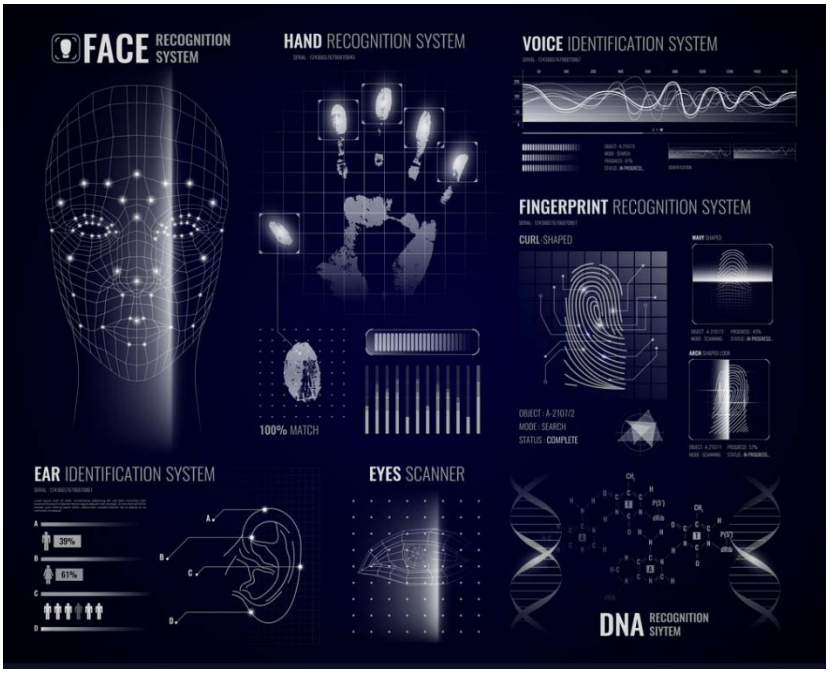
سازمان تنظیم مقررات و ارتباطات رادیویی

روش های احراز هویت بیومتریک در دنیا



معاونت راهبردی و توسعه بازار

دفتر سازمان‌های تخصصی بین‌المللی

زمستان ۹۸

فهرست مطالب

معرفی علم بیومتریک

یکی از مهم‌ترین و دقیق‌ترین سیستم‌های تشخیص هویت، بیومتریک است. علم بیومتریک، تکنولوژیی برای اندازه‌گیری و آنالیز مشخصات بدن افراد جهت تشخیص هویت شخص می‌باشد.

همه سیستم‌های بیومتریک دارای معماری ویژه‌ای برای پردازش نمونه‌ی مورد بررسی و احراز هویت می‌باشند. روش‌های مختلفی برای تشخیص هویت در بیومتریک وجود دارد که هر یک با توجه به دقت و کارایی لازمه، مورد استفاده قرار می‌گیرند. اثر انگشت به دلیل اینکه برای هر فرد منحصربه‌فرد است و با گذشت زمان هیچ گونه تغییری نمی‌کند، در میان سیستم‌های بیومتریک بیشتر مورد استفاده قرار می‌گیرد. البته سیستم‌های دیگر مانند عنبیه چشم، شبکیه چشم و نمودار حرارتی چهره هم از فردی به فرد دیگر متفاوت هستند. برای افزایش کارایی و امنیت و دقت سیستم می‌توانیم از ترکیبات بیومتریک استفاده کنیم. در گذشته جهت شناسایی مجرم، از روال شناسایی اثر انگشت و چهره‌نگاری استفاده می‌شده، اما اکنون سیستم‌های مکانیزه‌ای ایجاد شده‌است. بسیاری از جنبه‌های مختلف فیزیولوژی، شیمی یا رفتار انسان برای احراز هویت بیومتریک قابل استفاده است. بیومتریک به تکنولوژیی برای اندازه‌گیری و آنالیز مشخصات بدن افراد جهت تشخیص هویت شخص اشاره دارد. عموماً در سیستم‌های بیومتریک از دو نوع ویژگی مختلف افراد جهت شناسایی استفاده می‌شود. پارامترهای فیزیولوژیکی که اساس شناسایی در این کلاس، اندازه‌گیری و آنالیز مشخصه‌های ثابت یک شخص از جمله اثر انگشت، شناسایی از روی شبکیه چشم، شناسایی از طرق عنبیه چشم، شناسایی از روی هندسه دست، می‌باشد. پارامترهای رفتاری، شناسایی الگوهای رفتاری مشخص یک فرد از طریق صدا، شدت ضربه شخص بر روی کیبورد.

سیستم های بیومتریک و تشخیص هویت

سیستم شناسایی بیومتریک و تشخیص هویت در بسیاری از موارد با هم اشتراک دارند اما به طور کامل شبیه هم نیستند. در واقع بیومتریک از ویژگی‌ها و مشخصه‌های رفتاری و فیزیکی فرد استفاده می‌کند و سپس تصمیم می‌گیرد که آیا این همان کسی است که ادعا می‌کند یا خیر؟

در حالی‌که تشخیص هویت تنها از برخی ویژگی‌های فیزیکی فرد استفاده می‌کند و اغلب در تحقیقات جنایی کاربرد دارد تا امنیتی. قطعاً افراد هر روز احتیاط‌های امنیتی ساده‌ای را به کار می گیرید مثلاً از کلید برای ورود به خانه یا اتومبیل استفاده می‌کنید یا از پسورد وارد کامپیوتر شخصی خود می‌شوید و احتمالاً تاکنون اضطراب ناشی از گم شدن کلید و یا فراموش کردن کلمه رمز را تجربه کردید. اگر کلیدتان را گم کرده و یا کلمه رمز را روی یک تکه کاغذ نوشته باشید، شخص دیگری می‌تواند آن را پیدا و به راحتی از آن استفاده کند، به طوری که انگار خود شما است. اما این سیستم طوری طراحی شده که به جای استفاده از چیزی که دارید مثل یک کاغذ و یا چیزی که می‌دانید مثل کلمه رمز از آنچه که وجودتان را ساخته استفاده می‌کند یعنی ویژگی‌های فردی. چیزهایی که هیچ‌گاه گم، دزدیده و یا فراموش نمی‌شوند، همیشه و همه جا همراه هستند و خیلی

دشوار است که بتوان از آن‌ها کپی گرفت. به همین دلیل کارشناسان این شیوه شناسایی را بسیار امن‌تر و مطمئن‌تر از هر روش دیگری می‌دانند.

مزایای استفاده از فناوری بیومتریک

بیومتریک‌ها بسته به نوع کاربردشان در امور امنیتی و کنترلی، مزیت‌های فراوانی دارند که به مهم‌ترین آن‌ها اشاره می‌شود.

۱- افزایش ایمنی

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

۲- افرایش راحتی

دلایلی که در توضیح افزایش ایمنی ذکر شد خود گواهی بر سهولت استفاده از بیومتریک‌ها به جای ابزار رایج فعلی می‌باشد و با استفاده از تکنولوژی‌های بیومتریک سرعت دستیابی به منابع موردنظر افرایش می‌یابد. هزینه نگهداری از سیستم‌ها و مسائل امنیتی مربوطه کاهش چشمگیری می‌یابد.

