مقایسه بین روش های تشخیص هویت افراد به کمک تکنیک های بیومتریک

حسین اثباتی ، آتنا عباس زاده
کارشناس ارشد مهندسی برق کنترل، شرکت صنایع سیمان زابل ، hosseinesbati1@gmail.com
کارشناس ارشد مهندسی برق کنترل، شرکت صنایع سیمان زابل atena.abbaszadeh@gmail.com
مسئول مکاتبات: حسین اثباتی

چکیده – هر کدام از روش های تشخیص هویت بیومتریک دارای نقاط ضعف و قدرتی هستند که با ترکیب آن ها با دیگر روش های امنیتی می توان ضعف های موجود را از بین برد . امروزه تعیین هویت قطعی افراد در مبادله اطلاعات یک عنصر حیاتی در ایمنی داده ها است . بنابراین روش های مختلفی برای تعیین هویت افراد وجود دارد از این روش‌ها نه تنها برای تامین امنیت سیستم‌های کامپیوتری بلکه برای افزایش ایمنی شرکت‌ها و مکان‌ها نیز استفاده می‌شود . امروزه در امور مربوط به امنیت اماکنی مانند دانشگاه ها، فرودگاه ها، وزارتخانه ها و حتی شبکه‌های کامپیوتری استفاده از روش های بیومتریک در تشخیص هویت یا تایید هویت افراد بسیار متداول شده است .سیستم‌های پیشرفته حضور و غیاب ادارات ، سیستم‌های محافظتی ورود خروج اماکن خاص ، نوت‌بوک‌های مجهز به finger print و... از دیگر نمونه هایی است که در آن از روش‌های مختلف تشخیص هویت بیومتریک استفاده می‌شود . به این ترتیب سیستم‌های بیومتریک با ارائه کار کرد بهتر، هزینه‌های بالاتر خود را جبران می‌کنند.

کلید واژه– تشخیص هویت بیومتریک، تایید هویت، تشخیص چهره.

۱- مقدمه

بیومتریک عبارت است از استفاده اتوماتیک یا نیمه اتوماتیک از ویژگی های فیزیولوژیک یا ویژگی های رفتاری که به بدن انسان بستگی دارند برای تشخیص یا تایید هویت فرد است . درمورد مشکلات روش های قدیمی که از شماره رمز عبور به جای سامانه بیومتریک استفاده می کنند مثل سامانه های کارت خودپرداز بانکی ، وقتی فرد می خواهد از کارت خود استفاده کند لازم است شماره تشخیص هویت شخصی خود را وارد کند، در این سامانه تایید یا تشخیص هویت برمبنای چیزی که شخص به همراه دارد (کارت) که این یک مشکل بالقوه در این سیستم است زیرا کارت ممکن است دزدیده شود و شماره رمز را هم فرد دیگری می تواند با خود داشته باشد . در حالی که در سامانه های بیومتریک این مشکلات وجود ندارند و امکان تقلب در آن ها خیلی کم است و می توانند به عنوان سامانه های ایده آل تشخیص هویت مورد استفاده قرار گیرند. در این سیستم ها، ویژگی بیومتریک فرد توسط دستگاه گرفته شده و کد آن استخراج می شود . سپس با کدهای ذخیره شده در پایگاه داده ها مقایسه می شود و درصورتی که فرد مورد نظر شناسایی شود دستگاه ، اپراتور را آگاه می کند . برای شناسایی معمولا یک انسان نیز در چرخه شناسایی وجود دارد که تصمیم نهایی را می گیرد. در کاربردهای عملی، کارایی سیستم عبارت است از تعادل بین درصد تشخیص دادن به اشتباه (FAR) و نرخ تشخیص ندادن به اشتباه (FRR) . که FRR عبارت است از تعداد افرادی که اشتباه تشخیص داده شده اند و FAR برابر با تعداد افرادی است که در پایگاه داده وجود دارد ولی تایید هویت نشده اند. یک سامانه بیومتریک شامل یک مرحله پیش ثبت نام است و بیومتریک شخص پس از این مرحله می تواند به دفعات توسط سامانه تایید هویت شود . در سامانه هایی که از خصوصیات رفتاری شخص استفاده می کنند ، این ویژگی ها نباید نسبت به تغییرات حساس باشند . این تغییرات می توانند سلامتی فرد یا حالت روحی فرد در طول زمان باشد.

۲- اصول کلی تشخیص هویت بیومتریک[1]

کلمه بیومتریک از ترکیب دو کلمه یونانیbios به معنای زندگی و کلمه metrikos به معنای تخمین تشکیل شده است و با عنوان زیست سنج معرفی می شود. سامانه های بیومتریک دارای دو خصوصیت بسیار مهم هستند که قابلیت اطمینان آن ها را بالا می برند و عبارتنداز اینکه :

الف- شخص که می خواهد تایید هویت شود، باید شخصا در هنگام فرایند حضور داشته باشد.

ب- تشخیص هویت نیازی ندارد که شخص اطلاعاتی را حفظ و یا یادآوری کند یا اینکه چیزی را با خود همراه داشته باشد.

یک سیستم بیومتری اساسا یک سیستم تشخیص الگو است که یک شخص را بر اساس بردار ویژگی های خاص، فیزیولوژیک خاص، یا رفتاری که دارد بازشناسی می کند . بردار ویژگی ها پس از استخراج معمولا در پایگاه داده ذخیره می شود . سیستم‌های بیومتریک باید با درصد قابل توجهی قابل اعتماد باشند تا سیستم در تشخیص افراد و اجازه دسترسی آنها اشتباه نکند. یک شناسه بیو متریک خوب که می تواند به عنوان ویژگی در سامانه بیومتریک مورد استفاده قرار گیرد، باید خصوصیاتی همچون منحصر به فرد بودن، استخراج پذیری، قابلیت تفکیک پذیری بالا و پایداری را داشته باشد.

یک سیستم بیومتریک شامل ۴ بخش بنیادی است:

- **بلوک سنسور**[2]: قسمت نمونه برداری که اطلاعات خام مورد نیاز را جمع آوری میکند(مانند تصویر اثر انگشت).
- **بلوک استخراج ویژگی ها**[3]: قسمت پردازش برای استخراج ویژگی ها از اطلاعات مرحله قبل.
- **بلوک مقایسه**[4]: قسمت مطابقت که بررسی می کند آیا اطلاعات جمع آوری شدهبا اطلاعات الگو مطابقت می کند یا خیر؟
- **بلوک تصمیم**[5]: قسمتی که اطلاعات ورودی (ویژگی ها) را با اطلاعات ذخیره شده مقایسه می کند و اگرشباهت از درصد معلومی بالاتر بود به فرد اجازه دسترسیمی دهد در غیر اینصورت پیغام خطا می دهد [۶]

خصیصه هایی که به منظور بیومتریک استفاده می شوند باید دارای ۴ ویژگی زیر باشند :

- **Universality** : تمامی افراد داشته باشند.
- **Distinctiveness** : در دو فرد مشابه نباشد.
- **Permanence** : در طول زمان تغییر نیابد.
- **Collectability** : قابل جمع آوری باشد.

