Zaznavanje neustrezne poravnave obraznih slik iz predlog biometričnih modelov

Klemen Vovk[1], **Peter Rot**[1,2], **Klemen Grm**[2]

[1]*Univerza v Ljubljani, Fakulteta za računalništvo in informatiko, Večna pot 113, 1000 Ljubljana, Slovenija*
[2]*Univerza v Ljubljani, Fakulteta za elektrotehniko, Tržaška 25, 1000 Ljubljana, Slovenija*
E-pošta: kv4582@student.uni-lj.si

Povzetek

Uspešnost sodobnih modelov za razpoznavanje obrazov je tesno povezana z natančnostjo poravnave vhodnih obraznih slik, saj so ti modeli večinoma učeni na standardno poravnanih slikah. Neustrezno poravnane vhodne slike tem modelom obenem predstavljajo tihi način odpovedi, saj s programskega stališča pri obdelovanju podatkov ne pride do nikakršne napake. V prispevku sistematično preučimo vpliv različnih vrst in stopenj neustrezne poravnave (zasuk, premik, sprememba velikosti) na uspešnost razpoznave, pri čemer uporabimo standardni verifikacijski protokol LFW View 2 in modela AdaFace ter MagFace. Rezultati kažejo, da sta robustna na manjše napake poravnave, a odpovesta pri večjih odmikih. Nadalje raziskujemo možnost samodejne zaznave neustrezne poravnave še pred fazo odločanja v biometričnem sistemu. Ugotovimo, da obstaja močna korelacija med normo izluščene predloge in kakovostjo poravnave. Na tej osnovi naučimo preprost binarni razvrščevalnik, ki le iz norme predloge oceni ustreznost poravnave. Metoda je lahka za izvedbo, ne zahteva dodatnih vhodnih podatkov in omogoča zgodnje zaznavanje neustrezno poravnanih slik, kar omogoča samodejno sprožitev ponovnega zajema slike.

1 Uvod

V tem delu obravnavamo vpliv kakovosti poravnave obraznih slik na delovanje biometričnih sistemov za razpoznavanje obrazov. Sodobni modeli [1, 2] so običajno naučeni na poravnanih slikah, zato je uspešnost teh modelov tesno povezana z natančnostjo poravnave vhodnih slik.

Osredotočamo se na dva raziskovalna problema:

1. **P1:** Kako različne vrste in stopnje neustrezne poravnave (npr. razlike v velikosti, zasuku ali lokaciji obraza) vplivajo na uspešnost modelov za razpoznavanje obrazov?

2. **P2:** Ali je mogoče neustrezno poravnavo samodejno zaznati še pred fazo odločanja v biometričnem sistemu?

Na podlagi odgovorov na omenjena problema dobimo vpogled v robustnost modelov za razpoznavanje obrazov. Če se izkaže, da je nek model robusten na razlike v poravnavi oz. prisotnost le te, bi lahko poravnavo izpustili. V primeru, da je neustrezno poravnavo mogoče samodejno zaznati bi lahko preprečili nadaljnjo obdelavo takšnih slik ali sprožili korektivne postopke (npr. uporaba drugega modela za zaznavo obraza ali popravljanje transformacijske matrike za poravnavo) oz. ponovni zajem slike.

Za naslovitev P1 smo sistematično simulirali neustrezne poravnave v različnih oblikah (pokvarili smo jih z zasukom, premikom ali spreminjanjem velikosti) ter merili vpliv na uspešnost verifikacije. Za P2 smo raziskali korelacijo norme predlog modela za razpoznavanje obrazov in (ustreznosti) poravnave. Prispevka članka sta sledeča: 1) kvantitativna analiza vpliva različnih vrst in stopenj neustrezne poravnave na model za razpoznavanje obrazov in 2) predstavitev učinkovite metode za samodejno zaznavanje neustrezne poravnave, ki temelji na normi predlog modelov za razpoznavanje obrazov.

