ارائه یک روش ترتیبی پویا بر اساس یادگیری عمیق به منظور بهبود کارایی سیستم‌های تطبیق بیومتریکی مبتنی بر کارت هوشمند

محمد صبری، محمدشهرام معین و فربد رزازی

چکیده: امروزه با افزایش تهدیداتی نظیر تروریسم و جرایم سایبری، فرایند تصدیق هویت افراد اهمیت چشم‌گیری یافته و متضمن امنیت ملی یک کشور تلقی می‌گردد. در این پژوهش، یک روش ترتیبی بر اساس یادگیری عمیق جهت مدیریت پویای جریان الگوریتم سیستم‌های تصدیق هویت چند بیومتریکی ارائه شده است. روش پیشنهادی دارای این مزیت است که معیارهای ویژگی به صورت ضمنی و اتوماتیک توسط یک شبکه عمیق با معماری انتها به انتها استخراج می‌گردند. یک سیستم تصدیق هویت چند بیومتریکی شامل دو انگشت و چهره مبتنی بر روش پیشنهادی نیز پیاده‌سازی گردیده است. بر طبق نتایج، در مجموع تصدیق هویت برای ۹۱/۴۲٪ موارد بر اساس اثر انگشت انجام شده و فقط برای ۸/۵۸٪ موارد نیاز به استفاده از مشخصه چهره بوده است. این در حالی است که روش پیشنهادی نسبت به انگشت اول و دوم به ترتیب ۳۵ و ۳۰٪ دقت بالاتری نیز داشته است. دستاوردهای این پژوهش می‌تواند نقش مهمی در مقبولیت و موفقیت پروژه‌های عملیاتی و میزان اثربخشی آنها در فرایند تصدیق هویت داشته باشد زیرا از یک طرف دارای دقت بیشتری بوده و از طرف دیگر منجر به کاهش هزینه یعنی زمان مورد نیاز برای فرایند اخذ و تطبیق گردیده که باعث می‌شود هم‌زمان رضایتمندی خدمت‌گیرنده و امنیت خدمت‌دهنده فراهم آید.

کلیدواژه: **تصدیق هویت، یادگیری عمیق، تطبیق در بستر کارت، چند بیومتریکی.**

۱- مقدمه

نیاز حاکمیتی برای هر دولتی در جهان این است که یک «نظام تصدیق هویتی» دقیق، کارامد و فراگیر در اشل «ملی» برای تک‌تک آحاد ملت برقرار نماید تا بتواند به شکل صحیح به ارائه خدمات پرداخته و در راستای تأمین امنیت و عدالت اجتماعی گام بردارد.

سه روش اصلی برای تصدیق هویت افراد وجود دارد. روش اول بر اساس "آنچه فرد می‌داند" مانند کلمه عبور یا کد شناسایی استوار است. روش دوم متکی بر "آنچه فرد در اختیار دارد" مانند کلید، توکن یا کارت شناسایی است. روش سوم نیز مبتنی بر "آنچه فرد هست" مانند چهره یا صوت می‌باشد. کلمات عبور می‌توانند حدس زده شوند [۱] یا با لیستی از کلمات کاندید مورد حمله واقع شوند [۲]. نتایج پژوهش مؤسسه استاندارد بین‌المللی آمریکا در [۳] ضعف سیستم‌های مبتنی بر کلمه عبور را نشان می‌دهد. توکن یا کارت شناسایی نیز قابل جایگزینی، جعل یا دزدیده‌شدن می‌باشد. بنابراین روش‌های مبتنی بر کلمه عبور یا کارت شناسایی به تنهایی نمی‌توانند امنیت بالایی را فراهم آورند.

امروزه استفاده از روش‌های دسته سوم به صورت روزافزونی رو به افزایش است. بیومتریک بر ویژگی‌های منحصر به فرد فیزیکی (نظیر اثر انگشت، چهره یا عنبیه) یا ویژگی‌های رفتاری (نظیر نحوه راه‌رفتن یا تایپ‌کردن) استوار است. این ویژگی‌ها به سادگی قابل جعل، سرقت یا اشتراک‌گذاری نمی‌باشند [۴]. تصدیق هویت مبتنی بر مشخصه‌های بیومتریک یا به طور خلاصه بیومتریک‌ها، بر این اصل استوار هستند که شخص مدعی "چه کسی است؟" به جای این که "چه چیز می‌داند؟" یا "چه چیز حمل می‌کند؟" [۵]. به این دلایل بیومتریک در بسیاری از کاربردها جایگزین روش‌های سنتی مبتنی بر کلمه عبور یا توکن گردیده است [۶].

بیومتریک نه تنها از دیرباز در کاربردهای حساس نظیر شناسایی مجرمان، کنترل تردد در پادگان‌های نظامی و سایت‌های هسته‌ای مورد بهره‌برداری قرار گرفته است، بلکه امروزه در بخش‌های دولتی و خصوصی نظیر بانک‌ها، ورود به تلفن همراه، اینترنت اشیا و کاربردهای گوناگون دیگر نیز مورد استفاده قرار می‌گیرد. بزرگ‌ترین پروژه بیومتریکی در دنیا در کشور هند با هدف پالایش نظام هویتی طراحی و اجرا شده است. در این پروژه طی مدت هفت سال از جمعیتی در حدود ۱/۲ میلیارد نفر (به طور میانگین یک میلیون نفر در هر روز) مشخصه‌های بیومتریکی شامل ده اثر انگشت، تصویر چهره و عنبیه جمع‌آوری و شماره ملی واحد تحت عنوان Adhaar برای آنها صادر گردیده است[1].

با افزایش تهدیداتی نظیر تروریسم و جرایم سایبری، فرایند تصدیق هویت افراد اهمیت چشم‌گیری یافته و متضمن امنیت ملی یک کشور تلقی می‌گردد. در همین راستا در دهه اخیر، بهره‌برداری از بیومتریک در حوزه اسناد هویتی به سرعت در حال گسترش است. پیشرفت تکنولوژی چاپ و صدور اسناد هویتی و همچنین بهره‌گیری از کارت‌های هوشمند الکترونیکی، باعث شده تا خلق یک هویت جدید از طریق تولید یک سند هویتی جعلی عملاً غیر ممکن باشد. در کشور آمریکا طی یک سال گذشته تعداد ۳.۵۶۴ پرونده مربوط به دزدی پاسپورت مورد بررسی قرار گرفته و ۵۸۳ نفر در این خصوص بازداشت شده‌اند[2]. این آمار مؤید آن است که جاعلین به جای تولید سند جعلی، اخیراً تغییر رویه داده و درصدد سوء استفاده از اسناد متعلق به یک هویت واقعی می‌باشند. برای مقابله با این گونه تهدیدات، امروزه استفاده از مشخصه‌های بیومتریکی به منظور ایجاد ارتباط و وابستگی دایمی بین سند و صاحب سند مورد اقبال قرار گرفته است.

این مقاله در تاریخ ۵ تیر ماه ۱۳۹۷ دریافت و در تاریخ ۲۱ آبان ماه ۱۳۹۸ بازنگری شد.

محمد صبری، دانشکده مهندسی برق و کامپیوتر، دانشگاه آزاد اسلامی، واحد علوم و تحقیقات، تهران، ایران، (email: sabri@srbiau.ac.ir).

محمدشهرام معین (نویسنده مسئول)، پژوهشکده فناوری اطلاعات، پژوهشگاه ارتباطات و فناوری اطلاعات، تهران، ایران، (email: moin@itrc.ac.ir).

فربد رزازی، دانشکده مهندسی برق و کامپیوتر، دانشگاه آزاد اسلامی، واحد علوم و تحقیقات، تهران، ایران، (email: razzazi@srbiau.ac.ir).

1. https://uidai.gov.in/ (2018)

2. https://www.us-passport-service-guide.com/passport-fraud.html (2018)

تکنولوژی تطبیق در بستر کارت هوشمند (MOC)[1] با ترکیب کارت هوشمند و بیومتریک در واقع عملیات تصدیق هویت مبتنی بر دو مؤلفه[2] (آنچه که فرد در اختیار دارد و آنچه که هست) را ارائه می‌دهد و در بسیاری از پروژه‌های عملیاتی مورد استفاده قرار گرفته است. در کشور آمریکا به منظور یکپارچه‌کردن اعتبارنامه‌های شناسایی افراد برای دسترسی به اطلاعات و مدارک دولتی یا واردشدن به اماکن خاص، مطابق با استاندارد FIPS۲۰۱ [۷] برای همه کارمندان و پیمانکاران دولتی کارت هوشمند PIV[3] با قابلیت MOC با دو اثر انگشت صادر گردیده است [۸].

در چنین پروژه‌هایی نمونه گالری (مرجع)[4]، در هنگام ثبت نام افراد اخذ می‌گردد. سپس در زمان صدور کارت، بردار ویژگی استخراج‌شده از نمونه گالری به صورت رمزشده در حافظه امن کارت هوشمند ذخیره می‌گردد. در هر بار فراخوانی سرویس تصدیق هویت توسط کارت، بردار ویژگی نمونه مورد جستجو (پراب)[5] از طریق پروتکل‌های امن و استاندارد برای کارت ارسال می‌شود. سپس عملیات تطبیق در محیط کارت اجرا شده و فقط نتیجه آن برگردانده می‌شود. بدین ترتیب مشخصه بیومتریکی صاحب کارت هرگز از محیط کارت خارج نمی‌شود و فقط توسط خود کارت قابل خواندن است. این طراحی باعث شده تا نیازی به ذخیره اطلاعات بیومتریک در یک پایگاه داده واحد مرکزی وجود نداشته باشد و لذا از این طریق حریم خصوصی حفظ شده و امنیت بالاتری نیز فراهم می‌آید.

البته بهره‌برداری از MOC با چالش‌هایی نیز همراه است. پردازنده‌های تعبیه‌شده در کارت‌های هوشمند دارای منابع پردازشی محدود می‌باشند. لذا به ناچار الگوریتم تطبیق مورد استفاده در MOC باید به نحوی سفارشی‌سازی شود که دارای پیچیدگی محاسباتی کمی باشد. به طور مثال الگوریتم تطبیق مبتنی بر گراف[6] نسبت به چرخش در هر زاویه‌ای مقاوم[7] است [۹]. در حالی که نسخه ساده‌شده الگوریتم تطبیقی که مناسب برای اجرا بر روی پردازنده‌های کارت هوشمند یا موبایل باشد، حداکثر تا ۴۵ درجه می‌تواند نسبت به چرخش مقاوم باشد. حافظه در دسترس کارت برای ذخیره‌سازی بردار ویژگی نیز بسیار محدود می‌باشد و از این رو بردار ویژگی باید به فضای کوچک‌تری نگاشت شده و سپس هرس شود.

در استاندارد ISO ۱۹۷۹۴-۲ [۱۰] برای ذخیره‌سازی اطلاعات هر مینوشیا[8] که به عنوان متداول‌ترین ویژگی قابل استخراج از اثر انگشت شناخته می‌شود، شش بایت برای حالت نرمال در نظر گرفته شده است. این در حالی است که در همین استاندارد برای ذخیره‌سازی هر مینوشیا در کارت هوشمند فقط سه بایت در نظر گرفته شده است. در [۱۱] ارزیابی جامعی برای بررسی میزان افت کارایی محصولات MOC شرکت‌های تجاری مختلف به دلیل وجود این محدودیت‌ها انجام شده و نتایج آن به تفصیل گزارش گردیده است.

