انتخاب بیومتریک مناسب جهت افزایش امنیت دستگاه‌های خودپرداز

مسعود رفیقی[1]، حمیدرضا ترسلی[2]

۱- دکترای مهندسی فناوری اطلاعات، هیئت‌علمی مجتمع دانشگاهی فناوری اطلاعات، ارتباطات و امنیت، دانشگاه صنعتی مالک اشتر تهران، ایران

۲- کارشناسی ارشد مهندسی فناوری اطلاعات گرایش امنیت، دپارتمان مهندسی فناوری اطلاعات، موسسه آموزش عالی تعالی، قم، ایران

چکیده:

امروزه استفاده از بیومتریک در پزشکی، تجارت، کسب‌وکار، بانکداری و هویت امری عادی است اما باید بدانیم که این فن‌آوری است که باعث بهبود امنیت، کاهش تقلب، کم کردن هزینه‌های دولتی، بهبود حفظ حریم خصوصی و اجرای قوانین می‌باشد. معاملات مالی در بانک‌ها با بیومتریک بسیار امن‌تر شده است. فناوری بیومتریک در افزایش امنیت و تسهیل کار سیستم- های مکانیزه بانکی نیز کاربرد فراوان پیداکرده است. یکی از روش‌های موردبررسی بیومتریک، تعیین هویت انسان، تشخیص چهره توسط کامپیوتر می‌باشد که معمولاً با عنوان شناسایی چهره بیان می‌گردد. تشخیص چهره استفاده‌های فراوانی در شناسایی بزهکاران، کارت‌های اعتباری، سیستم‌های امنیتی و موارد متعدد دیگر داشته و به دلیل کاربردهای فراوان، در سال‌های اخیر، موردتوجه قرارگرفته است. در این تحقیق از بیومتریک چهره به‌منظور افزایش امنیت دستگاه‌های خودپرداز استفاده می‌کنیم. ابتدا بعد از واردکردن کارت کد واژه یا رمز عبور توسط کاربر وارد می شود، سپس بعد از تأیید کد واژه، چهره فرد شناسایی می‌شود. بعد از تشخیص و تأیید چهره عنبیه فرد شناسایی می‌شود، سپس بعد از تأیید عنبیه چشم، اثرانگشت فرد تشخیص داده می شود. بعد از تأیید و تشخیص چهره، عنبیه چشم و اثرانگشت تراکنش بانکی برای کاربر باز می‌شود و کاربر می‌تواند عملیات بانکی خود را با استفاده از دستگاه خودپرداز انجام دهد. هر یک از تشخیص چهره، عنبیه چشم و اثرانگشت در ۴ مرحله اصلی انجام می‌شود:۱- پیش‌پردازش. ۲- استخراج ویژگی با استفاده از فیلتر گابور وزن دهی شده. ۳- کاهش ابعاد بردار ویژگی با استفاده از الگوریتم PCA. ۴- دسته‌بندی با استفاده از دسته‌بندی SVM. نتایج آزمایش‌های ما بر روی پایگاه داده چهره ORL، پایگاه داده عنبیه چشم و اثرانگشت نشان می‌دهد که روش پیشنهادی کارایی و دقت بالایی در تأمین امنیت دستگاه‌های خودپرداز دارد.

کلمات کلیدی: تشخیص هویت، روش‌های بیومتریک، تشخیص چهره، تشخیص عنبیه چشم، تشخیص اثرانگشت، فیلتر گابور وزن دهی شده، الگوریتم PCA، الگوریتمSVM.

۱- مقدمه

از گذشته دور بشر به دنبال راهی برای شخصی‌سازی اطلاعات و کارهای خود بود. با پیشرفت هر چه بیشتر تکنولوژی انسان به راه‌های جهت رسیدن به هدف خود که همان امنیت در اطلاعات است دست‌یافت. بشر به دنبال امنیت بیشتر در ورود و خروج اطلاعات می‌باشد. با پیشرفت تکنولوژی و تحقیقات گسترده متخصصان روشی به نام بیومتریک ارائه شد که ورود و خروج اطلاعات بر اساس مشخصات فردی انجام می‌شود. مثلاً با استفاده از صدا، اثرانگشت ، چهره و ...

امروزه نیز تأمین امنیت یکی از شاخه‌های بسیار فعال علوم و تحقیقات است و با گسترش هر چه بیشتر ارتباطات و اشتراک منابع مال و فنی و نیاز به آن بیشتر احساس می‌شود روش‌های به‌کاررفته در هر دوره قوت و ضعف فناوری را به همراه دارد. به‌طورکلی می‌توان گفت در هر دوره‌ای پیشرفت‌های حاصل شده در روش‌های شناسایی در جهت بالا بردن دقت و اتوماسیون بیشتر فرایندهای لازم بوده است. سیستم‌های کامپیوتری سرعت، دقت و برنامه‌ریزی‌های پیچیده را برای ما به ارمغان آورده است.

از مدت‌ها قبل مشخصاتی مثل چهره، رنگ چشم، قد، رنگ موی سر و... برای شناسایی افراد بکار می‌رفته و معمول بوده است که این مشخصات همانند نام و نام خانوادگی افراد در شناسنامه یا کارت‌های شناسایی آن‌ها ثبت شود. ویژگی‌های یادشده به همراه مشخصات فیزیولوژیکی و زیستی و مشخصات رفتاری مجموعه روش‌هایی را در برمی‌گیرد که به بیومتریک معروف هستند (پدرو[1] و همکاران، ۲۰۱۶)

امنیت دستگاه‌های خودپرداز یکی از مباحث جدی است. وقتی کارت را وارد دستگاه می‌کنید، دستگاه نمی‌تواند کارت را بخواند، از شما می‌پرسد که گذرواژه را وارد کنید. در این زمان هکرها می‌توانند از گذرواژه شما استفاده کنند و آن را دریافت کنند. راه‌حل این مشکل، استفاده از بیومتریک افراد در این سیستم می‌باشد. بیومتریک، اندازه‌گیری ویژگی رفتاری و فیزیکی اشخاص است که می‌تواند با دیگر نمونه‌های شناسایی قابل‌مقایسه باشد. در این پژوهش سعی می‌کنیم تا با استفاده از ویژگی‌های بیومتریکی چهره، عنبیه چشم، اثرانگشت و کد واژه، امنیت دستگاه‌های خودپرداز را بهتر کنیم و عوامل مؤثر در انتخاب بیومتریک مناسب را بررسی کنیم. کد واژه را در اینجا کد ملی اشخاص در نظر می‌گیریم، سپس برای تشخیص چهره، تشخیص عنبیه چشم و تشخیص اثرانگشت از فیلتر گابور وزن دهی شده و دسته‌بندی ماشین بردار پشتیبان استفاده می‌کنیم. همچنین در این پژوهش، ما سعی کردیم روش‌هایی ارائه دهیم تا مشکلات روش‌های پیشین را تا حد زیادی مرتفع سازیم.

[1] - Pedro

جدول (۱) سابقه تحقیقات و خلاء های موجود

معایب	مزایا	احراز هویت	نویسنده	سال انتشار	عنوان مقاله
مشکل در استفاده از رمز یکبار مصرف در ارسال آن به کاربر از طریق پیامک	این عمل کلاهبرداری را که از طریق سرقت کارت به وجود می آمد، به طور کامل از بین می برد	ویژگی های مثل تشخیص چهره و رمز یکبار مصرف(OTP) به منظور بهبود امنیت حساب های شخصی کاربران استفاده می شود.	کاروواليا و همکارانش	۲۰۱۵	بهبود امنیت دستگاه های ATM با استفاده از ویژگی های تشخیص چهره
خراب شدن دوربین جاسازی شده	این سیستم در بحث فراموش کردن کارت امید بخش است و تجربه کاربران ATM را بهبود می دهد	قریم های زمانی کوتاه از ATM مورد استفاده است و حرکت ها این مسئله را در تشخیص چهره، مشکل می سازد. آنها سیستم پیشنهادی را تحت چالش های واقعی از ATM مورد ارزیابی قرار دادند	درمان و همکارانش	۲۰۱۳	کاهش میزان استرداد در دستگاه های ATM با استفاده از روش های تعیین و تشخیص چهره و جاسازی دوربین در دستگاه های ATM
مشکل در ارسال پیامک به مشتری از طریق مودم GSM و دقت پایین تشخیص اثر انگشت	بدون نیاز به کارتهای بانکی، از طریق حسگر اثر انگشت در دستگاه، تائید هویت شده و از امکانات و خدمات بانکی استفاده نمایند	کاربر تقاضای برداشت از حساب را داشته باشد، یک پیامک به موبایل وی ارسال می گردد .در این پیامک، مبلغ برداشتی و یک کد امنیتی نوشته شده است. ارسال پیامک به مشتری از طریق مودم GSM انجام می شود.	ترکمانی و همکاران	۱۳۹۴	دستگاه خودپرداز مجهز به حسگر اثر انگشت و مودم GSM
دقت تشخیص و امنیت پایین با استفاده از بیومتری اثر انگشت	مطالعه موردی(بررسی بیومتری های مختلف در امنیت دستگاه های خودپرداز)	پیاده سازی یا حسگر اثر انگشت یا توجه به ویژگیهای خودپردازهای موجود نیاز به عوض کردن کامل الگوریتم تشخیص هویت دستگاهها یا اضافه کردن حسگر اثر انگشت به دستگاه های فعلی است	حسن پور و رشیدی	۱۳۹۲	آشنایی باستفاده ازمتدهای بیومتریک احراز هویت دردستگاه های خودپرداز