۳- جلوگیری از تقلب

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

۴- تشخیص مظنونین

با استفاده از بیومتریک ها هویت واقعی افراد آشکار می‌شود. یکی از مهمترین دلایل گسترش استفاده از این تکنولوژی مبارزه با تروریسم، مهاجرتهای غیرقانونی، فرار از قانون می باشد.

از جمله مزایای فناوری بیومتریک غیرقابل حدس زدن، غیرقابل فراموشی، غیرقابل سرقت، سرعت و راحتی استفاده، کاهش هزینه‌های امنیتی جهت استفاده از نیروی انسانی ورزیده، غیرقابل تقلب، امکان تعیین هویت اصلی و واقعی افراد به دلیل منحصر به فرد بودن پارامترهای شناسایی افراد، امنیت بالا، شناسای مجرمان، تجارت الکترونیکی، حفظ اسرار شهروندان، حفظ هویت شهروندان، ممانعت از فرار قانون، مبارزه با تروریسم، تشخیص مظنونین، جلوگیری از مهاجرت‌های غیرقانونی، ارائه مطلوب خدمات عمومی از طرف دولت، مدیریت بحران‌ها از طرف دولت، غیرقابل جعل بودن، کنترل دسترسی فیزیکی

و منطقی به منابع مالی، صدور مدارک شناسایی قابل اعتماد و اطمینان و تقویت سپر امنیتی در برابر دسترسی‌های غیر مجاز، می‌باشند.

از جمله معایب فناوری بیومتریک هزینه تمام شده بالا، عدم امکان استفاده از این فناوری برای کشورهای فقیر و توسعه نیافته، عدم امکان استفاده در سازمان‌های کوچک به دلیل مقرون به صرفه نبودن، عدم ثبت اطلاعات بعضی افراد به علل مختلف از جمله جراحت یا معلولیت، عدم اطلاعات متمایزکننده یا حساسیت بعضی از سیستم‌ها، عدم همراهی یا همکاری افراد در ارائه ثبت کامل اطلاعات به سبب تفکر نفی آزادی شخصی، طراحی سیستمی با نرخ خطای بسیار کم جهت تضمین صحت و تأیید هویت واقعی افراد، طراحی سیستمی با سرعت بالا جهت ذخیره نمودن اطلاعات افراد جدید (مانند رشد جمعیت) و طراحی سیستمی با دقت بالا جهت صحت و تأیید هویت واقعی افراد (قابلیت ثبت و پردازش ۲ تا چند ویژگی فیزیولوژیکی و رفتاری را داشته باشد)، می‌باشند.

تکنولوژی‌های بیومتریک

دستگاه‌های بیومتریک انواع زیادی دارند ، اما پنج نوع امنیت بیومتریک اصلی هستندکه معمولاً مورد استفاده قرار می‌گیرند. بیومتریک در اصل شناخت شخصیت انسانی است که برای هر فردی منحصر به فرد است و شامل تشخیص چهره، اثر انگشت، تشخیص صدا، اسکن شبکیه چشم، عنبیه، هندسه دست، تشخیص امضاء، آزمایش DNA، تشخیص از روی سیاهرگ دست، نمودار حرارتی چهره، شدت ضربه بر روی صفحه کلید، شکل گوش و بوی بدن می‌باشد. فناوری بیومتریک برای ایمن نگه داشتن دستگاه‌ها استفاده می‌شود و بهترین راه برای اطمینان از این که دارایی‌ها و اطلاعات ارزشمند مردم محافظت می‌شود.

شناسایی از طریق اثر انگشت

یکی از قدیمی‌ترین روش‌های تشخیص هویت، روش شناسایی از طریق اثر انگشت می‌باشد. نوک انگشت دارای یکسری خطوط است که از یک طرف انگشت به طرف دیگر ادامه دارد. این خطوط دارای یکسری نقاط مشخص می‌باشند.

این خطوط شامل کمان‌ها، مارپیچ‌ها، حلقه‌ها، انتهای لبه‌ها، انشعاب‌ها، نقطه‌ها (شیارهای نزدیک به لبه‌ها)، جزایر (دو انشعاب نزدیک به هم)، تقاطع (نقطه تلاقی دو یا چند لبه)، منفذها می‌باشند. در واقع ما در این سری از سیستم‌ها الگوهای تولید شده را مورد مقایسه قرار می‌دهیم. این روش دارای مزایای بسیاری از جمله منحصربه‌فرد بودن اثر انگشت برای هر شخص، مقاوم بودن در برابر گذشت زمان، به بلوغ رسیدن تکنولوژی، استفاده راحت، دارای نرخ خطای پایین، ارزان و عامه پسند، می‌باشد.

شناسایی از طریق چهره

فرم هندسی یک چهره نیز از پارامترهای مورد اندازه‌گیری در سیستم‌های بیومتریک است ولی نمی‌توان گفت که جزء خصیصه‌های منحصربه‌فرد افراد است لذا این سیستم‌ها در جاهایی که تعداد کاربران کم است و نیز زمان‌های الگوبرداری درازمدت نیست، مناسب هستند. از دیگر کاربردهای این سیستم‌ها، استفاده در سیستم‌های مالتی بیومتریک جهت افزایش دقت است. تصویر چهره یک کاربر می‌تواند توسط یک دوربین سیاه و سفید با استاندارد که یک رزولوشن ۲۴۰*۳۲۰ و حداقل ۳ تا ۴ فریم را تولید کند، گرفته شود. دو روند اصلی برای تشخیص چهره انجام می‌شود: روند کلی یا کل چهره و خصوصیات پایه‌ای چهره. خصوصیات پایه‌ای چهره بر شناسایی و تشخیص نقاط ثابت و معین در چهره که با مرور زمان کمترین حساسیت و تغییری را از خود نشان می‌دهند شامل قسمت‌هایی از چشم، اطراف بینی و دهان و بخش‌هایی که استخوان گونه را احاطه کرده‌اند تکیه دارد. روند کلی یا کل چهره، یک تصویر کامل و یکجا از چهره را مورد پردازش قرار می‌دهد. این متد از روش‌های تحلیل آماری و شبکه‌های عصبی برای پردازش چهره بهره می‌گیرد.

در کل سیستم‌های این چنینی دقت بالایی ندارند به دلیل اینکه چهرها کاملاً منحصربه‌فرد نیستند و گاه اتفاق می‌افتد که دو نفر (مخصوصا دوقلوها) از نظر چهره با هم مشابهند؛ لذا از این‌گونه سیستم‌ها فقط در مکان‌هایی استفاده می‌شوند که امنیت تا حد بسیار زیاد مورد نظر نباشد.

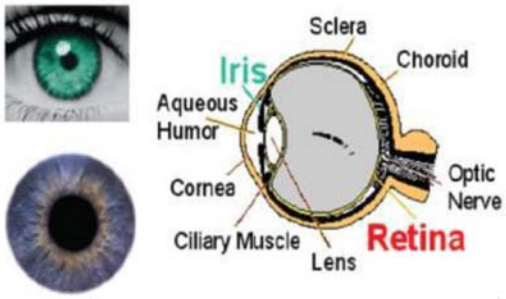
شناسایی از روی عنبیه چشم

عنبیه قسمت رنگی چشم است که ترکیبی است از نوعی ماهیچه به شکل دایره با یکسری خطوط شعاعی، لایه‌ای یا توری مانند که در پیش از تولد انسان شکل گرفته‌است و تا زمان مرگ تقریباً هیچ تغییری نمی‌کند. این ماهیچه شامل یکسری کارکترها مانند خطوط، حلقه‌ها، حفره‌ها، شیارها، تارها، لکه‌ها است که قابل تفکیک می‌باشند. می‌توان گفت که عنبیه چشم همه افراد با یکدیگر متفاوت است.

