SVEUČILIŠTE U ZAGREBU
FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA

Zagreb, 10. ožujka 2023.

ZAVRŠNI ZADATAK br. 1160

Pristupnik:	**Dominik Jambrović (0036534818)**
Studij:	Elektrotehnika i informacijska tehnologija i Računarstvo
Modul:	Računarstvo
Mentor:	prof. dr. sc. Siniša Šegvić

Zadatak: **Algoritmi za brzo učenje na neprijateljskim primjerima**

Opis zadatka:

Raspoznavanje slika važan je zadatak računalnog vida s mnogim zanimljivim primjenama. Trenutno stanje tehnike temelji se na dubokim modelima koji se uče s kraja na kraj. Međutim, veliki kapacitet tih modela omogućava kibernetičke prijetnje zasnovane na neprijateljskim primjerima. U okviru rada, potrebno je odabrati okvir za automatsku diferencijaciju te upoznati biblioteke za rukovanje matricama i slikama. Proučiti i ukratko opisati postojeće pristupe utemeljene na dubokom učenju. Odabrati klasifikacijski model te uhodati njegovo učenje na nekom javno dostupnom skupu podataka. Izvesti kibernetički napad zasnovan na neprijateljskim primjerima. Prikazati i ocijeniti uspješnost napada te opisati postupke obrane koji čim manje utječu na brzinu učenja modela. Radu priložiti izvorni i izvršni kod razvijenih postupaka, ispitne slijedove i rezultate, kao i potrebna objašnjenja i dokumentaciju. Citirati korištenu literaturu i navesti dobivenu pomoć.

Rok za predaju rada: 9. lipnja 2023.