Dešifrovanje CAPTCHA-e pomoću dubokog učenja

Strahinja Milojević
Petar Kulezić

jul 2018.

Uvod

- CAPTCHA je vrsta izazov-odgovor testa koji se koristi u računarstvu da odredi da li je korisnik čovek ili mašina.
- Pošto bi računar trebalo da bude nesposoban da reši taj test, svaki korisnik koji unese tačan odgovor smatra se čovekom.
- Skraćenica CAPTCHA dolazi od engleskog Completely Automated Public Turing test to tell Computers and Humans Apart (u prevodu: potpuno automatizovani javni Tjuringov test za razlikovanje računara i ljudi).

Uvod

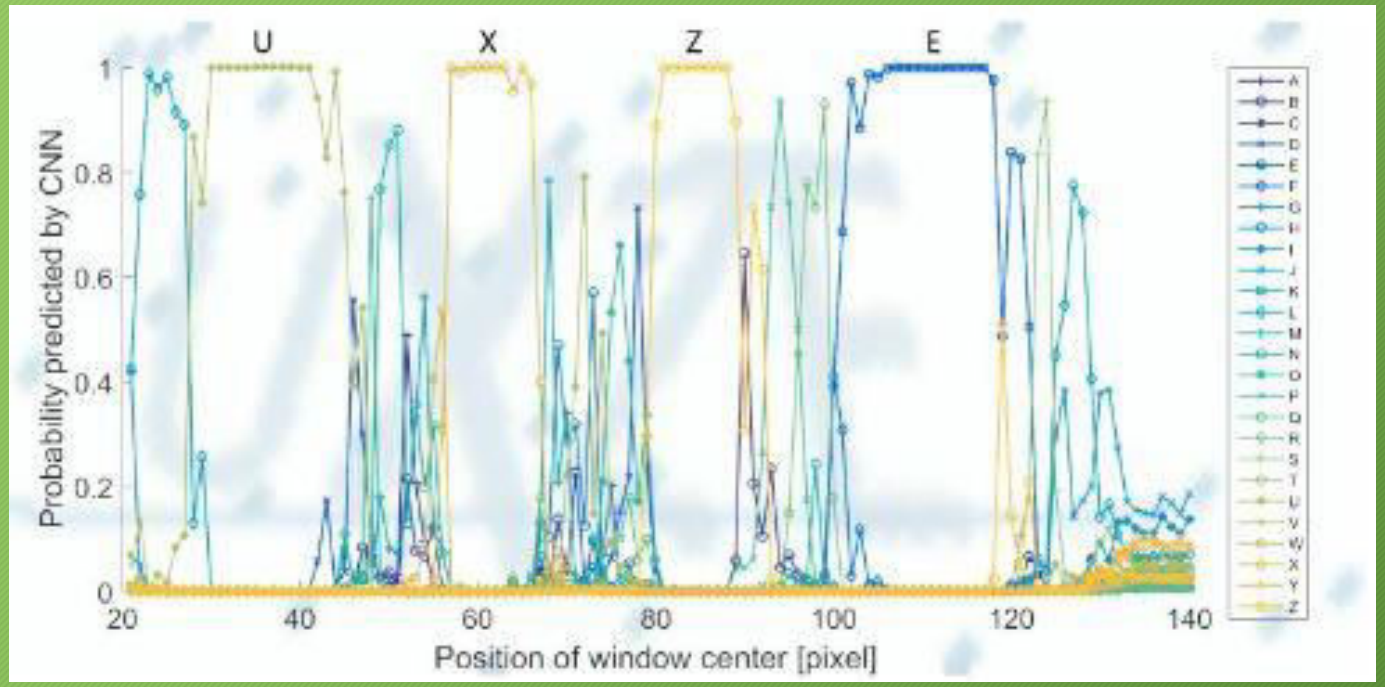
- CAPTCHA-e se primarno koriste na veb sajtovima u cilju sprečavanja botova od vršenja raznih akcija poput kreiranja lažnih naloga, slanja spam poruka, itd.
- Postoje razni algoritmi mašinskog učenja zasnovani na dubokim neuralnim mrežama za rešavanje problema kao što je čitanje ručno pisanog teksta, što je u principu slično dešifrovanju CAPTCHA teksta.

