دانشگاه صنعتی امیرکبیر
(پلی تکنیک تهران)

دانشکده مهندسی کامپیوتر

گزارش درس روش پژوهش و ارائه

عنوان

احراز هویت الکترونیک بر مبنای سنجه‌های بیومتریکی

نگارش

هدیه پورقاسم

استاد راهنما

دکتر رضا صفابخش

بهمن ماه ۱۳۹۹

ماحصل آموخته هایم راتقدیم می کنم به آنان که مهر آسمانی شان آرام بخش آلام زمینی ام است.

به استوارترین تکیه گاهم، دستان پرمهر پدرم،

به سبزترین نگاه زندگیم، چشمان سبز مادرم،

که هرچه آموختم در مکتب عشق شما آموختم و هرچه بکوشم قطره ای از دریای بی کران مهربانیتان را سپاس نتوانم بگویم.

امروز هستی ام به امید شماست و فردا کلید باغ بهشتم رضای شما، ره آوردی گران سنگ تر از این ارزان نداشتم تا به خاک پایتان نثار کنم، باشد که حاصل تلاشم نسیم گونه غبار خستگیتان را بزداید.

بوسه بر دستان پرمهرتان

سپاس‌گزاری

استاد گرامی جناب آقای دکتر صفابخش

دلسوزی، تلاش و کوشش حضرت عالی در تعلیم و تربیت، انتقال معلومات و تجربیات ارزشمند در کنار ایجاد فضایی دلنشین برای کسب علم و دانش و درک شرایط دانشجویان حقیقتا قابل ستایش است.

اینجانب بر خود وظیفه می‌دانم که در کسوت شاگردی از زحمات و خدمات ارزشمند شما استاد گران قدر تقدیر و تشکر نمایم.

هدیه پورقاسم

بهمن ۱۳۹۹

چکیده

احراز هویت، فرآیند شناسایی کاربرانی است که درخواست دسترسی به یک سیستم، شبکه یا دستگاه را دارند. امروزه با توجه به استفاده‌ی روزافزون مردم از سرویس‌های آنلاین و بالا رفتن آمار دزدی‌ها و کلاهبرداری‌های اینترنتی اهمیت احراز هویت الکترونیک چندین برابر شده است. باید توجه داشت که روش قدیمی داشتن یک رمز با تعدادی حروف و اعداد دیگر دارای امنیت کافی نیست و حمله به این رمزها امری ساده است، بنابراین روش‌های جدیدی برای احراز هویت بر مبنای سنجه‌های بیومتریکی[1] پیشنهاد شده‌اند که امنیت بیشتری دارند. احراز هویت بر مبنای سنجه‌های بیومتریکی به معنای تشخیص خودکار افراد براساس صفات فیزیولوژیکی و رفتاری آن‌ها است. تشخیص چهره، تشخیص اثر انگشت، تشخیص امضای دیجیتال، تشخیص صدا و تشخیص ضربه زدن به صفحه‌کلید و پویایی لمسی از روش‌های متداول احراز هویت بر مبنای سنجه‌های بیومتریکی هستند که هر یک دارای نقاط ضعف و نقاط قوتی می‌باشند.

این سیستم‌ها با چالش‌هایی در عملکرد تشخیص، امنیت سیستم و مسائل حریم خصوصی مواجه هستند. پژوهشگران پیشنهادهای مختلفی برای حل چالش‌های روش‌های این نوع احراز هویت مطرح کرده‌اند. در این مقاله تلاش شده‌است تا به صورت خلاصه بعضی از این پیشنهادات و روش‌ها معرفی، ارزیابی و مقایسه شوند و در نهایت روشی مطمئن برای بهبود احراز هویت از راه دور پیشنهاد شود.

واژه‌های کلیدی:

احراز هویت الکترونیک، سنجه‌های بیومتریکی

[1] Biometric authentication

فهرست مطالب

عنوان صفحه

فهرست اشکال

صفحه

فهرست جداول

فصل اول

مقدمه

مقدمه

به دلیل رشد سریع اینترنت و دستگاه‌های تلفن همراه، اهمیت سیستم‌های احراز هویت به طور گسترده‌ای در دسترسی به این سرویس‌ها و دستگاه‌ها، به منظور محافظت از دستگاه، محتویات و حساب‌های کاربری در حال افزایش است.

واضح است که با افزایش حساب‌های کاربری مختلف یک فرد، مدیریت رمزهای عبور بسیار دشوار می‌شود، زیرا به خاطر سپردن رمزهای عبور مختلف برای دسترسی به سیستم‌های مختلف، به ویژه آن‌هایی که دارای سطح امنیتی بالایی هستند، دشوار است. همچنین امروزه حمله به رمزهای عبوری که دارای تعدادی حرف و عدد هستند امر ساده‌ایست و امنیت و حریم خصوصی کاربران در خطر است. به منظور حل این مشکلات، سنجه‌های بیومتریکی به دلیل ویژگی های منحصر به فرد خود مورد مطالعه و در احراز هویت فردی مورد استفاده قرار گرفته‌اند. از فواید استفاده از سنجه‌های بیومتریکی در فرآیند احراز هویت می‌توان موارد زیر را نام برد:

۱. رمزهای بیومتریکی فراموش نمی‌شوند و قابل گم شدن نیستند.

۲. کپی کردن و یا اشتراک گذاری این رمزها دشوار است.

۳. جعل و توزیع رمزهای بیومتریکی دشوار است.

۴. نمی‌توان این رمزها را به راحتی حدس زد.

۵. شکستن رمز بیومتریکی یک فرد راحت تر از فرد دیگری نیست.

محققان در سال‌های اخیر تحقیقات گسترده و عمیقی در مورد احراز هویت بیومتریک انجام داده‌اند. برخی از محققان بر روش‌های رمزنگاری یا چارچوب‌های خاصی که در احراز هویت مبتنی بر سنجه‌های بیومتریکی استفاده می‌شود تمرکز کرده‌اند. بعضی مجموعه‌ای از روش‌های شناخت بیومتریک را بر اساس شبکه‌های عصبی با استفاده از صدا، عنبیه چشم، اثر انگشت، چاپ کف دست و چهره معرفی کرده‌اند و راه‌هایی برای بهبود آن‌ها نیز پیشنهاد داده‌اند، بعضی معتقداند که روش‌های بیومتریک تکی محدود هستند و روش‌های بیومتریک چند حالته برای ایجاد یک سیستم احراز هویت ایمن بسیار مطمئن‌تر هستند و بعضی تحقیقاتی بر مبنای پویایی ضربه کلید و پویایی لمسی انجام داده‌اند.

