

Međutim, iako model B pokazuje bolje rezultate nad većim skupovima podataka, vrijeme potrebno za njegovo treniranje je puno veće od ostalih modela. Treniranje je u prosjeku trajalo 80 puta duže od modela A, uz točnost veću za samo 0.03. Graf na slici 5. prikazuje trajanje testiranja nad većim skupovima podataka.



Slika 5. Vrijeme potrebno za treniranje modela (zadnjih 8 serija)

Na temelju rezultata se može zaključiti da je model A bolji od modela B. Prilikom treniranja s manjim skupom je pokazao bolje rezultate, odnosno imao je veću točnost uz manje trajanje treniranja. Kada je na raspolaganju bilo više podataka za treniranje, model B je ima neznatno veću točnost, uz puno veće trajanje treniranja. Model C pokazuje najbolje rezultate u oba slučaja. Iako je trajanje treniranja dvaput veće od trajanja treniranja modela A, u svim serijama ima najveću točnost. Najizraženija razlika u performansama je u već u 1. seriji, kada je treniranje provedeno sa samo 40 slika, pri čemu je točnost modela bila 0.71.

Modeli A i B pokazuju loše performanse sve dok se treniranje ne provede nad barem 70% skupa, pri čemu je točnost oba modela gotovo jednaka maksimalnoj vrijednosti, odnosno manja je za otprilike 5%. Točnost modela A je do 50% skupa samo 0.6, što je iznimno loše jer model koji klase pridružuje slučajnim odabirom ima očekivanu točnost 0.5. S druge strane, točnost modela C je bliska maksimalnoj vrijednosti već prilikom testiranja nad 5% skupa.

Iz rezultata je vidljivo da model C ima najmanje vrijeme testiranja i najveću točnost, što je posljedica same arhitekture neuronskih mreža. Mreže se sastoje od nekoliko slojeva koji na temelju ulaznih podataka određuju parametere s ciljem da se minimizira funkcija troška. Za određivanje navedenih parametara prvi sloj mreže koristi originalne podatke (u ovom istraživanju slike), dok ostali slojevi koriste izlaz iz prethodnog sloja. Zbog toga prvi sloj uči raspoznavati osnovne obrise, poput linija i jednostavnih krivulja, a svaki sljedeći uči raspoznavati sve kompleksnije oblike, uz ograničenje da broj neurona u zadnjem sloju mreže odgovara broju klasa u originalnim podacima. Kod učenja prijenosom se zadnji sloj postojeće mreže zamijenjuje s vlastitim, s odgovarajućim brojem neurona, dok svi ostali slojevi, odnosno sve ostalo što je mreža naučila raspoznavati, ostaju. Drugim riječima, za razliku od ostalih modela, model C koristi obrise i kompleksne oblike prethodno naučene na 10 milijuna ulaznih podataka, zbog čega pokazuje najbolje performanse i zbog čega se one minimalno mijenjaju s povećanjem skupa za treniranje.

5 Zaključak

U radu su analizirane performanse tri modela za klasifikaciju slika koji se temelje na konvolucijskim neuronskim mrežama. Modeli su trenirani s manjim i većim skupovima podataka, kako bi se utvrdila razlika u točnosti i trajanju cijelog postupka. Model koji je pokazao najlošije rezultate temelji se na postojećoj MobileNet v2 neuronskoj mreži jer je treniranje vrlo dugotrajno, a točnost nije mnogo veća od osnovnog modela s 9 slojeva.

Najbolje rezultate je pokazao model koji je koristio prethodno treniranu neuronsku mrežu, koja je trenirana na drugom skupu podataka. Uz neznatno duže trajanje treniranja od osnovnog modela, ovaj je model pokazao vrlo visoku točnost već u radu s minimalnim skupom podataka, odnosno kada je za treniranje korišteno samo 40 slika. Time je pokazana prednost učenja prijenosom, kod kojeg neuronska mreža ne treba učiti jednostavne i kompleksne oblike, već se podaci iz promatrane domene koriste za

minimalno podešavanje parametara i kombiniranje prethodno naučenih oblika u klase.

Jedan od mogućih daljnjih smjerova istraživanja je analiza utjecaja raznih tehnika pretprocesiranja na performanse sustava, odnosno utjecaja umjetnog povećanja skupa podataka (engl. augmentation). Tehnikama poput rotacije, translacije, promjene svjetline, boje i kontrasta moguće je povećati količinu podataka za treniranje i modelu omogućiti bolju generalizaciju. Također, moguće je razmotriti korištenje manje prikladnih prethodno treniranih neuronskih mreža i analizirati performanse korištenja mreže koja je trenirana na sasvim drugačijim slikama i skupovima podataka od onih koje je potrebno klasificirati.