تصویر عنبیه معمولاً توسط یک دوربین تک رنگ مادون قرمز مجهز به سنسور گرفته می‌شود. معمولاً فاصله دوربین تا چشم باید چیزی در حدود ۱۸ اینچ باشد. (تابش نور به عنبیه سپس اندازه‌گیری بازگشت آن) فرایند پردازش بدین شکل است که ابتدا مکان و اندازه مردمک در تصویر مشخص شده و سپس با به دست آوردن مکان و اندازه عنبیه، کلیه تصویر عنبیه که در میان این دو دایره قرار دارد به شکل مستطیلی با ابعاد معین تبدیل می‌شود، این تکنیک باعث می‌شود تا با کوچک یا بزرگ شدن مردمک تصویر مستطیل شکل تقریباً ثابت بماند تا در انجام فرایندهای بعدی مشکلی نباشد. تصویر موجود در مستطیلی با ابعاد معین دارای مشخصه‌های قابل تبدیل به کدهای باینری است، در این تبدیل‌ها روش‌های مختلفی وجود دارد که هر

یک مزایا و معایب خودرا دارند. پس از بدست آوردن الگوی باینری، با استفاده از بدست آوردن فاصله همینگ[1] بین الگوی موجود با الگوی بدست آمده می‌توان نتیجه تطبیق را بدست آورد.

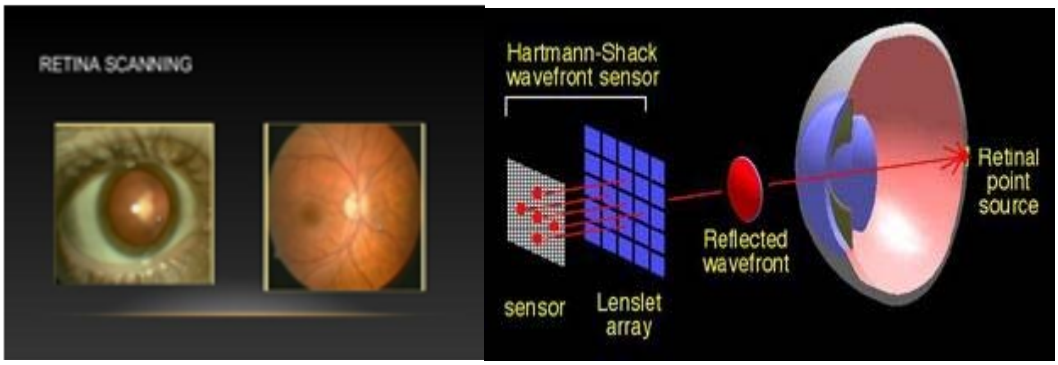
در روش‌های دیگری مانند نمونه‌یابی در مکان‌های مشخص با برداشت چند نمونه از قسمتی از تصویر عنبیه که مشخصات قابل توجهی دارد، در زمان تشخیص با استفاده از نمونه‌های ذخیره شده و مکان‌یابی نمونه‌ها، عنبیه افراد قابل تشخیص است. این سیستم دارای قابلیت خوبی در تشخیص افراد است بدین دلیل که عنبیه هم منحصربه‌فرد است و هم در برابر گذشت زمان مقاوم، ولی متأسفانه حجم الگوها در این روش بسیار بالا است، این تکنولوژی بسیار گران است، کاربر پسند نیست و به دلیل اینکه در حین نمونه برداری لازم است که چشم کاملاً بی حرکت باشد لذا الگو برداری ممکن است دقیق نباشد.



شناسایی از روی شبکیه چشم

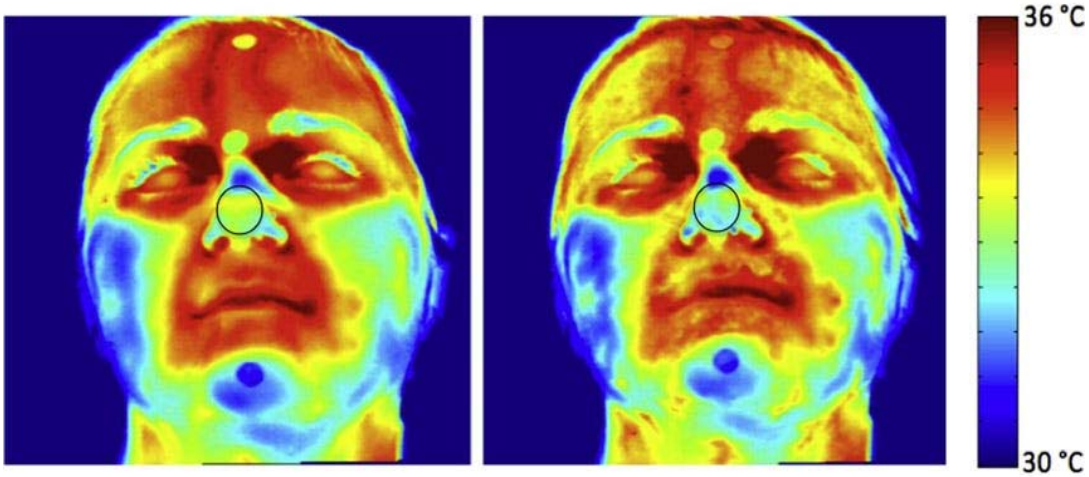
شبکیه چشم در منتهی‌الیه کره چشم قرار دارد که شامل یکسری رگ‌های خونی است که این مویرگ‌ها داری اشکال مختلفی هستند، این خصیصه در افراد منحصربه‌فرد است. با قرارگیری چشم کاربر در یک مکان مشخص، یک دسته نور ماوراء قرمز یا نور سبز با طول موج کوتاه به شبکیه چشم تابیده می‌شود و بازتاب آن توسط یک دوربین CCD اندازه‌گیری می‌شود. این روش تقریباً مشابه شناسایی از طریق عنبیه می‌باشد.

[1] در تئوری اطلاعات، فاصله همینگ برای دو رشته با طول مساوی، برابر تعداد مکان‌هایی است که سمبول‌های متناظر متفاوت هستند. به عبارت دیگر، کمترین تعداد جایگزینی‌هایی است که یک رشته به یک رشته دیگر تغییرپیدا کند، یا تعداد خطاهایی که یک رشته به رشته دیگر تبدیل گردد.



شناسایی از روی نمودار حرارتی چهره

نمودار حرارتی چهره نیز یکی دیگر از پارامترهایی است که در تمامی افراد حتی دوقلوها نیز متفاوت است. نمودار ترموگرام در برابر گذشت زمان (تا مدت محدودی)، آرایش و اصلاح کردن مقاوم است، حتی جراحی پلاستیک نیز باعث بروز آسیب به نمودار ترموگرام نمی‌شود. جهت تصویر برداری از چهره از یک دوربین مادون قرمز با طول موج ۳ الی ۵ میکرون یا ۸ الی ۱۲ میکرون بدین صورت که تا عمق ۴ سانتی‌متر زیر پوست را حس کند استفاده می‌شود.