در ادامه در بخش دوم چارچوب پیشنهادی خود را در معرفی می‌نماییم .در بخش سوم نحوه پیاده‌سازی و ارزیابی این چارچوب مطرح می‌شود و درنهایت در بخش چهارم به نتیجه‌گیری در مورد دستاوردهای این مقاله می‌پردازیم.

۲- چهارچوب پیشنهادی

در این بخش هر یک از بیومتریک های مناسب و مؤثر و ترکیب بیومتریک ها در جهت افزایش امنیت دستگاه‌های خودپرداز موردبررسی قرار می‌گیرد.

۲-۱- سیستم تشخیص چهره

دزدی و یا سرقت در خودپرداز مانند وارد شدن مجرم به سیستم و اجبار کاربر برای دسترسی به حسابش ممکن است اتفاق بیافتد. برای غلبه به این مشکل یک‌راه حل ساده تشخیص چهره است. بعد از تأیید کد واژه وارد مرحله تشخیص چهره می‌شویم. تشخیص چهره مهم‌ترین قسمت در سیستم پیشنهادی است که باید به‌درستی و با دقت بالا انجام شود تا سیستم بتواند کاربر سیستم خودپرداز را به‌درستی تشخیص دهد. بعدازاینکه کد واژه تأیید شد، در این مرحله کاربر باید به دوربین نصب‌شده در خودپرداز نگاه کند، درنتیجه چهره او تشخیص داده می‌شود و سیستم تصمیم می‌گیرد که آیا این‌چنین چهره‌ای در پایگاه داده بانک وجود دارد یا خیر. اگر کد واژه واردشده با چهره تشخیص داده‌شده، مطابقت نداشته باشد، حساب کاربر موقتی قفل شود و به کاربر اخطار داده می‌شود، در غیر این صورت، به سیستم تشخیص عنبیه چشم منتقل می شود. این ویژگی‌های ساده مؤثر و کارا است؛ بنابراین این سیستم مطمئن است و تراکنش فقط زمانی می‌تواند پردازش شود که فقط کاربر به ماشین دسترسی پیدا کند. در ادامه به شرح مراحل تشخیص چهره می‌پردازیم.

به‌طورکلی تکنیک‌های تشخیص چهره به دودسته تقسیم‌بندی می‌شود (ژانگ[1] و همکاران، ۲۰۱۴).

الف) روش‌هایی بر اساس ظاهر چهره

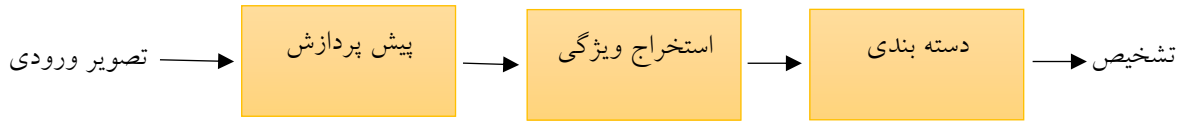
این روش از ویژگی‌های هندسی چهره (مانند بینی، چشم، دهان و...) و ارتباط هندسی بین آن‌ها استفاده می‌کند.

ب روش‌هایی بر اساس ویژگی

این روش‌ها از ویژگی‌های بافتی کل‌نگر استفاده می‌کنند. این روش‌ها بر روی کل چهره یا نواحی خاصی از چهره اجرا می شوند. روش‌هایی مانند تحلیل اجزای اصلی[2]، تحلیل اجزای مستقل[3]، تحلیل تفکیک خطی[4]، فیلتر گابور، الگوی باینری محلی و... جزء این دسته هستند.

ما درروش پیشنهادی، تشخیص چهره را بر اساس ویژگی‌های چهره انجام می‌دهیم.

تشخیص چهره در سه مرحله اصلی انجام می‌شود: ۱. تعیین ناحیه چهره. ۲. استخراج ویژگی چهره.۳. دسته‌بندی ویژگی‌های چهره. اولین و مهم‌ترین مرحله بعد از تعیین ناحیه چهره و پیش‌پردازش که باید در تشخیص انجام شود، استخراج ویژگی چهره است. تعیین دقیق ویژگی تأثیر زیادی در کارایی سیستم تشخیص چهره دارد. اگر ویژگی‌ها ناقص یا ناکافی باشد، حتی اگر بهترین دسته‌بندی انجام شود ممکن است سیستم جواب خوبی ندهد؛ بنابراین اینکه چطور ویژگی قدرتمند را از تصویر انتخاب کنیم، باید موردتوجه قرار گیرد. شکل (۱) دیاگرام کلی سیستم‌های تشخیص چهره را نشان می‌دهد.



شکل (۱): دیاگرام کلی سیستم‌های تشخیص چهره

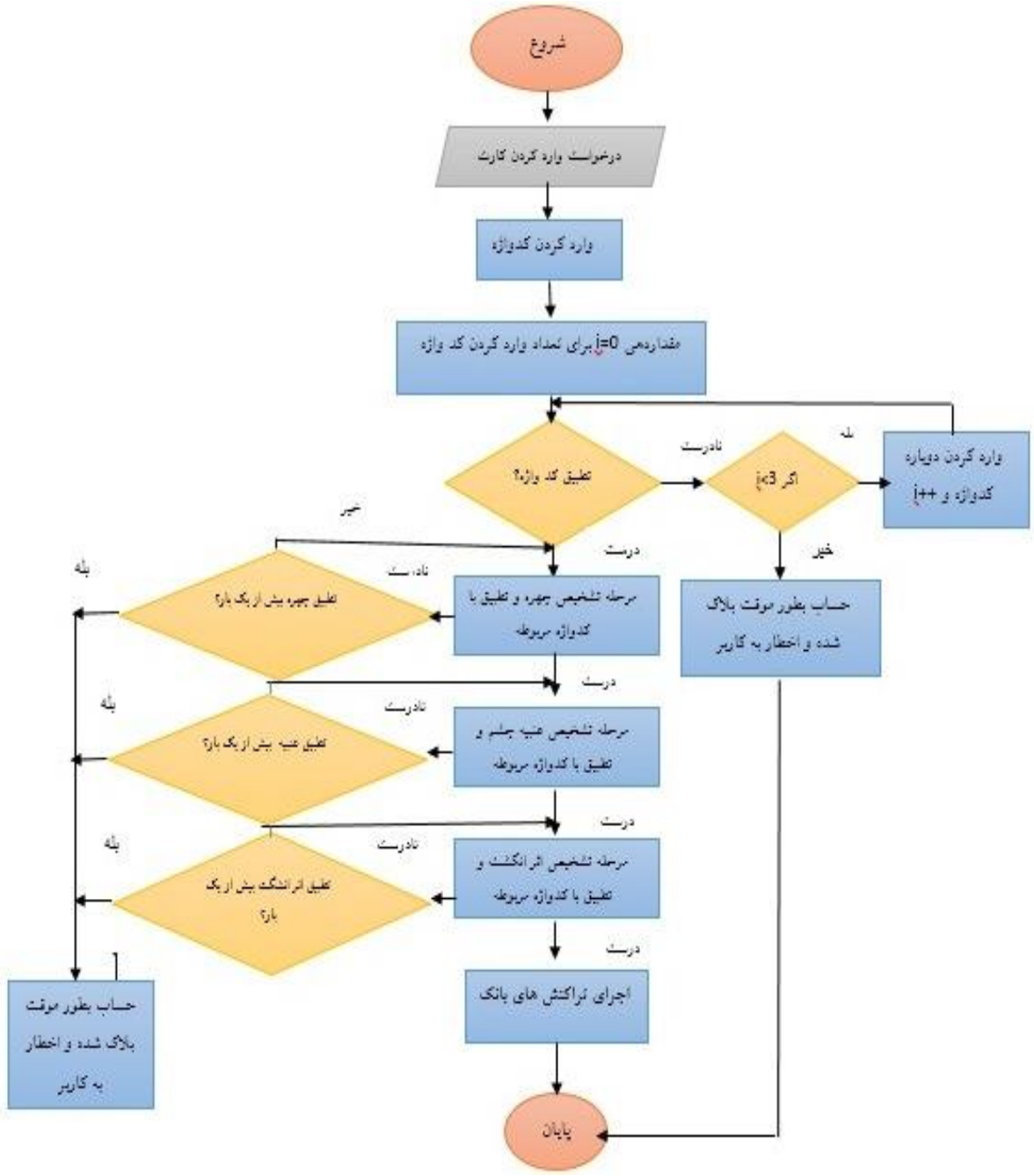
یکی از مشکلات این روش این است که زمانی که دوربین به‌درستی کار نکند یا خراب شود. در این مواقع به دلیل عملیات غیرطبیعی، از اجرای تراکنش باید جلوگیری شود؛ اما برای حل این مسئله، باید یک دکمه گزارش بر روی صفحه مانیتور ATM، در طول مرحله تشخیص چهره، معرفی شود. این اخطار به بانک ارجاع داده می‌شود و مشکل می‌تواند به‌زودی حل شود. اگر کاربر کد واژه را در زمان کوتاهی بعد از تشخیص چهره وارد نکرد، تراکنش می‌تواند به تأخیر بیافتد. برای غلبه به راین مشکل، یک دکمه دوباره فرستادن باید در این مرحله بر روی صفحه مانیتور ATM ظاهر شود. یا باید از بیومتری های دیگر مانند عنبیه چشم و اثرانگشت به‌منظور افزایش امنیت دستگاه‌های خودپرداز استفاده کرد. تشخیص هویت عنبیه چشم و اثرانگشت نیز مانند تشخیص چهره در سه مرحله اصلی انجام می‌شود.

