Verifikacija potpisa

1st Zrinka Pećanić
Fakultet elektotehnike i računarstva
Zagreb, Croatia
zrinka.pecanic@fer.hr

2nd Ana Vladić
Fakultet elektotehnike i računarstva
Zagreb, Croatia
ana.vladic@fer.hr

3rd Ivana Krišto
Fakultet elektotehnike i računarstva
Zagreb, Croatia
ivana.kristo@fer.hr

4th Lucija Marinčić
Fakultet elektotehnike i računarstva
Zagreb, Croatia
lucija.marincic@fer.hr

5th Matej Lopotar
Fakultet elektotehnike i računarstva
Zagreb, Croatia
matej.lopotar@fer.hr

***Abstract*—Cilj ovog rada bio je proučiti i implementirati metode verifikacije potpisa kao jedne od najraširenije i najprihvaćenije metode biometrike. U tu svrhu korištene su konvolucijske neuronske mreže (eng. Convolutional Neural Networks, CNN) za ekstrakciju značajki čiji su se razultati koristili dalje u klasifikaciji metodama kao što su algoritam slučajnih šuma (eng. Random Forest, RF) i metoda potpornih vektora (eng. Support Vector Machines, SVM), i alternativna metoda histograma orijentiranih gradijenata (eng. Histogram Oriented Gradients, HOG). Dobiveni rezultati su uspoređeni po standardnim metrikama kao što su točnost, preciznost i odziv.**

***Index Terms*—potpis, verifikacija, biometrika, konvolucija, neuronske mreže, ekstrakcija, analiza slike, obrada slike, značajke, klasifikacija, regresija, histogrami, gradijent**

I. Uvod

Biometrijski sustavi bave se prepoznavanjem pojedinca na temelju njegovih fizičkih karakteristika (otisak prsta, lice, šarenica) ili karakteristika ponašanja (govor, potpis). Biometrijska karakteristika treba biti univerzalna (svaka osoba je ima), jedinstvena (ne postoje dvije osobe s jednakom karakteristikom), nepromjenjiva i lako prikupljiva. Verifikacijom biometrijski sustav utvrđuje odgovara li stvarni identitet osobe onom identitetu s kojim se ta osoba predstavlja. Poželjna svojstva biometrijskog sustava su točnost, financijska isplativost, brzina i prihvatljivost od strane korisnika. [3] Prednosti potpisa kao biometrijske karakteristike je to što je potpis opće prihvaćeno sredstvo verifikacije pojedinca i ima svoje pravno značenje. Način prikupljanja potpisa nije invazivan i ljudi su naviknuti na njegovu upotrebu jer se u današnje vrijeme potpisi koriste za većinu stvari. Sustav za verifikaciju potpisa (engl. Handwritten Signature Verification, HSV) klasificira ulazni potpis kao ispravni potpis ili krivotvoreni potpis. [2] Ovisno o načinu prikupljanja potpisa, sustavi za verifikaciju potpisa mogu biti statički (engl. offline) ili dinamički (engl. online). Statički sustavi prikupljaju gotove potpise u obliku digitalne slike nakon što je proces potpisivanja završio. Dinamički sustavi potpise prikupljaju pomoću uređaja koji bilježe promjenu pozicije olovke u vremenu, a dodatno mogu mjeriti i elemente poput nagiba, brzine, ubrzanja i jačine pritiska olovke. [3] Ovisno o broju modela, sustav za verifikaciju potpisa može se sastojati od jednog modela koji klasificira potpise svih pojedinaca (engl. writer-independent system) ili od po jednog modela za svakog pojedinca (engl. writer-dependent system). Glavni izazovi su velika varijabilnost unutar klasa (potpisi jednog pojedinca imaju veliku varijabilnost u odnosu na fizičke karakteristike poput otiska prsta, mijenjaju se ovisno o psihofizičkom stanju pojedinca i uvjetima u kojima dolazi do potpisivanja), mala varijabilnost između pravih potpisa i kvalitetnih krivotvorina, mala količina dostupnih primjeraka potpisa za pojedinca kad je riječ o primjeni u stvarnom životu. Problem predstavlja prikupljanje primjera kvalitetnih krivotvorina. Mogu se promatrati tri vrste krivotvorina: nasumične krivotvorine (krivotvoritelj daje svoj nepromijenjen potpis), jednostavne krivotvorine (krivotvoritelj potpisuje odgovarajuće ime, ali ne pokušava imitirati ispravni potpis) i kvalitetne krivotvorine (krivotvoritelj uvježbava potpisivanje s ciljem imitiranja statičkih i dinamičkih karakteristika ispravnog potpisa). [3]