شناسایی از روی نحوه راه رفتن

معمولاً این روش در جاهایی که ارتباط مستقیم با افراد میسر نیست کاربرد دارد خصوصاً در فرودگاه‌ها و معابر امنیتی. (این سیستم شناسایی تقریباً یک سیستم شناسایی مخفی است) در این روش یک تصویر از شخص در هنگام راه رفتن بدست

می‌آید که معرف نمودار جابجایی و زمان برای وی است. در هنگام راه رفتن افراد حرکت پاها و سر افراد با یکدیگر متفاوت است (البته حرکت دستان نیز در برخی موارد کاربرد دارد) که الگوی بدست آمده از این قسمت‌ها می‌باشد.

شناسایی از روی هندسه دست

دراین سیستم دست در یک مکان مشخص قرار می‌گیرد. سپس با استفاده از یک دوربین دیجیتال CCD با کیفیت مطلوب ۳۲۰۰۰ پیکسل تصویر دست از دو نمای فوقانی و کناری گرفته می‌شود؛ که یک تصویر ۳بعدی از دست تولید می‌کند. از تصویر بدست آمده چندین قسمت دست اندازه‌گیری می‌شود، من‌جمله: انگشتان (طول، پهنا، ضخامت، انحنا) و پارامترهای هندسی دیگر که معمولاً حجم داده بدست آمده ۹بایت است.

شناسایی از روی صدا

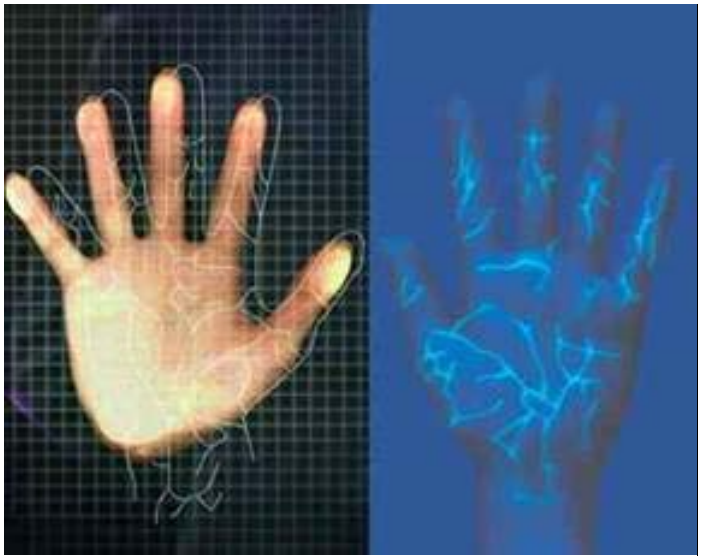
صدای انسان به دلیل لرزش‌های خاص تارهای صوتی و شکل حفره‌های دهانی و نحوه حرکت داده لب‌ها هنگام صحبت منحصربه‌فرد است. در سیستم شناسایی مبتنی بر الگوی صدا، بایستی تعدادی کلمه را تلفظ کرد. شیوه‌ای که در این سیستم شناسایی به کار گرفته می‌شود طیف‌نگار صدا نام دارد و به شکل امواج صدا ربطی ندارد. طیف‌نگار نموداری است که فرکانس صدا را به روی محوری عمودی و زمان را روی محوری افقی ثبت می‌کند.

شناسایی از روی دست‌خط

شاید گمان بر این باشد که این شیوه، ایده چندان مناسبی نیست چرا که بسیاری از انسان‌ها می‌توانند دست‌خط دیگر افراد را به خوبی تقلید کنند. درست است که جعل دست‌خط اسان به نظر می‌رسد اما این سیستم هوشمند فقط به شکل نهایی کلمه نگاه نمی‌کند، بلکه ان را تحلیل می‌کند. میزان فشار قلم بر روی کاغذ و سرعت و اهنگ نوشتن و ترتیب شکل دادن به حروف را بررسی و حتی عادات نوشتاری شما را ثبت می‌کند.

شناسایی از روی ورید[۲]

رگ‌های بدن انسان نیز همانند شبکیه و اثر انگشت از ویژگی‌های او به شمار می‌رود، حتی رگ‌های بدن دو قلوها هم مثل یکدیگر نیست به علاوه رگ‌های دست چپ و راست یک انسان هم با یکدیگر تطابق ندارد. برای استفاده از این نوع روش شناسایی می‌بایست کف یا پشت دست را روی صفحه اسکنر قرار داد، یک دوربین دیجیتال با استفاده از اشعه‌ای که فرکانس نزدیک به مادون قرمز است، تصویربرداری می‌کند. بدین ترتیب هموگلوبین موجود در خون رگ‌ها نور را جذب و باعث می‌شوند رگ‌ها در تصویر تیره دیده شوند.



شناسایی از روی امضا

امضا که از مهم‌ترین بیومتریک‌های رفتاری است، عبارت است از نوشتن نام یا نام خانوادگی (یا هر دو) یا رسم علامت خاصی که نشانه هویت صاحب علامت است، در ذیل اوراق و اسناد عادی یا رسمی که متضمن وقوع معامله یا تعهد یا قرار یا شهادت و مانند آن‌ها است یا بعدا باید روی ان اوراق تعهد یا معامله‌ای ثبت گردد.

---

[۲] Vein Scan

استانداردهای بیومتریک

برای اطمینان از اینکه سیستم‌های شناسایی بیومتریک قابل اعتماد، ایمن و کاربردی هستند، نیاز به پیشرفت استانداردهای بین‌المللی می‌باشد. به ویژه، دولت‌ها بعید است که سیستم غیر استاندارد ارائه شده توسط تنها یک تولیدکننده را بپذیرند. در مورد اینکه چه خصوصیات بیومتریک قابل اندازه‌گیری است و این اطمینان که معیارهای انتخابی بین هر دو فرد متمایز هستند، باید توافق کلی داشته باشند. همچنین استانداردها برای محافظت از داده‌های بیومتریک نیاز است تا حریم خصوصی حفظ گردد و از حمله‌هایی که راه را برای کلاهبرداری یا جعل هویت فراهم می‌کند، جلوگیری کند. اهداف اساسی در استانداردسازی باعث نصب آسان‌تر، اجرای ارزان‌تر و قابلیت اطمینان بیشتر سیستم‌های بیومتریک می‌شوند.

نخستین استانداردهای بیومتریک در دهه ۱۹۸۰ توسط دولت‌ها و سازمان‌های اجرای قانون ایجاد شدند تا از اطلاعات اثر انگشت استفاده شود، اما توسعه استانداردها تا سال ۲۰۰۲ آغاز نشده بود. نمایندگان ملی و بین‌المللی در حال تدوین این استانداردها هستند که شامل سازمان بین‌المللی استانداردسازی (ISO)، کمیسیون بین‌المللی الکترونیکی (IEC) و بخش استاندارد اتحادیه جهانی ارتباطات (ITU-T) می‌شوند. کنسرسیوم‌های صنعت همچنین استانداردهایی را که از اهداف اعضا حمایت می‌کند، توسعه می‌دهند در حالی که آژانس‌های تخصصی سازمان ملل متحد مانند سازمان بین‌المللی هوانوردی غیرنظامی (ICAO) و سازمان بین‌المللی کار (ILO)، استانداردهایی را در حوزه‌های خاص مربوط به خود ایجاد می‌کنند که ممکن است مورد توجه سازمان‌های دیگر قرار نگیرد. ICAO مسئولیت استانداردسازی اسناد مسافرتی قابل خواندن با ماشین، از جمله گذرنامه‌های الکترونیکی را بر عهده دارد، در حالی که سازمان بین‌المللی کار دستورالعمل‌های مربوط به اسناد هویتی بیومتریک را برای دریانوردان فراهم می‌کند.