۳- متدهای امروزی در بیومتریک

در این قسمت متدهای متداول و غیر متداول بیومتریک را معرفی خواهیم کردو تنها به بیان مزایا و معایب هر روش می پردازیم . لازم به توضیح است که از بیومتریک در دو فیلد مجزا می توان استفاده کرد :

۳-۱- تشخیص هویت[6]

در این فیلد سعی می شود که هویت شخص دقیقا مشخص گردد . شناسایی شامل مقایسه اطلاعات کسب شده در قالب خاصی با تمام کاربران در پایگاه داده است. مرحله تشخیص هویت یک جستجوی یک در چند است و بدین صورت است که سامانه ابتدا باید مشخص کند که ایا فرد در بانک اطلاعاتی موجود است یا نه و در صورت وجود فرد در بانک اطلاعاتی مشخص کند که این مشخصات شناسایی شده چه کسی است؟

---

[1] Biometric Methods

[2] Sensor Module

[3] **Module Feature Fxtraction**

[4] **MatchingModule**

[5] **Decision-Making Module**

[6] Identification

۳-۲- تایید هویت[۷]

در این فیلد بررسی می کنند که آیا فرد مطابق با هویت ادعا شده هست یا خیر، تایید فقط شامل مقایسه با یک قالب خاصی که ادعا شده است خواهد بود؟ در مرحله تایید هویت که یک مقایسه یک به یک است سامانه کد ورودی را با کد موجود و ادعا شده مقایسه می کند و بررسی میکند که آیا تشخیص هویت داده شده درست است یا نه. در بیشتر سامانه های بیو متریک مرحله ثبت نام در سامانه از مرحله تشخیص هویت جدا شده است . زیرا در مرحله ثبت نام باید مساله اینکه آیا فرد قبلا در سامانه ثبت نام کرده است یا نه مد نظر قرار گیرد تا از ثبت نام یک نفر در سامانه با چند هویت مختلف جلوگیری شود و قابلیت اطمینان سامانه بالا رود در حالی که در مرحله تشخیص هویت مساله مهم فقط یافتن فرد از بین کدهای ذخیره شده در پایگاه داده است . سیستم هایی که قادر به تشخیص هویت هستند، حتما می توانند تایید هویت را انجام دهند ولی بر عکس آن قطعی نیست.

۴- انواع تکنولوژی بیومتریک

تکنولوژی بیومتریک به دو دسته کلی تقسیم می شود :

* تکنیک های بیومتریک فیزیولوژیک :اثر انگشت، اثر کف دست و پا، اسکن عنبیه، اسکن یا هندسه دست و انگشت، اسکن صورت، اسکن صدا و اسکن شبکیه، اثر شیمیایی بو، طیف الکترومغناطیسی پوست، ناخن، کارتهای شناسایی بیومتزیک، DNA، نمایشگر دمای نقاط بدن، شناسایی از روی تپش‌های قلب.
* تکنیک های بیومتریک رفتاری : اسکن صورت یا تحلیل گفتار، طرز حرکت، چگونگی کار با کیبورد، حرکات لب، ورید و رگها، دست خط و امضای دستی وتشخیص چهره .

۴-۱- تشخیص هویت با اثر انگشت

به برآمدگی ها و فرورفتگی های موجود در پوست نوک انگشت اثر انگشت گویند . خطوطی که بر روی سر انگشتان همه انسان ها نقش بسته ازدیرباز مورد توجه همه بوده است ، این خطوط نقش های مختلفی دارند ، یکی از آن موارد ایجاد اصطکاک بین سر انگشتان و اشیاء متفاوت است مانند قلم که با استفاده از این اصطکاک می توان اشیاء را برداشت ، نوشت و یا لمس کرد . روش های شناسایی اثر انگشت یکی از جالب توجه ترین و متداول ترین متد مورد استفاده در بیومتریک و در عین ارزانی یکی از مطمئن ترین روش های تشخیص هویت است . این روش چیزی جز اثر پستی و بلندی های نوک انگشت هر فرد نیست . تکنیک های شناسایی اثر انگشت اطمینان و ثبات در تشخیص هویت را تضمین می کنند و بدین ترتیب در کاربردهای مختلف مورد استفاده قرار می گیرند . از طرف دیگر مشکلات عملی زیادی در سیستم های شناسایی با اثر انگشت وجود دارد . هر دفعه که یک اثر انگشت گرفته می شود ممکن است به دلیل قابلیت کشسانی پوست ، تغیراتی در شکل و محل اثر انگشت ایجاد شود . علاوه بر این اطمینان بالا و پردازش بلادرنگ ،فاکتورهای مهم مورد نیاز در سیستم خودکار شناسایی با اثر انگشت هستند . برای حل این مشکلات استخراج دوشاخه ها از تصاویر اثر انگشت و کاربرد آن ها در تطبیق اثر انگشت مورد بررسی قرار می گیرد . سابقا اثر انگشت را توسط فشار دادن انگشت جوهری بر روی کاغذ بدست می آوردند . در این شیوه ابتدا سطح انگشت را به جوهر آغشته کرده و سپس روی کاغذ می غلتانند . برای وارد کردن تصویر به دست آمده به یک سیستم کامپیوتری از یک پویشگر تخت استفاده می شود . تصویر به دست آمده از این روش بسیار اعوجاج داشته و حتی در تشخیص به صورت دستی نیز نیازمند یک فرد خبره است ولی امروزه از نوک انگشت تصویری دیجیتالی تهیه می‌شود . برای تهیه تصویر دیجیتالی اثر انگشت از سه نوع اسکنر استفاده می‌شود : اسکنرهای نوری[۸] ، اسکنرهای اولتراسوند[۹] و اسکنرهای نیمه هادی[۱۰]. نوع سوم مقرون به صرفه ترین اسکنر امروزی است و در اکثر نوت بوک ها از این نوع اسکنر استفاده می شود . نوع اول در اثر تماس مکرر انگشت با سطح آن ها چرب و مات می شد و کارایی شان به شدت افت می‌کرد ولی در سنسورهای نوع سوم این مشکل وجود ندارد . از انواع مشابه این روش می توان به اثر کف دست[۱۱] و اثر کف پا [۱۲] نیز اشاره کرد.

