بیومتریک

رویکردی نوین در تامین امنیت

مهدی هاتف[1]

چکیده

امروزه پدیده‌ای به نام بیومتریک[2] مطرح است که در صورت پیشرفت روز افزون می‌تواند دستاوردهای شگرفی در زمینه‌های امنیت نظامی، تجاری و مالی در بر داشته باشد . با توجه به این مطلب، لزوم بررسی، شناخت و برخورد با این پدیده به عنوان صنعتی نوین در جهت اطمینان عمومی به این تکنولوژی مفید، ضرورت می‌یابد. در این مقاله، ابتدا فناوری بیومتریک تعریف شده و سپس انواع، ویژگیها و روشهای پیاده سازی این تکنولوژی مورد بررسی قرار می‌گیرد. در ادامه به کاربردهای این تکنولوژی و وضعیت آن در ایران و جهان پرداخته شده و در نهایت برخی از نقاط ضعف و راهکارهای بهبود آن مورد توجه و بررسی قرار گرفته است. در این مجال سعی شده است جنبه‌های مختلف این تکنولوژی در حد مطلوب معرفی شود تا خواننده بتواند دید مناسبی در این زمینه پیدا کرده و با روشهای نوین برخوردهای امنیتی آشنا شود.

کلید واژه‌ها:

بیومتریک، تصدیق(تایید) هویت، رمز عبور، امنیت عبور، خصوصیات زیستی

---

۱. پژوهشگر دفتر تحقیقات کاربردی مع ط.ب.ب ناجا

2. *Biometric*

مقدمه

ما هر روز از تجهیزات امنیتی ابتدایی استفاده می‌کنیم . به عنوان مثال بـرای اینکـه وارد خانه مان بشویم کلید داریم، برای استفاده از کامپیوتر نیاز به اسم کاربر و رمز عبور داریـم و هنگام استفاده از عابر بانک، هم به کارت و هم به رمز عبور نیاز داریم. خیلی ناراحت کننـده است که کلیدمان را جا بگذاریم، رمزمان را فراموش کنیم و کـارت عـابر بانـک‌مـان را گـم کنیم. اما بدتر از آن وقتی است که کسی به جای ما از آنها استفاده کند، درست مثـل اینکـه خود ما از آن استفاده کرده باشیم. این در حالی است که با تغییرات سریع فنـاوری، ضـریب امنیت افراد و سازمانها نیز کاهش یافته و این امنیت مورد تهـاجم افـراد سـودجو و خرابکـار قرار گرفته است. بنابراین به تناسب پیشرفت سریع شبکه‌های کامپیوتری و ارتباطات، نیاز به روشهای مطمئن تایید هویت افراد هم بیشتر احساس می‌شود. روشهای معمـولی کـه امـروزه برای شناسایی هویت افراد استفاده می‌شود بر دو اساس است، چیزهایی کـه شـما مالـک آن هستید، مثل کلید خانه و کارت اعتباری که اگر گم بشوند بقیه می‌تواننـد تحـت شـرایطی از آن استفاده کنند یا چیزهایی که شما از آن اطلاع دارید مثل نام کاربر و رمز عبـور کـه اگـر خیلی ساده باشند با حدس زدن یا امتحان کردن به راحتـی بدسـت مـی‌آینـد و اگـر خیلـی پیچیده باشند به خاطر سپردن آنها مشکل خواهـد بـود و مجبـور مـی‌شـویم جـایی آنهـا را بنویسیم. در این صورت هم امکان گم یا دزدیده شدن آنها وجود دارد. حالا تصور کنید بـدن شما تبدیل به کلید یا رمز عبور بشود. خصوصـیات فیزیولوژیـک بـدن (ماننـد چهـره و اثـر انگشت) و عادات و رفتارهای شما (مانند دست خـط و صـدا) آنقـدر پیچیـده هسـتند کـه ضریب امنیت را بالا ببرند و مطمئنا نه آنها را جا می‌گذارید و نه فراموش می‌کنید. در واقـع سیستمهای بیومتریک از خود شما برای تایید هویت استفاده می‌کنند. (رستمی، ۱۳۸۶)

بیومتریک چیست؟

" **فناوری بیومتریک** " عبارتست از: روشهای **خودکار** بررسی صحت یا شناسایی هویـت یک **شخص زنده (انسان‌ها)** بر اساس مشخصات فیزیولوژیکی یا رفتاری.

در این تعریف، دو کلمه وجود دارد: «خودکار» و «شخص». لغت «خودکار»، بیومتریک را از حوزه بزرگ‌تر علم شناسایی انسان جدا می‌کند. تکنیکهای تصدیق هویت بیومتریک کـاملاً بوسیله ماشین که عموماً (و نه همیشه) یک کامپیوتر دیجیتال است انجام می‌شوند. بـا وجـود

اینکه تکنیک‌های شناسایی خودکار می‌توانند برای حیوانات، میوه‌ها و سبزیجات و ... نیز مورد استفاده قرار گیرند، موضوع تصدیق هویت بیومتریک، انسان‌های زنده هستند. به این دلیل، احتمالاً صحیح‌ترینست که به این حوزه «تصدیق هویت وابسته به بدن انسان» بگوییم.

کلمه کلیدی دوم «انسان» است. تکنیک‌های آماری، بویژه تکنیک‌هایی که از الگوهای اثر انگشت استفاده می‌کنند، برای متمایز کردن یا ارتباط دادن گروه‌های مختلف مردمی یا احتمالاً ارتباط دادن افراد با گروه‌ها مورد استفاده قرار گرفته اند ولی «بیومتریک » تنها برای شناخت انسانها به صورت فردی است. تمام مقیاس‌های مورد استفاده شامل اجزای فیزیولوژیکی و رفتاری هستند که هر دو آنها می‌توانند به طور وسیعی تغییر کنندیا در طیف وسیعی از جمعیت یکسان باشند. با وجود اینکه به نظر می‌رسد بعضی از مقیاسها بیشتر تحت تاثیر رفتارهستند و بعضی دیگر تحت تاثیر فیزیولوژی، هیچ تکنولوژی‌ای به طور خالص یکی از آنها نیست. اجزای رفتاری تمام مقیاسهای بیومتریک «فاکتورهای انسانی» یا جنبه «فیزیولوژیکی» را به خوبی به تصدیق هویت بیومتریک، نشان می‌دهد. *(Ross, Nandakumar, 2006 & Wayman, Jain, Maltoni & Maio, 2005)*

در عمل، اغلب عبارت «تصدیق هویت بیومتریک» به صورت «بیومتریک» مخفف می‌شود، با این وجود عبارت بیومتریک از نقطه نظر تاریخی، برای شاخه‌ای از زیست شناسی استفاده می‌شده است که با داده‌ها از نقطه نظر آماری و تحلیل کمی سروکار دارد.پس هدف از بیومتریک در این مقاله، با وجود تمام مشابهت‌ها و تفاوت‌های فردی، استفاده از کامپیوتر برای شناسایی فرد است. تصدیق هویت «صحیح» فراتر از هدف تکنولوژی بیومتریک است. در نهایت، عملکرد سیستم تصدیق هویت بیومتریک، و مناسب بودن آن برای هر کار ویژه ای، تعامل فرد با مکانیسم خودکار بستگی دارد. تعامل تکنولوژی با فیزیولوژی و روانشناسی انسان است که بیومتریک را به یک موضوع جالب تبدیل کرده است.

