دانشگاه صنعتی امیرکبیر
(پلی تکنیک تهران)
دانشکده مهندسی کامپیوتر

گزارش درس روش پژوهش و ارائه

احراز هویت الکترونیک بر مبنای سنجه‌های بیومتریکی

نگارش
پریا مهربد

استاد راهنما
دکتر رضا صفابخش

آبان ۹۹

سپاس گزاری

بی‌تردید تهیه‌ی این گزارش بدون راهنمایی‌های ارزشمند استاد بزرگوار **جناب آقای دکتر رضا صفابخش** میسر نمی‌شد. پس بر خود واجب می دانم از راهنمایی‌های ایشان صمیمانه سپاس گذاری کنم.

پریا مهربد

آبان ۹۹

چکیده

کاربرد گسترده‌ی احراز هویت در زندگی روزمره‌ی ما به سرعت در حال گسترش است. با پیشرفت فناوری، کاهش هزینه‌ی این سیستم‌ها و افزایش تمایل عموم به سمت انجام کارها به شکل غیرحضوری، سیستم‌های احراز هویت بیش از پیش به کار گرفته می‌شوند؛ اما، چالش‌هایی از قبیل انتخاب سنجه‌ی بیومتریک، دقت ناکافی و حفظ امنیت پایگاه داده و زیرساخت‌ها در این راه قرار دارند.

هدف این بررسی، شناسایی انواع سنجه‌های بیومتریک و مزایا و معایب آن‌ها، راهکارهای بهبود دقت سیستم‌های احراز هویت، راهکارهای جلوگیری از حملات، راهکارهای افزایش امنیت سیستم و الگوهای دیجیتال است.

کلید واژه: احراز هویت بیومتریک، اثر انگشت، تشخیص چهره، الگوی دیجیتال

فهرست مطالب

عنوان **صفحه**

فهرست اشکال

عنوان **صفحه**

فهرست جداول

عنوان **صفحه**

فصل اول

مقدمه

۱ – مقدمه

پیشـرفت‌ها در زمینه‌ی فناوری اطلاعات، موجب شـده تا برای اسـتفاده از برخی خدمات تمایل عمومی به بهره‌گیری از آنها به صورت غیرحضوری وجود داشته باشد که این امر مستلزم احراز هویت الکترونیکی است. گرچه احراز هویت الکترونیکی روند سندیت را سرعت می‌بخشد ولی چالش‌هایی از قبیل لزوم تامین زیرساخت‌ها و پایگاه داده‌های گسترده، تامین امنیت این روند و محدودیت کارایی را پیش رو دارد.

در میان روش‌های احراز هویت الکترونیکی روش احراز هویت بر مبنای سـنجه‌های بیومتریکی این امکان را می‌دهد که به جای آنکه « آنچه که می‌دانیم » یا « آنچه که داریم » را ارائه کنیم « آنچه که هسـتیم » را ارائه کنیم و این ویژگیسـت که این روش را از بقیه‌ی روش‌ها متمایز می‌کند. روش‌های سـنتی احراز هویت مانند اسـتفاده از رمز عبور یا مدارک شناسایی مشکلاتی مثل سرقت هویت را نمی‌توانند شکست دهند؛ این فرم از نمایش هویت یک فرد به سادگی می‌تواند فراموش شود، دزدیده شود، به اشتراک گذاشته شود، یا حتی حدس زده شود. اما در مورد احراز هویت بر مبنای سـنجه های بیومتریکی می‌توان گفت که چون این سـنجه‌ها به صـورت فیزیکی به کاربر متصـلند در معرض خطرهای اشـاره شـده درمورد روش‌های سـنتی قرار نمی‌گیرند در نتیجه این روش طبیعی‌تر و مطمئن‌تر اسـت. بعلاوه، این روش مزیت‌های منحصـر به فردی از جمله توانایی تشـخیص یک فرد با چند مدرک شـناسـایی(مثلا چند گذرنامه) را دارد. در این گزارش به بررسـی انواع سـنجه‌های بیومتریکی، چالش‌های احراز هویت بر مبنای این سنجه‌ها و راه‌حل‌های پیشنهادی برای حل این چالش‌ها می‌پردازیم.

فصل دوم

سنجه‌های بیومتریکی

۲ – سنجه‌های بیومتریکی

هرگونه اطلاعات بیومتریکی که به کمک آن بتوان افراد را از هم متمایز کرد یک سنجه‌ی بیومتریکی است. یک سنجه‌ی ایده‌آل آن است که تمام ویژگی‌های زیر را داشته باشد:

- جامعیت: بتوان همه‌ی افراد را از طریق این اطلاعات توصیف کرد.
- منحصر به فرد بودن: تا حد امکان بین هر دو فرد متفاوت باشد.
- ماندگاری: در طی طول زندگی یک فرد ثابت باشد.
- قابلیت جمع آوری: بتوان این ویژگی را به آسانی سنجید(اندازه گیری کرد).
- مقبولیت: کاربران در عمل از آن استفاده کنند(مربوط به اطمینان،راحتی استفاده، هزینه و ...).

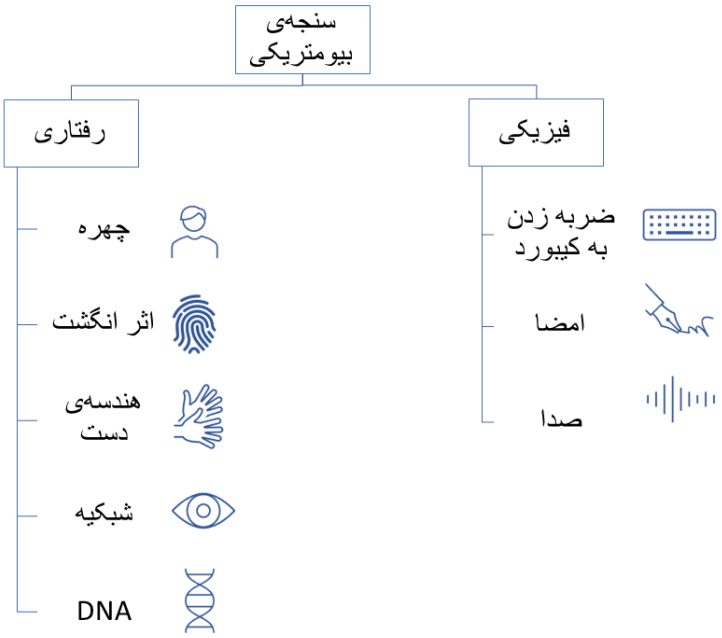
در بین ویژگی‌های بیومتریکی که برای احراز هویت استفاده می‌شود این معیارها در برخی قوی‌تر و در برخی ضعیف‌تر هستند ولی همانطور در بخش کاربردهای سنجه‌های بیومتریکی به آن اشاره می‌کنیم، این سنجه‌ها بسته به کاربرد نسبت به یکدیگر برتری می‌یابند. در جدول ۱ مقایسه‌ی کیفی سنجه‌های معروف در این معیارها آمده است[4].

