مطالعات اقتصاد، مدیریت مالی و حسابداری

دوره 1، شماره 1، زمستان 1394

صفحات 1-8

Print ISSN: xxxx-xxxx

Online ISSN: xxxx-xxxx

www.irijournals.com

بررسی فناوری بیومتریک و روش تشخیص چهره در فرآیندهایی مالی و امنیتی

محمد رضا محمدی احمدآباد

پژوهشگر، ایران

چکیده

این مقاله به معرفی سیستمهای تشخیص هویت که مهمترین و دقیق‌ترین آنها بیومتریک است خواهد پرداخت. پس از تعریف بیومتریک به تعریف معماری سیستم‌های بیومتریک می‌پردازیم و همچنین تشخیص چهره و کاربردهای آن در پردازش های مالی و امنیتی آن پرداخته شده است. در این مقاله همچنین در مورد چند تکنولوژی بیومتریک هم توضیح داده می‌شود مانند اثر انگشت، چهره و ... سپس به معرفی سیستم تشخیص چهره و کاربرد ها ، رمزنگاری و مسایل مربوطه و در انتها به معرفی مفهوم ترکیبات بیومتریک و روش‌های متنوع آن خواهیم پرداخت. استفاده از روش ترکیب بیومتریک کارایی، امنیت، دقت سیستم را افزایش می‌دهد.

امروزه تشخیص هویت در بسیاری از نرم افزار ها رایج شده است، به طوری که در سیستم های امنیتی جهت شناسایی، موتورهای جستجو و غیره مورد استفاده قرار می گیرد.طور کلی سیستم شناسایی انسان با استفاده از طیف وسیعی از اطلاعاتی که حواس پنجگانه اش (بینایی ، شنوایی ، بویایی ، چشایی و لامسه) در اختیارش قرار می دهند ، کار می کند.

با توجه به ساختار بیومتریک و تشخیص چهره و سایر روشهای این چنینی در پردازش های مالی نقش بسیار مهمی خواهند داشت و به امنیت ورود به ساختار مالی را برای ما به نوعی تضمین خواهند کرد به این نتیجه میرسیم که این فناوری خیلی به کمک ما خواهد آمد.

واژه‌های کلیدی: بیومتریک،کاربردهای بیومتریک ، تشخیص چهره ، رمزنگاری، فرایندهای مالی و امنیتی

مقدمه

از دیر باز انسان برای بقا، نیاز به تشخیص دوست از دشمن داشته است و تشخیص هویت برای وی امری حیاتی بوده و هست، لذا امروزه سعی در مکانیزه سازی سیستمهای شناسایی یا تشخیص هویت شده است. "این پیشرفتها دلیل بر نیاز جامعه و جهان است".[۱] نیازی که پیشرفت در آن باعث کاهش تخلفات، افزایش امنیت، تسریع در امور روزمره و ... شده است. در گذشته جهت شناسایی جرم و جنایتکار، از روال شناسایی اثر انگشت وچهره نگاری استفاده می‌شده، اما اکنون سیستمهای مکانیزه‌ای ایجاد شده است .فناوری بومتریک از جمله فناوری‌های نوظهور در عرصه‌ی فناوری اطلاعات است، که می تواند پاسخگوی این نیاز باشد. لیکن استفاده‌ی صحیح از آن مستلزم اتخاذ رویکردی جامع و همه جانبه‌نگر است.

استفاده از این فناوری قبل از هر چیز، مستلزم تحلیل و بررسی مسائل زیرساختی، فرهنگی، اقتصادی، حقوقی و اجتماعی در هر کاربرد خاص است، به گونه‌ای که ضرورت استفاده از این فناوری به طور کامل مشخص و به‌دنبال آن سیاست‌های لازم برای پیاده‌سازی و به‌کارگیری این سیستم‌ها اتخاذ شوند.

