Islamic Azad University , Shiraz Branch
نشریه تحلیل مدارها، داده ها و سامانه ها
Journal of Circuits, Data and Systems Analysis
sanad.iau.ir/journal/jcdsa

شناسایی چهره افراد بر اساس مدل معنایی برای موبایل بانک

لیلی نصرتی[۱] ، امیر مسعود بیدگلی[۲*]، حمید حاج سید جوادی[۳]

۱- گروه مهندسی کامپیوتر ، واحد تهران شمال، دانشگاه آزاد اسلامی، تهران، ایران
Nosrati.leili@gmail.com
۲- - گروه مهندسی کامپیوتر ، واحد تهران شمال، دانشگاه آزاد اسلامی، تهران، ایران
Am_bidgoli@iau-tnb.ac.ir
۳- دانشکده ریاضیات و علوم پایه، دانشگاه شاهد، تهران، ایران
s.h.seiedjavadi@gmail.com

چکیده: در این مقاله، یک پروتکل احراز هویت جدید برای بانکداری آنلاین بر اساس مدل معنایی ویژگی‌های استخراج شده از تصویر افراد معرفی شده است. رویکرد پیشنهادی با استفاده از تلفن‌های همراه هوشمند برای تصویربرداری دیجیتال برای مشتریان ارائه شده است. در این روش از خوشه‌بندی فازی برای دسته‌بندی ویژگی‌های تصاویر افراد مختلف استفاده شده است و با اعمال آن‌ها در روش‌های مختلف یادگیری ماشین، ترکیب روش‌های طبقه‌بندی یادگیری ماشینی برای بهبود عملکرد و افزایش قدرت در برابر حملات مختلف ارائه شده است. همچنین به منظور کاهش پیچیدگی طراحی ماشین برای کارهای عملیاتی، از روش کاهش ویژگی‌های استخراج شده از تصاویر چهره افراد به کمک الگوریتم ژنتیک و در قسمت آخر برای تصمیم‌گیری جهت احراز هویت فرد انتخاب شده، از سیستم منطق فازی بر اساس بالاترین دقت شناسایی فرد مورد نظر استفاده شده است. با استفاده از یک مجموعه داده عمومی، نتایج تجربی نشان داد که روش مبتنی بر الگوریتم ژنتیک بهترین انتخاب ویژگی برای ایجاد یک روش احراز هویت ضمنی برای محیط تلفن هوشمند است. نتیجه محاسبات دقت حدود ۹۹/۸۰٪ را با استفاده از تنها ۳۰ ویژگی از ۷۷ ویژگی برای احراز هویت کاربران نشان داد که بیانگر نیاز به منابع کمتر تلفن همراه است.

واژه های کلیدی: احراز هویت چهره، بانکداری همراه، مدل معنایی، الگوریتم ژنتیک، درخت تصمیم.

Face Detection based on Semantic Model for Mobile Banking

Leili Nosratii[1], Amir Masoud Bidgoli[*2], hamid haj seied javadi[3]

[1] Department of computer engineering, North Tehran Branch, Islamic Azad University, Tehran, Iran
nosrati.leili@gmail.com
[2] Department of computer engineering, North Tehran Branch, Islamic Azad University, Tehran, Iran
am_bidgoli@iau-tnb.ac.ir
[3] Mathematic department, Shahed University, Tehran, Iran

Abstract:

In this paper, a new authentication protocol for online banking based on the semantic model of features extracted from people's image is introduced. The proposed approach is presented using smart mobile phones for online digital imaging for customers. In this work, a fuzzy clustering has been used to categorize the characteristics of the images of different people and by applying them to different machine learning methods, a combined technique of machine learning classification methods has been presented to improve performance and increases strength against various attacks. Also to reduce the complexity of machine design for operational tasks, the technique of reducing features extracted from face images with the help of genetic algorithm has been used. In the last part, in order to make a decision for authentication selected by machine learning systems, a fuzzy logic system is presented based on the highest accuracy of identifying the desired person. Using a public dataset, the experimental results showed that the genetic algorithm-based technique is the

* نویسنده‌ی مسئول

best feature selection to create an implicit authentication method for the smartphone environment. The results showed an accuracy of about 99.80% using only 30 features out of 77 to authenticate users. At the same time, the results showed that the proposed method has a lower error rate compared to the related work.

Keywords: face detection authentication, mobile banking, semantic learning, Genetic Algorithm, Decision tree.

نوع مقاله: پژوهشی

DOI: 00.00000/0000

تاریخ ارسال مقاله: ۱۴۰۲/۰۷/۰۷ تاریخ پذیرش مقاله: ۱۴۰۲/۰۹/۱۵ تاریخ چاپ مقاله: ۱۴۰۲/۰۹/۲۸

۱- مقدمه

پیشرفت در فناوری دستگاه‌های تلفن همراه راه‌های جدید را برای بانکداری آنلاین امن‌تر کرده است. موسسات مالی پس از پی بردن به مزایای موبایل بانک، فرصت‌های بانکداری موبایلی را برای مشتریان خود فراهم کرده‌اند تا به آنها در هر زمان و مکان، امکان انجام عملیات بانکی مانند پرداخت صورت‌حساب، بررسی مانده حساب‌ها و انتقال پول را بدهند. یکی از مهمترین مسائل در بانکداری همراه امنیت است. احراز هویت در دستگاه‌های تلفن همراه می‌تواند نقطه عطفی باشد که بانکداری آنلاین و تلفن همراه را به روشی که امنیت کاربران را فراهم می‌کند، به هم متصل کند. بانکداری تلفن همراه به تلفن بانک همراه نیز معروف است. از آن به عنوان استفاده از تلفن همراه برای مشاغل مرتبط با بانکداری یاد می‌شود [۱]. برای تراکنش‌های مالی آنلاین، روش‌های سنتی در بانکداری تلفن همراه شامل اطلاعاتی است که مشتری می‌داند. چنین اقداماتی عمدتاً به شکل پین‌ها، رمزهای عبور، نشانه‌ها، کلیدها یا سؤالات امنیتی است که می‌توانند توسط کلاهبرداران به سرقت بروند یا حدس زده شوند. بنابراین، اعتماد نسبت به فناوری ممکن است تحت تأثیر قرار گیرد و افراد کمتری به بانکداری آنلاین روی بیاورند [۲].

ثابت شده است که انسان‌ها در به خاطر سپردن چهره یک فرد بسیار بهتر از نام او هستند. لذا یکی از رویکردهای امیدوارکننده برای ایجاد یک طرح رمز عبور ایمن، استفاده از مجموعه‌ای از تصاویر چهره افراد به عنوان رمزعبور به جای شماره‌های پین معمولی است. منطق معرفی سیستم رمز عبور بصری استفاده از دو فاکتور است: (۱) قدرت پردازش اطلاعات انسانی برای تشخیص تصاویر بصری، که برای رایانه‌ها کار دشواری تلقی می‌شود. (۲) قدرت پردازش سریالی سریع یک کامپیوتر دیجیتال برای به حداقل رساندن خطای انسانی در تعامل کامپیوتری. بنابراین ارائه راهکاری مبتنی بر یادآوری تصاویر چهره افراد برای شناسایی و احراز هویت در حوزه موبایل بانک کمک شایانی به حفظ امنیت اطلاعات و مقابله با حملات می‌کند.