مروری اجمالی بر تاریخچه بیومتریک

متون علمی در مورد اندازه گیری کمی رفتار و عادات و ویژگیهای ظاهری انسانها به منظور شناسایی، به سال‌های ۱۸۷۰ و سیستم اندازه گیری آلفونس برتیلون[1] بر می‌گردد. در

1. *Alphonse Bertillon*

امریکا سیستم برتیلون برای اندازه گیری بدن از جمله اندازه گیری قطر جمجمه و طول بازو و پا برای شناسایی زندانیان تا سال‌های ۱۹۲۰ استفاده می‌شد. هنری فولدز[1]، ویلیام هرشلر[2] و سرفرانسیس گالتون[3] شناسایی کمی از طریق اثرانگشت و اندازه گیری‌های صورت را در سال‌های ۱۸۸۰ پیشنهاد کردند. توسعه تکنیک‌های پردازش سیگنال‌های دیجیتال در سال‌های ۱۹۶۰ به سرعت به کار در زمینه شناسایی خودکار انسان انجامید. سیستم‌های شناسایی صوت و اثرانگشت، جزء اولین‌ها در این زمینه بودند. پتانسیل کاربرد این تکنولوژی برای کنترل فزاینده در ایمنی بالای دسترسی، قفل‌های شخصی و معامله‌های مالی در اوایل ۱۹۶۰ شناخته شد. دهه‌ی ۷۰ سال‌های توسعه و گسترش بکارگیری سیستم‌های هندسه دست و آغاز آزمایش در مقیاس بالا و افزایش علاقه به استفاده دولتی از این تکنولوژی‌های شناسایی خودکار شخصی بود. سیستم‌های تایید امضاء در دهه‌ی ۸۰ و سپس سیستم‌های تشخیص صورت، به میان آمدندو سیستم‌های شناسایی عنبیه در دهه‌ی ۹۰ توسعه یافتند. *(Wayman, Jain, Maltoni & Maio, 2005)*

در سالهای اخیر در ایران نیز فعالیتهایی در زمینه فناوری بیومتریک در حال شکل گیری است به طوری که اولین نشست راهبردی فناوری بیومتریک در کشور خردادماه ۸۵ توسط دفتر همکاریهای فناوری ریاست جمهوری و جمعی از نهادهای مرتبط برگزار شد؛ همچنین در کشور فعالیتهای عملی مانند ساختن دستگاه تشخیص چهره و یا شناخت افراد با استفاده از خطوط کف دست انجام شده است.

بهترین ویژگیها و مشخصه‌های بیومتریک

مشخصات فیزیولوژیکی و رفتاری، امروزه برای شناسایی خودکار از جمله اثر انگشت، صدا، عنبیه، شبکیه، دست، صورت، دست خط، و شکل انگشت استفاده می‌شود. ولی این تنها بخشی از ماجراست چرا که اندازه گیری‌های جدیدی (مانند شیوه راه رفتن، شکل گوش، انعکاس نوری پوست، و بوی بدن) رو به توسعه هستند. به دلیل طیف گسترده مشخصات مورد استفاده، نیاز به تصویربرداری برای این تکنولوژیها رو به افزایش است. این سیستم‌ها

1. Henry Faulds
2. William Herschel
3. Sir Francis Galtan

می‌توانند یک سیگنال تک بعدی مثل صدا را اندازه گیری کنند و یا چندین سیگنال تک بعدی (دست خط)، یک تصویر دو بعدی (اثرانگشت)، چند اندازه گیری دو بعدی (هندسه دست)، مجموعه زمانی از تصاویر دوبعدی (صورت و عنبیه)، یا یک تصویر سه بعدی (سیستم‌های شناسایی چهره) را اندازه گیری کنند. (*Wayman, Jain, Maltoni & Maio, 2005*)

ولی سوال اصلی اینجاست، کدام مشخصه بیومتریک بهترین است؟ مشخصه ایده آل بیومتریک، پنج کیفیت دارد:

۱- ثبات[1]
۲- تمایز[2]
۳- در دسترس بودن[3]
۴- قابلیت دستیابی[4]
۵- قابلیت پذیرش[5]

«ثبات» به معنای عدم تغییر در طول زمان است. «تمایز» به معنای نشان دادن زیادی تغییرات در میان جمعیت است. «در دسترس بودن » به معنای این است که کل جمعیت به طور ایده آل باید این مقیاس را داشته باشند. «قابلیت دستیابی» به معنای آسان بودن تصویر برداری با استفاده از حسگرهای الکترونیکی است. «قابلیت پذیرش» به این معنا است که افراد به گرفتن این اندازه گیریها اعتراض نداشته باشند.

امروزه نحوه‌ی اندازه گیری کمّی این پنج کیفیت مشخص شده است. **ثبات** با «نرخ عدم انطباق » اندازه گیری می‌شود که احتمال عدم تطابق نمونه گرفته شده با تصویر ثبت شده وجود دارد. **تمایز** بوسیله «نرخ انطباق خطا» اندازه گیری می‌شود و احتمال تطابق نمونه گرفته شده با تصویر ثبت شده‌ی یک کاربر دیگر وجود دارد. **در دسترس بودن** بوسیله نرخ «شکست به ثبت نام» اندازه گیری می‌شود، احتمال اینست که یک کاربر قادر به ارائه مشخصات خوانای خود به سیستم به دلیل نوع ثبت مشخصات نباشد، **قابلیت دستیابی** از

1. Robustness
2. Distinctiveness
3. Availability
4. Accessibility
5. Acceptability

طریق «نرخ خروجی» سیستم کمی می‌شود، یعنی تعداد افرادی‌که می‌توانند در یک زمان واحد مشخصاتشان پردازش شود که این زمان واحد می‌تواند یک دقیقه یا یک ساعت باشد . و **قابلیت پذیرش** بوسیله رای گیری از کاربران دستگاه، اندازه‌گیری می‌شود.