[1] - Zhang
[2] -Principal Component Analysis
[3] -Independent Component Analysis
[4] -Linear Discriminate Analysis

۲-۱-۱- بررسی سیستم ترکیب کد واژه با ترکیب بیومتریک های مختلف چهره، عنبیه چشم و اثرانگشت در تأمین افزایش امنیت دستگاه‌های خودپرداز

در این پژوهش روشی به‌منظور بهبود امنیت دستگاه‌های خودپرداز بر اساس کد واژه و ترکیب تشخیص چهره، عنبیه چشم و اثرانگشت ارائه کردیم. امنیت دستگاه‌های خودپرداز در سیستم پیشنهادی در ۴ مرحله اصلی انجام می‌شود:

۱. واردکردن کد واژه. ۲. تشخیص چهره. ۳. تشخیص عنبیه چشم. ۴. تشخیص اثرانگشت. اولین و مهم‌ترین مرحله بعد از واردکردن کد واژه، تشخیص چهره است که باید به‌درستی انجام شود. بعد از تشخیص درست چهره، عنبیه چشم تشخیص داده می‌شود، در صورت تأیید و تشخیص عنبیه چشم، اثرانگشت شناسایی می‌شود. در صورت تأیید هر چهار مرحله حساب کاربری کاربر باز می‌شود و می‌تواند به‌حساب شخصی خود دسترسی داشته باشد. تشخیص چهره، تشخیص عنبیه چشم و تشخیص اثرانگشت در سه مرحله اصلی پیش‌پردازش تصویر، استخراج ویژگی و دسته‌بندی انجام می‌شود. مهم‌ترین مرحله در تشخیص، استخراج ویژگی است، تعیین دقیق ویژگی تأثیر زیادی در کارایی سیستم تشخیص چهره دارد. اگر ویژگی‌ها ناقص یا ناکافی باشد، حتی اگر بهترین دسته‌بندی انجام شود ممکن است سیستم جواب خوبی ندهد؛ بنابراین اینکه چطور ویژگی قدرتمند را از تصویر انتخاب کنیم، باید موردتوجه قرار گیرد. برای تشخیص هر یک از بیومتریک های چهره، عنبیه چشم و اثرانگشت، فیلتر گابور محلی وزن دهی شده پیشنهاد شده است. در مرحله اول تصاویر پس از پیش‌پردازش به ۹ ناحیه مساوی تقسیم‌شده و سپس فیلتر گابور بر روی هر یک از نواحی اعمال شد تا ویژگی‌های محلی تصویر به‌دست‌آمده و در بردار ویژگی ذخیره می‌شود. سپس برای به دست آوردن وزن برای هر ناحیه از تصویر، میانگین آنتروپی را برای هر ناحیه به دست می‌آوریم. ازآنجاکه مفهوم آنتروپی، شدت تغییرات بی‌نظمی را نشان می‌دهد، هرچقدر میانگین آنتروپی یک ناحیه بیشتر باشد، نشان‌دهنده آن است که جزئیات و اهمیت آن ناحیه بیشتر است؛ بنابراین برای نواحی با میانگین آنتروپی بیشتر، وزن بیشتری در نظر گرفتیم تا دقت تشخیص جنسیت افزایش یابد. سپس در مرحله بعد با استفاده از روش SVM و اعمال وزن‌های به‌دست‌آمده در مرحله قبل به دسته‌بندی تصاویر چهره، عنبیه چشم و اثرانگشت پرداختیم. ما با استفاده از این روش‌ها و ترکیب بیومتریک های مختلف توانستیم دقت سیستم تشخیص و درنتیجه امنیت دستگاه‌های خودپرداز را بهبود دهیم. شمای کلی سیستم پیشنهادی در شکل (۲) نشان داده‌شده است. مهم‌ترین بخش در این قسمت، تشخیص عوامل مؤثر مانند تشخیص چهره، تشخیص عنبیه چشم و تشخیص اثرانگشت است که در ادامه بیشتر توضیح داده می‌شود.