[7] Verification

[8] optical

[9] ultrasound

[10] capacitors semiconductor

[11] Print Palm

[12] Foot print

۴-۲- تشخیص هویت با کف دست

مشابه تشخیص هویت با اثر انگشت، در اثر کف دست از الگوی خطوط و انحنا های موجود در دست فرد برای تشخیص هویت افراد استفاده می کنند . بر خلاف اثر انگشت از تصاویر کف دست می توان برای شناسایی افراد سالخورده و هم چنین کارگرانی که دارای اثر انگشت نا مناسب برای استفاده از بیومتریک اثر انگشت هستند استفاده کرد . این امر باعث می شود که این تکنولوژی برای کاربردهای امنیتی بسیار مناسب باشد زیرا افراد بیشتری می توانند در آن ثبت نام کنند . با وجود این که اثر کف دست برای بیش از ۱۰۰ سال مورد استفاده قرار گرفته است اما این روش هرگز برای تشخیص افراد در سیستم های اتوماتیک به کار نرفته است و فقط در مواردی از شکل دست و نه الگوی های موجود در آن استفاده شده است که نشان دهنده ناقص بودن تکنولوژی است . آزمایشات انجام شده روی اثر کف دست نشان می دهند که این روش دقیق است و امکان گمراه کردن آن وجود ندارد . از طرف دیگر مشخصات هندسی با روش بسیار ساده ای اندازه گیری می شوند به همین دلیل می توان به راحتی از یک دست غیر واقعی برای این کار استفاده کرد . این درجه از تفاوت دیدگاه ها نشان دهنده نامشخص بودن دقت بیومتریک اثر کف دست است. ابعاد کف دست بسیار بزرگتر از انگشت است در نتیجه انتظار می رود که اثر کف دست دقتی خیلی بیشتر از اثر انگشت داشته باشد و می توان نتیجه گرفت که دقت FRR در مورد بیومتریک اثر کف دست بیشتر از اثر انگشت است . در ضمن FAR نیز در این مورد بیشتر(بدتر) است چون این تکنولوژی امکان گمراه شدن زیادی دارد . برای کاربردهای امکان دسترسی ، اثر کف دست را می توان برای ثبت نام در سیستم تهیه کرد ، زیرا افراد از مراحل کارآگاه هستند همکاری می کنند . ولی برای جستجو ی افراد تقریبا غیر ممکن است که بتوان اثر انگشت یک تروریست را تهیه کرده در سیستم ثبت کرد . به علاوه از نظر عملی کار سختی است که از کف دست افراد بدون همکاری آن ها تصویر برداری کرد . بنابراین اثر کف دست برای کاربردهای امنیتی مناسب نیست.

شکل ۱- اثر کف دست و کف پا

۴-۳- تشخیص هویت با ژئومتری دست (هندسه دست)

در تشخیص هویت از روی ژئومتری دست از یک دوربین CCD برای ثبت نقاط کلیدی دست استفاده می‌شود. در این روش تصاویر دست از بالا و از کنار به دست آمده و مورد پردازش قرار می‌گیرد . در طی این پردازش، نقاط وخطهایی روی تصویر فرض می‌شود . از این نقاط و خطوط برای اندازه‌گیری طول ، پهنا و ضخامت هر یک از انگشت‌ها استفاده می‌شود . سپس سیستم تشخیص هویت این داده‌ها را در یک بانک اطلاعاتی ذخیره می‌کند تا بعداً داده‌های ورودی برای شناسایی شخص با آنها مقایسه شود روش هندسه دست نسبت به کثیف بودن دست فرد حساس نیست و بنابراین روش مناسبی برای کارگران است . یکی دیگر از مزایای این روش مستقل بودن آن از پلیس و مسائل جنایی است که باعث می شود افراد زیادی تمایل به ثبت نام در چنین سیستمی داشته باشند و بنابراین برای کاربردهای کنترل دسترسی مناسب است .ادعا می شود که از تصویر دست نمی توان در جستجوی یک نفر از بین چند نفر استفاده کرد و فقط به تایید هویت یک فرد خاص محدود می شود که باعث ناکار آمدی در کاربردها جستجو می شود . علت این امر کاملا روشن نیست ولی به هر حال می توان نتیجه گرفت که هندسه دست نیز دارای معایب روش های قبل است یعنی عدم قابلیت.

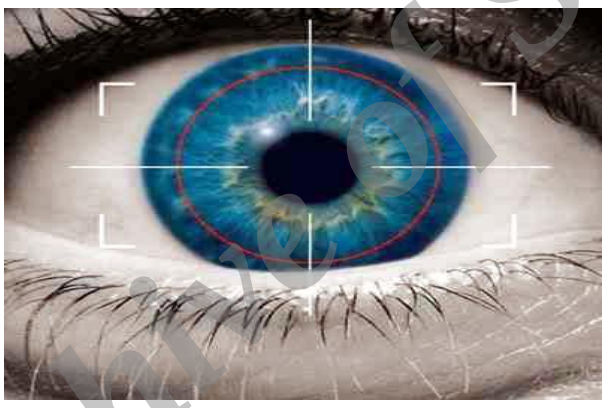
۴-۴- تشخیص هویت با استفاده از شیمیایی بو

نوع متفاوتی از بیومتریک ها ، تکنولوژی شیمیایی است که به بو نیز معروف است . بوی بدن انسان از حدود سی ماده شیمیایی مختلف تشکیل شده که میزان وجود این مواد یا عدم وجودشان یک بوی منحصر به فردی را در افراد به وجود می آورد . می توان این مواد شیمیایی را شناسایی کرده و از نتایج بررسی آنها به یک بیومتریک شناسایی دست پیدا کرد . کامل و جامع بودن این تکنولوژی مورد تردید است . مطالعات انجام شده در این زمینه نشان می دهد که تکنولوژی در ابتدای راه خود است . حتی اگر این روش ، روش مطمئنی برای شناسایی باشد ، این تکنولوژی نیازمند آنالیز شیمیایی پیچیده و زمان بری است که باعث مشکل شدن استفاده از آن در دنیای واقعی می شود . قابلیت اطمینان بو به معنای یک بیومتریک نا شناخته است همچنین انعطاف پذیری و منحصر به فرد بودن و قابلیت به کار رفتن به عنوان بیومتریک برای بو به عنوان مسائل ناشناخته مطرح می شود . به علاوه می توان نتیجه گرفت که

پیچیدگی و زمان بر بودن روش بیان می کند که این بیومتریک در کاربردهای بر خط قابل استفاده نیست و بنابراین برای جستجوی افراد مناسب نیست.معایب این روش شامل ناپایداری بودن ترکیبات شیمیایی در نتیجه تغییرات هورمونی و احساسی است . رژیم غذایی نیز باعث تغییر در این ترکیبات می شود . با توجه به مسائل بررسی شده نتیجه می شود علارغم اینکه ممکن است این روش در آینده مورد استفاده قرار گیرد ، نواقص موجود در این تکنولوژی باعث نامناسب بودن آن برای کاربردهای جستجو می شود .

۴-۵- تشخیص هویت با عنبیه چشم

در سال ۱۹۳۶ چشم پزشکی به نام frank burch پیشنهاد تشخیص افراد از طریق الگوی قرنیه را عنوان کرد . اما تا سال ۱۹۸۵ بود که توسط دو چشم پزشک به نام های Leonard flom و aran safir این مطلب بیان شد که قرنیه های افراد مختلف کاملا متفاوت است و در سال ۱۹۸۷ موضوع تشخیص هویت از طریق قرنیه افراد به نام آنها ثبت شد . درسال ۱۹۹۳ سازمان دفاع هسته ای برای ساخت و آزمایش اولین دستگاه تشخیص هویت از طریق الگوی قرنیه آغاز به کار کرد که این طرح در ۱۹۹۵ کاملا موفقیت آمیز به انجام رسید. امروزه نیاز به وسایل قابل ساختار شکل گیری عنبیه از ماه سوم جنین آغاز و تا ماه هشتم کاملا تثبیت می گردد . ظاهر و ساختار[۱۳] پیچیده عنبیه به ما این امکان را می دهد تا ویژگی های قابل قیاس زیادی از آن استخراج کنیم . تصویربرداری از سطح عنبیه کار چندان سختی نیست ولی نکات دردسر سازی دارد . مثلا اگر نور محیط تغییر کرده باشد و یا زاویه چرخش چشم مناسب نباشد و همچنین اگر کنتراست، رزولوشن و فوکوس تصویر تغییر کرده باشد، امکان خطا بسیار بالا می رود . این روش توانایی تشخیص هویت را نیز دارد .