بیش از ۳۰ استاندارد بین‌المللی در زمینه بیومتریک از زمان تأسیس کمیته فرعی ۳۷ بیومتریک در ژوئن ۲۰۰۲ توسط کمیته فنی مشترک JTC1 (ISO / IEC) تهیه شده است. کارهای استانداردسازی بیومتریک کمیته فنی مشترک JTC1 در کمیته

فرعی ۲۷ تکنیک‌های امنیت IT (که شامل حفاظت، الگوریتم امنیت و ارزیابی امنیت) و کمیته فرعی ۱۷ شناسایی افراد و کارت‌ها، انجام می‌شوند.

استانداردسازی بیومتریک در ITU-T از ۲۰۰۱ با گروه مطالعه ITU-T 17 آغاز گردید که هماهنگی کارها را با تمام گروه‌های مطالعاتی انجام می‌دهد. گروه مطالعاتی ITU-T 17 مسئول بررسی روش‌های فنی برای شناسایی و حفاظت از افراد است. کار این گروه مطالعاتی در جهت برطرف کردن چالش‌های فعلی برای امنیت بیشتر زیرساخت‌ها، خدمات و برنامه‌های شبکه شدت می‌گیرد.

توصیه‌نامه ITU-T X.1081 "مدل چند حالته تلبیومتریک چارچوبی برای توصیف جنبه‌های امنیتی و ایمنی بیومتریک" اولین استاندارد بیومتریک است که منتشر می‌شود. مدلی که می‌تواند به عنوان چارچوبی برای شناسایی و تعیین جنبه‌های ایمنی تلبیومتریک و طبقه‌بندی فناوری‌های بیومتریک استفاده شود.

در برخی کشورها گذرنامه‌های قابل خواندن با ماشین صادر می‌کنند که داده‌های بیومتریک را می‌توان برای تأیید هویت در مرزها ذخیره کرد. تصویر صورت و شاید نمایش دیجیتالی از اثر انگشت یا عنبیه در تراشه کوچک شناسایی فرکانس رادیویی (RFID) ذخیره می‌شود و این می‌تواند با اطلاعات موجود در پایگاه داده بیومتریک مقایسه شود.

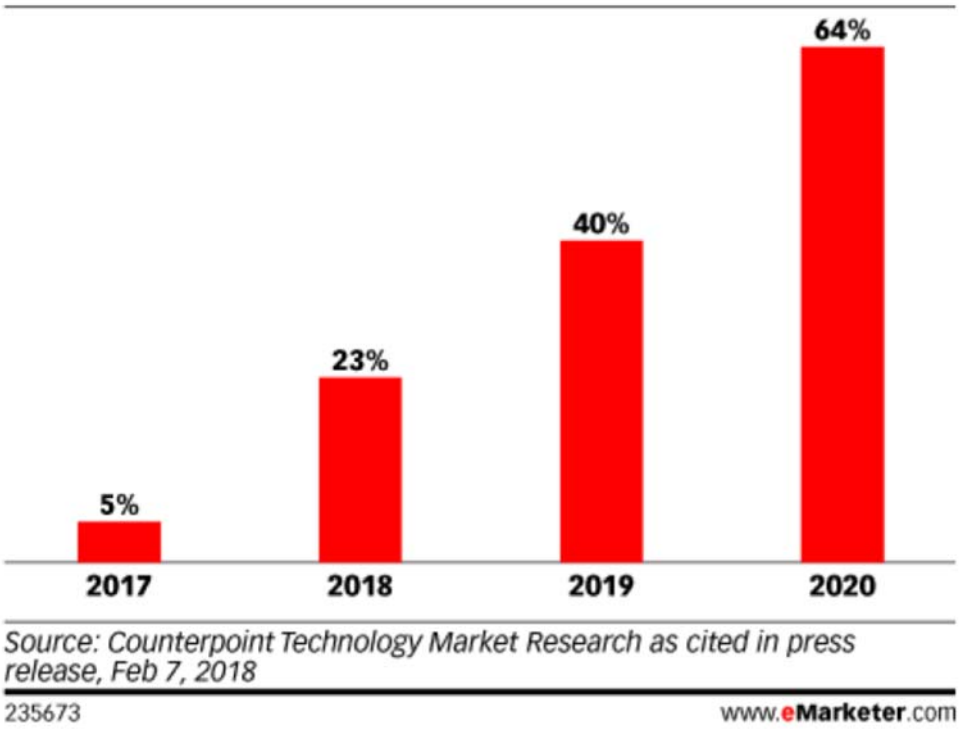
گروه مشترک متخصصان تصویر (JPEG)، یک گروه کاری ISO/IEC و ITU، مسئولیت JPEGروش‌های فشرده‌سازی تصویر از جمله JPEG2000، JPSearch و JPEG XR را با استانداردهای تصویربرداری بر عهده دارد. معمولاً از چنین روش‌هایی برای ذخیره عکس دیجیتالی روی تراشه در گذرنامه الکترونیکی استفاده می‌شود. استانداردهای فرمت JPEG یا JPEG2000 به ترتیب در توصیه های ITU-T T.81 و T.800 توسط گروه مطالعات ITU-T 16 توسعه یافته‌اند. JPEG XR (ISO/IEC 29199-2) یک استاندارد بین‌المللی است که در توصیه‌نامه ITU-T T832 اعمال می‌شود. یک قالب تصویری رمزگذاری شده است که در درجه اول برای ذخیره و تبادل محتوای عکاسی پیوسته طراحی شده است.

توصیه‌نامه‌های ITU-T X.1084 و X.1085، ۹ پروتکل احراز هویت را برای تلبیومتریک تعیین می‌کنند و توصیه‌نامه ITU-T X.1086 راهنمایی در مورد اقدامات متقابل برای ایجاد یک محیط امن و حفظ حریم خصوصی را ارائه می‌دهد. توصیه‌نامه ITU-T X.1087 روش‌هایی را برای محافظت از داده‌های بیومتریک چند حالته در برابر تلاش برای رهگیری، اصلاح یا جایگزینی داده ها ارائه می‌دهد. این مراحل شامل رمزگذاری، علامت‌گذاری به عنوان و تبدیل داده‌ها است. توصیه-نامه‌های ITU-T X.1088 و X.1089 به ترتیب چارچوبی را برای تولید و محافظت از کلیدهای دیجیتالی بیومتریک و راهی برای مدیریت احراز هویت بیومتریک فراهم می کنند.