2 Sorodna dela

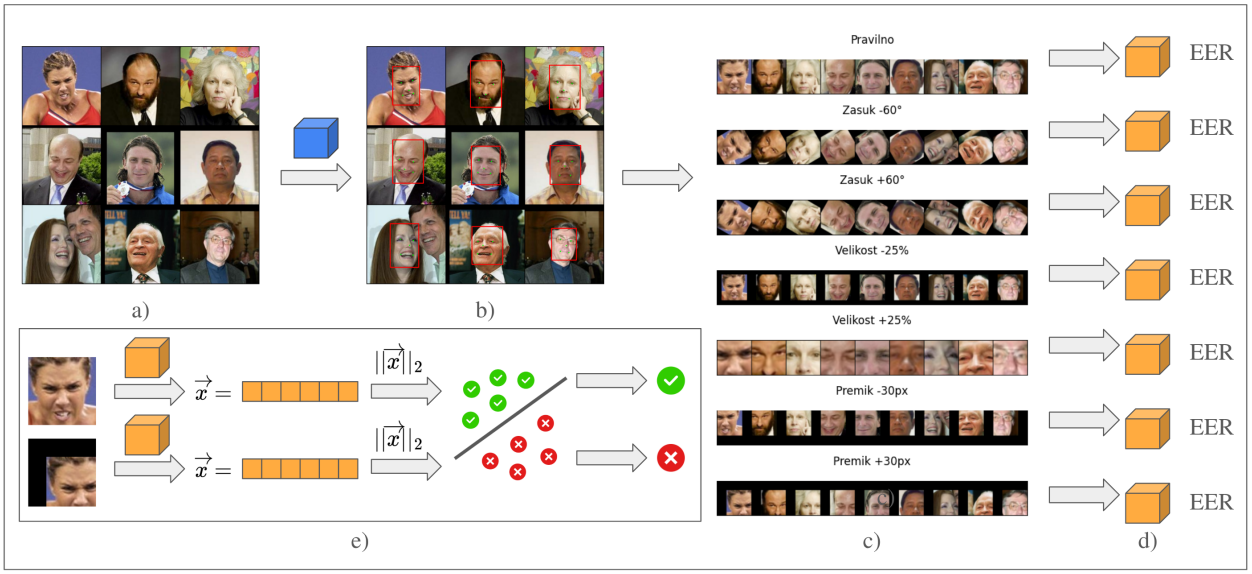
Problem občutljivosti sistemov za prepoznavanje obrazov na napake pri poravnavi je bil sistematično analiziran že leta 2004 s strani Shan et al. [3], kjer so pokazali, da že majhen odmik obraznih značilk (npr. oči) povzroči drastičen upad natančnosti pri klasičnih metodah. Kot rešitev so predlagali metodo, ki s podatkovnim ojačanjem (perturbacijami v ključnih točkah in posledično poravnavah) izboljša robustnost na poravnalne napake.

Kasneje Mehdipour Ghazi idr. [4] pokažejo, da tudi metode, ki temeljijo na globokih nevronskih mrežah kljub večji robustnosti ostajajo občutljive na napake poravnave - še posebej pri večjih perturbacijah ključnih točk.

Xu idr. [5] se osredotočajo na vpliv hiperparametrov, ki definirajo poravnavo. Predstavijo metodo FAPS, ki išče optimalne poravnalne parametre (velikost izreza in vertikalna lokacija) in na njih uči ter ocenjuje globoke modele. Z rezultati na različnih podatkovnih zbirkah pokažejo, da FAPS presega ročno zasnovane poravnave ter izboljša natančnost prepoznavanja.

Poravnava obrazov tako danes ostaja standardna predobdelava v sistemih za prepoznavanje obrazov. Du idr. [6] v svojem pregledu biometričnih sistemov poudarijo, da poravnava bistveno vpliva na kakovost izluščenih predlog, saj zagotavlja konsistentno lokacijo obraznih značilk in zmanjšuje znotrajrazredne variacije. Podobno Onaran idr. [7]

Raziskava financirana s strani ARIS projekta J2-50069 in ARIS programa P2-0250.



Slika 1: **Metodologija za simulacijo, ocenjevanje vpliva na uspešnost modelov za razpoznavanje in samodejno zaznavo neustrezne poravnave obraznih slik.** a) Obrazne slike iz podatkovne zbirke LFW. b) Na vsaki sliki z modelom za zaznavo obrazov RetinaFace zaznamo obraz in pet ključnih točk (središči oči, konico nosu ter koti ustnic), na podlagi katerih izvedemo poravnavo. c) V ocenjeno transformacijo sistematično vnesemo motnje (npr. sprememba velikosti, zasuk ali premik), s čimer za vsak tip motnje ustvarimo različico podatkovnega nabora LFW. d) Na vsaki različici ocenimo uspešnost modelov za razpoznavanje obrazov AdaFace in MagFace po standardnem protokolu LFW View 2. e) Glede na ocenjen vpliv posameznih motenj naučimo plitek razvrščevalnik, ki na podlagi norme predloge oceni ali gre za ustrezo poravnavo ali ne.

analizirajo vpliv poravnave na ocenjevanje kakovosti obraznih slik in ugotavljajo, da se številni podatkovni nabori implicitno zanašajo na že poravnane slike tako v fazi učenja kot testiranja.