II. Pregled literature

Rad u literaturi [1] koji koristi isti skup podataka kojim se bavi i ovaj rad ima nešto drugačiji pristup, ali isti cilj: verifikacija potpisa. Korišteni su podaci koji su sadržavali realistične potpise različitih ljudi na latinici, ali i na kineskom. Podaci su podijeljeni na dva dijela: statičke i dinamičke podatke. Statički podaci za trening sadrže potpise 10 autora. U podacima se nalazi 240 ispravnih potpisa te 123 krivotvorena. U statičkim podacima za testiranje nalaze se potpisi 54 autora s tim da je 648 ispravnih i 638 krivotvorenih potpisa. Potom je 6 različitih institucija predložilo 13 rješenja problema, neke institucije samo za statičke podatke, neke samo za dinamičke, a neke za oboje. Princip ispitivanja točnosti potpisa temeljio se na usporedbi potpisa s 12 referentnih koje su ispitanici napisali prije. Rezultati su, naravno, bili različiti jer su se korišteni algoritmi razlikovali. Jedan od češćih klasifikatora bio je stroj potpornih vektora (engl. Support Vector Machine, SVM) kao i k najbližih susjeda (engl. k Nearest Neighnors, kNN). Isto tako, jedna od "popularnijih" metoda bile su metode temeljene na geometriji. Takve metode analiziraju oblik i prostornu strukturu potpisa kako bi identificirali karakteristične značajke i razlikovali autentične potpise od krivotvorenih. Osim ovog

članka, kao primjer rješenja problema korišten je i *open source* materijal [4] koji sadrži slični skup podataka i 20-ak rješenja koja imaju isti pristup problemu kao i ovaj rad.

III. Opis rješenja projektnog tima

Cilj projekta bio je napraviti ekstrakciju značajki iz slika potpisa i naučiti model koji će dani par potpisa klasificirati kao par ispravnih potpisa (oznaka 0) ili lažno predstavljanje (oznaka 1). Za učenje i evaluaciju modela korišten je dio ICDAR skupa podataka, preciznije podskup nizozemskih *offline* potpisa. Za svaku od 69 osoba u skupu postoje ispravni i krivotvoreni potpisi. Skup podataka podijeljen je na skup za učenje (osobe 1-44), validaciju (osobe 45-54) i testiranje (osobe 55-69). Predloženi sustav za verifikaciju potpisa sastoji se od ekstrakcije značajki i klasifikacije. Ekstrakcijom značajki iz slike dobiva se reprezentacija slike koja služi kao ulaz u klasifikator. Klasifikator uči verificirati dani par potpisa. Primjeri za učenje sastoje se od dvije slike potpisa i oznake 0 (ispravni potpisi, odnosno dva potpisa iste osobe) ili 1 (lažno predstavljanje, odnosno jedan potpis je krivotvorina). Primjer pravog i krivotvorenog popisa prikazan je na slici 1. Ulaz u klasifikator je 256 značajki prve slike i 256 značajki druge slike, ukupno 512 značajki. Klasifikatori su učeni na primjerima sastavljenih od slika iz skupa za učenje, a testirani na primjerima sastavljenih od slika iz skupa za testiranje. Korišteni su sljedeći klasifikatori biblioteke Scikit-learn: LogisticRegression, SGDClassifier, svm.SVC i RandomForestClassifier.

