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

Nagy Zalán
V9T3UL
https://github.com/nazalan

Online kézírásos aláírás hitelesítő rendszer neurális hálózatok osztályozása alapján

Témalaboratórium
2023/24/ősz

KONZULENS
Szücs Cintia Lia

I. Bevezetés

Az információs technológia rohamos fejlődése és az online szolgáltatások elterjedése a digitális aláírások iránti növekvő igényt hozta magával. A digitális aláírásokat széles körben alkalmaznak elektronikus tranzakciók, szerződések és hivatalos dokumentumok esetében, ahol a biztonság és az azonosítás kritikus fontosságúak. Az egyre növekvő digitális térben azonban felmerül az online kézírásos aláírások hitelesítésének kérdése, mivel a hagyományos aláíráshoz hasonlóan az online kézírásos aláírások egyedi és azonosítható jellemzőkkel rendelkeznek.

A dolgozat célja, hogy bemutassa és értékelje az online kézírásos aláírások hitelesítésének egyik megközelítését, mely a neurális hálózatok osztályozó képességére támaszkodik.

A dolgozat részletesen foglalkozik a neurális hálózatok osztályozó szerepével, bemutatva azok előnyeit és kihívásait a kézírásos aláírások hitelesítése során. Emellett a dolgozat olyan konkrét eseteket is tárgyal, amelyekben a rendszer hatékonyságát és megbízhatóságát vizsgálja meg.

II. Adatbázis és az adatok digitális előfeldolgozása

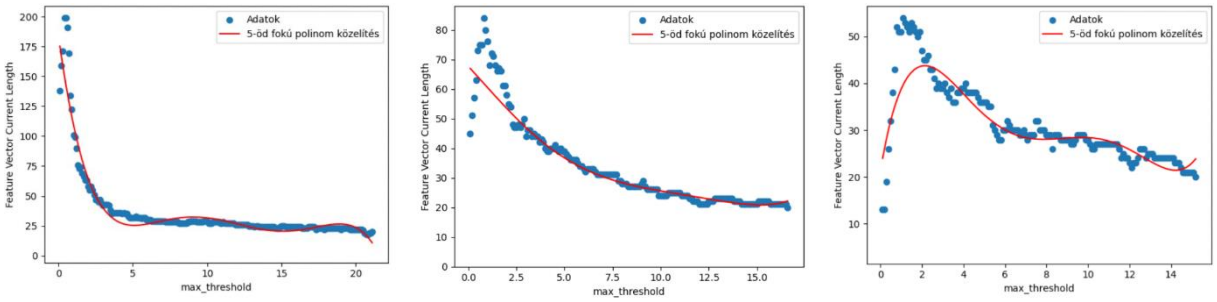
Az adatbázis, amely felhasználásra került a DeepSignDB. különböző formátumok és az eltérő adattartalmak miatt azonban az adatok összeállítása és rendezése komplex feladat volt. Az adatbázisban szereplő aláírások struktúrájából adódó kihívások közé tartozott, hogy azokat nem az adathalmazok, hanem a felhasználói azonosítók alapján lehetett azonosítani, amelyek a fájlnévben voltak kódolva, az aláírás hitelességével együtt. Habár az adatbázis rengeteg információt tartalmaz, a dolgozatban felhasznált része kizárólag az újjal írt aláírások (finger). Ennek a megszorításnak az oka a korlátozott rendelkezésre álló számítógép erőforrás.

A digitális előfeldolgozása kiemelt fontosságú lépés, amely előkészíti az adatokat a neurális hálózati osztályozási feladathoz. Az előfeldolgozás során eredetileg a referencia cikkben[1] leírt algoritmus alkalmazása volt a cél. A cikk egy, az alkotók által kitalált algoritmus mellett széles körben elterjedt módszereket és azok kombinációit használja. Ezek közé tartozik a diszkrét hullámtranszformáció, a dinamikus időtranszformációs algoritmus, a rejtett Markov-modell és a spektrális elemzés Fourier-transzformáció segítségével. Ugyanakkor a cikkben szereplő eljárás nem bizonyult elégségesen részletesnek, és számos hibát tartalmazott.