3 Metodologija

V tem poglavju podrobno opišemo uporabljene podatkovne zbirke, modele, mere uspešnosti ter eksperimentalne postopke za analizo vpliva neustrezne poravnave in razvoj metode za njeno samodejno zaznavanje. Oris celotne metodologije prikazuje slika 1.

3.1 Podatkovna zbirka in merjenje uspešnosti modela za razpoznavanje obrazov

Za vrednotenje uspešnosti smo uporabili protokol View 2 podatkovne zbirke LFW [8], ki vključuje 10-kratno prečno preverjanje na 6000 parih slik. Naloga je verifikacija, tj. ugotavljanje, ali je na obeh slikah v paru ista identiteta.

Uspešnost merimo z uravnoteženo napako (angl. *Equal Error Rate*, EER), ki označuje točko, kjer sta deleža lažno pozitivnih in lažno negativnih primerov enaka, formalno:

$$\begin{aligned} \mathrm{EER} &= \mathrm{FAR}(\tau^*) = \mathrm{FRR}(\tau^*), \\ \mathrm{FAR}(\tau) &= \frac{\mathrm{FP}}{\mathrm{FP}+\mathrm{TN}}, \\ \mathrm{FRR}(\tau) &= \frac{\mathrm{FN}}{\mathrm{FN}+\mathrm{TP}}, \end{aligned}$$

kjer je τ^* odločitveni prag, pri katerem velja $\mathrm{FAR}(\tau^*) = \mathrm{FRR}(\tau^*)$, TP, TN, FP, FN so deleži dejanskih pozitivnih in negativnih ter lažno pozitivnih in negativnih primerov.

3.2 Zaznavanje in poravnava obrazov

Za zaznavanje obrazov uporabljamo model Retinaface [9], ki za poljubno vhodno sliko vrne okvir, oceno zaupanja, da je v okviru obraz in 5 ključnih točk (središči oči, konica nosu, levi in desni kot ustnic). Na podlagi zaznanih in referenčnih ključnih točk lahko ocenimo afino transformacijo za poravnavo obraza (npr. z RANSAC [10]). V primeru, da zaznane ključne točke niso natančne lahko ocenjena transformacija povzroči neustrezno poravnavo.

3.3 Razpoznavanje obrazov

Uporabljamo vnaprej naučena modela AdaFace [2] in MagFace [1], ki iz poravnanih slik izluščita 512-dimenzionalne vektorje (predloge). Verifikacijo izvedemo s primerjavo kosinusne podobnosti med predlogama, odločitveni prag pa določimo na učni množici v vsakem krogu preverjanja.

3.4 Simulacija neustrezne poravnave

Na pravilno poravnane slike smo sistematično vnesli naslednje motnje (po eno hkrati):

- **Velikost:** poravnano sliko povečujemo ali zmanjšamo okoli njenega središča. Stopnjo spremembe definiramo kot $s \in [-100\%, +200\%]$.
- **Zasuk:** poravnano sliko zasukamo okoli njenega središča za kot $\theta \in [-180, 180]$
- **Premik:** poravnano sliko premaknemo po negativni diagonali za $t \in [-110px, +110px]$.

Za vsako stopnjo motnje smo pripravili ločeno različico podatkovnega nabora LFW, pri čemer smo posamezno vrsto motnje (zasuk, premik, spremembo velikosti) postopoma stopnjevali. Stopnjevanje smo nadaljevali

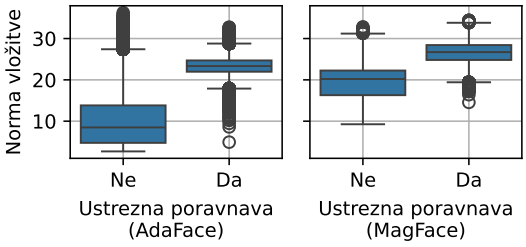
do točke, ko je uspešnost izbranega modela za razpoznavanje obrazov (AdaFace oziroma MagFace) po protokolu LFW View 2 dosegla raven naključnega ugibanja, tj. $EER = 50\%$. Za vsako stopnjo motnje smo izvedli 10-kratno prečno preverjanje, s čimer smo ocenili vrednost EER in kvantificirali negotovost rezultatov.

