

Offline Signature Identification Based on Deep Learning Using Convolutional Neural Networks

Majid Keshavarz Hedayati¹, Roya Rad^{2*}, Alireza Taghizade³

1. MSc Student, Computer & IT, Parand Branch, Islamic Azad University, Tehran, Iran.
2. Assistant Professor, Department of Computer & IT, Parand Branch, Islamic Azad University, Tehran, Iran.
3. Assistant Professor, Department of Computer & IT, Parand Branch, Islamic Azad University, Tehran, Iran.

Abstract

Introduction: In many daily affairs, it is necessary to confirm the identity of each person, such as banking affairs, document registration, property purchase, etc. Among the methods of identity verification, biometric characteristics are one of the most efficient methods, and signature is considered as one of the behavioral characteristics. In this research, a system was designed and implemented to detect and verify signatures with high accuracy and low error using machine vision and deep learning algorithms. In the offline signature Identification method, only the signature scanned image is needed, in order to obtain the features of the image for training. On the contrary, the online method where the signer himself is present and his characteristics are checked with special tools at the moment, such as the angle of the pen, starting points, slippage, etc.

The proposed method for offline signature detection includes 4 general steps including pre-processing, feature extraction, classification and evaluation.

Method: One of the challenges of signature Identification in previous methods was the model's need for heavy pre-processing and feature extraction, which sometimes became more complicated than the training process. By using deep learning in convolutional neural networks, these challenges have been solved. To classify signatures, deep neural networks and VGG19 and Inception V3 architecture were used. These architectures include convolution and pooling layers, which are the basis of feature extraction from the image during training, and classification was done based on these features. To prevent overfitting, transfer learning and data augmentation have also been used in the model training process. In the proposed system, it is possible to distinguish between the original and fake signature.

Results: This dataset includes Iranian signature samples of 115 people and 27 scanned signatures from each person, totaling 3105 numbers; In this dataset, there are also fake signatures that are used to test the model after training and evaluation. In the evaluation of the model on this dataset, 94.3% accuracy was obtained, which shows the strength of the proposed method compared to similar methods.

Discussion: High accuracy and low error are the characteristics of the method mentioned in this article. By using convolutional neural networks, due to maintaining local information, the relationship between neighboring pixels is learned, and this makes the model not sensitive to the change of location and center of gravity, noise, etc. As a result, the training process is better and high accuracy and error less is obtained.

Keywords: Signature Identification, Convolution neural network, Machin vision, Feature extraction, deep learning.



شناسایی آفلاین امضا براساس یادگیری عمیق با استفاده از شبکه‌های عصبی پیچشی

دوره پنجم، تابستان ۱۴۰۳
شماره دوم، صص: ۲۱۱-۲۲۰

تاریخ دریافت: ۱۴۰۳/۰۱/۲۷
تاریخ پذیرش: ۱۴۰۳/۰۳/۰۹

مجید کشاورز هدایتی^۱، رویا راد^{۲*}، علیرضا تقی‌زاده^۳

۱. دانشجوی کارشناسی‌ارشد، گروه کامپیوتر و IT، واحد پرند، دانشگاه آزاد اسلامی، تهران، ایران. arjivan.majid@gmail.com

۲. استادیار، گروه کامپیوتر و IT، واحد پرند، دانشگاه آزاد اسلامی، تهران، ایران. (نویسنده

مسئول) raad@piaou.ac.ir

۳. استادیار، گروه کامپیوتر و IT، واحد پرند، دانشگاه آزاد اسلامی، تهران، ایران.

a.taghizadeh@piaou.ac.ir

چکیده: یکی از کارآمدترین روش‌های شناسایی و تأیید هویت، استفاده از مشخصه‌های زیست‌سنجی یا بیومتریک است. امضا به این دلیل که یکی از مشخصه‌های رفتاری فرد در علم بیومتریک است، گزینه بسیار خوبی برای تأیید هویت هر فرد است. این پژوهش به طراحی و پیاده‌سازی سیستمی برای تشخیص و تأیید امضا با استفاده از الگوریتم‌های بینایی ماشین و یادگیری عمیق می‌پردازد. روش پیشنهادی برای تشخیص امضای آفلاین شامل ۴ مرحله کلی شامل پیش‌پردازش، استخراج ویژگی، دسته‌بندی و ارزیابی است. دسته‌بندی امضا بر اساس شبکه‌های عصبی پیچشی با دو معماری VGG19 و Inception V3 پیاده‌سازی شده‌است. برای جلوگیری از بیش‌برازش از یادگیری انتقالی و داده‌افزایی نیز در روند آموزش مدل استفاده شده‌است. علاوه بر تشخیص امضا از سیستم پیشنهادی می‌توان برای تأیید اصلی یا جعلی بودن امضا نیز استفاده نمود. آموزش و آزمایش مدل بر روی دیتاست UTSig^۱ صورت گرفته که شامل نمونه امضاهای اسکن شده ایرانی‌ها و توسط دانشگاه تهران تهیه گردیده‌است. این دیتاست از نمونه امضای ۱۱۵ نفر و از هر نفر ۲۷ امضا تشکیل شده‌است؛ در این دیتاست امضاهای جعلی نیز موجود است که برای ارزیابی مدل پس از آموزش و در مرحله تأیید امضا از آن‌ها استفاده شده‌است. در ارزیابی مدل بر روی این دیتاست دقت ۹۴٫۳٪ به دست آمد که نشان‌دهنده قدرت روش پیشنهادی نسبت به روش‌های مشابه است.

واژه‌های کلیدی: شناسایی امضا، شبکه‌های عصبی پیچشی، بینایی ماشین، استخراج ویژگی، یادگیری عمیق.

۱- مقدمه

امروزه برای تشخیص و تأیید هویت افراد از ویژگی‌های بیومتریک آن‌ها استفاده می‌شود. استفاده از خصوصیات بیومتریک مشکلاتی نظیر فراموشی رمز را نداشته و امکان سوءاستفاده از آن بسیار کم است. امضای دستی به عنوان مهم‌ترین ابزار شناسایی هویت فردی در اسناد مکتوب، یکی از ساده‌ترین و کم‌هزینه‌ترین ابزارهای بیومتریک است.

برخی از این خصوصیات افراد به صورت رفتاری و یا فیزیکی هستند. امضا از جمله خصوصیات رفتاری افراد است که توسط سایرین قابل جعل شدن است. با پیشرفت فناوری و نیاز به امنیت بیشتر در جوامع مدرن، سیستم‌های شناسایی امضا برای تأیید هویت فردی و تشخیص تقلب در امضاها اهمیت بیشتری یافته‌اند.

سیستم تشخیص امضا دو وظیفه عمده را برعهده دارد: شناسایی صاحب امضا و تصمیم‌گیری در خصوص اینکه آیا امضا جعلی یا صحیح است. این کار به روش‌های آنالین و آفلاین قابل انجام است. در روش آنالین نیاز به قلم نوری و تجهیزات خاص است که امضا روی آن ثبت شود و همزمان نمونه بر اساس نقاط فشار، زاویه چرخش خودکار روی صفحه و همچنین جهت رسم خطوط بر روی صفحه و ... بررسی می‌شود. در این روش نیاز به حضور شخص برای ثبت امضا می‌باشد. اما در روش آفلاین تنها نیاز به تصویر امضا (نه خود شخص) است و سیستم با استفاده از نتیجه آموزش روی مجموعه‌ای از امضاها اقدام به سنجش تصویر امضای کند. روش آفلاین دارای مراحل مختلفی از قبیل جمع‌آوری اطلاعات، پیش‌پردازش و استخراج ویژگی‌هاست. پس از استخراج ویژگی‌ها، مقایسه با الگوهای ذخیره شده انجام شده، میزان تطابق و شباهت بررسی می‌شود. در صورتی که درصد تطابق بالا باشد، امضا شناسایی می‌گردد. برای افزایش دقت، معمولاً الگوریتم‌های یادگیری ماشین، شبکه‌های عصبی و الگوریتم‌های تشخیص الگو استفاده می‌شود.