شکل ۲ – تصویر برداری از عنبیه

۴-۶- تشخیص هویت با استفاده طرز حرکت[۱۴]

روش های زیادی برای تشخیص هویت افراد از روی راه رفتن در تصاویر ویدیویی ارائه شده اند که می توان آن ها را به دو دسته کلی طبقه بندی کرد رهیافت های آماری و رهیافت های مبتنی بر مدل. رهیافت های ارائه شده شامل سه فاز کلی هستند : پیش پردازش، استخراج ویژگی، تشخیص.

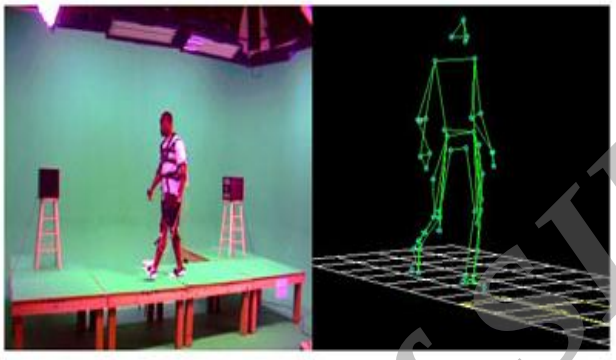
بررسی این رهیافت ها نشان می دهد که در فاز پیش پردازش معمولا یک الگوریتم حذف زمینه ساده صورت می پذیرد و تا کنون کار جدی در این فاز صورت نگرفته است . در روشی برای تشخیص هویت افراد از روی راه رفتن از پیش پردازش به منظور تخمین دقیق پس زمینه و برای آشکار سازی شی ء از رهیافت جدید مبتنی بر مجموعه های فازی و در فاز تشخیص نیز یک الگوریتم جدید بر مبنای انحراف زمانی دینامیک[۱۵] (dtw) استفاده شده است . روش dtw یک تکنیک مبتنی بر برنامه نویسی پویا جهت نرمال سازی غیر خطی زمان است. در این روش فاصله اقلیدسی هر جزء بردار ویژگی استخراج

[۱۳] Pattern

[14] gait

[15] dynamic time warping

شده از دنباله تصاویر تست با هر جزء از بردارهای ویژگی دنباله مرجع محاسبه می شود. این متد یکی از روش های جدید است که تا به حال بطور رسمی از آن استفاده نشده و مستلزم تحقیقات بیشتری است. این روش دقت بالایی ندارد و می تواند در مواردی که احتیاج به امنیت بالایی نیست، استفاده شود. مهمترین مزیت این روش اینست که می توانند از فاصله غیر نزدیک هویت فرد را تشخیص دهند (مانند تصاویر در شبکه دوربین مدار بسته) در حالیکه بقیه متدهای بیومتریک مانند اثر انگشت احتیاج به همکاری شخص و نزدیک بودن او برای ضبط اطلاعات می باشد .در این سیستم نحوه تحرک اندام های مختلف بدن هنگام راه رفتن بررسی و تحلیل می گردد.



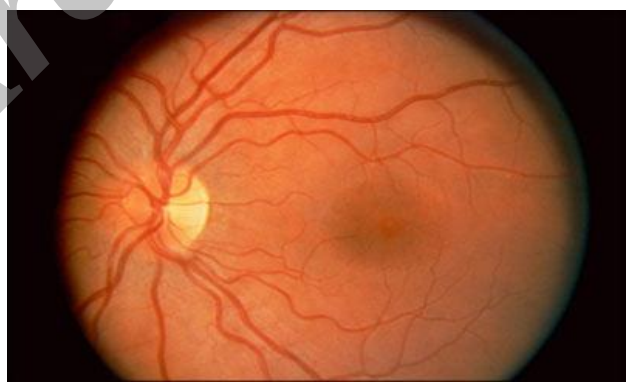
شکل ۳- بررسی نحوه حرکت اندام های مختلف بدن هنگام راه رفتن

طرز راه رفتن یکی از اعمال رفتاری است و امکان دارد در گذر زمان تغییر یابد . از طرفی از آنجا که برای پردازش این روش احتیاج به پردازش بر روی تصاویر ویدیویی است ، روشی با پردازش سنگین و در نتیجه گرانقیمت است . به همین دلایل این روش اصلا رایج نشده است.

.

۴-۷- تشخیص هویت با استفاده از شبکیه چشم

در این روش از سطح شبکیه تصویربرداری می شود و ساختار رگ‌های پشت شبکیه مورد پردازش قرار می گیرد. ساختار این رگ‌ها برای هر فرد با فرد دیگری، حتی در دو قلوهای همسان نیز فرق دارد. از آن جهت که امکان دسترسی به شبکیه وجود ندارد، این روش در مقایسه با روش های دیگر مانند اثر انگشت، عنبیه و ... از امنیت بالاتری برخوردار است. بطور مثال در اثر انگشت می توان از لایه های پوست مصنوعی و در عنبیه از لنزهای خاص برای تقلب استفاده کرد، ولی امکان دسترسی به شبکیه برای تقلب وجود ندارد .



شکل ۴ : ساختار رگ‌های پشت شبکیه

محدودیت های تصویربرداری همانند عنبیه است ولی با حساسیت کمتر. از طرفی به دلیل تابش نور اندکی به درون مردمک برای تصویربرداری این روش تا حدودی آزار دهنده است و مانع عمومیت یافتن آن شده است. این سیستم توانایی تشخیص هویت را دارد.

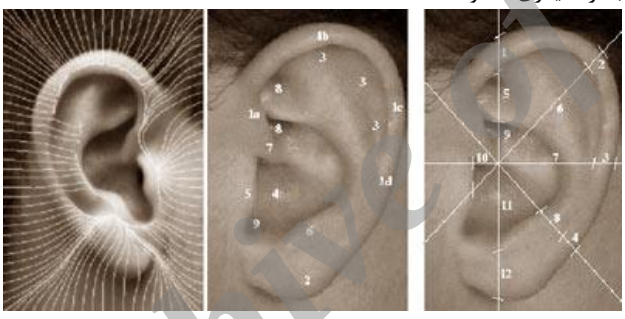
۴-۸- تشخیص هویت با در نظر گرفتن چگونگی تایپ با کیبورد[16]