بیان مساله

بیومتریک

واژه بیومتریک، به طیف گسترده‌ای از فناوری‌هایی گفته می‌شود، که هویت افراد را به کمک اندازه گیری و تحلیل خصوصیات انسانی شناسایی میکنند. به عبارتی دیگر، هر خصوصیت فیزیولوژیکی یا ویژگی رفتاری منحصر به فرد و متمایز کننده، مقاوم و قابل سنجش که بتواند برای تعیین یا تأیید خودکار هویت افراد بکار رود بیومتریک نام دارد.

اجزای سیستم بیومتریک

سیستم بیومتریک از 3 جزء اصلی تشکیل می شود:

1-ابزار اندازه گیری :ابزار طراحی شده در سیستم بیومتریک در حقیقت نقش واسطه با کاربر را برعهده دارد و لذا باید به راحتی توسط کاربران قابل استفاده باشد و در عین حال احتمال خطا در آن بسیار کم باشد.

2- نرم افزار :این نرم افزار که براساس الگوریتم های ریاضی طراحی شده است، متغیرهای سنجش شده را با الگوی مرجع موجود در بانک اطلاعات مقایسه می کند.

3- سخت افزار :در طراحی سامانه بیومتریکی، به قطعات سخت افزاری و کاربرد آنها باید بیش از سایر دستگاه های مشابه توجه نشان داد تا در انجام محاسبات دچار خطا نشود.

تکنیکهای بیومتری

بررسی های بیومتریک به دو دسته عمده تقسیم می شود:

در این روش، طرز انجام کاری توسط کاربر سنجیده می (Behavioral): 1- تکنیک های رفتاری شود .مانند امضا کردن یا بیان کردن یک عبارت.

در این حالت، یک خصوصیت فیزیکی مانند اثر انگشت (Physiometric) : 2- تکنیک های فیزیکی یا الگوی عنبیه مورد سنجش قرار می گیرد.

مزایای فناوری های بیومتریک

1- غیر قابل حدس زدن

2- غیر قابل فراموشی و غیر قابل سرقت

3- سرعت و راحتی استفاده

4- عدم نیاز به هزینه های امنیتی جهت استفاده از نیروی انسانی

5- غیر قابل تقلب

6-امکان تعیین هویت اصلی و واقعی افراد

تکنیکهای فیزیولوژیکی

باز شناسی هویت از طریق اثر انگشت

این روش قدیمی ترین روش آزمایش تشخیص هویت از راه دور است .اگرچه قبلاً اثر انگشت تنها در زمینه جرم قابل بحث بود، تحقیقات در بسیاری کشورها سطحی از پذیرش را نشان میدهد که به این روش اجازه استفاده در برنامه های عمومی را می دهد .سیستمها میتوانند جزئیاتی از اثر انگشت)نقاطی مانند تقاطعها یا کناره های برجستگیها (یا کل تصویر را بگیرند .الگوهای مرجع که برای حفظ این جزئیات بکار میرود در حدود 100 بایت هستند که در مقایسه با تصویر کاملی که از اثر انگشت با حجم 500 تا 1500 بایت میباشد,بسیار کوچکتر هستند.

در حال حاضر اثر انگشت خوانهای زیادی در دامنه وسیعی وجود دارند که به همراه بعضی کارتخوانها استفاده میشوند .اگرچه در حال حاضر قیمت آنها چندان پایین نیست اما میزان عرضه آنان در فروشگاههای کامپیوتر عادی باعث افت سریع قیمت آنان خواهد شد .به طور مثال شرکت هواپیمایی آلمان لوفتانزا ، آزمایش بلیت های بیومتریک را آغاز کرده است .این بلیت ها با اطلاعات مربوط به اثر انگشت شصت مسافران رمزگذاری شده اند و انتظار میرود سرعت کنترل را بدون پیچیدگی های

امنیتی افزایش دهند.

