ششمین کنفرانس بین المللی انجمن رمز ایران
۱۵ و ۱۶ مهر ماه ۱۳۸۸، دانشگاه اصفهان
انجمن رمز ایران
دانشگاه اصفهان

طراحی و پیاده‌سازی یک سیستم احراز هویت با استفاده از اثر انگشت و RFID بر پایه مدل HMAX *

نرگس پیروی[۱]، شهرام جعفری [۲]

[۱] دانشگاه آزاد اسلامی واحد زرقان
narges.peyravi@gmail.com
[۲] دانشکده مهندسی برق و کامپیوتر دانشگاه شیراز
jafaris@shirazu.ac.ir

چکیده

در این مقاله سیستمی جهت احراز هویت افراد، چه در فضای فیزیکی و چه در فضای سایبر پیشنهاد می‌شود تا تعاملات در محیطی امن صورت پذیرد. در این سیستم کارت بدون تماسی (contact-less)، بر پایه فناوری RFID، جهت احراز هویت صادر می‌گردد که حاوی تصاویر اثر انگشت شخص می‌باشد. سیستم در دو فاز ایجاد کارت احراز هویت و فرایند احراز هویت طراحی شده است. در این مقاله جهت پیاده‌سازی استخراج خصیصه (feature extraction) تصاویر اثر انگشت از مدل HMAX که از سیستم بیولوژیکی مغز انسان گرفته شده است استفاده کرده و پس از تست مدل بر روی ۱۰۰ تصویر اثر انگشت از مجموعه داده‌های FVC و اخذ میانگین خصیصه‌های هر تصویر دریافتیم سیستم پیشنهادی ما با حد آستانه ۰/۹ به طور ۱۰۰% قادر به پاسخ گویی می‌باشد همچنین نتایج به دست آمده نشان می‌دهد که روش پیشنهادی نسبت به مدل PCA نه تنها ضریب شناسایی بالاتری دارد بلکه این روش نسبت به تغییر مقیاس و موقعیت تصاویر، پایداری بیشتری نشان می‌دهد.

واژه‌های کلیدی

احراز هویت، اثر انگشت، کارت بدون تماسRFID ، مدل HMAX ، استخراج خصیصه (feature extraction)

۱- مقدمه

تبادل امن اطلاعات به خصوص در فضای سایبر به عنوان یکی از بحث برانگیز ترین موضوعات امنیتی مطرح است. از آنجایی که معمولا تبادلات الکترونیکی رو در رو(face to face) نیست لذا تایید هویت افراد شرکت کننده در تعاملات موضوعی در خور توجه به حساب می‌آید. مطالعات اخیر نشان مي‌دهد که دزدي هويت (theft Identity) از سوابق و صورت حساب‌ها بسیار رایج تر از قبل شده است و به علاوه تقلب اينترنتي کم هزينه تر از انواع ديگر تقلب‌هاست که اين امر اهميت توجه به سيستم‌هاي امنيتي را بيش از پيش مورد تأکيد قرار مي دهد.در این راستا، امروزه سیستم‌های بسیاری جهت این مهم طراحی و پیاده‌سازی شده اند که هر کدام محدودیت‌های خاص خود را دارا می‌باشند.[۱]

سیستم‌های سنتی تعیین یا تایید هویت مبتنی بر دانش (آنچه که فرد می‌داند مانند رمز عبور) یا مبتنی بر نشانه [۲] (آنچه که فرد در اختیار دارد مانند گذرنامه و کارت اعتباری)، نا امن، خسته کننده، وقت گیر و زمان بر، ناکارآمد و گران هستند. در واقع در سیستم‌های مبتنی بر دانش به تمامی افراد مجاز، یک شناسه تعلق می‌گیرد و شخص متناظر با آن، یک رمز عبور اتخاذ می‌کند. شخص (مجاز یا غیرمجاز) که یک شناسه را وارد می‌کند، تنها در صورتی مجاز شناخته می‌شود که از رمز عبور متناظر با آن مطلع باشد. این در حالی است که امنیت در این روش ممکن است به دلیل فاش شدن رمز عبور بر یک فرد غیرمجاز شکسته شود. به طور کلی در سیستم‌های مبتنی بر نشانه به تمامی افرادی که مجاز شناخته شده اند، یک نشانه تعلق می‌گیرد. افرادی که دارای چنین نشانه‌ای نیستند، اجازه ورود به سیستم را ندارند. ضمن آن که جایگزینی و تعویض توکنها (کارتهای مغناطیسی) به دلیل به

* این پروژه در تاریخ ۸۷/۱۰/۲۳ با شماره قرارداد ۵۰۰/۱۹۳۷۱ مورد حمایت مالی مرکز مخابرات ایران قرار گرفته است.

سرقت رفتن یا گم کردن آنها وقت گیر و گران بوده و همچنین به خاطر سپردن کلمات عبور و جلوگیری از فاش شدن آن، مشکل است.با استناد به بحثهای انجام شده در زمینه نقاط ضعف روشهای احراز هویت با به کارگیری از توکنها و کلمات عبور، از آنجا که این روشها مبتنی بر صفات ذاتی فرد نبوده و توانایی تمایز بین شخص اصلی و شخصی که به نوعی توانسته توکن یا دانش شخص مجاز را به دست آورد را دارا نیستند لذا در سالهای اخیر، توجه جامعه پژوهشی به سمت سیستم‌های بیومتریکی تعیین و تایید هویت معطوف شده است.این روش در حقیقت بر پایه آنچه شخص هست استوار است زیرا شخص مورد بررسی برای شناسایی باید خود به صورت فیزیکی در محل حضور داشته باشد.به این منظور در دو دهه گذشته، سیستم‌های بیومتریکی مبتنی بر عنبیه چشم، هندسه دست و اثر انگشت و ... توسعه یافته اند.

