بیومتریک ابزار امنیت شهروند هزاره سوم

علی‌اکبر جلالی، دانشیار دانشکده مهندسی برق، دانشگاه علم و صنعت ایران
مزدک رجبی نسب،کارشناس مهندسی برق دانشگاه علم و صنعت ایران
تاریخ دریافت: ۸۷/۷/۲ تاریخ پذیرش:۸۷/۹/۱۴

چکیده

جامعه اطلاعاتی در تمام کشورهای جهان با نسبت‌های مختلفی در حال شکل‌گیری و گسترش است. در بسیاری از ادبیات کشورهای جهان، شهرهای الکترونیکی، سازمان‌های مجازی و شهروند الکترونیکی واژگان‌های عادی و قابل فهم مردم شده است. امنیت در کنار زیرساخت توسعه این پدیده‌های هزاره سوم همواره جزو سئوالات مطرح شهروندان در جهان بوده است. مهندسان و متخصصان فناوری اطلاعات با همکاری آژانس‌های امنیتی هر روز ابزار و ایده‌های جدیدی را در حوزه سخت افزاری و نرم‌افزاری برای احساس امنیت بیشتر شهروندان طراحی، پیاده‌سازی و معرفی می‌کنند. در میان مجموعه سخت افزارهای امنیتی ارائه شده تاکنون، بیومتریک را بهترین دانسته و آن را تکنولوژی امنیتی قرن آینده خوانده‌اند.

با توسعه کاربردهای فناوری اطلاعات مانند تجارت الکترونیکی که در آن کارت‌های اعتباری، پول دیجیتالی، امضاء دیجیتالی، تعهدات دیجیتالی، نقل و انتقالات وجوه به صورت الکترونیکی و ده‌ها مورد دیگر که نیازمند امنیت ویژه است، نیاز به ابزارهای امنیتی نوینی دارد. از مجموعه ابزارها و تکنولوژی‌های موجود در خانواده بیومتریک، بعضی از آنها که مستقیماً مورد استفاده

شهروندان در منزل بوده و پلیس آگاهی نیز می تواند با دسترسی به اطلاعات حاصل از آنها زمینه امنیت بیشتر را فراهم کند از اهمیت بیشتری برخوردار شده است. در این مقاله ضمن معرفی مشخصه‌های بیومتریک، به بیان کاربرد و جایگاه آنها در سامانه‌های امنیتی پرداخته شده است و به صورت ویژه به یک طرح عملی سخت‌افزاری و نرم‌افزاری مرتبط با انگشت نگاری که در دانشگاه علم و صنعت ایران ساخته شده، پرداخته شده است.

کلمات کلیدی: بیومتریک (Biometrics)، فناوری اطلاعات (Information Technology)، پلیس آگاهی (C.I.D Police)، انگشت نگاری (Fingerprinting)، امنیت شهروندان(The safety of Citizens)

نشانی نویسنده مسئول: دانشگاه علم و صنعت ایران، گروه کنترل دانشکده مهندسی برق

مقدمه:

با توسعه کاربردهای فن‌آوری اطلاعات انتظار مردم برای این که بتوانند بیشتر امور خود را در منزل انجام دهند افزایش یافته است. پلیس آگاهی در یک اقدام مؤثر می‌تواند بعضی از خدمات خود را به منزل شهروندان منتقل کند. انگشت‌نگاری یکی از مواردی است که در حوزه استفاده از ویژگی‌های بیومتریک به راحتی قابل پیاده‌سازی در منازل است. برای تأیید یا تعیین هویت فردی که خدمات را درخواست می کند، سامانه‌ها نیازمند طرح شناخت شخص قابل اعتماد است. هدف از این طرح‌ها اطمینان از این امر است که خدمات فقط در دسترس کاربر قانونی و نه کس دیگری، قرار می‌گیرد. فقدان طرح‌های شناخت شخصی قدرتمند این سامانه‌ها در برابر حمله‌های یک نفوذگر آسیب‌پذیر است. تشخیص بیومتریک یا زیست‌سنجی، شناخت اتوماتیک افراد براساس ویژگی‌های فردی و یا فیزیولوژیکی است. با استفاده از بیومتریک، تأیید و ایجاد هویت فردی بر اساس این که «او چه کسی است» و نه این که «او چه چیزی دارد» (برای مثال کارت شناسایی) و یا «چه چیزی به خاطر می‌آورد» (برای مثال رمز عبور) امکان‌پذیر است. روش‌های مرسوم نشانه‌مدار و دانش‌مدار در واقع تشخیص شخصی مثبتی را فراهم نمی‌کند، زیرا آنها بر جایگزینی از هویت فرد تکیه دارد.

بنابراین آشـکار اسـت که هر سامانه‌ای که تشخیص شخصی قابل اعتماد را اطمینان می‌دهد، لزوماً شامل عنصر بیومتریک است.

نخسـتین کاری که در زمینه انگشـت‌نگاری و سـازماندهی آن صورت گرفت، تلاش‌های مارچلومالپیگی[1] در سـال ۱۶۸۶ میلادی بود. مالپیگی، اسـتاد کالبدشناسـی در ایتالیا، خطوط برجسـته نوک انگشـت‌های انسان را در زیر میکروسکوپ مورد مطالعه قرار داد و متوجه شد این خطوط برجسـته با طرح‌هایی حلقوی و مارپیچی مرتب شـده اسـت. آلفونس برتیلون[2]، رییس بخش شناسـایی جرائم اداره پلیس در پاریس، در اواسـط قرن نوزدهم، ایده استفاده از مشخصه‌های بیومتریک را برای شناسایی جرائم گسترش داد. اولین بار در سال ۱۸۵۸ در اروپا از اثرانگشـت برای شناسایی زندانیان استفاده شد. در سال‌های ۱۸۸۰–۱۸۸۹، سر فرانسیس گالتون[3] دانشمند انگلیسی، دست‌اندرکار تدوین روشی برای طبقه‌بندی اثر انگشت اشخاص شـد. چند سـال بعد یکی از مأموران پلیس لندن به نام سـر ادوارد هنری[4]، روش او را آسان‌تر کرد. بلافاصله پس از آن، اسـتفاده از اثر انگشـت به عنوان وسـیله‌ای برای شناسایی افراد و کشف جرم، تقریبا در تمام کشورها آغاز شد. درست بعد از این اکتشاف، بسیاری از ادارات اجرای قانون، ایده نگاه کردن در اثر انگشـت مجرمان و ذخیره آن در پایگاه داده‌ها (در واقع پرونده کارتی) را پذیرفتند[۱].

سامانه‌های بیومتریک:

سـامانه بیومتریک اساسـاً یک سـامانه تشخیص الگو اسـت که با به‌دست آوردن داده‌های بیومتریک از یک فرد عمل می‌کند. این سامانه یک مجموعه ویژگی از داده‌های به‌دست آمده اسـتخراج کـرده و این مجموعه ویژگـی را در برابر مجموعه الگوها در پایگاه داده مقایسـه می‌کنـد. هـر ویژگـی رفتاری و یا فیزیولوژیکی با شـرایط زیر به عنوان مشـخصه بیومتریک

1. Marcello Malpighi
2. Alphonse Bertillon
3. Francis Galton
4. Edward Henri

استفاده می‌شود[۲]:

۱. جهانی بودن[۱]: هر فرد باید این ویژگی را داشته باشد.