3.5 Samodejna zaznava neustrezne poravnave

Naša hipoteza je, da se kakovost poravnave obraza odraža v značilnostih predloge, ki jo generira model za razpoznavanje obrazov.

Na podlagi opažene korelacije med L_2 normo predlog in kakovostjo poravnave (glej sliko 2) smo naučili preprost binarni razvrščevalnik (npr. logistično regresijo ali plitek MLP), ki na osnovi norme odloča, ali je poravnava ustrezna. Za učenje razvrščevalnika smo potrebovali zlati standard, tj. označene primere ustreznih in neustreznih poravnav, ki smo jih določili empirično: za ustrezno poravnane smo šteli tiste različice naborov LFW, pri katerih je bila uspešnost razpoznavanja znatno slabša (vse različice, kjer je $EER > 0.5\%$ po protokolu View2, kot opisano v poglavju 3.1). Postopek izvedemo ločeno za predloge in norme predlog posameznega modela za razpoznavanje obrazov.

Uspešnost razvrščevalnika ocenimo z desetkratnim prečnim preverjanjem, pri čemer pazimo, da posamezne različice LFW ne delimo med učnim in testnim delom, ter da sta pozitivni in negativni razred v vsakem krogu uravnotežena. Negativni razred sestavimo tako, da izberemo enako število različic LFW kot v pozitivnem razredu, pri čemer prednostno izbiramo najmanjše stopnje motenj. Uspešnost ocenjujemo z običajnimi metrikami za binarno razvrščanje (točnost, natančnost, priklic, F1 in AUC), negotovost pa kvantificiramo s standardnim odklonom metrik prek vseh krogov prečnega preverjanja.

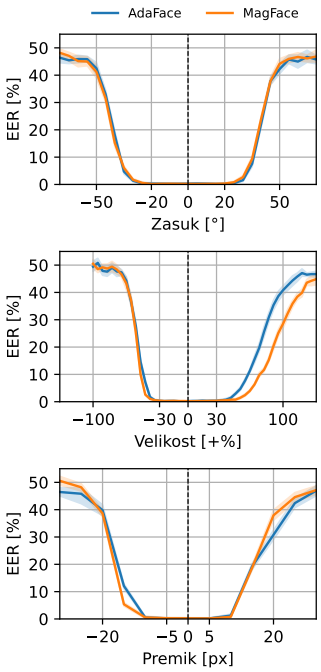


Slika 2: **Korelacija norme predlog in ustreznosti poravnave.** Predloge neustrezno poravnanih slik imajo manjše norme od predlog poravnanih slik za modela AdaFace in MagFace.

4 Rezultati

Kot odgovor na P1 na sliki 3 prikažemo vpliv vnosa opisanih motenj poravnave na uspešnost modelov AdaFace in MagFace. Oba modela se v uspešnosti podobno odzivata na motnje v poravnavi: robustna sta na manjše motnje v poravnavi (zasuk do ± 20, sprememba velikosti do $\pm 30\%$ in premik do $\pm 5px$).

Skupno pripravimo 176 različic nabora LFW z različnimi vrstami in stopnjami motenj. Za zlati standard označimo 23 ustrezno in 153 neustrezno poravnanih različic[1] (od teh jih izberemo 23 z najmanjšo jakostjo motnje).



Slika 3: **Vpliv tipa in stopnje motnje na uspešnost modelov za razpoznavanje obrazov na LFW View 2.** Zaradi preglednosti grafe odrežemo na obeh straneh, ko EER doseže 50%.

Ugotovimo tudi, da je neustrezno poravnavo možno samodejno zaznati pred fazo odločanja (P2): rezultati razvrščevalnikov za zaznavanje neustrezne poravnave so prikazani v tabeli 1. Norme predlog so učinkovit približek kakovosti poravnave. Relativno visoki standardni odkloni pri nekaterih metrikah, zlasti natančnosti, kažejo na opazno negotovost modelov. To pripišemo pristranskosti pri vzorčenju negativnega razreda, saj se v posameznih krogih prečnega preverjanja v testni množici lahko znajdejo izključno bolj pokvarjene različice LFW, ki jih je lažje razvrstiti in posledično umetno zvišajo uspešnost v teh krogih. To potrdijo tudi matrike zamenjav prikazane na sliki 4.