از آنجا که مشخصه‌های بیومتریکی فراموش نمی شوند (مانند رمز عبور)، گم نمی شوند یا به آسانی نیز نمی توان آن را به اشتراک گذاشت، رویکردی کاراتر و مطمئن تر برای حل مساله احراز هویت خواهند بود[۲]

۲- تایید هویت از طریق شاخص بیومتریک

پیشینه مطالعه و بررسی خطوط کف دست به دوران باستان برمی گردد که در ابتدا از خطوط کف دست برای پیشگویی و طالع بینی استفاده می‌شد. در بسیاری از بناها و نقاشی‌های تاریخی هندی‌ها، کف دست و خطوط موجود روی آن به چشم می‌خورد و در حدود ۳هزار سال پیش در چین، کف بینی بسیار مورد علاقه و توجه بوده است.[۲]

بحث احراز هویت دارای پیشینه ای طولانی است به طوری که در گذشته جهت مسائل پلیسی و جنایی به کار برده می‌شدند اما امروزه در امور امنیتی کاربرد بسیاری دارند.استفاده از اطلاعات بیومتریک مانند انگشت نگاری، چهره نگاری، عنبیه نگاری، هندسه دست نگاری، صوت نگاری، امضانگاری و تایپ نگاری و ... هر کدام مقوله ای مجزا و قابل بحث را در بر دارند که سالهاست مورد توجه صاحب نظران و پژوهشگران قرار گرفته است و نتایج خوبی نیز در بر داشته است.

یک سیستم بیومتریکی در واقع یک سیستم شناسایی الگواست که با تشخیص صحت خصوصیات رفتاری یا فیزیولوژیکی یک فرد به شناسایی شخص می‌پردازد. در حالت عادی، خصوصیات منحصربه فرد شخص مانند اثر انگشت، خطوط کف دست یا هندسه سه بعدی دست از طریق یک سنسور اخذ شده و به یک سیستم شناسایی الگو داده می‌شود تا نتیجه موفقیت یا شکست در بازشناسی اعلام شود. مراحل شناسایی بیومتری به چند بخش تقسیم می‌شود:

اخذ داده: داده‌های بیومتریکی (تصویر / سیگنال) از طریق یک ابزار ورودی فراهم می‌شوند.

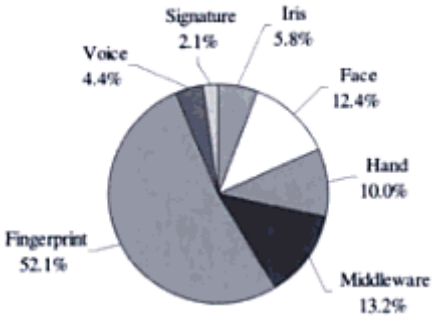
پیش پردازش تصویر / سیگنال : در این مرحله، عملیات بهسازی تصویر / سیگنال مانند تقطیع، حذف نویز، نرمالیزه کردن چرخش و انتقال انجام می‌شود.

استخراج ویژگی : منظور از ویژگی، خاصیت پایدار و منحصربه فردی است که برای چندین نمونه از یک داده بیومتریکی مربوط به یک فرد، تقریبا یکسان و برای افراد مختلف، متفاوت است.

از این ویژگی‌ها استفاده می‌شود تا برای هر فرد، یک کلیشه ایجاد شده و در پایگاه داده سیستم ذخیره شود. هنگامی که فرد جدیدی وارد سیستم می‌شود، ویژگی‌های وی استخراج شده و یک کلیشه برای او ساخته می‌شود. منظور از تطبیق، بررسی میزان شباهت کلیشه این فرد جدید با کلیشه‌هایی است که برای افراد مختلف ایجاد شده و در پایگاه داده سیستم، موجود است.

اگر میزان شباهت از یک حد آستانه ای کمتر باشد، در آن صورت، هویت این فرد جدید تصدیق می‌شود. یک سیستم بیومتریکی عموما دارای سه فاز عملیاتی ثبت اطلاعات، تعیین هویت و تایید هویت است البته برخی از سیستم‌ها فقط شامل یکی از دو حالت تعیین و تایید هویت هستند. به طور کلی قبل از آن که کاربری توسط سیستم، مورد شناسایی قرار گیرد، باید اطلاعات مربوط به آن فرد در سیستم ثبت شود. مشخصه بیومتریکی کاربر به وسیله سنسور بیومتریک، اسکن شده و پس از اعمال یک سری پردازش‌های اولیه بر تصویر خام به دست آمده، ویژگی‌هایی برای توصیف فشرده و مناسب از این نمونه، استخراج می‌شود و با توجه به نوع کاربرد، یک کلیشه برای آن کاربر ایجاد شده و در پایگاه داده سیستم ذخیره می‌شود. در حالت تعیین هویت هم، هدف آن است که از میان تعدادی هویت مرجع (کلیشه‌هایی که برای کاربران در داخل پایگاه داده سیستم ذخیره شده است)، آن مدل هویتی که نزدیکترین و بیشترین شباهت به هویت نامشخص ورودی را دارد، پیدا شود. در حقیقت هویت یک شخص را از طریق جستجو در کل پایگاه داده شناسایی می‌کند، به بیان دیگر از یک مقایسه و تطبیق یک به کل استفاده می‌شود. با توجه به این تعریف واضح است که هر چه تعداد هویتهای مرجع بیشتر باشد احتمال خطا در تعیین هویت بیشتر می‌شود.[۳] [۴]

