**آموزشکده فنی و حرفه ای سما**

**واحد پارس آبادمغان**

**گروه کامپیوتر**

**پایان نامه برای دریافت درجه کاردانی**

**کامپیوتر - نرم افزار**

## عنوان:

# سیستم های بیومتریک

## استاد راهنما:

**مهندس جعفر محرمی**

## دانشجو:

**فرهاد عباس زاده**

## شماره دانشجویی:

911824286

## تابستان

1393

## تقدیم به :

**تقدیم به پدر و مادر بزرگوارم که تمام مشکلات و سختی های زندگی را در طول دوران تحصیلم تحمل کرده و مرا همراهی و یاری نموده و مشوق بنده در ادامه تحصیلم بودند.**

**و**

**تمامی اساتید بزرگوار و دوستان و انسان های خیر خواه**

# تشکر و سپاسگزاری

از دست و زبان که بر آید  از عهده ی  شکرش به در آید.

بعد از حمد و سپاس خالق یزدان  و با سپاس گزاری از :

**استاد محترم راهنما  جناب آقای  مهندس جعفر محرمی**

**و**

**تمامی آنان که زیبا می اندیشند.**

# فهرست مطالب

## مقدمه

برای صدور اجازه ورود برای یک فرد  نیاز داریم وی را شناسایی و هویت وی را تایید کنیم و مورد نظر ما انجام بررسیهایی است که بصورت خودکار توسط یک سیستم صورت بگیرد.

در اصل تمام روشهای شناسایی با سه مورد زیر در ارتباط است ::

1- آنچه که شما میدانید (یک کلمه عبور یا PIN)

2- آنچه که شما دارید (یک کارت یا نشانه های دیگر)

3- آنچه که شما هستید (مشخصات فیزیکی یا رفتاری)

مورد آخر به نام زیست سنجی (Biometrics) نیز شناخته میشود.

کلمه بیو متریک از کلمه یونانی  bios به معنای زندگی و کلمه metrikos به معنای اندازه گیری تشکیل شده است. همه ما می دانیم که ما برای  شناسایی همدیگر از یک سری ویژگی هایی استفاده می کنیم که برای هر شخص به طور انحصاری است و از شخصی به شخص دیگر فرق می کند که از آن جمله می توان به صورت و گفتار و طرز راه رفتن می توان اشاره کرد. امروزه در زمینه های فراوانی ما به وسایلی نیاز داریم که هویت اشخاص را شناسایی کند و بر اساس ویژگیهای بدن اشخاص آن هارا بازشناسی کند و این زمینه هر روز بیشتر و بیشتر رشد پیدا می کند و علاقه مندان فراوانی را پیدا کرده است. علاوه بر این ها امروزه ID و password کارتهایی که بکار برده می شوند دسترسی را محدود می کنند اما این روشها به راحتی می توانند شکسته شوند و لذا غیر قابل اطمینان هستند. بیو متری را نمی توان  امانت داد یا گرفت نمی توان خرید یا فراموش کرد و جعل آن هم عملا غیر ممکن است.

یک سیستم بیو متری اساساً یک سیستم تشخیص الگو است که یک شخص را بر اساس بردار ویژگی های خاص فیزیولوژیک خاص یا رفتاری که دارد باز شناسی می کند. بردار ویژگی ها پس از استخراج معمولا در پایگاه داده ذخیره می گردد. یک سیستم بیومتری بر اساس ویژگی های فیزیولوژیک اصولا

دارای ضریب اطمینان بالایی است .سیستم های بیو متری می توانند در دو مد تایید و شناسایی کار کنند. در حالی که شناسایی شامل مقایسه اطلاعات کسب شده در قالب خاصی با تمام کاربران در پایگاه داده است ، تایید فقط شامل مقایسه با یک قالب خاصی که ادعا شده است را می شود. بنابراین لازم است که به این دو مسئله به صورت جدا پرداخته شود.