بدیهی است که امنیت و حریم خصوصی احراز هویت بیومتریک بسیار مهم است. با این حال، این مسئله در بسیاری از سیستمهای بیومتریک موجود به طور کامل مورد توجه قرار نگرفته است. بسیاری از محققان هنگام طراحی سیستم‌های خود، حملات احتمالی را در نظر نگرفته‌اند.

از خطرات احتمالی در یک سیستم احراز هویت بر مبنای سنجه‌های بیومتریکی، امکان حملات تکرار[۲] و افشای حریم خصوصی ویژگی بیومتریک[۳] را می‌توان نام برد. این حملات باعث می‌شوند سیستم در معرض خطر قرار گیرد. در نتیجه اطلاعات و علایق کاربر تهدید می‌شود. اطلاعات بیومتریک مورد استفاده در سیستم احراز هویت بخشی از حریم خصوصی کاربر است که مستلزم حفاظت ویژه است. اگر چنین اطلاعات خصوصی درز کند، مهاجمان می‌توانند از آن‌ها سواستفاده کنند. این امر ممکن است امنیت اطلاعات کاربر را در سیستم‌های دیگر تهدید کند و خسارات زیادی را به کاربران وارد کند.

در این گزارش، ابتدا نقاط ضعف و خطرات احتمالی سیستم‌های احراز هویت بر مبنای سنجه‌های بیومتریکی را بررسی می‌کنیم و به بررسی ویژگی‌هایی که یک سیستم احراز هویت بیومتریک ایده‌آل باید داشته باشد می‌پردازیم، سپس روش‌های بهبود پیشنهادی برای استفاده از ویژگی‌های ایستا و پویای بیومتریکی را بیان می‌کنیم و بر مبنای ویژگی‌های یک سیستم احراز هویت بیومتریک ایده‌آل، این روش‌ها را مورد مقایسه و بررسی قرار می‌دهیم. در پایان تلاش شده است تا یک سیستم اهراز هویت بر مبنای سنجه‌های بیومتریک، که در برابر خطرات و تهدیدات احتمالی بهترین عملکرد را داشته باشد، ارائه گردد.

[۲] Replay attack
[۳] Privacy disclosure of the biometric

فصل دوم

آشنایی با سیستم‌های احراز هویت بر مبنای سنجه‌های بیومتریکی

سیستم‌های احراز هویت بر مبنای ویژگی‌های بیومتریکی در مرحله‌ی ثبت‌نام، ویژگی‌های بیومتریکی مورد نیاز سیستم احراز هویت را از طریق یک سنسور یا گیرنده از کاربر دریافت می‌کنند و در سیستم ثبت می‌کند. از آن پس هر مرتبه که کاربر قصد ورود و دسترسی به سیستم و اطلاعات خود را داشته باشد باید ویژگی بیومتریکی مورد نیاز سیستم را توسط سنسور به سیستم بدهد، سپس سیستم داده‌ی وارد شده را با داده‌ی ثبت شده توسط کاربر در مرحله‌ی ثبت‌نام مقایسه کرده و بسته به تشخیص الگوریتم‌های سیستم، مشخص می‌کند که فرد اجازه‌ی دسترسی دارد یا خیر.

۲-۱ ساختار یک سیستم احراز هویت بر مبنای سنجه‌های بیومتریکی

یک سیستم احراز هویت بر مبنای سنجه‌های بیومتریکی معمولا از سه ماژول تشکیل شده است[۱]:

۱- نماینده‌ی کاربر[۴]

که درخواست تایید مجاز بودن هویت می‌کند و به خدمات اینترنت یا سایر دستگاه‌ها دسترسی پیدا می‌کند.

۲- ارائه دهنده‌ی هویت[۵]

که می تواند هویت کاربر را با توجه به داده‌های دریافت شده از نماینده‌ی کاربر و پایگاه داده ذخیره شده آن تأیید کند.

۳- بخش متکی[۶]

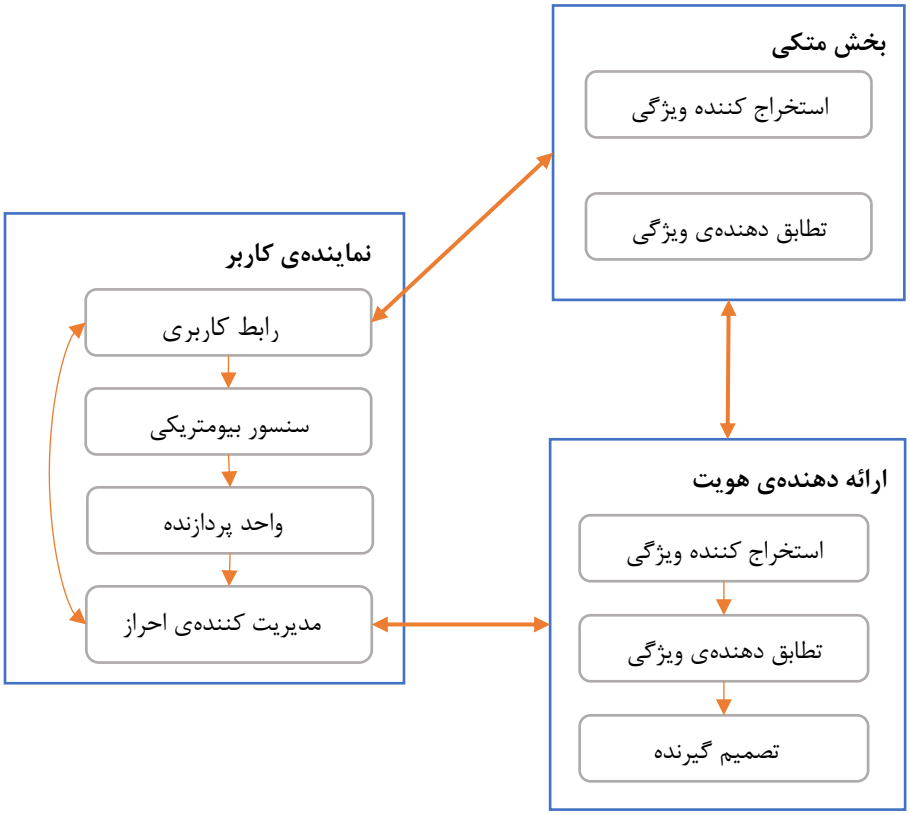
که می تواند کنترل دسترسی را طبق تصمیم ارائه دهنده‌ی هویت اعمال کند.