علاوه بر محدودیت منابع در دسترس، ذکر این نکته نیز حایز اهمیت است که معمولاً نمونه گالری در زمان ثبت نام در شرایط کنترل‌شده و تحت نظارت اپراتور جمع‌آوری می‌شود. بدین ترتیب در صورت تشخیص اپراتور فرایند نمونه‌برداری تکرار شده و از این رو معمولاً نمونه اخذشده دارای کیفیت مناسبی می‌باشد. این در حالی است که در زمان استفاده از کارت برای فراخوانی سرویس تصدیق هویت، اغلب نمونه پراب در شرایط غیر کنترل شده و بدون دخالت اپراتور اخذ می‌گردد. قرارگیری غیر صحیح انگشت بر روی اسکنر، خشکی یا رطوبت بیش از اندازه پوست هنگام اخذ اثر انگشت، فشار بیش از حد انگشت یا کثیفی سنسور از جمله مشکلات شایع اخذ اثر انگشت در شرایط غیر کنترل شده می‌باشد. لذا در شرایط واقعی همواره نمونه‌های پراب کیفیت پایین‌تری نسبت به نمونه‌های گالری دارند. لازم به ذکر است که با توجه به الگوریتم تطبیق سبک[9] و بردار ویژگی با طول محدود که MOC باید داشته باشد، کارایی آن به شدت تحت تأثیر کیفیت نمونه‌ها قرار می‌گیرد. لذا از یک سو بنا به مشکلاتی که همواره در هنگام اخذ نمونه‌های بیومتریکی وجود دارد و از سوی دیگر بنا به محدودیت‌های منابع پردازشی و ملاحظات الگوریتم تطبیق سفارشی‌شده قابل اجرا بر روی پردازنده‌های کارت هوشمند، کارایی MOC در هنگام استفاده در محیط‌های عملیاتی معمولاً از آنچه انتظار می‌رود بسیار پایین‌تر است. در این صورت ممکن است به کارگیری سرویس تصدیق هویت مبتنی بر کارت مورد اقبال خدمت‌گیرنده و خدمت‌دهنده قرار نگیرد. زیرا از یک طرف افزایش نرخ خطای FNMR[10] (عدم تطبیق یک جفت نمونه مشابه) منجر به نارضایتی خدمت‌گیرنده می‌شود و از طرفی دیگر نیز افزایش نرخ خطای FMR[11] (تطبیق یک جفت نمونه نامشابه) باعث کاهش امنیت سرویس‌های ارائه‌شده توسط خدمت‌دهنده می‌گردد.

برای افزایش دقت یک سیستم تصدیق هویت مبتنی بر بیومتریک، بهره‌برداری از همجوشی چندبیومتریکی[12] بسیار پرکاربرد است. اما با توجه به توضیحات ارائه‌شده در خصوص محدویت‌های MOC، قابلیت بهره‌برداری از چندبیومتریکی به شکل مؤثر توسط آن وجود ندارد. به این منظور در [۱۲] رویکردی بر اساس ساختار سلسله‌مراتبی پویا با هدف افزایش کارایی سیستم‌های MOC مبتنی بر کیفیت مشخصه‌های بیومتریکی ارائه شده است. در این ساختار برای هر مشخصه، مجموعه‌ای از معیارهای کیفیت به صورت صریح و غیر اتوماتیک[13] تعریف می‌گردد و بر اساس آن تصمیم‌گیری در خصوص نحوه انجام عملیات تطبیق اتخاذ می‌گردد. اصولاً در چنین سیستم‌هایی، غایت مقصود این است که سیستمی طراحی شود که در عین فراهم‌آوردن رضایتمندی کاربر (استفاده از حداقل تعداد مشخصه)، دقت مورد نیاز را هم داشته باشد. چالش اصلی در جهت نیل به این هدف، چگونگی تعریف معیارهای کیفیت می‌باشد. به عبارت دیگر چون جریان الگوریتم بر اساس این ویژگی‌ها مدیریت می‌شود، باید تعریف آنها نیز به نحوی باشد که پیش‌بینی‌کننده[14] درستی از نتیجه تطبیق باشند.

تعیین کیفیت مشخصه‌های بیومتریکی همواره یکی از موضوعات مطرح تحقیقاتی می‌باشد. به طور کلی معیارهای کیفیت را می‌توان به دو دسته تقسیم نمود. معیارهای دسته اول کلی بوده و ویژگی‌های سراسری تصویر نظیر Average intensity، Edge spread، Spectral energy و

1. Match on Card
2. Two Factor Authentication
3. Personal Identity Verification
4. Gallery, Reference
5. Probe, Query
6. Graph Matching
7. Rotation Invariant
8. Minutia
9. Light Matching Algorithm
10. False Not Match Rate
11. False Match Rate
12. Multibiometric Fusion
13. Handcrafted Descriptor
14. Predictor

غیره را بررسی می‌کند [۱۳]. دسته دوم معیارهای مختص هر مشخصه بیومتریکی[1] تعریف می‌شود که به طور مثال در [۱۴] برای چهره Pose، Occlusion و در [۱۵] برای اثر انگشت می‌توان از وضوح لبه‌ها[2] و تعداد مینوشیا نام برد. مشکل دسته اول این است که ویژگی‌های کلی تصاویر را بررسی می‌کند که ممکن است ارتباطی با امتیاز شباهت و خطای تطبیق نداشته باشد و لزوماً پیش‌بینی‌کننده امتیاز شباهت نباشد و به همین علت کاربرد کمتری از دسته دوم دارد. مشکل روش دوم این است که اولاً در آن تعداد معیارها محدود می‌باشد و ثانیاً این که پایگاه داده‌ای که شامل همه نمونه‌های دارای مشکل باشد در دسترس نیست. در اغلب پژوهش‌های انجام‌گرفته نیز کارایی معیارهای تعریف‌شده بر روی پایگاه داده کوچک واقعی یا پایگاه داده نسبتاً بزرگ با نویز مصنوعی گزارش شده‌اند [۱۶] تا [۱۸]. به این علت استفاده از این معیارها در محیط‌های واقعی کارایی کمتری از آنچه انتظار می‌رود در پی خواهد داشت.

در این پژوهش به منظور اجتناب از ملاحظات و چالش‌های تعیین ویژگی‌های کیفیت صریح و غیر اتوماتیک، روش جدیدی مبتنی بر یادگیری عمیق[3] جهت مدیریت پویای جریان الگوریتم برای یک سیستم تصدیق هویت چندبیومتریکی با ساختار ترتیبی ارائه گردیده است. روش پیشنهادی دارای این مزیت است که معیارهای ویژگی به صورت ضمنی و اتوماتیک توسط یک شبکه عمیق با معماری انتها به انتها[4] استخراج می‌گردند. بر همین اساس، یک سیستم تصدیق هویت چندبیومتریکی شامل دو انگشت و چهره مبتنی بر روش پیشنهادی نیز پیاده‌سازی گردیده است. نتایج گزارش‌شده نشان می‌دهد که روش پیشنهادی علاوه بر دقت بالاتر، دارای پیچیدگی محاسباتی کمتری نیز می‌باشد که می‌تواند توأمان رضایتمندی خدمت‌گیرنده و امنیت خدمت‌دهنده را در محیط عملیاتی فراهم آورد.

ساختار مقاله به این ترتیب است: بخش دوم به مروری اجمالی بر پژوهش‌های مرتبط اختصاص دارد. در بخش سوم جزئیات روش پیشنهادی شامل معماری شبکه عمیق و نحوه آموزش آن ارائه گردیده است. بخش چهارم شامل مشخصات پایگاه داده، سناریوی ارزیابی، نتایج آزمایشات و تحلیل آن است و در بخش پنجم جمع‌بندی ارائه شده است.

۲- مروری بر پژوهش‌های پیشین

در این بخش ابتدا مروری بر پژوهش‌های مرتبط با تطبیق در بستر کارت صورت خواهد گرفت. سپس روش‌های موجود برای همجوشی مشخصه‌های بیومتریکی بررسی شده و در انتها برخی از پژوهش‌های حاوی کاربردهای یادگیری عمیق در حوزه بیومتریک ارائه شده است.

مقالات منتشرشده مرتبط با سیستم‌های تطبیق در بستر کارت را می‌توان به دو دسته تقسیم نمود. یک دسته با هدف ارائه الگوریتم سبک مناسب پردازنده‌های ضعیف کارت هوشمند بوده و دسته دوم تمرکز بر بررسی امنیت این سیستم‌ها داشته‌اند.

در خصوص دسته اول، روش‌های مختلفی برای تبدیل مختصات مکانی و زاویه مینوشیاها به بردار ویژگی دودویی ارائه شده است. این نحوه ذخیره‌سازی منجر به حصول دقت بالاتر و استفاده حافظه کمتر گردیده و از این رو برای تطبیق در بستر کارت مطلوب می‌باشد.

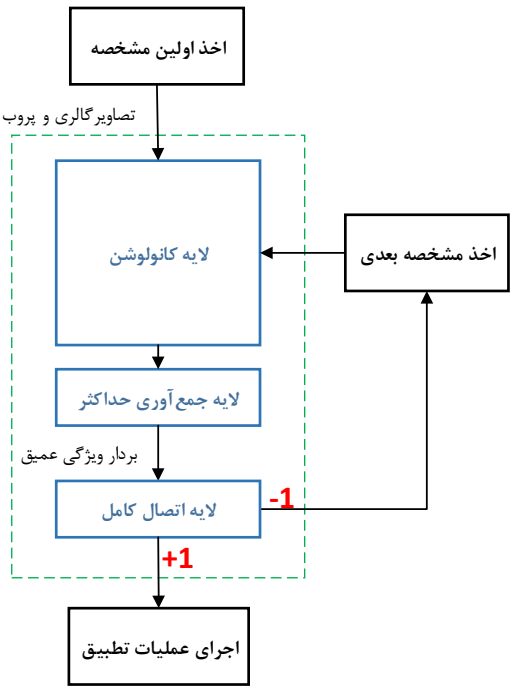
نویسندگان در [۱۹] چهار روش مختلف ذخیره‌سازی دودویی را بررسی و کارایی آنها را در محیط‌های دارای اعوجاج گزارش نمودند. در [۲۰] با هدف ارائه الگوریتم تطبیق با پیچیدگی محاسباتی کم که برای کارت‌های هوشمند مناسب باشد، یک روش کدگذاری و تطبیق ارائه شده است. در این روش علاوه بر اطلاعات مکانی هر مینوشیا، ارتباط مکانی آنها نیز به عنوان معیار ویژگی استخراج شده و در هنگام تطبیق مورد استفاده قرار گرفته است. در این مقاله ادعا شده که با به کارگیری روش کدگذاری پیشنهادی می‌توان بسیاری از مینوشیاهای غیر متناظر در گالری و پروب را هرس نمود و از این طریق پیچیدگی محاسباتی الگوریتم تطبیق را کاهش داد.

در خصوص دسته دوم می‌توان به [۲۱] اشاره داشت که یک چارچوب برای ارزیابی امنیتی سیستم‌های تطبیق در بستر کارت ارائه گردیده است. در [۲۲] نیز آسیب‌پذیری‌های سیستم تطبیق در بستر کارت مورد بررسی قرار گرفته است. در این مقاله با به کارگیری ایده مطرح‌شده در [۲۳] مینوشیاها رمز شده و بدین ترتیب ادعا شده که امکان دستکاری نتیجه تطبیق وجود ندارد.

به غیر از [۱۲] که در ادامه به طور مفصل بررسی خواهد شد، در هیچ یک از این مقالات موضوع استفاده از چندبیومتریکی در سیستم‌های تطبیق در بستر کارت با توجه به محدودیت‌ها و ملاحظات خاص آن مورد تحلیل قرار نگرفته است. البته همجوشی مشخصه‌های بیومتریکی به طور مفصل در ادبیات حوزه بیومتریک بررسی شده که در ادامه به برخی از آنها اشاره می‌شود.

در [۲۴] مروری بر روش‌های گوناگون همجوشی در سطح امتیاز انجام شده و مزایا و معایب هر کدام به تفکیک مورد تحلیل قرار گرفته است. در [۲۵] یک روش ترکیبی در سطح امتیاز برای همجوشی مشخصه‌های تصویر چهره و کف دست ارائه شده است. در این پژوهش کارایی و پیچیدگی روش‌های مختلف همجوشی با روش پیشنهادی مورد تحلیل قرار گرفته است. در [۲۶] یک سیستم تطبیق چهره با همجوشی دینامیکی بر اساس دو الگوریتم Local Binary Pattern و Log Polar Gabor معرفی شده است. به ازای هر درخواست به این سیستم با استفاده از چند طبقه‌بند و "آزمون نسبت احتمال[5]" نوع الگوریتم تطبیق تعیین می‌شود. این روش منجر به کاهش میانگین زمان اجرای فرایند تطبیق و پیچیدگی محاسبات گردیده است. در [۲۷] یک ساختار سلسله‌مراتبی برای ایجاد یک سیستم بازشناسی مبتنی بر مشخصه‌های بیومتریک ارائه شده است. این ساختار از چندین مرحله تشکیل می‌شود که در هر مرحله از یک طبقه‌بند ضعیف استفاده شده است. این طبقه‌بندها وظیفه دارند پایگاه داده را فیلتر نموده و یک لیست کاندیدا برای مرحله بعدی تولید نمایند. در آخرین مرحله نیز یک طبقه‌بند قوی قرار داده شده تا تصمیم نهایی را از آخرین لیست اتخاذ نماید. نتایج این پژوهش نشان داده که لزوماً اضافه‌کردن یک مرحله به ساختار سلسله‌مراتبی منجر به افزایش دقت نخواهد گردید. از این رو برای هر سیستم یک نقطه اشباع وجود دارد که مصالحه بین دقت و زمان در آنجا است. در [۲۸] یک روش همجوشی انطباقی برای مواجهه با چالش‌های محیط‌های غیر کنترل شده با بهره‌گیری از یادگیری برخط ارائه شده است. در این روش مجموعه‌ای از طبقه‌بندها وظیفه دارند بر اساس کیفیت نمونه‌ها تشخیص دهند از چه روش همجوشی به ازای هر درخواست به سیستم استفاده شود. همچنین به ازای هر درخواست که تشخیص اشتباه داده شود، طبقه‌بندها با به

1. Modality Specific Image Quality
2. Ridge Richness
3. Deep Learning
4. End-to-End Architecture
5. Liklihood Ratio Test



شکل ۱: روندنمای کلی روش پیشنهادی.