۲. تمایز[۲]: هر دو فرد باید برحسب این ویژگی، متفاوت باشند.

۳. دوام[۳]: این ویژگی باید در یک دوره زمانی برای یک فرد ثابت باشد.

۴. قابلیت جمع‌آوری[۴]: این ویژگی را بتوان به صورت کمّی اندازه‌گیری کرد.

با این حال، در یک سامانه بیومتریک عملی برخی از مسائل دیگر وجود دارد که باید مد نظر قرار گیرد:

۱. عملکرد[۵]: به سرعت و دقت تشخیص قابل دسترسی، منابع لازم برای دستیابی به سرعت و دقت مطلوب تشخیص و نیز عوامل محیطی و عملیاتی اشاره دارد که بر سرعت و دقت تأثیر می‌گذارد.

۲. قابلیت پذیرش[۶]: به میزانی اشاره دارد که افراد مایل هستند استفاده از شناسه (ویژگی) بیومتریک خاص را در زندگی روزانه‌شان بپذیرند.

۳. آسیب‌پذیری[۷]: این موضوع استحکام این مشخصه در برابر حملات نفوذگران را نشان می‌دهد.

سامانه بیومتریک عملی باید دقت، سرعت و شرایط مدیریت را در نظر بگیرد تا بصورت عام پذیرفته شده و سامانه را درمقابل تلاش‌های نفوذگران مقاوم سازد.

---

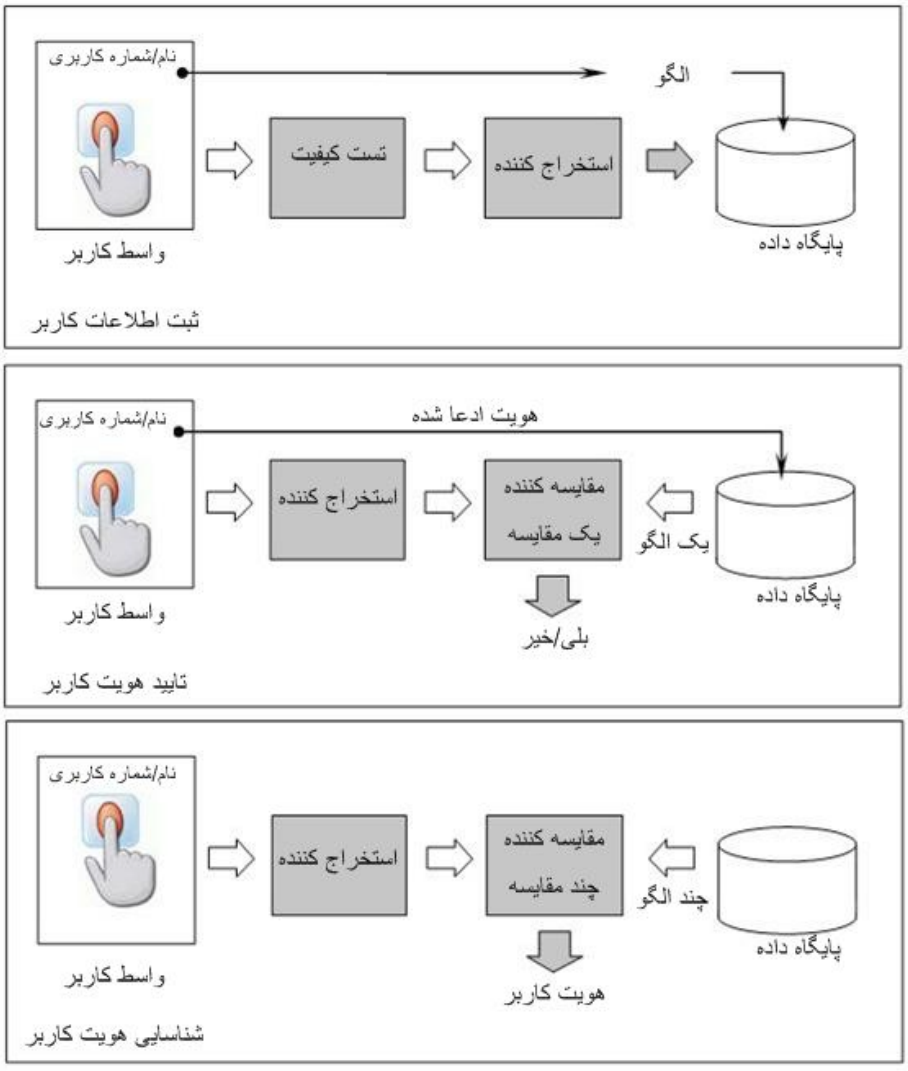
1. Universality
2. Distinctiveness
3. Permanence
4. Collectability
5. Performance
6. Acceptability
7. Circumvention

بسته به بافت کاربرد، یک سامانه بیومتریک می‌تواند یا در حالت تأیید[1] یا حالت شناسایی[2] عمل کند.

۱. **در حالت تأیید**، سامانه، هویت فرد را با مقایسه داده‌های بیومتریک به‌دست آمده با الگو یا الگوهای بیومتریک که در پایگاه داده‌های سامانه ذخیره شده، تأیید می‌کند. در این سامانه فرد از طریق شماره شناسایی شخصی[3]، نام کاربری یا کارت هوشمند، یک هویت را ادعا و مطالبه می‌کند و سامانه، برای تعیین این که آیا این ادعا صحت دارد یا نه، مقایسه یک به یک انجام می‌دهد. تأیید هویت، برای تشخیص مثبت استفاده می‌شود، که هدف از آن، جلوگیری از استفاده از یک هویت توسط افراد متعدد است.

۲. **در حالت شناسایی**، سامانه فرد را از طریق جستجوی الگو همه کاربران در پایگاه داده‌ها تشخیص می‌دهد. بنابراین سامانه، مقایسه یک به چند را برای معین کردن هویت فرد اجرا می‌کند (مثلاً این داده‌های بیومتریک چه کسی است؟) شناسایی، عنصر مهمی در کاربردهای تشخیص منفی است که در آن سامانه بیان می‌کند که آیا این فرد، کسی است که هویت خود را انکار کرده؟ هدف از تشخیص منفی، جلوگیری از استفاده از چندین هویت توسط یک فرد است. شناسایی را همچنین می‌توان برای سهولت در تشخیص مثبت استفاده کرد (لازم نیست کاربر، هویت خود را مشخص کند). در حالی که روش‌های سنتی تشخیص فرد مانند رمز عبور، شماره شناسایی شخصی، کلید و نشانه را می‌توان برای تشخیص مثبت استفاده کرد، تشخیص منفی را فقط می‌توان از طریق بیومتریک به‌دست آورد.