# فصل اول

## سیستم بیومتریک

سیستم بیومتریک یک سیستم  تشخیص الگو است که هویت اشخاص را تعیین یا تأیید می کند و این عملیات را با استفاده از اطلاعات بیومتریک کاربران انجام می دهد. نخستین گام در استفاده از این سیستم ثبت اطلاعات بیومتریکی کاربران در بانک اطلاعات (Data Base) سیستم است که پس از ثبت اطلاعات افراد در این سامانه، دو نوع خدمت از سامانه بیومتریکی در خواست می شود: تأیید هویت و تعیین هویت.

در فرایند تعیین هویت، سؤالی که مطرح می شود این است که او چه کسی است؟

دستگاه بیومتریک پس از دریافت داده های بیومتریک توسط شخص متقاضی به انجام عمل مقایسه می پردازد که این مقایسه میان اطلاعات بیومتریک شخص با اطلاعات موجود در بانک اطلاعات انجام می گیرد.در این حالت، فرض بر این است که اطلاعات فرد در بانک اطلاعات موجود است.

اما در فرایند تأیید هویت، سؤالی که به دنبال پاسخش می گردیم، این است که آیا او همان فردی است که ادعا می کند؟

در تأیید هویت، ابتدا متقاضی با استفاده از نام یا وارد کردن رمز عبور و یا یک مدرک شناسایی ادعا می کند که هویت خاصی را دارد. سپس سامانه به مقایسه داده های بیومتریکی مدعی با داده های ثبت شده در بانک مشخصات می پردازد و ادعای وی را مورد بررسی قرار می دهد و نتیجه را اعلام می کند.

آزمایش زیست سنجی (Biometric) در سیستم بیومتریک شامل سه گام است: ثبت مشخصات، مقایسه و به روز رسانی.

1- **ثبت مشخصات**: کاربران با سنجش های اولیه در سیستم ثبت نام می شوند. این عمل در چندین مرحله برای ثبت اطلاعات دقیق انجام می گیرد.

2- **مقایسه**: گام بعدی مقایسه نمونه با الگوی مرجع است. در این مرحله تعیین سطوح مناسب خطای مجاز (tolerance) خصوصاً برای سنجش رفتاری از اهمیت ویژه ای برخوردار است.

3- **به روز رسانی**: تمامی سیستم های بیومتریک مخصوصاً آن هایی که از خصوصیات رفتاری کاربر استفاده می کنند، باید برای به روزرسانی الگوی مرجع طراحی شده باشند.

یک سیستم بیومتری ساده دارای چهار بخش اساسی است :

1- بلوک سنسور: که کار دریافت اطلاعات بیومتری را بر عهده دارد.

2- بلوک استخراج ویژگیها: که اطلاعات گرفته شده را می گیرد و بردار ویژگی های آن را استخراج می کند.

3- بلوک مقایسه: که کار مقایسه بردار حاصل شده با قالبها را بر عهده دارد.

4- بلوک تصمیم: که این قسمت هویت را شناسایی می کند یا هویت را قبول کرده یا رد می کند.

## اجزای سیستم بیومتریک

سیستم بیومتریک از 3 جزء اصلی تشکیل می شود:

1- ابزار اندازه گیری: ابزار طراحی شده در سیستم بیومتریک در حقیقت نقش واسطه با کاربر را برعهده دارد و لذا باید به راحتی توسط کاربران قابل استفاده باشد و در عین حال احتمال خطا در آن بسیار کم باشد.

2- نرم افزار: این نرم افزار که براساس الگوریتم های ریاضی طراحی شده است، متغیرهای سنجش شده را با الگوی مرجع موجود در بانک اطلاعات مقایسه می کند.

3- سخت افزار: در طراحی سامانه بیومتریکی، به قطعات سخت افزاری و کاربرد آنها باید بیش از سایر دستگاه های مشابه توجه نشان داد تا در انجام محاسبات دچار خطا نشود.

## تکنیک های بیومتری

بررسی های بیومتریک به دو دسته عمده تقسیم می شود:

1- تکنیک های رفتاری (Behavioral): در این روش، طرز انجام کاری توسط کاربر سنجیده می شود. مانند امضا کردن یا بیان کردن یک عبارت.

2- تکنیک های فیزیکی (Physiometric) : در این حالت، یک خصوصیت فیزیکی مانند اثر انگشت یا الگوی عنبیه مورد سنجش قرار می گیرد.