وضعیت احراز هویت بیومتریک در دنیا

احراز هویت بیومتریک سال‌هاست که توسط نیروی انتظامی مورد استفاده قرار می‌گیرد. با این حال، اپل در سال ۲۰۱۳ با اضافه کردن حسگر اثر انگشت در آیفون 5S این فناوری را به بازار انبوه مصرف‌کننده وارد کرده و متعاقباً سایر تولیدکنندگان لوازم الکترونیکی این فناوری را در تجهیزات خود گنجانده‌اند. اکثر عموم، تشخیص هویت بیومتریک را آسان‌تر و راحت‌تر از رمزهای عبور یا پین کدها می‌دانند، اما به طور فزاینده نگران حریم خصوصی و امنیت دیجیتال هستند.

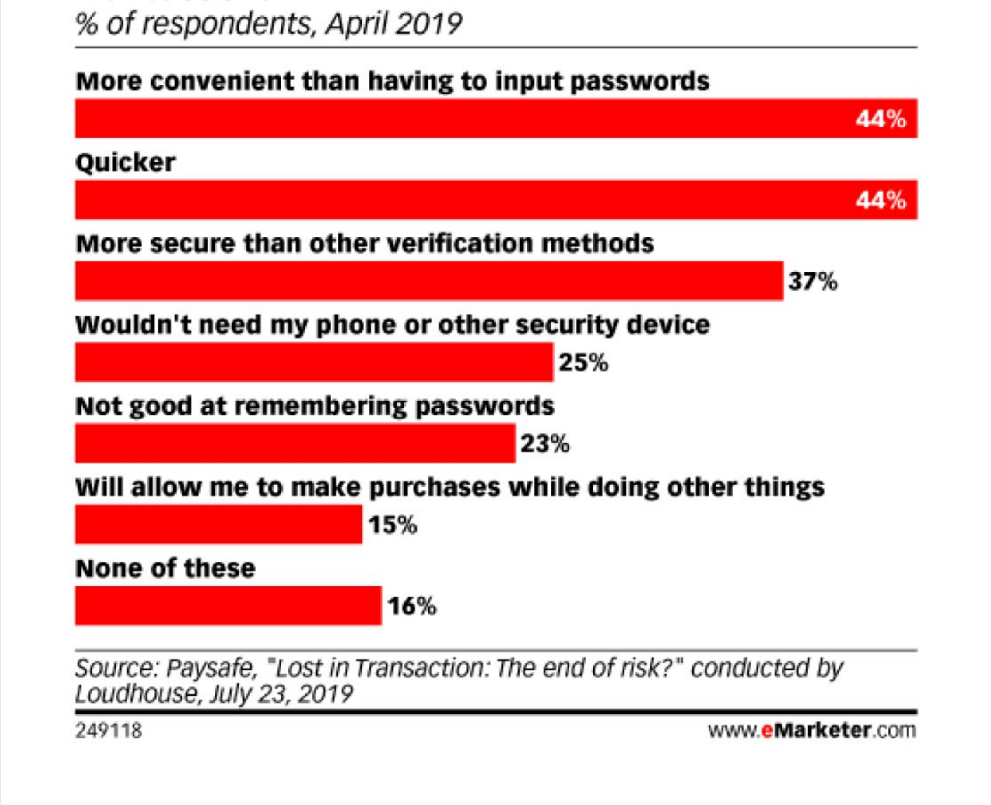
طبق تحقیقات شرکت Counterpoint[۳]، در سال ۲۰۲۰، ۶۴٪ از تلفن‌های هوشمند در سراسر جهان با فناوری تشخیص چهره عرضه می‌شوند که این رقم تنها ۲۳٪ در سال ۲۰۱۸ بوده است.



شکل ۱:سهم تلفن‌های هوشمند مجهز به سیستم تشخیص چهره طی سال‌های ۲۰۱۷ و ۲۰۲۰

[۳] شرکت آسیایی تحلیل صنعت جهانی که دفتر مرکزی آن در هنگ‌کنگ است و تحلیلگران در کشورهای مختلف از جمله کره جنوبی، هند، انگلستان، امریکا، چین و آرژانتین مستقر هستند.

طبق تحقیقات شرکت eMarketer[۴] تقریباً نیمی از مصرف‌کنندگان در سراسر جهان برای پرداخت های خود از بیومتریک (معمولاً فناوری تشخیص چهره) استفاده می‌کنند. طبق تحقیقات انجام شده در بین کاربران اینترنت مورد بررسی در ایالات متحده، انگلیس، اتریش، بلغارستان، کانادا و آلمان، ۴۴٪ از پاسخ‌دهندگان، سرعت را یکی از اصلی‌ترین مزیت‌های استفاده از این فناوری برای پرداخت کالاها یا خدمات می‌دانند وتقریباً یک‌چهارم گفتند که در یادآوری رمزهای عبور خود مشکل دارند.



شکل ۲: آنچه کاربران اینترنت در سراسر جهان به عنوان مزایای استفاده از بیومتریک می‌دانند

فرودگاه‌ها اغلب نه تنها به عنوان دروازه ورود به شهر بلکه به عنوان نماد زیبایی شهرهایی که به هم وصل می‌کنند، محسوب می‌شوند. آنها همچنین می‌توانند برای کشورها و شهرهای مهم، یک پنجره سودآور برای جذب مشاغل باشند. فرودگاه‌ها هرچقدر به فناوری‌های پیشرفته مجهز بوده و مسافر پسندتر به نظر برسند، تأثیر مثبتی بر منابع مالی محلی خواهد گذاشت. بنابراین فرودگاه‌ها یک بستر ایده‌آل برای گردآوری و استفاده فناوری‌های جدید هستند تا به‌این‌ترتیب از رشد جهانی ترافیک مسافر بهره‌مند شده و سرمایه‌گذاری بیشتری به‌صورت مستقیم یا غیرمستقیم جذب کنند.

[۴] eMarketer یک شرکت تحقیقاتی امریکایی در زمینه بازاریابی دیجیتال، رسانه‌ها و تجارت می‌باشد که در سال ۱۹۹۶ تاسیس شده است.

در سال ۲۰۱۹ ، قلمرو بیومتریک در فرودگاه‌ها به واقعیت تبدیل شده و آینده‌ای از هوش مصنوعی در حمل‌ونقل هوایی را در پیش گرفته است. استفاده از فناوری تشخیص چهره در فرودگاه‌هایی همچون آتن، نیویورک، لندن و همچنین شهرهای اصلی چین آغاز شده است. رویکردهای جایگزین همچون استفاده از شناسایی اثر کف دست (در کره جنوبی) نیز بخشی از این روند است.

در ثبت ویزای بیومتریک، اطلاعاتی شامل مشخصات فیزیکی منحصر به فردی مانند اثر انگشت، مشخصات صورت و الگوی عنبیه ی چشم است که در تعیین هویت افراد ثبت و از آن استفاده می شود و در واقع اطلاعات ویزای بیومتریک برای این انجام می گیرد که از راه مجراهای دیگری هویت افراد را بتوان به راحتی تشخیص داد و در این پیامد، کلیه‌ی افرادی که قصد سفر و دریافت ویزای شینگن یا کشور کانادا را دارند باید به هنگام مراجعه به سفارت یا دفتر کارگزار سفارت، اطلاعات بیومتریک خود مانند اثر انگشت و تصویر چهره‌ی خود را در درگاه های مخصوص آنان ثبت نمایند. در سال ۲۰۱۵ بود که کلیه‌ی کشورهای عضو و متحد ویزای شینگن به سیستم اطلاعات ویزای بیومتریک پیوستند.