با شناسایی مقدارکمیتها و اندازه‌های هر کیفیت، می‌توان اجرای بعضی از آزمایشها برای تعیین اندازه‌های خصوصیات کاربران را ساده‌تر کرد، بنابراین تعیین «بهترین» مشخصه بیومتریک با وزن دهی به ارزش اهمیت هر مورد بدست می‌آید. متاسفانه، در تمام مشخصه‌های بیومتریک، کیفیت‌های مورد نظر به میزان زیادی با مشخصات کاربر، جمعیت (رفتار و فیزیولوژی) و به سیستم سخت‌افزاری/نرم‌افزاری بستگی دارد.در نتیجه، اینکه مشخص کنیم کدام مشخصه بیومتریک برای تمام کاربردها، جمعیتها، تکنولوژیها و سیاست‌های اجرایی بهترین است، ناممکن می‌باشد. تاکنون، در برخی کاربردهای خاص بعضی مشخصات بیومتریک مناسبتر از دیگر مشخصه‌ها تشخیص داده شده است و مجریان سیستم به دنبال بکارگیری بهترین و آشکار ترین مشخصه‌های بیومتریک برای تصدیق هویت به صورت کاملا کاربردی می‌باشند. (*Wayman, Jain, Maltoni & Maio, 2005*)

کاربردهای یک سیستم بیومتریک

اهداف عملی کاربردهای بیومتریک همانند سایر تکنولوژیها متغیر هستند. بعضی از سیستمها به دنبال اشخاص شناخته شده هستند؛ برخی به دنبال اشخاص ناشناس هستند؛ عده‌ای هم به هویت ادعا شده رسیدگی می‌کنند؛ و بعضی بررسی می‌کنند که شخص اصلاً هیچ هویتی در سیستم نداشته باشد. برخی سیستمها یک یا چند نمونه ثبت شده را نسبت به پایگاه داده بزرگ میلیونها الگوی قبلاً ثبت شده، مورد تحقیق قرار می‌دهند؛ بعضی از سیستمها، نمونه‌های ثبت شده را نسبت به الگوهای هویت شناسایی شده و هویت تقلبی مقایسه می‌کنند معدودی از سیستمها یک یا چند الگو را نسبت به تنها یک «الگو» یا «مدل» بررسی می‌کنند.

علاوه بر این کاربردهای بیومتریک متناسب با محیط‌های کاربردی می‌تواند تغییرات زیادی کند، اینکه محیط بیرونی یا داخلی، تحت نظارت یا بدون نظارت و یا با افراد آموزش دیده یا افراد آموزش ندیده است، در استفاده از ابزارها و سیستمهای مورد استفاده متغیر می‌باشد. ما برای درک تمام تکنولوژیها – اهداف کاربردی و محیطی – به یک روش

سیستماتیک نیازمندیم. (*Wayman, Jain, Maltoni & Maio, 2005*) در ادامه بـه هریـک از این طبقه‌بندیها (کاربردی و محیطی) پرداخته شده است.

الف) طبقه بندی بر اساس موارد استفاده

یک سیستم بیومتریک می‌تواند فقط برای آزمایش یکی از دو فرضیه ممکن ذیل طراحـی شود:

۱- نمونه‌های ثبت شده از شخص برای سیستم شناخته شده است.

۲- نمونه‌های ثبت شده از شخص برای سیستم ناشناخته است.

کاربردهایی که برای آزمایش فرضیه اول می‌باشد سیستمهای «شناسـایی مثبـت» اسـت (تایید ادعای صحیح یک ثبت نام)، در حالیکه کاربردهایی که فرضیه دوم را بررسی می‌کنند، سیستم‌های «شناسایی منفی» هستند (تایید ادعای عدم ثبت نام) تمام سیستم‌های بیومتریک از نوع اول یا دوم هستند. این مهمترین وجه تمایز بین انواع سیستمها است.

شناسایی «مثبت» و «منفی»، همزاد یکدیگر هستند، سیستم‌های شناسـایی مثبـت عمومـاً برای جلوگیری از شناسایی چندین کاربر با استفاده از یک هویت به کار مـی‌رود، در حالیکـه سیستم‌های شناسایی منفی برای جلوگیری از استفاده یک کاربر از هویتهای چندگانه بـه کـار می‌رود. در سیستم‌های شناسایی مثبت، ذخیره الگو یا مدل ثبت شده مـی‌توانـد بـه صـورت متمرکز یا نامتمرکز باشد از جمله قرار دادن بر روی کارت‌های هوشمند یا نـوار مغناطیسـی یا دیسکهای نوری، اما سیستم‌های شناسایی منفـی بـه ذخیـره سـازی متمرکـز نیـاز دارنـد. سیستم‌های شناسایی مثبت، چنانچه هیچ تطابقی بین نمونه‌های ثبت شده و الگوهای ثبت نـام شده پیدا نکنند، تقاضای کاربر برای شناسایی را رد می‌کنند. سیستم‌های شناسایی منفـی اگـر تطابقی پیدا کنند، تقاضای کـاربر را رد مـی‌کننـد. بـدون در نظـر گـرفتن نـوع سیسـتم، رد کردن‌های نادرست، برای کاربران باعث اذیت می‌شـود و پـذیرش‌هـای نادرسـت، تقلـب را امکان پذیر می‌کند.

استفاده از بیومتریک در سیستمهای شناسایی مثبت می‌تواند داوطلبانه باشد زیرا روشهای دیگری برای بررسی هویت مورد تقاضا وجـود دارد. آنهـایی کـه عـدم اسـتفاده از روشـهای بیومتریک را انتخاب می‌کنند می‌توانند هویت خود را به صورتهای دیگر تایید کنند، مـثلاً بـا ارائه گذرنامه یا گواهینامه رانندگی، اما در سیسـتمهای شناسـایی منفـی اسـتفاده از سیسـتم

بیومتریک باید برای تمامی کاربران الزامی باشد زیرا هیچ روش دیگری برای تایید یک هویت ناشناخته وجود ندارد.کسانی که به دنبال فریب سیستم شناسایی مثبت هستند باید یک الگوی تطابقی از خود را در سیستم ایجاد کنند و آنهایی که به دنبال فریب سیستمهای شناسایی منفی هستند باید نمونه‌های دیگری را که با الگوهای ثبت شده قبلی فرق دارند، در سیستم ایجاد نمایند. به طور کلی بعضی از سیستمها یک نمونه ورودی را با یک الگوی ذخیره شده مقایسه می‌کنند و یک «بررسی» را انجام می‌دهند(تطبیق یک به یک)، و بعضی دیگر از سیستم ها، یک نمونه ورودی را با تعدادی الگوی ذخیره شده مقایسه می‌کنند و یک «شناسایی» را انجام می‌دهند(تطبیق یک به چند). در جدول شماره(۱)، به طور خلاصه تعدادی از تفاوتهای سیستمهای مثبت و منفی بیان شده است. (*Wayman, Jain, Maltoni & Maio, 2005)*

جدول شماره(۱): روش شناسایی سیستمهای «مثبت» و «منفی»

« مثبت »	« منفی »
برای اثبات اینکه من شخصی هستم که سیستم مرا می‌شناسد	برای اثبات اینکه من شخصی هستم که سیستم مرا نمی شناسد
برای جلوگیری از استفاده چند کاربر از یک هویت	برای جلوگیری از استفاده یک کاربر از چندین هویت
مقایسه یک نمونه گرفته شده با یک نمونه ادعا شده در سیستم. «یک به یک»؛ در اکثر سیستمها به این شکل عمل می‌شود	مقایسه یک نمونه گرفته شده با همه‌ی نمونه‌های موجود در سیستم «یک به چند»
یک «تطبیق اشتباه» منجر به یک «پذیرش اشتباه» می‌شود	یک «تطبیق اشتباه» یا یک «خطا در دریافت» موجب یک «عدم پذیرش اشتباه» می‌شود
یک «عدم تطبیق اشتباه» یا یک «خطا در دریافت» موجب یک «رد اشتباه» می‌شود	یک «عدم تطبیق اشتباه» موجب یک «پذیرش اشتباه» می‌شود
یک روش شناسایی جایگزین وجود دارد	هیچ روش شناسایی جایگزینی وجود ندارد
می تواند داوطلبانه باشد	باید برای همه اجباری باشد
سیستم بوسیله‌ی مشخصات بیومتریک شخص دیگری فریب می‌خورد	سیستم بدون نیاز به مشخصات شخص دیگر یا باعوض کردن مشخصات فریب می‌خورد