کارگیری یک مکانیزم یادگیری برخط مجدداً آموزش داده می‌شوند تا عملکرد بهتری داشته باشند.

در [۱۲] به منظور بهره‌مندی از مزایای چندبیومتریکی با هدف افزایش کارایی سیستم تطبیق در بستر کارت، رویکردی بر اساس ساختار سلسله‌مراتبی پویا ارائه گردیده است. در ساختار ارائه‌شده مودال‌ها پشت سر هم چیده می‌شوند و به ترتیب در صورت لزوم اخذ می‌شوند. برای نیل به چنین هدفی، مجموعه‌ای از معیارهای ویژگی به صورت صریح و غیر اتوماتیک به ازای هر مشخصه تعریف شده است. مقادیر بردارهای کیفیت برای زوج نمونه تصویر گالری و پروب توسط یک مؤلفه استخراج شده و به عنوان ورودی به یک طبقه‌بند داده شده تا تصمیم مناسب بر اساس آنها اخذ شود. این طبقه‌بند قبلاً بر اساس مقادیر ورودی و خروجی مورد انتظار تعلیم دیده و در زمان اجرا وظیفه مدیریت جریان الگوریتم را بر عهده دارد. همان طور که اشاره شد چالش اصلی این روش، نحوه تعریف معیارهای کیفیت می‌باشد که در این پژوهش برای رفع آن از یادگیری عمیق استفاده شده است.

طی چند سال گذشته، شبکه‌های عصبی عمیق به دلیل توانایی بالا در یادگیری و شناسایی الگوهای پیچیده توجه پژوهشگران بسیار زیادی را به خود جلب نموده است. این شبکه‌ها برای کاربردهای گوناگونی در حوزه بیومتریک آموزش داده شده و به کار گرفته شده‌اند. تشخیص کلاس اثر انگشت به منظور خوشه‌بندی پایگاه داده در سامانه‌های بازشناسی کاربرد دارد. در [۲۹] برای تشخیص کلاس اثر انگشت از یادگیری عمیق استفاده شده است. دو شبکه مختلف برای این وظیفه طراحی و کارایی آنها با روش‌های کلاسیک مبتنی بر یادگیری ماشین مقایسه شده است. نتایج نشان می‌دهد روش پیشنهادی، علاوه بر این که نیازی به تعریف معیارهای غیر اتوماتیک صریح نداشته، کارایی بالاتری را نیز داشته است. با پیشرفت تکنولوژی اخذ اثر انگشت و متداول‌شدن بیش از پیش اسکنرهای dpi ۱۰۰۰ حفره‌های[1] اثر انگشت به عنوان یک ویژگی در الگوریتم‌های تطبیق به کار می‌روند. در [۳۰] با به کارگیری "یادگیری انتقالی[2]" شبکه VGG[3] [۳۱] برای این وظیفه تنظیم مجدد[4] شده است. در [۳۲] و [۳۳] نیز با هدف استخراج مینوشیا از تصاویر اثر انگشت از شبکه عمیق استفاده شده است. کیفیت تصویر رگ انگشتان بر دقت عملیات تطبیق تأثیر بسیار زیادی دارد. تعیین کیفیت اتوماتیک این مشخصه پیچیده می‌باشد و حتی تشخیص غیر اتوماتیک آن نیز احتیاج به دانش خاص و تخصص ویژه‌ای دارد. در [۳۴] برای این کاربرد یک شبکه اختصاصی شامل سه لایه کانولوشنی و دو لایه اتصال کامل طراحی و آموزش داده شده است. تشخیص مدل سنسور برای هر سامانه بازشناسی مفید است و می‌تواند در مرحله پیش‌پردازش برای حذف نویز و افزایش تعامل‌پذیری[5] به کار رود. در [۳۵] برای تشخیص مدل‌های مختلف سنسور عنبیه از یادگیری عمیق استفاده شده است. در این مقاله همچنین نشان داده شده که تعیین مدل سنسور توانسته دقت بازشناسی را افزایش دهد. یکی دیگر از وظایف پیچیده که اخیراً با به کارگیری شبکه‌های عمیق حل شده است، تشخیص جعلی‌بودن اثر انگشت [۳۶] تا [۳۸] می‌باشد. در [۳۹] نیز برای تعیین کیفیت تصویر چهره از شبکه عصبی عمیق استفاده شده است. بر طبق نتایج این پژوهش استفاده از معیار کیفیت در سامانه بازشناسی توانسته نرخ خطای FMR را کاهش دهد اما تأثیری بر روی نرخ FNMR نداشته است.

بر طبق مقالات بررسی‌شده، روش‌های یادگیری عمیق نیازی به تعریف صریح بردارهای ویژگی نداشته و بردارهای مذکور به صورت اتوماتیک توسط خود شبکه از تصاویر ورودی استخراج می‌گردند. بنابراین با استفاده از این قابلیت و توانایی شبکه‌های عمیق در یادگیری الگوهای پیچیده، در این پژوهش سعی شده راه حلی برای چالش‌های اشاره‌شده ارائه گردد.

۳- روش پیشنهادی

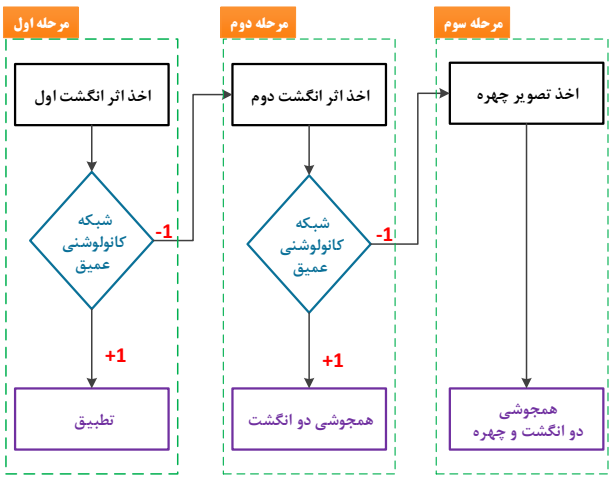
در بخش ۳-۱ چارچوب کلی پیشنهادی و در بخش‌های ۳-۲ و ۳-۳ به ترتیب معماری شبکه و فرایند آموزش آن ارائه شده‌اند.

۳-۱ چارچوب ترتیبی پویای پیشنهادی

در روش پیشنهادی، مشخصه‌های بیومتریکی پشت سر هم در یک زنجیره قرار می‌گیرند و تک به تک در صورت نیاز اخذ شده و برای انجام عملیات تطبیق مورد استفاده قرار می‌گیرند. تشخیص لزوم اخذ نمونه جدید توسط یک شبکه عمیق با معماری انتها به انتها با هدف مدیریت جریان پویای الگوریتم صورت می‌پذیرد که از آن تحت عنوان بلوک تصمیم‌ساز اتوماتیک نیز یاد می‌شود. این شبکه برای انجام وظیفه مد نظر مطابق با یک سناریوی طراحی‌شده آموزش داده می‌شود. روندنمای کلی روش پیشنهادی در شکل ۱ نشان داده شده است. در ساختار ارائه‌شده از یک سو زمان، پیچیدگی محاسبات و میزان عدم رضایتمندی کاربر تحت عنوان پارامتر هزینه و از سوی دیگر نرخ خطای عملیات تطبیق با یکدیگر در تداخل هستند. هرچه بلوک تصمیم‌ساز تعداد بیشتری از درخواست‌های تطبیق را به مراحل بعدی هدایت کند، هزینه بیشتر خواهد شد. اما در عوض احتمال رخداد خطای تطبیق (به دلیل افزایش اطلاعات در دسترس)

1. Pore

2. Transfer Learning
3. Visual Geometry Group
4. Fine Tune
5. Interoperability



شکل ۲: ساختار ترتیبی بر اساس دو انگشت و چهره.

نیز کاهش می‌یابد. در شرایط ایده‌آل، بلوک تصمیم‌ساز باید قادر باشد تشخیص دهد برای هر درخواست که به سیستم داده می‌شود، حداقل چه تعداد مودال برای تطبیق با اطمینان کافی مورد نیاز هست.

ساختار ترتیبی شکل ۱ بر اساس مشخصه‌های بیومتریکی شامل دو اثر انگشت و چهره در شکل ۲ سازماندهی شده است.

انتخاب دو انگشت در این ساختار به این دلیل است که استفاده از آنها در MOC بسیار متداول و پرکاربرد است [۷] و [۱۱]. مشخصه چهره نیز به این دلیل انتخاب شده که در اغلب پروژه‌های مدیریت هویت اخذ می‌گردد و در دسترس می‌باشد. علاوه بر این از دیرباز تصویر چهره صاحب سند بر روی سند شناسایی الصاق می‌گردید. امروزه نه تنها تصویر چهره بر روی سند چاپ می‌شود بلکه بر طبق استاندارد [۴۰] جزو اقلام اطلاعاتی اجباری جهت ذخیره‌سازی در تراشه نیز محسوب می‌گردد. لذا در زمان تصدیق هویت، تصویر چهره در صورت نیاز می‌تواند به سادگی واکشی شده و به عنوان مشخصه کمکی[1] مورد استفاده قرار گیرد. لازم به تأکید است که روش پیشنهادی بدون نقض نتایج، قابل تعمیم به هر تعداد و هر نوع مشخصه بیومتریکی بوده و الزامی به استفاده از مشخصه‌های یادشده در ساختار پیشنهادی نمی‌باشد.

همان طور که اشاره گردید اجبار به اخذ همگی مشخصه‌ها به منظور استفاده در عملیات تطبیق منجر به افزایش زمان و نارضایتی کاربران می‌گردد. به این علت روش پیشنهادی به نحوی طراحی شده که جریان الگوریتم به ازای هر درخواست به سیستم تصدیق هویت به صورت پویا مدیریت گردد.

ایده مقاله این است که تصمیم‌گیری در خصوص این که عملیات تطبیق در کدام مرحله انجام شود، توسط شبکه عصبی عمیق اتخاذ گردد. فرایند تصمیم‌گیری شامل دو مرحله اصلی است: ۱) استخراج بردار ویژگی عمیق[2] از تصویر ورودی و ۲) تصمیم‌گیری که همان طبقه‌بندی دوکلاسه به یکی از دو حالت '۱+' (انجام عملیات تطبیق در این مرحله) یا '۱-' (موکول‌نمودن عملیات تطبیق به مرحله بعدی) می‌باشد.

بنابراین هر زمان که یک درخواست برای تصدیق هویت به سیستم داده می‌شود، در ابتدا فقط اولین مشخصه یعنی اثر انگشت اول از کاربر اخذ می‌گردد. این تصویر (نمونه پراب) به همراه تصویر گالری به عنوان ورودی به شبکه داده می‌شود. شبکه بر اساس مدلی که قبلاً یاد گرفته، تعیین می‌کند که آیا عملیات تطبیق این درخواست می‌تواند با اطمینان کافی در همین مرحله انجام شود یا استفاده از مشخصه‌های دیگری نیز برای انجام عملیات تطبیق با اطمینان مورد نیاز است.