در همین راستا، روش‌های یادگیری عمیق به عنوان رویکردی نوین در حوزه شناسایی امضای آفلاین بسیار مورد توجه است. این روش‌ها با استفاده از شبکه‌های عصبی عمیق، با مدل‌ها و الگوریتم‌هایی پیچیده، قادر به استخراج ویژگی‌های معنادارتری از امضاها هستند و توانایی تشخیص دقیق‌تر و قابلیت تعمیم‌پذیری بالاتری ارائه می‌دهند.

در این مقاله، به بررسی معماری‌های شبکه‌های عصبی عمیق مورد استفاده در شناسایی امضای آفلاین، استخراج ویژگی‌های امضا، و روش‌های آموزش و بهینه‌سازی این شبکه‌ها می‌پردازیم. همچنین، مجموعه داده‌های مورد استفاده و معیارهای ارزیابی در شناسایی امضای آفلاین را بررسی خواهیم کرد.

۲- پیشینه پژوهش

افراسیابی و منصوری زاده در تحقیقی با عنوان "تشخیص امضا با استفاده از شبکه عصبی و مقایسه امضای ایرانی و خارجی" به استخراج ویژگی‌های محلی و عمومی از امضاها ایرانی و خارجی پرداختند. آن‌ها

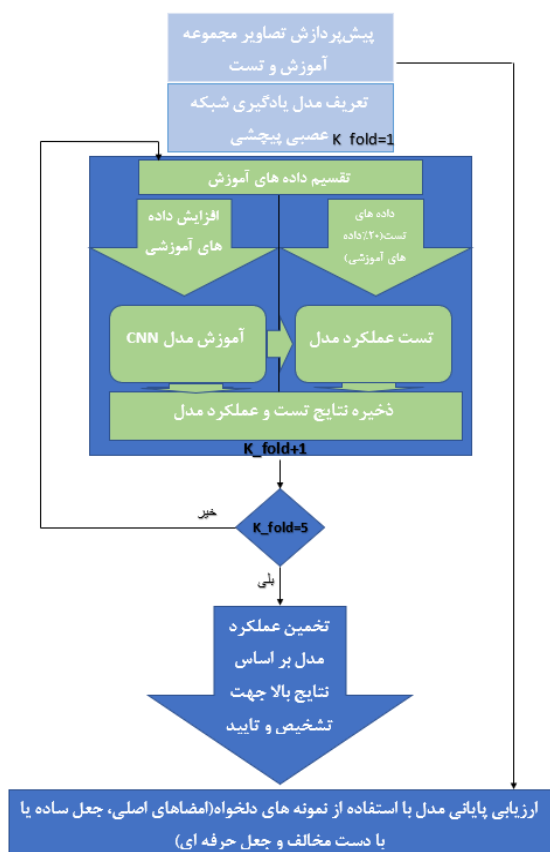
با استفاده از ویژگی‌های گشتاور ثابت و تبدیل موجک در دو شبکه عصبی مجزا، یکی برای تشخیص امضا و دیگری برای جعلی بودن یا نبودن مبادرت به تشخیص و آموزش امضا کردند. ویژگی‌های استخراج شده در شبکه عصبی پرسپترون بررسی شد و محققین نتیجه گرفتند که امضاها را خارجی نسبت به جعلی بودن حساس‌ترند، ولی نسبت تشخیص امضا در نمونه‌های ایرانی بیشتر است. [۱]

عبدی پور و همکاران در تحقیقی با نام "تشخیص امضا توسط یک الگوریتم داده‌کاوی قوی و ارائه یک دسته ویژگی" به مطالعه الگوریتم انتخاب ویژگی به منظور تشخیص صحت امضا پرداختند. آن‌ها با استفاده از روش انتخاب ویژگی FS-SFS^۲ و الگوریتم دسته‌بندی ماشین بردار پشتیبان، از بین ویژگی‌های بافت تصویر که توسط روش‌های استخراج ویژگی گابور و LBP^۳ و HOG^۴ به دست آمدند، را انتخاب کردند. ویژگی‌های انتخاب شده به شبکه عصبی پرسپترون چندلایه برای دسته‌بندی داده شد. محققین نتیجه گرفتند که الگوریتم پیشنهادی، انعطاف‌پذیری بسیار بالایی در تشخیص گونه‌های مختلف امضا دارد. [۲]

الهام کشاورز و همکاران در تحقیقی با عنوان "تشخیص امضای آفلاین با استفاده از بردار پشتیبان" با استفاده از روش‌های استخراج ویژگی moment و HOG و LBP مبادرت به ساخت بردار ویژگی نمودند که یک خط متمایزکننده بین امضاها را اصلی و جعلی باشد. نتایج به دست آمده از استخراج ویژگی منجر به تولید الگویی با حفظ فاصله اطمینان با اندازه قابل تنظیم مرز جداکننده بین نمونه‌های اصلی و جعلی شد. محققین نتیجه گرفتند که این الگوریتم نسبت به داده‌های نویزی و داده‌های جدید پایداری بالایی دارد و قدرت تعمیم آن بالاست. در مقابل نسبت به داده‌های زیاد هزینه محاسباتی زیادی دارد. همچنین وابسته به انتخاب ویژگی است که تعیین کننده بردار پشتیبان برای تعیین مرز بین امضاهاست. [۳]

جیوش پودار و همکاران در تحقیقی تحت عنوان "تشخیص امضای آفلاین و تشخیص جعل با استفاده از یادگیری عمیق" تلاش داشتند تا روشی جدید برای تأیید و تشخیص امضا ارائه کنند. آن‌ها از الگوریتم CNN برای شناسایی و الگوریتم SURF و Haris برای تشخیص جعل بهره‌بردند که در هر الگوریتم پیش‌پردازش جداگانه‌ای روی تصاویر انجام شد. محققین نتیجه گرفتند که این روش با کمترین خطا امضاها را جعلی را شناسایی می‌کند و برای احراز هویت چندین سند مانند چک، سوابق حقوقی، گواهینامه‌ها و غیره می‌توان از این روش کمک گرفت. [۴]

ویکتوریا ریز و همکاران در مقاله‌ای با نام "تأیید دست‌نویس امضا آفلاین با استفاده از تولید مصنوعی ترکیبی از امضاها و شبکه‌های عصبی سیامی" استفاده از شبکه‌های عصبی سیامی را برای کمک به حل مشکل تأیید امضای دستی آفلاین با جعل‌های تصادفی در زمینه‌ای مستقل از نویسنده پیشنهاد دادند. آن‌ها با ترکیب امضاها مصنوعی با امضاها واقعی دی‌تاست‌هایی از جمله CEDAR و MCYT و GPDSSynthetic و SigComp^{۱۱} و کم کردن پارامترهای شبکه