تحقیقات صورت گرفته بر روی شاخص‌های بیومتریک نشان می‌دهند که استفاده از اثر انگشت در سیستم‌های تایید هویت به دلیل کارآمد بودن، استفاده آسان‌تر، پایداری و در دسترس بودن بیشترین استفاده را دارد. شکل (۱) درصد استفاده از شاخص‌های بیومتریک را نشان می‌دهد.[۵]



شکل ۱: درصد استفاده از شاخص‌های بیومتریک[۵]

۳- شناسایی از طریق امواج رادیویی (RFID)

شناسایی از طریق امواج رادیویی (RFID: Radio Frequency Identification) وکاربردهای آن به حدود سال ۱۹۷۰بر می‌گردد اما به دلیل قیمت بالا این وسیله تا سالهای اخیر در مصارف تجاری کاربرد زیادی نداشته است. در سال ۱۹۷۱ ماریو کاردولورسما به عنوان اولین مبدع تکنولوژی امروزی RFID شناخته شد. وی یک سیستم گیرنده و فرستنده رادیویی را برای بنادر نیویورک بکار برد.[۶]

به طور کلی یک سیستم RFID از سه قسمت زیر تشکیل شده است :

- A Scanning antenna : برای برقراری ارتباط و ارسال امواج رادیویی به برچسب.

- A Transceiver with a decoder : برای تفسیر داده‌ها.

- A Transponder (the RFID tag) : که اطلاعات لازم در آن ذخیره شده است.

RFID Tag خود از دو قسمت تشکیل شده: ۱) chip ۲)Antenna

آنتن (Scanning Antenna) امواج رادیویی را در محدوده نسبتا کوچکی منتشرمی‌کند. این امواج رادیویی دو عمل اصلی انجام می‌دهند:

۱)وسیله‌ای برای ارتباط با RFID Tag(transponder) است.

۲)انرژی مورد نیاز tag برای برقراری ارتباط را فراهم می‌کند. (در مورد tag های passive)

وقتی که یک tag در میدان الکترومغناطیسی ایجاد شده در اطراف reader قرار می‌گیرد، سیگنال‌های فعال کننده که توسط آنتن فرستاده شده‌اند، روی آن اثر گذاشته و به عبارتی تراشه RFID را بیدار می‌کند و این تراشه اطلاعات موجود در tag را در اختیار آنتن قرار می‌دهد. نقش transceiver در این عملیات کنترل خطوط ارتباطی وداده‌ها است.

در واقع یک دستگاه reader ترکیبی است از یک scanning antenna و transceiver.

به طور کلی سه نوع RFID tag وجود دارد که عبارتند از:

- Tagهای Passive : این نوع tagها هیچ منبع تولید انرژی درونی ندارند و انرژی خود را از طریق سیگنال‌های RF که توسط دستگاه Reader ارسال و توسط آنتن موجود در tag دریافت می‌شود، تامین می‌کنند.

- Tagهای Semi-passive : بسیار شبیه tagهای Passive است، با این تفاوت که باتری کوچکی در آن‌ها وجود دارد و انرژی لازم برای فعال شدن مدار داخل آن‌ها را فراهم می‌سازد.

- Tagهای Active : این tagها دارای یک منبع انرژی داخلی می‌باشند که توانایی انتقال اطلاعات در فواصل دورتر را فراهم می‌کند.

در تراشه RFID می‌توانم اطلاعات بسیاری در قالب کدهایی قرار داد این کد قابل انطباق با سایر سیستم‌های کد گذاری است. امروزه پرکاربردترین استفاده از RFID در استفاده از EPC(electronic product code) به عنوان کد منحصر به فرد کالاست که به صورت استاندارد می‌باشد. سازمانی که سیستم کدینگ را توسعه داد ورایج کرد، در سراسر دنیا تحت عنوان سازمانی به نام GS1 می‌باشد. این سازمان، EPC global را توسعه داد. با توجه به گستردگی سیستم کدگذاری EPC حجم اطلاعات گسترده‌ای در برچسب‌های RFID ذخیره می‌شود و امکان قرار دادن کلیه اطلاعات کالا در هر برچسب وجود دارد.[۷]

۴- سیستم کدگذاری EPLC به جای EPC

یکی از مسائل مهم در سیستم RFID اطلاعاتی است که در تراشه RFID قرار می‌گیرد و اینکه این اطلاعات چگونه و چه مقدار است ؟ در سیستم RFID که در بالا شرح داده شد از EPC یاد شد. در واقع این کد یک شماره شناسایی منحصر به فرد است که حجم اطلاعات گسترده ای در برچسب‌های RFID ذخیره می‌کند و به واسطه آن می‌توان اطلاعات منحصر به فرد هر چیزی را به دست آورد. این کد قابل انطباق با سایر سیستم‌های شماره گذاری از جمله بارکد است که در ۳ کلاس ۶۴ بیتی ؛۹۶ بیتی و۲۵۶ بیتی ارائه می‌شود. امروزه ظرفیت‌ها و کلاسهای بیشتری برای EPC تولید و ارائه شده است. بنابراین ظرفیت بسیار عظیمی در EPC قابل گنجانیدن است. این کدها بایستی بر مبنای یک سری استانداردهای جهانی استوار باشند. سازمانی که سیستم کدینگ بارکد را توسعه داد ورایج کرد، در سراسر دنیا تحت عنوان سازمانی به نام GS1 می‌باشد. این سازمان، EPC global را توسعه داده وهمین ساختار کدینگ را برای کالاها(در ساختار الکترونیکی محصول)، در سطح جهانی توسعه داده که به هر حال