در صورتی که فرایند اخذ نمونه از متقاضی به شکل صحیح انجام شود و مشخصه اخذشده نیز دارای کیفیت مطلوب باشد، انتظار می‌رود تطبیق در اولین مرحله انجام شود. در این حالت با توجه به این که فقط یک مشخصه از کاربر اخذ شده، کمترین زمان مورد نیاز برای انجام عملیات تطبیق و بیشترین میزان رضایتمندی کاربر را نیز در پی خواهد داشت. در صورت موکول‌شدن عملیات تطبیق به مرحله بعدی، انگشت دوم نیز باید اخذ گردد. در این حالت عملیات تطبیق با همجوشی دو انگشت انجام می‌شود یا به مرحله بعدی موکول می‌گردد. در صورت تعویق تصمیم‌گیری به مرحله سوم، نیاز به اخذ مشخصه کمکی یعنی چهره نیز می‌باشد. این حالت به دلیل استفاده از دو مودال مختلف و افزایش زمان تصدیق هویت بیشترین هزینه و نارضایتی کاربر را در پی خواهد داشت.

از آنجایی که اغلب افراد قادر به ارائه اثر انگشت با کیفیت مناسب هستند، مطلوب آن است که فقط تعداد اندکی از افراد به این مرحله هدایت شوند. روش پیشنهادی راه حلی برای برآورده‌شدن هدف مذکور به صورت اتوماتیک و پویا می‌باشد که کمکی شایان در کاهش هزینه و افزایش دقت سیستم‌های تصدیق هویت بیومتریکی خواهد داشت. در بخش بعدی معماری شبکه عمیق و فرایند آموزش آن ارائه شده است.

۳-۲ معماری شبکه عمیق

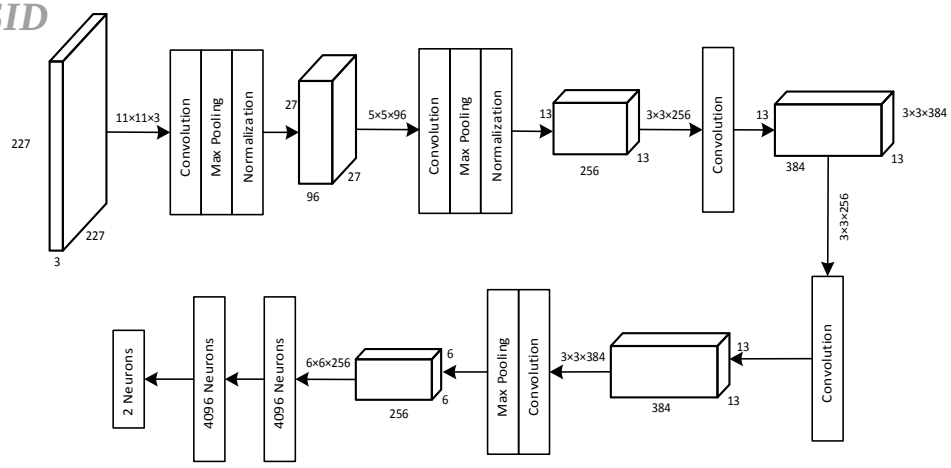
در این پژوهش برای مدیریت پویای جریان الگوریتم در یک سیستم تصدیق هویت بیومتریکی، از یک شبکه کانولوشنی از پیش آموزش داده شده با استفاده از تکنیک یادگیری انتقالی[3] تحت عنوان بلوک تصمیم‌ساز استفاده شده است.

چون انتظار می‌رود در یک سیستم تصدیق هویت بیومتریکی، مدیریت جریان الگوریتم بلادرنگ باشد، لذا علاوه بر دقت، مشخصه سرعت نیز اهمیت ویژه‌ای خواهد داشت. بر همین اساس از بین شبکه‌های برتر در چالش ILSVRC[4]، شبکه [۴۱] که کم‌عمق‌ترین شبکه بوده (دارای عمق ۸) جهت تنظیم دقیق[5] و استفاده در بلوک تصمیم‌ساز انتخاب شده است.

لازم به ذکر است به دلیل فقدان تعداد بسیار زیاد داده، تکنیک یادگیری انتقالی انتخاب شده تا این شبکه از پیش آموزش داده شده برای وظیفه مد نظر تنظیم دقیق شود.

معماری این شبکه در شکل ۳ نشان داده شده و سایز کرنل و ابعاد ورودی هر لایه نیز در جدول ۱ ارائه شده است. همان طور که نشان داده شده، این شبکه یک توالی از لایه‌های کانولوشنی می‌باشد. ترکیب متنوعی از این لایه‌ها بر روی هم قرار گرفته‌اند تا شبکه تشکیل شود. برخی از لایه‌ها دارای پارامتر بوده که در حقیقت همان وزن‌ها و بایاس‌های نرون‌ها می‌باشند و برخی دیگر فاقد پارامتر هستند. در این شبکه از لایه‌های کانولوشن، انتخاب بیشینه[6] و اتصال کامل[7] استفاده شده است. پنج لایه کانولوشنی به همراه سه لایه انتخاب بیشینه جهت استخراج بردارهای ویژگی در نظر گرفته شده و سه لایه اتصال کامل نیز برای طبقه‌بندی می‌باشد.

1. Axillary Trait
2. Deep Feature Extraction
3. Transfer Learning
4. Imagenet Large Scale Visual Recognition Challenge
5. Fine-Tune
6. Max Pooling
7. Fully-Connected



شکل ۳: معماری بلوک تصمیم‌ساز.

جدول ۱: ابعاد ورودی لایه‌های شبکه و سایز کرنل.

نوع لایه	ابعاد کرنل	گام (Stride)	تابع فعال‌ساز
Convolution	۱۱×۱۱×۹۶	۴	ReLU
Pooling	۳×۳	۲	–
Convolution	۵×۵×۲۵۶	۱	ReLU
Pooling	۳×۳	۲	–
Convolution	۳×۳×۳۸۴	۱	ReLU
Convolution	۳×۳×۳۸۴	۱	ReLU
Convolution	۳×۳×۲۵۶	۱	ReLU
Pooling	۳×۳	۲	–
Fully Connected	۴۰۹۶	–	ReLU + Dropout
Fully Connected	۵۱۲	–	ReLU + Dropout
Fully Connected	۲	–	Softmax

ورودی هر لایه $(h_i^{(l)})$ از خروجی لایه قبلی آن $(h_j^{(l-1)})$ طبق رابطه زیر محاسبه می‌شود که ورودی لایه اول $(l=1)$ برابر با لایه ورودی یعنی تصاویر گالری و پروب می‌باشد

$$h_i^{(l)} = \sum_{j=1}^{d} h_j^{(l-1)} * w_{i,j}^{(l)} + b_i^{(l)} \qquad (1)$$

در این رابطه d تعداد بعد ورودی، * بیانگر عملگر کانولوشن، $w_{ij}^{(l)}$ وزن متناظر ارتباط واحد j در لایه $l-1$ با واحد i در لایه l و $b_i^{(l)}$ پارامتر بایاس متناظر با واحد i در لایه l است. در این شبکه، تابع ReLU[1] طبق رابطه زیر به عنوان تابع فعال‌ساز[2] غیر خطی مورد استفاده قرار گرفته است

$$f(x) = \max(0, x) \qquad (2)$$

لازم به ذکر است که مشکل این تابع فعال‌ساز، پدیدآمدن نرون‌های مرده است. در این مقاله برای غلبه بر این مشکل بر طبق جدول ۲، نرخ اولیه یادگیری کوچکی در نظر گرفته شده است. در انتهای شبکه نیز برای طبقه‌بندی از سه لایه اتصال کامل به همراه تابع Softmax طبق رابطه زیر استفاده گردیده است

$$y_i = \frac{\exp(y_i')}{\sum_{j=1}^{n} \exp(y_j')} \qquad (3)$$

1. Rectified Linear Unit
2. Activation Function

جدول ۲: مقادیر ابرپارامترهای فرایند آموزش.

ردیف	ابرپارامتر	مقدار
۱	Batch size	۱۲۸
۲	Dropout	۰/۵
۳	Initial learning rate (α_0)	۰/۲
۴	Learning Decay Rate	۱
۵	Moment Decay Rate (β)	۰/۹

۳-۳ فرایند آموزش

در فرایند آموزش، ابتدا امتیازات اصلی[3] و جعلی[4] برای داده‌های مجموعه آموزش به دست می‌آید. اگر مجموعه داده آموزش شامل تعداد n تصویر باشد که از هر کدام m نمونه موجود باشد، آن گاه (۴) و (۵) به ترتیب تعداد مقایسه‌های اصلی و جعلی را نشان می‌دهد

$$\text{تعداد مقایسه‌های اصلی} = n \times C_m^2 = n \times \frac{m!}{(m-2)! \times 2!} \qquad (4)$$

$$\text{تعداد مقایسه‌های جعلی} = C_n^2 \times m \times m = \frac{n!}{(n-2)! \times 2!} \times m^2 \qquad (5)$$

سپس ماتریس امتیازات بر اساس (۶) ساخته می‌شود که در آن N مجموع تعداد مقایسه‌های اصلی و جعلی می‌باشد. در این رابطه، Img_g تصویر گالری و Img_p تصویر پراب به عنوان ورودی در نظر گرفته شده و L نیز برچسب متناظر با تطبیق این دو تصویر می‌باشد که نحوه تعیین آن در ادامه توضیح داده شده است

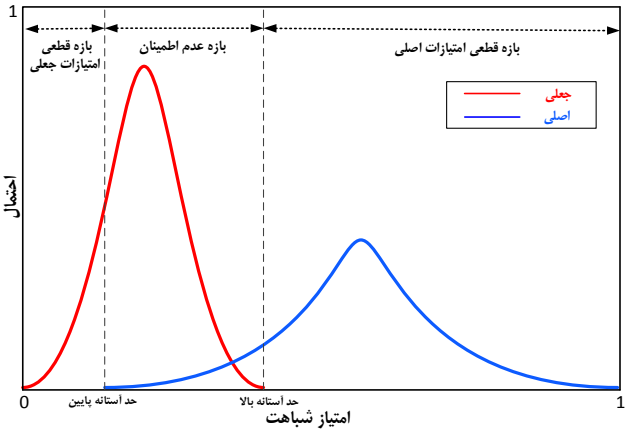
$$S_{n\times m} = \{(Img_{g_i}, Img_{p_i}), L_i\} \ , \ i = 1, \ldots, N \qquad (6)$$

در این پژوهش برچسب داده‌های مجموعه آموزش بر اساس بازه عدم اطمینان[5] تعیین شده است. بازه عدم اطمینان از روی هیستوگرام امتیازات اصلی و جعلی تعریف می‌شود. بر اساس (۷) و (۸) دو حد آستانه پایین و بالا برای این بازه تعیین می‌گردد

$$TH_{low} = \min(Score_{Genuine}) \qquad (7)$$

$$TH_{High} = \max(Score_{Imposter}) \qquad (8)$$

3. Genuine
4. Imposter
5. Uncertainty Region



شکل ۴: نمایش بازه عدم اطمینان در هیستوگرام امتیاز شباهت.

نواحی کمتر از حد آستانه پایین و بیشتر از حد آستانه بالا معادل با حالت '۱+' (انجام عملیات تطبیق در مرحله جاری) در نظر گرفته می‌شود. زیرا همان طور که در شکل ۴ نشان داده شده، در صورتی که امتیاز حاصل از یک درخواست تصدیق هویت بیشتر از حد آستانه بالا باشد، می‌توان با اطمینان بالا آن را تأیید[1] نمود. به همین ترتیب اگر امتیاز مقایسه کوچک‌تر از حد آستانه پایین باشد، می‌توان با اطمینان بالا آن را نیز به عنوان یک درخواست جعلی رد[2] نمود. ناحیه بین حدود آستانه که امتیازات اصلی و جعلی با یکدیگر در تداخل هستند، نیز معادل با کلاس '۱-' (تعویق عملیات تطبیق به مرحله بعدی) در نظر گرفته می‌شود. زیرا امتیاز کویری که در این ناحیه باشد، با احتمال متفاوت ممکن است متعلق به کلاس اصلی یا جعلی باشد. لذا تصمیم‌گیری در مورد آن به مرحله بعدی موکول می‌شود.

بنابراین آموزش شبکه عمیق که در بلوک تصمیم‌ساز مورد استفاده قرار گرفته است، بر اساس بازه عدم اطمینان امتیازات تطبیق‌کننده مبتنی بر کارت هوشمند (MOC) صورت پذیرفته است. به طور مثال تعداد مینوشیا (حداکثر ۶۴) یا فاکتور چرخش (حداکثر ۴۵ درجه)، از عوامل تأثیرگذار بر نتیجه تطبیق‌کننده کارتی است که شبکه سعی در یاد گرفتن و پیش‌بینی آن دارد. این در حالی است که اغلب تطبیق‌کننده‌های غیر کارتی به تعداد مینوشیا یا میزان چرخش حساس نمی‌باشند. بر این اساس از آنجا که هدف مقاله، حل چالش‌های بهره‌برداری از کارت هوشمند در محیط‌های عملیاتی بوده، لذا چالش‌ها و محدودیت‌های تطبیق‌کننده کارتی مد نظر قرار گرفته است.