ویژگی	جامعیت	منحصر به فردی	ماندگاری	قابلیت جمع‌آوری	مقبولیت
چهره	✓	X	ضعیف	✓	✓
اثر انگشت	✓	✓	✓	✓	✓
هندسه‌ی دست	✓	X	✓	✓	✓
عنبیه	✓	✓	✓	✓	ضعیف
DNA	✓	✓	✓	ضعیف	ضعیف
ضربه زدن به کیبورد	✓	✓	ضعیف	✓	✓
صدا	✓	✓	ضعیف	✓	✓

جدول ۱ – مقایسه‌ی کیفی سنجه‌های بیومتریکی بر اساس معیارهای جامعیت، منحصر به فردی، ماندگاری، مقبولیت

۲-۱- انواع سنجه‌های بیومتریکی

به طور کلی می‌توان سنجه‌های بیومتریکی را به دو دسته‌ی اصلی (فیزیکی و رفتاری) تقسیم کرد(شکل ۱). با توجه به جدول ۱ می‌توان نتیجه گرفت که سنجه‌های رفتاری مقبولیت دارند ولی از ماندگاری ضعیفی برخوردارند. در ادامه برخی از این ویژگی‌ها را به اختصار بررسی می‌کنیم ولی دو ویژگی اثر انگشت و چهره را به تفصیل بررسی می کنیم[3].



شکل ۱- دسته بندی سنجه‌های بیومتریک به دو دسته‌ی فیزیکی و رفتاری و نمونه‌های آن.

۲-۱-۱- عنبیه

در این روش تصویر عنبیه‌ی فرد توسط اسکنر تهیه می‌شود و تصویر آن بر اساس تکنیک‌های محاسباتی تشخیص الگو(pattern recognition) بدست می‌آید، سپس از این تصویر الگو دیجیتال (template) ساخته شده و در پایگاه‌داده ذخیره می‌شود. دقت سیستم‌های تشخیص عنبیه ۹۰ تا ۹۹ درصد است و حتی لنزهای چشمی مانعی برای اسکنر نیست و تاثیری در نتیجه نمی‌گذارد، ولی این روش با چالش‌هایی نیز روبه‌رو است؛ هرگونه بازتاب نور می‌تواند روی اسکنر و نتیجه تاثیر بگذارد، قیمت دستگاه‌های این سیستم بسیار بالاست و به علت

تغییر اندازه‌ی مردمک چشم در نورهای متفاوت، شکل عنبیه نیز تغییر می‌کند و این امر در کاهش دقت تشخیص دخیل است[3].

۲-۱-۲- شبکیه

شبکیه‌ی چشم یکی دیگر از سنجه‌های منحصر به فرد و تغییر ناپذیر است و به همین دلیل، این سنجه قابل اطمینان و دقیق است. در اسکنر های retina رگ‌های خونی شبکیه اسکن می‌شوند، نور مادون قرمز با حداقل انرژی بر روی چشم فرد تابیده می شود (زیرا عروق خونی در شبکیه چشم می توانند آنها را جذب کنند) و تصویر شبکیه گرفته می شود. عروق خونی شبکیه در این تصاویر بسیار کلیدی هستند و این تصویر آنقدر پیچیده است که حتی در بین دوقلوها مشترک نیست.

مشکل اصلی در مقبولیات این سیستم‌ها از آن جهت است که سیستم، تا زمانی که تصویر با کیفیت ثبت نشده باشد، به کاربر اجازه ورود نمی‌دهد. به همین دلیل ، شرایطی پیش می آید که کاربر برای تأیید نیاز به تلاش سه تا چهار بار دارد. به علت بیماری‌های چشمی مثل آب‌مروارید ممکن است این روش نتواند به درستی احراز هویت کند ولی در اکثر موارد دقت بالایی در تشخیص دارد و به همین دلیل در کاربردهای نظامی سطح بالا یا سازمان‌های دولتی استفاده می‌شود[3].

۲-۱-۳- ضربه زدن به کیبورد

این سنجه‌ی بیومتریکی زیرمجموعه‌ی سنجه‌های رفتاریست. منحصر به فرد بودن این سنجه، معلول ویژگی‌های رفتاری افراد در طریقه‌ی تایپ کردن آنهاست؛ برای مثال، افراد راست دست برای دسترسی به کلیدهای سمت راست کیبورد راحت‌ترند یا بعضی زمان بیشتری برای پیدا کردن بعضی از حروف صرف می‌کنند یا به جای فشردن یک کلید همیشه به اشتباه کلید دیگری را میفشارند؛ موارد ذکر شده بعلاوه‌ی ویژگی‌های دیگر مانند سرعت تایپ کردن یا زمان فشردن و رها کردن کلید و ... لحاظ شده و طبق این ویژگی‌ها الگوی دیجیتال ساخته می‌شود.البته وقتی که این سنجه زمانی که با روش‌های دیگر مثل رمز یا PIN ترکیب می‌شود موثرتر است[3].

۲-۱-۴- هندسه ی دست

استفاده ازهندسه‌ی دست، یکی از قدیمی ترین روش‌های احراز هویت بیومتریکی است اما همیشه منحصر به فرد نیست. در سال ۱۹۹۶ ، بازی های المپیک از تشخیص هندسه دست برای محافظت از دسترسی به دهکده المپیک استفاده کردند. برای تهیه‌ی اطلاعات از هندسه‌ی دست ۳ تصویر (تصویر از کف دست، نمای بالا و پهلو) با استفاده از یک آینه زاویه دار گرفته می شوند.در ادامه‌ی این فرآیند ، تجزیه و تحلیل تقریباً ۳۱۰۰۰ نقطه دست با اندازه گیری ۹۰ مورد از جمله فاصله بندها، طول و ضخامت انگشتان و بسیاری موارد دیگر انجام می شود[3] .