منبع: *(Wayman, Jain, Maltoni & Maio, 2005)*

ب) طبقه بندی بر اساس محیط‌های کاربردی

در اوایل دهه ۱۹۹۰، همگام با کسب تجربه در استفاده از ابزارهای بیومتریک، معلوم شد که تغییر در محیط‌های کاربردی، اثر قابل توجهی بر نحوه عملکرد ابزار دارد. در واقع، مشخصات محیط کاربردی در انتخاب بهترین تکنولوژی بیومتریک و پیش بینی مشخصات عملکردی سیستم،اساسی است. روش ذیل برای تحلیل محیط عملکردی پیشنهادی، از طریق متمایز کردن کاربردها براساس تقسیم بندی آنها به شش گروه، فراتر از کاربردهای "مثبت" و "منفی" که قبلا به آنها پرداخته ایم، ارائه شده است. (*Wayman, Jain, Maltoni & Maio, 2005)*

۱- محسوس در برابر نامحسوس[1]

بخش اول، "محسوس/ نامحسوس" است. اگر کاربر آگاه باشد که توسط شناساگر بیومتریک، اندازه گیری می شود، استفاده محسوس است و اگر آگاه نباشد، استفاده نامحسوس می‌باشد.

۲- آشنا در مقابل ناآشنا[2]

بخش دوم "آشنا/ ناآشنا"، این سیستم برای کاربران داوطلب به کار می رود. کاربرانی که یک ویژگی بیومتریک را به صورت روزانه به سیستم ارائه می دهند می توانند بعد از زمان کوتاهی، برای سیستم آشنا در نظر گرفته شوند. کاربرانی که به تازگی توسط سیستم، اطلاعات بیومتریک آنها گرفته نشده، ناآشنا در نظر گرفته می شوند.

۳- با مراقب در مقابل بی مراقب[3]

بخش سوم " بامراقب/بی‌مراقب" است و به این امر دلالت دارد که آیا استفاده از ابزار بیومتریک در طول عملکرد بوسیله مدیریت سیستم مشاهده و هدایت می شود؛ سیستمهای بدون مراقب عموماً به عملکرد نظارت شده نیازدارند در حالیکه سیستمهای با مراقب ممکن است به نظارت نیاز داشته باشند و یا نیاز نداشته باشند. تقریباً در تمام سیستم‌ها، فرآیند اجرا را نظارت می‌کنند، این در حالی است که بعضی از سیستمها نیز این نظارت را ندارند.

---

1. Overt vs Covert
2. Habituated vs Non-Habituated
3. Attended vs Non-Attended

۴- محیط استاندارد در مقابل محیط غیر استاندارد[1]

بخش چهارم محیط فعالیت "استاندارد/ غیر استاندارد" است. اگر کاربرد به صورت داخلی در دمای استاندارد ۲۰ درجه سانتیگراد و فشار یک اتمسفر و دیگر شرایط محیطی بویژه در شرایط نوری قابل کنترل، انجام گیرد، سیستم دریک "محیط استاندارد" است. سیستم‌های بیرونی و احتمالاً بعضی از سیستمهای درونی غیر معمول سیستم‌هایی در "محیط غیر استاندارد" در نظر گرفته می شوند.

۵- عمومی در مقابل شخصی[2]

بخش پنجم "عمومی/ شخصی" است. آیا کاربران سیستم، مشتریان مدیریت سیستم (عمومی) هستند یا کارمند (شخصی) هستند؟ به وضوح، روش استفاده از ابزارها- که به صورت مستقیم بر عملکرد تاثیر دارد- به تناسب رابطه بین کاربران نهایی ومدیریت سیستم تغییر می نماید.

۶- باز در مقابل بسته[3]

بخش ششم "باز/ بسته" است. آیا سیستم، در حال حاضر یا آینده به تبادل داده با دیگر سیستمهای بیومتریکی که با مدیریت دیگری اجرا می‌شود نیاز دارد؟ به عنوان مثال، بعضی از آژانسهای سرویس اجتماعی در امریکا مایل به تبادل اطلاعات بیومتریک با دیگر ایالتها می‌باشند که اگر در یک سیستم باز باشد، جمع آوری داده‌ها، تراکم و استانداردهای جهانی ویژگیهای مورد نیاز هستند. اما یک سیستم بسته می‌تواند بخوبی بر روی مزیتهای کاملاً اختصاصی کار کند.

الگوی عمومی سیستم بیومتریک

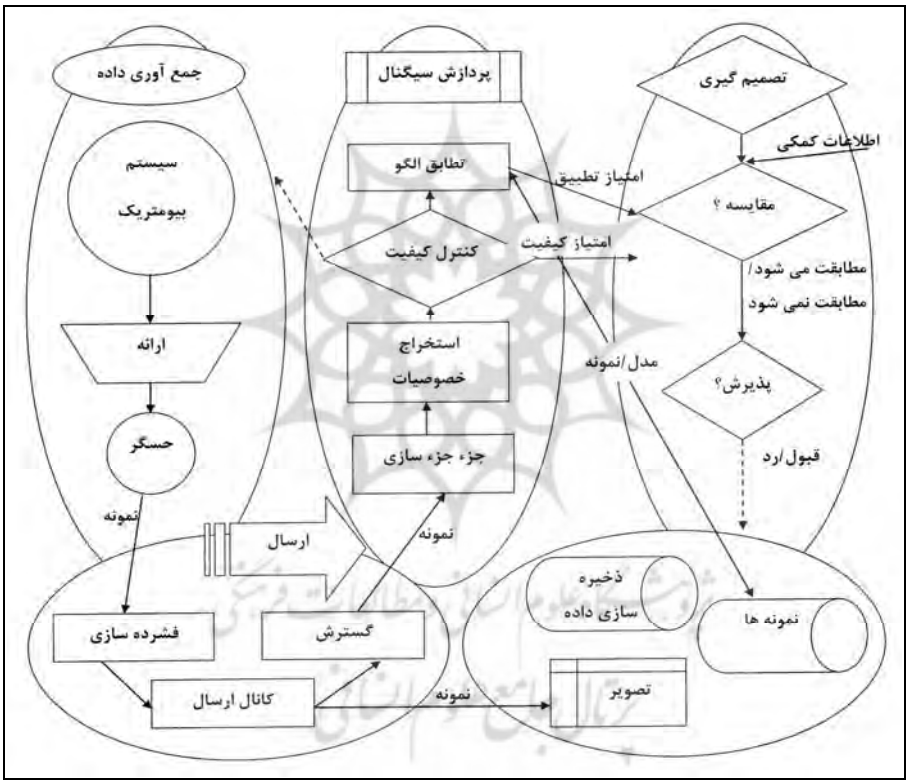
با وجود اینکه سیستمهای بیومتریک به تکنولوژیهای بسیارمتفاوتی وابسته هستند، می‌توان به طور عمومی راجع به آنها صحبت کرد، شکل بعد، یک سیستم عمومی تعیین بیومتریک را نشان می‌دهد که به پنج زیر سیستم تقسیم شده است:

---

1. Standard vs Non-Standard Environment
2. Public vs Private
3. Open vs Closed

۱- جمع آوری داده،
۲- ارسال،
۳- پردازش سیگنال،
۴- تصمیم گیری،
۵- ذخیره داده

شکل شماره (۱): سیستم عمومی بیومتریک



منبع: (Wayman, Jain, Maltoni & Maio, 2005)

بیومتری‌های مختلف در انسان

ویژگی‌های بیومتریک به طور عمده به دو دسته تقسیم می‌شوند:

الف) خصوصیات فیزیولوژیکی، که به ساختار و شکل بدن مربوط می‌شوند. قدیمی‌ترین آن‌ها اثر انگشت است که بیشتر از ۱۰۰سال پیش تاکنون استفاده می‌شده است. شناسایی از طریق چهره، ساختار رگ‌ها، ساختار دست، انگشت‌ها و اسکن عنبیه روشهای نوینی است که امروزه استفاده می‌شود.

ب)خصوصیات رفتاری، همانطور که از اسمش پیداست برخی از رفتارهای انسان را بررسی می‌کند. اولین ویژگی از این دست که به طور گسترده تا به امروز نیز استفاده می‌شود امضا است.البته امروزه بررسی دست خط و روش‌های جدیدتر مانند ریتم تایپ کردن و صدای افراد نیز استفاده می‌شود. (حسن‌آبادی، ۱۳۸۶)

اثر انگشت

یکی از قدیمی‌ترین و فراگیرترین روشها است که ویژگی‌های مربوط به نمونه‌های شیارهای سرانگشت مانند تعداد لبه‌ها، نوع طرح، فاصله بین لبه‌ها، نقطه مرکزی، و منافذ را اندازه‌گیری می‌کند. نمونه‌های آن از طریق تکنیکهای اسکن مسطح، اسکن گرداگرد (با استفاده از ۱۰ تصویر) و یا تصویر ۴ انگشت در یک زمان جمع‌آوری می‌شود.

ویژگی‌های مربوط به صورت

در این روش، هندسه مربوط به صورت یا به عبارتی فاصله بین اجزا (بینی و دهان و ...) و یا در مواردی وضعیت بافت پوست صورت بررسی می‌شود. نمونه‌های این روش با استفاده از دوربین ثابت، ویدئو و عکاسی با اشعه حرارتی مادون قرمز[1] جمع‌آوری شده و از طریق الگوریتمهای تحلیل ویژگی‌های محلی، شبکه‌های عصبی و تحلیل بافت سطحی پردازش می‌شوند.

تشخیص عنبیه چشم

در این روش ویژگی‌های وابسته به بافت تصادفی قسمتهای رنگی چشم اندازه‌گیری می‌شود و تا ۲۶۶ ویژگی منحصربفرد قابل شناسایی است. برای نمونه برداری از اشعه مادون

1. Thermal Imaging

قرمز در فاصله نزدیک استفاده می‌شود.از مشکلات این روش آن است کـه ممکـن اسـت از برخی بیماریهای چشم مانند آب مروارید متاثر شود.

وضعیت هندسی دست

در این روش ابعاد دست شامل شکل و طول انگشتان اندازه‌گیری می‌شود و به طور وسیع بـرای کنتـرل دسترسـی فیزیکـی در مکانهـایی ماننـد وزارت دفـاع و مراکـز هسـته‌ای و فرودگاه‌های آمریکا مورد استفاده قرار گرفته است. این روش درصـد خطـای بسـیار پـایینی دارد.

بازبینی گفتار

در این روش گام و اوج و همچنین آهنگ و تن صدای هر فرد با آنچـه بـه عنـوان مـدل صحبت او از قبل ذخیره شده، مقایسه می‌شود. یگانگی بر اسـاس تفاوتهـای تارهـای صـوتی، طول و شکل دهان و حفره بینی مشخص می‌شود. ایـن روش هـم رفتـاری و هـم فیزیولـوژی محسوب می‌شود و ممکن است به خاطر عواملی چون بیماری و اسـترس بـه درسـتی عمـل نکند.

بازبینی امضای حرکتی

در این روش ویژگی‌های امضای دستی هر فرد چون شکل، سرعت، فشار، زاویه قلم، توالی ترسیم و.. اندازه‌گیری می‌شود. در اینجا ویژگی‌های رفتاری بـا اسـتفاده از لـوح امضـا و قلـم مخصوص اندازه‌گیری شده و بیشتر در مراکز خرید کاربرد دارد. فاکتورهای رفتـاری ماننـد استرس، گیجی و حالت نشسته یا ایستاده این روش را متاثر می‌کند.

اسکن شبکیه چشم

در این روش باتاباندن نور از طریق مردمک چشم، نقشه و وضعیت رگهای خونی شـبکیه اندازه‌گیری می‌شود. این روش دشوارتر از اسکن عنبیـه اسـت و معمـولاً بـرای کاربردهـای امنیتی سطح بالا استفاده می‌شود.

چگونگی نواخت کلید

این روش که یک فاکتور رفتاری است و به عنوان «الگوی تایپ» هم شناخته می‌شود، چگونگی تعامل یک فرد با صفحه کلید و مواردی چون مدت فشرده شدن هر کلید، فرکانس خطا در تایپ، میزان فشار به کلید و ... را اندازه‌گیری می‌کند و معمولاً در هنگام اخذ کلمه عبور استفاده می‌شود.

دی.ان.ای (DNA)[1]

در این روش از ویژگی‌های ثابت رشته *DNA* هر فرد (بیش از ۶ میلیارد ویژگی برای هر فرد) برای تشخیص هویت استفاده شده و روشی فوق‌العاده دقیق است. به علت نیاز به نمونه‌گیری برای هر بار تصدیق هویت و همچنین زمان زیاد مورد نیاز برای بررسی (بیش از ۱۰ ساعت)، استفاده از این روش بسیار دشوار و محدود به موارد حساس است.

نقشه کف دست

این روش همانند روش اثرانگشت، ولی در مقیاسی بزرگتر از آن است و بنابراین ویژگی‌های بیشتری برای تصدیق هویت از آن قابل استخراج است. در این روش ویژگی‌های کف دست افراد مانند وضعیت شیارها، وضعیت خطوط کف دست و ناحیه دلتا و همچنین ویژگی‌های بافت پوست اندازه‌گیری می‌شود.

نقشه رگهای دست

از آنجا که نقشه رگهای پشت دست و همچنین رگهای مچ دست برای افراد مختلف متمایز است، این روش نیز برای تصدیق هویت قابل استفاده است. در این روش از اشعه مادون قرمز برای عکس‌برداری از رگها استفاده می‌شود. این روش هنوز در مرحله تحقیق است.