وقتی کاربر از طریق رابط کاربر سیستم، درخواست احراز هویت می‌دهد، سیستم از طریق یک کانال امن درخواست احراز هویت را به بخش ارائه دهنده‌ی هویت ارسال می‌کند. این بخش پس از دریافت درخواست احراز هویت، یک چالش برای بخش نماینده‌ی کاربر ارسال می‌کند. سپس این بخش می‌تواند سیگنال‌های بیومتریکی را از طریق یک سنسور بیومتریک جمع آوری کند و داده‌های جمع آوری شده را پیش پردازش کند (مانند کاهش سر و صدا و کدگذاری) و به چالش احراز هویت پاسخ دهد. نماینده‌ی کاربر باید پاسخ را از طریق یک کانال امن در شبکه به بخش ارائه دهنده‌ی هویت ارسال کند. هنگام دریافت پاسخ چالش، بخش ارائه دهنده‌ی هویت ویژگی‌های سیگنال‌های بیومتریک را استخراج می‌کند و آن‌ها را با سوابق موجود در پایگاه داده مطابقت می‌دهد. براساس

[۴] User Agent
[۵] Identity Provider
[۶] Relying Party

نتیجه مطابقت ، بخش ارائه دهنده‌ی هویت می‌تواند تصمیم بگیرد که آیا شخصی که در احراز هویت شرکت کرده است یک کاربر قانونی است یا خیر. در نهایت بخش متکی می‌تواند سیاست کنترل دسترسی کاربر فعلی را با توجه به تصمیم بخش ارائه دهنده‌ی هویت، مشخص کند.

قابل ذکر است که ماژول‌های ارائه دهنده‌ی هویت و بخش متکی به سه شکل وجود دارند. اول آن که هر دو درپایانه‌های محلی[۷] با هم وجود دارند و تمام مراحل احراز هویت در ترمینال انجام می‌شود. مورد دیگر این است که به عنوان بخشی از سرور در فضای ابری[۸] وجود دارند و برای تکمیل مراحل احراز هویت، ترمینال باید از طریق شبکه با سرور ارتباط برقرار کند. مورد سوم همانطور که در شکل ۱ نشان داده شده است ، جایی که این دو بخش جدا شده و متعلق به دو قسمت مختلف در سیستم هستند. این تمایز همچنین نقاط ضعف مختلفی را در سیستم احراز هویت بیومتریک به ارمغان می‌آورد.



شکل شماره ۲- ۱ نمونه‌ای از ساختار یک سیستم احراز هویت بر مبنای سنجه‌های بیومتریکی

[۷] Local terminal
[۸] Cloud

۲-۲ خطرهای بالقوه

نقاط آسیب‌پذیر در ساختار سیستم‌های احراز هویت بر مبنای سنجه‌های بیومترکی عبارت‌اند از:

۱- جعل سنسور[۹]

در این نوع حملات، ویژگی بیومتریک واقعی را با یک بازتولید مانند انگشت جعلی، عکس، ضبط صدا و غیره جایگزین می‌کنند. سیستم‌های بیومتریکی در برابر این حمله‌ها بسیار آسیب‌پذیراند. این یک ضعف جدی است که در پایانه های نماینده‌ی کاربر وجود دارد.

۲- ارسال مجدد سیگنال های بیومتریکی

این نوع حملات قادر به دور زدن حسگر و پخش مجدد سیگنال قبلاً ضبط شده به سیستم است. در فرآیند بارگذاری اطلاعات (ثبت نام یا احراز هویت)، ممکن است اطلاعات بیومتریک توسط مهاجم شبکه، از طریق شنود شبکه به سرقت برود. پس از آن، مهاجم می‌تواند اطلاعات بیومتریک را در احراز هویت بعدی بارگذاری مجدد کند تا حمله تکرار را کامل کند و به اطلاعات کاربر دسترسی یابد.

۳- حملات متداول شبکه به سرورها

وقتی بخش ارائه دهنده‌ی هویت و بخش متکی در یک سرور وجود داشته باشند، مهاجمان می‌توانند از طریق یک سری حملات شبکه به سیتسم دسترسی پیدا کنند سپس اطلاعات بیشتری را بدست آورند که فقط کاربران قانونی می‌توانند به آن‌ها دسترسی داشته باشند و قادر خواهند بود از این اطلاعات سوءاستفاده کنند.

۲-۳ انواع حملات با تمرکز بر انواع ویژگی‌های بیومتریکی

انواع مختلف حملات با تمرکز بر انواع ویژگی‌های بیولوژیکی را می‌توان به شکل زیر دسته‌بندی کرد:

۱- حمله به تشخیص چهره

به دست آوردن تصاویر و فیلم های چهره بسیار آسان است. حتی نیازی به سرقت عکس از کاربران نیست. مهاجمان می‌توانند به راحتی، به ویژه از طریق شبکه‌های اجتماعی عکس‌ها و تصاویر مورد نیازشان را بدست آورند و این امر تقلب در سیستم شناسایی چهره را بسیار ساده میکند.

[۹] Faking the sensor

۲- حمله به تشخیص عنبیه

با توسعه دوربین با وضوح بالا ، امروزه سرقت تصویر عنبیه و حمله به سیستم تشخیص مبتنی بر عنبیه امکان پذیر است اما هزینه این نوع حملات نسبتاً زیاد است.

۳- حمله به اثر انگشت و چاپ کف دست

به کمک انواع مختلفی از مواد می‌توان برای ساخت انگشت جعلی اقدام کرد و می‌توان اثر انگشت را از سطحی که کاربران لمس کرده‌اند جمع‌آوری کرد.

۴- حمله به صدا

صدا نوعی سیگنال بیولوژیکی است که به راحتی قابل جمع‌آوری است، زیرا سیگنال صوتی در یک محیط باز در همه‌ی جهات حرکت می‌کند. اگر یک مهاجم صدای کاربر را ضبط کرده و در حین احراز هویت کاربر مجدداً آن را پخش کند، احتمالاً سیستم احراز هویت مبتنی بر صدا فریب می‌خورد.

۵- حملات روی ضربه کلید و پویایی لمسی

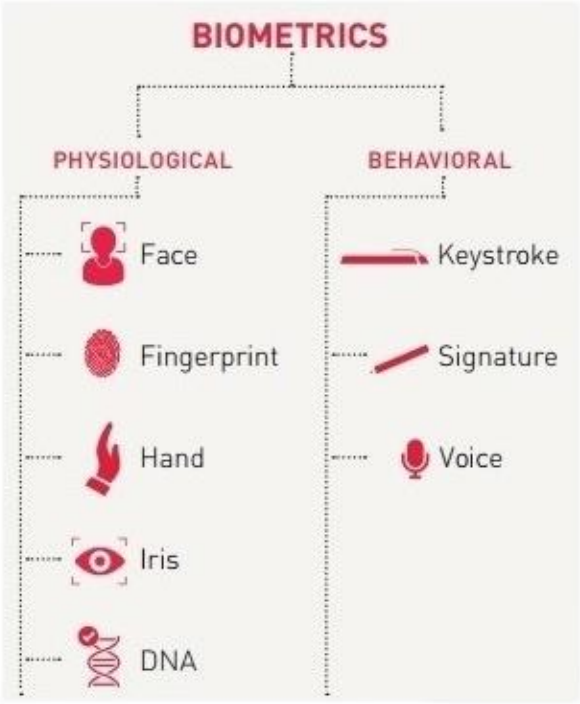
تقلید از رفتارهای دیگران دشوار است. با این حال ، این نوع سیستم احراز هویت مبتنی بر ضربه به کلید و پویایی لمسی در برابر حملات آماری آسیب پذیر است.