۲-۲- کاربرد احراز هویت بیومتریکی

به علت ویژگی‌های خاص سنجه‌های بیومتریکی ، احراز هویت بر مبنای این سنجه‌ها روز به روز بیشتر استفاده می‌شود و جای روش‌های سنتی را می گیرد تا جایی که در بسیاری از سیستم‌های شهری و نظامی استفاده می‌شوند و کاربرد آنها از این هم فراتر می‌رود و در حوزه های اجرای قانون ، کنترل مرز و خدمات مالی استفاده می‌شود. لزوم بررسی کاربردهای سیستم‌های احراز هویت از آن جهت است که بهبود عملکرد این سیستم ها در کاربردهای متفاوت معنای یکسان ندارد. در بعضی از کاربردها، امنیت مقدم بر راحتی استفاده است و در نتیجه برای این کاربردها اقدامات امنیتی بیشتری پیشنهاد می‌شود که ممکن است تجربه‌ی کاربری را سخت کند یا زمان پاسخ سیستم را طولانی کند. از طرفی، این سطح از امنیت برای تمام کاربردها توصیه نمی‌شود چون کاربران را ناراضی می کند پس در این کاربردها افزایش امنیت لزوما منتهی به بهبود عملکرد سیستم نمی‌شود. در ادامه به برخی از کاربردهای اصلی این روش احراز هویت می‌پردازیم[5].

۲-۲-۱- اجرای قانون

سیستم‌های احراز هویت بر مبنای سنجه‌های بیومتریکی با پیشرفت تکنولوژی در زمینه‌ی اجرای قانون با استقبال زیادی روبه‌رو شده‌اند. البته احراز هویت بیومتریکی یک روش قدیمی برای احراز هویت در زمینه‌ی اجرای قانون است و حتی تشخیص اثر انگشت حدود یک قرن است که مورد استفاده قرار می گیرد.

۲-۲-۲- کالاهای مصرفی

با پیشرفت تکنولوژی، سیستم‌های احراز هویت بیومتریکی ارزان‌تر و در دسترس‌تر شدند. در نتیجه این سیستم‌ها از کاربردهای نظامی و دولتی و ... به کالاهای مصرفی روزانه راه یافتند. قفل در و گاوصندوق، سیستم‌های نظارتی، اتومبیل و از همه مهم‌تر دستگاه های موبایل از موارد این کالاهای مصرفی هستند. با محبوب شدن تلفن‌های هوشمند ترکیب این دستگاه ها با احراز هویت بیومتریکی یک ترکیب برنده در بازار بوده و باعث شده عموم این احراز هویت را در گوشه و کنار زندگی خود بپذیرند.

۲-۲-۳- خدمات مالی

حفاظت از اموال برای مردم از اولویت‌هاست، به همین علت است که خدمات مالی بالغ‌ترین بازار احراز هویت بیومتریکی را بعد از خدمات اجرای قوانین دارد. شرکت‌های مالی نیز با این روند خود را سازگار می‌کنند؛ برای مثال یک شرکت کارت اعتباری‌ای به بازار عرضه کرده که درون خود یک سیستم خواندن اثر انگشت به صورت نهفته (embedded) تعبیه کرده و سعی بر آن دارد که به کارت‌های اعتباری یک لایه‌ی احراز هویت بیومتریکی اضافه کند و دو فاکتور مهم راحتی و امنیت را بالا ببرد.

نتیجه گیری

احراز هویت بیومتریک در حدود یک قرن است که در استخدام بشر درآمده و وی را در کاربردهای مختلف یاری می‌کند. در گذشته، به علت هزینه‌ی بالا در قبال دقت پایین، کاربرد احراز هویت بیومتریک در زمینه‌ی اجرای قوانین پررنگ‌تر بوده ولی با پیشرفت فناوری این سیستم‌ها و بهتر شدن عملکرد و دقت آن‌ها، در مراکز مالی و درنهایت با ارزان شدن فناوری در کاربردهای خانگی و روزمره راه یافتند. در سیستم‌های احراز هویت بیومتریکی انتخاب سنجه‌ی مورد بررسی بر مبنای کاربرد سیستم و معیارهایی از قبیل مقبولیت، قابلیت جمع‌آوری و ... انجام می‌شود. با بررسی سنجه‌ها و مقایسه‌ی آن‌ها می‌توان نتیجه گرفت که سنجه‌های فیزیکی از آن لحاظ که در طول زندگی فرد ثابت هستند، بر سنجه‌های رفتاری برتری دارند. در میان سنجه‌های فیزیکی نیز، مقبولیت (احتمال استفاده‌ی واقعی کاربران) و راحتی استفاده و هزینه‌ی دستگاه در بین روش‌ها تمایز ایجاد می‌کند. به طور کلی می‌توان گفت که بسته به هدف سیستم، باید روشی انتخاب شود که میان هزینه و مقبولیت تعادلی برقرار باشد.

فصل سوم

تشخیص اثر انگشت

۳ - تشخیص اثر انگشت

در مقایسه با بقیه‌ی سنجه‌های بیومتریکی، اثر انگشت به مدت طولانی‌تر و گسترده‌تر مورد استفاده قرار گرفته است. خطوط اثر انگشت و فاصله‌ی بین این خطوط حتی در بین دوقلوها منحصر به فرد و تقریبا در طول زندگی فرد ثابت است. این سنجه در بین عموم مقبولیت دارد و سیستم‌های مبتنی بر تشخیص اثر انگشت، قسمت بزرگی از بازار را به خود اختصاص داده‌اند. با وجود اینکه این سیستم‌ها، قابل اطمینان و مقبول هستند، تا دستیابی به سیستم‌های آرمانی با دقت و امنیت کافی فاصله دارند. از جمله‌ی این مشکلات می‌توان به خراب شدن اثر انگشت فرد به صورت فیزیکی اشاره کرد.

۳-۱- تشخیص زنده بودن اثر انگشت

تشخیص زنده بودن سنجه های بیومتریکی راهی برای سد کردن حملات ارائه‌ی اثر انگشت غیر زنده است. اخیرا تحقیقات زیادی در زمینه‌ی پیدا کردن راه‌هایی برای جلوگیری از این حملات انجام شده و روش‌های پیشنهادی به طور کلی به دو دسته‌ی نرم‌افزاری و سخت‌افزاری تقسیم می‌شوند. روش‌های نرم‌افزاری از اطلاعاتی که سنسورها در اختیارشان قرار می‌دهد استفاده می‌کنند و روش‌های سخت‌افزاری گران‌ترند. به چند تا از این روش‌ها در زمینه‌ی اثر انگشت اشاره می کنیم[5] :

از آنجا که تعرق ویژگی زنده بودن است، روشی مبتنی بر تشخیص و اندازه‌گیری پدیده‌ی تعریق ارائه شده که زنده بودن اثر انگشت را تشخیص می‌دهد این روش از ویژگی‌های آماری که سطح خاکستری بودن مقادیر تصویر(ماسک) در اطراف خطوط اثر انگشت[۱] را توصیف می‌کنند، بهره می‌گیرد تا پدیده‌ی تعرق را کمّی و قابل اندازه گیری کنند.