شناسایی از روی چگونگی تایپ کلیدها یکی ازتازه ترین روش های شناسایی بیومتریک است و همانگونه که از نام آن بر می آید این روش حالت تایپ کلیدها را تحلیل می کند . برای این کار از کاربر خواسته می شود که یک گذر واژه یا یک متن مشخص را تایپ کند و سیستم با تحلیل فاصله های زمانی هر کلید و میان کلیدها به داده هایی می رسد وآنها را به عنوان داده های مرجع ذخیره می کند . برای کار این سیستم ، ورود دست کم هشت کاراکتر لازم است که البته ورود ۱۲ کاراکتر و بیشتر توصیه می شود . این کاراکترها می توانند در یک تا شش رشته متفاوت مانند گذر واژه ، نام کاربری یا آدرس پست الکترونیکی (Email) باشند . برای بالاتر بردن دقت، این روش را با فناوری های فراگیرنده ترکیب می کنند . یعنی هر چه کاربر بیشتر به سیستم وارد شود سیستم با دقت بیشتری او را شناسایی می کند . به طور متوسط میزان خطای این روش سه درصد است . همچنین می توان با چند پرسش کمکی ، ایمنی را باز هم بالاتر برد . از انجا که تنها کاربر مورد نظر ما پاسخ این پرسشها را می داند و چگونگی ورود اطلاعات از سوی او منحصر بخود اوست امنیت باز هم افزایش می یابد. کارشناسان بر این باورند که هر فرد هنگام تایپ بر کیبورد ، از الگوی رفتاری خاصی جهت ضربه زدن به کیبورد استفاده می کند. به این روش ریتم تایپ[17] نیز گفته می شود. در این سیستم کاربر کلمه خاصی را بطور متناوب وارد می‌کند و نحوه تایپ (فواصل زمانی بین ضربه خوردن کلیدها) ثبت و سپس تحلیل می‌گردد . این متد برای تشخیص هویت نمی تواند کارا باشد و تنها در بعضی مواقع برای تایید هویت بکار گرفته می شود. از این روش در تعدادی از کامپیوترهای شخصی و نوتبوک ها برای افزایش امنیت استفاده شده است .

۴-۹- تشخیص هویت از طریق گوش[18]

از گوش به دو شکل برای تشخیص هویت استفاده می شود :

- شکل و ساختار لاله گوش در افراد مختلف متفاوت است
- اکوی صدای خروجی از کانال گوش برای هر فرد با فرد دیگری متفاوت است.



شکل ۵ - شکل و ساختار لاله گوش

تا به حال این روش کارایی زیاد و قابل اعتمادی برای تشخیص هویت نداشته است و مواردی اندک برای تایید هویت از آن استفاده شده است.

۴-۱۰- تشخیص هویت با استفاده از ورید و رگها[19]

در این روش از رگ های زیر پوست فرد تصویر تهیه می شود و ساختار آنها مورد پردازش و تحلیل قرار می گیرند. ساختار این رگ‌ها برای افراد مختلف منحصربفرد است. روش های مختلفی برای تصویربرداری وجود دارد که معمول ترین آنها دوربین های مادون قرمز و سنسورهای حرارتی لمسی مادون قرمز است .حالت رگ‌های هر شخص مانند اثر انگشت او یک ویژگی منحصر بفرد است . وضعیت رگ‌ها حتی میان دو دوقلوی همسان هم ناهمسان است . تنها مشخصه‌ای از رگ‌ها که با گذشت زمان تغییر می‌کند، اندازه آنهاست. بنابراین پژوهشگران شرکت فوجیتسو از همین ویژگی برای تشخیص هویت افراد استفاده کرده‌اند. در روش شناسایی از روی رگ‌ها، نور مادون قرمز به کف دست تابانده می‌شود. با این کار وضعیت رگ‌هایی که زیر پوست قرار دارند به دست می‌آید. سپس این مشخصات با داده‌های مرجع مقایسه می‌شود . جزئیات این جریان از قرار زیر است: هموگلوبین موجود در خون بخش‌هایی از طیف نور را

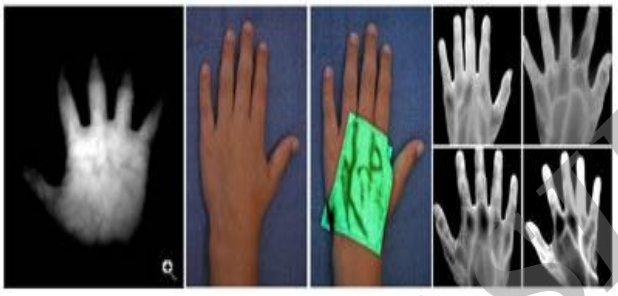
[16] KEY STROKE

[17] typing rhythm

[18] Ear

[19] Patterns vascular & vein

جذب می‌کند که طول موج آنها حدود ۷/۶×۱۰ است. به این ترتیب رگ‌ها خطوطی تیره رنگ می‌شوند و حسگر، اطلاعات تصویر را دریافت و ذخیره می‌کند . یکی از برتری‌های روش شناسایی از روی وضعیت رگ‌ها آن است که نیازی به تماس فیزیکی ندارد و از این نظر روشی پاکیزه است . همچنین میزان دقت آن تا حد قابل قبولی بالاست . به عبارت دیگر درصد خطای آن حدود ۰/۰۰۰۰۸ درصد است . درصد خطای اسکن کردن رگ‌ها حدود ۰/۰۰۰۰۸ درصد است . بر پایه اعلام شرکت فوجیتسو این روش به ویژه برای مراکز بازرگانی سودمند است . این روش به عنوان یک جایگزین مستقیم و سریع برای انگشت نگاری ، با صرفه و دقیق است و اکنون در برخی مراکز به کار برده می‌شود . عموما از رگ‌های پشت کف دست ، کف دست و رگ‌های انگشتان دست برای این نوع بیومتریک استفاده می شود. از آن جهت که شکل و حالت پوست در نتیجه این سیستم تاثیر ندارد، این روش نسبت به روش های اثر انگشت و شکل هندسی دست دارای امنیت بیشتر است.



شکل ۶- تصویربرداری از رگ های زیر پوست

۴-۱۱- تشخیص هویت از طریق لب ها[20]

تا به حال این نوع از بیومتریک پیشرفت و کاربرد خاصی نیافته است . از لب به عنوان بیومتریک به یکی از سه طریق زیر استفاده می شود :

- اثر لب[21] : همانند اثر انگشت است با این تفاوت که اثر لب را ثبت می کنند . لب نیز همانند انگشت دارای منحنی ها و خط و خطوط مختص به هر فرد است . این روش تا حد زیادی قابل اعتماد است.
- نحوه تحرک لب ها[22] : این روش همانند Gait یک روش رفتاری است و در تشخیص گوینده به ما کمک می کند؟ روش دقیقی نیست و می تواند تنها برای تایید هویت استفاده شود .
- شکل لب ها : می تواند برای تایید هویت به کار رود و مرسوم نیست.

۴-۱۲- تشخیص هویت از طریق ناخن

این متد کاملا جدید است و تحقیقات گسترده ای روی آن صورت نگرفته است . از ناخن به دو شکل برای بیومتریک استفاده می کنند :

- رشته های گوشت زیر ناخن[23] : اگر در ابعاد میکروسکوپی به سطح نرم زیر ناخن نگاه کنیم ، در می‌یابیم این سطح دارای برآمدگی هایی موازی و رشته مانند است . این قسمت شامل مویرگ‌ها ، اعصاب و ... است . در طول سن این برآمدگی ها یا رشد طولی دارند یا پهن تر می گردند ولی در هرحال وجود دارند . ادعا می شود که ساختار و شکل این رشته ها همانند اثر انگشت و عنبیه در افراد مختلف ، متفاوت است .
- Nail RFID : این روش بسیار به ندرت استفاده شده است . در این روش یک میکرو چیپ RFID بر روی سطح ناخن قرار می گیرد و میزان خاصیت خازنی بین سطح بالایی ناخن و سطح گوشت را می سنجد . این میزان خازن برای هر فرد منحصربفرد است .