در خصوص Data Augmentation اگرچه باعث می‌شود از پیش‌برازش ممانعت به عمل آمده و شبکه جزئیات دقیق‌تری را فرا گیرد، اما باید توجه داشت که این تکنیک وقتی مؤثر می‌باشد که برچسب داده تغییر نکند. به طور مثال چرخش آینه‌ای یا کراپ تصادفی یکی از روش‌های معمول می‌باشد که در مسأله مورد بررسی در این مقاله هر دوی آنها باعث خواهد شد یک جفت نمونه از کلاس اصلی به کلاس جعلی تبدیل شده و برچسب متفاوتی بگیرند. به این علت در این مقاله با تکیه بر دانش کاربردی مسأله، فقط از دو روش چرخش ۵± درجه و کراپ از مرکز برای Data Augmentation استفاده شده است.

برای مقداردهی اولیه وزن‌های نورون‌ها از قانون مقداردهی اولیه Xavier استفاده شده است [۴۲]. ذکر این نکته ضروری است که حتماً

1. Accept
2. Reject

باید واریانس وزن‌ها در هر لایه برابر با مقدار $۲/m$ باشد. در این رابطه m تعداد ویژگی‌های ورودی به هر نورون است و بنابراین مقدار اولیه وزن هر لایه با استفاده از (۹) مشخص می‌شود

$$W^l = Guassian\ Random\ Number(Shape\ of\ Layer) \times \tanh\sqrt{\frac{۲}{m}} \quad (۹)$$

تابع هزینه[3] در فرایند آموزش، برای اندازه‌گیری میزان اختلاف کلاس پیش‌بینی‌شده و کلاس واقعی مورد استفاده قرار می‌گیرد. در این پژوهش برای محاسبه این اختلاف از تابع هزینه cross entropy مطابق (۱۰) استفاده شده است

$$J(W.b) = -\sum_{i=۱}^{m} y_i \times \log(h_{w.b}(x_i)) \quad (۱۰)$$

ذکر این نکته ضروری است که تابع cross entropy یک تابع متقارن نیست و حتماً باید لگاریتم کلاس پیش‌بینی‌شده محاسبه گردد. همچنین برای جلوگیری از بیش‌برازش نیاز است که یک ترم تنظیم‌کننده به تابع هزینه اضافه گردد. رابطه (۱۱) این موضوع را لحاظ نموده است

$$J(W.b) = -\sum_{i=۱}^{m} y_i \times \log(h_{w.b}(x_i)) + \frac{\lambda}{۲m}\sum_{l=۱}^{L}\left\|W^l\right\|^۲ \quad (۱۱)$$

در این رابطه λ پارامتر تنظیم‌کننده و W وزن لایه‌های مختلف است. در ترم تنظیم[4] می‌توان وزن بایاس‌ها را نیز دخیل نمود ولی از آنجایی که W در مقایسه با b تعداد بعد بسیار بالایی دارد از آن صرف نظر شده است. در شبکه‌های عصبی و به خصوص از نوع کانولوشن، برای جلوگیری از بیش‌برازش[5] از این روش استفاده می‌شود که با توجه به مقدار dropout درصدی از نورون‌های موجود هرس می‌شوند. در مقابل پارامتر dropout پارامتر keep prob وجود دارد که این دو پارامتر مکمل همدیگر می‌باشند و جمع آنها همواره برابر یک است.

به منظور بهینه‌سازی تابع هزینه در شبکه‌های عصبی معمولاً از روش [۴۳] استفاده می‌شود. این روش به منظور پیداکردن نقطه بهینه اغلب دارای نوسانات زیاد در ابعاد مختلف شامل ابعاد اوزان و بایاس می‌باشد. برای جلوگیری از این نوسانات، در این پژوهش از روش ارائه‌شده در [۴۴] استفاده شده است. در این روش به منظور کاهش تعداد گام‌های لازم برای رسیدن به مقادیر بهینه از مفهوم exponentially moving average استفاده می‌شود. روش کار به این صورت است که در طول هر تکرار مقدار dW و db با توجه به (۱۲) و (۱۳) بر روی mini batch جاری محاسبه می‌شود

$$\frac{\partial}{\partial W_{ij}^{(l)}} J(W.b) = a_j^{(l)}\delta_i^{(l+۱)} \quad (۱۲)$$

$$\frac{\partial}{\partial b_i^{(l)}} J(W.b) = \delta_i^{(l+۱)} \quad (۱۳)$$

در گام بعدی مقادیر V_{dW} و V_{db} با توجه به (۱۴) و (۱۵) محاسبه می‌گردد. ذکر این نکته ضروری است که در ابتدا مقادیر V_{dW} و V_{db} به صفر مقداردهی اولیه می‌شوند

3. Loss Function
4. Regularization
5. Over Fitting

جدول ۳: مشخصات پایگاه داده.

مودال	افراد	نمونه	دستگاه	رزولوشن	فرمت
اثر انگشت	۵۰۰	۵	URU۴۰۰۰	۳۲۸×۳۵۶	۸ bit gray-level bmp
چهره	۵۰۰	۵	Logitech	۶۴۰×۴۸۰	۱۶ bit RGB bmp

جدول ۴: یک رکورد از پایگاه داده شامل آثار انگشت و چهره.

مودال	نمونه اول	نمونه دوم	نمونه سوم	نمونه چهارم	نمونه پنجم
انگشت اول					
انگشت دوم					
چهره					

$$V_{dW} = \beta V_{dW} + (1-\beta)dW \quad (14)$$

$$V_{db} = \beta V_{db} + (1-\beta)db \quad (15)$$

که ابرپارامتر β به عنوان decay momentum شناخته می‌شود و هدف اصلی آن کنترل میانگین وزن نمایی روی مقادیر اخیر V_{dW} و V_{db} است. در این پژوهش بر اساس روش ارائه‌شده در [۴۵] مقدار β برابر با ۰/۹ تنظیم شده است. این مقدار بیانگر آن است که میانگین‌گیری بر روی ۱۰ مقدار آخر مشاهده‌شده انجام می‌گیرد. در گام بعدی به روز رسانی مقادیر وزن و بایاس به ترتیب مطابق (۱۶) و (۱۷) انجام می‌گیرد

$$W = W - \alpha V_{dW} \quad (16)$$

$$b = b - \alpha V_{db} \quad (17)$$

که ابرپارامتر α، نرخ یادگیری است و با مقدار اولیه $\alpha_0 = 0/2$ تنظیم شده است. به ازای هر تکرار روی داده آموزش که به عنوان *epoch* شناخته می‌شود، مقدار نرخ یادگیری با توجه به (۱۸) کاهش می‌یابد. در این رابطه ابرپارامتر *Decay Rate* با مقدار یک تنظیم می‌شود. مقادیر مربوط به ابرپارامترهای مختلف تنظیم‌شده در جدول ۲ ارائه شده است

$$\alpha = \frac{1}{1 + decayRate \times epochNum} \times \alpha_0 \quad (18)$$

٤- آزمایشات

در این بخش ابتدا مشخصات پایگاه داده و تطبیق‌کننده‌های مورد استفاده در این پژوهش معرفی شده و سپس سناریوی آزمایش و در انتها نتایج و تحلیل آنها ارائه گردیده است.

٤-۱ مشخصات پایگاه داده و تطبیق‌کننده‌ها

کارایی روش پیشنهادی بر روی بخش اثر انگشت و چهره از پایگاه داده CASIA v۵.۰ [1] ارزیابی شده است. بخش اثر انگشت این پایگاه داده شامل ۲۰.۰۰۰ تصویر از ۵۰۰ داوطلب می‌باشد. از هر داوطلب ۴۰ تصویر اثر انگشت موجود است که شامل ۵ نمونه از ۸ انگشت فرد می‌باشد (انگشتان کوچک راست و چپ اخذ نشده‌اند). تصاویر اثر انگشت در یک مرحله توسط اسکنر URU۴۰۰۰ شرکت Digital Persona اخذ شده است. همه تصاویر دارای رزولوشن ۳۵۶×۳۲۸ پیکسل و فرمت bmp هشت‌بیتی خاکستری می‌باشند. به منظور ایجاد تفاوت محسوس درون کلاسی[2]، در هنگام جمع‌آوری پایگاه داده از داوطلبین خواسته شده تا انگشتان خود را با میزان فشار متفاوت بر روی اسکنر قرار دهند و همزمان نیز با زوایای مختلف بچرخانند.

بخش چهره این پایگاه داده شامل ۲۵۰۰ تصویر رنگی چهره از ۵۰۰ داوطلب می‌باشد. از هر داوطلب ۵ نمونه تصویر موجود است. این تصاویر با استفاده از وب‌کم Logitech در یک مرحله اخذ شده‌اند. همه تصاویر دارای رزولوشن ۶۴۰×۴۸۰ پیکسل و فرمت bmp شانزده‌بیتی رنگی می‌باشند. مقادیر مختلف شدت روشنایی[3]، زاویه سر، حالت چهره، عینک و فاصله وب‌کم تا سوژه به منظور ایجاد تفاوت‌های درون کلاسی در هنگام نمونه‌برداری در نظر گرفته شده‌اند.

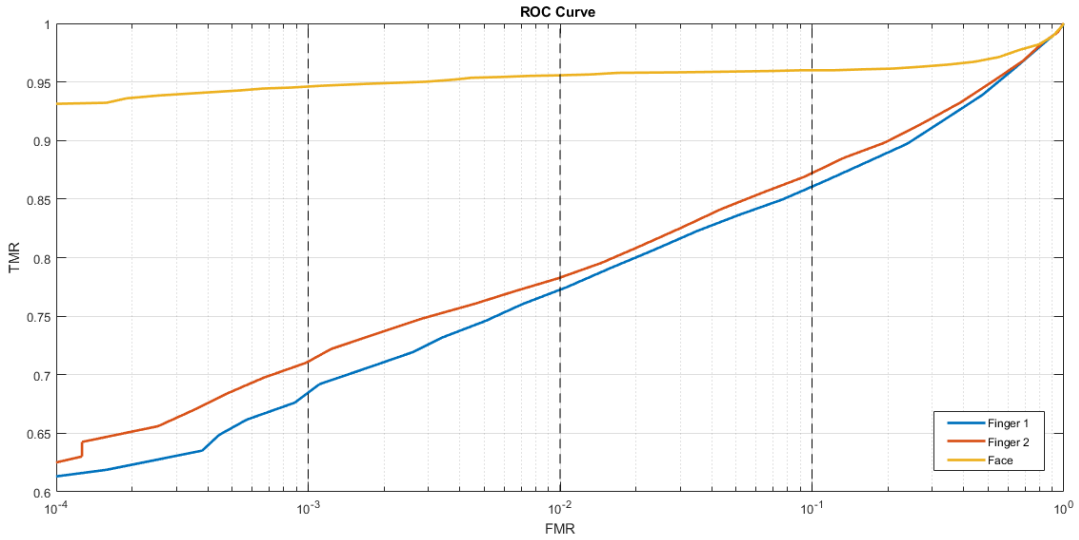
داوطلبین از میان فارغ‌التحصیلان دانشگاه، کارگران، پیش‌خدمت‌ها و سایر مشاغل گوناگون انتخاب شده‌اند. لذا این پایگاه داده به دلیل وجود افراد در محدوده‌های سنی گوناگون، مشاغل مختلف و تفاوت‌های درون کلاسی ایجادشده در هر دو بخش اثر انگشت و چهره دارای کیفیت‌های متنوع داده‌های بیومتریکی بوده و برای ارزیابی روش پیشنهادی مناسب می‌باشد. در این پژوهش دو انگشت به صورت تصادفی به یک تصویر چهره نگاشت شده و در مجموع یک پایگاه داده کیمرا[4] (یعنی تصویر چهره و دو انگشت مربوط به اشخاص متفاوت هست) ساخته شده است. جدول ۳ مشخصات این پایگاه داده و جدول ۴ نیز یک رکورد از این پایگاه داده را نشان می‌دهد.

1. http://biometrics.idealtest.org

2. Intra-Class Variations

3. Illumination

4. Chimera



شکل ۵: منحنی ROC مربوط به تطبیق‌کننده‌های پایه.