1 - Verification
2 - Identification
3 - PIN



شکل ۱: نمودار کلی ثبت، تأیید و شناسایی

مشـکل تأیید را می‌توان به صورت زیر مطرح کرد: با در نظرگرفتن بردار مشـخصه ورودی X_Q (که از داده‌های بیومتریک اسـتخراج شـده اسـت) و هویت مطالبه شده I، مشخص کند که آیا (I, X_Q) به طبقه w_1 تعلق دارد یا w_2، که در آن w_1 نشـان می‌دهد که این ادعا صحت

دارد (کاربر حقیقی) و w_2 نشان می‌دهد که این ادعا کذب است (فریب کار). X_Q با X_I تطبیق داده می‌شود[۲].

$$(I, X_Q) \in \begin{cases} \omega_1 & if\ S(X_Q, X_I) \geq t \\ \omega_2 & Otherwise \end{cases}$$

S تابعی است که شباهت بین بردارهای مشخصه X_Q و X_I را اندازه گیری می کند و t آستانه از پیش تعریف شـده اسـت. مقدار $S(X_Q, X_I)$ نمره شباهت بین مشخصه بیومتریک کاربر و هویت ادعا شده است. بنابراین هویت ادعا شده براساس متغیرهای X_I، I، X_Q و t و تابع S طبقه‌بندی می‌شـود. باید توجه داشـت که اندازه‌گیری‌های بیومتریک (برای مثال اثر انگشت) یک فرد در زمان‌های مختلف، تقریباً هرگز یکسان نیست و این دلیل معرفی آستانه t است.

از طرف دیگر شناسـایی را می‌توان بدین صورت بیان کرد: با در نظرگرفتن بردار مشـخصه ورودی X_Q، هویـت $I_k, k \in \{1+N, N, \ldots, 1, 2\}$ را تعییـن کنیـد. در اینجـا $I_N \ldots, I_2, I_1$ هویت‌هایی هست که در این سامانه ثبت نام شده و I_{N+1} مورد رد شده را نشان می‌دهد که در آن هیچ هویت مناسبی را نمی‌توان برای کاربر تعیین و مشخص کرد]۲[.

$$X_Q \in \begin{cases} I_K & if\ \max_k (X_Q, X_k) \geq t \quad K = 1,2,\ldots,N \\ I_{N+1} & Otherwise \end{cases}$$

سامانه‌های بیومتریک با استفاده از چهار مدول اصلی زیر طراحی می‌شوند[۴]:

۱. **مدول حسـگر**: که داده‌های بیومتریک یک فرد را می‌گیرد. مانند حسـگر اثر انگشـت که ساختار برآمده و تورفته انگشت یک کاربر را نشان می‌دهد.

۲. **مدول اسـتخراج ویژگی**: که در آن داده‌های بیومتریک به‌دسـت آمده برای اسـتخراج مجموعه‌ای از ویژگی‌های برجسـته یا متمایز پردازش می‌شـود. برای مثال، موقعیت و جهت در اثر انگشت در مدول استخراج مشخصه سامانه بیومتریک مبتنی بر اثر انگشت استخراج می‌شود.

۳. **مدول تطبیق**: که در آن مشـخصه‌هایی که در زمان تشـخیص استخراج می‌شود، در برابر الگوهای ذخیره شده برای تولید مقادیر تطبیق مقایسه می‌شود. برای مثال در مدول تطبیق

یک سامانه اثرانگشت، تعداد تطبیق بین تصاویر ورودی و الگوی اثر انگشت تعیین شده و نمره تطبیق گزارش می‌شود. مدول تطبیق نیز یک مدول تصمیم‌گیری را حفظ می‌کند که در آن هویت مطالبه شـده کاربر تأیید شـده (تأیید) و یا هویت کاربر براساس نمره تطبیق ایجاد می‌شود (شناسایی).

۴. مـدول پایـگاه داده‌های سـامانه: که برای ذخیره الگوهای بیومتریک کاربران اسـتفاده می‌شود. مدول ثبت نام مسئول ثبت نام کاربران در پایگاه داده‌ها است.

در مرحله ثبت‌نام، مشخصه بیومتریک یک فرد برای تولید الگو به وسیله حسگر بیومتریک اسـکن می‌شـود. برای اطمینان از این که نمونه به‌دست آمده را می‌توان به طور قابل اعتمادی برای تولید الگو پردازش کرد، کنترل کیفیت به طور کلی انجام می‌شـود. بسـته به کاربرد، الگو را می‌توان در پایگاه داده‌های مرکزی سامانه بیومتریک ذخیره کرده و یا در کارت هوشمند که برای فرد صادر شده، ثبت کرد.

خطاهای سامانه‌های بیومتریک

دو نمونه از یک ویژگی بیومتریک یک شـخص (برای مثال دو اثر انگشـت سبابه کاربر) به واسـطه شـرایط ناقص (برای مثال نویز حسگر و انگشت خشـک)، تغییرات در ویژگی‌های رفتاری یا فیزیولوژیکی کاربر (مثلاً برش‌ها و کوفتگی‌ها در انگشـت)، شـرایط محیطی (مثلاً دما و رطوبت)، و تعامل کاربر با حسگر (مثلاً جابجایی انگشت) دقیقاً یکسان نیست. بنابراین، پاسخ سامانه بیومتریک، نمره تطبیق $S(X_Q,X_I)$ است که شباهت بین ورودی و الگو را تعیین می‌کند. هر چقدر این مقدار بالاتر باشـد، احتمال آن که سـامانه این دو اندازه‌گیری بیومتریک را از یک فرد اعلام کند، معین‌تر است. تصمیم سامانه به وسیله آستانه t تنظیم می‌شود: جفت نمونه‌های بیومتریک که نمره‌ای بالاتر از t یا مسـاوی با آن تولید می‌کند، جفت‌های یکسـان نامیـده می‌شـود (یعنی متعلق به یک فرد)؛ جفت نمونه‌هـای بیومتریک که نمره‌ای پایین‌تر از t تولید می‌کند، جفت‌های غیر یکسـان نامیده می‌شـود (یعنی متعلق به افراد مختلف). توزیع

نمرات تولید شده از جفت‌های نمونه‌هایی از یک فرد، توزیع خالص[1] و از افراد مختلف توزیع فریبکارانه[2] نامیده می‌شود. سامانه تأیید بیومتریک، دو نوع خطا ایجاد می‌کند:

۱. اندازه‌گیری‌های بیومتریک از دو فرد مختلف، یکسان اعلام شود (تطبیق غلط).

۲. اندازه‌گیری‌های بیومتریک از یک فرد، متفاوت اعلام شود (عدم تطبیق غلط).

این دو نوع خطا به ترتیب پذیرش غلط و رد غلط نامیده می‌شود. در هر سامانه بیومتریک یک رابطه جایگزینی بین میزان تطبیق غلط (FMR[3]) و میزان عدم تطبیق غلط (FNMR[4]) وجود دارد. در واقع، FMR و FNMR کارکردهای آستانه سامانه (t) هستند؛ کاهش آن سامانه را در مقابل نویز و تغییرات ورودی مقاوم‌تر می‌کند یعنی FMR افزایش می‌یابد. از طرف دیگر، اگر t افزایش یابد سامانه سخت‌گیرتر شده و FNMR افزایش می‌یابد. عملکرد سامانه را به ازای مقادیر t می‌توان به شکل منحنی مشخصه کارکرد دریافت کننده (ROC[5]) نشان داد. منحنی ROC تابعی از FMR است.