حفظ حریم خصوصی و محرمانه بودن داده‌های بیومتریک هنوز یک چالش است و روش‌های امنیتی قبلی مانند رمزگذاری و واترمارک دیجیتال برای استفاده بلادرنگ موفق نیستند. امروزه فرآیند احراز هویت کاربر با تهدیدات امنیتی بسیاری مواجه است. لذا سطح امنیت دستگاه‌های بیومتریک باید افزایش یابد تا بتوان یک سیستم کارآمد به ویژه برای بانکداری آنلاین ارائه نمود. با یک سیستم احراز هویت آنلاین، مشکلاتی از جمله عدم اطمینان در شناسایی صحیح افراد وجود خواهد داشت و فرآیند احراز هویت شامل چالش‌های بیشتری نیز می‌شود زیرا همه چیز توسط اینترنت اشیاء به هم متصل می‌شود. علاوه بر این، به دلیل تغییر در چهره افراد و حتی موقعیت سر در مقابل دوربین گوشی هوشمند، احراز هویت چهره برای سیستم شناسایی دشوار و نامشخص است. بنابراین، ارائه یک روش مدل معنایی می‌تواند به تقویت سیستم احراز هویت کمک کند. احراز هویت تلفن همراه می‌تولند راه حل مناسبی باشد که بانکداری آنلاین، بانکداری تلفن همراه و پرداخت‌های از طریق تلفن همراه را به روشی امن، به هم متصل کند [۴]. احراز هویت به تنهایی مستعد آسیب‌پذیری است، در موارد سرقت یا اشخاص ثالث قابل اعتماد، امنیت آن می‌تواند به راحتی نقض شود و هکرهای رمز عبور به راحتی می‌توانند امنیت را از بین ببرند زیرا اکثر رمزهای عبور ضعیف هستند. بانکداری امن همراه، به مشتریان این اطمینان را می‌دهد که بدانند اطلاعات آنها امن است و می‌توانند با اطمینان تراکنش‌های امن انجام دهند.

به منظور ایجاد امنیت در سیستم بانکداری آنلاین که موبایل بانک یکی از آن سیستم‌هاست، تاکنون روش‌های مختلفی ارائه شده است. هر کدام از این روش‌ها با منطق و استراتژی خاصی سعی در کشف حمله داشته و از نفوذ به سیستم جلوگیری کرده‌اند. علیرغم تلاش‌های زیادی که صورت گرفته، این روش‌ها همچنان با چالش‌های امنیتی مواجه بوده و نتوانسته‌اند از نظر امنیتی عملکرد مناسبی را در این سیستم‌ها حفظ کنند. بنابراین در این مقاله مدلی را ارائه خواهیم داد که با استفاده از قابلیت های معنایی مبتنی بر منطق فازی به کشف هویت نمونه‌ها و احراز هویت افراد به کمک تصویربرداری آنلاین تلفن همراه می‌پردازد. مدل پیشنهادی در این مقاله بر اساس رویکرد شبکه عصبی مصنوعی ANN، شبکه فازی عصبی ANFIS و درخت تصمیم برای احراز هویت افراد پیاده‌سازی شده است. در این کار یک الگوریتم احراز هویت چهره برای بانکداری موبایلی تحت نرم افزار متلب مدلسازی شده و سپس طرح‌ها، روش‌ها و سایر موارد پیشنهادی برای سیستم مورد نظر پیاده‌سازی و بررسی می‌شوند. در نهایت، نتایج شبیه‌سازی با سایر روش‌های احراز هویت مقایسه شده و در این زمینه تلاش خواهیم کرد تا به یک فناوری هوشمند برای بانکداری ایمن و راحت مبتنی بر شناسایی هویت افراد بر اساس تصویر چهره با تماس‌های تلفن همراه دست یابیم. با توجه به نقاط ضعف و نفوذپذیری الگوریتم‌های موجود برای احراز هویت در موبایل بانک‌ها، در این مستند تلاش شده پس از بررسی روش‌های احراز هویت موجود و مقایسه آن‌ها، یک روش یکپارچه جدید مبتنی بر مدل معنایی در موبایل بلنک و بستر رایانش ابری برای برقراری امنیت و دقت بیشتر ارائه شود.

فناوری تشخیص چهره (FRT) خود را به عنوان یک ابزار همه‌کاره برای پشتیبانی از تأیید هویت و احراز هویت تثبیت کرده است. گام‌های بزرگی در توسعه راه‌حل‌های FRT دقیق و مقاوم در برابر دستکاری، با کمک فناوری‌های یادگیری ماشین (ML) و هوش مصنوعی (AL) چه بر روی تراشه و چه در فضای ابری برداشته شده است. این تحولات منجر به اعتماد بیشتر بلنک‌ها در به کارگیری این فناوری برای طیف گسترده‌ای از کاربردها و موارد استفاده شده است. استفاده از الگوریتم‌های تکاملی به عنوان یک رویکرد جدید در این مقاله می‌تولند به ایجاد یک مدل معنایی در فرایند شناسایی کمک کند. بر این اساس، ما با کمک سازگاری ویژگی‌های استخراج شده از مجموعه تصاویر افراد با کمک الگوریتم ژنتیک، توانسته‌ایم به افزایش امنیت برای FRT کمک کنیم. بانک‌ها همچنین به طور مستقیم از قدرت فناوری ML و AL و الگوریتم‌های تکاملی برای بهبود عملکرد بیومتریک و شناسایی هویت استفاده می‌کنند. این امر ضروری است و به بانک‌ها این اطمینان را می‌دهد که فناوری بیومتریک ایمن و قابل اعتماد است.

صورت انسان دائماً اطلاعات را آگاهانه و ناخودآگاه منتقل می‌کند. با این حال، به همان اندازه که تفسیر بصری این اطلاعات برای انسان‌ها اساسی است، برای ماشین‌ها یک چالش بزرگ است. روش‌های مرسوم برای تشخیص و تحلیل ویژگی‌های معنایی صورت عمدتاً فاقد استحکام هستند و از زمان محاسباتی بالا رنج می‌برند. هدف این مقاله کشف راه‌هایی برای ماشین‌ها جهت یادگیری تفسیر اطلاعات معنایی موجود در چهره‌ها به شیوه‌ای خودکار و بدون نیاز به طراحی دستی آشکارسازهای ویژگی، با استفاده از رویکرد یادگیری عمیق است. قسمت‌های اصلی این مقاله به شرح زیر خلاصه می‌شوند: (۱) یک سیستم احراز هویت چهره مبتنی بر هوش مصنوعی، با استفاده از پیاده‌سازی یک مدل معنایی برای احراز هویت پویا ارائه می‌شود. (۲) روش پیشنهادی در مدلسازی نرم بر اساس طبقه‌بندی افراد طراحی و آزمایش شده است. مجموعه داده شامل ویدیوهای ضبط شده توسط چندین کاربر، دوربین‌های مختلف گوشی‌های هوشمند و تصاویر افراد در سایت‌های مختلف و در جهات مختلف است. (۳) طبقه‌بندی ویژگی‌های استخراج‌شده از انواع مختلف تصاویر بر اساس یک مدل خوشه‌بندی معنایی مبتنی بر کیلومترهای فازی برای سه مجموعه از روش‌های یادگیری ماشین است: ANN، ANFIS و درخت تصمیم. (۴) برای کاهش پیچیدگی‌های پردازش مجموعه ویژگی‌های استخراج شده برای هر تصویر، از روش انطباق معنایی ویژگی‌ها با افراد مورد نظر استفاده می‌شود تا بتوان آن را توسط پردازنده‌های انواع تلفن‌های همراه پیاده سازی کرد. در این روش، از الگوریتم ژنتیک برای آموزش سیستم‌های یادگیری ماشینی با کاهش ویژگی‌ها از طریق حذف ویژگی‌های ناسازگار با افراد واقعی در حال آزمایش استفاده می‌شود.

بخش‌های باقی مانده از مقاله پژوهشی به روش زیر ساختار یافته است. بخش ۲ شامل مروری بر کارهای تحقیقاتی قبلی انجام شده توسط محققان، بخش ۳ ارائه روش پیشنهادی، بخش ۴ آزمون‌های شبیه‌سازی و استنباط آنها و بخش ۵ نتیجه‌گیری و گسترش کار در آینده می‌باشند.