به یک توانمندی وهمزبانی در شناسایی کالاها رسیده است. کد EPC دارای چهار قسمت است. [۸]

دو رقم اول(۸ بیت) برای header می‌باشد و بخش بعدی عدد EPC manager با ۲۸ بیت، که تا ۲۶۸ میلیون یا بیشتر شماره می‌تواند بگیرد. قسمت بعدی object class که ۲۴ بیت است وتا ۱۶ میلیون شماره، ظرفیت دارد. بخش بعد شماره سریال با ۳۶ بیت است. که تا حدود ۶۸ میلیارد شماره می‌تواند در اینجا بدان اختصاص داده شود. این پدیده شماره گذاری، که مدام در حال توسعه می‌باشد، ظرفیتی را ایجاد کرده که تا کنون بشر برای هیچ نوع سیستم کدینگی نمی توانسته ایجاد کند. بنابراین وقتی این کد را با این ظرفیت اطلاعاتی بتوان ایجاد کرد پس هر اطلاعاتی را که نیاز باشد می‌توان در آن قرار داد و به صورت یک برچسب RFID در آورد.(به طوری که برآورد شده اگر بخواهند روی تک تک دانه‌های برنج محصول کل دنیا برچسب RFID بچسبانند سریالهای EPC گنجایش یک چنین ظرفیتی را دارد وهیچ دو دانه برنجی را نمی توان با سریال مشابه پیداکرد.) [۸]

با توجه به گستردگی این سیستم کدگذاری و اهمیت بحث شناسایی افراد از طریق کد منحصر به فرد، می‌توان به جای کد محصول الکترونیکی (EPC) از کد شخصی الکترونیکی EPLC(Electronic personal code) استفاده کرد به این صورت که برای هر شخصی کد منحصر به فردی اختصاص داده شود و از این کد که معمولا تعدادی عدد و حرف (حدود پانزده رقم) است به عنوان ایندکس اطلاعات وی در پایگاه داده مرکزی استفاده شود.به عبارت دیگر از آنجا که این کد منحصر به فرد است با وجود آن اطلاعات وی با سرعت از پایگاه داده فراخوانی می‌شود. [۹] [۱۰] [۱۱] در زیر به شرح و بیان این سیستم می‌پردازیم.

۵- هدف و بیان سیستم

هدف از طراحی سیستم تایید هویت، تبادل امن اطلاعات و یکپارچه سازی احراز هویت است. در این راستا می‌توان به موارد ذیل اشاره کرد :

۱- تسهیل تعاملات و تبادل اطلاعات در بستری امن به دلیل اطمینان از احراز هویت طرفین همچنین اطمینان از اینکه شخص شرکت کننده در تعاملات همان شخصی است که خود را معرفی می‌کند.

۲- تایید هویت افراد شرکت کننده در تبادل اطلاعات به خصوص تعاملات تجاری قبل از ورود به سیستم اصلی

۳- یکپارچه سازی سیستم تایید هویت به صورت ملی و حتی جهانی از طریق ایجاد پایگاه داده متمرکز (core databases).

۴- استفاده از RFID به دلیل استفاده از تکنولوژی نانو، قرار دادن حجم عظیم اطلاعات در فضایی کوچک، منحصر به فرد بودن سیستم کدگذاری، عدم کپی برداری و شبیه سازی، غیر تماسی بودن، دریافت اطلاعات در هر مکان و هر زمان توسط قرائتگرها (RFID reader) حتی به صورت سیار و با استفاده از ابزار بی سیم.

۵- به کارگیری شاخص بیومتریک به منظور منحصر به فرد کردن سیستم شناسایی و اطمینان از به کارگیری این سیستم توسط خود شخص و بهینه سازی سیستم امنیتی.

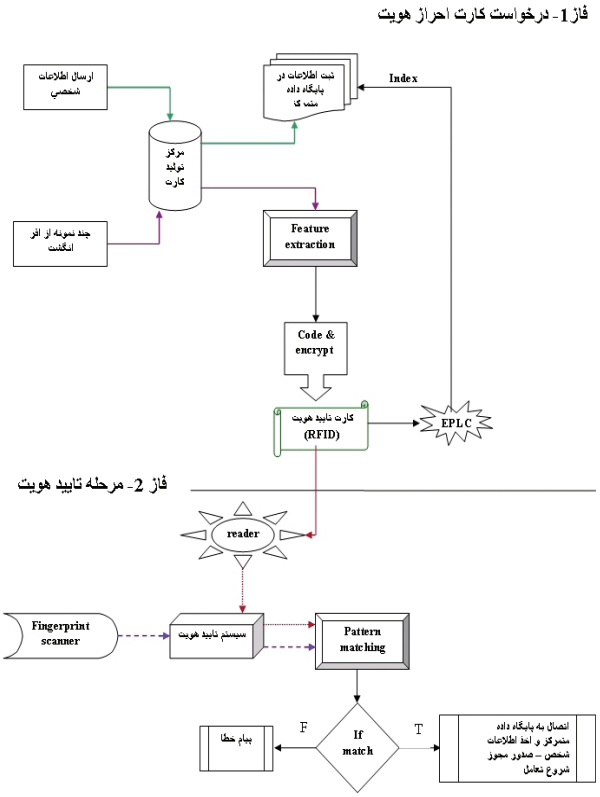
با توجه به اهداف ذکر شده می‌توان چنین سیستمی را به صورت زیر تشریح کرد :