شکل ۱: فلوچارت تشخیص امضا بر اساس شبکه‌های عصبی پیچشی

۳-۱- شبکه عصبی پیچشی

یادگیری عمیق شاخه‌ای از الگوریتم‌های یادگیری ماشین است که بر روش‌های مبتنی بر شبکه‌های عصبی مصنوعی تمرکز دارد. شبکه‌های عصبی پیچشی به عنوان یکی از الگوریتم‌های یادگیری عمیق در حوزه‌ها و کاربردهای متفاوتی استفاده می‌شوند اما به صورت ویژه در پروژه‌های پردازش ویدئو، عکس و بینایی ماشین کارایی بالایی دارند. بینایی ماشین همچون چشم انسان تصاویر را می‌آموزد و نتایج خوبی را به منظور تشخیص و دسته‌بندی تصاویر ارائه می‌دهد. شبکه‌های عصبی پیچشی به گونه‌ای طراحی شده‌اند که روی ورودی‌های با ساختار ماتریسی (دو بعدی و سه بعدی) به خوبی کار کرده، ساختار ورودی را عوض نمی‌کنند، بنابراین به ارتباط بین پیکسل‌های همسایه اهمیت می‌دهند. همین امر باعث می‌شود که ویژگی‌های معنادارتری را از تصاویر طی فرایند آموزش یادگیرند. لایه‌های مختلف شبکه عصبی پیچشی عبارت‌اند از:

- لایه ورودی: تصاویر امضا تبدیل به باینری شده و در سه کانال رنگ RGB^۰ آماده ورود به لایه پیچشی می‌شوند.
- لایه پیچشی: لایه‌ای است با اندازه‌های مختلف که روی تصاویر عمل پیچش را انجام می‌دهد. در واقع روی تصویر فیلترهای خاصی اعمال شده، نتیجه عمل پیچش روی آن‌ها به لایه‌های بعد اعمال می‌گردد.

نتایج بهتری در تشخیص امضا به روش شبکه‌های عصبی سیامی به دست آوردند. محققین نتیجه گرفتند که داده‌های مصنوعی در برابر داده‌های افزوده در تشخیص جعل و روند آموزش بهتر عمل می‌کنند. [۵] الیاس زویبدر مقاله‌ای با عنوان "تأیید امضای مستقل از نویسنده بر اساس روابط پیکسل‌های نامتقارن و مجموعه داده‌های غیرمستقیم آزمایش" به وسیله آموزش غیرمستقیم از ۴ پایگاه داده امضا استفاده کردند و یک طرح تشخیص ویژگی ارائه دادند که به انتقال‌های مرتبه اول بین آرایش‌های شبکه نامتقارن ساختارهای پیکسل ساده متکی است. آن‌ها با استفاده از الگوریتم انتخاب ویژگی در یک فضای فاصله که بر اساس رویکرد عدم شباهت تشکیل شده، پیکسل‌های نامتقارن دو تصویر را مقایسه کرده و اصل یا جعلی بودن امضا را تشخیص دادند. محققین به این نتیجه رسیدند که در امضاها مقدار نازکی تصویر می‌تواند در تخمین خطا مؤثر باشد. [۶]

در روش‌های قبلی ابتدا روی تصاویر پیش‌پردازش‌های مختلفی صورت می‌گرفت، حساسیت نسبت به جابجایی تصاویر، مرکز ثقل و تغییر اندازه تصویر و ... همچنین نحوه استخراج ویژگی بسیار مهم بود و بر اساس همین ویژگی‌های استخراج شده آموزش و تشخیص صورت می‌گرفت. با استفاده از شبکه‌های عصبی پیچشی این چالش‌ها نیز از پیش رو برداشته شد. استخراج ویژگی در روند آموزش انجام می‌گردد و دیگر حساسیت نسبت به جابجایی به دلیل حفظ ارتباط پیکسل‌های همسایه نیز حل شد.

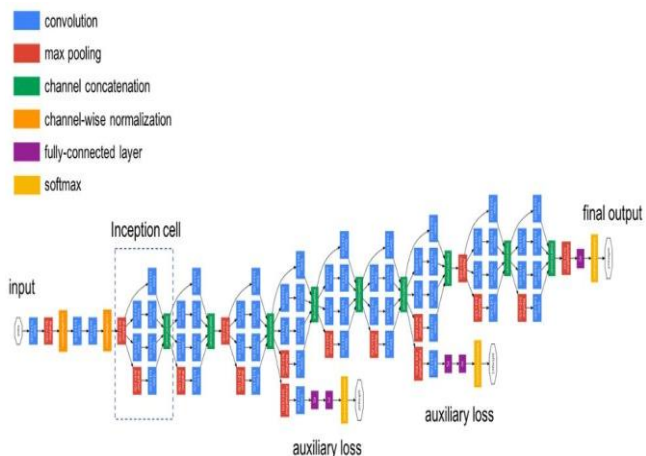
۳- روش پیشنهادی

شناسایی امضا یکی از ساده‌ترین راه‌ها برای تشخیص هویت فردی است. با توجه به پیشینه تحقیق، متوجه شدیم یکی از نقاط ضعف روش‌های قبلی شناسایی امضا، وابستگی زیاد به شیوه انتخاب ویژگی و همچنین نیاز به پیش‌پردازش‌های مختلف روی تصاویر بود. بنابراین برای رفع این مشکل از الگوریتم‌های یادگیری عمیق و دو معماری Inception V3 و VGG19 استفاده کردیم که نوعی از شبکه‌های عصبی پیچشی هستند. هدف از انتخاب روش شبکه‌های عصبی پیچشی، این است که برای آموزش روی تصاویر نتایج بهتری دارند.

ابتدا در مرحله پیش‌پردازش، تصاویر، هم‌اندازه ورودی شبکه شدند، سپس مدل از پیش آموزش دیده بارگذاری شده، در ادامه لایه تجمیع میانگین دو بعدی و لایه کاملاً متصل و در نهایت لایه softmax برای دسته‌بندی استفاده شد. تعدادی از تصاویر برای آزمون و بقیه برای آموزش مدل انتخاب گردید، البته برای ارزیابی کارایی مدل از روش k-fold استفاده شده، طی ۵ مرتبه و هر بار به صورت تصادفی تعدادی از تصاویر برای آزمون و مابقی برای آموزش در نظر گرفته شدند و در نهایت میانگین دقت به دست آمده در پایان هر مرحله به عنوان نتیجه دقت در نظر گرفته شد. با توجه به دقت حاصل شده در مدل، توانایی شناسایی امضا و همچنین تأیید جعلی یا اصلی بودن به خوبی معلوم شد. در شکل ۱ نحوه تشخیص امضای مدل به نمایش درآمده است.

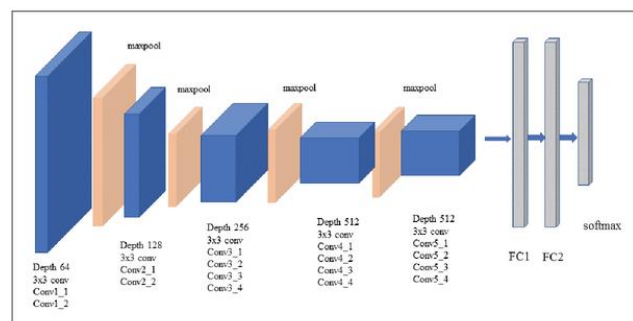
- لایه تجميع: برای تجميع ویژگی هنگام نمونه‌برداری کاهشی استفاده می‌شود، تا بتوان وارد لایه‌های عمیق‌تر شبکه شد.
 - لایه کاملاً متصل که ویژگی ۲ بعدی حاصل را به بردار ویژگی یک‌بعدی برای ادامه فرآیند دسته‌بندی تبدیل می‌کند.
- در این پژوهش با استفاده از دو معماری Inception V3 و VGG19 از شبکه‌های عصبی پیچشی به یادگیری و تشخیص امضا پرداخته شده‌است. در تصویر شماره ۲ نمای کلی این معماری‌ها نشان داده شده‌است.