مسأله‌ی تشخیص اثر انگشت را می‌توان به شکل یک مساله‌ی دسته‌بندی باینری (زنده-غیرزنده) دید. نقطه‌ی کلیدی حل این مسئله آن است که مجموعه‌ای از الگوها و ویژگی‌های منحصر به فرد را جمع‌آوری کنیم و

[۱] Ridges

دسته‌بندی را براساس این ویژگی‌ها انجام دهیم. در نهایت ماژول دسته‌بندی احتمال زنده بودن یا نبودن سنجه‌ی ارائه شده را خروجی می‌دهد.

در تصویر اثر انگشت‌های تقلبی عدم یکنواختی مشاهده می‌شود. پس روش‌هایی مبتنی بر توصیف کننده‌های تصویر ارائه شده تا با استفاده از پراکندگی در گرادیان تصویر، زنده بودن یا نبودن تصویر را تشخیص دهند.

نتیجه گیری

در حدود یک قرن پیش از اثر انگشت برای احراز هویت بیومتریک استفاده شده است و همچنان سیستم‌های احراز هویت مبتنی بر این سنجه قسمت بزرگی از بازار را به خود اختصاص می‌دهند. از این سیستم‌ها در حضور و غیاب مدارس و آموزشگاه‌ها تا قفل انبار و گاوصندوق استفاده می‌شود. از آنجا که اثرانگشت به راحتی از سطوح لمس شده قابل جمع آوریست، ارائه‌ی اثر انگشت غیرواقعی تهدید بزرگی برای این سیستم‌هاست. برای مقابله با این خطر نیز، روش‌هایی پیشنهاد شده که به توضیح مختصر چند روش از جمله توصیف گرادیان تصویر و روش مبتنی بر تشخیص و اندازه‌گیری پدیده‌ی تعریق و روش مبتنی بر الگوریتم دسته بندی پرداختیم.

فصل چهارم

تشخیص چهره

٤ – تشخیص چهره

تشخیص چهره یکی از روش‌های احراز هویت بیومتریک است که در بسیاری از کاربردها و به صورت گسترده استفاده می‌شود. یکی از کاربردهای شاخص آن باز کردن قفل گوشی‌های همراه است که اولین بار توسط شرکت اپل در سری گوشی‌های آیفون ارائه شد. در تشخیص چهره مراحل زیر طی می‌شود:

ثبت‌نام: شخص در فاصله‌ی ۲ پا از دوربین می‌ایستد، در سیستم های ۲بعدی مستقیما از شخص یک تصویر دو بعدی گرفته می‌شود ولی در سیستم‌های ۳ بعدی یک ویدیوی زنده‌ی ۳ بعدی از شخص گرفته می‌شود و سپس به تصویر ۲ بعدی تبدیل می‌شود.

استخراج ویژگی: نزدیک به ۸۰ نقطه‌ی گره‌ای منحصر به فرد در صورت هر فرد وجود دارد.این نقاط از ویژگی‌های هر فرد مثل فاصله‌ی بین دو چشم یا ارتفاع پیشانی استخراج می‌شود و سپس به شکل یک الگو در پایگاه داده‌ی سیستم ذخیره می‌شود.

رنگ چهره نیز بررسی می‌شود. چند الگوریتم به طور همزمان برای استخراج این داده ها کار می کنند و از این داده ها ، یک کد عددی ایجاد می شود که به عنوان چاپ چهره[۲] شناخته می شود و نشان دهنده چهره در پایگاه داده است.

مقایسه: در این مرحله الگوی جدید با الگوهای داخل پایگاه داده مقایسه می‌شود. این مقایسه از طریق یک تطبیق دهنده انجام می‌شود و میزان شباهت الگوی ورودی و الگوهای پایگاه داده به صورت عددی اندازه‌گیری می‌شود.

تطابق: اگر با یکی از نمونه ها تطابق داشت (میزان شباهت از آستانه‌ی تعیین شده بیشتر باشد) کاربر اجازه‌ی ورود پیدا می کند.

در کاربردهایی که دوربین تشخیص چهره در دستگاه‌های قابل حمل مثل موبایل و لپ تاپ می‌باشد، باید در نظر گرفت که تغییر در محیط یا تغییر در سخت‌افزار بر عملکرد تشخیص تاثیر می‌گذارد. در تاریکی نمی‌توان از تشخیص چهره استفاده کرد ولی حتی اگر از تاریکی صرف نظر کنیم، در فضای باز با نور زیاد و سایه های شدید نیز

[۲] Face print

عملکرد الگوریتم با مشـــکل مواجه می‌شـــود. با اینکه به لطف الگوریتم‌های پیشـــرفته تصـــحیح نور، مکانیزم های تشخیص دقیق، مکانیزم‌های صفحه‌بندی و ترازبندی یا تکنیک های پیشرفته یادگیری ماشین، سیستم‌های تشخیص چهره در مقابل تغییر محیط مستحکم‌تر شدند، باز هم تغییر در سخت‌افزار و محیط چالش برانگیز است. در این مواقع برای افزایش راحتی و امنیت از ترکیب چند سنجه‌ی بیومتریکی استفاده می‌شود چون تشخیص چهره ممکن است تحت تاثیر محیط باشد ولی سنجه‌های بیومتریکی دیگر اعم از صدا و اثر انگشت از تغییرات محیط مصون هستند[2].

۴-۱- تشخیص زنده بودن چهره

چهره از ســـنجه‌های بیومتریک اســـت که به راحتی در اختیار همه قرار می‌گیرد. امروزه تهیه‌ی عکســـی از چهره‌ی یک فرد در شبکه‌های اجتماعی بسیار آسان است. این مشکل باعث شده تحقیقاتی در زمینه‌ی جلوگیری از این حملات که spoofing attack نام دارند صورت بگیرد. در طی این حملات فرد فریبکار با نشان دادن عکس از چهره‌ی فرد واجد شرایط، وارد سیستم می‌شود. روش‌ها و الگوریتم‌های زیادی برای تشخیص زنده بودن چهره پیشـــنهاد شـــده که از ســـاده‌ترین آن‌ها می‌توان به آزمون پلک زدن اشـــاره کرد؛ گرچه بعضـــی از این الگوریتم ها پیچیده‌ترند و حتی بافت و نور صحنه را تحلیل می‌کنند.