استراتژی های دفاعی معمول برای این حملات عبارتند از: سیستم بیومتریک چند حالته ، استفاده از تکنیک‌های رمزنگاری و ذخیره اطلاعات حساس در مکان امن مانند شخص ثالث مورد اعتماد. اما این روش ها نمی‌توانند از همه حملات محافظت کنند.

۲-۴ دسته‌بندی ویژگی‌های بیومتریکی مورد استفاده در سیستم‌های احراز هویت

ویژگی‌های بیومتریک مورد استفاده در سیستم‌های اهراز هویت را می‌توان به دو گروه کلی، ویژگی‌های ایستا و پویا دسته‌بندی کرد. ویژگی‌های ایستا، مشخصات فیزیکی کاربر هستند و معمولاً با گذشت زمان تغییر نمی‌کنند. نتایج نمونه برداری این ویژگی‌ها بیشتر بصورت تصویری می‌باشد. از جمله روش‌های استفاده از این ویژگی‌ها، تشخیص چهره، تشخیص عنبیه و تشخیص اثر انگشت را می‌توان نام برد.

ویژگی‌های پویا، عمدتاً در مورد مشخصات رفتاری کاربر است. آن‌ها معمولاً در حوزه زمان بررسی می‌شوند. استخراج ویژگی[۱۰] در پردازش داده‌های رفتاری جمع‌آوری شده، یک چالش اصلی احراز هویت بر مبنای این ویژگی‌ها است. از ویژگی‌های پویا، در روش‌های احراز هویت به کمک تشخیص صدا، سیگنال‌های الکتروکاردیوگرافی و تشخیص ضربه زدن به صفحه‌کلید و پویایی لمسی، استفاده می‌شود.



شکل شماره ۲- ۲: دسته‌بندی ویژگی‌های بیومتریکی و نمونه‌های آن‌ها

۲-۵ مبنای ارزیابی عملکرد یک سیستم احراز هویت بر مبنای سنجه‌های بیومتریکی

می‌توان ویژگی‌های ویژگی‌های مهم و قابل توجه‌ای که یک سیستم احراز هویت ایده‌آل باید داشته باشد، را دسته‌بندی و خلاصه کرد و نتیجه گرفت که برای ارزیابی یک سیستم احراز هویت بر مبنای سنجه‌های بیومتریکی باید عملکرد آن را از نظر دقت، کارایی، قابلیت استفاده، امنیت و حریم خصوصی در نظر گرفت. در ادامه راجع به هر یک از این موارد توضیحات بیشتری داده می‌شود.

[۱۰] Feature extraction

۱- دقت

این مورد را می‌توان با سه کمیت نرخ پذیرش نادرست[۱۱]، نرخ عدم پذیرش نادرست[۱۲]، نرخ خطای برابر[۱۳] و دقت احراز هویت، اندازه‌گیری کرد.

نرخ پذیرش نادرست به صورت احتمال شناسایی یک متقلب به عنوان یک کاربر قانونی و نرخ عدم پذیرش نادرست به صورت احتمال شناسایی یک کاربر قانونی به عنوان یک متقلب تعریف می‌شوند. نرخ خطای برابر، به نرخ زمانی که نسبت پذیرش نادرست برابر با نسبت مردود نادرست باشد، دارد و هر چه این مقدار کمتر باشد، دقت سیستم بیومتریکی بالاتر است. دقت احراز هویت، احتمال شناسایی صحیح یک فرد را نشان می‌دهد. این مقدار با نرخ خطای برابر مرتبط است و مجموع این دو مقدار ۱۰۰٪ می‌شود.

۲- کارایی

زمان مورد نیاز برای سیستم برای انجام یک احراز هویت را نشان می‌دهد. معمولا شامل زمان صرف شده برای جمع آوری داده‌ها، پردازش داده‌ها، استخراج ویژگی‌ها و همچنین تصمیم گیری در مورد احراز هویت می‌شود.

۳- قابلیت استفاده

این قابلیت ویژگی‌های جهانی بودن، منحصر به فرد بودن، ماندگاری، مقبولیت و نیاز به تجهیزات اضافی را در بر می‌گیرد. جهانی بودن به این معنا که هر شخصی باید دارای آن ویژگی بیومتریک خاص باشد. منحصر به فرد بودن به این معنا که ویژگی خاص بیولوژیکی هر دو نفر متفاوت باشد. ماندگاری به این معنی است که، ویژگی بیومتریک با گذشت زمان تغییر نکند. مقبولیت به منظور آن که، کاربران باید سیستم احراز هویت بیومتریک و روش جمع‌آوری داده‌های بیومتریکی طراحی شده، را قبول کنند. نیاز به تجهیزات اضافی، به این منظور که، آیا برای جمع‌آوری سیگنال‌های بیومتریک به تجهیزات اضافی خاصی نیاز است یا خیر.

۴- امنیت

همانطور که ذکر شد، سیستم‌های احراز هویت بیومتریک در برابر حملات مختلفی آسیب‌پذیر هستند. بنابراین، سیستم باید توانایی خاصی در مقاومت در برابر حملات مختلف مهاجمان داشته باشد.

