یادداشت علمی

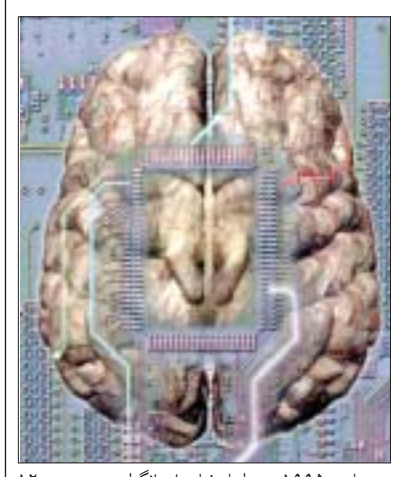
مراقبت از افکار

در جنگ الکترونیکی

ترجمه: علیرضا سزاوار

دکتر ماتسودا پدر جامعه اطلاعاتی در سال ۱۹۸۰ عنوان کرد که آزادی ما با استفاده از علم سایبرنتیک (که برای اکثر مردم ناشناخته است) تهدید می شود. این فناوری مغز انسان‌ها را به وسیله تراشه‌های کاسته شده در بدن، به ماهواره‌های تحت نظارت ابرکامپیوترهای زمینی ارتباط می دهد. از روش های مراقبت از افکار استفاده می کند تا رفتار و اخلاق انسان ها را تغییر دهد. تاثیرگذاری بر کارکرد مغز یک هدف مهم برای اهداف نظامی و اطلاعاتی است. ۳۰سال پیش پرتو ایکس می توانست تراشه های کاشته شده در بدن انسان را که به اندازه یک سانتی متر بود نشان دهد. امروزه این تراشه ها تا اندازه یک دانه برنج کوچک شده‌اند. این تراشه‌ها در ابتدا از سیلیکون ساخته می شدند، ولی امروزه از جنس آرسنیدگالیم هستند. امروزه آنها به قدری کوچک‌اند که با عمل جراحی و یا حتی شلیک مخفیانه که شخص متوجه آن نمی شود، در بخش های مختلف بدن از جمله گردن و پشت سر نصب می شوند که تقریباً غیرقابل شناسایی و درآوردن هستند.

روش کار به گونه‌ای است که حتی امکان کارگذاری این تراشه ها در بدن هر بچه تازه به دنیا آمده‌ای نیز وجود دارد که از آن پس تا پایان عمر، عمل شناسایی فرد به وسیله تراشه‌ها انجام می شود. تراشه‌های امروزی با فرکانس پایین رادیویی کار می کنند و آنها را هدف می گیرند. به این ترتیب فرد تراشه گذاری شده با استفاده از ماهواره‌ها در تمام جهان به راحتی ردیابی می شود. وقتی یک تراشه هفت میکرومتری (یک‌دهم یک تار موی انسانی) در عصب بینایی چشم قرار می گیرد می تواند ضربان عصبی مغز را جذب کند و تمام اطلاعات دریافت شده شخص را به ابرکامپیوتر مربوطه انتقال داده و سپس از طریق تراشه برای تجربه مجدد به شخص بازگردانده می شود. یک کامپیوتر می تواند با استفاده از روش مشاهده دور (RMS) سیگنال های رمزگذاری شده را بفرستد و بر رفتار شخص تاثیر بگذارد. این روش باعث می شود که شخص سالم دچار توهم شود یا صداهایی بشنود. هر فکر، عکس العمل، دیدن و شنیدن مجموعه‌ای از پتانسیل های عصبی معین را در مغز و میدان الکترومغناطیسی آن ایجاد می کنند که می تواند به صورت فکر، عکس و صدا درآید. روش نظارت الکترونیکی می تواند به صورت همزمان میلیون ها نفر را تعقیب و اداره کند. هر یک از ما همان طور که یک اثر انگشت منحصر به فرد داریم، در مغزمان نیز یک فرکانس انعکاس ویژه داریم که منحصر به فرد است. سیگنال های الکترومغناطیسی را می توان به مغز فرستاد و باعث شد که انسان هدف صداهای مورد نظر را بشنود یا تصویرهای مورد نظر را ببیند. این یکی از روش های جنگ الکترونیکی است. پیش از آنکه فضانوردان آمریکایی به فضا بروند، تراشه گذاری می شوند تا افکار و احساسات آنها ۲۴ ساعته به ثبت برسد. روزنامه واشینگتن پست گزارش داد که