[20] lips

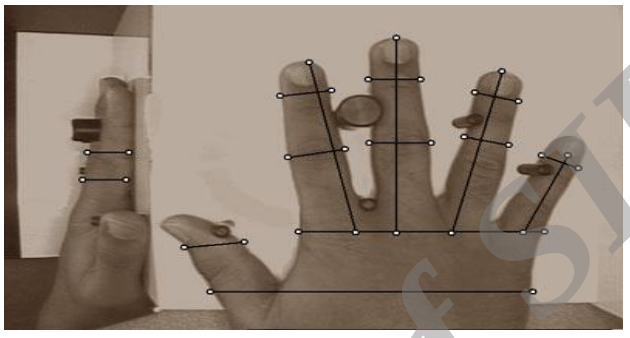
[21] Lips print

[22] Lips movement

[23] Bed nail

۴-۱۳- تشخیص هویت از طریق شکل هندسی دست و انگشت[۲۴]

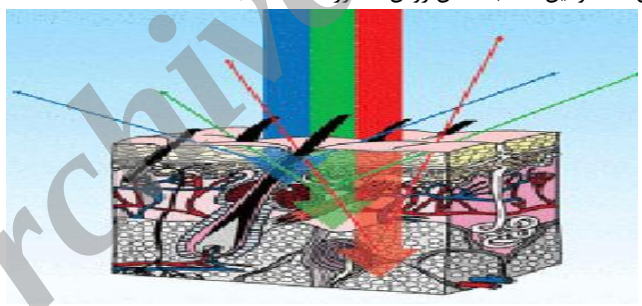
آنچه که در این روش مورد تحلیل و مقایسه قرار می گیرد ، طول و قطر انگشت ها ، مکان مفاصل ، شکل و سایز کف دست است . این تکنیک بسیار ساده و مقرون به صرفه است . تغییرات ظاهر پوست مانند خشکی انگشت ، در نتیجه مقایسه تاثیر گذار نیست در حالیکه در روش اثر انگشت لازم است که پوست حالت غیر خشک و معمولی داشته باشد . با این حال ساختار هندسی بیان شده در افراد مختلف واقعا یک پدیده متفاوت نیست و ممکن است چند نفری یافت شوند که دارای مشخصات یکسان باشند ، از این رو این روش برای تشخیص هویت در بین خیل انبوه کاربران استفاده نمی شود و معمولا تنها برای تایید هویت (بعد از تشخیص هویت اولیه مانند اثر انگشت) و یا برای وارد شدن به اتاقی در یک دپارتمان (ورودی دپارتمان نیز محدود به روش های بیومتریک است) از آن استفاده می شود . از طرفی ساختار هندسی اشاره شده می تواند در طول رشد و یا عوامل دیگر مانند استفاده از انگشتر تغییر یابد و این مسائل به شدت از کارایی این روش می کاهند .



شکل ۷- تحلیل و مقایسه طول و قطر انگشت ها، مکان مفاصل، شکل و سایز کف دست

۴-۱۴- طیف الکترومغناطیسی پوست [۲۵]

در این روش توسط دیودهای نوری (LED) به سطح پوست یک سری نور خالص با طول موج های مختلف می‌تابانند وتوسط تعدادی فتو دیود میزان شدت موج برگشتی از سطح پوست را ثبت و سپس اطلاعات را تحلیل می کنند . میزان جذب و انعکاس نور (به طور کلی هر موجی متناسب با طول موجش) توسط پوست هر فرد متفاوت با دیگران است و این مطلب اساس روش مذکور است.



شکل ۸- میزان جذب و انعکاس نور پوست هر فرد متفاوت با دیگران است

۴-۱۵- تشخیص هویت از طریق صدا

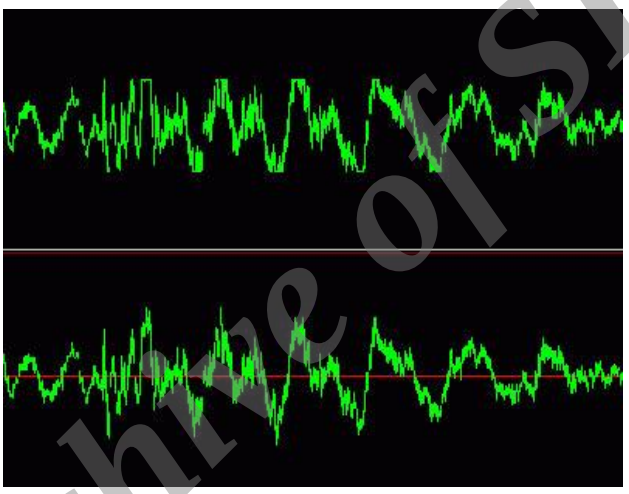
در روش شناسایی از روی صدا نخست آن را تغییر داده و سپس با یک داده مرجع مقایسه می کنند . روش های شناسایی از روی صدا در حال گسترش هستند تا وابستگی آن به یک متن مشخص از بین برود بیشتر افراد هنگامی که از تشخیص صدا صحبت می شود به فکر فرکانس صدا و دستگاه اسیلوسکوپ (دستگاهی که موج را بر روی نموداری در روی محور افقی گرفته و با تصویری از آن بر روی محور عمودی و اندازه گیری ولتاژ ، صداها را از یکدیگر تمیز می دهد) می افتند در صورتی که در فناوری جدید از دستگاه طیف نگار صدا[۲۶] استفاده می شود. دستگاه طیف نگار در واقع یک گراف را متصور می کند،

[24] Finger geometry & hand

[25] Spectrum skin

[26] sound spectrogram

فرکانس صدا را بر روی محور عمودی و زمان را بر روی محور افقی تصویر می کند و در این صورت هر صدایی گراف ویژه خودش را خواهد داشت . این دستگاه از رنگ ها و سایه ها در تصویر کردن گراف استفاده می کند تا دقت شناسایی بیشتر شود و کیفیت آوا شنودی صدا بالاتر رود . هم اکنون در برخی از شرکت های اروپایی و امریکایی از این مدل تشخیص هویت استفاده می کنند زیرا در این مدل دیگر احتیاج به حضور فیزیکی نیست و به راحتی کاربر می تواند با فرستادن صدای خود حتی از طریق اینترنت هویت خود را نشان داده و از آرشیوهای محرمانه استفاده کند . البته تشخیص هویت اشخاص از طریق صدا نسبت به اثر انگشت یا اسکن چشم امنیت کمتری دارد . برای کاستن از پارازیت ها و عوامل مزاحم ، به عنوان ابزار ورودی از یک میکروفون با کیفیت خوب استفاده می شود . به بیان دیگر در این سیستم ، صدا را بر پایه زمان و دامنه ضبط می کند و پس از استاندارد کردن مقیاس زمانی ، بسامدها و ارتفاع صوت با داده های مرجع مقایسه می شوند . از آنجا که سخن گفتن عملی پویا و قابل تغییر است حتی کوچکترین عوامل مانند سرماخودگی می تواند باعث تغییر صدا و پایین آمدن وضوح آن شود اما اینگونه عوامل روی چیزهایی مانند لهجه،تاکیدروی کلمات یا سرعت کلام تقریبا تاثیری ندارند . این روش بسیار برای ما انسان ها آشناست بطوریکه در مکالمات تلفنی به راحتی و بدون آنکه چهره فرد را ببینیم، قادر به تشخیص هویت طرف مقابل هستیم . در سیستم های پردازشی این فیلد به نام "تایید گوینده" شهرت یافته است و الگوریتم های زیادی بدین منظور معرفی شده اند . یکی از ساده ترین انواع این الگوریتم ها بر اساس بمی یا زیری صدای فرد است. صدای هر فرد در حالت عادی و از آن دقیق تر هنگام ادای کلمه رمز دارای دامنه های خاصی از فرکانس های مختلف است. در حقیقت طیف سیگنال صدای فرد هنگام ادای کلمه عبور را با طیف ثبت شده در دیتابیس مقایسه می کنند .