دوره 1، شماره 1، زمستان 1394، صفحات 1-8

سیستم تشخیص چهره

امروزه تشخیص هویت در بسیاری از نرم افزار ها رایج شده است، به طوری که در سیستم های امنیتی جهت شناسایی، موتورهای جستجو و غیره مورد استفاده قرار می گیرد.

طور کلی سیستم شناسایی انسان با استفاده از طیف وسیعی از اطلاعاتی که حواس پنجگانه اش (بینایی ، شنوایی ، بویایی ، چشایی و لامسه) در اختیارش قرار می دهند ، کار می کند. این اطلاعات بصورت جداگانه و یا در کنار هم ، هم برای به خاطر سپردن و هم برای بازشناسی به کار می روند. علاوه بر این موارد اطلاعات محیطی نیز در شناسایی انسانی نقش مهمی دارند. برای مثال شناسایی مجری یک برنامه ی تلویزیونی در همان برنامه بسیار راحت تر از شناسایی او در خیابان و یا هر محل دیگری است. سیستم های تشخیص چهره نیز به عنوان یکی از سیستم های تشخیص هویت از این قاعده جدا نیست و امروزه روز بروز دارای کاربرد های بیشتری می شوند این سیستم ها به دلیل آسانی در نمونه برداری و دردسترس بودن سریع روز به روز بیشتر مخاطب پیدا میکنند. سیستم های پردازش چهره عمدتا به دو دسته تقسیم شده یکی جهت شناسایی چهره در تصویر و درگری جهت شناسایی چهره کشف شده در تصویر، به عبارت دیگر ابتدا تمامی چهره ها از پس زمینه و جزییات زاید جدا شده سپس تمامی چهره های تشخیص داده شده با چهره های موجود در دیتا بیس(چهره های ثبت شده و دارای هویت مشخص) مقایسه شده و با توجه به میزان شباهت ، شبیه ترین چهره به تصاویر موجود پیدا می شود.

لذا این شرکت با توجه به نیاز توسعه دهندهگان اقدام به تهیه کتابخانه ای نموده که علاوه بر سهولت استفاده ، دقت و سرعت بالایی نیز دارد، این تکنولوژی به نرم افزار شما امکان میدهد تا تنها با یک عکس از هر فرد بتوانید سیستم جستجوی مناسبی بر اساس عکس چهره افراد مختلف در بسته نرم افزاری خود ارائه دهید. این محصول از ابتدا تا انتها تماما بومی بوده و بوسیله نخبگان و متخصصین برجسته داخلی طراحی و توسعه داده شده است.

کاربرد های تشخیص چهره

موارد کاربرد بیشماری را می توان برای استفاده از پردازش تصاویر در نظر گرفت:

- تشخیص مجرم از روی بایگانی عکس وی و ثبت و جستجوی سوابق
- کنترل نامحصوص و امنیت تردد در اماکن عمومی
- هویت شناسی فرد از روی تصویر در ازای اثر انگشت
- پیاده سازی سیستم های جستجو بر اساس تصویر
- استفاده در شناسایی فرد در بانکها و موسسات مالی اعتباری
- و ...

دوره 1، شماره 1، زمستان 1394، صفحات 1-8

امنیت اطلاعات

امنیت اطلاعات یعنی حفاظت اطلاعات و سیستم‌های اطلاعاتی از فعالیت‌های غیرمجاز. این فعالیت‌ها عبارتند از دسترسی، استفاده، افشاء، خواندن، نسخه برداری یا ضبط، خراب کردن، تغییر، دستکاری.

واژه‌های امنیت اطلاعات، امنیت کامپیوتری و اطلاعات مطمئن گاه به اشتباه به جای هم بکار برده می‌شود. اگر چه اینها موضوعات به هم مرتبط هستند و همگی دارای هدف مشترک حفظ محرمانگی اطلاعات، یکپارچه بودن اطلاعات و قابل دسترس بودن را دارند ولی تفاوت‌های ظریفی بین آنها وجود دارد. این تفاوت‌ها در درجه اول در رویکرد به موضوع امنیت اطلاعات، روش‌های استفاده شده برای حل مسئله، و موضوعاتی که تمرکز کرده‌اند دارد.
امنیت اطلاعات به محرمانگی، یکپارچگی و در دسترس بودن داده‌ها مربوط است بدون در نظر گرفتن فرم اطلاعات اعم از الکترونیکی، چاپ، و یا اشکال دیگر.