در ماه مه ۱۹۹۵، ویلیام شاهزاده انگلیسی در سن ۱۲ سالگی تراشه گذاری شد؛ بنابراین هرگاه ربوده شود امواج رادیویی با فرکانس مشخص به راحتی او را پیدا می کند. سیگنال های تراشه به وسیله یک ماهواره مخصوص به صفحه کامپیوتر مرکز پلیس ارتباط می یابند و در آنجا حرکات شاهزاده ردیابی می شود. در واقع او را می توان در تمام نقاط جهان ردیابی کرد. خبرگزاری ها گزارش نکردند که شخصی بودن مسائل فرد تراشه گذاری شده برای بقیه عمر وی از بین می رود یا خیر؟ مراقبت کننده مخفی می تواند با استفاده از فرکانس های مختلف خصوصیات احساسی شخص را عوض کند، فردی می تواند پرخاشگر شده و یا به نحوی دیگر تحت تاثیر قرار گیرد. بنابراین می توان سرباز ماشینی به وجود آورد. این مجموعه فناوری از دهه ۸۰ در برخی از کشورهای عضو ناتو استفاده شده است، بدون اینکه مردم عادی و دانشگاهیان چیزی راجع به آن بشنوند. بنابراین درباره چنین روش نظارت فکری مهاجمی مطالب بسیار کمی در مقالات علمی و دانشگاهی وجود دارد. روش های مراقبت از فکر را می توان برای مقاصد سیاسی استفاده کرد. هدف مراقبت کننده مغز این است که انسان‌های هدف برخلاف خواسته یا منافع وی عمل نمی کنند. این گروه انسان‌ها را حتی می توان برنامه ریزی کرد تا جنایتی انجام دهند که پس از آن، از عملی که انجام داده‌اند هیچ چیز را به خاطر نمی آورند. این جنگ ساکت توسط سازمان های اطلاعاتی و نظامی روی سربازان و افراد ناشناس انجام می شود. تحریک الکتریکی مغز از سال ۱۹۸۰ به طور سدی برای نظارت بر مردم بدون آگاهی و رضایتشان صورت می گیرد. در صورتی که تمام قراردادهای جهانی حقوق بشر بدون استثنا تحت نظارت قرار گرفتن انسان ها را (حتی در زندان ها) ممنوع کرده‌اند، چه برسد به مردم معمولی. علاوه بر مراقبت فکری الکترونیکی، شیوه‌های شیمیایی نیز گسترش یافته است. داروهای تغییردهنده افکار و گازهای مختلف قابل تنفس را که می توانند افکار انسان را تغییر دهند، وارد مجاری هوایی و لوله های آب می کنند. به این ترتیب در بسیاری از کشورها باکتری و ویروس ها را آزمایش می کنند. ابرفناوری امروز، وظایف و کارکردهای مغز ما را از طریق تراشه و یا حتی بدون آن، به ماهواره‌ها و از آنجا به کامپیوترهایی در ایالات متحده متصل می کنند. آخرین ابرکامپیوترها به قدری قوی هستند که می توانند تمام مردم روی زمین را تحت نظر داشته باشند.

WWW.Csmonitor.com

نگاهی به روش های بیومتریک شناسایی افراد

پیشتاز سیستم های امنیتی

تریسی ویلسون

ترجمه: مریم انصاری

فرض کنید جیمزباند هستید و برای انجام ماموریتتان مجبورید به یک آزمایشگاه سری وارد شوید و سلاح مرگباری را که توسط انسانی تبهکار ساخته شده خنثی کنید و جهان را از خطری جدی نجات دهید. ولی برای ورود به این مکان بایستی از یک سیستم امنیتی فوق‌العاده پیشرفته عبور کنید. هم‌اکنون به اطلاعاتی فرای حرف رمز یا کلمه عبور احتیاج دارید چون سیستم عنبیه، صدا و الگوی دست آن تبهکار را تقاضا می کند.

امروزه ممکن است بارها در زندگی روزمره خود مثلاً در فرودگاه‌ها، بیمارستان‌ها، هتل‌ها و سوپرمارکت‌های بزرگ و حتی در پارک دیسنی (Disney) با این فناوری مواجه شوید. این اماکن هر روز بیش از گذشته خود را به سیستم شناسایی بیومتریک مجهز می کنند. این سیستم برای افزایش ضریب امنیت بر پایه ویژگی‌های فیزیکی و رفتاری شما بنا نهاده شده است. بیومتریک از دست‌خط، الگوی دست، الگوی صدا و ساختار عنبیه و رگ‌های شما برای شناسایی استفاده می کند. در این مقاله از چگونگی کارکرد این سیستم و اینکه چرا اکثر ساختمان‌های تجاری و حکومتی از این فناوری استفاده می کنند، باخبر می شویم. آیا جیمز باند داستان ما می تواند با لنز تماسی تقلبی، صدای ضبط شده و یا دستی که شبیه دست آن فرد تبهکار ساخته شده است، وارد آزمایشگاه سری شود؟

