



Digitális személyazonosítás mesterséges intelligenciával

Készítette

Kovács Gábor

Programtervező informatikus Bsc

Témavezető

Dr. Kovásznai Gergely

Tanszékvezető, egyetemi docens

EGER, 2025

Tartalomjegyzék

0.1. Neurális hálózatok tesztelése	2
0.1.1. Pontosság és metrikák	2
0.1.2. Eredmények kiértékelése	4

0.1. Neurális hálózatok tesztelése

A projektben három különböző *neurális hálózatot* használtam: az *OCR modellt*, a *határoló doboz detektáló modellt* és a *nemfelismerő modellt*. Ezek mindegyike *kulcsszerepet* játszik a személyi igazolványok adatainak *automatikus feldolgozásában*.

0.1.1. Pontosság és metrikák

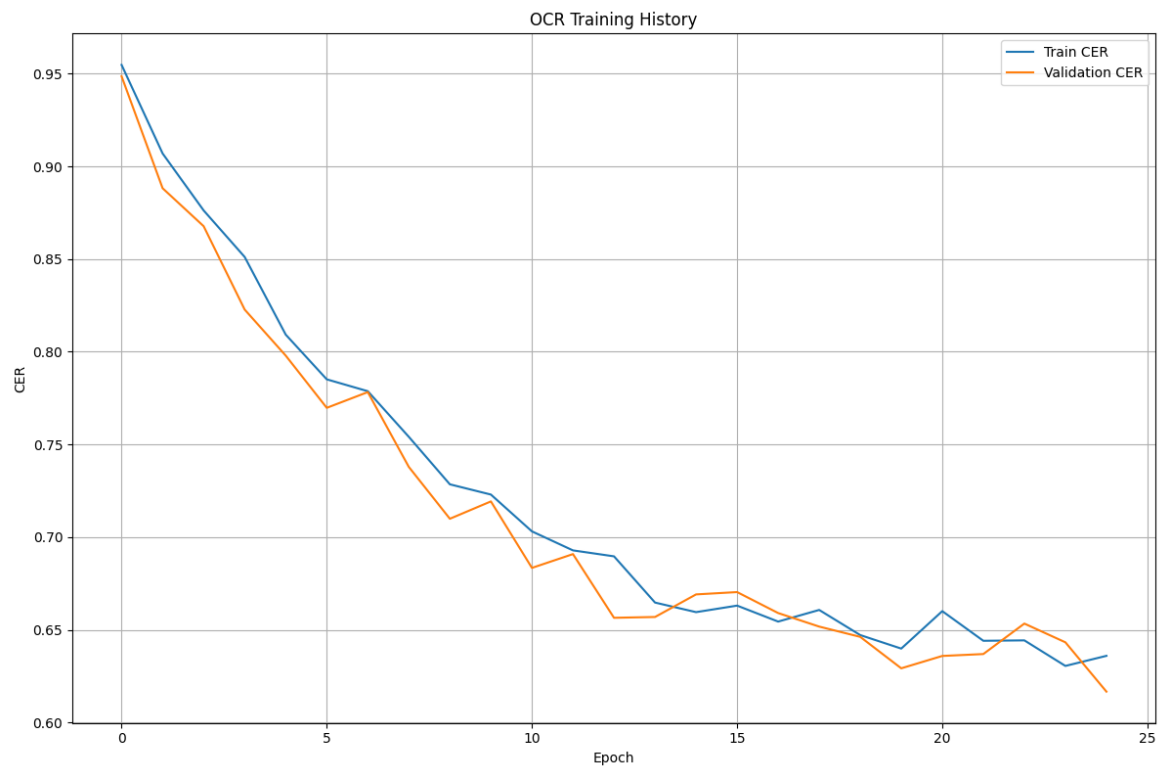
A modellek teljesítményének kiértékeléséhez különböző *metrikákat* használtam, valamint elemeztem a tanulási folyamat során rögzített értékeket.

Az *OCR modell* tanítása során a CER értéke folyamatosan csökkent, ahogy a az 1 ábrán látható. A kezdeti 0,95-ös értékről a 25. epochra 0,62-re javult, ami jelentős előrelépés, bár még mindig magas hibaarányt jelez.