بسیاری از این روش‌ها از الگوریتم‌های یادگیری ماشین برای تشخیص استفاده می‌کنند، ولی این الگوریتم‌ها به شـدت به مجموعه داده‌هایی که برای یادگیری این الگوریتم‌ها اسـتفاده می‌شـود وابسـته اند و این یعنی اسـتحکام روش تشخیص زنده بودن چهره به این مجموعه داده‌ها و فناوری مورد استفاده برای گرفتن عکس چهره و تحلیل آن وابســته اســت. این وابســتگی نگرانی‌هایی را برمی‌انگیزد چون اگر حمله‌ای قبلا در داده‌های آموزشـــی نبوده باشـــد نمی‌توان شناسایی آن حمله را تضمین کرد.از آنجا که صحت این الگوریتم‌ها به روشی که فریبکار استفاده می‌کند تا چهره‌ی غیرزنده را ارائه دهد وابسته است، استفاده از تنها یک الگوریتم برای تشخیص زنده بودن تصویر توصیه نمی‌شود.

یک راه حل قوی، ترکیبی از چندین روش و الگوریتم و ترکیب ابزار تجزیه و تحلیل خودکار با تعامل کاربر اســـت. اگر ســـیســـتم بتواند واکنشـــی را در کاربر ایجاد کند و ســـپس این واکنش را تجزیه و تحلیل کند، هر چهره‌ی غیرزنده‌ای از فرد واجد شرایط اعم از عکس یا ویدیو، نامعتبر شناخته می‌شود. متاسفانه تعامل با کاربر زمان بر است و قابلیت استفاده از سیستم را کم رنگ می‌کند. پس چالش اصلی برقراری تعادل بین امنیت و راحتی است.

در کاربردهایی که امنیت در اولویت قرار دارد، می‌توان از این تعامل بین کاربر و سیستم بهره برد ولی در کاربردهایی که روزانه توسط عوام استفاده می‌شود (مانند باز کردن قفل تلفن همراه توسط تشخیص چهره‌ی مالک) می‌توان راحتی و سرعت احراز هویت را، اهم قرار داد[2].

ذخیره‌ی الگوی اطلاعات چهره

ممکن است هکرها با هک کردن سیستم به الگوهای ذخیره شده دسترسی پیدا کنند.یک نمونه اخیر را می توان در نشت کردن داده های دولت ایالات متحده در دسامبر ۲۰۱۴ یافت ، زمانی که ۵.۶ میلیون اثر انگشت به سرقت رفت .با استفاده از آنها ، هکر می تواند به سیستم یا سیستم های دیگر دسترسی داشته باشد و حتی کاربران را در سیستم های مختلف ردیابی کند .برای ذخیره‌ی الگوها، چالش اصلی آن است که بتوانیم از چند الگوریتم تشخیص چهره استفاده کنیم و با تحلیل سیگنالهای خروجی آنها بی‌نظمی و آنتروپی کافی برای ساختن یک الگو را بدست آوریم تا به کارایی خوبی در نرخ تشخیص و زمان پاسخ برسیم و در عین حال امنیت سیستم را حفظ کنیم.

نتیجه گیری

تشخیص چهره یکی از سنجه‌های بیومتریکی پرکاربرد است وسیستم‌های مبتنی بر تشخیص چهره در بسیاری از کاربردها از شناسایی مجرمان و عبور و مرور فرودگاهی تا باز کردن قفل تلفن همراه استفاده می‌شوند. کاربر در طی مراحل ثبت‌نام یا ورود باید در مقابل دوربین بایستد تا تصویرش توسط الگوریتم‌های استخراج ویژگی تحلیل شده و به الگوی دیجیتال تبدیل شود. نقش الگوریتم‌های یادگیری ماشین در تشخیص و تطابق این سیستم‌ها نسبت به سیستم‌های مبتنی بر سنجه‌های دیگر پررنگ‌تر است؛ به همین رو، تغییرات در محیط می‌تواند باعث خرابی و کاهش کارکرد سیستم شود. برای جلوگیری از تاثیر عوامل محیطی بر عملکرد الگوریتم پیشنهاد می‌شود از ترکیب چند سنجه برای احراز هویت استفاده شود.

فصل پنجم

امنیت سیستم های احراز هویت

۵ – امنیت سیستم های احراز هویت

۵-۱- حملات مخالف

دو خرابی اصلی برای سیستم‌های بیومتریکی وجود دارد و هدف حملات آن است که یکی یا هر دوی این خرابی‌ها در سیستم اتفاق افتد. البته تنها دلیل بروز این خرابی ها حملات نیست و محدودیت‌های ذاتی نیز می‌توانند این خرابی‌ها را حاصل شوند[1].

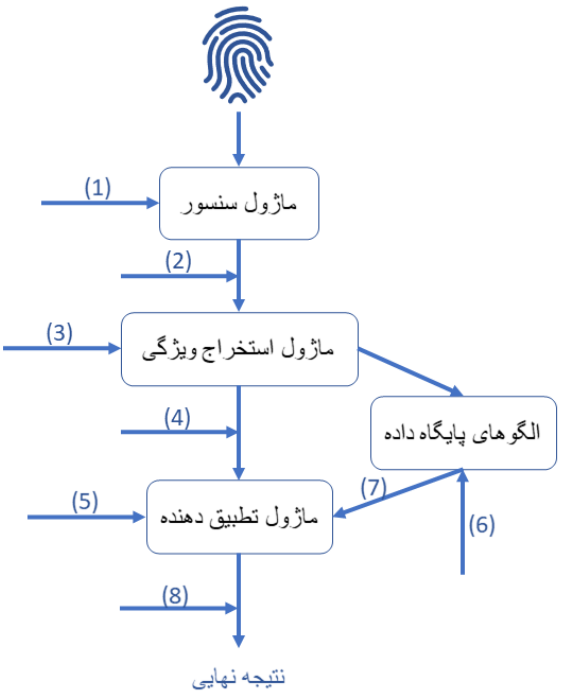
۱ –عدم سرویس دهی[۳]: سیستم اجازه‌ی دسترسی به کاربر مشروع را ندهد.

۲ –نفوذ[۴]: سناریویی که در آن سیستم به اشتباه یک متقلب را به عنوان یک کاربر مجاز شناسایی می کند.