شکل (۲): دیاگرام سیستم پیشنهادی

۳- پیاده‌سازی و ارزیابی

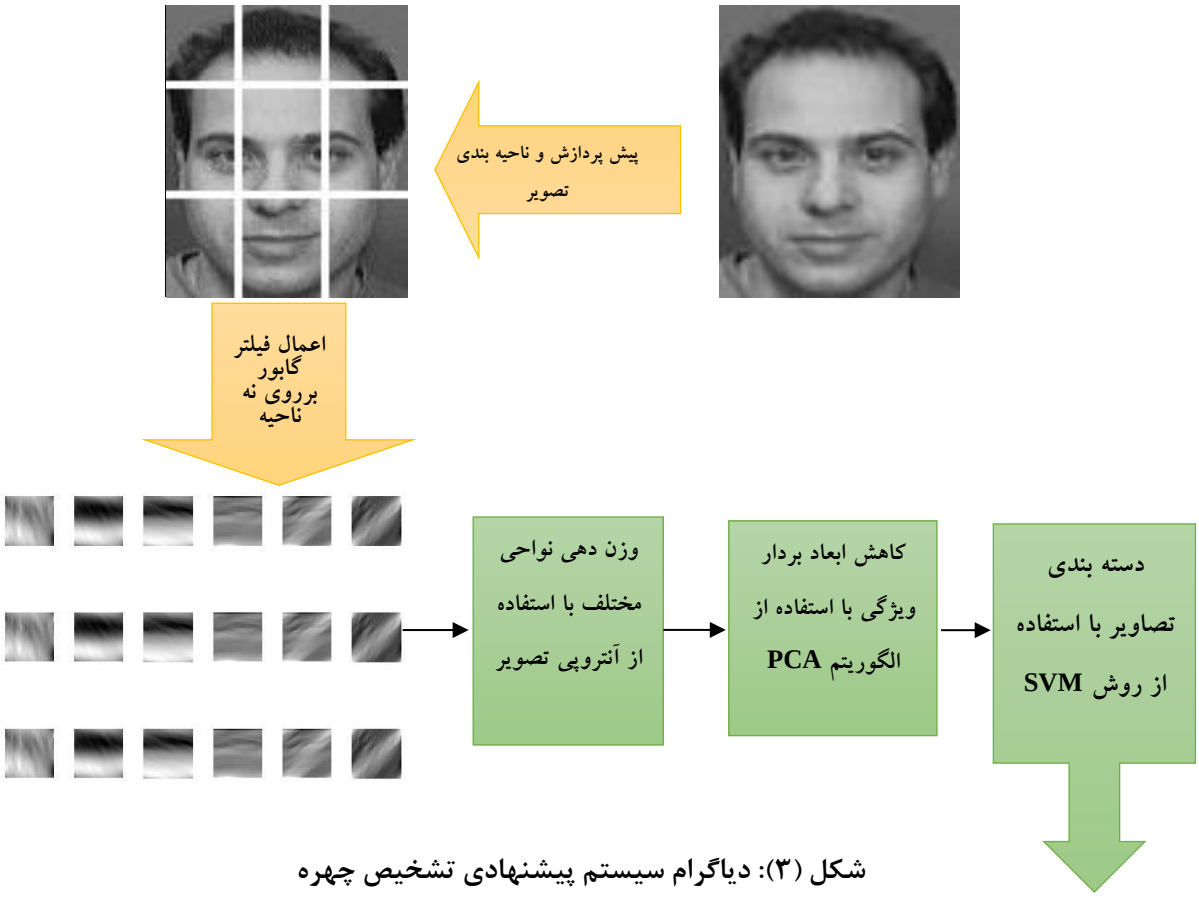
۳-۱- واردکردن کد واژه

در مرحله اول کاربر کارت را وارد دستگاه خودپرداز می‌کند، پس از شناسایی کارت و واردکردن رمز عبور، از کاربر خوا سته می شود که کد واژه خود را که می‌تواند کد ملی ا شخاص با شد، وارد کند. کاربر کد واژه را وارد می‌کند، اگر چنین

کد واژه‌ای در پایگاه داده سیستم بانک وجود داشته باشد، کاربر وارد مرحله بعد که مرحله تشخیص چهره است می‌شود، در غیر این صورت اگر کد واژه اشتباه باشد، اگر کمتر از سه بار است که کاربر برای واردکردن کد واژه تلاش می‌کند، به او اجازه داده می شود که دوباره کد واژه را وارد کند، اگر سه بار یا بیشتر کد واژه را وارد کند، کارت او به‌طور موقت مسدود می‌شود و به کاربر اخطار داده می‌شود.

۳-۱-۱- سیستم پیشنهادی تشخیص هویت از طریق چهره، عنبیه چشم و اثرانگشت

دیاگرام سیستم پیشنهادی تشخیص چهره در شکل (۳) نشان داده‌شده است. سیستم پیشنهادی تشخیص عنبیه چشم و اثرانگشت هم به‌صورت مشابه انجام می‌شود. هریک از این بخش‌ها در ادامه بیشتر توضیح داده می‌شوند.



شکل (۳): دیاگرام سیستم پیشنهادی تشخیص چهره

- **پیش‌پردازش تصویر**

به منظور ساختن یک سیستم قدرتمند برای تعیین مکان ویژگی چهره، اولین مرحله تعیین ناحیه چهره از تصویر ورودی است. از یک روش قدرتمندی که توسط ویولا[1] و جونز[2] پیشنهادشده استفاده می‌شود که در الگوریتمشان از تصاویر انتگرالی و ویژگی‌های Harr-like استفاده شده است. بعد از تعیین ناحیه چهره و قبل از استخراج ویژگی، تصویر ورودی

[1] - Viola
[2] - Jones

باید نرمالیزه شود. مراحل پیش‌پردازش به صورت زیر است: ۱. تبدیل تصویر رنگی ورودی به تصویر سطح خاکستری[3] ۲. نرمالیزه کردن تصویر چهره به‌اندازه ۲۱۰×۲۱۰ ۴. هموار کردن[4] تصویر چهره برای از بین بردن نویز.

- **ناحیه بندی تصویر**

پس از پیش‌پردازش، تصاویر باید ناحیه بندی شوند تا فیلتر گابور بر روی هر ناحیه اعمال شود؛ بنابراین تصاویر را به ۹ ناحیه مساوی تقسیم می‌کنیم تا نواحی مهم، تقریباً در یک ناحیه قرار می‌گیرند. شکل (۴)، ناحیه بندی تصویر ورودی را نشان می‌دهد. همچنین شکل (۵)، شماره نواحی مختلف تصویر چهره را نشان می‌دهد.

شکل (۴): ناحیه بندی تصویر ورودی

شکل (۵): شماره نواحی تصویر چهره

- **اعمال فیلتر گابور**

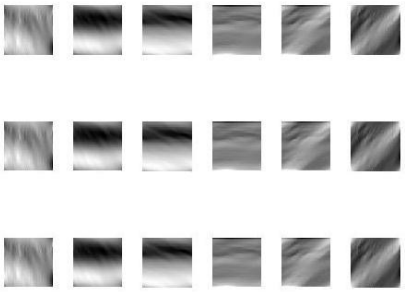
ازآنجاکه مهم‌ترین مرحله در تشخیص چهره، استخراج ویژگی‌های مهم در تصویر است، بنابراین ما در این پژوهش تمرکز زیادی به مرحله استخراج ویژگی خواهیم داشت. فیلتر گابور یکی از موفق‌ترین متد برای پردازش و استخراج ویژگی‌های تصاویر است. موجک گابور به‌طور وسیعی در کاربردهای بینایی کامپیوتر و درروشنایی مختلف کاربرد دارد؛ که برای استخراج تغییرات آشکار، مثلاً در مقیاس‌های مختلف و در زاویه‌های مختلف موردا ستفاده قرار می‌گیرد. فیلتر گابور دارای ویژگی‌های محلی بهینه در هر دو دامنه فرکانسی و مکانی است و به‌طور موفق در کاربردهای استخراج ویژگی تصویر و تشخیص الگو استفاده‌شده است. موجک گابور به‌صورت زیر محاسبه می‌شود:

$$W_{\mu,v}(z) = \frac{k_{\pi,v}^2}{\sigma^2} \exp\left(-\frac{k_{\pi,v}^2 z^2}{2\sigma^2}\right) * \left[\exp\left(ik_{\pi,v} * z\right) - \exp\left(-\frac{\sigma^2}{2}\right)\right] \quad (۱)$$

[3] - gray-level
[4] -smoothing

$$k_{\pi,v} = k_v e^{i\varphi_u} \quad (۲)$$
$$k_v = \frac{k_{max}}{f^v},\ \ f = \sqrt{2},\ \varphi_\pi = \mu\pi/n$$
$$\mu = 0,1,\dots 5,\ \ v = 0,1,2$$

Z=(x,y) مختصات x,y از منحنی است و سیگما انحراف معیار از پنجره گوسین است. سه پارامتر برای فیلتر گابور وجود دارد: مکان[5]، فرکانس و زاویه. μ,v زاویه و مقیاسی برای فیلتر گابور به‌حساب می‌آید. k_{max} مقدار ماکزیمم فرکانس و f^v فرکانس خاص بین دامنه فرکانس اســـت (ژانگ و همکاران، ۲۰۱۴)؛ بنابراین با توجه به فرمول‌های بالا فیلتر گابور ۱۸ تا تصویر در زاویه و فرکانس‌های مختلف ایجاد می‌کند. موجک گابور از convolution تصویر ورودی و تبدیل گابور به وجود می‌آید. بر اســـاس طرح انتگرال و تبدیل دوبعدی گابور، ویژگی‌های چهره به دســـت می‌آید. ما فرکانس $v = 0,1,2$ و زاویه، $\mu = \frac{\pi}{6}, \frac{2\pi}{6}, \frac{3\pi}{6}, \frac{4\pi}{6}, \frac{5\pi}{6}, \pi$ را برای این تبدیل در نظر می‌گیریم. ما در این کار، پس‌ازاینکه ناحیه صورت را به ۹ ناحیه مساوی تقسیم کردیم، بر روی هر ناحیه فیلتر گابور را اعمال می‌کنیم. شکل (۶) اعمال فیلتر گابور بر روی یکی از ۹ ناحیه را نشان می‌دهد.