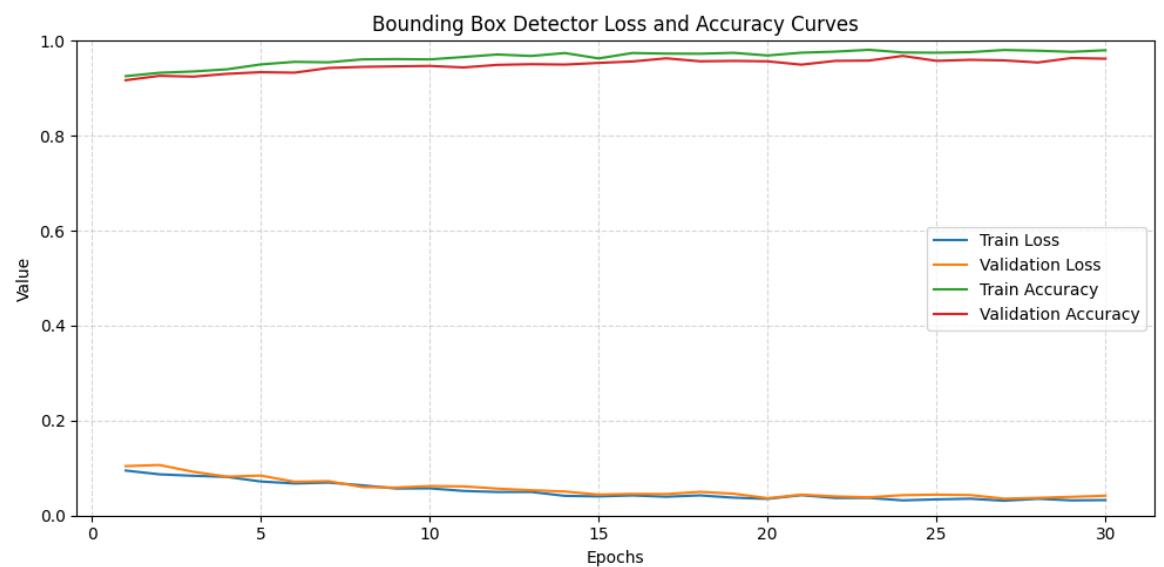
A *tesztelés* során kiderült, hogy a modell jelentős problémákkal küzd az *ékezetes karakterek* felismerése terén. Különösen az „á”, „é”, „ő” és „ű” betűk okoztak nehézséget, amelyeket gyakran ékezet nélküli megfelelőiként azonosított. Emellett a *szóközők felismerése* is következtelen volt, ami különösen a nevek feldolgozásánál okozott problémákat, mivel ezeket gyakran egybeírta vagy indokolatlanul több részre tagolta.

A *határoló doboz detektáló modell* jóval meggyőzőbb eredményeket mutatott, amint az a 2 ábrán látható. A veszteségfüggvény értékei egyenletesen csökkentek, míg a pontosság már a korai epochokban is 90% feletti értéket ért el, majd 98% körül stabilizálódott.

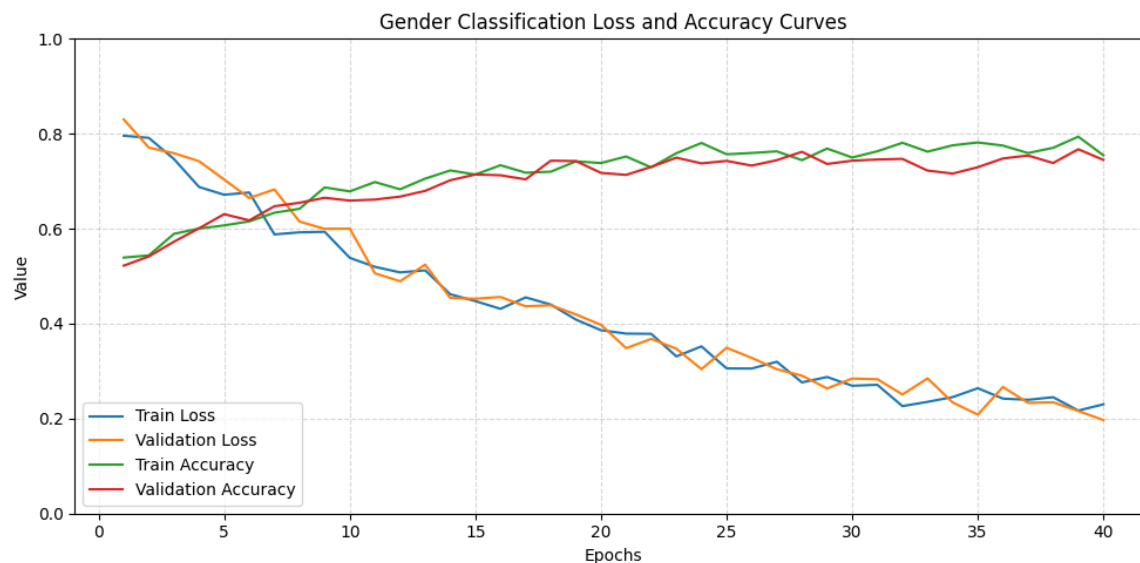
Ugyanakkor a tesztelés során kiderült, hogy a modell érzékeny a *perspektívaorzításra*. Amikor a felhasználók *ferdén fotózták* a személyi igazolványt (20 foknál nagyobb szögben), a határdobozok jelentősen *elcsúsztak*, ami az OCR modell számára tovább nehezítette a pontos szövegfelismerést. Különösen a kártya alsó részén található mezők (lejárati dátum, CAN kód) esetében volt észlelhető ez a probléma.