[۱۱] False Acceptance Rate
[۱۲] False Rejection Rate
[۱۳] Equal Error Rate

۵- حریم خصوصی

وقتی سیستم مورد حملات قرار می گیرد ، اغلب با نشت اطلاعات بیولوژیکی کاربر همراه است که این نیز نوعی افشای حریم خصوصی است. این ویژگی را می‌توان بر مبنای میزان موفقیت مأموریت، غیرقابل برگشت بودن، قابلیت تجدیدپذیری و غیرقابل ارتباط بودن، ارزیابی کرد. میزان موفقیت ماموریت، نشان دهنده‌ی احتمال مقاومت موفقیت‌آمیز در برابر حملات و محافظت از حریم خصوصی داده‌های بیومتریکی است. غیرقابل برگشت بودن یعنی به منظور محافظت از داده‌های خصوصی، برخی از الگوریتم‌ها ممکن است در اطلاعات بیومتریک تغییر شکل دهند. این تغییرات باید برگشت‌ناپذیر باشد، بنابراین ما می‌توانیم اطمینان حاصل کنیم که هنگام حمله به یک پایگاه داده ذخیره بیومتریک، مهاجمان نمی‌توانند اطلاعات بیومتریک خصوصی کاربر واقعی را از طریق داده‌های ذخیره شده در پایگاه داده بازیابی کنند. قابلیت تجدیدپذیری یعنی زمانی که اطلاعات بیومتریک مورد استفاده در حال حاضر به سرقت می‌روند، کاربر باید بتواند اطلاعات احراز هویت قبلاً بارگذاری شده را برداشت کرده و با استفاده از اطلاعات بیولوژیکی جدید یا تغییر یافته دوباره ثبت‌نام کرده و حساب خود را تأیید کند.

خوب است که اطلاعات بیولوژیکی واقعی کاربر رابطی به دنیای خارج نداشته باشند. همچنین اگر سیستمی فقط از اطلاعات تغییریافته یا غیرمستقیم برای احراز هویت استفاده کند، دارای ویژگی غیرقابل ارتباط بودن داده‌هاست. در این حالت از آنجا که اطلاعات واقعی به شبکه‌های رایانه‌ای متصل نیستند، احتمال هک شدن توسط حملات متناظر از شبکه بسیار کاهش می‌یابد.

۲-۶ جمع‌بندی

همان‌طور که در این فصل توضیح داده‌شد، سیستم‌های احراز هویت بر مبنای سنجه‌های بیومتریکی، در برابر حملات مختلفی آسیب‌پذیر هستند. در روش‌هایی چون تشخیص چهره، تشخیص اثر انگشت و تشخیص صدا احتمال کلاهبرداری و جعل تصویر چهره، ساخت اثر انگشت جعلی و ضبط صدای فرد، زیاد است و این سیستم‌ها در کنار نقاط قوت خود، دارای نقاط ضعف زیادی هستند. در فصل‌های بعد، راه‌حل‌های پژوهشگران برای بهبود سیستم‌های احراز هویت به کمک ویژگی‌های ایستا و پویا، معرفی می‌شوند و بر اساس مبناهایی که برای بررسی عملکرد در این فصل توضیح داده شد، مورد مقایسه و بررسی قرار می‌گیرند.

فصل سوم

بررسی روش‌های بهبود پیشنهادی برای استفاده از ویژگی‌های ایستا

در این فصل روش‌های بهبود پیشنهادی برای بهبود احراز هویت بر مبنای تصویر چهره و تشخیص زنده بودن و همچنین روش‌های بهبود الگوریتم‌های تشخیص اثر انگشت و تشخیص زنده بودن در آن را معرفی کرده و به طور کلی ارزیابی می‌کنیم.

۳-۱ روش‌های بهبود تشخیص چهره و زنده بودن

ما انسان‌ها معمولا افراد را با مشاهده و مقایسه‌ی چهره از یکدیگر تمییز می‌دهیم و این روش تشخیص در سیستم‌های کامپیوتری نیز بسیار رایج است. با این حال تفاوت کمی بین چهره‌ی افراد مختلف وجود دارد و ساختارهای تمام چهره‌ها مشابه است، حتی شکل اندام‌های صورت نیز مشابه است. همچنین فرم صورت بسیار ناپایدار است و عواملی چون سن، زاویه مشاهده و روشنایی نیز بر تشخیص افراد برمبنای چهره تاثیر می‌گذارد. به طور کلی می‌توان نتیجه گرفت که این روش بسیار جهان‌شمول است اما از نظر ماندگاری و منحصر به فرد بودن مطلوب نیست.

۳-۱-۱ مدل توزیع نقطه‌ای[۱۴]

این مدل برای شناسایی تشخیص چهره‌ی دو بعدی با تمرکز بر تغییر ژست در چهره، پیشنهاد شده‌است[۲]. در این مدل از بردارهای ویژه و پارامترهای ژست برای سنتز تصاویر تصحیح شده ژست براساس تاب خوردگی مبتنی بر خطوط نازک استفاده شده‌است.

این مدل از مدل‌های سه بعدی پیشنهادی نظیر خود، در زاویه‌های چرخشی ۴۵ تا ۴۵- عملکرد بهتری داشته است و استفاده از آن برای کاربران راحت‌تر است چون می‌توانند در با هر ژستی عکس خود را به سیستم بدهند و باعث افزایش مقبولیت توسط کاربران می‌شود. دقت تشخیص چهره‌ی این مدل تنها در حدود ۳۰ درصد است، همچنین مهاجمان هر عکسی با هر ژستی که از کاربر داشته باشند، می‌توانند به اطلاعات کاربر نفوذ کنند. از آنجا که راه‌حلی برای این مشکل در نظر گرفته نشده است، احتمال آن که سیستم در معرض حملات تکرار قرار گیرد بسیار افزایش میابد. بنابراین، این مدل دقت و امنیت پایینی دارد و از لحاظ قابلیت استفاده، سطح متوسطی دارد.

[۱۴] Point distribution model

۳-۱-۲ اندازه‌گیری میزان نفوذ سطح[۱۵]

یک چارچوب اتوماتیک مبتنی بر روش Simulated Annealing-based و اندازه‌گیری میزان نفوذ سطح برای انجام تشخیص چهره سه بعدی است و با ترکیب چهار ناحیه‌ی مختلف چهره نتیجه‌ی احراز هویت را مشخص می‌کند[۳]. همچنین الگوریتمی اصلاح شده، برای کنترل بهتر حالات چهره پیشنهاد شده‌است.

این روش در زمان ارائه‌ی خود، بالاترین دقت را روی داده‌های پایگاه داده‌ی FRGC v2 داشته است و توانسته دقت تصدیق[۱۶] نود و شش درصد و نرخ پذیرش اشتباه ۰.۱ درصد را ثبت کند. همچنین دارای سرعت پردازش مطلوبی است. از دیگر فواید آن اسکن سه بعدی چهره است و در این حالت مهاجمان به راحتی قادر به حمله به سیستم نخواهند بود و سیستم تا حدی توانایی تشخیص زنده بودن دارد. باید توجه داشت که ممکن است، قابلیت اسکن سه بعدی بر دستگاه‌های تلفن همراه یا سیستم‌های کامپیوتر کاربران موجود نباشد. همچنین داده‌های با ابعاد بالا به دست آمده، حاوی اطلاعات زیادی از چهره کاربر هستند و ممکن است منجر به افشای حریم خصوصی شود. بنابراین این روش، دقت، کارایی و قابلیت استفاده در سطح معمول را دارد و دارای امنیت بالایی است.

