

Bevezetés a mesterséges intelligenciába

Captcha megoldó program

Projekt specifikáció

Ekart Csaba

2019. február 27.

1. Probléma specifikáció és motiváció

A CAPTCHA a számítástechnikában olyan automatikus teszt, ami képes megkülönböztetni az emberi felhasználót a számítógéptől. A szó az angol Completely Automated Public Turing test to tell Computers and Humans Apart kifejezés rövidítése. [1]

Lényege, hogy egy olyan feladványt generálunk, amely teljesítésére csak ember képes, viszont könnyen ellenőrizhető a megadott válasz helyessége. Célja az, hogy bizonyos weboldalakat megvédjen a különböző botoktól és az általuk generált SPAM-től.

A tesztek az utóbbi években a leggyakrabban egy torz szöveget tartalmazó kép megfejtéséből álltak, azonban a manapság ezt váltja a Google általfejlesztett reCAPTCHA, melyen csupán egy checkboxra kell kattintani a felhasználónak. A váltásra nem véletlenül volt szükség. Az utóbbi években elterjedt tanuló algoritmusok segítségével már olyan CAPTCHA megoldó programokat lehet létrehozni, melyek rendkívül nagy (99.81%) pontossággal meg tudták oldani ezeket a feladatokat, hatékonyabban, mint az emberek. [2]

Projekt munkámban kizárólag ezen korábbi szöveges CAPTCHA-kkal fogok foglalkozni.



1. ábra. A régi szöveges CAPTCHA és az új, egyszerűbb, és biztonságosabb reCAPTCHA

A szöveges CAPTCHA megoldása számomra egyszerre egy valós és érdekes probléma, másfelől fontos határvonalnak tartom a mindennapokban használt mesterséges intelligenciák elterjedésében, éppen ezért választottam projekttem témájának.

2. A projekt megvalósításához szükséges technikák és módszerek

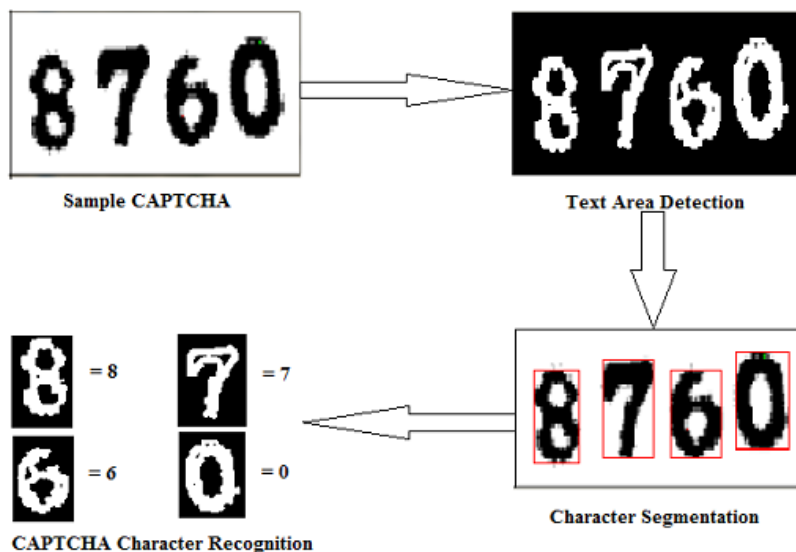
Ahhoz, hogy a CAPTCHA rendszert megtudjuk oldani, visszafele kell gondolkodni, és a feladványok generálásából kiindulni, majd ezek alapján felállítani a szükséges lépéseket. A kapott folyamat három fő lépése az alábbiak lesznek: [3]

1. **Preprocessing (Előzetes feldolgozás):** A következő lépések könnyebbé tételének érdekében tett lépések. Pl. Képjavítás, háttér eltávolítása, stb.
2. **Segmentation (Szegegmentálás):** A szöveget megpróbáljuk elválasztani a háttértől, majd külön karakterekre bontani.

3. Recognition (felismerés): Meghatározzuk a kép alapján a karaktert.

Praktikusan úgy implementálható az algoritmus, hogy minden szegmentálási típushoz külön algoritmust rendelünk, majd a karaktereket gépi tanulás segítségével ismerjük fel.

A karakter felismerés könnyen teljesíthető, ebben a gépi tanulás hatékonyabb is az embernél, azonban a karakterek szétválasztása, főleg, hogy gyakran szándékosan összeérnek, már egy nehezebb feladat. Erre számos különböző technika alkalmazható, pl. Flood-filling segmentation, Histogram segmentation, Pattern matching, Snake segmentation, karakterek kontúrja, struktúrája stb. [4]



2. ábra. A CAPTCHA megoldásához szükséges folyamat fő lépései

Hivatkozások

- [1] <https://hu.wikipedia.org/wiki/Captcha>
- [2] <https://arxiv.org/pdf/1312.6082v4.pdf>
- [3] Christos Makris and Christopher Town - Character segmentation for Automatic CAPTCHA solving
University of Cambridge Computer Laboratory
<https://benthamopen.com/contents/pdf/COMPSCI/COMPSCI-1-1.pdf>
- [4] Jun Chen, Xiangyang Luo, Yanqing Guo - A Survey on Breaking Technique of Text-Based CAPTCHA
<https://www.hindawi.com/journals/scn/2017/6898617/>