■ بیومتریک و تشخیص هویت

سیستم شناسایی بیومتریک و تشخیص هویت در بسیاری از موارد با هم اشتراک دارند اما به‌طور کامل شبیه هم نیستند. در واقع بیومتریک از ویژگی‌ها و مشخصه‌های رفتاری و فیزیکی فرد استفاده می کند و سپس تصمیم می گیرد که آیا این همان کسی است که ادعا می کنید یا خیر. درحالی که تشخیص هویت تنها از برخی ویژگی‌های فیزیکی فرد استفاده می کند و اغلب در تحقیقات جنایی کاربرد دارد تا امنیتی. قطعاً شما هر روزه احتیاط‌های امنیتی ساده‌ای را به کار می گیرید. از کلید برای ورود به خانه یا اتومبیل خود استفاده می کنید با Username-password وارد کامپیوتر شخصی‌تان می شوید و احتمالاً تاکنون اضطراب ناشی از گم‌شدن کلید و یا فراموش کردن کلمه رمز را تجربه کردید. اگر کلیدتان را گم کنید و یا کلمه رمز را روی یک تکه کاغذ بنویسید شخص دیگری می تواند آن را پیدا و به راحتی از آن استفاده کند، به‌طوری که انگار خود شما است. اما این سیستم طوری طراحی شده که به‌جای استفاده از چیزی که شما دارید (مثل یک کلید) و یا چیزی که شما می دانید (مثل کلمه رمز) از آنچه که وجودتان را ساخته استفاده می کنید یعنی ویژگی‌های فردی شما. چیزهایی که هیچ‌گاه گم، دزدیده و یا فراموش نمی شوند. همیشه و همه جا همراهتان هستند و خیلی دشوار است که بتوان از آنها کپی گرفت. به همین دلیل کارشناسان این شیوه شناسایی را بسیار ایمن‌تر و مطمئن‌تر از هر روش دیگری می دانند. سیستم شناسایی بیومتریک ظاهراً بسیار پیچیده و حرفه‌ای به‌نظر می رسد درحالی که همه آنها از سه مرحله برای شناسایی استفاده می کنند:

۱- دریافت اطلاعات: اولین باری که از سیستم استفاده می کنید، اطلاعات اساسی شما از قبیل نام و شماره شناسنامه‌تان را به‌طور دقیق ثبت می کند. سپس از ویژگی‌ها و مشخصه‌های خاص عکس می گیرد و آنها را نگهداری می کند.

۲- ذخیره‌سازی اطلاعات: برعکس آنچه که ممکن است تا به حال بارها در فیلم‌های سینمایی دیده باشیم. اکثر این سیستم‌ها تصویر یا صدای ثبت شده در مرحله یک را به‌طور کامل ذخیره نمی کنند بلکه این ویژگی‌ها را تحلیل کرده و به کد و یا نمودار تبدیل می کنند. بعضی از این سیستم‌ها این اطلاعات را بر روی یک کارت هوشمند (Smart Card) ضبط می کنند که می توانید آن را با خود همراه ببرید.

۳- مقایسه و تطبیق اطلاعات داده شده با اطلاعات ذخیره شده: برای بار دوم که از این سیستم استفاده می کنید داده‌ها را با اطلاعات ذخیره شده در خود مقایسه می کند. اگر این اطلاعات با یکدیگر همخوانی داشتند، سیستم شما را می پذیرد. در غیر این صورت اجازه ورود نخواهید داشت.

سیستم بیومتریک از سه بخش تشکیل شده:

۱- حس‌گر (Sensor) که مشخصه مورد استفاده برای شناسایی را پیدا می کند.

۲- کامپیوتری که اطلاعات را دریافت و ذخیره‌سازی می کند.

۳- نرم‌افزاری که مشخصه‌ها را تحلیل و آنها را به کد یا نمودار تبدیل می کند و عمل تطبیق را انجام می دهد.

■ نحوه عملکرد شناسایی از طریق دست‌خط

در نگاه نخست استفاده از دست‌خط برای شناسایی افراد ایده چندان مناسبی به‌نظر نمی رسد چرا که بسیاری از انسان‌ها می توانند دست‌خط دیگر افراد را در مدت کوتاهی و با چند بار تمرین به خوبی تقلید کنند. بله ممکن است کپی از امضای یک نفر و یا جعل دست‌خط او آسان و امکان‌پذیر به‌نظر برسد اما این سیستم هوشمند فقط به شکل نهایی امضا یا کلمه توجه نمی کند، بلکه آن را تحلیل می کند. میزان فشار قلم بر روی کاغذ و سرعت و آهنگ نوشتن و ترتیب شکل دادن به حروف را بررسی و حتی عادات نوشتاری شما را ثبت می کند. مثلاً نقطه و یا علامتی که معمولاً بعد از نوشتن کلمه یا متنی می گذارید. برخلاف شکل‌های ساده حروف که به آسانی جعل می شوند تقلید این خصایص فردی از آنچه که می پندارید بسیار مشکل‌تر است. حتی اگر شخصی از امضای شما کپی داشته باشد و عین آن را بر روی صفحه رسم کند، به احتمال بسیار زیاد سیستم امضا را نخواهد پذیرفت. حس‌گر سیستم حس لامسه بسیار حساسی دارد یا حتی مجهز به خودکاری با حس‌گرهای بسیار قوی است و بدین‌ترتیب فشار، جهت و حالت گرفتن خودکار را بررسی می کند، حتی زوایای میان خودکار و صفحه ثبت می شوند. سپس نرم‌افزار متن نوشته شده را به نمودار تبدیل می کند و عمل مقایسه انجام می شود. این سیستم به قدری هوشمند است که می تواند تغییرهای بسیار جزیی و کوچک دست‌خط شخص را از روزی به روز دیگر و تا هر زمان دیگر تشخیص دهد و به‌طور خودکار آنها را به ثبت برساند.