از نمونه‌های حملات رایج که پیش‌تر هم به آن اشاره شد می‌توان حملات ارائه‌ی چهره‌ی غیرزنده را نام برد. حملات می‌توانند به فرم‌های مختلف و بر قسمت‌های مختلف سیستم پیاده شوند. بر اساس هدف حملات می‌توان آن‌ها را به طور کلی به ۴ دسته تقسیم کرد[5]:

- حملات به واسط، مانند سنسور (نقطه‌ی ۱)
- حملات به ماژول‌ها، مانند ماژول استخراج ویژگی(نقطه‌ی ۳ و ۵)
- حملات به رابط‌های بین ماژول‌ها(نقاط ۲ و ۴و ۷و ۸)
- حملات به الگوهای داخل پایگاه داده

در شکل ۲ مراحل ضبط، ثبت و تطبیق سنجه‌ی بیومتریکی و نقاط اهداف حمله‌ی مرتبط مشخص است. در جدول ۲ نیز انواع حملات و نقاط هدفشان ذکر شده است.



شکل ۲- بخش‌های مختلف سیستم احراز هویت و نقاط هدف حملات.

[۳] Denial of service

[۴] Intrusion

شماره	حمله	نقاط حمله
۱	ارائه‌ی سنجه‌ی تقلبی به سنسور	۱
۲	سواستفاده از تشابه(برای مثال دوقلوها)	۱
۳	فرد فریبکار از سنجه‌های خود برای ورود به سیستم استفاده می‌کند و به دلیل خطاهای سیستم، واجد شرایط شناخته می‌شود	۱
۴	دستکاری و تخریب سنسور به شکل فیزیکی تا از دسترس خارج شود	۱
۵	فرد فریبکار سنجه‌ی بیومتریکی را ضبط و برای سیستم بازپخش می‌کند	۲ و ۴
۶	قطع راه ارتباطی و خارج کردن سیستم از دسترس	۲ و ۴
۷	دستکاری کانال‌های ارتباطی به نحوی که دیگر سیستم به فرد مقبول و واجد شرایط، اجازه دسترسی و ورود ندهد	۲ و ۴
۸	مداوم تصویر مورد نظر تغییر پیدا کند تا نمره‌ی تطبیق مورد نظر بدست آید و با تصویر خواسته شده تطبیق پیدا کند	۲ و ۴
۹	مرتبا به سیستم نمونه‌هایی تزریق شود تا مانع ورود افراد واقعی شود	۲ و ۴
۱۰	تزریق برنامه‌های است تروبان	۳ و ۵
۱۱	هکر به صورت غیرقانونی به اطلاعات الگوهای ذخیره شده دستیابی پیدا کند	۶
۱۲	هکر الگوها را تغییر دهد یا به الگوها اضافه کند	۶
۱۳	الگوها، از یکی از کانال‌های ارتباطی خوانده شوند و دوباره برای سیستم بازپخش شوند	۷
۱۴	تغییر اطلاعاتی که از تغییر کانال‌های ارتباطی می‌گذرد برای آنکه از ورود فرد واجد شرایط به سیستم جلوگیری شود	۷
۱۵	تغییر نتیجه‌ی تطبیق ارسال شده(matching/non-matching) برای آنکه مانع ورود فرد واجد شرایط شود یا اجازه‌ی ورود فریبکار داده شود	۷

جدول ۲- انواع حملات و نقطه‌های هدف این حملات که در شکل ۲ مشخص شده است.

۵-۲- الگوهای دیجیتال

فرآیند کلی احراز هویت در سیستم‌های احراز هویت بیومتریک در زمان ثبت نام، با بدست آوردن اطلاعات بیومتریک از طریق سنسور مربوطه شروع می‌شود؛ سپس، مشخصه‌های این نمونه از روش‌های نرم‌افزاری و با الگوریتم‌های استخراج ویژگی[۵] بدست می‌آیند و در آخر، سیستم این الگو[۶] را به همراه بقیه‌ی اطلاعات شناسایی از جمله نام و شماره‌ی ملی در پایگاه داده ذخیره می‌کند. در زمان احراز هویت (ورود کاربر) دوباره اطلاعات از طریق سنسورها جمع‌آوری شده و با استفاده از استخراج کننده‌های ویژگی، مشخصه‌های نمونه به صورت الگویی درمی‌آید. در مرحله‌ی بعد این الگو با استفاده از یک تطبیق دهنده[۲] با تمام الگوهای ذخیره شده در پایگاه داده مقایسه می‌شود و این تطبیق دهنده یک نمره‌ی تطبیق[۳] که نشان دهنده‌ی میزان شباهت الگوی ورودی و الگوی داخل پایگاه داده است را برمی‌گرداند[*1*].

یکی از مسائل حیاتی در حوزه‌ی امنیت، ذخیره‌ی این الگوها در پایگاه داده است. گرچه روش‌های جایگزین ذخیره‌ی الگو به شکل غیرمجتمع (مانند ذخیره‌ی اثرانگشت در کارت ملی هوشمند) ریسک‌ها و خطرهای امنیتی را کاهش می‌دهند ولی جوابگوی کاربردهایی که توانایی تکثیر را نیاز دارند نیستند. معیارهای تامین امنیت الگوی ذخیره شده عبارتند از[*2*]:

۱- **معکوس ناپذیری:** ویژگی یک تبدیل بیومتریک است(ساختن مرجعی از اطلاعات) به شکلی که دسترسی به اطلاعات مرجع تبدیل یافته منجر به دسترسی به اطلاعات خود سنجه نشود؛ یعنی، نباید بتوان از روی الگوی ذخیره شده اطلاعات سنجه را محاسبه کرد(یا باید این محاسبه سخت و هزینه بر باشد).

۲- **تبعیض آمیزی:** شمای حفاظت از الگو نباید دقت احراز هویت را کاهش دهد.

۳- **تجدید ناپذیری:** توانایی جلوگیری از تأیید موفقیت آمیز یک مرجع بیومتریک خاص و مرجع هویت مربوط به آن؛ یعنی، باید بتوان چند الگوی امن از یک سنجه درست کرد که این الگوها قابل پیوند به اطلاعات آن سنجه نباشند. این ویژگی، سیستم بیومتریک را قادر می سازد در صورت به خطر افتادن پایگاه داده،

[۵] Feature extractor

[۶] template

الگوهای جدید بیومتریک را لغو و دوباره منتشـــر کند؛ همچنین، از تطبیق ضـــربدری[۷] در ســـطح پایگاه داده ها جلوگیری می‌کند.