چگونگی راه رفتن

این روش یک روش بیومتریک رفتاری است و مشخصاتی مانند میزان تاب خوردن بازوها، ریتم راه رفتن، میزان حالت فنری و سبکبال راه رفتن، طول قدمها، فاصله بین سر و پا، فاصله بین سر و لگن خاصره و ... اندازه‌گیری می‌شود.

---

1. Deoxyribonucleic Acid

شکل گوش

شکل و اندازه گوش بر خلاف صورت، در سنین مختلف و همچنین در حالات و فشارهای روحی و روانی مختلف تغییر نکرده و تقریباً ثابت است و از این رو به عنوان یک روش جدید مورد توجه قرار گرفته است.

بوی بدن

این روش بیومتریک بر این حقیقت استوار است که هر انسانی بوی مخصوص به خود را دارد و وابسته به ترکیبات شیمیایی فراری میباشد که از طریق بدن متصاعد می‌شوداین ترکیبات از طریق سنسورهایی قابل جمع‌آوری و ذخیره هستند. این روش نیز در مرحله تحقیق است و مزایا و معایب مخصوص به خود را دارد، از جمله اینکه بدن انسان بر اثر حالتها و فعالیتهای مختلف، بوهای متفاوتی را از خود متصاعد می‌کند.

ساختار ناخن

ذخیره بر روی ناخن روشی است که در آن با استفاده از لیزر بر روی ناخن نوشته می‌شود که این نوشته در هنگام تابیده شدن نور ماورای بنفش از طریق میکروسکوپ قابل خواندن می‌باشد. این روش به عنوان یکی از روشهای جدید تصدیق هویت پیشنهاد شده است.

تشخیص لبخند

در این روش چگونگی تغییر فرم ماهیچه‌های صورت در دو حالت قبل و بعد از لبخند اندازه‌گیری می‌شود. این روش از طریق گریم و یا اندازه لبخند افراد متاثر نمی‌شود و آنقدر حساس است که حتی در حالتی که فرد سعی می‌کند چهره خود را بدون تغییر نشان دهد، انقباض ماهیچه‌ها را اندازه‌گیری می‌کند.

کاربردهای بیومتریک در ایجاد امنیت

کاربردهای گوناگونی برای سامانه‌های بیومتریکی در حوزه‌های گوناگون امنیتی متصور است. در این میان کاربردهایی برای بیومتریک‌ها قابل ذکر است که عبارتند از:

شناسایی مجرمان

انگشت نگاری جز متداولترین فناوریهای بیومتریکی مورد استفاده در این حوزه می‌باشد. مراجع قضایی تقریباً در تمام جهان اثرانگشت را بعنوان یک مدرک مستند در مباحث جرم شناسی به رسمیت می‌شناسند. بانک داده‌های یکپارچه اف بی‌آ ی[1] که به *IAFIS*[2] مشهور است، هم اکنون دارای ۴۰ میلیون ثبت ۱۰ انگشتی است که روزانه هزاران جستجو جهت شناسایی مجرمان، در آن انجام می‌شود. این بانک داده با دیگر بانکهای اطلاعاتی موجود در سامانه‌های نظارتی و پیگردی امریکا در ارتباط است. همچنین اخیراً این اطلاعات با بانک اطلاعات بیومتریکی اسکاتلندیارد[3] هم به اشتراک گذاشته شده تا امکان استفاده همزمان از اطلاعات این منابع میسر شود.

کاربردهای تجاری(تجارت الکترونیک/ تلفنی، خرده فروشی/ خودپردازها/ پایانه‌های فروش)

تراکنشهای مالی و اعتباری، تأیید هویت مشتریان و دسترسی به حسابها یا صندوق امانات و... از جمله مهمترین کاربردهای بیومتریک در این حوزه بشمار می‌رود که تا کنون مجموعه‌ی متنوعی از بیومتریکهای مختلف برای این منظور استفاده شده است. بخشی از این کاربردها ممکن است حفاظتهای داخلی یا زیرساختی از قبیل کنترل دسترسی به اماکن امنیتی یا شبکه‌های رایانه‌ای برای جابجایی سرمایه‌های الکترونیکی باشد. یا درکاربردی گسترده تر شاید حفاظت از اسرار و هویت افراد باشد. به ویژه اولین کاربردی که به ذهن خطور می‌کند، حفاظت ازخود پردازها، کارتهای اعتباری و چکها، با شناسه‌های بیومتریکی می‌باشد. امروزه کارتهای خود پرداز با رمزهای عبور حفاظت می‌شوندکه چالشهای امنیتی و کاربری فراوانی را در پی داشته است. در این شرایط فناوری بیومتریکی رفته رفته جایگزین رمزهای عبور می‌گردد. در ژاپن رگ‌نگاری کف‌دست، در کانادا عنبیه نگاری، در امریکا و اروپا انگشت‌نگاری و چهره‌نگاری پرکاربردترین بیومتریکها در حوزه‌ی بانکداری الکترونیکی و تجارت الکترونیک محسوب می‌شود.

---

1. Federal Bureau of Investigation (FBI)
2. Integrated Autmated Fingerprint Identifiction System (IAFIS)
3. Scotland Yard

دسترسی به رایانه‌های شخصی/ شبکه

انگشت نگاری پرکاربردترین بیومتریک در این حوزه است. اخیراً مایکروسافت[1] سیستم عامل خود را مجهز به رابط برنامه کاربردی بیومتریک کرده است. لپ تاپهای جدید آی‌بی‌ام[2] و هم حافظه‌های فلش شرکت ترانسند[3] مجهز به حسگر انگشت نگاری شده اند.

دسترسی فیزیکی/ زمانی و حضور

نسل جدید سیستمهای ساعت زنی و حضور و غیاب هم از جمله تجهیزاتی است که به فناوری بیومتریک مجهز شده است. انگشت نگاری، دست نگاری و چهره نگاری از جمله‌ی پرکاربردترین بیومتریکها در این بخش می‌باشد. این سیستمها در سالهای اخیر رواج زیادی پیدا کرده اند و اخیراً در کشور خودمان هم نمونه‌های مختلفی از آن ارائه شده است.

شناسایی شهروندان

طیف وسیعی از بیومتریکها در کاربردهای گوناگون شناسایی شهروندان مورد استفاده قرار می‌گیرد که انگشت نگاری در صدر قرار دارد.