شکل (۶): اعمال فیلتر گابور بر روی یکی از ۹ ناحیه

- **وزن دهی نواحی مختلف تصویر**

الف تعیین آنتروپی نواحی مختلف تصویر

در مرحله قبل، ویژگی‌های ناحیه‌های مختلف تصـــویر را به دســـت آوردیم. در این بخش، به‌منظور تعیین وزن، میانگین آنتروپی هر یک از نواحی را به دست خواهیم آورد.

بر ا ساس نظریه شانون (بانسال[6] و همکاران، ۲۰۱۶) مقدار اطلاعات متغیر تصادفی گسسته X(x1,x2,…,xs)، با احتمال P(X) (p(x1),p(x2), …, p(xs))، به‌وسیله آنتروپی H(x) به‌صورت زیر تعریف می‌شود:

$$H(x) = \sum_{i=1}^{s} p(x_i) \log\left(\frac{1}{p(x_i)}\right) = -\sum_{i=1}^{s} p(x_i)\log(p(x_i)) \quad (۳)$$

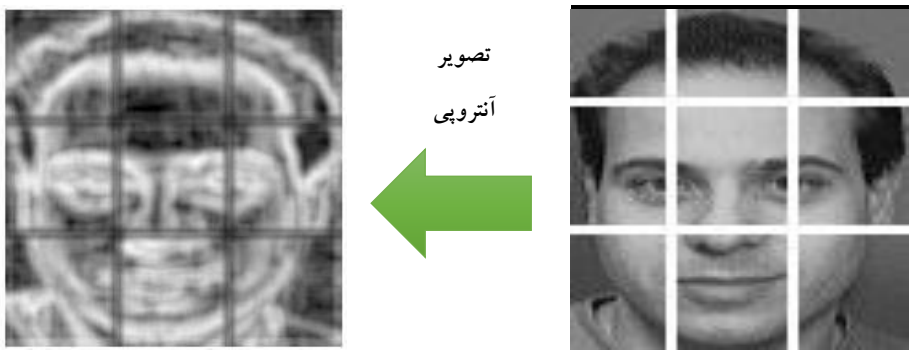
برای یک تصویر دیجیتال f(x,y)، آنتروپی تصویر به‌صورت زیر تعریف می‌شود:

[5] -location
[6] - Bansal

$$H\left[f\left(x,y\right)\right] = -\sum_{i=1}^{s} P_i \log(P_i) \qquad (۴)$$

به‌طوری‌که P_i، احتمال i امین مقدار سطح خاکستری و s، تعداد کل مقدار سطح خاکستری می‌باشد.

برای به دست آوردن تصاویر آنتروپی مربوط به هر یک از نواحی تصویر، از رابطه (۴) استفاده می‌کنیم. شکل (۷)، تصویر آنتروپی مربوط به یک تصویر چهره ورودی را نشان می‌دهد.

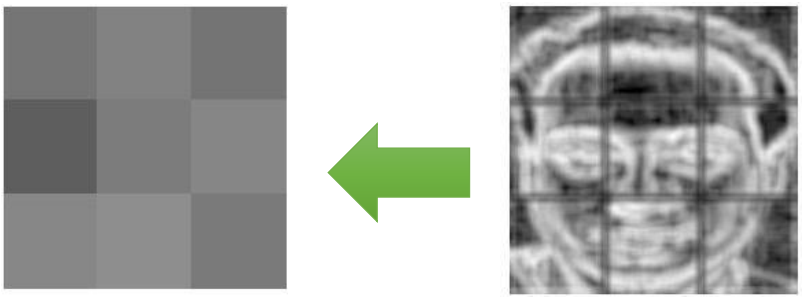


شکل (۷): تصویر آنتروپی مربوط به نواحی مختلف تصویر

همان‌طور که ملاحظه می‌کنید، شکل (۸) تصویر آنتروپی مربوط به نواحی مختلف تصویر چهره را نشان می‌دهد.

ب تعیین وزن نواحی با استفاده از آنتروپی

همان‌طور که در بخش قبل شرح داده شد، تصویر آنتروپی یک تصویر ورودی چهره را به دست آوردیم. ازآنجاکه مفهوم آنتروپی، شدت تغییرات بی‌نظمی را نشان می‌دهد، هرچقدر میانگین آنتروپی یک ناحیه بیشتر باشد، نشان‌دهنده آن است که جزئیات و اهمیت آن ناحیه بیشتر است. شکل (۳-۱۰) میانگین آنتروپی مربوط به نواحی مختلف تصویر را نشان می‌دهد.



شکل (۸): میانگین آنتروپی مربوط به نواحی مختلف تصویر

بنابراین زمانی که می‌خواهیم از فیلتر گابور برای استخراج ویژگی نواحی مختلف استفاده کنیم، برای نواحی با جزئیات بیشتر، از پارامتر مرتبه بیشتر استفاده می‌کنیم تا جزئیات نواحی بااهمیت بیشتر، بهتر نمایش داده شوند.

- **اعمال الگوریتم آنالیز اجزای اصلی (PCA[7])**

آنالیز مؤلفه اصلی یاPCA، یک تکنیک است که برای کاهش ابعاد فضای ویژگی مورداستفاده قرار می‌گیرد. PCA، یک مجموعه داده را می‌گیرد و یک زیر فضای خطی با بعد کمتر می سازد که در این حالت واریانس نقاط داده از مقدار میانگین بهتر شرح داده می شود. PCA، یک تبدیل خطی ا ست که برای ساده کردن یک مجموعه داده چندبعدی به یک مجموعه داده با ابعاد کمتر مورداستفاده قرار می‌گیرد. با استفاده از PCA، مرتبه پائین مؤلفه‌های اصلی حفظ می‌شوند و مرتبه بالای مؤلفه‌ها حذف می‌شوند، با این کار، آن دسته از مجموعه داده‌ها که بیشتر واریانس را توزیع می‌کنند، حفظ می‌شوند (ریچا[8] و همکاران، ۲۰۱۵).

مزیتی که PCA نسبت به یک تبدیل خطی بهینه دارد، این ا ست که زیر فضایی که بزرگ‌ترین واریانس را دارد، حفظ می‌شود. برخلاف دیگر تبدیلات خطی، PCA یک مجموعه ثابت از بردارهای پایه ندارد و بردارهای پایه‌اش به مجموعه داده وابسته هستند. در این پژوهش، تابع princomp برنامه متلب، مورداستفاده قرار می‌گیرد تا ابعاد بردار ویژگی را کاهش دهد. طول بردار ویژگی ۱۶۲۰۰ است. با اعمال این الگوریتم و با توجه به داشتن ۹ ناحیه برای هر تصویر چهره، درنهایت طول هر بردار ویژگی ۸۰۰۰ خواهد شد.

- **دسته‌بندی تصاویر با استفاده از روش ماشین بردار پشتیبان[9]**

SVM یک ابزار پردازشی غیرخطی داده است که در تعداد زیادی فیلدها مانند تشخیص ضایعه پوستی، تشخیص چهره، یادگیری پایگاه داده و تشخیص درستی، دسته‌بندی متن موفق بوده است، زیرا از سقوط در مینیمم نقطه محلی آشکارشده در روش‌های قدیمی جلوگیری می‌کند؛ و یکی از تکنیک‌های موفق و قوی برای د سته‌بندی چهره ا ست و برای ت شخیص چهره با استفاده از بردار ویژگی‌های استخراج‌شده عمل می کند. این روش ازجمله روش‌های نسبتاً جدیدی است که در سال‌های اخیر کارایی خوبی نسبت به روش‌های قدیمی‌تر برای طبقه‌بندی ازجمله شبکه‌های عصبی پرسپترون و نزدیک‌ترین هم سایه نشان داده ا ست. برخلاف شبکه های ع صبی در ماکزیمم های محلی گیر نمی‌افتد. برای داده‌های با ابعاد بالا تقریباً خوب جواب می‌دهد .مصالحه بین پیچیدگی دسته‌بندی کننده و میزان خطا به‌طور واضح کنترل می‌شود.

SVM یک نقشه مجازی از داده‌ها را در یک ابعاد بزرگ که ممکن ا ست نامحدود با شد به‌عنوان فضای ویژگی نمایش می‌دهد و سپس یک نقشه جداکننده خطی را برای جدا کردن داده‌ها در یک فضایی با ابعاد بزرگ جستجو می‌کند. SVM توانایی تعمیم و کارایی بالایی در نمونه‌های کوچک و غیرخطی و ابعاد بالا دارد.