اگر الگوی بیومتریک ذخیره شده کاربر I به وسیله X_I نشان داده شود و ورودی به دست آمده برای تشخیص با X_Q نشان داده شود، فرضیه‌های زیر را خواهیم داشت:

H_0: ورودی X_Q از شخص یکسان با الگوی X_I نمی‌باشد.

H_1: ورودی X_Q از شخص یکسان با الگوی X_I می‌باشد.

تصمیمات مرتبط به ترتیب زیر است:

D_0: شخصی نیست که ادعا می‌کند.

D_1: شخصی است که ادعا می‌کند.

قانون تصمیم به ترتیب زیر می‌باشد. اگر نمره تطبیق $S(X_Q,X_I)$ کمتر از آستانه سامانه باشد، D_0 انتخاب می‌شود. در این روش خطاها به صورت زیر بیان می‌شوند:

1. Genuine Distribution
2. Impostor Distribution
3. False Match Rate
4. False Non Match Rate
5. Receiver Operating Characteristic

نوع ۱: تطبیق غلط (D_1 زمانی انتخاب شود که H_0 درست باشد).

نوع ۲: عدم تطبیق غلط (D_0 زمانی انتخاب شود که H_1 درست باشد).

FMR احتمال خطای نوع ۱ و FNMR احتمال خطای نوع ۲ به ترتیب زیر می‌باشند[۴].

$$FMR = P(D_1|H_0)$$

$$FNMR = P(D_0|H_1)$$

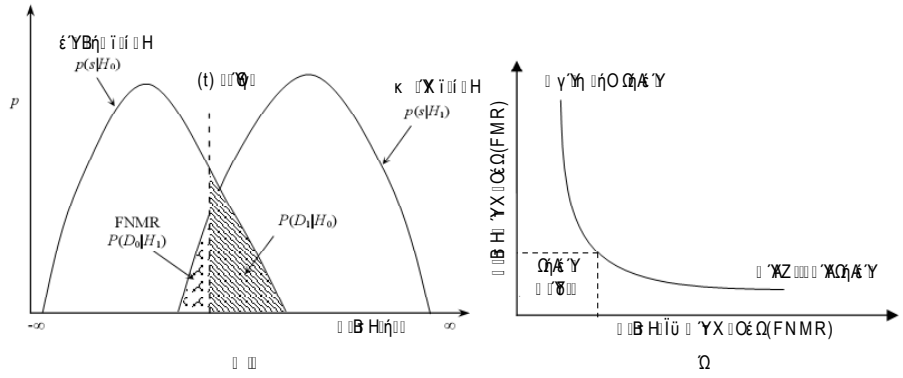
برای ارزیابی صحت و درستی سامانه بیومتریک باید نمرات تولید شده از چندین تصویر از یک انگشت (توزیع $P(S(X_Q,X_1)|H_1)$) و نمرات تولید شده از چندین تصویر از انگشت‌های مختلف (توزیع $P(S(X_Q,X_0)|H_1)$) جمع‌آوری کنیم. شکل (۲) محاسبه FMR و FMNR بر روی توزیع خالص و توزیع فریبکارانه را نشان می‌دهد[۴].

$$FMR = \int_t^{\infty} \rho(S(X_Q,X_1)|H_0).\delta$$

$$FNMR = \int_{-\infty}^{t} \rho(S(X_Q,X_1)|H_1).\delta$$

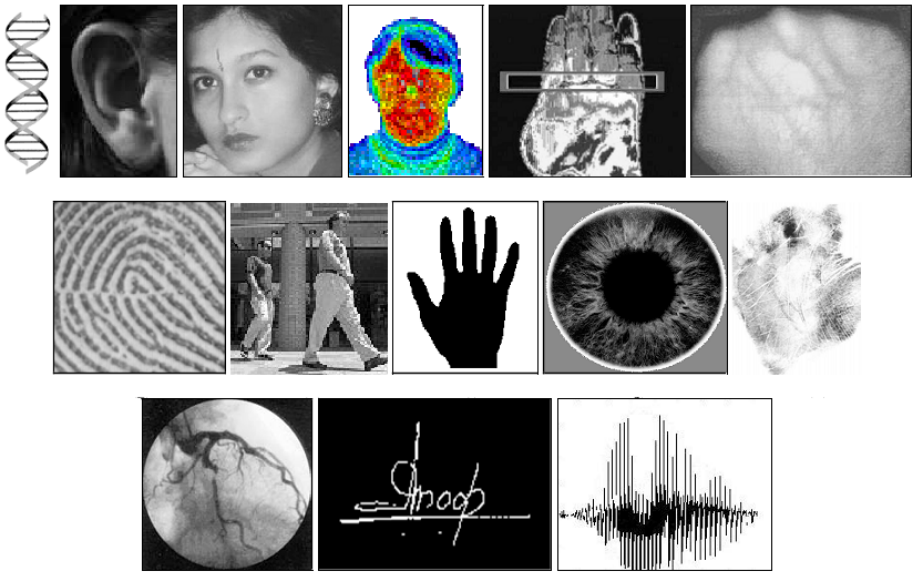
علاوه بر خطاهای فوق، کوتاهی در گرفتن صحیح مشخصه کاربران (FTC[1]) و کوتاهی در ثبت صحیح کاربران (FTE[2]) نیز برای تعیین صحت سامانه بیومتریک استفاده می‌شود. درجه FTE زمانی بروز می‌کند که سامانه نتواند مشخصه بیومتریک با کیفیت مناسب به‌دست آورد. از طرف دیگر درجه FTE، به درصد خطایی که هنگام ثبت کاربران روی می‌دهد، اشاره دارد. به خاطر وابستگی‌های متقابل بین درجات کوتاهی و درجات خطا، کلیه این موارد مشخصات مهمی را در سامانه بیومتریک تشکیل می‌دهد و باید در زمان ارزیابی عملکرد گزارش شود.

1. Failure to Capture
2. Failure to Enroll



شکل۲: میزان خطای سامانه بیومتریک

شـرایط صحت سـامانه بیومتریک، وابسـتگی زیادی به کاربرد دارد. برای مثال، در برخی از کاربردهای پزشـکی قانونی، مانند شناسـایی جرائم، یکی از مسـائل مهم طراحی، درجه FNMR است یعنی نمی‌خواهیم شناسایی مجرم را حتی با خطر بررسی دستی تعداد زیادی از تطبیق‌های نادرسـت که به وسـیله سـامانه بیومتریک تولید شده، از دست بدهیم. از طرف دیگر FMR می‌تواند یکی از مهم‌ترین عوامل در کاربرد کنترل دسترسی ایمن باشد که در آن هدف اصلی جلوگیری از دسترسـی نفوذگران اسـت. شرایط عملکرد بیشتر کاربردها بین این دو بی‌نهایت قرار دارد. برای مثال، در کاربردهایی مانند تأیید کارت ATM بانک، تطبیق غلط به معنای از دسـت رفتن چند صد دلار اسـت در حالی که ممکن است FNMR بالا منجر به یک مشتری ارزشمند شود.