الگوی دست: شکل دست و انگشت افراد، یک ویژگی منحصر به فرد به‌شمار می رود البته نه به اندازه دیگر ویژگی‌هایی چون اثر انگشت و عنبیه. از آنجا که مکان‌های تجاری و مدارس تنها نیاز به تصدیق هویت کاربر دارند و نه تشخیص آن بنابراین به‌جای اینکه از امکانات امنیتی بالاتری استفاده کنند اغلب اسکنرهای الگوی دست و انگشت را به‌کار می گیرند. به‌عنوان مثال در پارک دیسنی از اسکنرهای الگوی انگشت برای تائید ورود دارنده بلیت به داخل پارک استفاده می شود. بسیاری از مکان‌های تجاری نیز به جای کارت ورود و خروج از اسکنرهای الگوی دست استفاده می کنند. این سیستم‌ها مجهز به یک دوربین دیجیتال هستند، کافی است دست خود را به آرامی بر روی یک صفحه صاف و مسطح بگذارید و انگشتانتان را در یک ردیف قرار دهید تا اسکنر بتواند به‌طور دقیق عمل خود را انجام دهد. پس از آن دوربین یک یا چند عکس از دست شما و یا اثری که بر روی صفحه ایجاد کرده است می اندازد. از این اطلاعات استفاده می کند تا طول، عرض، ضخامت و همه ابعاد و انحنای دست و انگشتان شما را اندازه‌گیری کند و آنگاه این داده‌ها را به یک الگوریتم عددی تبدیل می کند. این روش مزایا و معایبی دارد. در واقع انسان‌ها به راحتی اجازه می دهند تا از دست آنها اسکن گرفته شود درحالی که ثبت اثر انگشت و عنبیه را نوعی تجاوز به حریم شخصی‌شان به حساب می آورند. اما از طرفی دست بسیاری از افراد در طول زمان به‌خاطر جراحی یا بیماری‌هایی چون ورم مفاصل و آرتروز انگشتان دچار تغییر شکل و یا تغییر وزن می شود. به همین دلیل است که بعضی از این سیستم‌ها اطلاعاتشان را همواره به روز (Up to date) می کنند تا حتی کوچک‌ترین تغییرات را هم به ثبت برسانند.

الگوی صدا: صدای شما به دلیل لرزش‌های خاص تارهای صوتی و شکل حفره‌های دهانی‌تان و نحوه حرکت دادن لب‌هایتان هنگام صحبت منحصر به فرد است. برای ثبت‌نام در یک سیستم شناسایی که براساس الگوی صدا عمل می کند، بایستی تعدادی کلمه را تلفظ کنید یا می توانید از تکیه کلام‌هایتان استفاده کنید، هیچ فرقی نمی کند چه کلمه‌ای بگویید. وقتی درباره الگوی صدایی صحبت می شود اغلب تصور می کنند که این روش همان نمودار موجی‌ای است که در اسلوسکوپ به‌کار می رود، اما شیوه‌ای که در این سیستم شناسایی به‌کار گرفته می شود طیف‌نگار صدا نام دارد و به شکل امواج صدا ربطی ندارد. طیف‌نگار در اصل نموداری است که فرکانس صدا را به روی محوری عمودی و زمان را روی محوری افقی ثبت می کند. گویش‌ها، لهجه‌ها و صداهای مختلف شکل‌های مختلفی بر روی نمودار ایجاد می کنند. طیف‌نگار صدا از رنگ‌ها و سایه‌های خاکستری استفاده می کند تا کیفیت صدا را به خوبی نمایش دهد. بعضی از شرکت‌ها از این طریق، برای شناسایی کارمندانشان استفاده می کنند و کاربران می توانند بدون اینکه در محل حضور فیزیکی داشته باشند به اطلاعات شرکت دست یابند. درحالی که اسکنر الگوی دست یا عنبیه حتماً به حضور فرد نیاز دارد. در روش الگوی صدا کاربر می تواند در خانه بنشیند و با یک تلفن کسب اجازه کند. متاسفانه افرادی می توانند بدین‌ترتیب سر بعضی از سیستم‌ها را کلاه بگذارند به‌خصوص سیستم‌هایی که با تلفن نیز کار می کنند. اگر ضریب امنیت سیستم پایین باشد این سیستم گاهی نمی تواند تفاوت صدای زنده را از صدای ضبط شده تشخیص دهد، به همین دلیل بعضی از این سیستم‌ها برای جلوگیری از چنین خطایی از چندین رمز که به‌طور اتفاقی انتخاب شده‌اند، استفاده می کند. یا به‌جای ثبت کردن الگوی یک‌سری کلمات مشخص الگوی صدایی کلی را به‌کار می گیرند.