Podaci

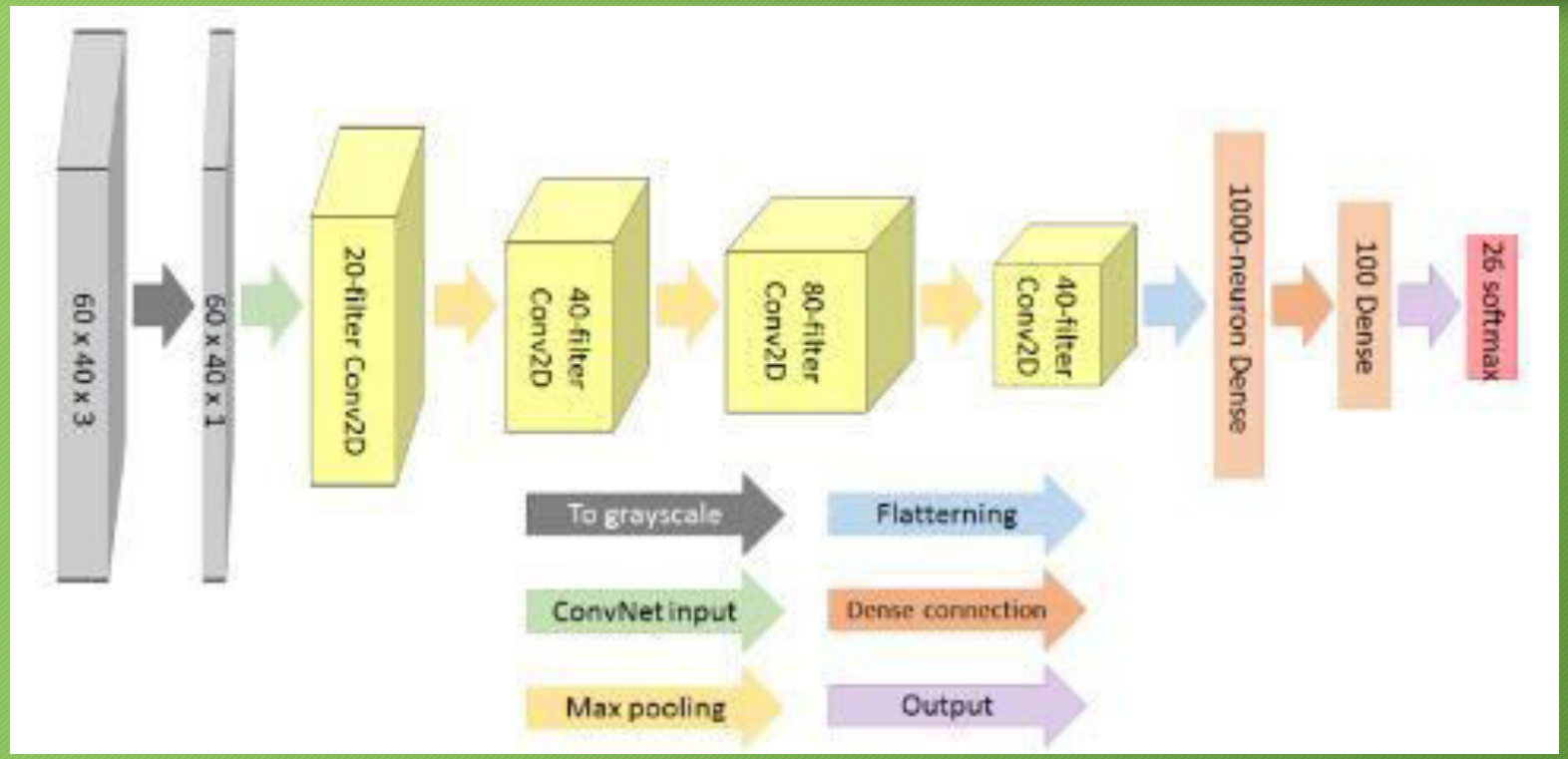
- Podaci (slike) su generisani pomoću biblioteke captcha na slučajan način.
- Četvoroslovne reči, dimenzije slika 160 x 60
- Skup za obučavanje: 5000 slika
- Skup za testiranje: 1000 slika
- Primer:

Priprema podataka

- Sečenje slika na 4 dela
- Binarizovanje RGB modela slika, radi boljih performansi



Struktura neuronske mreže



- Problem sa preprilagođavanjem, performanse poboljšane za 15% izbacivanjem 20% podataka u poslednja 2 sloja (funkcija Dense)

Preciznost predviđanja

	Skup za obučavanje	Skup za testiranje
1. slovo	0.9224	0.767
2. slovo	0.8562	0.702
3. slovo	0.9070	0.651
4. slovo	0.9518	0.74

Linkovi

- Git repozitorijum:
  - https://github.com/strahinja94/CAPTCHA_breaking

- Literatura:
  - http://cs229.stanford.edu/proj2017/final-reports/5239112.pdf
  - http://ml.matf.bg.ac.rs/readings/ml.pdf
  - https://codepen.io/birjolaxew/post/cracking-captchas-with-neural-networks