شکل۳: مثال‌هایی از ویژگی‌های بیومتریک

مقایسه بیومتریک‌های گوناگون

مشخصه‌های بیومتریک متعددی وجود دارند و در کاربردهای متنوعی استفاده می‌شوند(شکل ۳). هر مشخصه نقاط ضعف و قوت خاص خود را دارد و انتخاب یک مشخصه به کاربرد بستگی دارد. انتظار نمی‌رود که هیچ بیومتریکی، شرایط تمام کاربردها را به صورت مؤثری رعایت کند. به عبارت دیگر، هیچ بیومتریکی، «بهینه» نیست. تطبیق بین یک بیومتریک خاص و یک کاربرد، بسته به حالت عملیاتی ساخته شده از کاربرد و خواص ویژگی‌های بیومتریک تعیین می‌شود. مقدمه مختصری در باب مشخصه‌های بیومتریک متداول در زیر آمده است[۵].

۱. **DNA**: کد منحصر به فرد برای شناسایی فرد است (به استثنای این واقعیت که دوقلوها الگوهای DNA یکسانی دارند.) با این حال، در حال حاضر در پزشکی قانونی و برای تشخیص فرد استفاده می‌شود.

۲. چهره: تشـخیص چهره، روشـی غیر تهاجمی[1] اسـت و تصویر چهره احتمالاً رایج‌ترین ویژگی بیومتریک اسـت که انسـان‌ها برای تشخیص فردی استفاده می‌کنند. متداول‌ترین روش‌ها برای تشخیص چهره براساس این موارد است: (۱) ترکیب چهره از قبیل چشم، ابرو، بینی، لب و روابط فضایی یا سه بعدی آنها (۲) تحلیل کلی از تصویر چهره که چهره را به عنوان ترکیب سنجیده شده‌ای از تعدادی از چهره‌های متعارف نشان می‌دهد.

۳. دما نگاری مادون قرمز: الگوی حرارت تابشـی از بدن انسـان، ویژگی یک فرد بوده و می‌توان به وسیله دوربین مادون قرمز بدون مزاحمت و همانند طیف منظم به‌دست آورد. این تکنولوژی را می‌توان برای تشـخیص پنهانی اسـتفاده کرد. حسـگرهای مادون قرمز خیلی گران هستند که عاملی است که مانع از استفاده گسترده دما نگار می‌شود.

۴. اثر انگشـت: انسـان‌ها در طی قرون از اثر انگشت برای شناسایی افراد استفاده کرده‌اند و صحت تطبیق با اسـتفاده از اثر انگشـت، خیلی بالا بوده اسـت. اثر انگشـت، الگوی برآمدگی‌ها و فرورفتگی‌ها در سطح اثر انگشت است که شکل‌گیری آن در طی هفت ماه اول رشـد جنین تعیین می‌شـود. اثر انگشـت‌های دوقلوها متفاوت است. امروزه هزینه اسـکنر اثر انگشـت ۲۰ دلار آمریکا است. دقت سامانه‌های تشخیص اثر انگشت موجود برای سـامانه‌های تأیید و سـامانه‌های شناسایی کوچک تا متوسط شامل چند صد کاربر، مناسـب اسـت. چند اثر انگشـت یک فرد، اطلاعات بیشـتری را فراهم آورده و امکان تشـخیص در مقیاس بزرگ شـامل میلیون‌ها هویت فردی را فراهم می‌کند. مشـکلی که سـامانه‌های فعلی تشـخیص اثر انگشـت دارد، این است که آنها مستلزم مقدار زیادی از منابع محاسـباتی اسـت، به‌خصوص زمانی که در حالت شناسایی عمل و کار می‌کند. در نهایت، اثر انگشـت بخش کوچکی از جمعیت به خاطر عوامل ژنتیکی و به دلایل سـنی، محیطی و یا شـغلی، ممکن اسـت برای شناسایی اتوماتیک مناسب نباشد (مثلاً کارگران ممکن اسـت بریدگی‌ها و کوفتگی‌های زیادی روی اثر انگشـت داشـته باشند که به تغییر ادامه می‌دهد).

1. Non-Intrusive

۵. **عنبیه**: عنبیه، منطقه حلقه‌ای چشـــم اســـت که مردمک و سفیده چشم آن را در برگرفته‌اند. بافت عنبیه در زمان رشد جنین تشکیل شده و در دو سال اول حیات ثابت می‌شود. بافت پیچیده عنبیه، اطلاعات خیلی متمایز و مفیدی را برای تشـــخیص فرد در بردارد. صحت و سرعت سامانه‌های تشخیص مبتنی بر عنبیه بسیار امیدوار کننده است. هر عنبیه متمایز و مشخص بوده و همچنین عنبیه‌های دوقلوها نیز متفاوت است. علاوه بر این، شناسایی عنبیه‌های مصنوعی تا اندازه‌ای ســـاده اســـت. اگرچه سامانه‌های اولیه تشخیص مبتنی بر عنبیه مســـتلزم حضور قابل ملاحظه کاربر بودند و اما ســـامانه‌های جدید ثمربخش شده و با کاربر صمیمی و خوب است.

۶. **ضربه کلید**: هر فرد به روشـــی مشـــخص روی صفحه کلید تایپ می‌کند. انتظار نمی‌رود کـــه این بیومتریک رفتاری منحصر به‌فرد باشـــد، امـــا اطلاعاتی را برای تأیید هویت ارائه می‌دهد.

۷. **اثر کف دست**: کف دست‌های انسان مانند اثر انگشت، شامل الگویی از برآمدگی و فرو رفتگی‌ها اســـت. منطقه کف دســـت، بزرگتر از منطقه انگشت بوده و در نتیجه کف دست، حتی متمایزتر از اثر انگشـــتان اســـت. به خاطر این که اســـکن‌های کف دست نیاز دارد تا منطقه بزرگی را پویش کند، بزرگتر بوده و پرهزینه تر از اسکن‌های اثر انگشت است. کف دست انسان نیز دربردارنده مشخصه‌های دیگری است، مانند خطوط اصلی و چین‌هایی که می‌توان با اســـکنری با رزولوشـــن پایین‌تر ثبت کرد که ارزان‌تر خواهد بود. بالاخره، به هنگام استفاده از اسکنر کف دست با رزولوشن بالا، تمام مشخصه‌های کف دست مانند هندسه دست، برآمدگی و فرورفتگی، خطوط اصلی و چین و چروک‌ها را می‌توان ترکیب کرده و سامانه بیومتریک دقیقی را درست کرد.

۸. **اسکن شبکیه**: سامانه عروقی شبکیه‌ای دارای ساختاری غنی بوده و یکی از ویژگی‌های هر فرد و هر چشم است. گفته می‌شود که ایمن‌ترین شاخص بیومتریک است. زیرا تغییر و تکرار سامانه عروقی شبکیه‌ای آسان نیست. اسکن شبکیه نیازمند همکاری خود فرد است. از طرفی سامانه عروقی شبکیه‌ای می‌تواند برخی از شرایط پزشکی مانند فشار خون را نمایان

سازد. مجموعه این عوامل مانع از پذیرش عمومی این بیومتریک می‌شود.