در حال حاضر مرسوم‌ترین شیوه تشخیص هویت مشتریان بانکی در ایران ارائه کارت شناسایی (کارت ملی و شناسنامه) است. هنوز هم مشتریانی هستند که با ارائه گواهی‌نامه رانندگی اصرار به دریافت خدمات دارند و تلاش کارمندان در راضی نمودن این افراد که این کار غیرقانونی است در خیلی موارد راه به جایی ندارد. سیستم‌های بیومتریک در بانکداری اگر چه خالی از اشکال نیستند و در برخی مواقع قابل جعل به نظر می‌رسند اما حقیقت این است در مقایسه با سیستم‌های مرسوم کنونی به شدت پیشرفته و قابل اتکا می‌باشند.

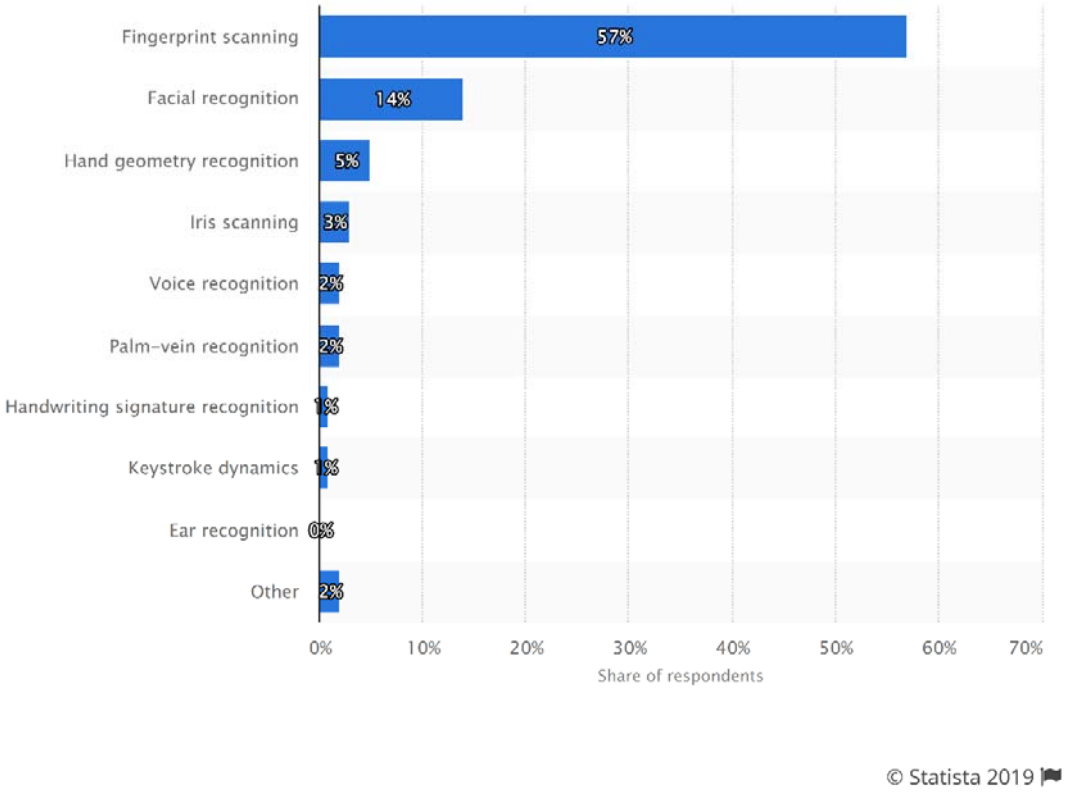
بسیاری بانک‌ها استفاده از این روش را از نظر هزینه‌ای به‌صرفه نمی‌دانند اما یک مقایسه ساده با هزینه‌هایی که جعل به بانک‌ها تحمیل خواهد کرد و یا هزینه‌های گزافی که جهت ارسال پیامک برای ارائه مشخصات فردی مشتریان به بانک‌ها صرف می‌شود چندان هم رقم بالایی نخواهد بود.

اثر انگشت چیزی نیست که مشتری آن را جا بگذارد. درحال حاضر جا گذاشتن مدارک شناسایی شاید برای ساعت‌ها و روزها کارهای برخی مشتریان را با تاخیر مواجه می نماید. به این ترتیب مباره با پولشویی هم تسهیل می‌شود و جنایتکاران برای پیشبرد اهداف سودجویانه‌شان با مشکلات بیشتری مواجه خواهند شد.

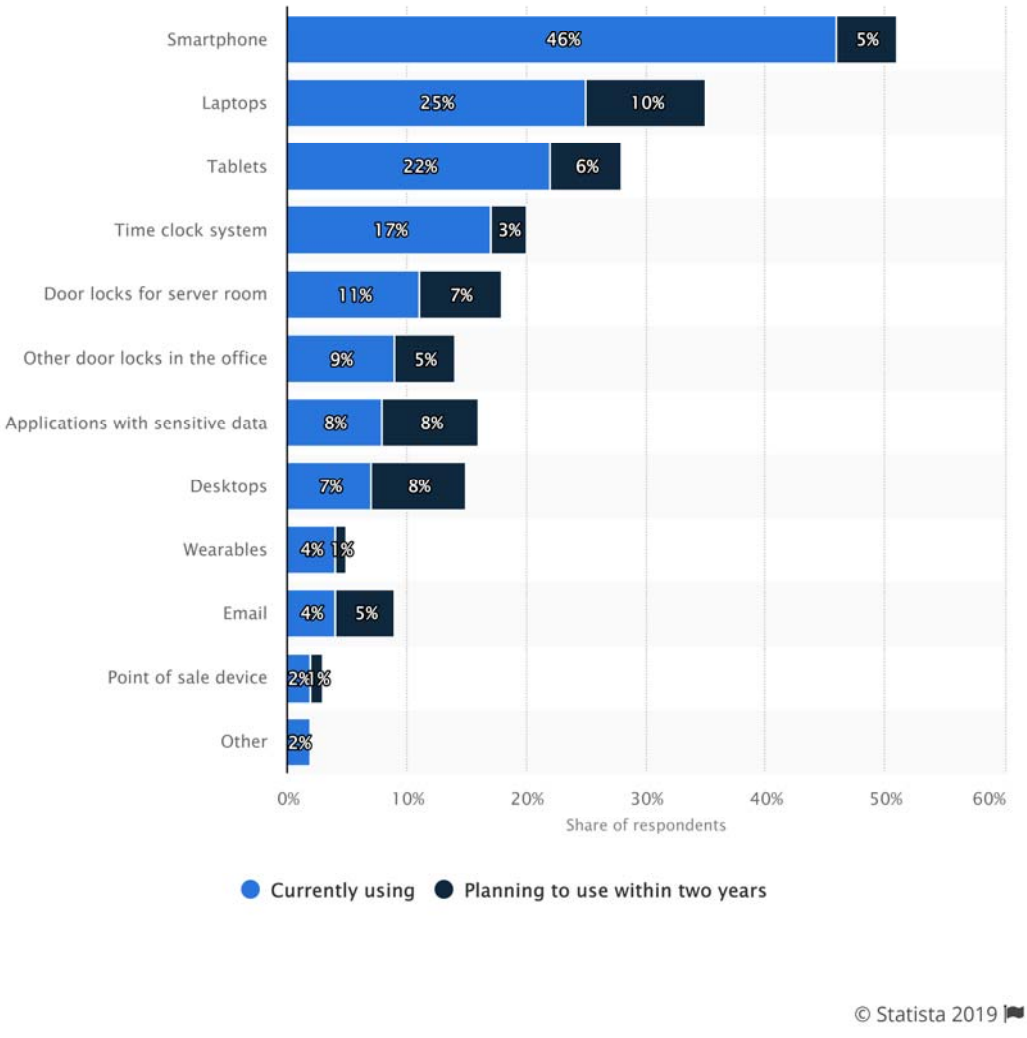
همچنین با ایجاد بانک اطلاعات بیومتریک مشتریان، طی مدت کوتاهی بانک عظیمی از اطلاعات اشخاص جامعه ایجاد می‌شود که می‌تواند مورد استفاده سایر دستگاه‌های اجرایی کشور نیز قرارگیرد (دستگاه‌هایی که ارائه خدمات آنان منوط به تشخیص هویت متقاضیان خدمات است).