هر شخص جهت دارا بودن کارت شناسایی RFID یا کارت شناسایی بدون تماس (contact less) درخواست خود را به مرکز تهیه و ایجاد کارت که یک مرکز متمرکز است ارسال می‌کند این مرکز اطلاعات شخصی و کاملی از آن فرد را در پایگاه داده خود وارد کرده به علاوه نمونه‌هایی از یک شاخص بیومتریک شخص را مثلا تصاویری از اثر انگشت وی را گرفته،فشرده سازی و کد کرده و در برچسب RFID مخصوص او قرار می‌دهد. برچسب RFID دارای شماره منحصر به فردی است که EPLC نامیده می‌شود و ایندکس اطلاعات او در پایگاه داده نیز به حساب می‌آید. برچسب RFID درکارتی تعبیه شده و به عنوان کارت تایید هویت به شخص داده می‌شود[۱,۱۲] . زمانی که شخص تقاضای شرکت در تعاملی را دارد که تایید هویت وی مهم و دارای اهمیت می‌باشد با استفاده از این کارت می‌تواند هویت خود را محرز کند به این صورت که توسط اسکنر شاخص بیومتریک (اسکنر اثر انگشت) ابتدا شاخص بیومتریک خود را ارسال می‌کند و اطلاعات درون کارت خود را نیز توسط RFID Reader ارسال می‌کند و قبل از ورود به سیستم اصلی ابتدا بر اساس مدل HMAX ویژگی‌های تصاویر استخراج شده شاخص بیومتریک وی با آنچه که در کارت از قبل موجود بوده است تطبیق الگو داده می‌شود و در صورت صحت و تایید، اطلاعات او از پایگاه داده متمرکز بازیابی می‌شود این بازیابی با سرعت زیادی نسبت به حجم عظیم اطلاعات و با وجود EPLC وی که در واقع ایندکس پایگاه داده است انجام می‌گیرد.

روال کار در این سیستم در دو فاز انجام می‌شود یکی ایجاد کارت و ورود اطلاعات به پایگاه داده و دیگر سیستم تایید هویت که در شکل (۲) آورده شده است.

از آنجا که امروزه دستگاه‌های قرائتگر (RFID reader) و حتی حسگرها یا اسکنرهای بیومتریک دارای اندازه کوچکی بوده و به راحتی قابل نصب بر روی ابزارهای الکترونیکی و سیار مانند کامپیوترها، لپ تاب‌ها، گوشی‌های تلفن همراه و ... است لذا

استفاده از این سیستم تایید هویت به راحتی امکان پذیر می‌باشد[۱۴]



شکل ۲: طرح فاز اول و دوم سیستم تایید هویت

۶- پیاده‌سازی سیستم پیشنهادی و نتایج حاصل

سیستم پیشنهادی در مرحله استخراج خصیصه‌های تصاویر اثر انگشت و تطابق الگو در تصاویر موجود در برچسب RFID و تصاویری که از حسگر اثر انگشت گرفته می شود بر روی FVC dataset [۱۵] بر پایه مدل HMAX و با استفاده از نرم‌افزار matab۲۰۰۸ پیاده‌سازی و تست شده است.

در ابتدا مختصری به مدل HMAX می‌پردازیم.

۶-۱- مدل HMAX

از آنجایی که مدل HMAX بر اساس سیستم بینایی در مغز انسان کار می‌کند آزمایشات انجام شده نشان می‌دهد که نسبت به چرخش تصاویر و تغییر سایز آنها پایدار تر می‌باشد. این مدل از ترکیب دو لایه (complex) C و(simple) S تشکیل شده است که متناوبا تکرار می‌شوند [۱۶]. لایه C خود دو لایه C1 و C2 و لایه S نیز لایه‌های S1 و S2 را تشکیل می‌دهند.

ورودی لایه S1 تصاویر واقعی می‌باشد. این لایه عملکرد عصبهای ناحیه V1 مغز را شبیه سازی می‌کند. در این لایه از فیلتر گا بور استفاده شده است. این فیلتر به خطوط با سایز و اندازه خاص حساس بوده و از تصویری که به آن داده می‌شود فقط خطوط با اندازه و جهت خاص را استخراج می‌نماید. این فیلتر جهت محاسبه خطوط از فرمول زیر استفاده می‌کند : [۱۷]

$$G(x,y) = \exp\left(-\frac{(X^2+\gamma^2Y^2)}{2\sigma^2}\right) \times \cos\left(\frac{2\pi}{\lambda}X\right),$$

$$\text{where } X = x\cos\theta + y\sin\theta \text{ and } Y = -x\sin\theta + y\cos\theta.$$

پنج پارامتر فیلتر فوق شامل: جهت θ، ضریب انحراف δ، پهنای موثر σ، فاز Φ، طول موج λ می‌باشد که خصوصیات سلولهای مکانی حوزه دید را تعیین می‌کند. فیلتر گابور به منظور شبیه‌سازی نورونهای V1 در مغز انسان استفاده می‌شود، که این فیلتر با جهت‌ها و پهناهای متفاوت بر روی تصویر ورودی اعمال می‌گردد. هر کدام از این فیلترها برروی یک لبه با پهنا و زاویه چرخش خاص در تصویر اعمال می‌شوند[۱۷و۱۸].واحدهای S1، مانند دیگر واحدهای ساده در مدل، عمل میزان‌سازی را بین الگوی ورودی X و بردار وزنی آن‌ها(w)، توسط فیلتر گابور اعمال می‌کنند. پاسخ واحد S1، زمانی حداکثر است که X و w دقیقاً بر هم منطبق باشند. به طورکلی، معمولاً زمانی به پاسخ بهینه و مناسب دست می‌یابیم که جهت محرک‌ها (به عنوان مثال: خط با طول و عرض بهینه، لبه، یا شبکه ای بهینه در فرکانس مکانی) با جهت فیلتر منطبق باشند و زمانی پاسخ کاهش می‌یابد که جهت محرک و فیلتر تفاوت بیشتری داشته باشند و یا به عبارت دیگر، نامتشابه باشند. در نتیجه ی اعمال فیلتر گابور در چهار جهت θ و ۱۶ مقیاس S بر روی تصویر، یک نقشه 64=4×16 از $(S1)^s_\theta$ در ۸ باند ایجاد می‌گردد. (به عنوان مثال: باند ۱ شامل خروجی فیلتر با سایز ۷ و ۹ به همراه کلیه جهت‌هایشان می‌باشد، باند ۲ نیز شامل خروجی فیلترهای ۱۱ و ۱۳ است). جدول(۱) پارامترهای تنظیم شده برای پیاده‌سازی را نشان می‌دهد.