۹. صدا: ترکیبی از بیومتریک‌های فیزیولوژیکی و رفتاری است. ویژگی‌های فیزیولوژیکی کلام انسان مانند نوع تار صوتی در مورد یک فرد تغییری نمی کند، اما بخش رفتاری به مرور زمان و به واسطه سن و شرایط پزشکی تغییر کرده و ممکن است برای شناسایی در مقیاس بزرگ مناسب نباشد. سامانه‌های تشخیص صدا وابسته به متن براساس ادای عبارت ثابت و از پیش تعیین شده است. طراحی سامانه تشخیص مبتنی بر صدا مشکل‌تر از سامانه وابسته به متن است. عیب و نقص تشخیص مبتنی بر صدا این است که مشخصه‌های کلامی به برخی از عوامل مانند نویز پس زمینه حساس است.

مقایسه چند مشخصه بیومتریک براساس هفت عامل مهم در توصیف مشخصه‌های بیومتریک در جدول زیر آمده است.

جدول ۱: مقایسه تکنولوژی‌های متنوع

مشخصه بیومتریک	آسیب پذیری	قابلیت پذیرش	عملکرد	قابلیت جمع آوری	دوام	تمایز	جهانی بودن
DNA	L	L	H	L	H	H	H
گوش	M	H	M	M	H	M	M
چهره	H	H	L	H	M	L	H
دما نگار	L	H	M	H	L	H	H
اثرانگشت	M	M	H	M	H	H	M
کف دست	M	M	M	H	M	M	M
عنبیه	L	L	H	M	H	H	H
ضربه کلید	M	M	L	M	L	L	L
بو	L	M	L	L	H	H	H
شبکیه	L	L	H	L	M	H	H
امضا	H	H	L	H	L	L	L
صدا	H	H	L	M	L	L	M

کاربرد سامانه‌های بیومتریک

کاربرد سامانه‌های بیومتریک را می‌توان به صورت زیر طبقه‌بندی کرد:[۶].

۱- کاربردهای تجاری مانند ورود به شبکه کامپیوتری، تجارت الکترونیک، کارت اعتباری، کنترل دسترسی فیزیکی.

۲- کاربردهای دولتی مانند کارت شناسایی ملی، گواهینامه رانندگی و کنترل پاسپورت.

۳- کاربردهای پزشک قانونی مانند شناسایی جسد، بررسی جرم، شناسایی تروریست.

پیش از این در کاربردهای تجاری از سامانه‌های دانش‌مدار (PIN یا کلمه عبور)، درکاربردهای دولتی از سامانه‌های نشانه‌مدار (کارت شناسایی) و در کاربردهای پزشکی قانونی از مشخصه‌های بیومتریک استفاده می‌شده است. سامانه‌های بیومتریک در کاربردهای داخلی گسترش یافته است.

جدول۲: مثال‌هایی از کاربردهای بیومتریک

سامانه تأیید اثر انگشت که توسط شرکت Digital Persona ساخته شده و برای ورود به کامپیوتر و شبکه استفاده می‌شود.

POS مبتنی بر اثر انگشت که مشتریان را قبل از تأیید کارت‌های اعتباری تأیید می‌کند.

قفل در مبتنی بر اثر انگشت، ساخته شرکت Bio Thentica Corporation برای محدود کردن دسترسی فیزیکی استفاده می‌شود.

سامانه خدمات تسریع یافته سرویس مهاجرت و قبول تابعیت (INSPASS)

سامانه FacePass از Viisage در کاربردهای تأیید POS استفاده می‌شود.

پذیرش اجتماعی

عوامل انسانی تا حد زیادی موفقیت سامانه شناسایی بیومتریک را تحمیل می‌کند. سهولت و راحتی در تعامل با سامانه بیومتریک در پذیرش آن دخالت دارد. برای مثال، اگر یک سامانه بیومتریک بتواند ویژگی یک فرد را بدون تماس اندازه‌گیری کند، مانند استفاده از چهره، صدا

یـا عنبیـه می‌توان آن را قابل قبول تلقی کرد. ویژگی‌های بیومتریک که مسـتلزم دخالت کاربر است توسط بسیاری از افراد به عنوان تهدید تلقی می‌شود.

فرآیند تشـخیص، مجموعه‌ای از اطلاعات مربوط به خصوصی بودن را به دنبال می‌کشـد. برای مثال اگر شخصی هر بار هنگام خرید شناسایی شود، اطلاعات مربوط به این که این فرد از کجا خرید می‌کند و چه چیزی می‌خرد، می‌تواند به وسیله بازاریاب‌ها جمع‌آوری و استفاده شـود. خصوصی بودن در سـامانه‌های تشخیص بیومتریک جدی‌تر می‌شود. زیرا ویژگی‌های بیومتریک می‌تواند اطلاعات بیشتری را درباره پس زمینه و سابقه یک فرد فراهم کند.

در نگاهـی مثبت، سـامانه‌های بیومتریـک را می‌توان به عنوان یکـی از مؤثرترین ابزار ها برای حفاظت از حریم خصوصی اسـتفاده کرد. در واقع این سـامانه‌ها با نگهبانی از هویت و یکپارچگی حریم خصوصی را امن می‌کند. برای مثال اگر فردی کارت اعتباری‌اش را گم کرده و یـک بیگانه آن را پیدا کند، سـابقه اعتباری این فرد بـه خطر می‌افتد، اما اگر کارت اعتباری را بتوان فقط زمانی اسـتفاده کرد که کاربر توسـط ویژگی بیومتریک خود شناسایی شود، کاربر در برابر این تهدید محافظت می‌شـود. شـاخص‌های بیومتریک را نیز می‌توان برای محدود کردن دسترسی به اطلاعات شخصی استفاده کرد. برای مثال سامانه بیومتریکی اطلاعات بیمار می‌تواند به طور قابل اعتمادی اطمینان دهد که دسترسـی به سـوابق پزشکی فقط در دسترس بیمار و پرسـنل پزشـکی مجاز قرار می‌گیرد. با این وجود بسـیاری از افراد، درباره استفاده از ویژگی‌های بیولوژیکی خصوصی‌شـان در سامانه‌های تشخیص هویت ناراضی هستند. برای کاهش ترس و استرس شرکت‌ها و آژانس‌هایی که سامانه‌های بیومتریک را به کار می‌برند، باید کاربران این سامانه را مطمئن ساخت که اطلاعات بیومتریک محرمانه آنها محفوظ می‌ماند و فقط برای هدفی که جمع‌آوری شده استفاده می‌شود. تدوین مقررات برای اطمینان از این که این اطلاعات خصوصی مانده و سوءاستفاده از آنها جرم دارد، لازم است[۷].

بیشتر سامانه‌های بیومتریک تجاری که امروزه در دسترس است، ویژگی فیزیکی را به شکل اصلـی ذخیـره نکرده و بازنمایی دیجیتالی را به فرم رمز ذخیره می‌کند. این کار برای دو هدف انجـام می‌شـود. اولاً ویژگی‌هـای فیزیکی دقیق را نمی‌توان از الگـوی دیجیتال بازیابی کرد،

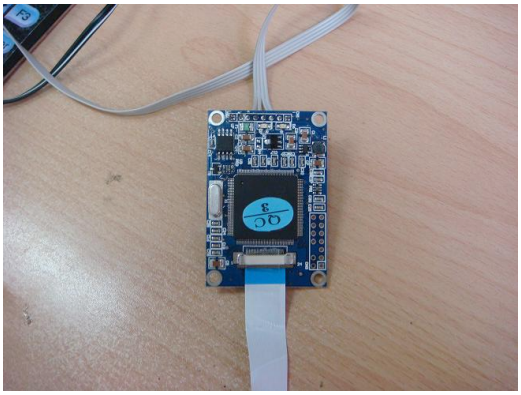
بنابراین حریم خصوصی را امن می‌کند. دوم آن که رمزدار کردن اطمینان می‌دهد که فقط کاربر معرفی شده می‌تواند از الگو استفاده کند.