۳-۱-۳ مدل مورد استفاده‌ی شرکت اپل

در سال ۲۰۱۷ شرکت اپل استفاده از تشخیص چهره برای احراز هویت را در دستگاه‌های خود، آغاز کرد و مدلی به نام iProov پیشنهاد داد. این مدل از الگوریتم‌های یادگیری ماشین برای بهبود مستمر دقتش استفاده می‌کند. در این مدل از الگوریتم‌های تشخیص زنده بودن نیز استفاده شده است.

این مدل معمولا زمان نسبتا کمی برای احراز هویت صرف می‌کند و در بین کاربران بسیار قابل قبول است. این قابلیت که سیستم تنها زمانی عملیات احراز هویت را نجام می‌دهد که کاربر به لنز دستگاه نگاه کند، باعث افزایش امنیت سیستم شده‌است. به طور کلی این مدل، دقت و قابلیت استفاده در سطح معمول را دارد و کارایی و امنیت بالایی دارد اما از لحاظ حریم خصوصی کاربران، عملکرد ضعیفی دارد.

۳-۲ بهبود تشخیص اثر انگشت

سیستم‌های احراز هویت مبتنی بر اثر انگشت، در طیف وسیعی از صنایع پذیرفته شده‌اند. اثر انگشت به عنوان یک ویژگی بیولوژیکی دارای حد خوبی از تفاوت بین کاربران و ثبات در طی زمان است و به جز برای عده معدودی که دارای ناتوانی‌هایی باشند، دارای خاصیت جهانی بودن است. همچنین به دلیل سادگی در استفاده، بین کاربران

[۱۵] Surface Interpenetration Measure

[۱۶] Verification accuracy

مقبولیت بسیار بالایی دارد. امروزه حسگرهای اثر انگشت به طور گسترده‌ای توسعه یافته‌اند و هزینه‌ی بالایی ندارند. این ویژگی سبب شده است، این حسگرها در اکثر تلفن‌های هوشمند مورد استفاده قرار گیرند.

سیستم‌ها و روش‌های مختلفی با دقت تشخیص بسیار بالا برای تشخیص اثر انگشت تا کنون پیشنهاد شده‌اند اما امنیت و حریم خصوصی در آن‌ها در نظر گرفته نشده است. مهاجمان می‌توانند اثر انگشت جعلی ایجاد کرده و سیستم‌های احراز هویت را دور بزنند. علاوه بر این، اطلاعات جمع‌آوری شده و ذخیره شده در سیستم با خطر نشت مواجه است. این سیستم‌ها هیچ گونه محافظت اساسی در مورد اطلاعات خصوصی حساس ندارند. بنابراین، این سیستم‌ها دارای دقت بالا، کارایی بالا و قابلیت استفاده در سطح بالا هستند، اما اطمینان از امنیت و حریم خصوصی ندارند.

به منظور اطمینان از امنیت و حفظ حریم خصوصی کاربر در سیستم‌های احراز هویت میتنی بر اثر انگشت، استفاده از روش‌های تشخیص زنده بودن پیشنهاد شده است.

۳-۲-۱ استفاده از ویژگی‌های بیومتریکی رگ انگشت

جاداو و نرکار (۲۰۱۵) استدلال کرده‌اند که یک سیستم احراز هویت بیومتریک مبتنی بر رگ انگشت از سایر سیستم های بیومتریک بهتر است زیرا نرخ جعل کمتری دارد[٤]. آن‌ها الگوریتمی برای پردازش تصویر رگ معرفی کرده‌اند و برای تطبیق الگو، از یک مدار مجتمع دیجیتال برنامه‌پذیر استفاده کردند. نتایج آزمایش نشان داد که دقت این روش پیشنهادی با می‌تواند به ۹۷ درصد برسد.

روند احراز هویت این روش حدود ۲ ثانیه هزینه دارد. بنابراین، این روش به سطح متوسطی از دقت، کارایی و قابلیت استفاده می‌رسد و امنیت آن بالا است.

۳-۲-۲ استفاده از طیف مادون قرمز با طول موج کوتاه[۱۷]

این روش مبتنی بر بیومتریک دست برمبنای طیف مادون قرمز با طول موج کوتاه (SWIR) را ارائه شده است. در این سیستم، دوربین متداول مورد استفاده در سیستم احراز هویت مبتنی بر دست، با یک دوربین SWIR همراه با یک طیف‌سنج نوری جایگزین شده است. آزمایش‌های آن‌ها نشان داد که خواص طیفی بافت دست انسان برای ایجاد تبعیض در بین کاربران زیادی موثر است و عملکرد بهتری نسبت به سایر ویژگی های دست دارد. طی آزمونی که در آن ۱۵۴ سوژه مورد آزمایش قرار گرفتند، این روش خطای برابر ۳.۲۲ درصد داشته است[٥].

[۱۷] Short Wavelength Infrared (SWIR)

۳-۳ جمع‌بندی

در این فصل تعدادی از روش‌های پیشنهادی برای بهبود تشخیص چهره و تشخیص اثر انگشت شد. به طور خلاصه می‌توان گفت، برای بهبود عملکرد سیستم‌های مبتنی بر تشخیص چهره، الگوریتم‌های متخلف و پیشرفته‌ای برای تشخیص چهره پیشنهاد شد که هر یک خصوصیات خاصی از چهره را استخراج و پردازش می‌کنند و برای بهبود عملکرد سیستم‌های مبتنی بر تشخیص اثر انگشت، روش‌هایی برای تشخیص زنده بودن ارائه شده است. برخی از روش‌های تشخیص زنده بودن، حتی می‌توانند برای احراز هویت بر مبنای تشخیص چهره و تشخیص عنبیه نیز استفاده شوند، اما مشکل این سیستم‌ها این است که آن‌ها به داده‌های اضافی مانند طیف، بو، تصاویر حرارتی و غیره احتیاج دارند که به طور معمول به سخت افزار اضافی (به عنوان مثال سنسورها) نیازمند اند. در فصل بعد به معرفی تعدادی از روش‌های بهبود تشخیص صدا و تشخیص ضربه پرداخته می‌شود.

فصل چهارم

بررسی روش‌های بهبود پیشنهادی برای استفاده از ویژگی‌های پویا

ویژگی های پویا عمدتا در مورد ویژگی‌های رفتاری کاربر است. آن‌ها معمولاً پیوستگی را در حوزه زمان نشان می‌دهند. استخراج ویژگی[۱۸] یک مرحله مهم در پردازش داده‌های رفتاری جمع‌آوری شده برای احراز هویت است. در این فصل روش‌های بهبود پیشنهادی برای بهبود احراز هویت بر مبنای صدا و تشخیص ضربه و پویایی لمسی را معرفی کرده و به طور کلی ارزیابی می‌کنیم.