در لایه S1، ۱۶ سایز مختلف از فیلتر گابور بر روی تصویر در ۴ جهت اعمال می شود.در کل خروجی این لایه 4*16فیلتر عکس می باشد.

خروجی لایه S1 به لایه C1 داده می‌شود این لایه عملکرد عصبهای ناحیه V2 مغز را را شبیه سازی می نماید. در این لایه ۱۶ تصویر خروجی لایه S۱ را به ۸ دسته یا باند تقسیم نموده و در تصاویر هر باند را به طور جداگانه ماکزیمم می گیرد. و برای هر یک از چهار جهت این اعمال به طور مجزا انجام می شود.

در این لایه به تعداد K بار از تصویر لایه C1 نمونه برداشته می‌شود. این نمونه برداری‌ها به صورت تصادفی صورت می‌گیرد. سایز نمونه‌ها ۴*۴ و ۸*۸ و ۱۲*۱۲ می باشد. سپس این نمونه‌ها ذخیره می‌شوند.

لایه S2 عملکرد عصبهای ناحیه V4 را شبیه‌سازی می‌نماید. ورودی این لایه خروجی لایه C1 است. در این لایه به تعداد K بار از تصویر لایه C1 نمونه برداشته می شود. این نمونه‌ها با تک تک

نمونه‌هایی که قبلا ذخیره شده اند مقایسه می گردد و نتیجه این مقایسه در یک بردار K تایی است که ذخیره می گردد.

قابل ذکر است که این کار به ازای ۸ باند و در چهار جهت متفاوت به طور جداگانه صورت می گیرد.

ورودی لایه C2 خروجی لایه S2 است. در این لایه به ازای تمام تصاویر و در تمام جهت‌ها ماکزیمم گرفته می شود و در نهایت یک بردار K تایی از تصویر حاصل می گردد.[۱۸][۱۹]

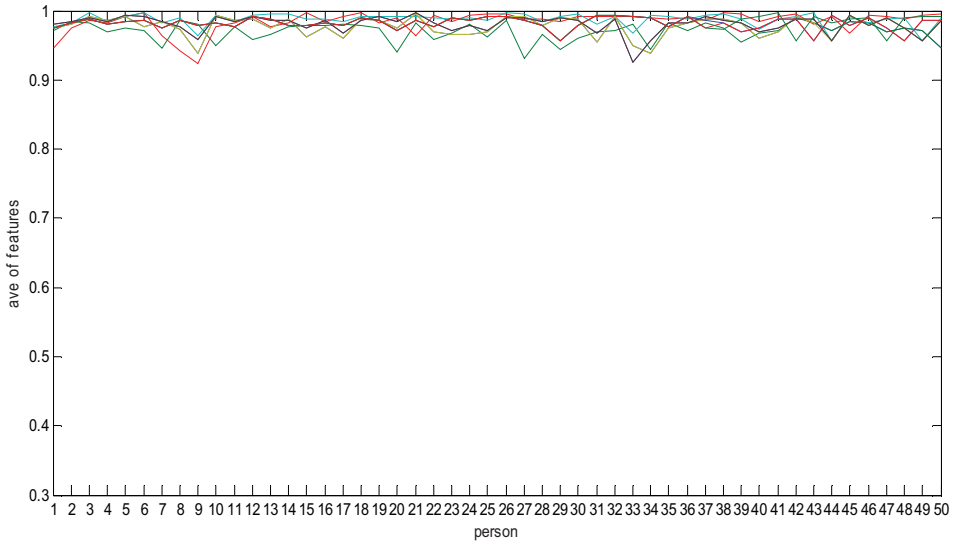
جدول ۱: پارامترهای تنظیم شده در مدل HMAX [۱۸]

باند(Σ)	۱	۲	۳	۴	۵	۶	۷	۸
اندازه فیلتر(s)	۷&۹	&۱۳ ۱۱	&۱۷ ۱۵	&۲۱ ۱۹	&۲۵ ۲۳	&۲۹ ۲۷	&۳۳ ۳۱	۳۵&۳۷
پهنای موثر(σ)	&۳.۶ ۲.۸	&۵.۴ ۴.۵	&۷.۳ ۶.۳	&۹.۲ ۸.۲	&۱۱.۳ ۱۰.۲	&۱۳.۴ ۱۲.۳	&۱۵.۸ ۱۴.۶	&۱۸.۲ ۱۷.۰
طول موج (λ)	&۴.۶ ۳.۵	&۶.۸ ۵.۶	&۹.۱ ۷.۹	&۱۱.۵ ۱۰.۳	&۱۴.۱ ۱۲.۷	&۱۶.۸ ۱۵.۴	&۱۹.۷ ۱۸.۲	&۲۲.۸ ۲۱.۲
اندازه پنجره(N^{Σ})	۸	۱۰	۱۲	۱۴	۱۶	۱۸	۲۰	۲۲
جهت(θ)	0 و $\frac{\pi}{4}$ و $\frac{\pi}{2}$ و $\frac{3\pi}{4}$							
اندازه patchها ی n_i	۴×۴ و ۸×۸ و ۱۲×۱۲ و ۱۶×۱۶ (×۴ جهت)							