در مدل Inception V3 از تعدادی بلوک‌های Inception استفاده شده است. این بلوک‌ها شامل چندین فیلتر مختلف برای استخراج ویژگی است که به‌طور موازی تصویر را دریافت‌نموده و مجموع نقشه ویژگی‌های استخراج‌شده به ورودی لایه بعد اعمال می‌شود. با این کار سرعت آموزش مدل خیلی بهتر می‌شود درعین حال که به‌دلیل طراحی خاص این بلوک‌ها بار محاسباتی خیلی زیاد نمی‌گردد.



شکل ۲: مدل Inception V3 [۷]

در شکل ۳ معماری مدل VGG آمده‌است که دارای ۲۱ لایه متشکل از چندین لایه پیچش و تجميع است.



شکل ۳: معماری مدل VGG19 [۸]

۳-۲- یادگیری انتقالی

آموزش مدل از ابتدا، بسیار زمان‌بر است و تنظیم تمام پارامترها برای رسیدن به نتیجه مطلوب دشوار خواهد بود. یکی از مزیت‌های یادگیری عمیق به‌خصوص در حوزه بینایی ماشین که نیاز به محاسبات بالا را کمتر می‌کند، استفاده از یادگیری انتقالی است. یادگیری انتقالی به استفاده از دانشی گفته می‌شود که یک مدل برای حل مسئله‌ای با حجم زیادی داده به‌دست آورده و برای مسئله دیگری که این حجم از داده را در دسترس ندارد، استفاده می‌کند.

برای پایه کار آموزش مدل با تصاویر امضا، از مدلی از پیش آموزش‌دیده با وزن‌های دیتاست MNIST از گیت هاب استفاده شد. در تشخیص امضا با استفاده از یادگیری انتقالی، کار لایه‌های اول و میانی که به‌ترتیب تشخیص لبه‌ها و تشخیص شکل‌هاست، بر اساس وزن‌های از پیش دانلودشده انجام می‌شود و فقط لایه‌های آخر را دوباره آموزش می‌دهیم تا به خروجی مطلوب برسیم. بنابراین آموزش تنها روی لایه‌های جدید که مطابق با دسته‌بندی مدنظر است انجام خواهد شد.

خروجی مدل‌های آموزش‌دیده با دیتاست MNIST با ۱۰۰۰ دسته مجزا انجام شده‌است. درحالی‌که برای مدل دسته‌بندی امضا در این مقاله ۱۱۵ کلاس امضا موجود است. بنابراین به پیش تنظیم خروجی برای دسته‌های موردنظر نیاز است. برای این کار از یک لایه تجميع میانگینی^۶ استفاده می‌شود. اضافه کردن یک لایه کاملاً متصل^۷ روشی متداول برای یادگیری ترکیبات غیرخطی از ویژگی‌های سطح بالاست که توسط خروجی لایه پیچشی نمایش داده می‌شوند. لایه کاملاً متصل، یک تابع غیرخطی احتمالی در آن فضا را یاد می‌گیرد. اما تعداد پارامترهای مدل را افزایش می‌دهد و هزینه محاسباتی را بالاتر خواهد برد؛ به همین دلیل از تجميع میانگینی استفاده می‌شود که وظیفه کاهش اندازه مکانی (فضایی) ویژگی پیچش‌شده را برعهده دارد. این کار به‌منظور کاهش توان محاسباتی مورد نیاز برای پردازش داده‌ها از طریق کاهش ابعاد صورت می‌گیرد. پس از این کاهش، از یک لایه کاملاً متصل استفاده می‌شود.

۳-۳- دیتاست

دیتاست مورد استفاده در این مقاله شامل ۳۱۰۵ تصویر امضا است که از ۱۱۵ نفر و از هر نفر ۲۷ امضا گرفته شده‌است. این دیتاست توسط دانشگاه تهران و با نام UTSig ثبت شده‌است. از این مجموعه به‌صورت تصادفی تعداد ۶۲۱ تصویر یعنی ۲۰٪ دیتاست برای آزمایش و تعداد ۲۴۸۴ تصویر برای آموزش به‌کاربرده می‌شود. این تعداد با استفاده از داده افزایی ۴ برابر می‌شود و با تعیین دسته‌های آموزش یا batch های ۱۲۵ تایی در هر دور آموزش، در مجموع ۷۸ دسته وجود خواهد داشت.

شکل ۴ نمونه امضاهایی از چهار دسته از این دیتاست را نشان می‌دهد. امضاکنندگان به‌صورت تصادفی و ناشناس از بین دانشجویان کارشناسی و کارشناسی‌ارشد دانشگاه تهران و صنعتی شریف انتخاب شده‌اند. سن آن‌ها بین ۱۸ تا ۳۱ سال (میانگین ۲۴) و ۹۰ درصد آن‌ها دست‌راست-نویس بودند. [۹]

- تابع بهینه‌ساز: به الگوریتم‌ها یا روش‌هایی اطلاق می‌شود که برای تغییر ویژگی‌های شبکه عصبی از قبیل وزن و نرخ یادگیری به کار برده می‌شوند.
- نرخ یادگیری: یک ابر پارامتر است که میزان تغییر مدل را در پاسخ به خطای تخمینی در هر بار به‌روزرسانی وزن مدل کنترل می‌کند.
- تابع زیان^{۱۰}: تابعی برای محاسبه خطای مدل است که بهینه‌ساز برای کم کردن آن تلاش می‌کند.
- متریک: معیار ارزیابی شبکه عصبی.

همچنین باید تعداد دوره‌های تکرار و اندازه دسته‌ها برای آموزش نیز تنظیم شود که روی کیفیت آموزش تأثیری می‌گذارد. این پارامترها در پژوهش حاضر پس از چندین بار آموزش و سعی و خطا به این صورت تنظیم شده است:

برای مدل Inception V3: تابع بهینه‌ساز ADAM، نرخ یادگیری ۰.۰۰۰۰۱، تابع خطای آن‌تروپی متقاطع دودویی^{۱۱}، متریک دقت و همچنین تعداد تکرار ۱۰۰ دور.

برای مدل VGG: تابع بهینه‌ساز RMSprop، نرخ یادگیری ۰.۰۰۰۰۵۵ و بقیه پارامترها مانند مدل Inception V3، با نرخ یادگیری ۰.۰۰۰۰۱ مدل VGG19 دچار بیش‌برازش شد و روند آموزش نتایج خوبی نداشت.

۳-۵-۱- بررسی تعداد پارامترها در مدل

بعد از بارگذاری مدل، لازم است مطابق دسته‌بندی جدید (یعنی ۱۱۵ دسته امضا)، لایه‌های جدید اضافه شوند. لایه flatten، لایه‌ای است که تمام ویژگی‌های لایه‌های قبل را به یک بردار ویژگی تبدیل می‌کند تا بتوان دسته‌بندی را انجام داد؛ اما این لایه به شدت تعداد پارامترها را بالا می‌برد. برای اینکه تعداد پارامترها کاهش یابد و بار محاسباتی کمتر شود از یک لایه تجمیع میانگین قبل از آن استفاده شد. در جدول ۱ تعداد پارامترهای هر دو مدل با استفاده از لایه flatten و لایه تجمیع میانگین مقایسه شده است. در مدل Inception V3 در صورتی که لایه flatten را اضافه کنیم تعداد پارامترها حدود ۱۵۶ میلیون می‌شود که حدود ۱۳۶ میلیون پارامتر آن باید آموزش ببیند و تعداد پارامترها با لایه تجمیع میانگین به مقدار ۲۴ میلیون پارامتر می‌رسد که تنها ۲ میلیون پارامتر آن برای آموزش است. تعداد پارامترها در مدل Inception V3 به دلیل بلوک‌های موازی Inception بیشتر از VGG19 است، ولی در مقابل سرعت و عملکرد مدل برای یادگیری بهتر شده است.