۲- بررسی ادبیات

از آنجایکه سیستم‌های فعلی احراز هویت کاربر تلفن همراه مبتنی بر کدهای پین، اثر انگشت و تشخیص چهره دارای کاستی‌های متعددی هستند، در این مقاله تجزیه و تحلیل مقایسه‌ای از ویژگی‌های بیومتریک رفتاری تک‌وجهی و چندوجهی به‌دست‌آمده در حال انجام فعالیت‌های مختلف روی تلفن مانند تایپ کردن، اسکرول کردن، کشیدن و ضربه زدن روی صفحه، با در نظر گرفتن صفحه لمسی و داده‌های حسگر همزمان پس‌زمینه مانند (شتاب‌سنج، سنسور گرانش، ژیروسکوپ، شتاب‌سنج خطی و مغناطیس‌سنج) انجام شده است. یک شبکه عصبی بازگشتی جداگانه (RNN) با از دست دادن سه گانه برای هر مدالیته به کار گرفته شده است و سپس، ترکیب وزنی مدالیته‌های مختلف از طریق امتیاز دهی استخراج شده‌اند[۵]. همچنین یک راه‌حل جامع برای امنیت خانه‌های هوشمند پیاده‌سازی شده که به بهبود حریم خصوصی و امنیت با استفاده از دو فناوری مستقل و نوظهور احراز هویت چهره و تشخیص گفتار توسط تلفن همراه، تبلت، رایانه شخصی کمک می‌کند. کل فرآیند مورد اشاره با کمک شبکه های عصبی انجام می‌شود [۶]. بعلاوه، یک راه حل ترکیبی برای رسیدگی به دو چالش کلیدی احراز هویت، حریم خصوصی داده‌ها و محدودیت‌های منابع دستگاه‌های تلفن همراه نیز ارائه شده است. در مورد اول از رمزگذاری جزئی همورفیک براساس الگوریتم Paillier برای رمزگذاری استفاده شده و در دومی از ترکیبی از شبکه عصبی پیچیده عمیق و الگوی سه‌گانه محلی برای تشخیص چهره استفاده شده است [۷].

از آنجا که ورودی شبکه‌های عصبی عمیق (DNN) در برابر اغتشاشات نامحسوس استحکام ندارند، مدل‌های تشخیص چهره (FRMs) مبتنی بر DNN این آسیب‌پذیری را به ارث می‌برند. در این مقاله روشی برای ارزیابی و توصیف استحکام FRM ها در برابر اختلالات معنایی ورودی آنها پیشنهاد شده است. در این روش، با طراحی حملات متخاصم که به دنبال ایجاد تغییرات در حفظ هویت چهره‌ها هستند، FRMها را دچار نقص می‌کند. به طور خاص، با توجه به یک چهره، حملات انواع حفظ هویت چهره را پیدا می‌کنند به طوری که یک FRM قادر به تشخیص تصاویر متعلق به همان هویت نیست. این تغییرات مدل‌سازی می‌شوند و در نهایت با ترکیب با روش صدور گواهی تضمین-های نظری در خصوص عملکرد یک FRM و همچنین یک توصیف رسمی از اینکه چگونه یک FRM ممکن است مفهوم هویت چهره را مدل سازی کند ارائه می شود [۸]. همچنین به علت چالش‌های موجود در تشخیص چهره مبتنی بر ویدئو که ناشی از تعداد زیاد فریم‌ها و اختلافات درونی آنها می‌باشد یک مدل معنایی جدید برای بهبود عملکرد تشخیص چهره مبتنی بر ویدیو پیشنهاد شده است. ایده اصلی ساخت یک زیرفضای کم‌بعدی مناسب برای هر فرد است که بر اساس آن یک

مدل معنایی برای طبقه‌بندی فریم‌های کلیدی فرد در کلاس خاص ساخته می‌شود. پس از طبقه‌بندی معنایی، از فریم‌های کلیدی متعلق به همان کلاس‌ها، یعنی همان معناشناسی، برای آموزش طبقه‌بندی‌کننده‌های خطی برای تشخیص استفاده می‌شود [۹].

به طور معمول، احراز هویت کاربران تلفن هوشمند با استفاده از مکانیسم‌هایی (رمز عبور یا الگوی امنیتی) برای تأیید هویت کاربر انجام می‌شود که اگرچه این مکانیسم ها ارزان، ساده و به اندازه کافی سریع برای ورود مکرر هستند، اما در برابر حملاتی مانند Shoulder surfing یا Smudge attack آسیب‌پذیر هستند. این مشکل را می‌توان با احراز هویت کاربران با استفاده از رفتار آنها (به عنوان مثال، رفتار لمسی) در هنگام استفاده از تلفن‌های هوشمند برطرف کرد. چنین رفتارهایی شامل فشار انگشت، اندازه و زمان فشار هنگام ضربه زدن به کلیدها است. انتخاب ویژگی‌ها (از میان این رفتارها) می‌تواند نقش مهمی در عملکرد فرآیند احراز هویت داشته باشد. برای مورد مذکور یک روش احراز هویت ضمنی برای کاربران گوشی‌های هوشمند ارائه شده که در حالی که هزینه اضافی سخت‌افزار خاص را تحمیل نمی‌کند، به قابلیت‌های محدود گوشی‌های هوشمند می‌پردازد [۱۰].

در بسیاری از برنامه‌های کاربردی تشخیص ویژگی چهره (FAR) در دنیای واقعی، تنها داده‌های برچسب‌گذاری شده محدودی در دسترس هستند که منجر به بدتر شدن قابل‌توجه عملکرد اکثر روش‌های FAR که مبتنی بر یادگیری عمیق می‌باشند می‌شود. در همین راستا روشی به نام یادگیری وصله مکانی- معنایی (SSPL) پیشنهاد شده که آموزش آن شامل دو مرحله است. ابتدا، سه کار کمکی، متشکل از یک وظیفه چرخش وصله (PRT)، یک وظیفه تقسیم‌بندی وصله (PST) و یک وظیفه طبقه‌بندی وصله (PCT)، برای یادگیری رابطه مکانی- معنایی از داده‌های چهره بدون برچسب در مقیاس بزرگ ارائه می‌شود. به طور خاص، PRT از اطلاعات فضایی تصاویر چهره به روش یادگیری خود نظارتی بهره برداری می‌کند، PST و PCT به ترتیب اطلاعات معنایی در سطح پیکسل و سطح تصویر چهره را بر اساس مدل تجزیه چهره ضبط می‌کنند. دانش مکانی- معنایی آموخته شده از وظایف کمکی به وظیفه FAR منتقل می‌شود و این امکان را فراهم می‌کند که فقط تعداد محدودی از داده‌های برچسب گذاری شده برای تنظیم دقیق مدل از پیش آموزش دیده شده مورد استفاده قرار گیرد [۱۱]. از طرفی از طریق شناسایی و پیاده‌سازی منابع فشرده‌ترین الگوریتم‌ها بر روی هسته‌های DSP Lcore و تحلیل تصویر معنایی برای تشخیص چهره، فن‌آوری‌های ایجاد دوربین‌های هوشمند برای تجزیه و تحلیل تصویر معنایی بر اساس هسته های Lcore را شرح داده شده است [۱۳].