A referencia cikk szerzői által kitalált algoritmus lépései közé tartozik két tömb és egy küszöbérték inicializálása, majd az egyik tömb koordinátákkal való feltöltése. Az algoritmus ezután egyeneseket épít az összegyűjtött pontokon keresztül, kiszűrve azokat, amelyek nem felelnek meg meghatározott küszöbértéknek. Azokat a pontokat, amelyeket nem szűrt ki az eljárás, a kezdetben inicializált másik tömbben tárolja. Ebben a tömbben tárolt pontokból számolja az átlagos vízszintes és függőleges mozgási sebességeket. Majd egy jellemző vektort alkot a szakaszok közötti átlagos mozgási sebességek komponenseiből.

[1] Online Handwritten Signature Verification System Based on Neural Network Classification - Dmitrii I. Dikii és Viktoriia D. Artemeva

Azonban gyakorlati alkalmazás során felmerült az a probléma, hogy a különböző aláírásokat az eljárás végén egységes hosszra kellett hozni, és ehhez mindig meg kellett találni a megfelelő küszöbértéket, amely pontosan annyi pontot szűr ki, amellyel előáll egy adott hosszúságú jellemző vektor. Egyes esetekben azonban ez a küszöbérték nehezen vagy egyáltalán nem állt elő. A várakozásokkal ellentétben a küszöbérték lineáris növelése a kimeneti vektor nem lineáris változását okozta, ahogyan az alábbi *ábra* is mutatja. Ez a felmerülő probléma ellehetetlenítette az algoritmus hatékony alkalmazását.



A digitális előfeldolgozása lényegesen leegyszerűsödött az eredeti tervekhez képest, így az a következő lépésekből áll:

1. Adatok beolvasása: Az aláírások és személyek adatait fájlokból és mappákból olvassuk be, majd strukturált formában tároljuk azokat az adatbázisban.
2. Vektorok egyesítése: Az aláírásokat háromdimenziós vektorokként tároljuk, amelyek tartalmazzák az x- és y-koordinátákat, valamint az időbélyeg értékeit. Ezeket a vektorokat egyesítjük egy mátrixba a könnyebb kezelhetőség és további feldolgozás érdekében.
3. Normalizáció: A MinMaxScaler segítségével normalizáljuk a vektorokat a -1 és 1 közötti értéktartományba, ami optimalizálja a neurális hálózat tanulási folyamatát.
4. Nullákkal kiegészítés: A vektorokat a leghosszabb aláírás hosszáig kiegészítjük nullákkal, hogy azok azonos hosszúak legyenek. Ez a lépés szükségszerű a későbbi felhasználás érdekében.

Ezen folyamatok eredményeképpen előáll a neurális hálózatok számára alkalmas bemeneti adathalmaz, amely tartalmazza a normalizált és nullákkal kiegészített vektorokat.

III. Mesterséges neurális háló

A digitális aláírások hitelesítéséhez alkalmazott módszerek közül a mintaillesztés mellett a mesterséges neurális hálók is hatékonyak lehetnek. A hálók képessége, hogy tanuljanak és azonosítsák a mintázatokat, kiválóan alkalmazható a kézírásos aláírások hitelesítésére.

Kezdetben a fentebb említett cikk mintájára készült a hálózat, így referencia aláírás nélkül kísérelte meg az aláírások hitelesítését. Azonban hamar kiderült, hogy a hálózat nem teljesített megfelelően, és az eredmények nem voltak kielégítők. A hiányzó referencia aláírás miatt a hálózatnak nehézségei adódtak a kategorizálásban. Felismerhető volt, hogy a cikkben bemutatott előfeldolgozási lépések hiánya hátráltatta a hálózatot, és szükség van egy hatékonyabb módszerre az aláírások értékeléséhez. Ennek eredményeként a referencia aláírásos módszerre esett a választás. Az ezen a módszeren alapuló megoldásban a hálózat nem egyetlen

aláírásról dönti el, hogy az eredeti vagy hamis, hanem egyazon személytől rendelkezésre áll egy referencia aláírás, ami mindig eredeti és egy másodlagos aláírás, ami lehet eredeti és hamis is. Az ilyen módon előkészített adatok segítségével a hálózat képes volt hatékonyan megkülönböztetni az aláírásokat, javítva ezzel az azonosítás terén elért eredményeket.