5 Zaključek

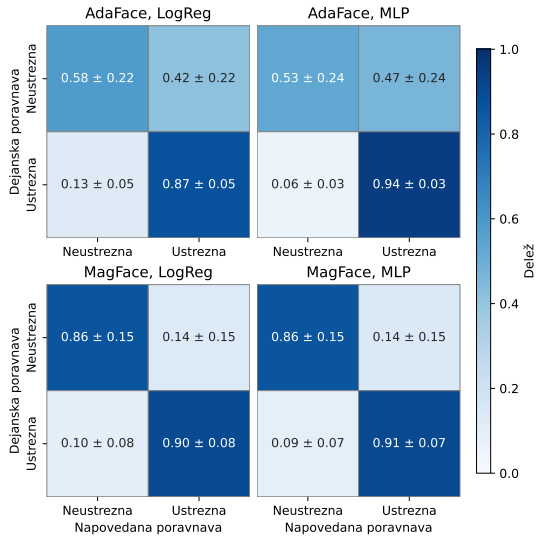
V prispevku smo obravnavali vpliv različnih kakovosti poravnave obraznih slik na uspešnost modelov za razpoznavanje obrazov. Ugotovili smo, da so modeli razmeroma odporni na manjše napake poravnave, a večje motnje močno znižajo uspešnost.

Empirično ugotovimo, da obstaja korelacija med normo predloge in kakovostjo poravnave. Ta lastnost omogoča konstrukcijo preprostih razvrščevalnikov, ki samo na podlagi norme ocenijo ustreznost poravnave. Napovedi o ustreznosti poravnave lahko uporabimo kot indikator za

[1] v primeru, da je različica LFW z isto vrsto in stopnjo motnje označena kot ustrezno poravnana pri enem in neustrezno poravnana pri drugem modelu, jo za zlati standard označimo kot neustrezno poravnano. Takšne so bile 3 različice.

Tabela 1: **Uspešnost razvrščevalnikov za zaznavanje neustrezne poravnave obraza na podlagi značilk različnih modelov za razpoznavanje obrazov (AdaFace in MagFace).** Primerjamo dva razvrščevalnika (logistična regresija in MLP s skritim slojem velikost 100 in ReLU aktivacijsko funkcijo) ter dva tipa vhodnih značilk: predloge in zgolj njihove L_2 norme. Rezultati so podani kot povprečje in standardni odklon metrik desetkratnega prečnega preverjanja, izraženi v obliki vrednost$_{\pm\text{odklon}}$.

Razvrščevalnik	Model	Značilke	Točnost ↑	Natančnost ↑	Priklic ↑	F1 ↑	AUC ↑
LogReg	AdaFace	predloge	$0.90_{\pm 0.06}$	$0.88_{\pm 0.14}$	$0.93_{\pm 0.04}$	$0.90_{\pm 0.07}$	$0.97_{\pm 0.04}$
MLP	AdaFace	predloge	$0.96_{\pm 0.06}$	$0.96_{\pm 0.09}$	$0.96_{\pm 0.08}$	$0.95_{\pm 0.06}$	$1.00_{\pm 0.01}$
LogReg	AdaFace	norme predlog	$0.74_{\pm 0.10}$	$0.70_{\pm 0.17}$	$0.87_{\pm 0.06}$	$0.76_{\pm 0.12}$	$0.74_{\pm 0.16}$
MLP	AdaFace	norme predlog	$0.76_{\pm 0.10}$	$0.69_{\pm 0.18}$	$0.94_{\pm 0.03}$	$0.79_{\pm 0.13}$	$0.77_{\pm 0.15}$
LogReg	MagFace	predloge	$0.85_{\pm 0.07}$	$0.83_{\pm 0.17}$	$0.89_{\pm 0.04}$	$0.85_{\pm 0.09}$	$0.93_{\pm 0.07}$
MLP	MagFace	predloge	$0.95_{\pm 0.06}$	$0.95_{\pm 0.10}$	$0.96_{\pm 0.08}$	$0.95_{\pm 0.06}$	$0.99_{\pm 0.02}$
LogReg	MagFace	norme predlog	$0.88_{\pm 0.09}$	$0.87_{\pm 0.14}$	$0.90_{\pm 0.09}$	$0.88_{\pm 0.09}$	$0.95_{\pm 0.06}$
MLP	MagFace	norme predlog	$0.88_{\pm 0.09}$	$0.87_{\pm 0.14}$	$0.91_{\pm 0.08}$	$0.88_{\pm 0.08}$	$0.95_{\pm 0.06}$