در رویکردی دیگر با مورد مطالعه قرار گرفتن تشخیص چهره انسان بدون محدودیت با استفاده از بیومتریک‌های نرم‌مقایسه‌ای در یک گالری برچسب انسانی (و بالعکس) برای برچسب‌گذاری مقایسه‌ای خودکار، بیومتریک‌نرم صورت پیشنهاد شده است [۱۵]. در روشی دیگر دسته‌ای از طبقه‌بندی‌کننده‌های ویژگی باینری که توصیف‌های بصری فشرده از چهره‌ها را ارائه می‌دهند، آموزش داده شده‌اند و این طبقه‌بندی کننده‌ها روی تصویر کاربر فعلی یک دستگاه تلفن همراه اعمال می‌شوند تا ویژگی‌ها را استخراج کنند و سپس احراز هویت با مقایسه ویژگی‌های محاسبه‌شده با ویژگی‌های ثبت‌شده کاربر اصلی انجام می‌شود و به این ترتیب روشی با استفاده از ویژگی‌های چهره برای احراز هویت مداوم کاربران گوشی‌های هوشمند ارائه شده است [۱۲]. در رویکردی دیگر اثرات عوامل مختلف و فراپارامترهای شبکه‌های عصبی عمیق برای یک پیکربندی شبکه‌ای بهینه مورد بررسی قرار گرفته است که بتواند ویژگی-های معنایی چهره مانند احساسات، سن، جنسیت، قومیت و غیره را به درستی تشخیص دهد. در این روش علاوه بر بررسی رابطه بین اثر مفاهیم سطح بالا بر روی ویژگی‌های سطح پایین از طریق تجزیه و تحلیل شباهت‌ها در توصیفگرهای سطح پایین، ایده جدیدی از استفاده از یک شبکه عمیق برای تولید مدل‌های ظاهری فعال سه‌بعدی چهره‌ها از تصاویر دوبعدی دنیای واقعی نشان داده می‌شود [۱۴]. در مدل یکپارچه بعدی به طور منسجم در مورد تصاویر مشاهده شده، هویت‌ها، دانش جزئی در مورد نام‌ها، و زمینه موقعیتی هر مشاهده دلیل ارائه می‌شود. هنگامی که مدل در برابر هویت‌های شناخته شده به عملکرد تشخیصی خوبی دست می‌یابد، می‌تواند هویت‌های جدیدی را از داده‌های نظارت نشده ارائه دهد و یاد می‌گیرد که بسته به اینکه کدام هویت‌ها تمایل دارند با هم مشاهده شوند، هویت‌ها را با زمینه‌های مختلف مرتبط کند. علاوه بر این، مؤلفه نیمه نظارت شده پیشنهادی می‌تواند نه تنها آشنایان را که نامشان مشخص است، بلکه چهره‌های آشنای بدون برچسب و غریبه‌ها را نیز در چارچوبی یکپارچه مدیریت کند [۱۶].

۳- روش شناسی

از آنجایی که ما به تکامل یک سیستم احراز هویت چهره علاقه‌مندیم، این مطالعه یک رویکرد معنایی را پیشنهاد می‌کند که هم تشخیص امنیتی و هم چالش‌های تأیید چهره را بررسی می‌کند. در بخش‌های بعدی ابتدا به معرفی مفاهیم و پیشینه‌های مورد استفاده در این مقاله می‌پردازیم؛ سپس رویکرد تلفیقی مبتنی بر مدل معنایی پیشنهادی این مستند را برای تأیید چهره توصیف می‌کنیم. ما طرح‌های تک تصویری را در مقابل رویکردهای مبتنی بر ویدئو برای احراز هویت با چهره مقایسه می‌کنیم. هر دو مورد، برای کاربردهای متفاوت استفاده می‌شوند و در بسیاری موارد، این روش‌ها می‌توانند با موفقیت ترکیب شوند، یکدیگر را تکمیل کنند و اقدامات امنیتی در برابر حملات را بهبود بخشند.

۳-۱- زمینه

در این مطالعه، سه روش یادگیری ماشین برای احراز هویت چهره مورد بحث قرار گرفته است. اساس تقسیم‌بندی اطلاعات شامل ویژگی‌های

استخراج‌شده، ارائه خوشه‌بندی K-Means فازی و کاهش ویژگی‌ها با کمک الگوریتم ژنتیک است که در ادامه بیان می‌شود.

۳-۱-۱- فراگیری ماشین

یادگیری ماشینی روشی برای به کار انداختن ماشین از طریق توانایی استدلال بر اساس نتایج یادگیری است. به عبارت دیگر، هنگامی که مجموعه داده‌های دقیقی در اختیار یک ماشین قرار می گیرد، ماشین به تنهایی قوانین مربوطه را یاد می‌گیرد و نتیجه مربوط به این قوانین را برای داده‌ها به عنوان خروجی ارائه می‌دهد. در میان این روش‌های یادگیری ماشینی، یادگیری عمیق، که نورون‌های انسانی را کپی می‌کند و چندین لایه از لایه‌های یادگیری را بین ورودی‌ها و خروجی‌ها سازماندهی می‌کند تا نتایج پیشرونده‌تری ارائه کند، در کانون توجه قرار دارد [۱۷]. یادگیری عمیق (DL) می تواند برای استخراج انتزاعات پیچیده و سطح بالا از نمایش داده ها استفاده شود. این کار با استفاده از یک معماری سلسله مراتبی و لایه‌ای یادگیری انجام می‌شود، که در آن ویژگی‌های انتزاعی بیشتر یعنی سطح بالاتر بیان می‌شوند و در بالای موارد انتزاعی کمتر یعنی سطح پایین توصیف می‌شوند. روش‌های DL می‌توانند حجم عظیمی از داده‌های بدون نظارت را تجزیه و تحلیل کنند و از آن‌ها بیاموزند، که این روش برای BDA مناسب است؛ در BDA داده‌های خام عمدتاً بدون برچسب و طبقه‌بندی نشده هستند [۱۸].

در میان مدل‌های یادگیری ماشین مبتنی بر یادگیری عمیق، شبکه عصبی مصنوعی [۱۹]، استنتاج فازی مبتنی بر شبکه تطبیقی (ANFS) [۲۰] و درخت تصمیم (DT) [۲۱] روش‌های مهمی هستند که برای تشخیص اشیا استفاده می‌شوند. در این تحقیق از این ابزارها برای احراز هویت افراد با ترکیبی از ویژگی‌های استخراج شده استفاده کرده‌ایم.

۳-۱-۲- خوشه بندی K-Means فازی

روش K-Means یک الگوریتم خوشه‌بندی است که مجموعه‌ای از نقاط داده را به خوشه‌ها اختصاص می‌دهد به صورتی که نقاط داده در همان خوشه شباهت بالایی داشته باشند. الگوریتم K-Means به دلیل کارایی آن مورد استفاده بوده و با تغییرات و تعمیم‌های متنوعی در طول سال‌ها توسعه یافته است. در میان انواع مختلف الگوریتم K-Means ، الگوریتم K-Means فازی (FKM) محبوب‌ترین است [۲۲-۲۳]. به این ترتیب، برای مقابله با برخی از مشکلات در طول خوشه‌بندی، مانند تعداد خوشه‌ها و مراکز اولیه خوشه، یک اصطلاح پنالتی به تابع هدف FKM معرفی شده است [۲۴]. خوشه‌بندی X به خوشه‌های C توسط این الگوریتم برای به حداقل رساندن تابع هدف زیر است:

$$f[U,V]=\sum_{i=1}^{n}\sum_{k=1}^{c}u_{ik}\,d_{ik}+\gamma\sum_{i=1}^{n}\sum_{k=1}^{c}u_{ik}\,logu_{ik} \quad (۱)$$

منوط به

$$\sum_{i=1}^{n}u_{ik}=1\,,u_{ik}\in(0,1],1\le i\le n\,,1\le k\le c \quad (۲)$$

در جایی که U یک ماتریس تقسیم‌بندی NC، V یک ماتریس CMM حاوی مراکز خوشه و DIK یک تفاوت اندازه‌گیری بین مرکز خوشه KT و شی i-t است. روش به حداقل رساندن متناوب بین ماتریس عضویت U و ماتریس مرکز خوشه V را می‌توان برای (۱) اعمال کرد:

$$u_{ik}=\frac{\exp\left(\frac{-d_{ik}}{\gamma}\right)}{\sum_{s=1}^{c}\exp\left(\frac{-d_{is}}{\gamma}\right)} \quad (۳)$$

$$v_k=\frac{\sum_{i=1}^{n}\mathrm{u}_{ik}X_i}{\sum_{i=1}^{n}\mathrm{u}_{ik}} \quad (۴)$$

اولین عبارت در (۱) تابع هزینه الگوریتم استاندارد K-Means است. عبارت دوم برای به حداکثر رساندن آنتروپی منفی عضویت اشیاء به خوشه در فرآیند خوشه‌بندی اضافه می‌شود، که می‌تواند همزمان پراکندگی درون خوشه‌ای را به حداقل برساند و آنتروپی وزن منفی را جهت تعیین خوشه‌ها برای کمک به ارتباط اشیاء به حداکثر برساند.