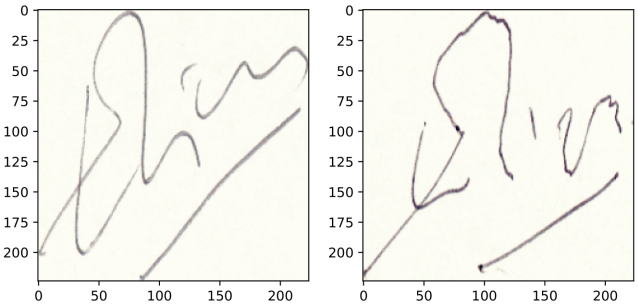

Fig. 1. Primjer ispravnog i krivotvorenog potpisa

Za ekstrakciju značajki korištene su dvije metode: prednaučeni konvolucijski model VGG-16 i histogrami orijentiranih gradijenata. Korištene su biblioteke TensorFlow, Scikit-learn i Scikit-image programskog jezika Python.

A. VGG-16

VGG-16 je konvolucijski model naučen za zadatak klasifikacije slika. Da bi služio kao ekstraktor značajki u našem sustavu, model je dodatno naučen pomoću primjera iz skupa za učenje i validaciju. Uče se samo posljednja 4 sloja VGG-16 modela. Na kraj VGG-16 modela dodani su potpuno povezani sloj s 256 neurona i ReLU aktivacijskom funkcijom te izlazni potpuno povezani sloj od 2 neurona i softmax aktivacijskom funkcijom. Slojevi izrađenog modela prikazani su u Tablici I. Izrađen model naučen je na zadatku klasifikacije slike u jednu od dvije klase: 1) pravi potpis, 2) krivotvoreni potpis. Za učenje i validaciju ovog modela korištene su slike potpisa iz skupa za učenje i validaciju označene oznakama za pravi/krivotvoreni potpis. Tijek učenja kroz 14 epoha grafički je prikazan na slikama 2 i 3 . Korišten je gubitak unakrsne entropije, optimizacijski postupak Adam i stopa učenja 2e-5. Naučeni model služi kao ekstraktor značajki svih slika iz skupa podataka. Za svaku sliku kao reprezentacija se uzima izlaz predzadnjeg potpuno povezanog sloja, dakle, svaka slika reprezentira se sa 256-dimenzionalnim vektorom značajki.

TABLE I
Slojevi i dimenzije ekstraktora značajki

Sloj	Izlaz
VGG16	7x7x512
Flatten	25088
Dense	256
Droput(0.5)	256
Dense	2

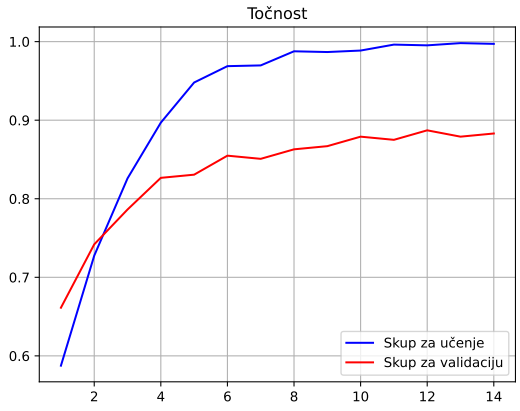

Fig. 2. Grafički prikaz točnosti na skupu za učenje i validaciju tijekom učenja ekstraktora značajki

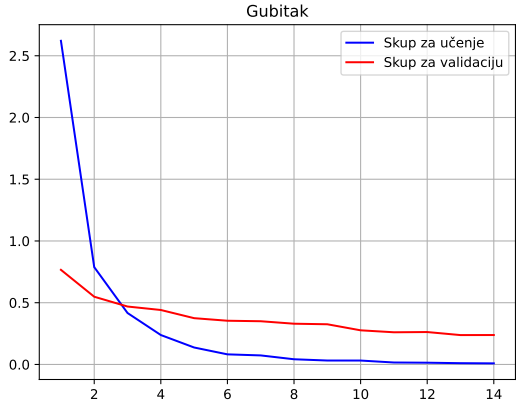

Fig. 3. Grafički prikaz gubitka na skupu za učenje i validaciju tijekom učenja ekstraktora značajki

B. Histogrami orijentiranih gradijenata (HOG)

Ovom metodom slika se dijeli na dijelove, za svaki od kojih se računa histogram orijentiranih gradijenata. Histogrami pokazuju frekvenciju pojavljivanja pojedinih smjerova gradijenata. HOG značajke za svaku sliku su dobivene funkcijom skimage.feature.hog() uz sljedeće parametre: *orientations*=8, *pixels_per_cell*=(16,16), *cells_per_block*=(4, 4). Vizualni prikaz HOG značajki jedne slike iz skupa prikazan je na slici 4.