نیم نگاه

۱- سیستم‌های شناسایی بیومتریک از مشخصه‌های فیزیکی فرد همانند اثر انگشت الگوی دست، ساختار عنبیه، رگ‌های دست فرد یا از مشخصه‌های رفتاری مانند: صدا دست‌خط یا حتی آهنگ و ریتم نوشتن استفاده می کند.

۲- سیستم بیومتریک به جای مقایسه تصویرهای واقعی از الگوریتم‌ها و کدهای عددی برای تحلیل اطلاعات استفاده می کند. این اطلاعات فضایی بسیار کم و در حد چند بیت اشغال می کند.

اسکن از عنبیه: شاید تصور کنید که استفاده از فناوری اسکن عنبیه برای ورود به مکانی حفاظت شده در آینده عملی می شود اما در حقیقت این فناوری هم‌اکنون سیستم امنیتی بسیاری از اماکن سری مهم دنیا را تشکیل می دهد. در قلب این سیستم یک (CCD Charge Coupled Device-) عناصر میکرو الکترونیکی که نور را به سیگنال تبدیل می کنند) وجود دارد. این سیستم برای اینکه تصویری شفاف و با کیفیت بالا از عنبیه شخص بگیرد از نوری قابل رویت با فرکانسی نزدیک به فرکانس اشعه مادون قرمز استفاده می کند. بدین‌ترتیب مردمک چشم شخص بسیار تیره‌تر به‌نظر می رسد و در نتیجه کار کامپیوتر را برای جداسازی مردمک از عنبیه راحت‌تر می کند. وقتی که درون چشمی را از اسکنر نگاه می کنید دوربین به صورت خودکار بر روی عنبیه چشم شما تنظیم می کند. برای اینکه مطمئن شوید در جای درستی ایستاده‌اید سیستم به یک آینه مجهز می شود یا دستگاه با صدای رسا به شما اعلام می کند که چشم خود را در جای دقیقی نگاه داشته‌اید یا خیر. معمولاً بایستی چشم شما ۱۰ تا ۲۵ سانتی‌متر از دوربین فاصله داشته باشد وقتی دوربین از عنبیه عکس می گیرد محل‌های زیر را مشخص می کند.

۱- مرکز مردمک ۲- لبه مردمک ۳- لبه عنبیه ۴- مژه و پلک چشم، سپس الگوی عنبیه را آنالیز و به رمز ترجمه می کند. با توجه به دقت بالای این روش این اسکنرها اغلب در موارد امنیتی شدید استفاده می شود. طبق تحقیق‌های انجام شده چشم انسان از ویژگی‌های کاملاً منحصر به فرد و یکتای او به‌شمار می رود. به‌طوری که احتمال اشتباه سیستم در این روش یک در ۱۰۷۸ است که بسیار قابل توجه است، همچنین اسکن از عنبیه این امکان را برای سیستم فراهم می سازد تا ۲۰۰ نقطه از عنبیه بررسی و مقایسه شود، در حالی که شناسایی از طریق اثر انگشت ۶۰ تا ۷۰ نقطه را بررسی می کند. در بدن انسان عنبیه چشم ساختاری ظاهری ولی به نوعی محافظت‌شده به حساب می آید، عضوی است که با گذر زمان دستخوش تغییر نمی شود و این ویژگی، این روش شناسایی را بیش از سایر روش‌ها ایده‌آل می سازد. در اکثر مواقع عنبیه چشم افراد پس از انجام عمل جراحی نیز بدون تغییر باقی می ماند. حتی افراد نابینا نیز می توانند از این روش استفاده کنند، البته تا زمانی که چشم آنها عنبیه داشته باشد. استفاده از عینک یا لنزهای تماسی هیچ‌کدام بر روال کار تشخیص، اختلال ایجاد نمی کنند و سبب تشخیص نادرست نمی شوند.

اسکن از شبکیه چشم: بعضی از افراد اسکن عنبیه‌ای را با اسکن شبکیه‌ای اشتباه می کنند، در حالی که برای اسکن از شبکیه به نوری روشن و درخشان‌تر احتیاج داریم تا شبکیه چشم فرد به خوبی روشن شود. سپس حس‌گر از ساختار رگ‌های خونی که در پشت چشم شخص است عکس می گیرد. به عقیده برخی از کارشناسان اسکن از شبکیه چندان راحت و بی‌دردسر نیست و احتمال آنکه شبکیه انسان با گذر زمان تغییر کند، بسیار بالا است که این امر موجب تشخیص و شناسایی غلط می شود، اما اگر از این ضعف چشم‌پوشی کنیم این شیوه نیز از ضریب امنیتی بالایی برخوردار است چون واقعاً نمی توان ساختار رگ‌های خونی کسی را جعل کرد.