۳-۱-۳- الگوریتم ژنتیک

الگوریتم‌های ژنتیک فرآیند جستجوی مقادیر بهینه را در چندین نقطه به طور همزمان در یک نسل انجام می‌دهند [۱]. فرآیند تکرار با رویکرد تکاملی نسل به نسل انجام می‌شود، اما تعداد اعضای کروموزوم با بهترین تناسب برای هر نسل حفظ می‌شود زیرا آنها مجموعه ای از راه‌حل‌ها هستند [۲۴]. کروموزوم‌ها می‌توانند کدهای باینری، عدد صحیح یا اعشاری باشند. در فرآیند تکامل، تعدادی از ژن‌ها که کروموزوم را می‌سازند در یک فرآیند متقاطع و جهش هستند [۲۵]. الگوریتم‌های ژنتیک با استفاده از کروموزوم‌هایی که برای به دست آوردن جواب بهینه زنده نگه‌داشته می‌شوند از انتقال امکان‌پذیر برای انتخاب بهترین کروموزوم‌ها استفاده می‌کنند [۳۰ و ۳۱]. فرآیند تناسب هر کروموزوم به‌طور جداگانه با تغییر ژنوتیپ کروموزوم به فنوتیپ آن انجام می‌شود. رشته‌های باینری به متغیرهایی به شکل جفت های واقعی $[M,n]$ تبدیل می‌شوند. جمعیت اولیه، یک رشته باینری با طول N است که مردم نامیده می‌شوند. این فرآیند انتخاب را برای نسل بعدی توسط چرخ رولت حفظ می‌کند. بنابراین، کروموزوم با تناسب بالا شانس بیشتری برای انتخاب دارد. انتخاب افرادی که به نسل بعدی منتقل می‌شوند با تولید اعداد تصادفی $r\in(0,1)$ انجام می شود [۲۹]. روند فرآیند یک الگوریتم ژنتیک در شکل (۱) نشان داده شده است.

تقاطع از روش یک نقطه برش با جفت شدن دلخواهانه کروموزوم‌ها، سپس انتخاب یک نقطه متقاطع برای تنظیم محل برش در کروموزوم‌ها استفاده می‌کند. به عنوان مثال، کروموزوم‌های ۲ و ۵ به عنوان اولین جفت برای عبور انتخاب می‌شوند و $r=2$ نقطه متقاطع است. در این تحقیق، انتخاب $\alpha=0.01$ به این معنی است که حدود ۱٪ از ژن ها در جمعیت جهش می‌یابند. اگر مقدار ژن i صفر باشد، مقدار ژن به ۱ تغییر می‌کند، اما اگر مقدار آن ۱ باشد، به ۰ تغییر می‌کند. علاوه بر این،

ژن‌های کروموزوم‌های ۱، ۳ و ۴ با مقدار ۱ جهش می‌یابند. کروموزوم با ارزش تناسب بالا، احتمال تکثیر در نسل بعدی را خواهد داشت [۳۰].

۳-۲- کار پیشنهادی

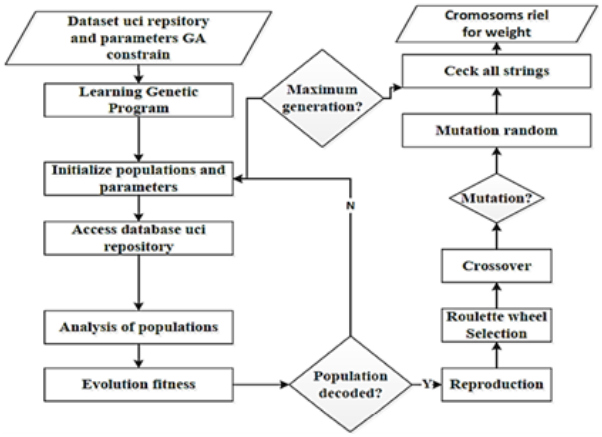
امروزه بانک‌ها به طور فزاینده‌ای از فناوری بیومتریک برای شناسایی بهتر مشتریان جدید، احراز هویت ایمن مشتریان فعلی، محافظت از تراکنش-های با ارزش بالا و مبارزه با کلاهبرداری استفاده می کنند. در واقع، از آنجایی که بانک‌ها بیومتریک را در همه جا از شعب فیزیکی سنتی گرفته تا جدیدترین پلتفرم‌های دیجیتال به کار می‌گیرند، این فناوری تنها ابزار قابل اعتماد برای احراز هویت و تامین امنیت مشتریان بانکی در همه کانال‌ها می‌باشد. روندهای منتهی به پذیرش بیومتریک در بین بانک ها متعدد و شامل موارد زیر است:

- ظهور تلفن‌های همراه و احراز هویت بیومتریک چند وجهی مبتنی بر تلفن همراه.
- ظهور کارت‌های بانکی بیومتریک به معنای «خداحافظی با کدهای پین».
- دریافت کراس کانال، پذیرش بیومتریک در تمام کانال‌های بانکی اتفاق می‌افتد، پشتیبانی فزاینده API های بانکداری باز، از طریق مقرراتی مانند 2PSD که استفاده از بیومتریک را در سناریوهای احراز هویت چند عاملی تشویق می‌کنند و دستگاه‌های اینترنت اشیاء که از صدا و تصویر پشتیبانی می‌کنند.

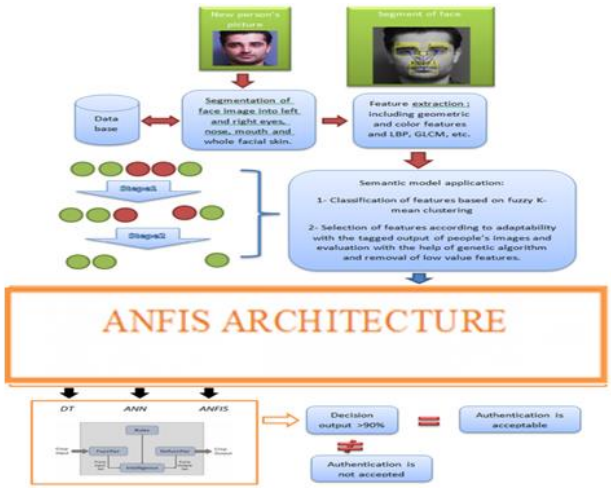
در این مقاله ضمن بررسی مشکلات امنیتی در بانکداری همراه به روش‌های احراز هویت در بانکداری آنلاین و موبایلی پرداخته شده و در این راستا روش جدیدی برای حل چالش اصلی امنیت و احراز هویت در حوزه بانکداری همراه ارائه شده است. روش پیشنهادی ترکیبی از روش-های داده‌کاوی شامل روش‌های یادگیری عمیق مانند شبکه عصبی مصنوعی (ANN)، شبکه فازی عصبی تطبیقی (ANFIS) و الگوریتم درخت تصمیم C4.5 است. در ادامه مراحل اجرای طرح احراز هویت با چهره افراد بر اساس مدل معنایی پیشنهادی شرح داده شده است. اساس مدل‌سازی معنایی این اثر، سازگاری ویژگی‌های استخراج شده از تصویر چهره افراد برای احراز هویت است.