۴-۱ بهبود تشخیص صدا

به عنوان نوعی ویژگی بیولوژیکی که معمولاً در اختیار انسان هاست (به استثنای تعداد معدودی از افراد دارای معلولیت صدا)، صدا دارای اختلافات بین کاربر و ثبات فردی کافی است. علاوه بر این، میکروفون مورد نیاز برای جمع‌آوری داده‌های صوتی تقریباً در همه دستگاه‌های تلفن همراه موجود است. می‌توان نتیجه گرفت، جهان شمول بودن، منحصر به فرد بودن، مقبولیت در این روش بسیار بالاست و نیازی به تجهیزات اضافی ندارد پس قابلیت استفاده این روش بسیار بالاست.

۴-۱-۱ استفاده از مدل مخفی مارکوف[۱۹]

پیش از این، HMM برای مدت طولانی در تشخیص گفتار استفاده می‌شده است، اما در این روش از HMM برای تأیید اعتبار صدا استفاده می‌شود. این روش مستقل از متن است و فقط به صدای گوینده متکی است و از HMM برای استخراج برخی از ویژگی‌های خاص از شکل موج صدا استفاده می‌شود. آزمون تجربی نشان داده است که دقت این روش زیاد نیست و حدود ۸۶ درصد است[۶].

کارایی[۲۰] این روش بررسی نشده است. اما در آزمایشی، از بین ۱۵۰ جعل کننده، تنها به دو مورد اجازه‌ی دسترسی داده شده است. بنابراین این روش می‌تواند تا حدی در برابر حمله مجدد[۲۱] مقاومت کند و در نتیجه از امنیت بالایی برخوردار است.

۴-۱-۲ مدل مخفی مارکوف- مدل مخلوط گاوسی[۲۲]

این مدل پیشنهادی، از روش مدل مخفی مارکوف- مدل مخلوط گاوسی (HMM-GMM) استفاده می‌کند و به خطای برابر ۳.۴ درصد دست می‌یابد. دقت این روش نزدیک به سطح بالایی است[۷].

[۱۸] Feature extraction
[۱۹] Hidden Markov Model (HMM)
[۲۰] Efficiency
[۲۱] Replay attack
[۲۲] Hidden Markov Model – Gaussian Mixture Model

۴-۲ بهبود تشخیص الگو ضربه و پویایی لمسی

محققان اشاره کرده اند که فشار انگشت اطلاعات متمایزکننده بیشتری نسبت به پویایی ضربه زدن به کلید می دهد. برای جمع‌آوری سیگنال‌های فشار باید یک سنسور فشار در صفحه وجود داشته باشد. تأیید اعتبار دینامیکی ضربه کلید معمولاً از یک طبقه‌بندی کننده[۲۳] با دو کلاس استفاده می‌کند. طبقه‌بندی توسط هر دو نمونه مثبت و منفی آموزش داده می‌شود. سپس یک فرد معتبر قابل تشخیص است. در سال‌های اخیر، از آنجا که تلفن‌های هوشمند دیگر از صفحه حساس به فشار استفاده نمی‌کنند، محققان شروع به تحقیق درباره پویایی لمسی کرده اند.

برخی محققان مسئله میزان بالای خطا در سیستم‌های احراز هویت بر اساس ویژگی‌های رفتاری را بررسی کردند. آن‌ها خاطرنشان کردند که اطلاعات زمانی مرتبط با وقوع خطاها ممکن است به حل این مشکل کمک کند و برای بررسی این موضوع از الگوریتم‌های یادگیری ماشین مانند، Nearest neighbor، Support vector machine و Random forest کمک گرفتند.

هنگامی که تلفن‌های هوشمند به تازگی تولید شدند، با ظهور صفحه‌های لمسی، چنین روش‌هایی مبتنی بر ضربه کلید و پویایی لمسی پدیدار شدند. با این حال، با تولید و استفاده از سنسورهای مختلف اثر انگشت، این نوع روش‌ها به سرعت با روش‌های تشخیص اثر انگشت جایگزین شدند، چرا که قابلیت استفاده از این روش‌ها بسیار پایین است.

۴-۳ جمع‌بندی

در این فصل، چند روش مختلف بهبود احراز هویت بر مبنای تشخیص صدا و پویایی لمسی و الگوریتم‌های پیشنهادی آن، معرفی و به طور کلی بررسی شد. در روش‌های تشخیص صدا همچنان خطر حمله از طریق ضبط صدای فرد و بخش دوباره‌ی آن برای ورود به سیستم وجود دارد، اما روش‌های پیشنهادی تا حد خوبی خطر جعل صدا را از بین می‌برند و صدای جعل شده را به خوبی تشخیص می‌دهند. روش‌های پویایی لمسی و الگوی ضربه اما، امروزه کارایی کمی دارند و مورد استفاده قرار نمی‌گیرند و روش‌های تشخیص اثر انگشت جایگزین آن‌ها شده‌اند. در فصل آینده به مقایسه‌ی دقیق‌تر روش‌های بهبود و سیستم‌های پیشنهادی می‌پردازیم.

[۲۳] Classifier

فصل پنجم

جمع‌بندی و نتیجه‌گیری و پیشنهادات

۵-۱ جمع‌بندی

تا کنون، سیستم‌های احراز هویت بر مبنای ویژگی‌های بیومتریکی، موارد استفاده، فواید و نقاط ضعف آن‌ها را بررسی کردیم. سپس، معیارهایی برای ارزیابی این سیستم‌ها ارائه دادیم و چند روش مختلف برای بهبود عملکرد این سیستم‌ها بیان کردیم. حال می‌خواهیم این روش‌ها را با توجه به معیارهای ارائه شده، با یکدیگر مقایسه و جمع‌بندی کنیم.

نتایج کیفی ارزیابی و مقایسه‌ی روش‌های معرفی شده از نظر دقت، کارایی، قابلیت استفاده، امنیت و حریم خصوصی، در جدول زیر آورده شده است.