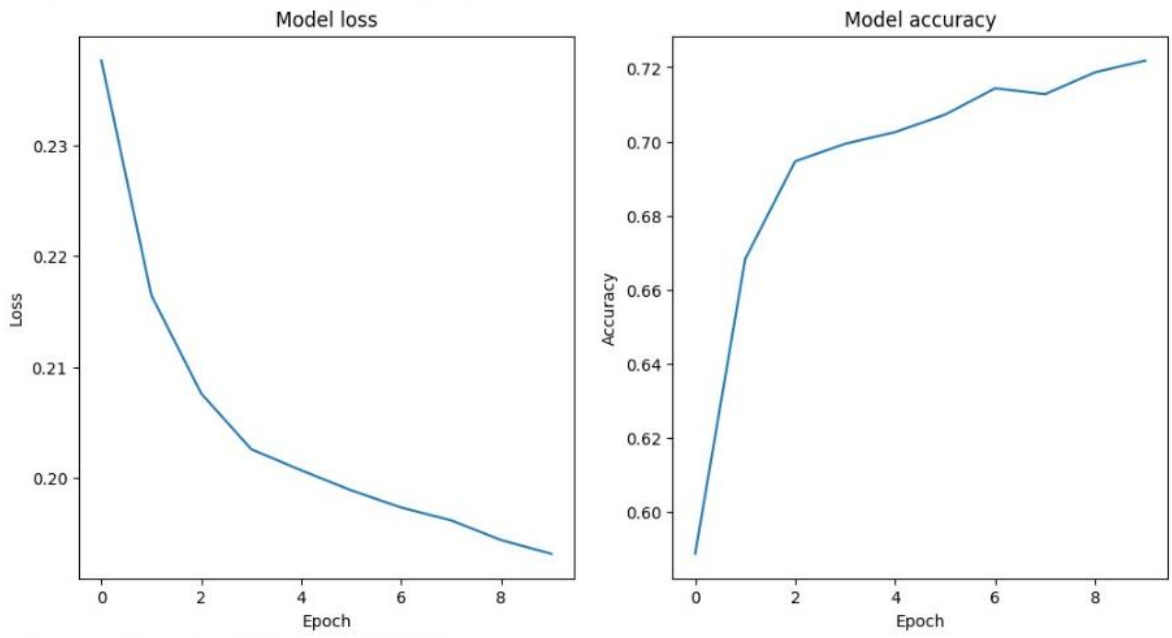
A véglegesen megalkotott neurális háló a következőképpen tagolható:

A hálózat két bemeneti ággal rendelkezik, amelyek különállóan fogadják be a referencia aláírások és a másodlagos aláírások vektorait. A bemeneti vektorokat háromdimenziós koordináták alkotják, beleértve az x- és y-koordinátákat, valamint az időbélyeg értékeit. Minden bemenetiághoz tartozik egy különálló réteg. Minden réteg két Dense rétegből áll, amelyek ReLU aktivációs függvénnyel rendelkeznek. A két ágat az összekapcsolás rétege követi, ami lehetővé teszi a hálózatnak, hogy egyszerre tanuljon mindkét típusú bemenetről. Az összekapcsolás réteg a két ágból érkező információkat kombinálja. Az összekapcsolás réteg után további két Dense réteg következik a hálózatban. Ezek a rétegek szolgálnak a bemeneti adatok további kombinációjára és a kimeneti osztály előállítására. A kimeneti réteg egyetlen neuronból áll, ami a sigmoid aktivációs függvényt használja. Az egyetlen neuron kimeneti értéke az aláírás eredetiségét jelzi, bináris osztályozás esetén (1: eredeti, 0: hamis).