شکل ۳ و شکل ۴ استفاده تجاری از احراز هویت بیومتریک در آمریکای شمالی و اروپا را از سال ۲۰۱۸ به ترتیب برای فناوری‌های مختلف بیومتریک و کاربردهای مختلف نشان می‌دهند. اسکن اثر انگشت متداول‌ترین روش احراز هویت

بیومتریک است و حدود ۵۷ درصد از پاسخ دهندگان اظهار داشتند که شرکت آن‌ها از این فناوری استفاده کرده است. تلفن‌های هوشمند رایج‌ترین بستر برای احراز هویت بیومتریک در محل کار هستند. ۴۶ درصد از پاسخ‌دهندگان گفتند که شرکت آن‌ها در حال حاضر برای این منظور از تلفن‌های هوشمند استفاده می‌کند.

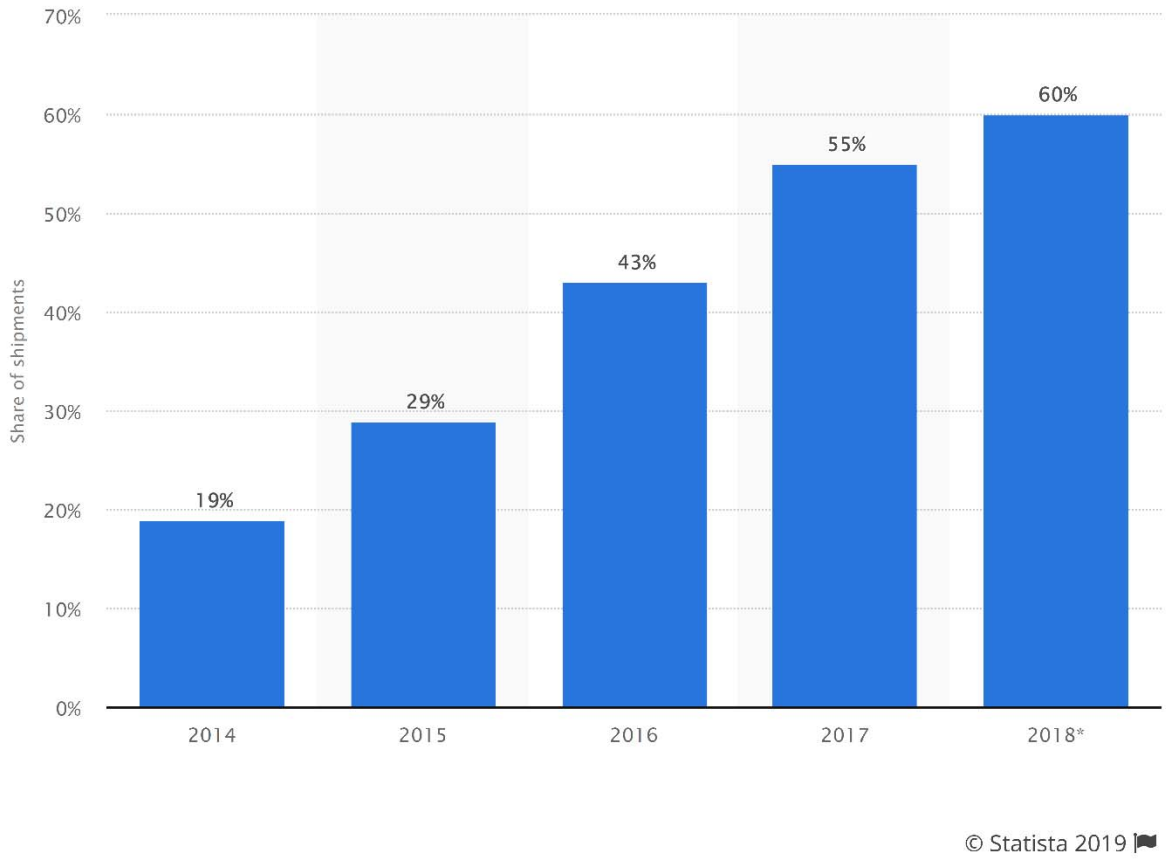


شکل ۳: استفاده تجاری از احراز هویت بیومتریک در امریکای شمالی و اروپا از سال ۲۰۱۸ بر حسب تکنولوژی



شکل ۴ : استفاده تجاری از احراز هویت بیومتریک در امریکای شمالی و اروپا از سال ۲۰۱۸ بر حسب بستر کاربرد

شکل ۵ سهم گوشی‌های هوشمند با حسگر اثر انگشت در سراسر جهان را از سال ۲۰۱۴ تا ۲۰۱۸ نشان می‌دهد. ۵۵ درصد از تلفن‌های هوشمند موجود در سراسر جهان در سال ۲۰۱۷ دارای حسگر اثر انگشت بودند.



شکل ۵: سهم گوشی‌های هوشمند با حسگر اثر انگشت در سراسر جهان از سال ۲۰۱۴ تا ۲۰۱۸

جمع بندی

از گذشته تشخیص هویت برای انسان، امری حیاتی بوده و هست. کارت‌های شناسایی و مغناطیسی، گذرنامه و شناسنامه دارای نواقصی مثل فرسوده شدن، مفقودی، امکان جعل و فراموشی می‌باشند که امروزه فناوری بیومتریک مبتنی بر ویژگی‌های فیزیولوژیکی و رفتاری افراد است روشی جدید، امن، با سرعت و دقت بالا در شناسایی دقیق و تشخیص هویت واقعی افراد استفاده می‌شود. از جمله ویژگی‌های فیزیولوژیکی می توان به الگوی عنبیه و شبکیه چشم، الگوی ورید، الگوی چهره و نمودار حرارتی صورت، الگوی هندسه دست و اثر انگشت و در عین حال از ویژگی‌های رفتاری می‌توان به الگوی صدا و نحوه مکالمه، الگوی نحوه امضاء، دست خط، نحوه تایپ کردن و نحوه راه رفتن افراد اشاره نمود. فناوری بیومتریک در مقابل اقلام هویتی سنتی دارای مزایای بسیاری مثل امنیت بالا، سرعت و راحتی استفاده و حفظ اسرار و هویت اشخاص و همچنین عدم امکان تقلب و کاهش تخلفات می باشد.