## تکنیکهای فیزیولوژیکی

### باز شناسی  هویت از طریق اثر انگشت

این روش قدیمی ترین روش آزمایش تشخیص هویت از راه دور است. اگرچه قبلاً اثر انگشت تنها در زمینه جرم قابل بحث بود، تحقیقات در بسیاری کشورها سطحی از پذیرش را نشان میدهد که به این روش اجازه استفاده در برنامه های عمومی را می دهد. سیستمها میتوانند جزئیاتی از اثر انگشت (نقاطی مانند تقاطعها یا کناره های برجستگیها) یا کل تصویر را بگیرند. الگوهای مرجع که برای حفظ این جزئیات بکار میرود در حدود 100 بایت هستند که در مقایسه با تصویر کاملی که از اثر انگشت با حجم 500 تا 1500 بایت میباشد,بسیار کوچکتر هستند.

در حال حاضر اثر انگشت خوانهای زیادی در دامنه وسیعی وجود دارند که به همراه بعضی کارتخوانها استفاده میشوند. اگرچه در حال حاضر قیمت آنها چندان پایین نیست اما میزان عرضه آنان در فروشگاههای کامپیوتر عادی باعث افت سریع قیمت آنان خواهد شد. به طور مثال شرکت هواپیمایی آلمان لوفتانزا ، آزمایش بلیت های بیومتریک را آغاز کرده است. این بلیت ها با اطلاعات مربوط به اثر انگشت شصت مسافران رمزگذاری شده اند و انتظار میرود سرعت کنترل را بدون پیچیدگی های امنیتی افزایش دهند.

در این بخش سعی بر آن شده است که اصول کلی، موانع و محدودیت های سیستمهای تشخیص اثر انگشت بررسی شوند.

## اصول کلی در سیستمهای تشخیص اثر انگشت:

همانگونه که اشاره شد، اثر انگشت یکی از روشهای مطمئن برای شناسایی افراد می باشد و در زمینه هایی نظیر رسیدگی به جرم، سیستم های کنترل حوادث، کنترل مرزهای ملی و ... به کار می رود. دلیل اصلی انتخاب اثر انگشت برای شناسایی افراد این است که اثر انگشت هر فرد منحصر به فرد بوده و بعضی از ویژگی های آن تا آخر عمر ثابت باقی می ماند و از همین ویژگی ها در تطبیق اثر انگشت استفاده می شود. برای تطبیق دستی اثر انگشت روشهای استانداردی وجود دارد، اما روش دستی تطبیق اثر انگشت کاری مشکل و بسیار وقت گیر بوده و کارایی لازم را ندارد.البته از آنجا که بانکهای اطلاعاتی دارای میلیونها اثر انگشت می باشد، عملاً تطبیق دستی اثر انگشت امری محال می شود.

به منظور اتوماتیک کردن تطبیق باید روشی برای تصویر و یا کد کردن اثر انگشت تعریف گردد. برای این منظور تصویر بایستی شرایط زیر را داشته باشد:

1- توانایی تمایز هر اثر انگشت در سطوح مختلف رزولوشن،

2- محاسبات ساده

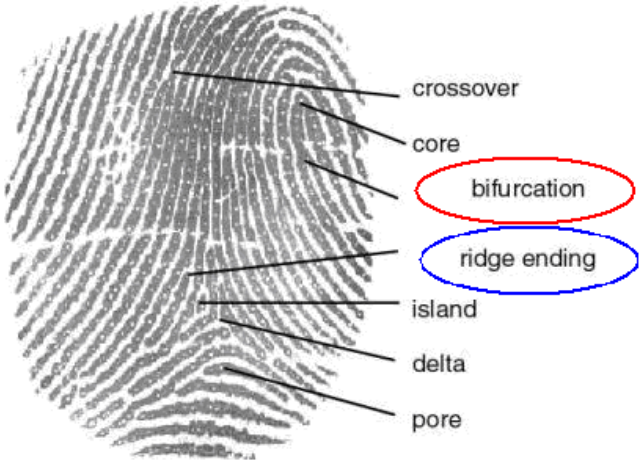
3- قابلیت بکارگیری در الگوریتم های تطبیق اتوماتیک،