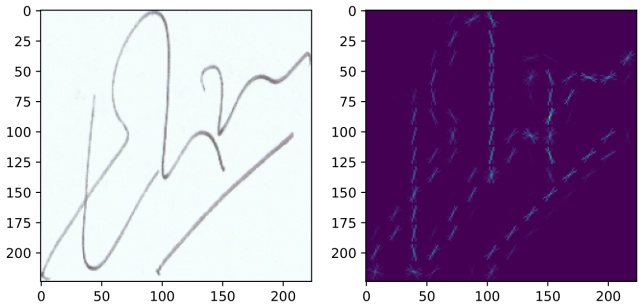

Fig. 4. Vizualni prikaz HOG značajki za jednu sliku

IV. Rezultati

A. VGG-16 značajke

Za slike reprezentirane značajkama dobivenima pomoću ekstraktora značajki, u Tablici II prikazane su točnosti klasifikatora na skupu za testiranje. Najbolja točnost od 92.02% postignuta je klasifikatorom Random Forest. Na slici 5 prikazana je konfuzijska matrica za Random Forest klasifikator.

TABLE II
Rezultati za različite klasifikatore

Klasifikator	Točnost
Logistička regresija	0.9083
Random Forest	0.9202
Linear SVM	0.8982
RBF SVM	0.9192

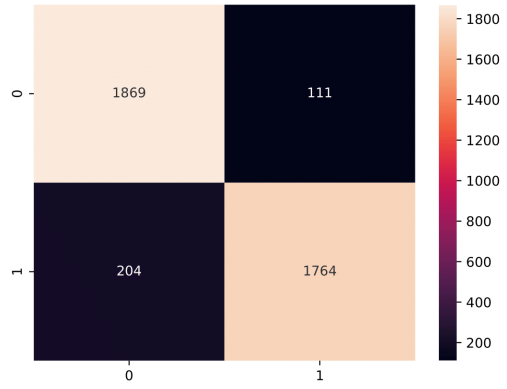

Fig. 5. Konfuzijska matrica za Random Forest klasifikator

Neki primjeri koji je Random Forest pogrešno klasificirao prikazani su na slici 6.

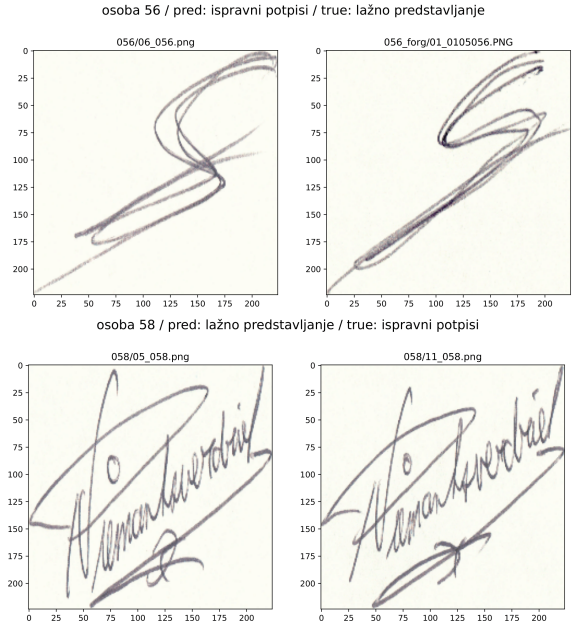

Fig. 6. Primjeri koje je Random Forest klasifikator s VGG-16 značajkama pogrešno klasificirao

B. HOG značajke

Za slike reprezentirane HOG značajkama, u Tablici III prikazane su postignute točnosti klasifikatora na skupu za testiranje. Zbog velikog broja značajki učenje je bilo sporo pa je isproban manji broj klasifikatora. Najveća točnost od 71.15% dobivena je za Random Forest klasifikator. HOG značajke daju lošije rezultate od VGG-16 značajki.