امنیت کامپیوتر در حصول اطمینان از در دسترس بودن و عملکرد صحیح سیستم کامپیوتری تمرکز دارد بدون نگرانی از اطلاعاتی که توسط این سیستم کامپیوتری ذخیره یا پردازش می‌شود.

دولت‌ها، مراکز نظامی، شرکت‌ها، موسسات مالی، بیمارستان‌ها، و مشاغل خصوصی مقدار زیادی اطلاعات محرمانه در مورد کارکنان، مشتریان، محصولات، تحقیقات، و وضعیت مالی گردآوری می‌کنند. بسیاری از این اطلاعات در حال حاضر بر روی کامپیوترهای الکترونیکی جمع‌آوری، پردازش و ذخیره و در شبکه به کامپیوترهای دیگر منتقل می‌شود. اگر اطلاعات محرمانه در مورد مشتریان و یا امور مالی یا محصول جدید موسسه‌ای به دست رقیب بیفتد، این درز اطلاعات ممکن است به خسارات مالی به کسب و کار، پیگرد قانونی و یا حتی ورشکستگی منجر شود. حفاظت از اطلاعات محرمانه یک نیاز تجاری، و در بسیاری از موارد نیز نیاز اخلاقی و قانونی است.

برای افراد، امنیت اطلاعات تأثیر معناداری بر حریم خصوصی دارد. البته در فرهنگ‌های مختلف این مفهوم حریم خصوصی تعبیرهای متفاوتی دارد.

کنترل

برای حراست از اطلاعات، باید دسترسی به اطلاعات کنترل شود. افراد مجاز باید و افراد غیرمجاز نباید توانایی دسترسی داشته باشند. بدین منظور روش‌ها و تکنیک‌های کنترل دسترسی ایجاد شده‌اند که در اینجا توضیح داده می‌شوند.

دسترسی به اطلاعات حفاظت شده باید محدود باشد به افراد، برنامه‌های کامپیوتری، فرآیندها و سیستم‌هایی که مجاز به دسترسی به اطلاعات هستند. این مستلزم وجود مکانیزم‌های برای کنترل دسترسی به اطلاعات حفاظت شده می‌باشد. پیچیدگی مکانیزم‌های کنترل دسترسی باید مطابق با ارزش اطلاعات مورد حفاظت باشد. اطلاعات حساس تر و با ارزش تر نیاز به مکانیزم کنترل دسترسی قوی تری دارند. اساس مکانیزم‌های کنترل دسترسی بر دو مقوله **احراز هویت** و **تصدیق هویت** است.

دوره 1، شماره 1، زمستان 1394، صفحات 1-8

احراز هویت تشخیص هویت کسی یا چیزی است. این هویت ممکن است توسط فرد ادعا شود و یا ما خود تشخیص دهیم. اگر یک فرد می‌گوید «سلام، نام من علی است» این یک ادعا است. اما این ادعا ممکن است درست یا غلط باشد. قبل از اینکه به علی اجازه دسترسی به اطلاعات حفاظت شده داده شود ضروری است که هویت این فرد بررسی شود که او چه کسی است و آیا همانی است که ادعا می‌کند.

تصدیق هویت عمل تأیید هویت است. زمانی که «علی» به بانک می‌رود تا پول برداشت کند، او به کارمند بانک می‌گوید که او «علی» است (این ادعای هویت است). کارمند بانک کارت شناسایی عکس دار تقاضا می‌کند، و «علی» ممکن است گواهینامه رانندگی خود را ارئه دهد. کارمند بانک عکس روی کارت شناسایی با چهره «علی» مطابقت می‌دهد تا مطمئن شود که فرد ادعا کننده «علی» است. اگر عکس و نام فرد با آنچه ادعا شده مطابقت دارند تصدیق هویت انجام شده است.