مبنای کاری دسته‌بندی کننده SVM دسته‌بندی خطی داده‌ها است و در تقسیم خطی داده‌ها سعی می‌کنیم خطی را انتخاب کنیم که حا شیه اطمینان بیشتری دا شته با شد. حل معادله پیدا کردن خط بهینه برای داده‌ها به‌و سیله روش‌های QPکه روش‌های شناخته شده‌ای در حل م سائل محدودیت دار هستند صورت می‌گیرد. قبل از تقسیم خطی برای اینکه ماشین بتواند داده‌های با پیچیدگی بالا را دسته‌بندی کند داده‌ها را به‌وسیله تابع ph به فضای با ابعاد خیلی بالاتر می‌بریم. برای اینکه بتوانیم م سئله ابعاد خیلی بالا را با ا ستفاده از این روش‌ها حل کنیم از قضیه دوگانی لاگرانژ برای تبدیلِ م سئله

[7] -principal component analysis
[8] - Reecha
[9] -support vector machine

مینیمم‌سازی موردنظر به فرم دوگانی آن‌که در آن به‌جای تابع پیچیده phi که ما را به فضایی با ابعاد بالا می‌برد، تابع ساده‌تری به نام تابع هسته که ضرب برداری تابع phi است، استفاده می‌کنیم.

۳-۲- مراحل پیاده‌سازی و تابع‌های مورداستفاده

در این قسمت مراحل پیاده‌سازی و تابع‌های بکار گرفته‌شده ارائه می‌شود:

الف واردکردن کد واژه و تأیید آن: در قسمت واردکردن کد واژه و تأیید آن برای هر شخص یک کد واژه تعریف کردیم. در اینجا ۱۰ شخص متفاوت داریم که برای هر ۱۰ شخص کد واژه ۱۰۰ تا ۱۰۹ اختصاص دادیم.

ب تشخیص چهره و تطبیق آن با کد واژه: در این قسمت چهره شخص شناسایی می‌شود و با کد واژه تطبیق داده می‌شود. مراحل تشخیص چهره و تابع‌های بکار رفته شده به‌صورت زیر است:

- مرحله پیش‌پردازش تصویر چهره: در این قسمت ابتدا تصویر با استفاده از دستور rgb2gray به فضای رنگی خاکستری برده می‌شود و سپس با استفاده از دستور imresize تغییر اندازه داده می‌شود و سپس با استفاده از دستور imfilter هموارسازی می‌شود.
- مرحله ناحیه بندی تصویر: در این مرحله تصویر به ۹ ناحیه مساوی تقسیم می‌شود.
- مرحله استخراج ویژگی با استفاده از الگوریتم فیلتر گابور: استخراج ویژگی با استفاده از فیلتر گابور انجام می‌شود. این کار با تابع استفاده از GabFilter اجرا می‌شود.
- مرحله وزن دهی نواحی مختلف با استفاده از آنتروپی: در این مرحله آنتروپی هر یک از نواحی با استفاده از تابع I_entropy و سپس میانگین آنتروپی هر یک از نواحی به‌منظور به دست آوردن وزن هر یک از نواحی با استفاده از دستور mean انجام می شود. در مرحله بعد وزن هر یک از نواحی در خروجی فیلتر گابور هر یک از نواحی ضرب می‌شود. طول بردار ویژگی به‌دست‌آمده برای یک تصویر ۱۶۲۰۰ می‌باشد.
- مرحله کاهش ابعاد بردار ویژگی با استفاده از الگوریتم PCA: در این مرحله از بین ۱۶۲۰۰ ویژگی استخراج‌شده ۸۰۰۰ تا از بهترین ویژگی با استفاده از دستور princom انتخاب می‌شود.
- مرحله دسته‌بندی و یا تشخیص با استفاده از دسته‌بند SVM: دسته‌بندی یا تشخیص چهره با استفاده از دستورsvmtrain و svmclassify به ترتیب به‌منظور آموزش تصاویر و دسته‌بندی بردار ویژگی به‌منظور تشخیص استفاده می‌شود.

ج تشخیص عنبیه چشم: در این مرحله بعد از تأیید چهره عنبیه چشم متناظر با چهره تشخیص داده می شود و با کد واژه تطبیق داده می‌شود. تمام مراحل تشخیص عنبیه چشم مانند مراحل تشخیص چهره (موارد بالا) می‌باشد.

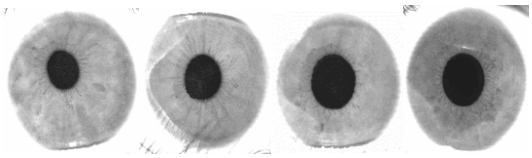
د تشخیص اثرانگشت: در این مرحله بعد از تأیید چهره و عنبیه چشم، اثرانگشت متناظر با چهره و عنبیه چشم تشخیص داده می شود و با کد واژه تطبیق داده می شود. تمام مراحل تشخیص اثرانگشت مانند مراحل تشخیص چهره (موارد بالا) می‌باشد.

و بعد از تأیید ۴ مرحله تأیید کد واژه، تشخیص چهره، عنبیه چشم و اثرانگشت، حساب و تراکنش بانکی برای کاربر باز می‌شود.

- **مجموعه داده‌های مورداستفاده**

ما در این پژوهش از پایگاه داده تصـــاویر چهره به نام ORLپایگاه داده عنبیه چشـــم به نام iris و پایگاه داده اثرانگشت به نام fingerprint استفاده می‌کنیم. پایگاه داده ORL شامل ۱۰۰ تصویر چهره مربوط به ۱۰ فرد متفاوت اســت. برای هر فرد ۱۰ تصــاویر متفاوت در حالت‌های مختلف ارائه‌شــده اســت. شــکل (۴-۱) نمونه‌هایی از پایگاه داده ORL را نشان می‌دهد. پایگاه داده عنبیه چشم نیز شامل ۱۰۰ تصویر از ۱۰ شخص متفاوت با ۱۰ تصاویر متفاوت برای هر عنبیه است. پایگاه داده اثرانگشت نیز شامل ۱۰۰ تصویر است؛ که این پایگاه داده مربوط به ۱۰ فرد متفاوت است. برای هر فرد ۱۰ تصاویر متفاوت از انگشت فرد ارائه‌شده است. شکل (۹) و شکل (۱۰) و شکل (۱۱) به ترتیب نمونه‌هایی از تصاویر پایگاه داده تصویر فرد، عنبیه چشم و اثرانگشت را نشان می‌دهد.

شکل (۹): نمونه‌هایی از تصاویر پایگاه داده ORL



شکل (۱۰): نمونه‌هایی از تصاویر پایگاه داده Iris

شکل (۱۱): نمونه‌هایی از تصاویر پایگاه داده Fingerprint

۳-۳- ارزیابی کارایی رویکرد سیستم پیشنهادی

ابتدا کد واژه که می‌تواند کد ملی فرد با شد در د ستگاه ATM تو سط فرد وارد می شود، سپس بعد از تأیید کد واژه و وجود دا شتن کد واژه در پایگاه داده‌های بانک مربوطه، وارد مرحله ت شخیص چهره می شویم، در این مرحله چهره شخص شنا سایی می شود، اگر چنین شخ صی در پایگاه داده بانک مربوطه وجود دا شته با شد و اگر کد واژه وارد شده با شخص

شناسایی شده مطابقت داشته باشد، وارد تشخیص عنبیه چشم می شویم، بعد از تأیید عنبیه چشم با شخص موردنظر اثرانگشت شخص موردبررسی قرار می‌گیرد، بعد از تأیید اثرانگشت با شخص موردنظر حساب کاربری شخص باز شده و تراکنش بانکی موردنظر شخص انجام می‌شود؛ بنابراین در این پژوهش بیشتر تمرکز بر روی تشخیص درست و دقیق چهره، عنبیه چشم و اثرانگشت شخص می‌باشد.

جدول (۲) بیومتریک های مختلف را با استفاده از یکسری معیارها باهم مقایسه می‌کند. استفاده از ترکیب چهره، عنبیه چشم و اثرانگشت مقاومت، کارایی، دقت نسبتاً خوبی نسبت به دیگر بیومتریک ها دارد.