1. ábra. OCR modell tanítási és validációs karakterhiba-arány (CER) értékei



2. ábra. Határoló doboz modell tanítási folyamata - pontosság és veszteség



3. ábra. Nemfelismerő modell tanítási és validációs metrikái

A *nemfelismerő modell* teljesítménye a 3 ábrán látható. A validációs pontosság csak lassan emelkedett, és a görbék mutatnak némi instabilitást. Az accuracy értéke a 40. epochra is csak 75% körül stabilizálódott.

A nemfelismerő modell jelentős nehézségekkel küzdött bizonyos esetekben. A *hosszú hajú férfiakat* gyakran nőként azonosította, míg a *rövid hajú nőket* férfiként. Ez a jelenség rávilágít, hogy a modell túlságosan a kulturális sztereotípiákra (pl. hajhosszra) támaszkodik a nemek meghatározásánál, ahelyett hogy az arc más jellemzőit venné figyelembe. Idősebb személyek esetében is magasabb volt a téves osztályozás aránya.

0.1.2. Eredmények kiértékelése

Az *OCR modell* kezdeti tesztelésekor alacsony pontosságot ért el. A *felismert karakterek* közel harmadában előfordult valamilyen *hiba*, különösen az *ékezetes betűk* esetében. A többszöri *finomhangolás* után azonban sikerült a teljesítményt jelentősen javítani.

A *határoló doboz detektáló modell* magas átlagos pontosságot ért el, ami összhangban van a tanulási görbén látható kiváló eredményekkel. A modell tanulási folyamata rendkívül stabil volt, már a korai szakaszban is magas teljesítményt mutatott. A perspektívaforzítás problémája azonban továbbra is fennáll, ami a valós használat során komoly korlátot jelenthet.

A *nemfelismerő modell* kezdeti *gyenge teljesítményét* jól tükrözi a tanulási görbe lassú emelkedése. Több javítási kísérlet után javult a pontosság, de még mindig elmarad az ideáltól. A modell túlzottan támaszkodik a felszíni jellemzőkre, mint a hajhossz vagy az arcforma, ami különösen problémás a nem szokványos megjelenésű személyek esetében.

A tanulási görbék elemzése alapján egyértelműen a *határoló doboz detektáló modell*

teljesített a legjobban, míg a nemfelismerő modell maradt a leggyengébb láncszem. Az OCR modellnél a CER értéke még a tanítás végén is viszonylag magas maradt, ami jelzi, hogy további fejlesztésekre lenne szükség.

A *fejlesztési javaslatok* között szerepel az *OCR modell* számára nagyobb és változatosabb, különösen ékezetes karaktereket tartalmazó adathalmaz használata, a *nemfelismerő modell*hez komplexebb architektúra kidolgozása, amely kevésbé támaszkodik sztereotipikus megjelenési jellemzőkre, valamint a *határoló doboz modell*hez automatikus perspektíva-korrekció beépítése, amely kompenzálja a ferdén készített fényképek torzítását.

Ezek a fejlesztések együttesen javíthatják a rendszer *megbízhatóságát* és *pontosságát* valós használati körülmények között, bár a jelenlegi állapotában is használható alapot nyújt a személyi igazolványok feldolgozásához, különösen emberi ellenőrzés mellett.