از سه نوع اطلاعات می‌توان برای احراز و تصدیق هویت فردی استفاده کرد: چیزی که فرد می‌داند، چیزی که فرد دارد، و یا کسی که فرد هست. نمونه‌هایی از چیزی که می‌داند شامل مواردی از قبیل کد، رمز عبور، و یا نام فامیل قبل از ازدواج مادر فرد باشد. نمونه‌هایی از چیزی که دارد شامل گواهینامه رانندگی یا کارت مغناطیسی بانک است. کسی که هست اشاره به تکنیک‌های بیومتریک هستند. نمونه‌هایی از بیومتریک شامل اثر انگشت، اثر کف دست، صدا و اسکن شبکیه چشم هستند. احراز و تصدیق هویت قوی نیاز به ارائه دو نوع از این سه نوع مختلف از اطلاعات است. به عنوان مثال، چیزی که فرد می‌داند به علاوه آنچه دارد یعنی مثلاً ورود رمز عبور علاوه بر نشان دادن کارت مخصوص بانک. این تکنیک را احراز و تصدیق هویت دو عامله گویند که قوی تر از یک عامله فقط کنترل گذرواژه است.

در سیستم‌های کامپیوتری امروزی، نام کاربری رایج‌ترین شکل احراز و رمز عبور رایج‌ترین شکل تصدیق هویت است. نام کاربری و گذرواژه به اندازه کافی به امنیت اطلاعات خدمت کرده‌اند اما در دنیای مدرن با سیستم‌های پیچیده‌تر از گذشته، دیگر کافی نمی‌باشند. نام کاربری و گذرواژه به تدریج با روش‌های پیچیده تری جایگزین می‌شوند.

پس از آنکه فرد، برنامه یا کامپیوتر با موفقیت احراز و تصدیق هویت شد سپس باید تعیین کرد که او به چه منابع اطلاعاتی و چه اقداماتی روی آنها مجاز به انجام است (اجرا، نمایش، ایجاد، حذف، یا تغییر). این عمل را **صدور مجوز** گویند.

صدور مجوز برای دسترسی به اطلاعات و خدمات کامپیوتری با برقراری سیاست و روش‌های مدیریتی آغاز می‌شود. سیاست دسترسی تبیین می‌کند که چه اطلاعات و خدمات کامپیوتری می‌تواند توسط چه کسی و تحت چه شرایطی دسترسی شود. مکانیسم‌های کنترل دسترسی سپس برای به اجرا درآوردن این سیاست‌ها نصب و تنظیم می‌شوند.

رویکردهای کنترل دسترسی مختلفی وجود دارند. سه رویکرد شناخته شده وجود دارند که عبارتند از: رویکرد صلاحدیدی، غیرصلاحدیدی و اجباری. در رویکرد صلاحدیدی خالق یا صاحب منابع اطلاعات قابلیت دسترسی به این منابع را تعیین می‌کند. رویکرد غیر صلاحدیدی تمام کنترل دسترسی متمرکز است و به صلاحدید افراد نیست. در روش اجباری، دسترسی به اطلاعات و یا محروم کردن بسته به طبقه‌بندی اطلاعات و رتبه فرد خواهان دسترسی دارد.