جدول (۲): مقایسه بیومتریک های مختلف

بیومتری های مختلف	هزینه محاسبات	دقت	کارایی	نقص‌ها	مقاومت و پایداری
عنبیه چشم	بالا	بالا	بالا	نورپردازی	بالا
شبکیه چشم	بالا	بالا	بالا	عینک	متوسط
چهره	متوسط	متوسط	متوسط	سن	متوسط
اثرانگشت	پایین	متوسط	متوسط	کثیف بودن، خشکی پوست	بالا
ترکیب چهره، عنبیه چشم و اثرانگشت	متوسط	بالا	بالا	-	بالا

جدول (۳) دقت روش پیشنهادی را با بیومتریک های مختلف نشان می‌دهد. این جدول نشان می‌دهد که روش پیشنهادی با ترکیب سه بیومتریک چهره، عنبیه چشم و اثرانگشت دقت و کارایی بالاتری دارد.

جدول (۳): مقایسه دقت روش پیشنهادی با بیومتریک های مختلف

روش پیشنهادی با بیومتریک های مختلف	دقت تشخیص (٪)
ترکیب کد واژه با چهره	٪۹۰
ترکیب کد واژه با عنبیه چشم	٪۹۳
ترکیب کد واژه با اثرانگشت	٪۹۰
ترکیب کد واژه با چهره، عنبیه چشم و اثرانگشت	٪۹۶

در ابتدا سیستم پیشنهادی در دو حالت موردبررسی قرار می‌گیرد. در حالت اول ۷۰٪ تصاویر را به‌عنوان داده‌های آموزش و ۳۰٪ باقیمانده را برای تست در نظر گرفتیم (از ۱۰ تصویر مربوط به یک شخص، ۷ تصویر را به‌عنوان آموزش و۳ تصویر باقیمانده را به‌عنوان تصویر تست در نظر می‌گیریم). در حالت دوم ۳۰٪ تصاویر را به‌عنوان داده‌های آموزش و۷۰٪ را برای تست در نظر گرفتیم. در این دو حالت تصاویر به صورت تصادفی انتخاب شده است. نتایج در جدول (۴) نشان داده‌شده است.

جدول (۴) مقایسه روش‌های پیشنهادی در حالت‌های مختلف

دقت روش پیشنهادی (٪)	حالت‌های مختلف
٪۸۶	٪۳۰ آموزش-٪۷۰ تست
٪۹۶	٪۷۰ آموزش-٪۳۰ تست

جدول (۵) دقت تشخیص روش پیشنهادی را با دیگر روش‌های پیشین مقایسه می‌کند، نتایج آزمایش‌های نشان می‌دهد روش پیشنهادی از دقت قابل قبولی نسبت به دیگر روش‌ها برخوردار است.

جدول (۵): مقایسه دقت بازشناسی روش پیشنهادی با دیگر روش‌ها

دقت تشخیص (٪)	روش‌های مختلف
٪۹۶	روش پیشنهادی
٪۹۱	تشخیص چهره با استفاده از LBP به‌منظور امنیت دستگاه‌های خودپرداز (درمان و همکارن، ۲۰۱۳)

برای ارزیابی روش پیشنهادی از دو معیار ارزیابی میزان پذیرش اشتباه (FAR[1]) و میزان رد کردن اشتباه (FRR[2]) استفاده می‌کنیم. این دو معیار در ادامه شرح داده می‌شود

- میزان پذیرش اشتباه

احتمال اینکه سیستم، فردی را اشتباه تشخیص دهد، یا یک فرد غاصب را پذیرش کند، به دست می‌آید و با استفاده از دو نوع نرخ خطابه دست می‌آید.

$$\text{میزان پذیرش اشتباه} = \frac{\text{تعداد پذیرش اشتباه}}{\text{تعداد سوء قصد داشتن فرد غاصب}} \quad (۵)$$

- میزان رد کردن اشتباه

احتمال اینکه سیستم فردی را اشتباه تشخیص دهد، تعریف می‌شود و به‌صورت زیر به دست می‌آید.

$$\text{میزان رد کردن اشتباه} = \frac{\text{تعداد رد کردن اشتباه}}{\text{تعداد تلاش تشخیص‌های}} \quad (۶)$$

جدول (۶) FRR و FAR روش پیشنهادی را نشان دهد. این جدول نشان می‌دهد که FAR یا میزان پذیرش اشتباه یعنی فرد را به‌اشتباه قبول کردن و حساب کاربری مربوطه را باز کردن، صفر است، یعنی روش پیشنهادی ما فردی را با اشتباه وارد سیستم نمی‌کند. FRR یا میزان رد کردن اشتباه در سیستم پیشنهادی ۰,۰۳ است، یعنی یک فرد را سیستم پیشنهادی به‌اشتباه رد می‌کند و حساب کاربری‌شان را باز نمی‌کند.

جدول (۶): مقایسه FRR و FAR روش پیشنهادی

میزان رد کردن اشتباه (FRR)	میزان پذیرش اشتباه (FAR)	روش-معیار ارزیابی
۰,۰۳	۰	روش پیشنهادی

۴- نتیجه‌گیری

در جهان مدرن تعداد زیادی از ما از دستگاه خودپرداز استفاده می‌کنیم. رشد سریع تکنولوژی بانک‌ها مزیت و معایبی برای فعالیت‌ها و تراکنش‌های بانکی در دستگاه‌های خودپرداز دارد. دستگاه خودپرداز یک ماشین الکترونیکی بانکی هستند که در مکان‌های مختلف وجود دارد و مشتریان می‌توانند تراکنش‌هایی را بدون کمک کارمند بانک انجام دهند. با کمک دستگاه خودپرداز، کاربر می‌تواند چندین فعالیت بانکی مانند انتقال وجه، دریافت وجه و پرداخت‌های مختلف را انجام دهد. این عمل برای کاربران مناسب است تا به‌حساب های بانکی‌شان دسترسی داشته باشند و تراکنش‌های مالی را انجام دهند. گیرنده حساب، فرض خواهد شد که کارت دستگاه خودپرداز و گذرواژه باشد. گذرواژه یا پسورد، در سیستم دستگاه خودپرداز خیلی مهم است که اکثراً برای امنیت و حفظ اطلاعات مالی مشتریان استفاده می‌شود. گذرواژه باید توسط کاربر یا مشتری به خاطر سپرده شود. جرائمی که در دستگاه خودپرداز اتفاق می‌افتد، بحث جدی است که نه‌تنها کاربران را تحت تأثیر قرار می‌دهد، بلکه متصدیان بانک‌ها نیز تحت تأثیر آن قرار می‌گیرند.

برای غلبه بر مسائل دزدی و سرقت در دستگاه‌های خودپرداز، یک مدل ترکیبی شامل ویژگی‌های مرسوم با ویژگی‌های اضافی مانند تشخیص چهره و رمز عبور مانند کد ملی استفاده می‌شود. پایگاه داده اطلاعاتی درباره جزئیات حساب کاربر، تصویر چهره کاربر و شماره موبایل و کد ملی کاربر را به‌منظور بهبود امنیت دارا است. ابتدا کاربر کارت را وارد دستگاه می‌کند، سپس تصویر زنده کاربر به‌طور اتوماتیک از طریق دوربین نصب شده بر روی دستگاه خودپرداز گرفته می‌شود و با تصویر ذخیره‌شده در پایگاه داده مقایسه می‌شود، اگر مطابقت داشت، کد واژه وارد می‌شود. این کد توسط کاربر در دستگاه خودپرداز وارد می‌شود. اگر کاربر کد واژه را درست وارد کند، تراکنش با موفقیت انجام می‌شود؛ بنابراین، ترکیب تشخیص چهره و کد واژه احتمال کلاه‌برداری را کاهش می‌دهد؛ بنابراین از ترکیب چهره، عنبیه چشم و اثرانگشت به‌عنوان تشخیص هویت کاربر استفاده می‌شود. ما در این پژوهش روشی مؤثر، کارا و با دقتی بالا به‌منظور تشخیص هویت از طریق ترکیب چهره، عنبیه چشم و اثرانگشت ارائه دادیم

یک سیستم تعیین هویت با استفاده از ویژگی تصویر چهره به‌طورمعمول کار خود را در چند مرحله انجام می‌دهد:۱ اخذ اطلاعات ۲ پیش‌پردازش ۳ استخراج ویژگی‌ها ۴ دسته‌بندی.