جدول شماره ۵- ۱: مقایسه کیفی روش‌های پیشنهادی

ویژگی بیومتریک	روش	دقت	کارایی	قابلیت استفاده	امنیت	حریم خصوصی
چهره	مدل توزیع نقطه‌ای	کم	-	متوسط	کم	-
	اندازه‌گیری میزان نفوذ سطح	متوسط	متوسط	متوسط	زیاد	-
	iProov	زیاد	زیاد	متوسط	زیاد	کم
اثر انگشت	استفاده از ویژگی‌های بیومتریک رگ انگشت	متوسط	متوسط	زیاد	زیاد	-
	استفاده از طیف مادون قرمز	متوسط	-	متوسط	زیاد	-
صدا	HMM	کم	-	زیاد	زیاد	-
	HMM-GMM	متوسط	-	زیاد	زیاد	-
تسخیص ضربه و پویایی لمسی	استفاده از الگوریتم‌های یادگیری ماشین	متوسط	کم	متوسط	متوسط	-

می‌توان مشاهده کرد که عملکرد کلی سیستم‌های احراز هویت بر اساس ویژگی‌های ایستا نسبتاً بالا است. این روش‌ها نه تنها با یک دقت بالا، بلکه با صرف هزینه زمانی بسیار کم، به بازدهی بالایی نیز دست می‌یابند. سیستم‌های شناسایی و احراز هویت اثر انگشت تقریباً در همه‌ی ابعاد زندگی روزمره ما اعمال شده‌اند. در مقابل،

عملکرد کلی سیستم‌های احراز هویت بر اساس ویژگی‌های پویا، با توجه به دقت و صحت کم و نیاز به تجهیزات اضافی، نسبتاً پایین است.

باید اضافه کرد که بسیاری از روش‌های پیشنهادی برای بهبود احراز هویت، همچنان در زمینه‌های امنیت و حریم خصوصی، ضعف‌های زیادی دارند و اکثر پژوهش‌ها به این موارد توجهی نمی‌کنند.

با توجه به محبوبیت دستگاه‌های تلفن همراه، بیشتر سیستم‌های بیومتریک را می‌توان در این دستگاه‌ها پیاده‌سازی کرد. با این حال، از نظر سخت افزاری، قابلیت محاسباتی و توان الکتریکی، محدودیت‌های زیادی در تلفن همراه وجود دارد و باید به هزینه‌های مربوطه نیز توجه کنیم. همچنین، دستگاه‌های تلفن همراه بیشتر مورد حمله قرار می‌گیرند و امنیت سیستم احراز هویت بیومتریک باید به طور جدی مورد توجه قرار گیرد.

۵-۲ نتیجه‌گیری

در این گزارش، پیشرفت‌های اخیر در زمینه احراز هویت بیومتریک را مرور کردیم. همچنین، به حملات بالقوه و خطرات امنیتی در احراز هویت بیومتریک اشاره کردیم و مجموعه‌ای از معیارهای ارزیابی را برای ارزیابی عملکرد کارهای موجود، پیشنهاد دادیم. سپس، تعدادی از روش‌های بهبود سیستم‌های احراز هویت بیومتریک موجود در دو دسته‌ی ویژگی‌های پویا و ایستا مطرح کردیم و در نهایت یک ارزیابی مقایسه‌ای برای این روش‌ها بر مبنای معیارهای پیشنهادی ارائه دادیم. در نهایت دریافتیم که اکثر سیستم های موجود از مسائل امنیتی و حریم خصوصی رنج می‌برند. همچنین، دقت احراز هویت برخی از سیستم ها بر اساس ویژگی‌های بیومتریک پویا باید بیشتر بهبود یابد.

۵-۳ پیشنهادات

به منظور دست‌یابی به یک سیستم احراز هویت بر مبنای ویژگی‌های بیومتریکی ایده‌آل، پیشنهاد می‌شود پژوهش‌های این حوزه بر مواردی که در ادامه بیان می‌شوند، متمرکز شوند.

در حال حاضر، سیستم احراز هویت بیومتریک مبتنی بر ویژگی‌های ایستا، مانند touchID و faceID که به طور گسترده‌ای در حال استفاده هستند، نیاز به فراهم کردن ابزاری برای تشخیص زنده بودن دارند. عملکرد دستیابی به زنده بودن باید به خوبی مورد مطالعه قرار گیرد تا به هزینه کم سیستم و بازده بالا دست یابد. همچنین، تقریباً همه سیستم‌های بیومتریک از حریم خصوصی کاربران بی‌بهره هستند. چگونگی محافظت از اطلاعات بیومتریک خصوصی کاربر، یک موضوع مهم تحقیقاتی قابل مطالعه است، به ویژه وقتی الگوهای بیومتریک کاربر در شخص ثالث ذخیره شده باشد که به طور کامل قابل اعتماد نیست.

طراحی رابط کاربری، طراحی تعامل کاربر و روش جمع‌آوری داده‌ها و در مجموع چگونگی طراحی سیستم احراز هویت بیومتریک قابل استفاده، موضوع مهمی است و بر مقبولیت و کارایی آن تاثیر زیادی می‌گذارد. همچنین، به منظور کارکرد سیستم به روشی کارآمد و دقیق برای رد و پذیرش کاربران، ایجاد الگوریتم مناسب پردازش داده‌های بیومتریک نقشی اساسی دارد. الگوریتم‌های پیشرفته باید بیشتر مورد تحقیق قرار گیرند تا همزمان از کارآیی، صحت، قابلیت استفاده و امنیت و حریم خصوصی پشتیبانی کنند.

منابع و مراجع

[۱] Rui, Z. and Yan, Z., *2018*. A survey on biometric authentication: Toward secure and privacy-preserving identification. *IEEE Access*, *7*, pp.*5994-6009*.

[۲] González-Jiménez, D. and Alba-Castro, J.L., *2007*. Toward pose-invariant *2*-d face recognition through point distribution models and facial symmetry. *IEEE Transactions on Information Forensics and Security*, *2*(*3*), pp.*413-429*.

[۳] Queirolo, C.C., Silva, L., Bellon, O.R. and Segundo, M.P., *2009*. *3*D face recognition using simulated annealing and the surface interpenetration measure. *IEEE transactions on pattern analysis and machine intelligence*, *32*(*2*), pp.*206-219*.

[٤] Jadhav, M. and Nerkar, P.M., *2015*, December. Implementation of an embedded hardware of FVRS on FPGA. In *2015 International Conference on Information Processing (ICIP)* (pp. *48-53*). IEEE.

[٥] Ferrer, M.A., Morales, A. and Díaz, A., *2014*. An approach to SWIR hyperspectral hand biometrics. *Information Sciences*, *268*, pp.*3-19*.

[٦] Jayamaha, R.M.M., Senadheera, M.R., Gamage, T.N.C., Weerasekara, K.P.B., Dissanayaka, G.A. and Kodagoda, G.N., *2008*, December. Voizlock-human voice authentication system using hidden markov model. In *2008 4th International Conference on Information and Automation for Sustainability* (pp. *330-۳35*). IEEE.

[۷] Gałka, J., Masior, M. and Salasa, M., *2014*. Voice authentication embedded solution for secured access control. *IEEE Transactions on Consumer Electronics*, *60*(*4*), pp.*653-661*.