اسکن از ورید: رگ‌های بدن انسان نیز همانند شبکیه و اثر انگشت از ویژگی‌های او به شمار می رود، حتی رگ‌های بدن دوقلوها هم مثل یکدیگر نیست به علاوه رگ‌های دست چپ و راست یک انسان هم با یکدیگر تطابق ندارد. از طرفی از آنجا که بسیاری از رگ‌های بدن از روی پوست دیده نمی شوند در نتیجه، کار برای افراد متقلب دشوار و غیرممکن خواهد شد. رگ‌های بدن انسان طی چندین سال دستخوش تغییرات بسیار جزیی می شوند که این نیز از دیگر مزیت‌های این روش به شمار می رود. برای استفاده از این نوع روش شناسایی می‌بایست کف یا پشت دست خود را روی صفحه اسکنر قرار دهید. یک دوربین عکاسی دیجیتال با استفاده از اشعه‌ای که فرکانس آن نزدیک به مادون قرمز است، از دست شما عکس می گیرد، بدین ترتیب که هموگلوبین موجود در خون رگ‌های شما این نور را جذب می کند و سبب می شود که رگ‌ها در تصویر تیره دیده شوند. این روش نیز، چون دیگر انواع بیومتریک از ساختار رگ‌های شما الگویی می سازد که بر پایه شکل و فرم و محل آنها بنا شده است. اسکنرهایی که الگوی رگ‌ها را آنالیز می کنند از نظر عملکرد با تست اسکن رگ که در بیمارستان‌ها انجام می شود کاملاً متفاوت است. برای اسکن از رگ که در پزشکی کاربرد دارد، غالباً از یک ذره رادیواکتیو استفاده می شود، اما در سیستم بیومتریک همان اشعه‌ای به کار می رود که از کنترل راه دور صادر می شود.

آینده بیومتریک: کاربردهای فناوری بیومتریک می تواند از صدور اجازه ورود یک شخص به مکانی خاص، بسیار فراتر رود. مثلاً در بیمارستان‌ها در بخش زایمان به محض اینکه نوزاد از مادر متولد می شود اسکن دقیقی از بدن او صورت می گیرد و بدین ترتیب امکان تعویض اشتباهی نوزادان به صفر می رسد. هم‌اکنون در بعضی از فرودگاه‌ها به جای بررسی گذرنامه و مدارک شناسایی از بیومتریک بهره می برند. کارشناسان چنین پیش‌بینی کرده‌اند که در آینده‌ای نه چندان دور از روش‌های جدیدتری برای شناسایی افراد از طریق بیومتریک استفاده می شود از قبیل استفاده از DNA بدن انسان، استفاده از ساختار اصلی ناخن و دندان‌ها، شکل گوش افراد، بوی بدن، الگوی پوست بدن و الگوی نبض.

■ آیا بیومتریک به حریم شخصی تجاوز می کند؟

بعضی از افراد به دلیل برخی مسائل فرهنگی با این سیستم مخالفت می کنند. آنها تصور می کنند بیومتریک دنیای شخصی آنها را شناسایی می کند و خصوصی‌ترین فعالیت‌شان را زیر نظر دارد. هنگامی که در خیابان راه می روند یا وارد فروشگاه یا موسسه‌ای می شوند، این سیستم بدون رضایت آنها به خصوصیات فردی‌شان دست می یابد. در واقع این افراد از این سیستم تصوری نابجا دارند. آنها می پندارند بیومتریک از یک مجموعه عظیم اطلاعات حیاتی افراد روی زمین تشکیل شده و نگرانند که آیا این مجموعه امن می ماند یا مانند هر نرم‌افزار دیگری ممکن است مورد حمله هکرها واقع شود. اما جالب است بدانیم این فناوری اصلاً قابلیت ذخیره‌سازی و طبقه‌بندی اطلاعات همه افراد روی زمین را ندارد و در واقع هر سیستمی مقدار کمی از اطلاعات درباره تعداد کمی کاربر وابسته به خود را ذخیره می کند و اطلاعاتی را که نماینده ویژگی‌های یک فرد است، در خود نگهداری نمی کند بلکه آنها را به کدهایی که فقط برای خودش تعریف شده است تبدیل می کند. اکثر این سیستم‌ها فقط در یک مکان خاص و جایی که آنها را مستقر ساخته‌اند، کار می کنند؛ مثلاً در ساختمان یک اداره یا بیمارستان. از طرفی اطلاعات یک سیستم لزوماً با بقیه سیستم‌ها سازگار نیست، اگرچه در حال حاضر چندین سازمان برآنند که اطلاعات بیومتریک سیستم‌های امنیتی خود را استاندارد و هماهنگ با یکدیگر سازند.

تصدیق هویت، تشخیص هویت: سیستم بیومتریک قادر است تایید کند که آیا شما همان شخصی هستید که ادعا می کنید یا خیر. همچنین با دریافت اطلاعات شما و مقایسه آن با فایل‌هایی که از خود شما در گذشته ذخیره کرده، هویت‌تان را تشخیص دهد. در واقع تصدیق، مقایسه یک به یک است. مقایسه الگوی دستی که اسکن می شود با الگوی دست فردی که ادعا می کنید و... مشخصات شما را با اطلاعات ذخیره شده فرد موردنظر مقایسه می کند، در حالی که تشخیص شخصیت شما و اینکه چه کسی هستید مستلزم این است که یک ویژگی شما را با همان ویژگی تمام افرادی که اسکن شده‌اند مقایسه کند. مثلاً اثر انگشت شما را با تمام اثر انگشت‌های ذخیره‌شده‌اش مقایسه می کند و در نهایت اگر قبلاً اسکن شده باشید شما را خواهد شناخت.