شکل ۹ : صدای هر فرد در حالت عادی دارای دامنه های خاصی از فرکانس های مختلف است.

۴-۱۶- تشخیص هویت از روی تپش های قلب

پژوهشگران دانشگاه ویسکانسین – مادیسون یک روش بیومتریک تازه برای شناسایی افراد پیدا کرده‌اند. این پژوهشگران تپش‌های قلب را مبنای کار خود قرار داده‌اند. آنها دریافته‌اند که هر قلب الگوی یکتای خود را برای تپش دارد. آنها از این کشف برای ساختن یک روش بیومتریک برای شناسایی افراد استفاده کرده‌اند. تقریباً مانند همه روش‌های بیومتریک، سیستم نخست یک الگو از تپش قلب می‌سازد. برای این کار از ویژگی‌های خاص که با حسگرهای متعارف مانند ECG جمع‌آوری می‌شوند، استفاده می‌شود. سپس داده‌های کلیدی کاردیوگرام برای مقایسه بعدی در بانک اطلاعاتی ذخیره می‌شود. برای هر چه بالاتر بردن ضریب اطمینان این روش، عملیات pre-processing و pre-screenin اهمیت ویژه‌ای دارند. در این مرحله، تپش‌های قلب به گونه‌ای شده و در مورد پردازش قرار می‌گیرد که بتوان داده‌های حاصل را در یک بانک اطلاعاتی ذخیره کرد. البته این روش هنوز دقت و اطمینان کافی را ندارد و هنوز در آغاز راه خود است. اما همه این پژوهش‌گران مطمئن هستند که شناسایی از روی تپش‌های قلب کاملاً شدنی است.

۴-۱۷- تشخیص هویت با استفاده از نمایشگر دمای نقاط بدن

نقاط مختلف یک جسم یا بدن بر اساس نوع و میزان حرارتش امواج مادون قرمز تابش می کند . این روش یک روش کلی برای بدست آوردن اطلاعات تصویر است و می تواند برای تصویربرداری در خیلی از فیلدهای اشاره شده در بالا مانند اثرانگشت، کف دست، رگ‌های زیر پوست، گوش و ... به کار رود. در این روش ها الگوی حرارتی تابش شده از صورت فرد، دست ها و یا حتی رگ‌های فرد را به کمک یک دوبین مادون قرمز ضبط و سپس پردازش مناسب را انجام

می دهند. این الگوها برای هر فرد منحصر به او می باشد. به دست آوردن این نوع اطلاعات خام از افراد مشکل نیست ولی دقت در تصویربرداری مشکل خواهد بود. چرا که، اگر فرد در محیطی با یک منبع حرارتی قوی باشد و یا در دستش یک فنجان چای گرم باشد، تمامی محاسبات اشتباه می شوند. از این رو برای استفاده از این شکل بیومتریک، اتاقک های مخصوصی در نظر می گیرند که یقینا سبب صرف وقت، هزینه، و همچنین عدم راحتی کاربر می شود.

۴-۱۸- تشخیص هویت با استفاده از DNA

بدون شک Deoxyribonucleic Acid یکی از مطمئن‌ترین روش های تایید هویت است. DNA ، کدی یک بعدی و منحصر به هر فرد است . در حالیکه این روش دقیق ترین شکل بیومتریک است ولی از آن در تامین امنیت شبکه ها و اماکن و... استفاده نمی شود ، زیرا این روش اصلا سریع نیست و همچنین تا به حال فرایندی اتوماتیک و مقرون به صرفه برای آن معرفی نشده است (فرایند به دست آوردن این کد ، احتیاج به ابزار و مواد شیمیایی خاصی دارد) . البته ساختار DNA در دوقلوها تا حد زیادی شبیه است و در دوقلوهای همسان کاملا یکسان است و عیب بزرگی برای این متد است ولی از دقت و صحت این روش در تشخیص هویت نمی کاهد .

۴-۱۹- تشخیص هویت با استفاده از تشخیص چهره

انسان ها به طور معمول بیش از هر روش بیومتریکی از تشخیص چهره برای شناخت و شناسایی همدیگر استفاده می کنند . از چهره به چندین نحو مختلف به منظور بیومتریک استفاده می شود :

- ساختار هندسی چهره : در این شیوه مشخصات فیزیکی صورت مانند مکان چشم ، بینی ، لب ، ... و ارتباط بین آنها را تحلیل می کنند . تصاویر تهیه شده می توانند سه بعدی نیز باشند. این شیوه بسیار پرکاربردتر از بقیه متدهاست .
- ساختار ظاهری پوست: در این روش چین و چروک های صورت بررسی می‌شود . این ساختار همانند اثر انگشت در افراد مختلف متفاوت است .
- مشخصه گرمایی صورت : در این مدل توسط دوربین های مادون قرمز از صورت تصویربرداری می شود . نقاط مختلف صورت براساس میزان حرارت و دمایی که دارند در تصویر دیده می‌شوند (نقشه ای از سطح صورت تهیه می شود) . از آنجا که تجمع رگ‌های زیر پوست صورت در هر فرد شکل متفاوتی دارد ، تمایز رنگ بین نقاط مختلف صورت ثابت می ماند البته این سیستم به دلیل محدودیت‌های مختلفی که دارد چندان عمومیت نیافته است .
- لبخند : تفاوت بین چهره در حالت عادی و هنگامی که لبخند می زنیم را تحلیل می کنند .

۴-۲۰- تشخیص هویت با استفاده از رادیوگرافی دندان:

برخلاف سایر روش های بیومتریک، تشخیص هویت از طریق دندان بسیار پیچیده است زیرا دندان با گذشت زمان بسیار تغییر می کند. یک دندان می تواند در اثر عمل جراحی یا تصادف از دست رود. به همین دلیل در مجامع قانونی اینروش تشخیص کمتر قابل قبول است و در برخی موارد (مانند قتل در آتش سوزی) تنها وسیله تشخیص همیت روش می تواند باشد. در این روش از بیومتریک از عکس های رادیولوژی که از دندان افراد مختلف گرفته می شود به عنوان اطلاعات اولیه پایگاه داده ها مورد استفاده قرار می گیرد. سپس بعد از مرگ یک فرد به طوری که نشود او را از طریق دیگر تشخیص داد از دندان های او عکس گرفته و با داده های قبلی تطابق داده می شود تا هویت فرد مورد نظر تعیین گردد.

۵- نتایج تجربی وتحلیل کاربرد روش ها

پس از بررسی روشهای مختلف در تشخیص هویت افراد، لازم است بر طبق جدول ۱ به ارزیابی این روشها بپردازیم. جهت ارزیابی روشها در نظر گرفتن چند نکته حائز اهمیت است. معیارهای ارزیابی روشها وابسته به پارامترهایی از جمله پایداری طولانی مدت، هزینه کم، استفاده آسان، صحت و نرخ خطا می باشد.