ساخت سیستم بیومتریک اثر انگشت

در بین این انواع سامانه‌های بیومتریک، امروزه اثر انگشت کاربرد و جایگاه ویژه ای پیدا کرده است. دلایل متعددی برای کاربرد زیاد آنها وجود دارد. از جمله آنها می‌توان به هزینه پایین حسگرها و خطوط اثر انگشت اشاره کرد. همچنین تنوع حسگرهای اثر انگشت از جمله حسگرهای نوری، خازنی و... دلیل دیگری بر این امر است. شاید امروز از دیگر پارامترهای بیومتریک مانند صدا و عنبیه چشم استفاده‌های زیادی شود، اما می‌توان گفت که اثر انگشت اولین نمونه مشخصه بیومتریک هست که به صورت جدی مورد توجه قرار گرفت و در صنعت به‌کار گرفته شد. به همین دلیل حسگرها و خطوط اثر انگشت را می‌توان به راحتی و در مقادیر زیاد به‌دست آورد. در این پروژه نیز به دلیل در دسترس بودن حسگرها و خطوط اثر انگشت یک سامانه اثر انگشت به عنوان نمونه‌ای از سامانه‌های بیومتریک ساخته شده است. ماژول مورد استفاده در این سامانه SM۶۲۱ است و توسط برنامه رایانه کنترل می‌شود. وصل بودن به رایانه توانایی کار کردن تحت شبکه‌ها را فراهم می‌آورد و قابلیت‌های فراوانی را برای سامانه‌های امنیتی به ارمغان می‌آورد. به عنوان نمونه می‌توان به امکان بررسی و تأیید هویت کاربران با یک پایگاه داده مرکزی اشاره کرد. امروزه در پیاده‌سازی سیستم‌های امنیتی تلاش برای متمرکز کردن کلیه امور از جمله تعیین هویت کاربران است.

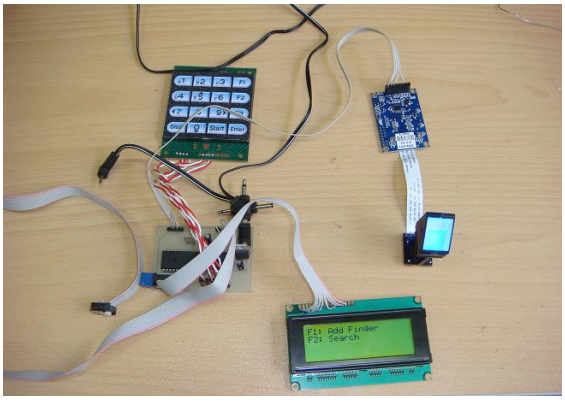
شکل۳: حسگر SM-6X

شکل۴: عمل تحت نظارت میکروکنترلر

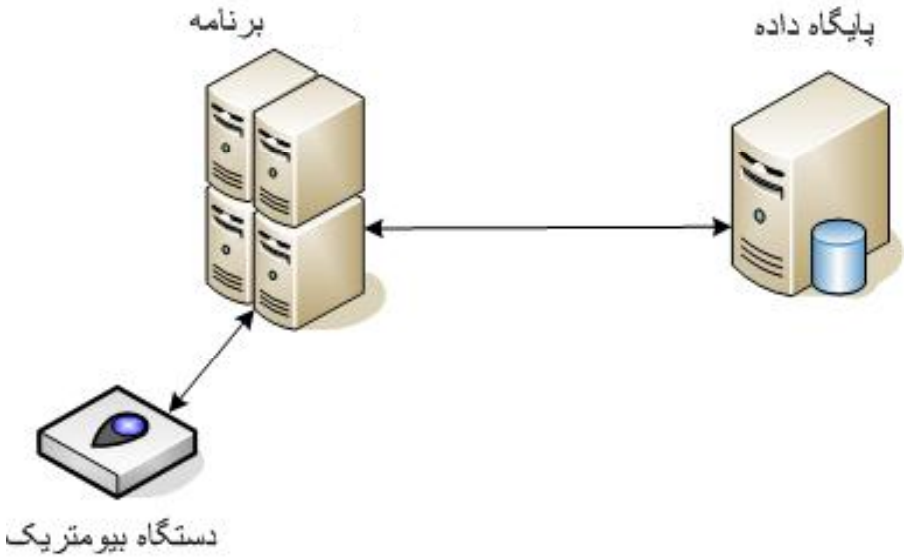


شکل۵: ماژول متصل

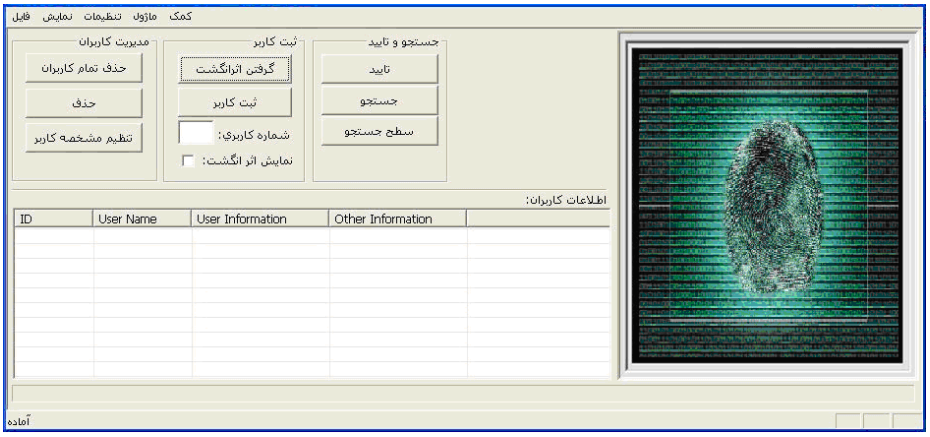
ماژول دارای ارتباط سـریال اسـت، اما به علت مزیت‌های فراوان ارتباط USB از یک مدار برای تبدیل ارتباط سـریال به USB اسـتفاده شـده تا به این وسـیله عمل نصب ماژول بـه رایانه آسـان شـود. برای این منظـور تبدیل (تبدیل ارتبـاط RS ۲۳۲ به USB) از قطعه ۲۳۲FT و از قطعه Max ۲۳۲ برای تنظیم سطح ولتاژ استفاده شده است. برنامه نوشته شده برای رایانه با خواندن و نوشـتن بر روی درگاه سـریال به مدیریت کاربران و تأیید هویت آنها می‌پردازد[۸].