A háló tanításakor a modell a két bemeneti ághoz tartozó vektorokat párhuzamosan dolgozza fel, az összekapcsoló réteg segítségével kombinálva az információkat. A tanító adatokat az eredetiségük alapján két osztályba soroljuk, majd a hálózatot megtanítjuk az osztályozásra.

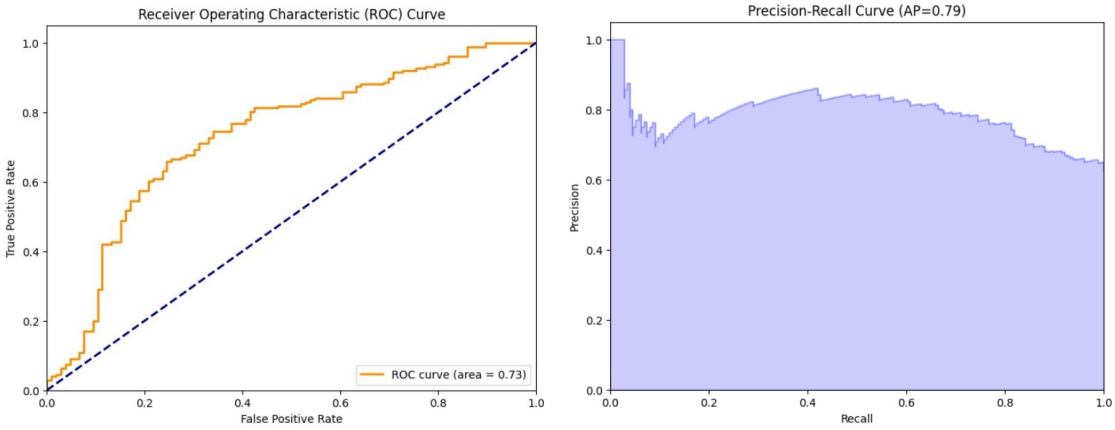
IV. Eredmények

A neurális hálózat tanítása során tíz epochon keresztül végeztünk iterációkat, és figyeltük a tanulás eredményeit. A modell folyamatos finomhangolása során az epochokban a veszteség és pontosság a következőképpen alakult: Az első epochtól a tizedik epochig látható volt a veszteség (loss) csökkenése és a pontosság (accuracy) növekedése. A kezdeti veszteség 0,2376-ról 0,1932-re csökkent, míg a pontosság 0,5887-ről 0,7218-ra növekedett.



A tanítás után a modellt tesztadatokon is értékeltük, és a következő eredményeket kaptuk: Az osztályozási jelentés (Classification Report) alapján a hálózat átlagosan 70%-os pontosságot mutatott a tesztadatokon. Az alábbi *táblázat* az egyes osztályok (eredeti vagy hamis aláírás) esetén részletesen is bemutatja a hálózat teljesítményét.

	precision	recall	f1-score	support
0	0,63	0,46	0,53	106
1	0,72	0,84	0,77	176
accuracy			0,70	282



V. Következtetés

A tanulmányban bemutatott neurális hálózat alkalmazása az online kézírásos aláírások hitelesítésére ígéretes eredményeket mutatott. Az adatok alapján látható, hogy a hálózat képes megkülönböztetni az eredeti és a hamis aláírásokat, és átlagosan 70%-os pontosságot ért el a tesztadatokon. Az elért eredmények figyelemre méltóak, különösen a korlátozott adatkészlet és a számítógép erőforrások szempontjából.

A hálózat tervezése során fontos volt az előfeldolgozási lépések kidolgozása, különösen az adatok beolvasása, vektorok egyesítése, normalizáció és nullákkal való kiegészítés. Ezek a lépések lehetővé tették a hálózatnak, hogy hatékonyan feldolgozza az aláírásokat és tanuljon azok jellemzőiről.

Az eredmények alapján további finomhangolások és a modell bővített adatkészlettel való tanítása elősegítheti a hálózat teljesítményének további javítását.