رمزنگاری

دوره 1، شماره 1، زمستان 1394، صفحات 1-8

در امنیت اطلاعات از رمزنگاری استفاده می‌شود تا اطلاعات به فرمی تبدیل شود که به غیر از کاربر مجاز کس دیگری نتواند از آن اطلاعات استفاده کند حتی اگر به آن اطلاعات دسترسی داشته باشد. اطلاعاتی که رمزگذاری شده تنها توسط کاربر مجازی که کلید رمز نگاری را دارد می تواند دوباره به فرم اولیه تبدیل شود (از طریق فرایند رمزگشایی). رمزنگاری برای حفاظت اطلاعات در حال انتقال (اعم از الکترونیکی و یا فیزیکی) و یا ذخیره شده است. رمزنگاری امکانات خوبی برای امنیت اطلاعات فراهم می‌کند از جمله روش‌های بهبود یافته تصدیق هویت، فشرده سازی پیام، امضاهای دیجیتالی، قابلیت عدم انکار و ارتباطات شبکه رمزگذاری شده .

رمزنگاری اگر درست پیاده‌سازی نشود می‌تواند مشکلات امنیتی در پی داشته باشد. راه حل‌های رمز نگاری باید با استفاده از استانداردهای پذیرفته شده که توسط کارشناسان مستقل و خبره بررسی دقیق شده انجام گیرد. همچنین طول و قدرت کلید استفاده شده در رمزنگاری بسیار مهم است. کلیدی ضعیف یا خیلی کوتاه منجر به رمزگذاری ضعیف خواهد شد. مدیریت کلید رمزنگاری موضوع مهمی است. رمز گذاری داده‌ها و اطلاعات و تبدیل کردن آنها به شکل رمز گذاری شده، روشی مؤثر در جلوگیری از انتشار اطلاعات محرمانه شرکت می‌باشد .

نتیجه گیری

فناوری های بیومتریک از جمله فناوری هایی به حساب می آیند که هزینه تمام شده نسبتاً بالایی دارند و بنابراین شاید در بعضی مواقع مقرون به صرفه نباشد .اما در یک مقایسه کلی تر، با توجه به امنیت بالای سیستم های بیومتریک نسبت به سیستم های سنتی مانند قفل و زنجیر و نگهبان و غیره شاید بتوان گفت که در دراز مدت استفاده از این فناوری برای سازمان ها به صرفه باشد و در مقابل نیز با توجه به تولید نسخه های جدید تر از این گونه سخت افزارها و تولید انبوه آنها، صرفه جویی بیشتر شامل حال کاربران شود و قیمت آنها بسیار پائین تر بیاید. در مورد این فناوری و همچنین تشخیص چهره در پردازش های مالی و امنیتی نقش بسیار موثری در امنیت و همچنین تسریع در عملکرد سیستم و ... خواهد داشت.

درباره نواقص این سیستم ها نیز می توان عنوان کرد که با توجه به امنیت بالای آنها شاید پس ازاتفاقی، خود شما هم نتوانید به حساب بانکی خود وارد شوید و پول برداشت کنید .آیا در آن لحظه هم نظرتان نسبت به فناوری های بیومتریک مثبت است .

با توجه به ساختار بیومتریک و تشخیص چهره و سایر روشهای این چنینی در پردازش های مالی نقش بسیار مهمی خواهند داشت و به امنیت ورود به ساختار مالی را برای ما به نوعی تضمین خواهند کرد به این نتیجه میرسیم که این فناوری خیلی به کمک ما خواهد آمد.

مراجع

1- Face Recognition by Elastic Bunch Graph Matching website, Bochum University: http://www.neuroinformatik.ruhr-unibochum.

de/VDM/research/computerVision/graphMatching/identification/faceRecognition/contents.html

2-biometric Person Authentication: Odor "Zhanna Korotkaya " Lappeenranta University of Technology

3- Biometric Systems Lab website, Bologna University:http://bias.csr.unibo.it/research/biolab/bio_tree.html.

4- An Introduction to Biometric Recognition Anil K. Jain, Fellow, IEEE, Arun Ross, Member, IEEE, and Salil Prabhakar, Member, IEEE JANUARY 2004

5- Security Technologies Lecture 9 :Authentication –part 2: Biometrics (based on lecture notes by Scarlet Schwiderski-Grosche)