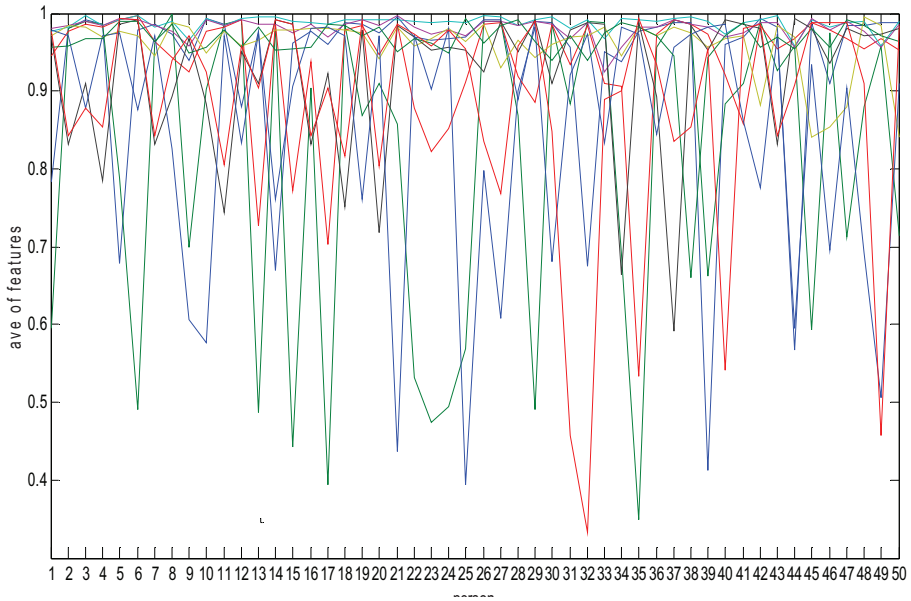
۶-۲- نتایج آزمایشات

جهت تست داده‌های موجود فرض می‌کنیم که از هر نفر هشت تصویر مختلف (اختلاف از نظر مقیاس و موقعیت) در کارت احراز هویت یا کارت RFID شخص موجود است این تصاویر با دو تصویری که از حسگر اثر انگشت دریافت می‌شود به سیستم پیشنهادی ما داده می‌شود در این سیستم خصیصه‌های تصاویر بر اساس مدل HMAX بیرون کشیده شده و در برداری قرار داده می‌شود مطابق این مدل برای هر تصویر یک بردار ۲۵۶*۱خواهیم داشت یعنی از هر تصویر ۲۵۶ خصیصه بیرون کشیده می‌شود. چون مطابق این مدل تصاویر نسبت به هم سنجیده می‌شوند، تست‌ها نشان می‌دهند که اگر دو تصویری که از حسگر گرفته شده است با هشت تصویر موجود در کارت احراز هویت یکسان باشد میانگین خصیصه‌های تصاویر، عددی بین ۱ تا ۰/۹۰۰۰ را نشان می‌دهدکه نشان دهنده این است که کارت متعلق به شخص موجود است یا به عبارت دیگر هویت شخص محرز می‌گردد اما اگر دو تصویر با دیگر تصاویر متفاوت باشد میانگین خصیصه‌های این دو تصویر عددی بین ۱ تا ۰/۳را نشان می‌دهد که می‌توان نتیجه گرفت کارت به شخص مورد نظر تعلق ندارد و احراز هویت منتفی است. بنابر نتایج به دست آمده می‌توان گفت اگر حد آستانه (threshold) را ۰/۹ در نظر بگیریم سیستم در تشخیص خصیصه‌های تصاویر صحیح عمل خواهد کرد. شکل (۳) نتیجه اجرای مدل را برای ۵۰ نفر که هویتشان مورد تایید است نشان می‌دهد به عبارت دیگر در این تست هشت تصویر موجود در کارت احراز هویت و دو تصویری که از حسگر گرفته شده است با هم تطابق داشته و همان طور که قابل مشاهده است میانگین خصیصه‌های هر تصویر در صورتیکه تمام تصاویر مربوط به یک شخص باشد بین ۱ تا ۰/۹ است اما مطابق شکل (۴) که حاصل اجرای مدل را بر روی۵۰ نفر دیگر است. همان طور که مشاهده می‌گردد میانگین خصیصه‌ها تصاویر اعداد متفاوتی را نشان می‌دهند که این اعداد بین ۱ تا ۰/۲ می‌باشند و می‌توان نتیجه گرفت تصاویر موجود در کارت احراز هویتشان با تصاویر گرفته شده از حسگر یکسان نیست و اجازه تعاملی به آن‌ها داده نمی‌شود. بنابر آزمایش‌های انجام شده بر روی ۱۰۰ تصویر اثر انگشت و شکل‌های فوق الذکر، حد آستانه ۰/۹ باعث می‌شود سیستم پیشنهادی ما ۱۰۰% درست عمل کرده و نتیجه خوبی ارائه دهد.

بر اساس تحقیقات انجام شده بر روی مدل PCA [۲۰]، این مدل فقط در شرایط کنترل شده جواب قابل قبولی ارائه می‌کند یعنی به تغییر سایز و تغییر محل تصاویر حساس بوده و نتایج یکسانی در بر ندارد اما مدل HMAX نیبت به این تغبرات پایداری بیشتری از خود نشان می‌دهد.