جدول ۵: تعداد مقایسه‌های اصلی و جعلی.

مجموعه	مقایسه	تعداد
آموزش	اصلی	۲۴۰۰
	جعلی	۳۵۹۷۰۰۰۰
تست	اصلی	۱۰۰۰۰
	جعلی	۶۲۳۷۵۰۰

جدول ۶: مقادیر EER و TMR در نقاط کاری متفاوت FMR مربوط به دقت پایه تطبیق‌کننده‌ها.

مشخصه	EER	TMR @ FMR = ۰٫۱	TMR @ FMR = ۰٫۰۱	TMR @ FMR = ۰٫۰۰۱
انگشت اول	۰٫۱۲۸۶	۰٫۸۶۱	۰٫۷۷۳	۰٫۶۸۵
انگشت دوم	۰٫۱۱۹۸	۰٫۸۷۲	۰٫۷۸۴	۰٫۷۱۱
چهره	۰٫۰۴۱۲	۰٫۹۶۱	۰٫۹۵۶	۰٫۹۴۶

از تطبیق‌کننده متن باز NBIS[1] که مبتنی بر مینوشیا است در قالب یک اپلت جاوا برای تطبیق اثر انگشت استفاده شده است. این اپلت در یک کارت هوشمند دارای پردازنده ۱۶بیتی با نرخ کلاک ۳۰ مگاهرتز بارگذاری شده است. هر مینوشیا نیز بر طبق مشخصات ارائه‌شده در بند هشتم استاندارد ISO/IEC ۱۹۷۹۴ [۱۰] مهیا شده است. از تطبیق‌کننده تجاری Neurotechnology VeriLook ۹.۰[2] که عملکرد آن در [۴۶] گزارش گردیده نیز به عنوان تطبیق‌کننده چهره استفاده گردیده است.

۴-۲ سناریوی آزمایش

مطابق توضیحات ارائه‌شده در بخش ۳-۱ جریان الگوریتم بر اساس کیفیت انگشت اول و سپس انگشت دوم مدیریت می‌گردد. لذا شبکه عمیق باید فقط بر اساس اثر انگشت آموزش داده شود. به منظور افزایش تعداد پایگاه داده، هر رکورد در بخش اثر انگشت که شامل هشت انگشت بوده به چهار رکورد با دو انگشت تبدیل می‌شود. بنابراین در کل ۲۰۰۰ رکورد با دو انگشت وجود دارد. از آنجایی که بخش تصویر چهره شامل ۵۰۰ رکورد است، ۵۰۰ رکورد از ۲۰۰۰ رکورد اثر انگشت برای مجموعه تست کنار گذاشته می‌شود. همچنین به منظور برقراری نسبت ۳۰ به ۷۰ برای مجموعه تست و آموزش، ۱۲۰۰ رکورد نیز برای مجموعه آموزش در نظر گرفته می‌شود. بر این اساس مجموعه تست شامل ۵۰۰ رکورد با سه مشخصه یعنی دو انگشت و چهره بوده و مجموعه آموزش نیز شامل ۱۲۰۰ رکورد با دو انگشت می‌باشد. لذا بر اساس (۴) و (۵)، تعداد مقایسه‌های مجموعه آموزش و تست به ازای هر مشخصه مطابق جدول ۵ می‌باشد. تقسیم‌بندی ۷۰ و ۳۰ به تعداد ده مرتبه تصادفی تکرار شده و میانگین دقت پایه مربوط به تطبیق‌کننده‌ها در شکل ۵ نشان داده شده است. همچنین میانگین مقادیر معیارهای EER و TMR در نقاط کاری FMR = ۰٫۰۰۱,۰٫۰۱,۰٫۱ نیز در جدول ۶ آمده است.

بر اساس [۴۷] ترتیب چینش مشخصه‌ها از ضعیف به قوی در یک ساختار سریال منجر به حصول بیشترین دقت می‌گردد. به این دلیل در این پژوهش از یک تطبیق‌کننده تجاری با کارایی بالا برای مشخصه چهره استفاده شده تا همان طور که در شکل ۵ قابل مشاهده است، مشخصه چهره دقت بیشتری نسبت به اثر انگشت داشته باشد. انتخاب مجموعه انگشتان اول و دوم از بین همه انگشتان نیز به گونه‌ای بوده که این فرض رعایت گردد.

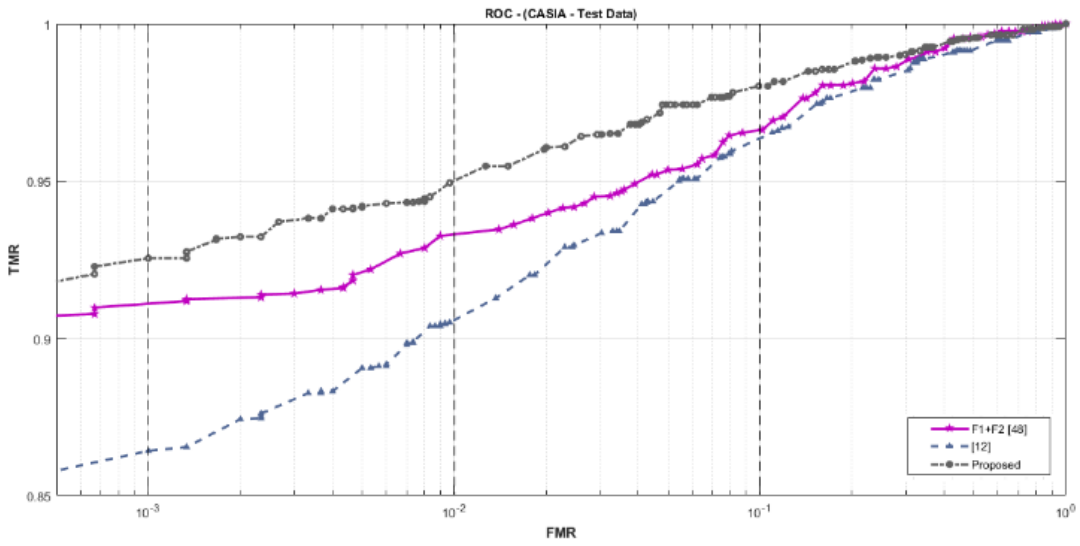
بر همین اساس ترتیب چینش مشخصه‌ها در شکل ۲ از مشخصه ضعیف به قوی در نظر گرفته شده است.

۴-۳ نتایج و تحلیل

کارایی روش پیشنهادی بر اساس نرخ دقت و میزان بارکاری[3] با ساختار سریال سه‌مرحله‌ای [۱۲] و همچنین همجوشی موازی جمع وزن‌دار دو انگشت با نرمال‌سازی Tanh [۴۸] مقایسه گردیده و نتایج آن در این بخش گزارش شده است.

برای انتخاب پارامترهای بهینه [۱۲] از جستجوی حریصانه بر اساس روش پیشنهادی در [۴۹] و تنظیم پارامتر *Gamma* از 2^{-15} تا 2^{5} و همچنین *Cost* از 2^{-5} تا 2^{15} با گام ۰٫۵ استفاده شده است. در این مرحله تنها از نمونه‌هایی در تعلیم طبقه‌بند دوم استفاده شده که در طبقه‌بند اول در بازه عدم اطمینان قرار گرفته بودند. سپس برای هر کدام از طبقه‌بندها، پارامترهایی به عنوان پارامتر بهینه انتخاب گردید که بیشترین دقت را برای هر دو کلاس در پی داشته است. این مقادیر برای

1. http://www.nist.gov/itl/iad/ig/nbis.cfm
2. http://www.neurotechnology.com/verilook.html
3. Workload



شکل ۶. منحنی‌های ROC روش پیشنهادی و دو روش مورد مقایسه.

جدول ۷: مقادیر EER و TMR در نقاط کاری متفاوت FMR.

روش	EER	TMR @ FMR = ۰٫۱	TMR @ FMR = ۰٫۰۱	TMR @ FMR = ۰٫۰۰۱
روش پیشنهادی	۰٫۰۳۴	۰٫۹۸۱	۰٫۹۵۱	۰٫۹۲۵
مرجع [۴۸]	۰٫۰۴۷	۰٫۹۶۶	۰٫۹۳۳	۰٫۹۱۱
مرجع [۱۲]	۰٫۰۵۲	۰٫۹۶۳	۰٫۹۰۶	۰٫۸۶۴

طبقه‌بند اول و دوم به ترتیب برابر $\begin{bmatrix} G_1 \\ C_1 \end{bmatrix} = \begin{bmatrix} 2^{-3} \\ 2^{3.5} \end{bmatrix}$ و $\begin{bmatrix} G_2 \\ C_2 \end{bmatrix} = \begin{bmatrix} 2^{-9.5} \\ 2^{-13.5} \end{bmatrix}$ در نظر گرفته شده است. برای همجوشی جمع وزن‌دار مطابق (۱۹) از معکوس خطای برابر[1] به دست آمده از جدول ۶ به عنوان وزن استفاده شده است. همچنین برای این که مجموع وزن‌ها همواره برابر یک باشد، از (۲۰) استفاده شده است

$$S_f = \omega_1 s_{f_1} + \omega_2 s_{f_2} \quad (۱۹)$$

$$\omega_1 = \frac{ERR_{f_2}}{ERR_{f_1} + ERR_{f_2}}, \quad \omega_2 = \frac{ERR_{f_1}}{ERR_{f_1} + ERR_{f_2}} \quad (۲۰)$$

منحنی ROC مربوط به روش‌های مذکور در شکل ۶ نشان داده شده است. به دلیل آن که روش پیشنهادی در همگی حدود آستانه دقت بالاتری از دو روش دیگر داشته، می‌توان اذعان داشت رویکرد پیشنهادی بر دو روش دیگر فائق آمده است. دقت هر سه روش بر اساس معیارهای EER و TMR در نقاط کاری FMR = ۰٫۰۰۱،۰٫۰۱،۰٫۱ در جدول ۷ گزارش شده است. برای اعتبارسنجی نتایج از آزمون واریانس HTER و T Test استفاده شده که مؤید پایداری فرایند تست می‌باشد. بر طبق جداول ۶ و ۷ روش پیشنهادی در نقطه کاری FMR = ۰٫۰۰۱ نسبت به انگشت اول و دوم به ترتیب ۳۵ و ۳۰٪ دقت بالاتری داشته است.

بارکاری هر مرحله به تفکیک مقایسه‌های اصلی و جعلی برای دو روشی که دارای ساختار سلسله‌مراتبی هستند نیز در جدول ۸ ارائه شده است. البته بارکاری برای [۴۸] به دلیل داشتن ساختار موازی موضوعیت نداشته و گزارش نشده است.

در یک سیستم تصدیق هویت عملیاتی، تعداد مقایسه‌های اصلی[2] که سیستم در طول حیات خودش انجام می‌دهد از مرتبه نمایی تعداد مقایسه‌های جعلی خواهد بود. در چنین سیستمی اساساً مقایسه‌های اصلی اهمیت داشته و میزان رضایتمندی کاربر نیز بر اساس آن سنجیده می‌شود. لازم به ذکر است که میزان بارکاری مقایسه‌های جعلی اهمیتی ندارد زیرا اساساً یک مقایسه جعلی توسط یک مهاجم به سیستم صورت می‌پذیرد. به عبارت دیگر هرچه بلوک تصمیم‌ساز (بدون افزایش نرخ خطا) بتواند بارکاری کمتری از مقایسه‌های اصلی را به مراحل انتهایی زنجیره هدایت نماید، مقبولیت و رضایتمندی بیشتر را برای خدمت‌دهنده و خدمت‌گیرنده فراهم می‌آورد. در این خصوص روش پیشنهادی توانسته عملکرد مناسب‌تری نسبت به [۱۲] داشته باشد. زیرا مطابق جدول ۸، تصدیق هویت برای مقایسه‌های اصلی در ۷۸٫۶۱٪ موارد بر اساس یک انگشت و در ۱۲٫۸۱٪ توسط دو انگشت انجام پذیرفته است. به طور کلی تصدیق هویت در مجموع برای ۹۱٫۴۲٪ موارد بر اساس اثر انگشت انجام شده و فقط برای ۸٫۵۸٪ موارد نیاز به استفاده از مشخصه چهره بوده است. برای مقایسه‌های جعلی نیز در ۷۹٫۵٪ موارد بر اساس اثر انگشت و فقط برای ۲۰٫۵٪ نیاز به استفاده از مشخصه سوم بوده است. لذا روش پیشنهادی توانسته ضمن کاهش زمان نمونه‌برداری و افزایش رضایتمندی کاربر، بارکاری کمتری را به مراحل انتهایی هدایت نموده و از این طریق پیچیدگی محاسبات (استخراج ویژگی و تطبیق) را کاهش دهد. این در حالی است که روش پیشنهادی دقت بالاتری هم نسبت به [۴۸] و [۱۲] داشته است.