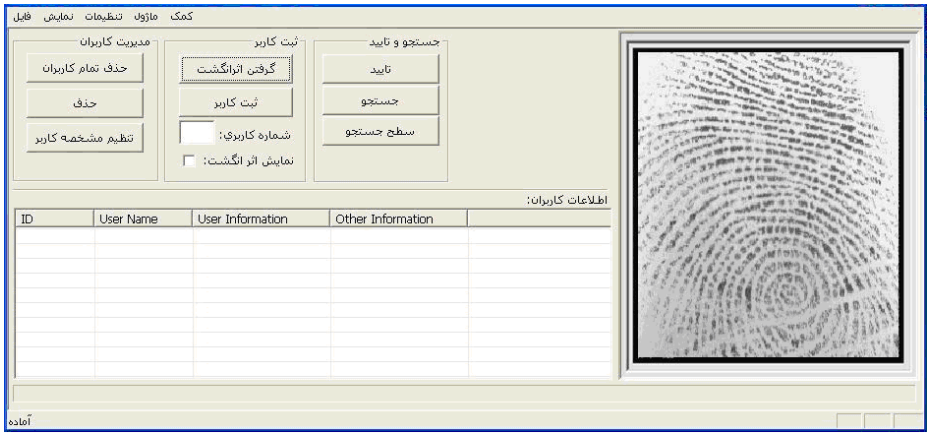
شکل۶: عمل تحت نظارت میکروکنترلر



شکل۷: نحوه عملکرد نرم افزار

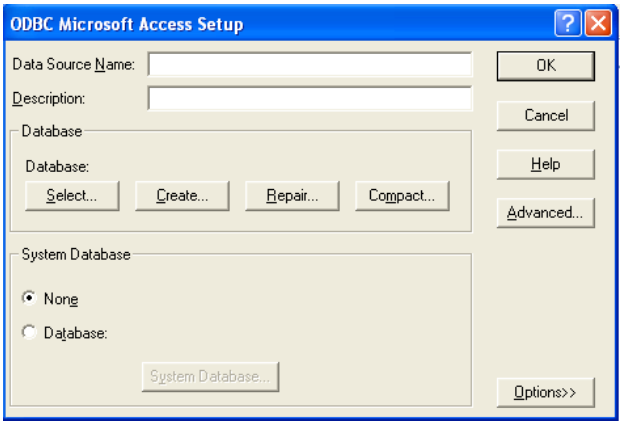


شکل ۸: نرم‌افزار مدیریت سامانه

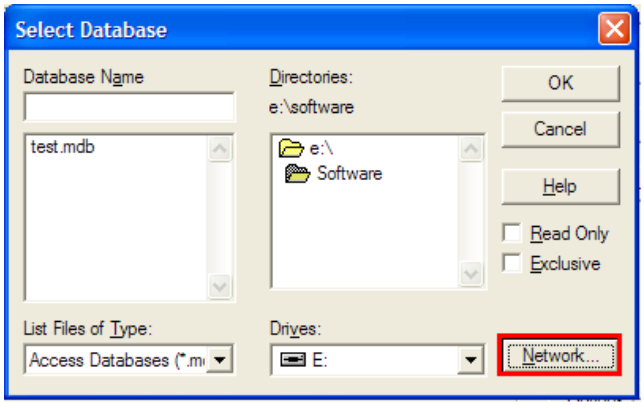


شکل ۹: نمونه‌ای از اجرا نرم‌افزار مدیریت سامانه

کنترل این ماژول توسط رایانه این قابلیت را به‌وجود می‌آورد که از قابلیت‌های آن در شبکه کامپیوتری بتوان استفاده کرد. در سامانه‌ها و شبکه‌های واقعی اطلاعات مربوط به کاربرانی که اجازه دسترسی به منابع را دارند به صورت متمرکز در یک پایگاه داده قرار دارد و دستگاه‌های مربوط به کنترل دسترسی به منابع در مکان دیگری قرار می‌گیرد. برای حفظ یکپارچگی و متمرکز نگه داشتن مکانیسم امنیتی اطلاعاتی که ازطریق دستگاه‌های احراز هویت مانند حسگرهای بیومتریک یا پایانه‌های کارت اعتباری به‌دست می‌آیند، باید با اطلاعات پایگاه داده مرکزی تطبیق داده شود. برای پیاده‌سازی این امر در این پروژه، نرم‌افزار قابلیت کارتحت شبکه را دارد. شکل ۱۰ و ۱۱ نحوه عملکرد این نرم‌افزار را نشان می‌دهد.



شکل ۱۰: امکانات نرم افزار برای اجرا در شبکه



شکل ۱۱: امکانات نرم‌افزار برای اجرا در شبکه

نتیجه‌گیری:

در میان مجموعه سخت‌افزارهای امنیتی ارائه شده تاکنون، استفاده از شاخص‌های بیومتریک به عنوان بهترین تکنولوژی امنیتی قرن آینده شناخته شده و همراه با گسترش کاربردهای فناوری اطلاعات در حال توسعه است. بیشتر کشورهای جهان استفاده از شاخص‌های بیومتریک را در شناسایی جزء تکنولوژی‌های برتر در نظر گرفته و به صورت ویژه استفاده از

آن را در پاسپورت اجباری کرده‌اند.

بیومتری می‌تواند مستقیماً در زمینه کاربردهای فناوری اطلاعات مانند تجارت الکترونیکی و دولت الکترونیکی که نیازمند به امنیت بیشتری است، مستقیماً مورد استفاده شهروندان قرار گرفته و پلیس آگاهی نیز می‌تواند با دسترسی به اطلاعات حاصل از آن زمینه امنیت بیشتر را فراهم کند. در این مقاله ضمن معرفی مشخصه‌های بیومتری، به بیان کاربرد و جایگاه آنها در سامانه‌های امنیتی پرداخته شد و به صورت ویژه یک طرح پیاده‌سازی شده مرتبط با انگشت نگاری در دانشگاه علم و صنعت ایران معرفی شد.

فهرست منابع:

[1] A. K. Jain, A. Ross, S. Prabhakav, **"An Introduction to Biometric Recognition"**, IEEE transaction on circuits and systems for video technology vol14, No1, 2004.

[2] A. Stoianov, A. Cavonkian, **"Biometric Encryption, a positive-sum technology that achieves strong authentication, security and privacy",** 2007

[۳] شهرام بختیاری، سعید قاضی مغربی، **"اصول امنیت سامانه ها وشبکه های رایانه ای"**، موسسه انتشارات علمی دانشگاه صنعتی شریف ۱۳۸۵.

[۴] احسان ملکیان، **"نفوذگری درشبکه و روشهای مقابله"**، انتشارات نص ۱۳۸۵.

[5] D.Maltoni, D.Maio, A.K.Jain, Handbook of Fingerprint Recognition, New York: Springer-Verlag, 2006.

[6] S. Prabhakar, S. Pankanti, A. K. Jain, **"Biometric Recognition: Security and Privacy Concerns"**, IEEE Security and Privacy Magazine, Vol. 1, No. 2, 2003.

[7] J. Dangman, **"Biometric Decision Landscapes",** University of Cambridge-Technical Report, 2005.

[۸] مزدک رجبی نسب، علی‌اکبر جلالی، ''بررسی سیستم‌های بیومتریک و ساخت یک سیستم بیومتریک نمونه''، پایان‌نامه تحصیلی کارشناسی، دانشکده برق دانشگاه علم و صنعت ایران، ۱۳۸۷