شکل ۴: نمونه‌های امضای دیتاست فارسی [۹]

۳-۴- داده‌افزایی^۸

یکی از نیازهای شبکه عصبی پیچشی، دیتاست بزرگ است، تا شبکه برای آموزش از عهده بار محاسباتی و پیچیدگی مدل برآید و بتواند ویژگی‌های مدل را در لایه‌های مختلف شبکه عصبی استخراج کرده، رو به بیش‌برازش^۹ نرود. طرز کار شبکه‌های عصبی به این صورت است که در هر لایه از مدل، ویژگی‌های مختلفی از تصویر را استخراج می‌کند. در لایه‌های بالاتر، ویژگی‌های سطح بالاتر و لایه‌های پایین‌تر ویژگی‌های ساده‌تر تصویر استخراج می‌شود. تعداد تصاویر به دلیل تعدد لایه‌های پیچشی، باید زیاد باشد و در صورت کم بودن تعداد تصاویر برای آموزش بهتر باید به گونه‌ای این کمبود را جبران نمود.

تعداد تصاویر دیتاست استفاده شده در این مقاله کم است که برای حل این مشکل از روش داده‌افزایی استفاده شد. داده‌افزایی تکنیکی است که برای افزایش تعداد داده‌ها با افزودن کپی‌های کمی تغییر یافته از داده‌های موجود استفاده می‌شود. این کار به کاهش بیش‌برازش در هنگام آموزش یک مدل یادگیری ماشین کمک می‌کند. در این مقاله برای ایجاد کپی از روش چرخش به میزان ۵ درجه و بزرگنمایی تصویر ۱۱۷٪ استفاده شده است. یکی از نکات مهم داده‌افزایی این است که این کار نباید ماهیت اصلی تصویر را از بین ببرد. به عنوان مثال امضایی با زاویه چرخش ۹۰ درجه، یک امضای جدید تلقی خواهد شد و قابل قبول نیست. بنابراین اگر چرخش امضا مدنظر است باید حد درست رعایت شود.

داده‌افزایی دو حالت آفلاین و آنلاین دارد؛ در حالت آفلاین بار محاسباتی بالاتر خواهد شد؛ چراکه از ابتدا داده‌ها چند برابر شده و دیتاست بزرگ‌تر می‌شود و بار محاسباتی زیادی به شبکه اعمال می‌شود. اما در حالت آنلاین که در این مقاله استفاده شده، دیتاست تغییری نخواهد داشت و در هر دور آموزش داده‌ها در هر دسته اضافه شده و در نتیجه آزمون دخالتی نخواهند داشت.

۳-۵- پارامترها

مدل، آبر پارامترهای مختلفی دارد که باید تعیین شود:

جدول ۱: بررسی تعداد پارامترهای مدل‌های VGG19 و Inception V3

ردیف	روش یادگیری	لایه	تعداد کل پارامتر	تعداد پارامتر قابل آموزش
۱	Inception	flatten	۱۵۶,۱۴۰,۴۳۶	۱۳۴,۳۳۷,۶۵۲
۲	Inception	AveragePooling2D	۲۴,۰۱۹,۸۶۰	۲,۲۱۷,۰۷۶
۳	VGG19	flatten	۳۳,۰۳۱,۰۹۲	۱۳,۰۰۶,۷۰۸
۴	VGG19	AveragePooling2D	۲۰,۶۶۸,۵۹۶	۶۴۴,۲۱۲

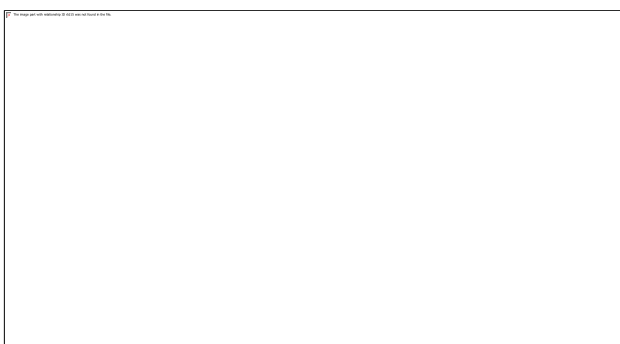
۳-۶- پیاده‌سازی

پیاده‌سازی این برنامه با زبان برنامه‌نویسی پایتون و در محیط اسپایدر انجام شده است. ابتدا تصاویر امضا از دیتاست UTSig دانلود و به منظور یادگیری ویژگی‌های امضا به آدرس محل تصاویر آموزشی در برنامه منتقل می‌شود.

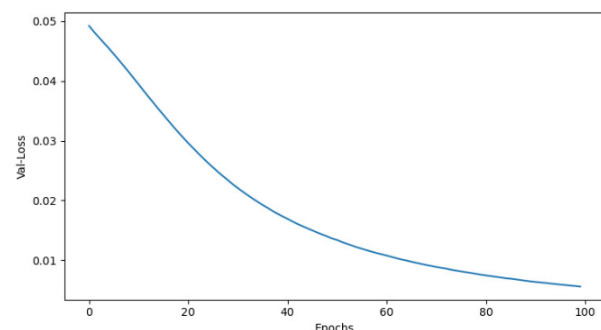
در شبکه‌های عصبی پیچشی، معمولاً پیش‌پردازش خاصی روی تصاویر انجام نمی‌شود، تنها اندازه تصاویر همسان با اندازه ورودی شبکه با ابعاد برابر با $299 \times 299 \times 3$ در Inception V3 و $224 \times 224 \times 3$ در مدل VGG تغییر داده شده و استانداردسازی می‌گردد. پس از پیش‌پردازش، مدل بارگذاری شده و ابر پارامترها تنظیم می‌گردند. سپس داده‌افزایی روی داده‌های آموزشی انجام شده، در نهایت آموزش مدل صورت می‌گیرد.

۴- نتایج

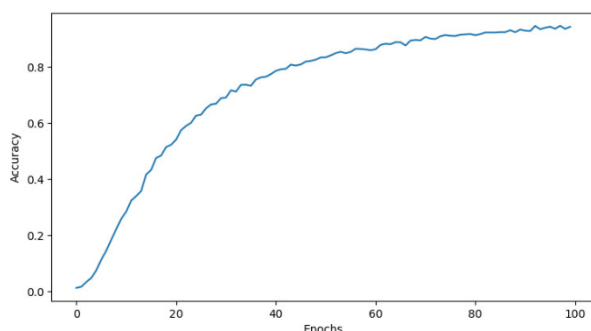
نتیجه آموزش مدل در ۱۰۰ بار تکرار، شامل خطای مدل، خطای آموزش، دقت مدل (دقت آزمایش) و دقت آموزش برای مدل Inception V3 در شکل ۵ و برای مدل VGG19 در شکل ۶ نشان داده شده است. همان‌طور که مشاهده می‌شود، مدل Inception V3 در نهایت به دقت ۹۴,۳٪ و خطای ۰,۰۵۸٪ رسید. اما برای مدل VGG19 دقت ۸۰٪ و خطای ۰,۱۵۴ به دست آمد که نسبت به مدل Inception V3 دقت کمتر و خطای بالاتری دارد. البته مدل VGG19 نسبت به Inception V3 کندتر است و نیاز به زمان بیشتری برای آموزش دارد.