■ بیومتریک چه می کند؟

در اغلب فیلم‌های سینمایی مراحل مختلف مقایسه مشخصه‌های افراد را به طریقی نشان می دهند که برای تماشاگر جالب باشد در حالی که این روش‌ها دقیق و واقعی نیستند برای مثال ظاهر اثر انگشت را با دیگر اثر انگشت‌های موجود در کامپیوتر یا پرونده‌ها مقایسه می کنند. این روش بسیار دشوار و کند است. سیستم بیومتریک به جای مقایسه تصاویر واقعی از الگوریتم‌های متنوع و کدهای عددی برای تحلیل اطلاعات استفاده می کند. این اطلاعات فضایی بسیار کم در حد چند بیت اشغال می کنند.

تشخیص دقیق: همه سیستم‌های بیومتریک از ویژگی‌های انسانی استفاده می کنند، اما اینکه کدام روش بهتر و دقیق‌تر است به میزان امنیت به کار رفته در سیستم، تعداد افرادی که از این روش استفاده می کنند و دقت سیستم مربوط می شود. اکثر سازنده‌ها، برای اینکه میزان ضریب امنیت را اندازه بگیرند عوامل زیر را بررسی می کنند و سیستم را نسبت به این موارد می سنجد:

۱- False Accepte Rate (FAR): سیستم چه تعداد از افرادی که خود را جای شخص دیگری جا زده‌اند به اشتباه می پذیرد.

۲- False Reject Rate (FRR): سیستم چه تعدادی از افرادی را که اجازه ورود دارند، نمی شناسد و به اشتباه نمی پذیرد.

۳- Faillure to Acquire Rate (FTA): چند بار کاربر بایستی ویژگی‌هایش را به سیستم معرفی کند تا سیستم او را بشناسد.

حتماً بارها در بسیاری از فیلم‌های سینمایی مشاهده کرده‌اید که سیستم بیومتریک را به طور غیرمعمول ساده جلوه می دهند و قهرمان داستان می تواند به راحتی از حس‌گرهای سیستم بیومتریک عبور کند، بدون اینکه اطلاعات واقعی خود را در اختیار سیستم قرار دهد یا فرد متقلب به راحتی سیستم را فریب می دهد و خود را جای فرد دیگری جا می زند. گاهی برعکس سیستم را بیش از حد هوشمند و پیچیده معرفی می کنند.

■ ترکیب چند اسکن با یکدیگر

در بعضی از سیستم‌های فوق امنیتی متخصصین از روش Layerd استفاده می کنند. Hulty Model سیستمی است که چند روش شناسایی از طریق بیومتریک را با هم ترکیب می سازد مثلاً اسکن عنبیه و الگوی صدا. و بدین‌ترتیب ضریب امنیت را افزایش می دهند.

howstuffworks.com

نوع سیستم بیومتریک	نوع تقلب	آیا سیستم اجازه ورود به فرد متقلب را می دهد؟
شناسایی دست‌خط	۱- کپی از امضا و دست‌خط جعلی ۲- عیناً دست‌خط یا امضا را تقلید کند	به احتمال بسیار زیاد خیر. چون سیستم عمل نوشتن را بررسی می کند و به شکل نهایی آن توجهی ندارد.
شناسایی الگوی دست	ساختن دست مصنوعی	احتمالاً بله. مگر اینکه سیستم، مجهز به انجام آزمون‌های حیاتی از قبیل اندازه‌گیری دمای بدن یا الگوی نبض فرد باشد.
شناسایی الگوی صدا	صدای ضبط شده	شاید. بعضی از سیستم‌ها صدای ضبط شده را از صدای زنده تشخیص نمی دهند، اما بقیه انواع اغلب این تفاوت را می شناسند.
الگوی رگ‌ها	عکس از عنبیه یا چاپ روی لنزهای تماسی	احتمالاً خیر. کیفیت چاپ بایستی بسیار بسیار بالا باشد. در ضمن اغلب سیستم‌ها وجود لنزهای تقلبی از عنبیه واقعی را به راحتی تشخیص می دهند.
شناسایی عنبیه	ساختن مدلی مصنوعی از رگ‌های فرد	احتمالاً خیر. ساختن کپی دقیق از رگ‌های یک فرد خصوصاً با استفاده از موادی که اسکنر به جعلی بودن آن پی نبرد کاری بسیار دشوار و حتی غیرممکن است.