جدول ۱ – بررسی روشهای مختلف در تشخیص هویت افراد

Biometric	Security level	Long – term Stability	Low Cost	Ease of Use	Accuracy
دست	●●	●●		●●●	●●●
شیمیایی بو	●●	●●●		●●	●●
عنبیه	●●●	●●●		●●	●●●●
طرز حرکت	●●●	●●●		●●	●●●
شبکیه	●●●	●●●		●	●●●●
چگونگی تایپ باکیبورد	●●	●		●●●	●
گوش	●●	●●		●	●●
ورید و رگها	●	●●		●●	●
لب	●●	●●		●●●	●●
ناخن	●●●	●		●●	●●
طیف پوست	●●	●●		●	●
نمایشگر دمای بدن	●	●		●●	●●
تپش قلب	●●●	●●		●●	●●●●
DNA	●●●	●●●		●	●●●●

جدول ۲- ویژگی های روش های شناسایی بیومتریک

روش	برتری ها و کاستی ها
اثر انگشت	برتری: میزان خطای بسیار ناچیز کاستی: مزاحمت برای کاربر
نمای۲بعدی و۳بعدی چهره	برتری:بیش از ۱۰سال است بکار می رود کاستی:زیاد بودن حجم داده ها،زمان وهزینه رابالا می برد
دست	برتری:بیش از ۱۰سال است بکار می رود کاستی:تفاوت اندازه ها گاهی به اندازه کافی نیست
تپش قلب	هنوز در دست بررسی و تحقیق است
عنبیه	برتری:اطمینان بالاو خطای بسیار کم کاستی:هراس کاربران از در معرض نور قرار دادن چشمان
شبکیه	برتری:اطمینان بالاو خطای بسیار کم کاستی:هراس کاربران از در معرض نور قرار دادن چشمان
صدا	برتری:کاربران آن را به سادگی می پذیرند کاستی:اشکال در یافتن فاصله واژه هاوسرعت ادای آنها، پردازش سنگین و سرعت کم
نحوه تایپ	برتری:ارزانی و پذیرش از سوی کاربران کاستی:زمان بررسی زیادومتغیر بودن ضربه آهنگ کلیدها
امضا	برتری: پذیرش از سوی کاربران کاستی:زمان بررسی زیادومتغیر بودن سرعت و حالت امضا
اسکن رگها	برتری:برای کاربران مزاحمتی ندارد وبه سادگی پذیرفته میشود کاستی:هزینه و زمان زیاد

۵-۱- روش های دیگر

در این قسمت روش های غیر متداول و تحت مطالعه را فقط نام می بریم:

- سیگنال قلبی و خون
- عطر و بو مربوط به هر فرد
- انعکاس صوت در مغز
- مقاوت الکتریکی پوست
- شکل ظاهری دست مشت شده
- چین خوردگی های پوست انگشت
- چگونگی در دست گرفتن اجسام
- صدای منتقل شده از استخوان های انگشت پس از تحریک یک پالس صوتی
- موج مغناطیسی منتشر شده از انسان
- نحوه رد گیری چشم
- توپوگرافی سطح قرنیه
- شکل سه بعدی انگشت
- طیف حاصل از سیگنال های مغزیEEG
- شکل سینوس های جلویی سر

۶- نتیجه گیری

یکی از مهمترین مسائل امروز، تامین امنیت جان، مال و اطلاعات است و بدون شک سیستم های بیومتریک یکی از پرکاربردترین سیستم ها برای نیل به این هدف هستند. در این مقاله سعی شد به شکلی مصور و در نهایت اختصار مروری بر روش های بیومتریک داشته باشیم. لازم به ذکر است که به دلیل ساده نگاری و اجتناب از گنگ شدن مطالب، از بیان جزئیات الگوریتم ها و ویژگی ها در طی مقاله پرهیز گشته بود. همان طور که از جدول شماره ۱ کاملامشخص می باشد هر سیستم بیومتریک دارای قوت و ضعف خاص خودش است و انتخاب هر روش خاص بسته به کاربرد آن دارد. هیچ روش بیومتریک به تنهایی انتظار نمی رود که به صورت کاملا موثر نیازهای یک کاربرد را برآورده سازدبه عبارت دیگر هیچ بیومتریکی بهینه نمی باشد. پر کاربرد ترین روش های بیومتریک برای تشخیص هویت افراد در حال حاضر،سیستم هایی هستند که داده های اثر انگشت، ویژگی های چهره، شبکیه چشم و عنبیه را دریافت کرده و با داده های موجود در بانک اطلاعاتی مقایسه می کنند.اگر داده ی دریافت شده با درصد قابل قبولی با داده های مرجع مطابقت داده شود، فرد شناسایی خواهد شد. با ورود سیستم های شناسایی بیومتریک، عمل وقت گیر ورود نام کاربری و گذرواژه حذف خواهد شد. گذاشتن انگشت روی حسگر با یک لبخند به دوربین کافی است تا اجازه کار با کامپیوتر را بدست آورید. افزون بر این سیستم های بیومتریک هم صد در صد قابل اطمینان نیستند و همچنان باید نگران عملکرد نادرست یا اختلال در آن بود. از همین رو بهتر است از ترکیب روش های بیومتریک استفاده شود.

۷- مراجع

[۱] سعید ابریشمی، " شناسایی چهره با استفاده از آنالیز مولفه های اصلی و شبکه های عصبی مصنوعی "،پایان نامه جهت اخذ مدرک کارشناسی ارشد مهندسی کامپیوتر، دانشگاه فردوسی مشهد، دانشکده مهندسی، زمستان ۱۳۷۸

[۲] سرور بهبهانی ، محمد کریمی مریدانی ، روش های تشخیص هویت ، مجله مهندسی پزشکی ، شماره ۱۱۰

[۳]امیرحسین جهانگیر ،مجید صارمی ،سیستم بی درنگ تشخیص چهره براساس تجزیه به مقادیر منفردوضرائب همبستگی محلی ،مجموعه مقالات کنفرانس بین المللی سالانه کامپیوترانجمن کامپیوترایران، دانشگاه علم وصنعت ایران، تهران،دیماه۱۳۹۲

[۴]ابراهیم روزگار،محمدشهرام معین،تجزیه وتحلیل تکنیکهای مختلف شناسائی چهره،گزارش داخلی مرکز تحقیقات مخابرات ایران،۱۳۹۱

[5]http://www.tebyan.net/science_technology/computermagazine/

[6] Ivanna K. Timotius, IwanSetyawan, and Andreas A. Febrianto ,'' Face Recognition between Two Person using Kernel Principal ComponentAnalysis and Support Vector Machines'', International Journal on Electrical Engineering and Informatics - Vol 2, Nom 1, 2012

[7] Omar Faruqe , Al MehediHasan ,'' Face Recognition Using PCA and SVM'', Dept. of Computer Science &Engineering,Rajshahi University of Engineering &Technology,Rajshahi, Bangladesh(2010)

[8] A. Lima, H. Zen, Y. Nankaku, C. Miyajima, K. Tokuda, T. Kitamura,''On the Use of Kernel PCA for Feature Extraction in Speech Recognition'', Proceeding of EuroSpeech, pp. 2625–2628, Sep. 2008.