این فرآیند شامل موارد زیر می باشد:

- فاز ۱: مجموعه داده‌های مورد استفاده در این مقاله می‌تواند شامل هر نوع داده‌ای باشد که در زمینه موبایل بانک استفاده می‌شود؛ اما با توجه به تمرکز این کار بر احراز هویت اشخاص حقیقی، سعی خواهد شد از مجموعه‌ای از تصاویر استفاده شود. تصویر افراد مختلف باید از زوایای مختلف مورد استفاده قرار گیرد. داده‌های [۲۵،۲۶] می‌تواند از جمله مجموعه داده‌های مورد استفاده در این تحقیق باشد.
- فاز ۲: تهیه داده‌گاهی در متون داده‌کاوی به عنوان یک موضوع جزئی و به عنوان گامی در فرآیند داده‌کاوی نادیده گرفته می‌شود. در برنامه-های کاربردی داده‌کاوی در دنیای واقعی، وضعیت برعکس است و تلاش بیشتری صرف آماده‌سازی داده‌ها، نسبت به روش‌های داده‌کاوی می‌شود. در این راستا دو وظیفه اصلی برای آماده‌سازی داده‌ها وجود دارد: (الف) سازماندهی استاندارد داده‌ها در اجرای پروژه‌های داده‌کاوی به منظور آماده سازی داده‌ها برای پردازش با داده‌کاوی و سایر ابزارهای مبتنی بر رایانه. (ب) تهیه مجموعه داده‌ها به گونه‌ای که به بهترین عملکرد روش‌های داده‌کاوی منجر شود.
- فاز ۳: انتخاب دسته‌بندی‌ها برای ادغام باید به گونه‌ای باشد که این دسته‌ها مکمل یکدیگر باشند و هر کدام به اختصار توضیح داده شوند. تفکیک نمونه‌های آموزشی و آزمون برای دسته‌هایی که مکمل یکدیگر هستند بر اساس ویژگی‌های استخراج شده مورد توجه است. خوشه‌بندی K-Means فازی نظارت شده برای مجموعه‌ای از نمونه‌های تصویر جهت آموزش یک سیستم یادگیری ماشین استفاده شده است. این مجموعه داده شامل ۷۷ ویژگی است که از تصاویر چهره افراد مورد مطالعه استخراج شده است.
- فاز ۴: از یک روش الگوریتم تکاملی برای هر دسته از ویژگی‌ها استفاده می‌شود تا مجموعه‌ای از ویژگی‌ها انتخاب شود که با برآورد صحیح افراد مطابقت داشته باشد. با توجه به الگوریتم ژنتیک پیشنهادی برای طبقه‌بندی و جداسازی نمونه‌ها برای این مرحله یک تابع هدف سازگاری تعریف شده است. تابع هدف در بخش بعدی معرفی می‌شود.



شکل (۱): مسیر نسل جدید در الگوریتم ژنتیک [۲۹]



شکل (۲): فلوچارت مراحل اجرای طرح احراز هویت چهره پیشنهادی بر اساس مدل معنایی

- فاز ۵: نتایج به دست آمده از دسته‌ها به صورت اکثریت آرا ترکیب می‌شوند. در این مرحله، مقادیر انتخاب شده برای خروجی نهایی از پاسخ‌ها بر اساس دسته‌بندی‌ها و بر اساس یک تصمیم جمعی فازی برای داده‌ها به دست می‌آید. قوانین فازی حاکم بر این تصمیم در بخش بعدی ارائه شده است. فرآیندهای اجرای طرح احراز هویت چهره پیشنهادی بر اساس مدل معنایی در شکل (۲) نشان داده شده است.

۳-۲-۱- روش‌های مدل معنایی با کمک سازگاری ویژگی با خروجی‌های برچسب‌گذاری شده افراد

این پروژه با توجه به مراحل ذکر شده به منظور انجام یک سیستم یادگیری ماشینی به عنوان یک سیستم آموزش و تست شامل ANN، ANFIS، DT بر اساس مدل معنایی پیشنهادی انجام شده است. در این رویکرد از دو روش برای ایجاد یک مدل معنایی استفاده شده است. در روش اول از خوشه‌بندی K-Means فازی برای دسته‌بندی ویژگی‌های استخراج شده از چهره افراد با کمک داده‌های آموزش تصویر استفاده شده است. بنابراین، با توجه به مقادیر خروجی داده‌های آموزشی، خوشه‌بندی ویژگی‌ها برای تصاویر افرادی که برای ایجاد حساب همراه بانک ثبت‌نام کرده‌اند، انجام شده است. خوشه‌بندی پیشنهادی ویژگی‌های استخراج شده، تصاویر را به سه دسته از ویژگی‌های مورد استفاده برای سیستم یادگیری ماشین تقسیم می‌کند.

روش دوم بر اساس توانایی کمک یک تابع هدف چند جمله‌ای برای هر ویژگی از تصاویر آموزشی است. در این روش پس از نرمال‌سازی ویژگی‌ها، از الگوریتم ژنتیک استفاده می‌کنیم. این الگوریتم ضرایب چندجمله‌ای را پس از ۳۰۰ دوره تکرار تعیین می‌کند. در این بخش، تابع هدف را به عنوان انحراف چندجمله‌ای مقادیر خروجی هدف برای تعداد تصاویر افراد مختلف تعریف می‌کنیم. ضرایب چند جمله‌ای، پاسخ‌های مستقل از الگوریتم ژنتیک را برای حداقل انحراف نهایی از مقادیر خروجی تصویر نشان می‌دهند. در این مرحله، پس از تعیین ضرایب چندملیتی مورد نظر برای همه ویژگی‌ها، هر کدام که خطای خروجی کمتری دارند، به عنوان ویژگی‌های تطبیقی با تصویر فرد شناسایی می‌شوند؛ که این ویژگی‌ها برای آموزش سیستم یادگیری ماشینی در دسته‌های خوشه‌ای انتخاب شده‌اند.

کد برنامه تابع شیء در زیر آمده است:

```
function z = Sphere(x,y)
%normalization
    Y = y(:,1);
    Yn = (Y - min(Y))/(max(Y) - min(Y));
    z = sum(abs(x(1) * Yn. ^5 + x(2) * Yn. ^4 + x(3)
                * Yn. ^3 + x(4) * Yn. ^2 + x(5) * Yn
                + x(6) - y(:,2)));
end
```

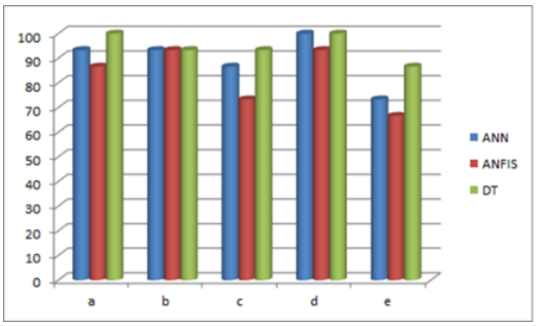
۳-۲-۲- پاسخ‌های سیستم‌های یادگیری ماشین

پس از انتخاب و طبقه‌بندی ویژگی‌های استخراج شده از تصاویر بر اساس تقسیم‌بندی‌های انجام شده، مجموعه‌ای از ویژگی‌ها به هر سیستم یادگیری ماشین اختصاص داده می‌شود. با توجه به آموزش داده شده، برای هر شخص واقعی به هر سیستم یادگیری ماشینی یک انتخاب با درصد مشخصی از دقت داده می‌شود. قوانین حاکم برای این تصمیم فازی در جدول (۱) آورده شده است. مقادیر ورودی سیستم فازی با کمک سطح دقت هر سیستم یادگیری ماشینی مورد نظر برای هر فرد در محدوده بین ۰ و ۱ تعریف می‌شود که برای هر فرد و هر سیستم یادگیری با کمک سیستم آموزش چهره از پیش تعیین شده است. مقدار ۱ برای هر شخص مورد نظر به این معنی است که تصویر این شخص توسط سیستم یادگیری ماشینی با دقت ۱۰۰ درصد به درستی شناسایی شده است. همچنین مقدار ۰ به این معنی است که فرد شناسایی شده به درستی توسط این سیستم یادگیری ماشینی با دقت ۰ درصد شناسایی شده است. رابطه دقت محاسبه شناسایی افراد توسط الگوریتم یادگیری مورد نظر به صورت زیر تعریف می‌شود:

دقت شناسایی افراد = تعداد تصاویر افراد به درستی شناسایی شده / تعداد کل تصاویر افراد برای آموزش سیستم یادگیری ماشین

جدول (۱): قواعد اساسی تصمیم‌گیری فازی

DT	ANN	ANFIS	Decision Output
Low	Low	Low	Low
Low	Low	Mid	Low
Low	Low	High	Low
Low	Mid	Low	Low
Low	Mid	Mid	Low
Low	Mid	High	Low
Low	High	Low	Low
Low	High	Mid	Low
Low	High	High	High
Mid	Low	Low	Low
Mid	Low	Mid	Low
Mid	Low	High	Low
Mid	Mid	Low	Low
Mid	Mid	Mid	Low
Mid	Mid	High	High
Mid	High	Low	Low
Mid	High	Mid	High
Mid	High	High	High
High	Low	Low	Low
High	Low	Mid	Low
High	Low	High	High
High	Mid	Low	Low
High	Mid	Mid	High
High	Mid	High	High
High	High	Low	High
High	High	Mid	High
High	High	High	High



شکل (۳): محاسبه دقت شناسایی افراد توسط DT، ANFIS و ANN برای ۵ نفر

۴- نتایج و بحث‌ها

به منظور آزمایش رویکردهای پیشـــنهادی، از پایگاه داده چهره AR [۲۵،۲۶] و فریم دوربین موبایل برای افراد مختلف اسـتفاده شـده اسـت که در آن برای هر فرد ۱۵ عکس با حالات چهره و تغییرات نور متفاوت وجود دارد. همچنین از پایگاه داده MUTC با ۳۷۵۵ چهره برای ۷۶ عضـو ثبت شـده اسـتفاده شـده که در آن یک فایل برای هر یک از پنج دوربین و یک فایل برای اطلاعات نشـانه‌های دسـتی وجود دارد. برای جلوگیری از جعل و کلاهبرداری از یک سـری تصـاویر با فریم های مختلف چهره افراد که از طریق دوربین‌های مختلف موبایل گرفته شـده اسـت، اسـتفاده شـده اسـت. این کار ضـمن افزایش ارزش عملی روش پیشـــنهادی در زمینه موبایل بانک، امکان اســـتفاده هکرها از تصـــاویر جعلی را تا حد زیادی کاهش می‌دهد. دلیل این امر اســـتفاده آنلاین از پردازش تصویر با فریم های مختلف است.

در رویکرد پیشنهادی، ویدیویی از یک کاربر که هر یک از چالش‌ها را انجام می‌دهد، یک تلاش فردی برای ورود به سیستم تلقی می‌شود. از آنجایی که اکتساب داده‌ها کنترل نمی‌شود، ویدئوهایی با طول‌های مختلف جمع‌آوری می‌شوند. بنابراین، یک خط لوله خودکار برای پردازش ویدیوهای ضبط شده به داده‌های ساختاریافته پیشنهاد شده که بعداً برای ایجاد ویژگی‌هایی برای احراز هویت چهره استفاده می‌شود. در این راستا ابتدا، ابرداده جهت‌گیری ویدئو استخراج شده تا بهترین عملکرد را از کتابخانه‌های نرم‌افزار MATLAB که برای تشخیص چهره و تشخیص نقطه‌نظر استفاده می‌شوند، داشته باشیم. سپس مجموعه‌ای از فریم‌ها از هر ویدیوی جمع‌آوری شده نمونه برداری می‌شوند. در مطالعه پیش‌رو، تمام ویدیوها با سرعت ۱۰ فریم در ثانیه (fps) نمونه‌برداری شده‌اند. پس از آن، برای پارادایم، تشخیص چهره طبق روش‌های ذکرشده بر اساس توابع و جعبه ابزار MATLAB مدل سازی و پیاده سازی شده است.

پیش پردازش تصاویر به منظور حذف نویز و افزایش کیفیت تصاویر با کمک مدل‌های اولیه انجام می‌شود. برای مشکل روشنایی در این کار سعی شده است که میانگین تضاد تصاویر برای همه نمونه‌ها و فریم‌ها در مقدار ۳۰ نرمال شود. برای استخراج ویژگی‌هایی مانند بافت، رنگ و مشخصات هندسی در قسمت‌های مختلف از توابع متفاوتی استفاده شده است. در مجموع ۷۷ ویژگی برای هر تصویر از شخص مورد نظر استخراج می‌شود که به دلیل ناکارآمدی برخی ویژگی‌های تصاویر نمونه، برای طبقه‌بندی هویت افراد، در پردازش‌های بعدی می‌بایست ارزش آن ویژگی‌ها کاهش یابد یا کلاً حذف شوند. با توجه به این دیدگاه، در این اثر، یک مدل معنایی برای خوشه‌بندی ویژگی‌ها بر اساس وابستگی آنها به افراد هدف و سازگاری آنها با کدهای احراز هویت افراد ارائه شده است. این مدل معنایی ضمن کمک به کاهش حجم پردازش اطلاعات برای سیستم‌های پردازشگر سیار به صورت بهینه از مهم‌ترین ویژگی‌های موجود استفاده می‌کند. با توجه به این فرآیندها، ویژگی‌ها به سه دسته تقسیم شده و با کمک روش‌های پیشنهادی مبتنی بر الگوریتم ژنتیک و خوشه بندی K-Means فازی، مجموعه ۷۷ ویژگی در سه گروه ۲، ۴ و ۲۴ طبقه بندی می‌شوند. در مجموع از ۳۰ ویژگی برای شناسایی تصویر چهره افراد استفاده شده است. در این مرحله، ویژگی‌های انتخاب شده و دسته‌بندی‌شده به‌ترتیب توسط گروه‌های ۲۴، ۴ و ۲ وارد سه سیستم یادگیری ماشین به نام‌های ANN، ANFIS و DT می‌شوند. آموزش با کمک این داده‌ها انجام می‌شود. اکنون برای داده‌های تصویر آزمایش شده، دقت احراز هویت هر فرد برای هر سیستم یادگیری ماشینی محاسبه می‌شود. شکل (۳) نتایج دقت شناسایی ۵ فرد آزمایش شده را برای هر سه سیستم یادگیری ماشینی به صورت نمودار میله‌ای نشان می‌دهد. در نهایت نتایج تصمیم‌گیری برای تصویر آزمایشی با کمک سیستم منطق فازی نمایش داده شده است. برای نمونه تصویر آزمایش شده، تا ۹۸/۵ درصد تشخیص صحیح چهره با کمک سیستم منطق تصمیم گیری فازی تضمین شده است.

۵- نتیجه

در این کار، یک روش احراز هویت چهره پویا مبتنی بر مدل معنایی با کمک خوشه‌بندی ویژگی با روش K-Means فازی و انتخاب ویژگی تطبیقی توسعه داده شده. روش‌های مهندسی ویژگی توسعه داده شده برای نشان دادن نشانه های زمان چالش و ویژگی‌های چهره مؤثر هستند. همچنین، مجموعه‌ای از معماری‌های یادگیری ماشین پیشنهاد و پیکربندی شده‌اند تا تأیید چهره را به طور مؤثر انجام دهند. مطالعه انجام شده رویکردی موثر برای سیستم‌های احراز هویت چهره ارائه می‌کند که می‌تواند در حوزه بانکداری موبایلی مورد استفاده قرار گیرد و امنیت حساب‌های بانکی و اعتماد مشتریان را افزایش دهد. در تحقیقات آتی، پارادایم‌هایی پیشنهاد شده‌اند که می‌توانند انواع مختلف حملات مبتنی بر بانکداری آنلاین و رسانه‌ای (حملات چاپی، حملات صفحه نمایش، ماسک‌های دوبعدی، ویدیوهای سرقت شده از رسانه، جعلی‌های عمیق) را شناسایی کنند.