خبرها

گذرنامه حاوی تراشه اطلاعات شخصی

ایسنا: وزارت امور خارجه آمریکا در نظر دارد تا صدور گذرنامه‌های حاوی چیپ‌های اطلاعات شخصی دارندگان آنها از جمله تشخیص فرکانس رادیویی صدای افراد (RFID) را از هفته جاری آغاز کند. این درحالی است که برخی کارشناسان امنیتی آمریکا نسبت به این نکته که این تراشه ها می توانند به صورت غیرقانونی در اختیار هکرها قرار گیرند، هشدار داده‌اند. این برنامه جدید از اداره گذرنامه دنور آمریکا آغاز می شود و تا اواسط سال ۲۰۰۷ میلادی از سوی ۱۷ سازمان و نهاد صدور گذرنامه در سراسر آمریکا مورد استفاده قرار خواهد گرفت. همچنین گفته می شود که تا سال ۲۰۱۷ میلادی تمامی گذرنامه‌های آمریکایی دارای این تراشه‌های اطلاعاتی خواهند شد.

مقام نخست کیفیت خودرو برای ژاپنی ها

موج: براساس نظرسنجی که درباره کیفیت خودروهای جهانی در آمریکا یعنی بزرگترین بازار خودروی جهان انجام شد، خودروسازان ژاپنی همچنان در صدر جدول باقی ماندند. از میان ۱۱ گروه طبقه‌بندی کیفی خودروها، خودروسازان تویوتا و هوندا توانستند مجموعاً در هفت گروه کیفی در صدر قرار گیرند. این درحالی بود که در چهار گروه کیفی باقی مانده، شرکت‌های فورد، جنرال‌موتورز و مزدا رتبه نخست کیفی را از آن خود کردند.

تشخیص شخصیت از طریق پیام‌های متنی

ایسنا: دانشمندان انگلیسی در نظر دارند با بررسی و مطالعه پیام‌های متنی تلفن همراه مشترکان، بتوانند به شخصیت ارسال‌کنندگان آن پی برده و به پلیس در تحقیقات جنایی کمک کنند. محققان دانشگاه «لی‌سستر» در نظر دارند با مطالعه پیام‌های sms مشترکان تلفن همراه، الگوهای زبانی به‌کار گرفته شده از سوی افراد را بررسی کرده و بتوانند به شخصیت ارسال‌کنندگان آن پی ببرند. براساس این گزارش، مطالعه شش‌ماهه این محققان بیشتر بر پایه بررسی زبان قراردادی در ارسال sms است. رئیس بخش تحقیقات دانشگاه «لی‌سستر» در این رابطه اعلام کرد: پیام‌های متنی تلفن همراه روش تقریباً جدیدی برای ارتباط است که شیوه غیررسمی در استفاده از زبان است؛ برای همین نمی توان انتظار داشت که مشترکان از زبان خاصی استفاده کنند، همین تفاوت زبان نوشتاری می تواند به شناسایی شخصیت ارسال‌کننده پیام کمک کند.

درایو «اچ‌دی- دی‌وی‌دی» مایکروسافت

ایسنا: مایکروسافت درایو ضمیمه اچ‌دی- دی‌وی‌دی در بازی ویدیویی Xbox ۳۶۰ را معرفی کرد. این محصول جدید در نشست دی‌وی‌دی در لس‌آنجلس به نمایش درآمد و مایکروسافت تصدیق کرد که از کریسمس آینده، قابل دسترس کاربران خواهد بود. کوین کولینز- مدیر ارشد برنامه‌های مایکروسافت- افزود: این درایو شبیه به CD-ROM‌های معمولی است و اطلاعات را وارد Xbox ۳۶۰ می کند. اچ‌دی- دی‌وی‌دی قالب جدید دی‌وی‌دی است که با قالب جدید دیگر یعنی اشعه- آبی رقابت سختی را آغاز کرده است؛ از طرف دیگر بازی رایانه‌ای Xbox ۳۶۰ نیز یکی از پرطرفدارترین بازی‌های رایانه‌ای در جهان محسوب می شود و رقابت جالبی با بازی پلی استیشن شرکت سونی دارد.

نیم میلیارد نفر مشترک تلویزیون موبایل

ایسنا: براساس نتایج جدیدترین مطالعات، تقریباً نیم میلیارد نفر در سراسر جهان تا سال ۲۰۱۱، از طریق گوشی تلفن همراه به تماشای برنامه‌های تلویزیونی اقدام خواهند کرد. این بررسی نشان می دهد، با توجه به سرویس‌های پخش تلویزیونی مانند DVB-H، انتظار می رود تا سال ۲۰۱۰ بازار جهانی تلویزیون موبایل شاهد رشد ۵۰ درصدی باشد. این گزارش حاکی از آن است که تا سال ۲۰۱۰، سرویس‌های پخش دیجیتالی رشد به مراتب سریع‌تری نسبت به اشتراک تلویزیون موبایل خواهد داشت.

تلفن همراه به جای پول و کارت اعتباری

تا یک‌سال آینده در ایالات متحده می توان به جای استفاده از کارت‌های اعتباری گوشی‌هایتان را از جلوی دستگاه‌های کارت خوان عبور دهید و بدین طریق هزینه خرید کالا و خدمات گوناگون را بپردازید. این کار با استفاده از تراشه‌ای ممکن خواهد شد که Near Field Communication نام گرفته است. این تراشه که در گوش