۵-۲-۱- روش های حفظ امنیت الگوی ذخیره شده

برای حفظ امنیت الگوهای ذخیره شده به طور کلی دو روش پیشنهاد شده[*1*]:

۱-**تبدیل ویژگی بیومتریک[۸]:** الگوی امن با استفاده از اعمال یک تابع تبدیل غیرقابل برگشت یا یک طرفه(براساس پارامترهای خاص کاربر) بر روی الگوی اصلی بدست می آید. در زمان ورود کاربر، سیستم همان تابع تبدیل را بر روی نمونه‌ی مورد جستجو اعمال می‌کند و تطبیق در فضای تبدیل یافته صورت می‌گیرد.

۲-سیستم های رمزنگاری بیومتریک[۹]: تنها بخشی از اطلاعات حاصل از الگوی بیومتریک معروف به طرح امن[۳] را ذخیره می کند. در حالی که طرح امن به خودی خود برای بازسازی الگوی اصلی کافی نیست، اما در حضور یک نمونه بیومتریک دیگر که با نمونه ثبت نام منطبق باشد، حاوی داده‌های کافی برای بازیابی الگوست.

طرح امن در واقع با پیوند دادن الگو بیومتریک و کلید رمزنگاری بدست می‌آید؛ اما، طرح امن یک الگوی رمزنگاری شـده توسـط روش‌های اسـتاندارد رمزنگاری نیسـت. در روش‌های رمزنگاری اسـتاندارد الگوی نمونه و الگوی رمزنگاری شده دو موجودیت مستقلند و الگوی رمزنگاری شده تا زمانی امن است که کلید استفاده شده در این رمزنگاری محفوظ باشـــد. اما طرح امن الگوی نمونه و کلید رمزنگاری را باهم به شـــکل یک موجودیت درمی‌آورد و هیچکدام به تنهایی با داشتن طرح امن قابل دستیابی نیستند. تنها در زمانی که سیستم در معرض یک الگوی مشابه قرار می‌گیرد، طرح امن می‌تواند الگوی نمونه‌ی اصلی و کلید رمزنگاری را با استفاده از تکنیک‌های تشخیص خطای مشترک، بازیابی کند.

---

[۷] Cross-matching

[۸] Biometric feature transformation

[۹] Biometric cryptosystems

تحقیقات دو روش برای تولید طرح امن پیشنهاد دادند. تعهد درهم[۱۰] و نقص درهم[۱۱]. تعهد درهم می‌تواند در مواقعی که الگوها به صورت آرایه‌های باینری با طول ثابت ذخیره شده‌اند استفاده شود و نقص درهم برای مواقعی استفاده می‌شود که الگوها به صورت مجموعه ای از نقاط ذخیره شده‌اند.

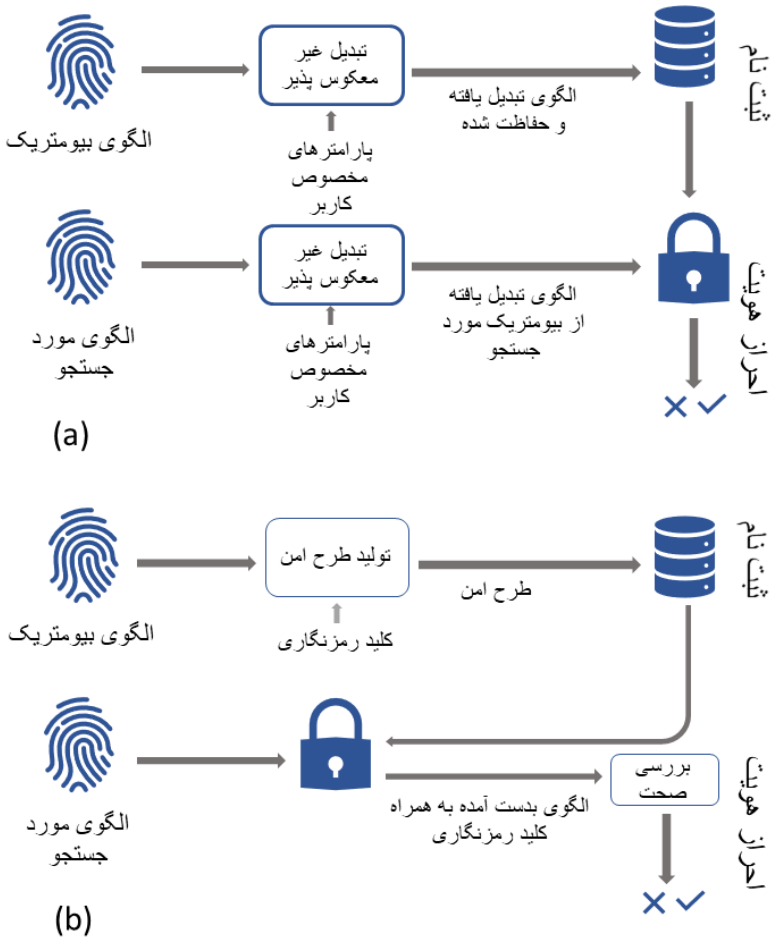
البته این دو روش، نمیتوانند چندین الگو از یک سنجه‌ی بیومتریکی تولید کنند به طوری که این الگوها پیوند پذیر نباشند؛ به عبارت دیگر، نتوان از طریق یکی به دیگری دست یافت. برای این مشکل یک راه حل آن است که قبل از رمزنگاری الگو و ساخت طرح امن، یک تابع تبدیل ویژگی روی داده اعمال شود[*1*].

۵-۲-۲- مقایسه‌ی روش‌های حفظ امنیت الگوی ذخیره شده

دو روش رمزنگاری بیومتریک و تبدیل ویژگی بیومتریک مزایا و معایب خود را دارند. تطبیق در روش تبدیل ویژگی بیومتریک آسان‌تراست؛ ولی، از معایب روش تبدیل ویژگی، دشواری پیدا کردن تابعی غیر معکوس‌پذیر است به طوری که خصوصیات فضای اصلی ویژگی را تغییر ندهد. روش های معقول در زمینه‌ی تئوری اطلاعات برای رمزنگاری داده‌های بیومتریکی و ساخت طرح امن وجود دارد ولی چالش اصلی در این روش آن است که داده‌های الگوهای بیومتریکی را بتوان در داده‌ساختار ها مثل رشته‌های باینری با طول ثابت ذخیره کرد. درنتیجه طراحی الگوریتم‌هایی برای تبدیل اطلاعات بیومتریک در ساختمان داده‌های استاندارد مثل رشته با طول ثابت یا مجموعه نقاط، بدون از دست دادن اطلاعات، از مباحث تحقیقاتی فعال است.