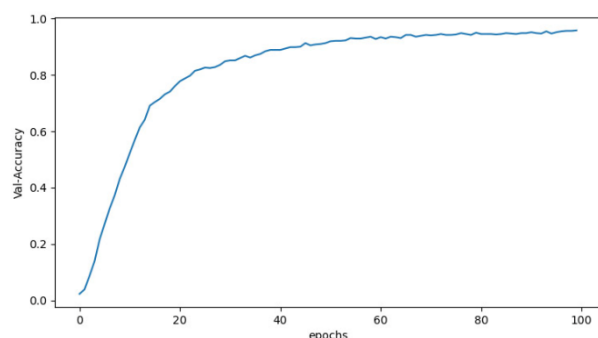
(الف)



(ب)



(ج)



(د)

شکل ۵: نمودارهای مربوط به Inception V3 - (الف) خطای مدل، (ب) خطای آموزش مدل، (ج) دقت مدل، (د) دقت آموزش مدل.

در نظر گرفته شدند و مابقی برای آموزش و این کار برای ۵ مرتبه تکرار شد تا از نتایج آن مدل ارزیابی شود.

جدول ۲: دقت و خطای به دست آمده در روش Inception V3 با استفاده از ارزیابی k-fold

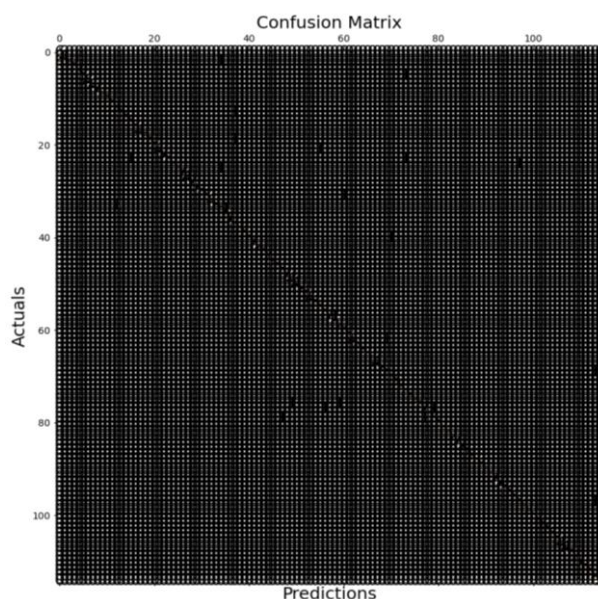
Fold5	Fold4	Fold3	Fold2	Fold1	K_fold
0.9339	0.9472	0.9504	0.9428	0.9416	Accuracy
0.00597	0.00578	0.00578	0.00577	0.0057	Loss

جدول ۳: دقت و خطای مدل در روش VGG19 با استفاده از ارزیابی k-fold

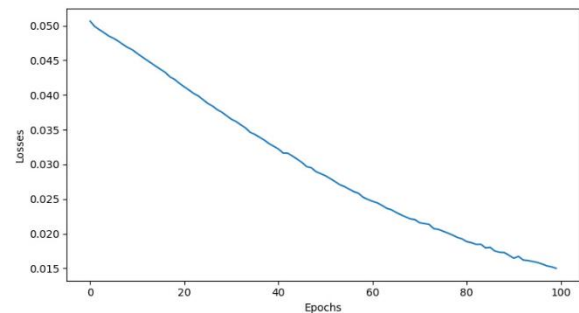
Fold5	Fold4	Fold3	Fold2	Fold1	K_fold
0.803	0.82	0.81	0.78	0.79	Accuracy
0.015	0.015	0.016	0.016	0.015	Loss

مقدار دقت به دست آمده طی ۵ بار تکرار در ارزیابی k-fold برای مدل Inception V3 به شرح جدول ۲ است که متوسط دقت مدل Inception V3 برای تشخیص امضا ۹۴٫۳٪ و متوسط زبان ۰٫۰۰۵۸ به دست آمد و در مدل VGG19 که در جدول ۳ مقدار دقت و خطای طی ۵ بار ارزیابی دقت ۸۰٪ و خطای ۰٫۰۱۵۴ به دست آمد. با توجه به نتایج مدل Inception V3 عملکرد بهتری نسبت به VGG19 داشت.

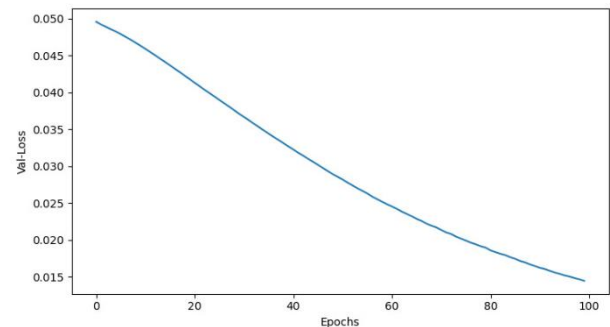
ماتریس درهم‌ریختگی^{۱۲} در مدل Inception V3 برای تشخیص امضا در تصویر ۷ نشان می‌دهد که عملکرد مدل چگونه بوده است. قطر اصلی ماتریس نشانگر عملکرد تصویر است و پراکندگی‌های خارج از قطر اصلی نمونه امضاهایی را نشان می‌دهد که مدل به اشتباه برچسب‌گذاری کرده است.



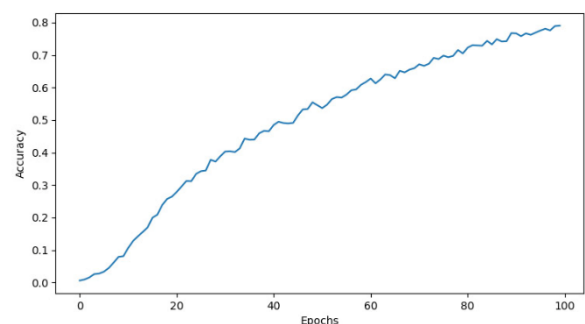
شکل ۷: ماتریس درهم‌ریختگی تشخیص امضای مدل Inception V3



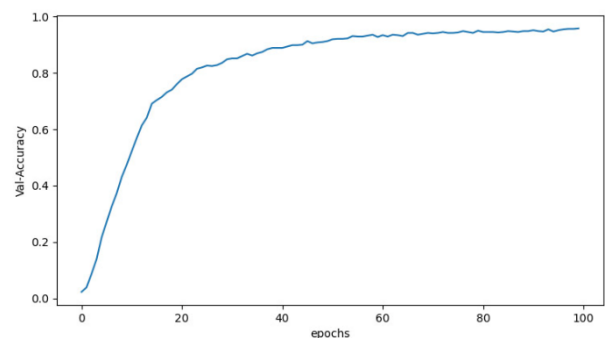
(الف)



(ب)



(ج)



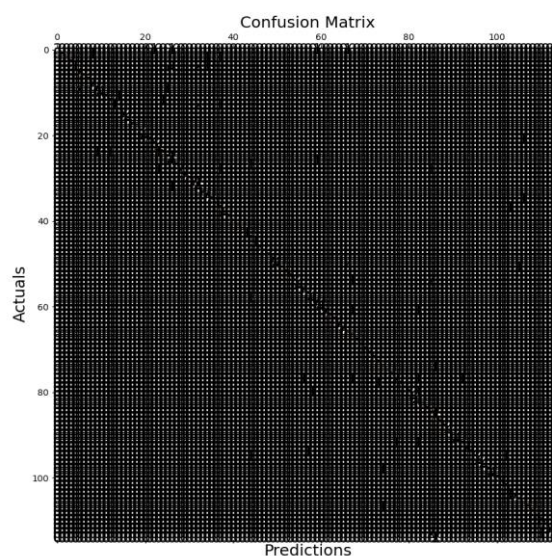
(د)

شکل ۶: نمودارهای مربوط به VGG19 - (الف) خطای مدل، (ب) خطای آموزش مدل، (ج) دقت مدل، (د) دقت آموزش مدل.