مراجع

[1] Smith-Creasey M, Albalooshi FA, & Rajarajan M (2018) Continuous face authentication scheme for mobile devices with tracking and liveness detection. Microprocess Microsyst 63:147-157.

[2] Jafri R & Arabnia HR (2009) A survey of face recognition techniques. J Inf Process Syst 5:41-68.
[3] Mohan J, & Rajesh R (2021) Enhancing home security through visual cryptography. Microprocess Microsyst 80:103355.
[4] Adesuyi F A, Oluwafemi O, Oludare AI & Rick A (2013) Secure authentication for mobile banking using facial recognition.
[5] Stragapede G et al. (2022) Mobile behavioral biometrics for passive authentication. Pattern Recognit Lett 157: 35-41.
[6] Saxena N & Varshney D (2021) Smart Home Security Solutions using Facial Authentication and Speaker Recognition through Artificial Neural Networks. International Journal of Cognitive Computing in Engineering 2:154-164.
[7] Zeroual A, Amroune M, Derdour M & Bentahar A (2021) Lightweight deep learning model to secure authentication in Mobile Cloud Computing. J. King Saud Univ. - Comput Inf Sci.
[8] Pérez JC, Alfarra M, Thabet A, Arbeláez P & Ghanem B (2022) Towards Assessing and Characterizing the Semantic Robustness of Face Recognition. arXiv preprint arXiv:2202.04978.
[9] Gong D, Zhu K, Li Z & Qiao Y (2013) in 2013 IEEE International Conference on Information and Automation (ICIA). 1369-1374 (IEEE).
[10] El-Soud MWA, Gaber T, AlFayez F & Eltoukhy MM (2021) Implicit authentication method for smartphone users based on rank aggregation and random forest. Alex Eng J 60:273-283.
[11] Shu Y et al. in Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition. 11916-11925.
[12] Samangouei P, Patel VM & Chellappa R (2017) Facial attributes for active authentication on mobile devices. Image Vis Comput 58:181-192.
[13] Yanakova E, Ishkova T, Belyaev A, Koldaev V & Kolobanova M (2019) in 2019 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus). 1848-1851 (IEEE).
[14] Gudi A (2015) Recognizing semantic features in faces using deep learning. arXiv preprint arXiv:1512.00743.
[15] Almudhahka NY, Nixon MS & Hare JS (2017) in 2017 12th IEEE International Conference on Automatic Face & Gesture Recognition (FG 2017). 180-185 (IEEE).
[16] de Castro D C & Nowozin S: in Proceedings of the European Conference on Computer Vision (ECCV). 745-761.
[17] Choi HS & Cho YH (2019) Analysis of Security Problems of Deep Learning Technology. Journal of the Korea Convergence Society 10: 9-16.
[18] Najafabadi MM et al. (2015) Deep learning applications and challenges in big data analytics. J Big Data 2:1-21.
[19] Kim Th: in International Conference on Information Security and Assurance. 138-148 (Springer).
[20] Sujatha K et al. in Proceedings of International Conference on Sustainable Computing in Science, Technology and Management (SUSCOM), Amity University Rajasthan, Jaipur-India.
[21] Redla SS, Mallik B & Mangalampalli VK (2020) in 2020 2nd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA). 223-229 (IEEE).
[22] Ruspini EH (1969) A new approach to clustering. Information and control 15:22-32.
[23] Bezdek JC (1980) A convergence theorem for the fuzzy ISODATA clustering algorithms. IEEE Trans Pattern Anal Mach Intell 1-8.
[24] Li MJ, Ng MK, Cheung Ym. & Huang JZ (2008) Agglomerative fuzzy K-Means clustering algorithm with selection of number of clusters. IEEE Trans Knowl Data Eng 20:1519-1534.
[25] Naruei I & Keynia F (2021) Wild horse optimizer: A new meta-heuristic algorithm for solving engineering optimization problems. Eng Comput 1-32.
[26] Wu YL, Tang CY, Hor MK & Wu PF (2011) Feature selection using genetic algorithm and cluster validation. Expert Syst Appl 38:2727-2732.
[27] Venkatesh B & Anuradha J (2019) A review of feature selection and its methods. Cybern Inf Technol 19:3-26.
[28] Malhotra R, Singh N & Singh Y (2011) Genetic algorithms: Concepts, design for optimization of process controllers. Comput Sci Inf Syst 4:39.
[29] Pei M, Goodman E & Punch W. in Proceedings of the 1st International Symposium on Intelligent Data Engineering and Learning, IDEAL. 371-384.
[30] Suardani LGP, Bhaskara IMA & Sudarma M (2018) Optimization of Feature Selection Using Genetic Algorithm with Naïve Bayes Classification for Home Improvement Recipients. Int J Eng Emerging Technol 3:66-70.
[31] Huszár VD & Adhikarla VK (2021) Live spoofing detection for automatic human activity recognition applications. Sensors 21:7339.
[32] Milborrow S, Morkel J & Nicolls F (2010) The MUCT landmarked face database. Pattern recognition association of South Africa 201.
[33] Cherifi F, Hemery B, Giot R, Pasquet M & Rosenberger C (2010) in Behavioral biometrics for human identification: Intelligent applications 57-74 (IGI Global, 2010).
[34] Maglogiannis I, Iliadis L, Macintyre J & Cortez P (2022) Artificial Intelligence Applications and Innovations: 18th IFIP WG 12.5 International Conference, AIAI 2022, Hersonissos, Crete, Greece, June 17–20, 2022, Proceedings, Part II. Vol. 647 (Springer Nature, 2022).
[35] Eberz S, Rasmussen KB, Lenders V & Martinovic I (2017) in Proceedings of the 2017 ACM on Asia conference on computer and communications security. 386-399.
[36] Buriro A, Crispo B, Frari FD, Klardie J & Wrona K: in International conference on passwords. 45-61 (Springer).
[37] Kumar R, Phoha VV & Raina R (2016) Authenticating users through their arm movement patterns. arXiv preprint arXiv:1603.02211.
[38] Shrestha B, Mohamed M & Saxena N (2016) Walk-unlock: Zero-interaction authentication protected with multi-modal gait biometrics. arXiv preprint arXiv:1605.00766.
[39] Ehatisham-ul-Haq M et al (2017) Authentication of smartphone users based on activity recognition and mobile sensing. Sensors 17:2043.
[40] Li G & Bours P (2018) in 2018 21st International Conference on Information Fusion (FUSION). 2091-2097 (IEEE).
[41] Buriro A, Crispo B & Conti M (2019) AnswerAuth: A bimodal behavioral biometric-based user authentication scheme for smartphones. J Inf Secur Appl 44:89-103.
[42] Volaka HC, Alptekin G, Basar OE, Isbilen M & Incel OD (2019) Towards continuous authentication on mobile phones using deep learning models. Procedia Comput Sci 155:177-184.

[43] Lamiche I, Bin G, Jing Y, Yu Z & Hadid A (2019) A continuous smartphone authentication method based on gait patterns and keystroke dynamics. J Ambient Intell Humaniz Comput 10: 4417-4430.
[44] Abuhamad M, Abuhmed T, Mohaisen D & Nyang D (2020) AUToSen: Deep-learning-based implicit continuous authentication using smartphone sensors. IEEE Internet Things J 7:5008-5020.Object Management Group. Unified Modeling Language: Superstructure, Version 2.0, ptc/03-07-06, July 2003, http://www.omg.org/cgi-bin/doc?ptc/2003-08-02.