نظارت

با توجه به ماهیت کاربری نامحسوس چهره نگاری، این فناوری کارکرد فوق العاده‌ای در نظارت محسوس و نامحسوس دارد. بسیاری از خیابانهای ناامن شهر لندن هم اکنون به دوربینهای مدار بسته‌ای مجهز شده است که امکان تشخیص هویت افراد سابقه‌دار یا تحت‌پیگرد توسط آنها به راحتی ممکن شده است. همانطور که در جریان شناسایی عاملین بمب‌گذاریهای سال گذشته از این فناوری استفاده شد. (*www.irbiometric.ir & www.biometric.ir*)

---

1. Microsoft
2. IBM
3. Transcend

مزایا و معایب سیستمهای بیومتریک در تأمین امنیت

روشهای بیومتریک اطمینان می‌دهند که هر فرد در صورت شناسایی، همان کسی است که ادعا کرده و به راحتی قابل جعل نبوده و کاربران در استفاده از آن راحتتر هستند. ولی استاندارد خاصی برای آنها در صنعت وجود ندارد و همچنین این سیستمها قابل استفاده از راه دور نیستند. ضمن اینکه امکان تشخیص نادرست نیز در آنها وجود دارد. همچنین از آنجا که داده‌های جمع‌آوری شده بیومتریک مربوط به مشخصات افراد بوده و بر خلاف کلمه عبور قابل تغییر نمی‌باشد، سرقت آنها می‌تواند مشکلات بسیاری را به وجود آورد. از اینرو استفاده از این روشها دارای مزایا و معایبی می‌باشد که در ذیل به آنها اشاره می‌کنیم:

الف) مزایا:

افزایش ایمنی:

کدها و رمزهای عبور به سادگی حدس زده می‌شوند یا قابل شکستن هستند. ابزار همراه مثل کلیدها، نشانها و کارتها قابل سرقت هستند. بسیاری از کاربران از اعداد یا کلمات واضح و قابل حدسی به عنوان رمز عبور استفاده می‌کنند. مخصوصاً وقتی تعداد رمزهای مورد استفاده زیاد باشد بعلت مشکل فراموشی، ساده انتخاب می‌شوند یا در جایی دم دست نوشته می‌شوند. در مقابل بیومتریکها قابل سرقت یا فراموشی نیستند. نیاز به نگهداری خاصی ندارند.

افزایش راحتی:

دلایلی که قبلا ذکر کردیم خود گواهی بر سهولت استفاده از بیومتریکها بجای ابزار رایج فعلی می‌باشد با استفاده از تکنولوژیهای بیومتریکی سرعت دستیابی به منابع مورد نظر افزایش می‌یابد. هزینه نگهداری از سیستمها و مسایل امنیتی مربوطه کاهش چشمگیری می‌یابد.

جلوگیری از تقلب:

در موارد استفاده از منافع عمومی، ورود به مراکز امنیتی، کاربردهای روزانه، انجام امور مالی و... بیومتریکها مانع تقلب افراد سودجو می‌شود.

تشخیص مظنونین:

با استفاده از بیومتریکها هویت واقعی افراد آشکار می‌شود یکی از مهمترین دلایل گسترش استفاده از این تکنولوژیها مبارزه با تروریسم، مهاجرتهای غیر قانونی، فرار از قانون و... می‌باشد.

ب) معایب:

در مقابل انتقاداتی هم به استفاده از بیومتریکها وارد است. در طرحهای عمومی که تمامی شهروندان جامعه ملزم به ارائه اطلاعات بیومتریکی خود هستند؛گروههای فعال حامی آزادیهای اجتماعی وجود این سیستمها را نافی آزادی انسانی می‌دانند و معتقدند این تکنولوژی در کشورهای مورد استفاده نتوانسته مانع تروریسم شود. گذشته از اینها هریک از سیستمهای بیومتریکی از ثبت اطلاعات بعضی افراد به علل مختلف (جراحت یا معلولیت، عدم اطلاعات متمایز کننده کامل)یا بعلت حساسیت بعضی سیستمها به شرایط محیطی از ثبت کامل همه داده‌ها عاجزند. *(www.irbiometric.ir & www.biometric.ir)*

چند نمونه از فعالیتهای عملی در زمینه تامین امنیت در جهان

الف) ابزارهای تعیین هویت چندگانه

تقاضا برای امنیت بیشتر در مرزها، شهرها، اماکن دولتی و شرکتها از رونق بیو متریک خبر می‌دهد. انتظار می‌رود سیستمهایی که به طور دیجیتالی به بررسی اثر انگشت افراد می‌پردازد، الگوهای عنبیه چشم آنان را تحلیل می‌کند، ابعاد منحصر به فرد چهره‌ها را می‌سنجد یا صدای افراد را تشخیص و تمییز می‌دهد، در سالهای اخیر یک تجارت چند میلیارد دلاری را تشکیل دهد. اما در این میان مشکلی وجود دارد:" هیچ روشی وجود نداردکه درمورد تمام افراد کاربرد داشته باشد ". در حدود ۳ درصد مردم فاقد اثر انگشتهای قابل تشخیص هستند و شاید ۷درصد افراد رنگدانه‌هایی درچشم خود داشته باشند که در اسکنهای عنبیه تداخل ایجاد کند. نقابها مانع کار نرم افزار شناسایی چهره می‌شوند و تغییرات مختلف در آرایش موها یا نور محیط در کار این نرم افزار اختلال ایجاد می‌کنند.

حتی می‌توان تکنولوژیهای بیومتریک را فریب داد. این امکان وجود دارد که اثر انگشت باقیمانده روی حسگر برداشته شده و توسط شخص دیگری استفاده شود و بسیاری از نرم افزارهای شناسایی چهره را می‌توان با عکسها یا کلیپهای ویدئویی فریب داد. به گفته‌ی، مدیر برنامه‌های رفتاری و بیومتریکی در دفتر علم و تکنولوژی وزارت امنیت داخلی ایالات‌متحده،"هیچ یک از تکنولوژی‌های بیومتریک بی عیب و نقص نیست" درحال حاضر، مراکز تحقیقاتی شرکتها و دانشگاهها در گوشه و کنار جهان، با تلفیق بیومتریکهای متعدد درسیستمهایی انعطاف پذیر و دقیق، سرگرم رفع این نقاط ضعف هستند. این بیومتریکهای به اصطلاح چند وجهی، معمولاً با در نظر گرفتن ضریب احتمالات هر کدام از سنجشهای بیومتریک و تلفیق آنها به یک نتیجه واحد در مورد تایید یا رد هویت افراد تصمیم می‌گیرند.

نرم افزار بایو آی دی فیس[1] در آلمان، برای احراز هویت افراد از شناسایی چهره، ثبت صدا و حرکات لب استفاده می‌کند و اولین کالای تجاری در زمینه بیومتریکهای چند وجهی به شمار می‌رود. پیش از این، تکنولوژی هیومن اسکن[2] برای حفاظت از برخی شبکه‌های کامپیوتری نظامی و ایمنی نگهداشتن پول مشتریان بانکها از دست شیادان و مدعیان دروغین مورد استفاده قرار می‌گرفت. اما این شرکت در سال جاری با همکاری شرکت آی بی کول[3] (یک شرکت تجاری سازی فناوری که دفتر مرکزی آن در مونیخ آلمان است) درصدد نصب آزمایشی این تکنولوژی است تا به تعیین هویت مسافران ورودی و خروجی از ایالات متحده و آلمان بپردازد.

شرکت آی دنتیکس[4] با افزودن یک بیومتریک دیگر به ترکیب دو سیستمی فعلی خود (نرم‌افزار شناسایی چهره و اسکنرهای اثر انگشت) درصدد تقویت آن برآمده است و این بیومتریک جدید استفاده از بافت پوست است. شناساگر جدید که به اثر پوست[5] مشهور شده آکنده از الگوریتم‌هایی است که الگوهای بافتی را از تصاویر دوربین دیجیتالی استخراج

1. BioID Face
2. Human Scan
3. IBCOL
4. Identix
5. Skinprint

می‌کنند. به گفته رئیس این شرکت، با کمک این تکنولوژی جدید، سیستم‌های شناسایی چهره می‌توانند با همان دقت اثر انگشت، دوقلوهای همسان را نیز از یکدیگر تشخیص دهند، دقتی که سال‌های سال استاندارد طلایی انواع بیومتریک محسوب می‌شد.