۱-۴- ارزیابی

در این مقاله برای ارزیابی مدل و اطمینان از عملکرد آن از روش اعتبارسنجی تقاطعی k-fold استفاده شده و مقدار $k=5$ در نظر گرفته شد؛ یعنی هر بار ۲۰٪ از داده‌های دیتاست به‌طور تصادفی برای ارزیابی

در شکل ۸ ماتریس درهم‌ریختگی برای مدل VGG19 محاسبه شده‌است.



تصویر ۸ : ماتریس درهم‌ریختگی تشخیص امضا مدل VGG19

۴-۲- مقایسه

روش‌های قبلی حساسیت زیادی نسبت به نویز، مرکز ثقل امضا، زاویه امضا و چرخش، اندازه امضا و حتی رنگی بودن دارند که نیاز به پیش‌پردازش زیادی روی تصاویر است. همچنین لازم است ویژگی‌های مختلفی از امضا استخراج شود که بسته به روش استخراج ویژگی نیز متفاوت خواهد بود و سپس برای به‌دست‌آوردن بهترین ویژگی‌ها، آن‌ها با هم مقایسه و احتمالاً ترکیب می‌شوند. درواقع معمولاً یافتن ویژگی مناسب از خود فرایند آموزش سیستم، زمان بیشتری می‌برد.

در روش شبکه‌های پیچشی عمیق ساختار ورودی تغییر نمی‌کند بنابراین به‌دلیل حفظ اتصال محلی، ارتباط بین پیکسل‌های همسایه نیز بررسی و آموخته می‌شود. همین امر باعث می‌شود مدل نسبت به نویز و اندازه و حتی مرکز ثقل حساس نباشد و نیاز به پیش‌پردازش خاصی نباشد. همچنین استخراج ویژگی برخلاف روش‌های قبلی که نیاز به محاسبات و عملیات پیچیده داشت، با استفاده از هسته‌های مختلف در حین آموزش به‌دست می‌آید.

سلیمانی و همکاران در مقاله‌ای با عنوان "UTSig یک دیتاست امضای آفلاین ایرانی"، با استفاده از روش ماشین بردار پشتیبان به طور سطحی به بررسی تشخیص امضا پرداخته‌است. [۹]

طبق جدول ۴ دقت روش مقاله فوق برابر با ۸۸٪ و خطا ۰٫۴۵ گزارش شده اما در روش پیشنهادی در این مقاله با استفاده از مدل Inception V3، نتیجه بهتری حاصل شده و دقت ۹۴٫۳٪ و خطای ۰٫۰۵۸ به‌دست آمد.

جدول ۴ : مقایسه دقت و خطای مدل در تشخیص امضا

روش	خطای آموزش	خطای آزمون	دقت آموزش	دقت آزمون
سلیمانی و همکاران [۹]	۰٫۲	۰٫۴۵	۰٫۹۴	۰٫۸۸
روش پیشنهادی	۰٫۰۰۵۸	۰٫۰۰۴	۰٫۹۴۳	۰٫۹۵۴۹

در جدول ۵ امتیاز F1 و فراخوانی دو مدل برای شناسایی امضا نشان داده شده‌است. همان‌طور که مشخص است مدل Inception V3 در مقایسه با مدل VGG به‌تر عمل کرده‌است.

جدول ۵ : امتیاز F1 و فراخوانی

ردیف	مدل	F1 score	Precision	Recall
۱	Inception V3	۰٫۹۵۲۲	۰٫۹۵۵۱	۰٫۹۵۸۳
۲	VGG19	۰٫۸۶۶۷	۰٫۸۶۷۵	۰٫۸۶۸۳

۴-۳- تأیید امضا

علاوه بر شناسایی امضا از مدل پیاده‌سازی شده می‌توان برای تأیید امضا نیز استفاده نمود. شکل ۹ ماتریسی را نشان می‌دهد که برای دسته‌بندی استفاده شده‌است. هر سطر مربوط به یک امضا و هر ستون مربوط به یک دسته (یک فرد) است. در این ماتریس امتیاز هر دسته برای هر امضا ذخیره شده، بیشترین امتیاز در هر سطر برای تشخیص امضا به‌کاربرده می‌شود. به عبارت دیگر شماره ستون مربوط به بیشترین مقدار در هر سطر، برچسب امضا است. مقدار این امتیاز، می‌تواند معیاری برای تأیید جعلی یا اصلی بودن امضا باشد. به این صورت که اگر بیشتر از ۰٫۷ باشد امضا اصلی و کمتر از این مقدار امضا جعلی معرفی خواهد شد.

0	1	2	3	4	5
1.36394e-07	0.886858	6.50842e-05	0.000622914	0.00276016	0.000727309
1.40169e-06	0.758196	0.000995526	0.00781918	0.000830606	0.00101793
3.41621e-08	0.768372	2.13705e-05	0.00529396	0.000142762	0.00118557
5.9265e-09	0.982051	9.88041e-06	0.000675221	6.82612e-05	0.000246122
4.06883e-06	0.331916	0.000680365	0.00135909	6.00239e-05	0.0022336
1.10735e-06	0.747377	0.000225884	0.0377118	0.00116358	0.00537688
8.1868e-07	0.00117619	0.745202	0.00690264	5.51637e-05	0.00891885
5.59319e-07	0.000281121	0.765444	0.00106421	2.03108e-05	0.00116023
9.4374e-07	0.000900214	0.722384	0.00748083	0.000213988	0.00261392
2.80861e-06	0.000595413	0.759692	0.00737251	0.00487452	0.000949852
5.29037e-06	0.00820603	0.00727647	0.138365	0.000786315	0.0389693
1.61608e-06	0.0103146	0.00125742	0.454763	0.00308751	0.0105155
1.34504e-07	0.0194924	0.000779455	0.622581	0.0533876	0.0322995
1.60567e-06	0.00965552	0.00371352	0.3124	0.00153755	0.0145692
5.42946e-07	0.00405434	0.00265197	0.0554087	0.0133683	0.0644154
1.57284e-06	0.000361797	0.0198637	0.827979	0.00134555	0.0173524

تصویر ۹ : ماتریس حاصل از امتیاز دسته‌بندی در خروجی مدل

پس از آموزش و تکمیل مدل، مدل ذخیره شده آماده استفاده است. از این مدل می‌توان برای تأیید امضاهای دیگر نیز استفاده کرد. برای این

کار پوشه‌ای به نام test در ابتدای برنامه بارگزاری شد که این پوشه حاوی تصاویر امضای اشخاص شامل امضای اصلی و جعلی است به ترتیب زیر:

- امضای ۱ تا ۳۰ امضای اصلی اشخاص
- امضای ۳۱ تا ۶۰ امضای جعل ساده
- امضای ۶۱ تا ۹۰ امضا با دست مخالف
- امضای ۹۱ تا ۱۱۵ امضای جعل ماهرانه

در شکل ۱۰ و ۱۱ نتیجه تشخیص و تأیید امضای مدل Inception که نسبت به مدل VGG نتیجه بهتری داشت آمده است.