Slika 4: **Povprečni matriki zamenjav za razvrščevalnika na podlagi norm AdaFace in MagFace predlog.** Matrike so povprečene prek vseh krogov 10-kratnega prečnega preverjanja za posamezen razvrščevalnik. Negotovost rezultatov kvantificiramo s standardnim odklonom deleža dejanskih in lažnih pozitivnih oz. negativnih primerov.

ponovni zajem slike in tako preprečimo nadaljnjo obdelavo neustrezno poravnanih obraznih slik.

Metoda je lahka za izvedbo in uporablja izključno podatke, ki so že na voljo v biometričnem sistemu. V prihodnje načrtujemo razširitev metode na druge zbirke in modele, ter preučitev povezave med normo predloge in drugimi vrstami degradacije slike (npr. zamegljenost, osvetlitev). Raziskali bi tudi nekaj metod za vizualizacijo odločitev modelov za razpoznavanje obrazov v primeru neustrezne poravnave (npr. integrirani gradienti [11]).

Literatura

[1] Qiang Meng, Shichao Zhao, Zhida Huang, and Feng Zhou. Magface: A universal representation for face recognition and quality assessment. In *Proceedings of the IEEE/CVF conference on computer vision and pattern recognition*, pages 14225–14234, 2021.

[2] Minchul Kim, Anil K Jain, and Xiaoming Liu. Adaface: Quality adaptive margin for face recognition. In *Proceedings of the IEEE/CVF conference on computer vision and pattern recognition*, pages 18750–18759, 2022.

[3] Shiguang Shan, Yizheng Chang, Wen Gao, Bo Cao, and Peng Yang. Curse of mis-alignment in face recognition: problem and a novel mis-alignment learning solution. In *Sixth IEEE International Conference on Automatic Face and Gesture Recognition, 2004. Proceedings.*, pages 314–320. IEEE, 2004.

[4] Mostafa Mehdipour Ghazi and Hazim Kemal Ekenel. A comprehensive analysis of deep learning based representation for face recognition. In *Proceedings of the IEEE conference on computer vision and pattern recognition workshops*, pages 34–41, 2016.

[5] Xiaqing Xu, Qiang Meng, Yunxiao Qin, Jianzhu Guo, Chenxu Zhao, Feng Zhou, and Zhen Lei. Searching for alignment in face recognition. In *Proceedings of the AAAI Conference on Artificial Intelligence*, volume 35, pages 3065–3073, 2021.

[6] Hang Du, Hailin Shi, Dan Zeng, Xiao-Ping Zhang, and Tao Mei. The elements of end-to-end deep face recognition: A survey of recent advances. *ACM computing surveys (CSUR)*, 54(10s):1–42, 2022.

[7] Eren Onaran, Erdi Sarıtaş, and Hazım Kemal Ekenel. Impact of face alignment on face image quality. *arXiv preprint arXiv:2412.11779*, 2024.

[8] Gary B Huang, Marwan Mattar, Tamara Berg, and Eric Learned-Miller. Labeled faces in the wild: A database forstudying face recognition in unconstrained environments. In *Workshop on faces in'Real-Life'Images: detection, alignment, and recognition*, 2008.

[9] Jiankang Deng, Jia Guo, Evangelos Ververas, Irene Kotsia, and Stefanos Zafeiriou. Retinaface: Single-shot multilevel face localisation in the wild. In *Proceedings of the IEEE/CVF conference on computer vision and pattern recognition*, pages 5203–5212, 2020.

[10] Martin A Fischler and Robert C Bolles. Random sample consensus: a paradigm for model fitting with applications to image analysis and automated cartography. *Communications of the ACM*, 24(6):381–395, 1981.

[11] Mukund Sundararajan, Ankur Taly, and Qiqi Yan. Axiomatic attribution for deep networks. In *International conference on machine learning*, pages 3319–3328. PMLR, 2017.