TABLE III
Rezultati za različite klasifikatore

Klasifikator	Točnost
SGDClassifier	0.6781
Random Forest	0.7115

V. Diskusija

Usporedbu s rezultatima iz literature otežava činjenica da postoje različiti oblici zadatka verifikacije potpisa koji primjenjuju različita rješenja te da dio skupova nije javno dostupan. U razvoju svojeg rješenja koristili smo podskup potpisa iz ICDAR skupa.

Najveća točnost postignuta je za ekstrakciju značajki i klasifikator koji koristi algoritam nasumične šume (engl. Random Forest) i iznosi 92.02%, dok za metodu histograma orijentiranih gradijenata najveća točnost iznosi 71.15%, što je usporedivo s rezultatima dobivenim u literaturi [1] gdje točnost na nizozemskom statičkom skupu podataka varira između 71% i 97%. Premda spomenuti rad predstavlja rješenje na problem verifikacije potpisa, on ne koristi istu metodologiju i drugačije

pristupa samom problemu. Ta metodologija uključuje klasifikaciju jednog novog potpisa nepoznate osobe na temelju prethodno prikupljenih potpisa za koje se zna da pripadaju vlasniku. S druge strane, u [4] dan je skup podataka sličan našemu i ponuđeno je dvadesetak *open source* rješenja. Ta rješenja pristupaju problemu na isti način kao i mi (klasifikacija parova potpisa). Njihovi rezultati su nešto lošiji (u svim bilježnicama najviša postignuta točnost je oko 50%). Primjećeno je da od tih dvadesetak rješenja jedno postiže točnost oko 99%, no taj autor kao skup za testiranje klasifikatora koristi podskup skupa za treniranje modela, zbog čega zaključujemo da taj rezultat nije legitiman.

VI. Zaključak

Cilj projekta bio je izraditi sustav za verifikaciju potpisa. Ostvareno rješenje sastoji se od ekstrakcija značajki i učenja klasifikatora. Zadatak sustava je za dani par potpisa odrediti je li riječ o ispravnom paru potpisa ili o slučaju krivotvorenja. Korišten je ICDAR skup podataka, točnije podskup statičkih nizozemskih potpisa na latinici. U prvoj metodi prednaučen VGG-16 konvolucijski model dodatno se uči na zadatku klasificiranja pojedinih potpisa kao ispravnih ili krivotvorenih. Druga metoda kao značajke izvlači histograme orijentiranih gradijenata. Na temelju dobivenih značajki naučeni su i uspoređeni klasifikatori. Za VGG-16 značajke najbolji rezultat je dobiven klasifikatorom Random Forest. Klasifikator s najvećom točnosti bio je Random Forest čije je točnost iznosila 92.02% na skupu za testiranje. HOG značajke daju lošije rezultate, a najveća točnost od 71.15% također je dobivena za klasifikator Random Forest. Ovi rezultati slični su i usporedivi s onima dobivenim u literaturi.

Daljnji rad na ovom problemu uključivao bi treniranje modela u više epoha ili na boljem stroju. Druga opcija bila bi promjena pristupa problemu i mijenjanje cijele metodologije na nešto sličnije već ranije spomenutom članku [1] s ciljem da se dobije veća točnost i eventuano primjenjivija verifikacija potpisa.

References

[1] M. Liwicki et al., "Signature Verification Competition for Online and Offline Skilled Forgeries (SigComp2011)," 2011 International Conference on Document Analysis and Recognition, Beijing, China, 2011, pp. 1480-1484, doi: 10.1109/ICDAR.2011.294.

[2] Souza, V. L. F., Oliveira, A. L. I., Sabourin, R. (2018). A writer-independent approach for offline signature verification using deep convolutional neural networks features. Proceedings - 2018 Brazilian Conference on Intelligent Systems, BRACIS 2018, 212–217.

[3] Impedovo, D., Pirlo, G. (2008). Automatic Signature Verification: The State of the Art. APPLICATIONS AND REVIEWS, 38(5)

[4] https://www.kaggle.com/datasets/divyanshrai/handwritten-signatures