امضای جعل ساده	امضاهای اصلی
امضای نفر ۱۳۱ ام کاملاً جعلی است و از روی نمونه ۱۲ جعل شده است	امضای نفر ۱ ام متعلق به نمونه امضای ۱ و اصلی میباشد
امضای نفر ۲۳۲ ام کاملاً جعلی است و از روی نمونه ۲۲ جعل شده است	امضای نفر ۲ ام متعلق به نمونه امضای ۲ و اصلی میباشد
امضای نفر ۳۳۳ ام مشابه امضای ۳۳ و جعل حرفه ای میباشد	امضای نفر ۳ ام متعلق به نمونه امضای ۳ و اصلی میباشد
امضای نفر ۳۴ با هیچکدام از امضاهای پایگاه داده مطابقت ندارد	امضای نفر ۴ ام متعلق به نمونه امضای ۴ و اصلی میباشد
امضای نفر ۳۵ ام مشابه امضای ۳۵ و جعل حرفه ای میباشد	امضای نفر ۵ ام متعلق به نمونه امضای ۵ و اصلی میباشد
امضای نفر ۳۶ ام متعلق به نمونه امضای ۳۶ و اصلی میباشد	امضای نفر ۶ ام متعلق به نمونه امضای ۶ و اصلی میباشد
امضای نفر ۳۷ ام کاملاً جعلی است و از روی نمونه ۶۳ جعل شده است	امضای نفر ۷ ام متعلق به نمونه امضای ۷ و اصلی میباشد

شکل ۱۰: نتیجه تشخیص و تأیید امضاهای اصلی و جعل ساده

امضای جعل ماهرانه	امضای با دست مخالف
امضای نفر ۹۱ ام کاملاً جعلی است و از روی نمونه ۱۸ جعل شده است	امضای نفر ۶۱ با هیچکدام از امضاهای پایگاه داده مطابقت ندارد
امضای نفر ۹۲ ام متعلق به نمونه امضای ۹۲ و اصلی میباشد	امضای نفر ۶۲ با هیچکدام از امضاهای پایگاه داده مطابقت ندارد
امضای نفر ۹۳ ام کاملاً جعلی است و از روی نمونه ۹۳ جعل شده است	امضای نفر ۶۳ با هیچکدام از امضاهای پایگاه داده مطابقت ندارد
امضای نفر ۹۴ با هیچکدام از امضاهای پایگاه داده مطابقت ندارد	امضای نفر ۶۴ با هیچکدام از امضاهای پایگاه داده مطابقت ندارد
امضای نفر ۹۵ ام متعلق به نمونه امضای ۹۵ و اصلی میباشد	امضای نفر ۶۵ ام متعلق به نمونه امضای ۶۵ و اصلی میباشد
امضای نفر ۹۶ ام کاملاً جعلی است و از روی نمونه ۹۶ جعل شده است	امضای نفر ۶۶ ام مشابه امضای ۴۴ و جعل حرفه ای میباشد
امضای نفر ۹۷ ام کاملاً جعلی است و از روی نمونه ۲۹ جعل شده است	امضای نفر ۶۷ ام کاملاً جعلی است و از روی نمونه ۸۹ جعل شده است

شکل ۱۱: نتیجه تشخیص و تأیید امضاهای با دست مخالف و جعل ماهرانه

۵- نتیجه گیری

شبکه عصبی پیچشی یکی از روش‌های یادگیری عمیق است که مزایای زیادی مثل دقت یادگیری بالا، استخراج ویژگی سطح بالا به صورت خودکار و مقاوم بودن تصاویر در مقابل تغییر اندازه و مرکز ثقل و ... دارد. در این پژوهش به منظور تشخیص امضا به صورت آفلاین از روش شبکه عصبی پیچشی و دو معماری Inception V3 و VGG19 استفاده شد. برای دستیابی به مدلی با دقت بالا یادگیری انتقالی و داده‌افزایی نیز انجام شد. با توجه به ارزیابی‌ها با استفاده از مدل Inception V3 و VGG19 بر روی دیتاست UTSig به ترتیب دقت ۹۴٫۳٪ و ۸۰٪ حاصل شد. عملکرد مدل Inception V3 بهتر بود و خطای این مدل نیز نسبت به

مدل VGG19 خیلی کمتر شد. همچنین دقت حاصل شده در این مدل نسبت به دقت مدل پایه در مرجع [۹] به میزان ۸٪ افزایش داشت. یکی از سختی‌های این روش یافتن مقدار مناسب ابر پارامترها مانند نرخ یادگیری، تعداد تکرار، اندازه دسته است که برای پیدا کردن بهترین مقدار این ابر پارامترها نیاز به زمان زیاد و سعی و خطا بود که می‌توان آن را با استفاده از روش‌های مانند جستجوی شبکه‌ای^{۱۳} بهبود بخشید.

مراجع

- [1] Afrasiabi, Mansourizadeh, "Signature identification using neural network and comparison of Iranian and foreign signatures", the first Iranian Information Technology Student Conference, Sanandaj, 2018.
- [2] Abdipour, Shokohi Rostami and Naderi, "Signature identification by a strong data mining algorithm and presentation of a feature set", International Conference on Science, Engineering, Technology and Technological Businesses, Tehran, 2018.
- [3] Keshavarz, Jamali and Rafiei, "Offline signature identification using support vector machine", the second conference of new achievements in electrical and computer engineering, Islamic Azad University, Joibar branch, 2013.
- [4] Jivesh Poddara, Vinanti Parikha, Santosh Kumar Bhartia, "Offline Signature Recognition and Forgery Detection using Deep Learning" Pandit Deendayal Petroleum University, Gandhinagar, Gujarat, India 2020
- [5] Victoria Ruiz, Ismael Linares, Angel Sanchez, JoseF. Velez, "Off-line Handwritten Signature Verification using Compositional Synthetic Generation of Signatures and Siamese Neural Networks", 2019
- [6] Elias N. Zois, Alex Alexandridis, George Economou, "Writer Independent Offline Signature Verification based on Asymmetric Pixel Relations and Unrelated Training-Testing Datasets", 2019
- [7] Szegedy, Christian, et al. "Rethinking the inception architecture for computer vision." *Proceedings of the IEEE conference on computer vision and pattern recognition* 2016.
- [8] Breast cancer screening using convolutional neural network and follow-up digital mammography - Scientific Figure on ResearchGate. Available from: https://www.researchgate.net/figure/llustration-of-the-network-architecture-of-VGG-19-model-conv-means-convolution-FC-means_fig2_325137356 [accessed 24 Jan, 2023]
- [9] Amir Soleimani 1,*, Kazim Fouladi 1, Babak N. Araabi, "UTSig: A Persian Offline Signature Dataset", IET journals, 2016,

پی نوشت

- 8 Data augmentation
- 9 Overfitting
- 10 Loss function
- 11 Binary_crossentropy
- 12 Confusion matrix
- 13 Grid search

- 1 <http://mlcm.ut.ac.ir/Datasets.html>
- 2 Sequential Forward Selection
- 3 Local binary pattern
- 4 Histogram Oriented Gradient
- 5 Red, Green, Blue
- 6 Average pooling
- 7 Fully-Connected