TANSZÉKVEZETŐ

DIPLOMATERVEZÉSI FELADAT

Csarnó Tamás Péter
Mechatronikai mérnök hallgató részére

Gépi tanulási eljárásokkal generált adatok adatvédelmi vizsgálata

Gépi tanulási rendszereket egyre szélesebb körben alkalmaznak komplex feladatok megoldására. Ezek között számos olyan eljárás is található, amelyek az adatot generálnak a bemenetből, mint például generatív modellek vagy a deep metric learning, de ide sorolhatóak a napjainkban egyre elterjedtebben használt gépi tanulásra épülő arcfelismerési rendszerek is.

A modern arcfelismerő eljárások az emberi arc fényképe alapján generálnak adatot, ami az adott ember arcát jellemzi. Bár az arcfelismerés technológiának sok hasznos alkalmazása létezik, komoly adatvédelmi kockázatot is rejthet, hiszen az arcfelismerés során generált arclenyomatok tartalmaznak személyes adatokat is.

A hallgató feladata legalább egy választott eljárás mélyrehatóbb vizsgálata adatvédelmi szempontból. A hallgató feladatának a következőkre kell kiterjednie:

- Átfogó jelleggel mutassa be az adat generáló gépi tanulási megoldásokat!
- Válasszon ki ezek közül legalább egy eljárást, és mutassa be!
- Elemezze hogyan van a generált vagy származtatott adatba kódolva a személyes adat, mutassa be ezeknek az adatoknak az adatvédelmi kockázatát!
- Javasoljon védekezési megoldást ezeknek a kockázatoknak a kiszűrésére!

Tanszéki konzulens: Dr. Gulyás Gábor György, tudományos munkatárs

Budapest, 2021. március 18.

Dr. Charaf Hassan
egyetemi tanár
tanszékvezető

Budapesti Műszaki és Gazdaságtudományi Egyetem
Villamosmérnöki és Informatikai Kar
Automatizálási és Alkalmazott Informatikai Tanszék

H-1117 Budapest, Magyar tudósok krt 2. Q.B.207
Telefon: 463-2870. Fax: 463-2871
www.aut.bme.hu