روش‌های تشخیص بر مبنای ترکیب چهره، عنبیه چشم و اثرانگشت عموماً مبتنی بر ویژگی هستند این روش‌ها دارای دقت بالایی می‌با شند درعین‌حال دارای پیچیدگی و سرعت اجرای پایین می‌با شند و اجزای صورت و نقاط خاص به‌عنوان ویژگی اســتفاده می‌کنند، ازآنجایی‌که این روش‌ها بروی تصــاویر باکیفیت و وضــوح‌بالا باید انجام شــود، بنابراین نیاز به اسکنرهای پیچیده می‌باشد و این امر ازلحاظ تجاری در سطح گسترده مقرون‌به‌صرفه نمی‌باشد. در این پژوهش به تعیین با استفاده از تصاویر با وضوح پایین از چهره، عنبیه چشم و اثرانگشت پرداختیم. درواقع مشکلات ذکرشده در بالا سبب شد تا به دنبال رو شی با شم که برای تصویر با دقت بالا و پیچیدگی کم منا سب با شد و درواقع هرچه تصاویر در کیفیت پایین‌تر پاسخ گوی باشد سیستم‌های زیست‌سنجی ازلحاظ تجاری مقرون‌به‌صرفه تر خواهد بود.

یکی از مراحل پیچیده و زمان‌بر در سیستم تشخیص هویت از طریق چهره، عنبیه چشم و اثرانگشت مرحله استخراج ویژگی است که دقت نهایی این سیستم به‌طور مستقیم به‌دقت الگوریتم‌های ارائه شده در این مرحله بستگی دارد. تاکنون کارهای زیادی در این راســتا انجام‌شــده اســت و هریک دارای معایب و مزایایی بوده‌اند. اکثر این روش‌ها دارای معایبی می‌باشند. فیلتر گابور، یکی از بهترین توصیفگرهایی است که می‌توان در مرحله استخراج ویژگی از آن استفاده نمود. لذا در این پایان‌نامه سعی شده است تا با استفاده از این توصیفگر، سیستم تشخیص چهره، عنبیه چشم و اثرانگشت را در مقابل برخی از این مشــکلات پایدار نماییم. ما در این پژوهش، یک ســیســتم تشــخیص هویت از طریق چهره، عنبیه چشــم و اثرانگشت مبتنی بر فیلتر گابور به صورت محلی وزن‌دار شده بر روی تصاویر ایستا ارائه کردیم. استفاده از رویکرد محلی وزن‌دار شده درروش پیشنهادی موجب شده است تا به بعضی از نواحی در تصویر وزن بیشتری داده شود و درنهایت این عمل منجر به افزایش نرخ تشــخیص شــود. همچنین در این پژوهش با اســتفاده از آنتروپی تصــویر و ناحیه بندی کردن آن توانســتیم تا برای هر ناحیه، وزن جداگانه تعیین کنیم. هرچقدر میانگین آنتروپی یک ناحیه از تصــویر بیشــتر باشــد، نشان‌دهنده آن است که آن ناحیه از تصویر دارای اهمیت و جزئیات بیشتری است؛ بنابراین با توجه به این مسئله و اهمیت نواحی، وزن هر ناحیه را تعیین کردیم. همان‌طور که نتایج نشــان می‌دهد اعمال وزن بر روی هر یک از نواحی منجر به افزایش دقت سیستم تشخیص از طریق چهره شده است.

سرانجام برای ارزیابی روش پیشنهادی، به مقایسه روش‌های مختلف با سیستم پیشنهادی پرداختیم. همچنین روش پیشــنهادی را در حالت‌های مختلف مورد ارزیابی قراردادیم. نتایج آزمایش‌های نشــان می‌دهد که ســیســتم پیشــنهادی در مقایسه با دیگر روش‌ها، بهبود قابل‌توجهی در دقت سیستم تشخیص و درنتیجه امنیت دستگاه‌های خودپرداز داشته است.

فهرست منابع

1. Geethanjali, N, and K.Thamaraiselvi, (2013), “Enhancing the Security of Biometrics in ATM”, International Journal of Scientific & Engineering Research, Volume 4, Issue 4, pp. 1192-1198.
2. Oko, s. and Jane Oruh. (2012), “ENHANCED ATM SECURITY SYSTEM USING BIOMETRICS”, IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 5, No 3. pp. 352-357.
3. Diebold I. (2002), “ATM fraud and security”, White Paper, New York.
4. Tiago Duarte, João Paulo Pimentão, Pedro Sousa, Sérgio Onofre, (2016), “Biometric access control systems: A review on technologies to improve their efficiency”, Power Electronics and Motion Control Conference (PEMC), 2016 IEEE International.

5. J.Wayman, A.Jain, D.Maltoni and D.Maio, (2005), "Biometric SystemsTechnology", Design and Performance Evaluation; © Springer-Verlag London Limited.

6. Battista Biggio, Giorgio Fumera, Paolo Russu_, Luca Didaci_, Fabio Roli, (2015), "Adversarial Biometric Recognition: A review on biometric system security from the adversarial machine-learning perspective", IEEE Signal Processing Magazine (Volume: 32, Issue: 5, Sept. 2015).
7. Ishan Nigam, Mayank Vatsa, Richa Singh, (2015), "Ocular biometrics: A survey of modalities and fusion approaches", Information Fusion (2015), doi: http://dx.doi.org/10.1016/j.inffus.2015.03.005.
8. Ravi Ahluwalia, (2016), "Banking's biometric future", Available online 2016 Elsevier.
9. Mohsin Karovaliya, Saifali Karedia, Sharad Oza, Dr.D.R.Kalbande, (2015), "Enhanced security for ATM machine with OTP and Facial recognition features»,International Conference on Advanced Computing Technologies and Applications (ICACTA-2015).

10. Ekberjan Derman, Y. Koray Gecici, Albert Ali Salah, (2013), "SHORT TERM FACE RECOGNITION FOR AUTOMATIC TELLER MACHINE (ATM) USERS", ICECCO.

11. O.A.Esan, S.M.Ngwira, I.O.Osunmakinde, (2013), "Bimodal Biometrics for Financial Infrastructure Security", Information Security for South Africa.
12. G. Renee Jebaline, S. Gomathi, (2015), "A Novel Method to Enhance the Security of ATM using Biometrics", International Conference on Circuit, Power and Computing Technologies [ICCPCT].
13. K John Peter, G.Nagarajan, G.Gimini Sahaya Glory, Sanjana Devi.V.V, Dr S.Arguman, Dr. K Sentamarai Kannan, (2011), "IMPROVING ATM SECURITY VIA FACE RECOGNITION", Electronics Computer Technology (ICECT), 3rd International Conference on 8-10 April.
14. Rajesh.V, Vishnupriya.S, (2014), "IBIO-A New Approach/or ATM Banking System", Iternational Conference on Electronics and Communication Systems(ICECS-2014),Feb.13 - 14,2014,Coimbatore,INDIA.
15. Gaurav Bhatnagar, Jonathan Wu, Balasubramanian Raman, (2012), "Fractional dual tree complex wavelet transform and its application to biometric security during communication and transmission", Future Generation Computer Systems.
16. Ligang Zhang, Dian Tjondronegoro, Vinod Chandran, "Random Gabor based templates for facial expression recognition in images with facial occlusion", Neurocomputing (2014), http://dx.doi.org/10.1016/j.neucom.2014.05.008.
17. Reecha Sharma, M.S. Patterh, "A new pose invariant face recognition system using PCA and ANFIS", Optik - International Journal for Light and Electron Optics, Volume 126, Issue 23, December 2015, Pages 3483–3487.
18. Mamta Bansal, Madasu Hanmandlu, "A new entropy function for feature extraction with the refined scores as a classifier for the unconstrained ear verification,Journal of Electrical Systems and Information Technology, 8 November 2016.
19. Ekberjan Derman, Y. Koray Gecici, Albert Ali Salah, 2013, SHORT TERM FACE RECOGNITION FOR AUTOMATIC TELLER MACHINE (ATM) USERS, IEEE, ICECCO.

۲۰. ترکمانی، محمدعلی؛ سید حسین احمدی؛ علی بیات و محمدرضا خدابخشی،۱۳۳۲ ، طراحی و ساخت دستگاه خودپرداز ATM مجهز به حسگر اثرانگشت و مودمGSM ، بیست و یکمین کنفرانس مهندسی برق ایران، مشهد، دانشگاه فردوسی مشهد.

۲۱. پایه‌دار، ساسان؛ زینب حسن‌پور و ابراهیم رشیدی،۱۳۳۲ ، آشنایی با استفاده از متدهای بیومتریک احراز هویت در دستگاه‌های خودپرداز، اولین همایش ملی رویکردهای نوین در مهندسی کامپیوتر و بازیابی اطلاعات، رودسر، دانشگاه آزاد اسلامی واحد رودسر و املش .