اما در یک نمونه بسیار خطیر، مقامات رژیم اشغالگر قدس، با تلفیق سیستم شناسایی چهره با بیومتریک "هندسه دست" از این نرم افزار استفاده کردند تا ورود و خروج ۵۰ هزار کارگر به نوار غزه را زیر نظر داشته باشند. (اریکا جونیتس)

جدول شماره (۲): چند نمونه از ساخت بیومتریکهای چند وجهی

گروه	راهبرد
Humanscan (ارلانگن، آلمان)	تحلیل چهره، صدا و حرکات لب برای ایمن سازی دستیابی فیزیکی و شبکه‌ای
Identix	ترکیب داده‌های بافت پوست با داده‌های اثر انگشت با چهره
ویجی کومار با گاواتولا-دانشگاه کرنگی ملون (پیتسبورگ)	ادغام داده‌های بیومتریکهای چهره، اثر انگشت و عنبیه
مایک فایر هورست -دانشگاه کنت انگلستان - ونوی ساینس (سوتهامپتون، انگلستان)	نرم افزاری برای مدیریت بیومتریکهای متعدد ازجمله صدا، چهره و اثر انگشت
آنیل جین دانشگاه ایالتی میشگان	ترکیب داده‌های بیومتریکهای مختلف از جمله چهره،اثر انگشت، عنبیه، هندسه دست وصدا و ترکیب سیستم‌های شرکت‌های مختلف

ب) صدور گذرنامه‌های بیومتریکی در کشورهای جهان

این علامت، نشان گذرنامه‌های بیومتریکی است که معمولا بر روی جلد این گذرنامه‌ها چاپ می‌گردد.یک گذرنامه بیومتریکی ترکیبی از صفحات کاغذ و مستندات شناسایی الکترونیکی افراد است که از مشخصات بیومتریکی برای تصدیق شهروندی افراد استفاده می‌شود. اطلاعات کلیدی گذرنامه روی یک ریزتراشه کامپیوتری بسیار کوچک ذخیره می‌گردد که بسیار شبیه به ذخیره اطلاعات بر روی کارتهای هوشمند می‌باشد. این گذرنامه‌ها اطلاعات شخص را بر روی ریزتراشه بدون تماس که بصورت نهفته در گذرنامه

قرار دارد ثبت می‌نمایند. این ریزتراشه قادر است اطلاعات امضای دیجیتال را برای اطمینان از صحت گذرنامه و اطلاعات بیومتریکی در خود نگاه دارد.

تا به حال کشورهای زیر در اروپا، امریکا، آسیا و اقیانوسیه بـه گذرنامـه‌هـای بیـومتریکی مجهز گشته‌اند "اتریش، بلژیک، جمهوری چک، دانمـارک، نـروژ، اسـتونی، فنلانـد، فرانسـه، آلمان، یونان، مجارستان، ایسلند، جمهوری ایرلند، ایتالیا، لیتـوانی، جمهـوری مقدونیـه، هلنـد، لهستان، پرتغال، اسلونی، اسپانیا، سوئد، سـوئیس، انگلسـتان، ایـالات متحـده امریکـا، کانـادا، استرالیا، نیوزلند، پاکستان، سنگاپور، مالزی، ژاپن و هنگ کنگ".

چند نمونه از فعالیتهای بیومتریک در ایران

الف) طراحی و صدورگذرنامه‌های بیومتریک توسط وزارت امور خارجه ایران

ب) طراحی سیستم شناسایی چهره در مرکز تحقیقات مخابرات ایران

ج) طراحی نرم افزار شناسایی افراد با استفاده از خطوط کف دست در دانشگاه مهندسـی کامپیوتر و فناوری اطلاعات دانشگاه صنعتی امیرکبیر

د) سیستمهای بیومتریک حضور و غیاب با استفاده از ثبت اثر انگشت

نتیجه گیری و ارائه پیشنهادات

جهت حفظ امنیت عمومی و امنیت در مراکز حساس نظـامی، تجـاری و اداری روشـهای بیومتریک روشهای بسیار مناسبی به نظر می‌رسند و پیش‌بینی‌ها حکایت از رشد ۱۰ برابـری کاربرد این فناوری در آینده نزدیک دارد. همچنین طبق برآوردهای اقتصادی درآمـد بـازار فناوری بیومتریک دنیا در بازدهی زمانی سالهای ۲۰۰۳ تا ۲۰۰۸ حدود ۷ برابر رشد می‌کند که نویدبخش رونق و همه گیـری اسـتفاده از انـواع ایـن فنـاوری در کاربردهـای گونـاگون می‌باشد. با این همه در بحث توسعه‌ی کاربری این فناوری مسایلی وجود دارد کـه در جـای خود چالش برانگیـز و در خـور تأمـل اسـت. میـزان تطبیـق ایـن فنـاوری بـا زیرسـاختها و سامانه‌های فناوری اطلاعات (شبکه، کارت هوشـمند، سـامانه‌هـای مـدیریت سـازمانی و...) نگرانیهای مربوط به سـامانه‌هـای امنیتـی و چالشـها و تبعـات اجتمـاعی و حقـوقی از جملـه

مهمترین مسایلی است که می‌بایست از سوی کاربران، مجریان و برنامه ریزان این حوزه مورد اهتمام و توجه ویژه قرار گیرد. باید توجه کرد که در حوزه‌ی تشخیص هویت همواره یک مصالحه بین افزایش امنیت و تحدید حریم خصوصی و آزادیهای فردی وجود دارد. طراحی و اجرای صحیح برنامه‌های کسب آمادگی پذیرش یک فناوری جدید و فرهنگ سازی کاربرد آن قبل از اجرای پروژه‌ها و نیز برنامه‌های حین کاربرد از جمله موارد ضروری جهت از بین بردن این تصور بشمار می‌رود.

منابع :

- حسن آبادی، مهدی (۱۳۸۶)، " تکنولوژیهای تصدیق هویت "، مجله رایانه شماره ۱۶۷.
- جونیتس، اریکا (۱۳۸۴)، " تقویت بیومتریک"، مجله رایانه شماره ۱۴۴.
- رستمی، مرضیه، "وقتی بدن ما رمز عبور است"، روزنامه جام جم مورخ ۲۱ تیر ۸۶.
- وب سایت ملی بیومتریک *http:// www.irbiometric.ir/*
- وب سایت اندیشکده بیومتریک فردا *http:// www.biometric.ir/*

- *A.A.Ross,K.Nandakumar,A.K.Jain (2006); Handbook of Multibiometrics; © Springer Science+Business Media, LLC*
- *J.Wayman, A.Jain, D.Maltoni and D.Maio(2005);Biometric SystemsTechnology, Design and Performance Evaluation; © Springer-Verlag London Limited*