آنالیز خطاهای حاصل از مقایسه‌های اصلی در مرحله اول نشان می‌دهد رویکرد پیشنهادی نسبت به روش [۱۲] توانسته تعداد بیشتری از نمونه‌هایی که منجر به خطا می‌شوند را شناسایی و به مراحل بعدی هدایت کند. البته تعدادی از نمونه‌ها نیز وجود داشته که رویکرد پیشنهادی بر خلاف روش [۱۲] قادر به شناسایی آنها نبوده و همچنین تعدادی نمونه نیز وجود داشته که هیچ یک از آنها قادر به تشخیص درست آنها نبوده‌اند. شکل ۷ سه نمونه از درخواست‌هایی را که در مرحله اول منجر به خطای FNMR گردیده نشان می‌دهد. ردیف اول فقط توسط روش پیشنهادی و ردیف دوم فقط توسط [۱۲] شناسایی شده و به مراحل بعدی هدایت شده

1. EER

2. Genuine Score

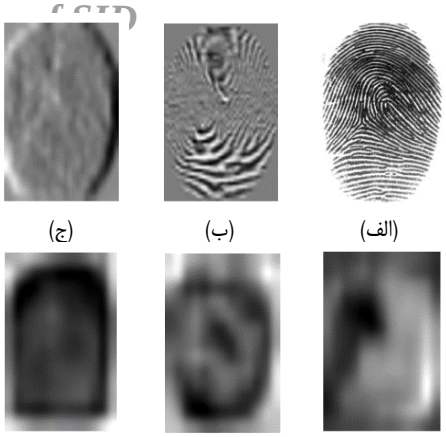
(الف) (ب)

شکل ۷: چند نمونه از موارد خطای عدم تطبیق اشتباه، (الف) گالری و (ب) پروب.

است. ردیف سوم توسط هیچ کدام قابل شناسایی نبوده و در هر دو روش جزو خطای FNMR بوده است. استفاده از کیفیت نمونه‌ها برای مدیریت پویای الگوریتم، ایده اصلی این مقاله می‌باشد. دلیل این موضوع این است که ارتباط مستقیمی بین امتیاز اصلی و کیفیت نمونه‌ها وجود دارد. به عبارت دیگر افت کیفیت نمونه‌های اصلی باعث کاهش امتیاز شباهت شده و می‌تواند منجر به بروز خطای FNMR گردد. بلوک تصمیم‌ساز در روش پیشنهادی با بهره‌برداری از همین موضوع و شناسایی چنین نمونه‌هایی، تصدیق هویت آنها را به مراحل بعدی هدایت نموده و از این طریق خطای FNMR کمتری را منجر شده است.

باید توجه داشت امتیاز تطبیق ناشی از دو نمونه نامشابه، عموماً صفر یا یک عدد کوچک نزدیک به صفر است. کم یا زیادبودن کیفیت نمونه‌های نامشابه در یک مقایسه جعلی نمی‌تواند امتیاز تطبیق جعلی کوچک را به صورت محسوسی تغییر دهد و به همین علت مشخصاً ارتباط مستقیمی بین کیفیت و امتیاز جعلی وجود ندارد و به همین علت هم روش پیشنهادی قادر به کاهش محسوس خطای FMR نبوده است.

بر طبق جدول ۱، پنج لایه کانولوشن در شبکه عمیق بلوک تصمیم‌ساز وجود دارد. ماکسیمم بردار ویژگی فعال‌شده در هر لایه کانولوشن برای یک تصویر نمونه پس از حذف پس‌زمینه در شکل ۸ نمایش داده شده است. در این شکل، کمترین و بیشترین مقدار فعال‌ساز به ترتیب به مقدار صفر و یک نگاشت شده است. پیکسل‌های سفید بیانگر مقادیر بزرگ مثبت فعال‌ساز و پیکسل‌های سیاه بیانگر مقادیر بزرگ منفی فعال‌ساز هستند و نقاط خاکستری عدم فعال‌شدن این نقاط را نشان می‌دهد.



(الف) (ب) (ج)

(د) (ه) (و)

شکل ۸: نمایش بردار ویژگی لایه‌های کانولوشن، (الف) تصویر نمونه، (ب) لایه دوم، (ج) لایه ششم، (د) لایه دهم، (ه) لایه دوازدهم و (و) لایه چهاردهم.

۵- جمع‌بندی

ارائه یک روش جدید برای مسأله مدیریت پویای جریان الگوریتم در یک سیستم تطبیق چندبیومتریکی سلسله‌مراتبی با ترکیب دانش کاربردی و یادگیری عمیق را می‌توان به عنوان هدف اصلی این پژوهش برشمرد.

در روش پیشنهادی برخلاف رویکرد [۱۲] که از یک طبقه‌بند خطی و ویژگی‌های غیر اتوماتیک استفاده می‌کند، ویژگی‌های مورد نیاز بلوک تصمیم‌ساز توسط یک شبکه عمیق به صورت اتوماتیک استخراج می‌شود که منجر به حصول دقت بالاتر و رضایتمندی کاربر می‌گردد. بر این اساس، یک سیستم تصدیق هویت چندبیومتریکی شامل دو انگشت و چهره مبتنی بر روش پیشنهادی پیاده‌سازی گردیده و مورد ارزیابی قرار گرفته است. بر طبق نتایج، در مجموع تصدیق هویت برای ۹۱/۴۲٪ موارد از مقایسه‌های اصلی بر اساس اثر انگشت انجام شده و فقط برای ۸/۵۸٪ موارد نیاز به استفاده از مشخصه کمکی یعنی چهره بوده است. این کاهش هزینه (شامل عملیات نمونه‌برداری، استخراج ویژگی و تطبیق) در حالی به دست آمده که دقت روش پیشنهادی بسیار بیشتر از تطبیق‌کننده کارتی مبتنی بر اثر انگشت و تقریباً هم‌اندازه با تطبیق‌کننده غیر کارتی مبتنی بر چهره بوده است.

بنابراین با قبول این واقعیت که استقرار و راه‌اندازی یک سیستم تصدیق هویت بیومتریکی صرفاً بر اساس دقت و بدون در نظر گرفتن هزینه استفاده از آن در محیط‌های واقعی عملیاتی نمی‌باشد، راه حل پیشنهادی توانسته با بهره‌گیری از یک بلوک تصمیم‌ساز اتوماتیک (شبکه عمیق) این چالش را بر طرف نماید. وظیفه بلوک تصمیم‌ساز تعیین حداقل تعداد مشخصه‌های بیومتریکی مورد نیاز برای تصدیق هویت است. پردازش مورد نیاز شبکه عمیق نسبت به هزینه کل عملیات مورد نیاز مشخصه اضافی (یعنی نمونه‌برداری، استخراج ویژگی و تطبیق) بسیار کمتر بوده و باعث می‌شود تا ضمن کاهش هزینه، راحتی کاربر نیز محقق گردد. تنها مشکل استفاده از شبکه عمیق پیشنهادی، فرایند آموزش پیچیده به دلیل پارامترهای زیاد آن است که البته فقط یک بار انجام شده و مشکلی در زمان استفاده (تست) از شبکه به وجود نمی‌آورد.

نوآوری این مقاله در ارائه یک بلوک تصمیم‌ساز اتوماتیک بر اساس یادگیری عمیق است که توانسته بر اساس کیفیت مشخصه‌ها به صورت پویا جریان الگوریتم را در یک سیستم تطبیق بیومتریکی مبتنی بر کارت هوشمند مدیریت نموده و از این طریق راه حلی برای برقراری مصالحه بین دقت و هزینه ارائه نماید. کارایی روش پیشنهادی از حیث دقت و

جدول ۸: بارکاری هر مرحله به تفکیک مقایسه‌های اصلی و جعلی.

روش	درصد بارکاری مقایسه‌های اصلی			درصد بارکاری مقایسه‌های جعلی		
	مرحله اول	مرحله دوم	مرحله سوم	مرحله اول	مرحله دوم	مرحله سوم
پیشنهادی	۷۸٫۶۱	۱۲٫۸۱	۸٫۵۸	۶۲٫۹۳	۱۶٫۵۷	۲۰٫۵۰
مرجع [۱۲]	۶۳٫۶۱	۲۳٫۷۳	۱۲٫۶۶	۴۷٫۷۰	۲۶٫۰۷	۲۶٫۲۳

بارکاری با ساختار سریال سه‌مرحله‌ای [۱۲] و همچنین همجوشی موازی جمع وزن‌دار دو انگشت با نرمال‌سازی tanh [۴۸] نیز مقایسه شده است.

به طور کلی رویکرد پیشنهادی دارای مزایای زیر می‌باشد:

۱) عدم نیاز به تعریف صریح و غیر اتوماتیک معیارهای کیفیت در بلوک تصمیم‌ساز

۲) عدم نیاز به استفاده و تعلیم طبقه‌بند جداگانه و استفاده مستقیم از تصاویر اولیه

۳) عدم نیاز به آموزش مجدد برون‌خط در فواصل کوتاه دوره‌ای در زمان استفاده در محیط عملیاتی به دلیل وجود ویژگی‌های عمیق متنوع و متعامد

۴) عدم نیاز به تأمین مجموعه آموزش بسیار بزرگ به دلیل بهره‌برداری از تکنیک یادگیری انتقالی و استفاده از یک شبکه از پیش آموزش داده شده

استفاده از دستاوردهای این پژوهش می‌تواند نقش مهمی در مقبولیت و موفقیت پروژه‌های عملیاتی و میزان اثربخشی آنها در فرایند تصدیق هویت داشته باشد. زیرا از یک طرف دارای دقت بیشتری بوده و از طرف دیگر منجر به کاهش هزینه یعنی زمان مورد نیاز برای اخذ و تطبیق می‌گردد. به طور مثال اگر در یک بانک برای تصدیق هویت مشتریان از روش پیشنهادی استفاده شود، به دلیل این که این روش دارای ساختار ترتیبی و پویا است، لذا درصد کمی نیاز به همجوشی همه مشخصه‌ها برای تصدیق هویت خواهند داشت. بدین ترتیب ضمن کاهش هزینه و میانگین زمان تصدیق هویت، رضایتمندی کاربر نیز فراهم آمده و از این طریق بین دقت و هزینه مصالحه برقرار می‌گردد.

نقطه ضعف روش پیشنهادی، وجود تعداد بسیار زیاد پارامتر در شبکه (حدود ۶۰ میلیون) می‌باشد. این موضوع باعث شده تا در زمان اجرا حافظه زیادی (در حدود ۴ گیگابایت) برای بارگذاری مدل شبکه مورد نیاز باشد. برای رفع این مشکل، امکان‌سنجی استفاده از شبکه عمیق سبک‌وزن [۵۰] به عنوان بلوک تصمیم‌ساز که اساساً جهت استفاده در پردازنده‌های ضعیف طراحی شده به عنوان کار آتی پیشنهاد می‌شود.

مراجع

[1] K. D. Mitnick and W. L. Simon, The Art of Deception: Controlling the Human Element of Security, John Wiley & Sons, 2011.

[2] D. V. Klein, "Foiling the cracker: a survey of, and improvements to, password security," in *Proc. of the 2nd USENIX Security Workshop*, pp. 5-14, Berkeley, CA, USA, Aug. 1990.

[3] R. Brunelli and D. Falavigna, "Person identification using multiple cues," *Pattern Analysis and Machine Intelligence, IEEE Trans. on*, vol. 17, no. 10, pp. 955-966, Apr. 1995.

[4] A. K. Jain, *et al.*, "Integrating faces, fingerprints, and soft biometric traits for user recognition," in *Proc. ECCV Workshop BioAW,* pp. 259-269 Prague, Czech Republic, 15-15 May 2004.

[5] R. Bolle, S. Pankanti, and A. K. Jain, Biometrics, Personal Identification in Networked Society: Personal Identification in Networked Society, Kluwer Academic Publishers, 2006.

[6] K. Nandakumar, Multibiometric Systems: Fusion Strategies and Template Security, Michigan State, p. 250, 2008.

[7] D. A. Cooper, *et al.*, *Interfaces for Personal Identity Verification,* (including updates as of 02-08-2016) 2016.