شکل ۳: نتایج حاصل از تایید هویت – حد آستانه بین ۱ تا ۰/۹



شکل ۴: نتایج حاصل از عدم تایید هویت - حد آستانه بین ۱ تا ۰/۳

۷- نتیجه

در این مقاله سیستمی جهت احراز هویت پیشنهاد نمودیم که با استفاده از شاخص بیومتریکی مانند اثر انگشت و کارت‌های بدون تماسی که بر اساس امواج رادیویی کار می‌کنند (RFID) پایه ریزی شده است. سیستم در دو فاز ایجاد کارت احراز هویت و فرایند احراز هویت کار می‌کند. جهت ایجاد کارت احراز هویت تمام اطلاعات شخص وارد پایگاه داده متمرکزی شده به علاوه تعدادی از تصاویر اثر انگشت وی در برچسب RFID قرار داده شده و به عنوان کارت احراز هویت به شخص داده می‌شود. زمانی که فرایند احراز هویت لازم به اجراست، شخص اطلاعات کارت احراز هویت خود را توسط RFID reader ارسال کرده و از طرف دیگر اثر انگشت خود را به حسگر اثر انگشت داده تا احراز هویت شود. سیستم مذکور خصیصه‌هایی از تصاویر ارسالی استخراج می‌کند (feature extraction) در صورتیکه بتواند تطابق الگویی (pattern matching) با حد آستانه (threshold) ۰/۹ ایجاد نماید هویت شخص تایید می‌گردد و در غیر این صورت شخص اجازه هیچگونه تعاملی ندارد. با تست‌های انجام شده بر اساس مدل HMAX سیستم به طور ۱۰۰% قادر به پاسخ گویی می‌باشد..

۸- سپاسگزاری

در اینجا بر خود لازم می‌دانیم از مرکز تحقیقات مخابرات ایران به دلیل حمایت مالی از انجام این پروژه کمال تشکر و قدردانی را داشته باشیم.

مراجع

[1] EFRAIM Turban, Dorothy leidner, Ephraim mclean, jamef wetherbe " Information Technology for management Transforming organizations in the digital economy" by Publisher : Wiley ; 5edition

[2] پورتال ملی بیومتریک ; http://irbiometric.ir/HomePage.aspx?TabID=0&Site=irbiometric&Lang=fa-IR; last updated: مهر ۱۳۸۷;

[3] http://mashreghzamindaily.blogfa.com/post-45.aspx

[۴] محمد محمدی پیرو" ; امنیت فیزیکی ;" مجتمع دانشگاهی فناوری اطلاعات، ارتباطات و امنیت,دانشگاه صنعتی مالک اشتر; سمینار امنیت ۱۳۸۶

[5] Davide Maltoni, Anil K. Jain, Dario Maio, Salil Prabhakar ; " Handbook of fingerprint recognition" ; Edition: 2, illustrated, annotated ; Published by Springer, 2003 ;ISBN 0387954317, 9780387954318

[6] Yuh-Jzer Joung;" Radio Frequency Identification"; Dept. of Information Management National Taiwan University Feb, 2006

[7] Klaus Finkenzeller, and Racher Waddington," RFID handbook-Fundaments and Application in Contactless Smart card and Identification",Carl Hanser Verlag, Munich/FRG,2004

[۸] دکتر محمود زرگر ";" مدیریت زنجیره تامین - بخش RFID، پاییز۸۵.

[9] http://www.rfida.com/2005/09/rfid-automated-document-authentication.htm

[10] http://www.rfidsolutionsonline.com/article.mvc/RFID-For-Personal-Identification-And-Informat-0001#article

[11] Institute for Technology Assessment and Systems Analysis (ITAS), Karlsruhe;" RFID and Identity Management in Everyday Life"; IPOL/A/STOA/2006-22

[12] http://www.precisebiometrics.com/precise-match-on-card-1.aspx

[13] AUTO-ID Labs at MIT; http://autoid.mit.edu/CS/; last updated: Apr 7 2008; visited:Sep 10 2008

[14] Weiping Zhu , Dong Wang , Huanye Sheng; "Mobile RFID Technology for Improving M-Commerce".; Dep. Of Computer Science & Engineering,Shanghai Jiaotong University ; Proceedings of the 2005 IEEE International Conference on e-Business Engineering (ICEBE'05)

[15] http://bias.csr.unibo.it/fvc2004/default.asp

[16] T. Serre and M. Riesenhuber.;" Realistic modeling of simple and complex cell tuning in the hmax model, and implications for invariant object recognition in cortex." Technical Report CBCL Paper 239 / AI Memo 2004- 017,Massachusetts Institute of Technology,Cambridge,MA, July 2004.

[17] D. Hubel and T. Wiesel.;" Receptive fields and functional architecture in two nonstriate visual areas" (18 and 19) of the cat. J.Neurophys.,28:229–89, 1965

[18] T. Yang and J. H. R. Maunsell. ;"The effect of perceptual learning on neuronal responses in monkey visual area V4". J. Neurosci., 24:1617–1626, 2004.

[19] T.J. Gawne and J.M. Martin.;" Response of primate visual cortical V4 neurons to simultaneously presented stimuli".J.Neurophysiol., 88:1128–1135, 2002

[20] Sara Motamed, karim Faez, Mahboubeh Yaqubi;" Fingerprint Verification using HMAX model and SVM classification";16 th Iranian conference on electrical engineering ; tarbiat modares university may 13 -15 ,2008