Literatura

Cao, L. (2017). Data science: a comprehensive overview. *ACM Computing Surveys (CSUR)*, *50*(3), 1-42.

He, K., Zhang, X., Ren, S., Sun, J. (2016). Deep residual learning for image recognition. U *Proceedings of the IEEE conference on computer vision and pattern recognition* (str. 770-778).

Hu, C., Shi, W. (2022). Impact of Scaled Image on Robustness of Deep Neural Networks. *arXiv e-prints*, arXiv-2209.

ImageNet. (2021). https://www.image-net.org/

Jain, A., Patel, H., Nagalapatti, L., Gupta, N., Mehta, S., Guttula, S., Munigala, V. (2020). Overview and importance of data quality for machine learning tasks. U *Proceedings of the 26th ACM SIGKDD international conference on knowledge discovery & data mining* (str. 3561-3562).

Kaggle (2023). Kaggle: your machine learning and data science community. (2023). https://www.kaggle.com/

Li, Y. (2017). Deep Reinforcement Learning: An Overview. *arXiv e-prints*, arXiv-1701.

Mamaev, A. (2021). Flowers recognition. *Kaggle*. Preuzeto s https://www.kaggle.com/datasets/alxmamaev/flowers-recognition

Moerland, T. M., Broekens, J., Jonker, C. M. (2020). A Framework for Reinforcement Learning and Planning. U *ICAPS 2020: 30th International Conference on Automated Planning and Scheduling* (str. 50-52). Association for the Advancement of Artificial Intelligence (AAAI).

Molnar, C. (2020). *Interpretable machine learning*. Preuzeto s https://www.lulu.com

Paullada, A., Raji, I. D., Bender, E. M., Denton, E., Hanna, A. (2021). Data and its (dis) contents: A survey of dataset development and use in machine learning research. *Patterns, 2*(11).

Sandler, M., Howard, A., Zhu, M., Zhmoginov, A., Chen, L. C. (2018). Mobilenetv2: Inverted residuals and linear bottlenecks. U *Proceedings of the IEEE conference on computer vision and pattern recognition* (str. 4510-4520).

Sarker, I. H. (2021a). Machine learning: algorithms, Real-World applications and research directions. *SN Computer Science, 2*(3).

Sarker, I. H. (2021b). Deep Learning: a comprehensive overview on techniques, taxonomy, applications and research directions. *SN Computer Science*, *2*(6).

Shimodaira, H. (2000). Improving predictive inference under covariate shift by weighting the log-likelihood function. *Journal of Statistical Planning and Inference, 90*(2), 227–244.

TensorFlow Hub. (2023). TensorFlow. Preuzeto s https://www.tensorflow.org/hub

Wang, Z., Dai, Z., Póczos, B., Carbonell, J. (2019). Characterizing and avoiding negative transfer. U *Proceedings of the IEEE/CVF conference on computer vision and pattern recognition* (str. 11293-11302).

Weiss, K., Khoshgoftaar, T. M., Wang, D. (2016). A survey of transfer learning. *Journal of Big data*, *3*(1), 1-40.

Zhuang, F., Qi, Z., Duan, K., Xi, D., Zhu, Y., Zhu, H., He, Q. (2020). A comprehensive survey on transfer learning. *Proceedings of the IEEE*, *109*(1), 43-76.

Machine learning in conditions of low data availability

Abstract

Machine learning is the subject of numerous scientific and professional research projects and is an important component of systems used in medicine, banking, computer security, communications and numerous other fields. It is one of the most active areas of research with constant progress and development of new algorithms and approaches as well as improvement of existing methods. The performance of the machine learning model is significantly affected by the dataset used for training, i.e. the quality of the

data, the uniform distribution of values and the size of the set. This is a potential problem with machine learning methods that require pre-labelled data, as data acquisition can be extremely complex, expensive and time-consuming. In this case, the classical machine learning model will most likely not perform well. One approach to solve this problem is to apply transfer learning, where the model uses a dataset not only from the target domain but also from other, and ideally related domains. In the work, conditions with lower availability of datasets were simulated, under which the performance of three models was analyzed, one of which was based on a previously trained model. The process of creating training sets is described, and the results of analyzing the three models with different sized sets are presented.

Keywords: *machine learning; transfer learning; classification; training set; system performance*