[8] C. L. Wilson, P. J. Grother, and R. Chandramouli, Biometric data specification for personal identity verification, 2006.

[9] D. Isenor and S. G. Zaky, "Fingerprint identification using graph matching," *Pattern Recognition*, vol. 19, no. 2, pp. 113-122, Jan. 1986.

[10] ISO/IEC 19794-2:2011, Information Technology-Biometric Data Interchange Formats-Part 2: Finger Minutiae Data, 2011.

[11] P. J. Grother and W. J. Salamon, MINEX II Performance of Fingerprint Match-on-Card Algorithms-Phase II/III Report, 2009.

[12] M. Sabri, M. S. Moin, and F. Razzazi, "A new framework for match on card and match on host quality based multimodal biometric authentication," *J. of Signal Processing Systems*, vol. 91, no. 2, pp. 163-177, Feb. 2018 2018.

[13] N. Poh, T. Bourlai, and J. Kittler, "A multimodal biometric test bed for quality-dependent, cost-sensitive and client-specific score-level fusion algorithms," *Pattern Recognition*, vol. 43, no. 3, pp. 1094-1105, Mar. 2010.

[14] M. Vatsa, *et al.*, "On the dynamic selection of biometric fusion algorithms," *IEEE Trans. on Information Forensics and Security,* vol. 5, no. 3, pp. 470-479, Sept. 2010.

[15] M. A. Olsen, V. Smida, and C. Busch, "Finger image quality assessment features-definitions and evaluation," *IET Biometrics*, vol. 5, no. 2, pp. 47-64, May 2016.

[16] S. Bharadwaj, M. Vatsa, and R. Singh, "Biometric quality: a review of fingerprint, iris, and face," *EURASIP J. on Image and Video Processing*, vol. 2014, no. 1, pp. 34-62, Jul. 2014.

[17] L. Best-Rowden and A. K. Jain, *Automatic Face Image Quality Prediction*, arXiv preprint arXiv:1706.09887, 2017.

[18] J. Chen, *et al.*, "Face image quality assessment based on learning to rank," *IEEE Signal Processing Letters*, vol. 22, no. 1, pp. 90-94, Aug. 2015.

[19] C. S. Mlambo and M. B. Shabalala, "Distortion analysis on binary representation of minutiae based fingerprint matching for match-on-card," in *Proc. IEEE Symp. Series on Computational Intelligence,* pp. 349-353, Cape Town, South Africa, 7-10 Dec. 2015.

[20] M. Govan and T. Buggy, "A computationally efficient fingerprint matching algorithm for implementation on smartcards," in *Proc. First IEEE Int. Conf. on Biometrics: Theory, Applications, and Systems, BTAS,* 6 pp., Crystal City, VA, USA, 27-29 Sept. 2007.

[21] B. Vibert, C. Rosenberger, and A. Ninassi, "Security and performance evaluation platform of biometric match on card," in *Proc. IEEE World Congress on Computer and Information Technology, WCCIT'13,* 6 pp., Sousse, Tunisia, 22-24 Jun. 2013.

[22] K. K. Nair, A. Helberg, and J. Van der Merwe, "An approach to improve the match-on-card fingerprint authentication system security," in *Proc. IEEE 6th Int. Conf. on Digital Information and Communication Technology and Its Applications, DICTAP'16,* pp. 119-125, Konya, Turkey, 21-23 Jul. 2016.

[23] A. Nagar, K. Nandakumar, and A. K. Jain, "Biometric template transformation: a security analysis," Media Forensics and Security II. 2010. International Society for Optics and Photonics.

[24] A. Lumini and L. Nanni, "Overview of the combination of biometric matchers," *Information Fusion*, , vol. 33, no. 4, pp. 71-85, Jan. 2017.

[25] R. Raghavendra, *et al.*, "Designing efficient fusion schemes for multimodal biometric systems using face and palmprint," *Pattern Recognition*, vol. 44, no. 5, pp. 1076-1088, May 2011.

[26] M. Vatsa, *et al.*, "On the dynamic selection of biometric fusion algorithms," *IEEE Trans. on Information Forensics and Security*, vol. 5, no. 3, pp. 470-479, Jul. 2010.

[27] A. Baig, *et al.*, "Cascaded multimodal biometric recognition framework," *IET Biometrics*, vol. 3, no. 1, pp. 16-28, Aug. 2013.

[28] S. Bharadwaj, *et al.*, "QFuse: online learning framework for adaptive biometric system," *Pattern Recognition*, vol. 48, no. 11, pp. 3428-3439, Aug. 2015.

[29] D. Peralta, *et al.*, "On the use of convolutional neural networks for robust classification of multiple fingerprint captures," *International J. of Intelligent Systems*, vol. 33, no. 1, pp. 213-230, Jan. 2018.

[30] H. U. Jang, *et al.*, "DeepPore: fingerprint pore extraction using deep convolutional neural networks," *IEEE Signal Processing Letters*, vol. 24, no. 12, pp. 1808-1812, Oct. 2017.

[31] K. Simonyan and A. Zisserman, *Very Deep Convolutional Networks for Large-Scale Image Recognition*, arXiv preprint arXiv:1409.1556, 2014.

[32] Y. Tang, F. Gao, and J. Feng, Latent Fingerprint Minutia Extraction Using Fully Convolutional Network, arXiv preprint arXiv:1609.09850, 2016.

[33] Y. Tang, et al., FingerNet: An Unified Deep Network for Fingerprint Minutiae Extraction, arXiv preprint arXiv:1709.02228, 2017.

[34] H. Qin and M. A. El Yacoubi, "Deep representation for finger-vein image quality assessment," *IEEE Trans. on Circuits and Systems for Video Technology*, vol. 28, no. 8, pp. 1677-1693, Mar. 2017.

[35] F. Marra, *et al.*, "A deep learning approach for iris sensor model identification," *Pattern Recognition Letters*, vol. 113, no. 1, pp. 46-53, Oct. 2017.

[36] D. Menotti, *et al.*, "Deep representations for iris, face, and fingerprint spoofing detection," *IEEE Trans. on Information Forensics and Security*, vol. 10, no. 4, pp. 864-879, Feb. 2015.

[37] R. F. Nogueira, R. de Alencar Lotufo, and R. C. Machado, "Fingerprint liveness detection using convolutional neural networks," *IEEE Trans. on Information Forensics and Security*, vol. 11, no. 6, pp. 1206-1213, Jan. 2016.

[38] T. Chugh, K. Cao, and A. K. Jain, "Fingerprint spoof buster: use of minutiae-centered patches," *IEEE Trans. on Information Forensics and Security*, vol. 13, no. 9, pp. 2190-2202, Mar. 2018.

[39] L. Best-Rowden and A. K. Jain, "Learning face image quality from human assessments," *IEEE Trans. on Information Forensics and Security*, vol. 13, no. 12, pp. 3064-3077, Jan. 2018.

[40] ICAO, D., 9303-Machine Readable Travel Documents-Part 9: Deployment of Biometric Identification and Electronic Storage of Data in eMRTDs, International Civil Aviation Organization (ICAO), 2015,

[41] A. Krizhevsky, I. Sutskever, and G. E. Hinton, "Imagenet classification with deep convolutional neural networks," *Advances in Neural Information Processing Systems*, vol. 1, no. 1, pp. 1097-1105, Dec. 2012.

[42] X. Glorot and Y. Bengio, "Understanding the difficulty of training deep feedforward neural networks," in *Proc. of the 13th International Conf. on Artificial Intelligence and Statistics*, vol. 9, pp. 249-256, Sardinia, Italy, 13-15 May 2010.

[43] L. Bottou, "Large-scale machine learning with stochastic gradient descent," in *Proc. of 19th Int. Symp. on Computational Statistics, COMPSTAT'10,* pp. 177-186, Paris, France, 22-27 Aug. 2010.

[44] I. Sutskever, *et al.*, "On the importance of initialization and momentum in deep learning," in *Proc. Int Conf. on Machine Learning*, *ICML'13,* vol. 28, pp. 1139-1147, Jun. 2013.

[45] A. Karpathy, *Class Notes for Cs231n: Convolutional Neural Networks for Visual Recognition*, Dept. of Comp. Sci., Stanford University, Palo Alto, CA, USA, spring 2017. [Online]. Available: http://cs231n.github.io/python-numpy-tutorial/

[46] C. I. Watson, *et al.*, *Fingerprint Vendor Technology Evaluation*, 2012, NIST, NIST Interagency/Internal Report (NISTIR), Jan. 2015.

[47] M. S. Hossain and K. A. Rahman, "An empirical study on verifier order selection in serial fusion based multi-biometric verification system," in *Proc. Int. Conf. on Industrial, Engineering and Other Applications of Applied Intelligent Systems,* pp. 249-258, Arras, France, 27-30 Jun. 2017.

[48] A. Jain, K. Nandakumar, and A. Ross, "Score normalization in multimodal biometric systems," *Pattern Recognition*, vol. 38, no. 12, pp. 2270-2285, Dec. 2005.

[49] C. W. Hsu, C. C. Chang, and C. J. Lin, *A Practical Guide to Support Vector Classification*, Technical Report, Department of Computer Science, National Taiwan University,Taipei, 2003.

[50] A. G. Howard, et al., Mobilenets: Efficient Convolutional Neural Networks for Mobile Vision Applications, arXiv preprint arXiv:1704.04861, 2017.

محمد صبری در سال ۱۳۸۶ مدرک کارشناسی مهندسی کامپیوتر گرایش نرم‌افزار را از دانشگاه فردوسی مشهد و در سال ۱۳۸۸ و ۱۳۹۷ مدرک کارشناسی ارشد و دکتری مهندسی کامپیوتر گرایش هوش مصنوعی را به ترتیب از دانشگاه شهید چمران اهواز و دانشگاه آزاد اسلامی واحد علوم و تحقیقات تهران دریافت نمود. نام‌برده از سال ۱۳۸۸ در دانشکده مهندسی کامپیوتر دانشگاه آزاد اسلامی واحد شهر قدس تهران مشغول به فعالیت گردید و اینک نیز عضو هیأت علمی این دانشکده می‌باشد. وی در چندین پروژه ملی مدیریت هویت مبتنی بر بیومتریک فعالیت داشته است. زمینه‌های علمی مورد علاقه ایشان در حوزه سیستم‌های هوشمند، یادگیری ماشین، سیستم‌های مدیریت هویت و بیومتریک می‌باشد.

محمدشهرام معین مدارک کارشناسی مهندسی الکترونیک، کارشناسی ارشد مهندسی الکترونیک و دکترای مهندسی برق را به ترتیب از دانشگاه صنعتی امیرکبیر در سال ۱۳۶۷، دانشکده فنی دانشگاه تهران در سال ۱۳۶۹ و پلی‌تکنیک مونترال کانادا در سال ۱۳۷۹ اخذ نموده است. ایشان با مرتبه دانشیاری به عنوان رئیس پژوهشکده فناوری اطلاعات در پژوهشگاه ارتباطات و فناوری اطلاعات مشغول به کار است و مجری پروژه‌های متعددی در حوزه‌های بیومتریک، چندرسانه‌ای و کلان داده‌ها بوده و در پروژه ملی مدیریت هویت مبتنی بر بیومتریک نیز فعالیت داشته است. دکتر معین سردبیر نشریه علمی- پژوهشی فناوری اطلاعات و ارتباطات ایران می‌باشد. زمینه‌های تحقیقاتی مورد علاقه ایشان بازشناسی الگو، پردازش تصویر، تحلیل داده‌ها و بیومتریک است.

فربد رزازی تحصیلات خود را در مقطع کارشناسی و کارشناسی ارشد به ترتیب در سال‌های ۱۳۷۳ و ۱۳۷۶ رشته مهندسی برق با گرایش مخابرات سیستم از دانشگاه صنعتی شریف اخذ نموده است. سپس وی دکترای خود را در سال ۱۳۸۲ در رشته مهندسی برق با گرایش مخابرات سیستم از دانشگاه صنعتی امیرکبیر دریافت کرده است. از سال ۱۳۷۷ وی به عضویت هیأت علمی دانشگاه آزاد اسلامی واحد علوم و تحقیقات تهران درآمد که در حال حاضر با رتبه دانشیار در این دانشگاه مشغول به کار است. زمینه‌های تحقیقاتی ایشان در حال حاضر، سیستمهای پردازش سیگنال در کاربردهای نظارتی، احراز هویت، جرم‌کاوی و حفظ حریم شخصی است.