[۱۰] Fuzzy commitment

[۱۱] Fuzzy fault



شکل ۳- حفظ امنیت الگوها با استفاده از (a) روش تبدیل ویژگی بیومتریک و (b) سیستم‌های رمزنگاری بیومتریک.

نتیجه گیری

طی ثبت‌نام و ورود، سیستم احراز هویت مراحلی از جمله بدست آوردن اطلاعات از طریق سنسورها، ذخیره‌ی این اطلاعات در پایگاه داده و جستجو کردن نمونه‌ی وروی در پایگاه داده را طی می‌کند. در طی این عملیات یا ارتباط بین این مراحل ممکن است به قصد بروز خرابی، حملاتی به سیستم اعمال شود؛ این خرابی‌ها موجب عدم ورود کاربر موثق یا ورود کاربر ناموثق به سیستم می‌شوند. برای آنکه از اطلاعات بیومتریک در پایگاه داده حفاظت کنیم آن ها را به فرم الگوهای دیجیتال درمی‌آوریم تا در صورت نفوذ فرد ناموثق، اطلاعات بیومتریک اصلی در اختیار همگان قرار نگیرد. روش‌های تبدیل ویژگی بیومتریک و سیستم‌های رمزنگاری بیومتریک از راه های پیشنهادی برای تولید این الگوهای دیجیتال هستند.

نتیجه گیری و پیشنهادها

پیشنهادها

در کل می‌توان برای بهبود عملکرد سیستم‌های احراز هویت از ترکیب چند سنجه‌ی بیومتریک استفاده کرد. در احراز هویت به کمک هر سنجه، استفاده از الگوریتم‌های یادگیری ماشین رایج است ولی برای جلوگیری از حملات، می‌توان روش‌های مکملی را پیشنهاد داد. برای مثال استفاده از تشخیص گردش خون می‌تواند برای جلوگیری از حملات ارائه‌ی سنجه‌ی غیرزنده موثر واقع شود.

برای حفظ امنیت الگوی ذخیره شده نیز می‌توان از ترکیب هردو روش سیستم های رمزنگاری بیومتریک و تبدیل ویژگی بیومتریک استفاده کرد. این روش به روش رمزنگاری بیومتریک پیوندی[۱۲] نیز معروف است و مطالعاتی روی آن انجام شده است. برای ایمنی بیشتر و کاهش نواقص هردو روش پیشنهاد میشود از روش پیوندی استفاده شود.

نتیجه گیری

در این گزارش به مقایسه‌ی سنجه‌های بیومتریکی مختلف پرداخته شد؛ به طور کلی، استفاده از سنجه‌های عنبیه و شبکیه به علت هزینه و دقت بالا در کاربردهای نظامی یا سطوح بالای دولتی توصیه شده است ولی در کاربردهای روزمره مثل حضور وغیاب و باز کردن قفل گاوصندوق یا تلفن، استفاده از سیستم‌های مبتنی بر اثرانگشت و تشخیص چهره به علت دقت بالا و ارزانی سنسورها ارجحیت دارند. در اکثر موارد، ترکیب چند سنجه‌ی بیومتریکی باعث افزایش دقت سیستم می‌شود(البته به بهای کند شدن فرآیند احراز هویت). به طور کلی هدف آن است که با انتخاب سنجه‌ی مناسب، سیستم به تعادلی از راحتی استفاده و دقت برسد.

در فرآیند ثبت‌نام، اطلاعات کاربر از طریق سنسورها ضبط می‌شود، ویژگی‌های تصویر ضبط شده استخراج می‌شود و الگوی دیجیتال طبق این ویژگی‌ها ساخته شده و در پایگاه داده ذخیره می‌شود. در هنگام احراز هویت نیز مراحل مشابه طی شده و الگوی ساخته شده با الگوهای ذخیره شده در پایگاه داده مقایسه شده تا نمونه‌ی مشابهی پیدا شود. در تمامی این مراحل امکان دارد که هکرها برای بروز خرابی در سیستم به ماژول‌های تمامی این مراحل و ارتباط بین این ماژول‌ها حمله کنند. هدف حملات، سخت‌افزار یا نرم‌افزار می‌تواند باشد، یکی از حملات نرم‌افزاری

[۱۲] Hybrid biometric cryptosystems

ارائه‌ی سنجه‌ی غیرزنده[۱۳] است؛ بسته به سنجه‌ی بیومتریک، با به کار گرفتن الگوریتم‌های یادگیری ماشین می‌توانیم از این حملات جلوگیری کنیم.

سنجه‌های بیومتریک غیرقابل تعویض هستند و با تنها یک بار افشا شدن، دیگر قابل استفاده نیستند؛ از همین رو، اقدامات امنیتی برای جلوگیری از افشا شدن اطلاعات اصلی بیومتریک ضروری است. از جمله‌ی این اقدامات حفظ الگوی دیجیتال ذخیره شده در پایگاه داده است. این الگوها با استفاده از دو روش تبدیل ویژگی و سیستم‌های رمزنگاری بیومتریک تولید می‌شوند. در سیستم‌های رمزنگاری بیومتریک طرح امنی ساخته می‌شود که تنها در کنار اطلاعاتی شبیه اطلاعات جستجو شده، الگوی ذخیره شده را افشا می‌کنند. دو روش تعهد درهم و نقص درهم نیز برای تولید طرح امن پیشنهاد شده‌اند و در بعضی موارد از ترکیب این دو روش استفاده می‌شود.

[۱۳] spoofing attack

منابع و مراجع

[1] Jain, A. K., & Nandakumar, K. (*2012*). *Biometric Authentication: System Security and User Privacy. Computer, 45(11), 87–92.*

[2] Vazquez-Fernandez, E., & Gonzalez-Jimenez, D. (*2016*). *Face recognition for authentication on mobile devices. Image and Vision Computing, 55, 31–33.*

[3] Kakkad, V., Patel, M., & Shah, M. (*2019*). *Biometric authentication and image encryption for image security in cloud framework. Multiscale and Multidisciplinary Modeling, Experiments and Design.*

[4] El-Abed, M., Charrier, C., & Rosenberger, C. (*2012*). *Evaluation of Biometric Systems. New Trends and Developments in Biometrics.*

[5] Yang, W., Wang, S., Hu, J., Zheng, G., & Valli, C. (*2019*). *Security and Accuracy of Fingerprint-Based Biometrics: A Review. Symmetry, 11(2), 141.*