4- پایداری و عدم تغییر با نویز و خرابی ها

5- کارا بودن و نشان دادن تصاویر به صورت فشرده

اگر تصویر به صورت خام ذخیره شود، حافظه زیادی مورد نیاز است و سیستم کارایی لازم را نخواهد داشت. در روشهای ساختاری ویژگی ها از تصویر استخراج و تصویر با این ویژگی ها شناخته شده و همچنین با استفاده از همین ویژگیها عمل تطبیق صورت می گیرد.

اثر انگشت از برآمدگی ها و فرو رفتگی ای فلو مانندی تشکیل شده است که بسته به وضعیت قرار گرفتن آنها ویژگی های مختلفی به وجود می آید. تا کنون 18 ویژگی برای اثر انگشت شناخته شده است که دو ویژگی مهم آن ، انتهای برآمدگی و دوشاخه شدن برآمدگی می باشدکه اصطلاحاً به آنها مینوتیا می گویند. در شکل زیر این دو ویژگی نشان داده شده است:




**شکل 1: ویژگی های مینوتا در اثر انگشت**

اطلاعات مینوتیا در مولفه های x ، y و زاویه برآمدگی ها آنها قرار دارد.ساختار توپولوژیکی مینوتای یک اثر انگشت منحصر به فرد بوده و با گذشت زمان تغییر نمی کند. در نتیجه می توان تشخیص اثر انگشت را بر مبنای تطبیق ساختار توپولوژیکی مینوتیا استوار ساخت. در یک تصویر انگشت با کیفیت نسبتاً خوب در حدود 70 تا 80 مینوتا وجود دارد که البته این تعداد در تصویرهای جزئی به حدود 20 تا 30 ویژگی کاهش می یابد، اما باز هم بااین تعداد می توان عمل تطبیق اثر انگشت را انجام داد.

اکثر سیستمهای تشخیص اثر انگشت، ساختاری بر مبنای مینوتیا دارند. در این سیستمها سه مرحله اساسی برای تشخیص وجود دارد که عبارتند از:

1- پیش پردازش

2- استخراج مینوتیا

3- تطبیق مینوتیا

مرحله اول برای افزایش کیفیت تصویر انجام می گیرد، مرحله دوم برای استخراج ویژگی های تصویر و مرحله آخر برای مقایسه مورد استفاده قرار می گیرد.

در مورد تطبیق، روشهای گوناگونی وجود دارد که از جمله می توان به موارد ذیل اشاره کرد:

1- تطبیق مجموعه نقاط

2- تطبیق گراف

3- همشکلی دو زیر گراف

البته عمل تطبیق بنا به دلایل زیر نیاز به محاسبات پیچیده دارد:

1- معمولاً کیفیت اثر انگشت پایین است.

2- بانک اطلاعاتی اثر انگشت ها بزرگ است.

3- تصویر هایی که به صورت ساختاری آسیب دیده اند، به الگوریتم های نیرومندی جهت تطبیق نیاز دارند.

در سیستمهای تشخیص اثر انگشت موجود دربازار که از این دو ویژگی (انتهای برآمدگی و دوشاخه شدن برآمدگی) استفاده می شود، به علت بزرگ بودن بانک اطلاعاتی و نویز دار بودن تصاویر، یک تطبیق یک به یک عملاً مشکل بوده و از این رو یکسری از تصویر های تطبیق یافته تهیه و سپس تطبیق نهایی توسط افراد متخصص انجام می گیرد.

**استخراج سایر ویژگی ها**:

علاوه بر ویژگی های بیان شده ، در بسیاری از سیستمهای تشخیص اثر انگشت، از ویژگی های سطح بالا نیز استفاده می شود. این امر باعث افزایش صحت عمل تطبیق می گردد. یکی از این ویژگی های مهم کلاس الگوی اثر انگشت می باشد.

اثر انگشت به پنج کلاس اصلی تقسیم می شود ک عبارت اند از:

1- کمان

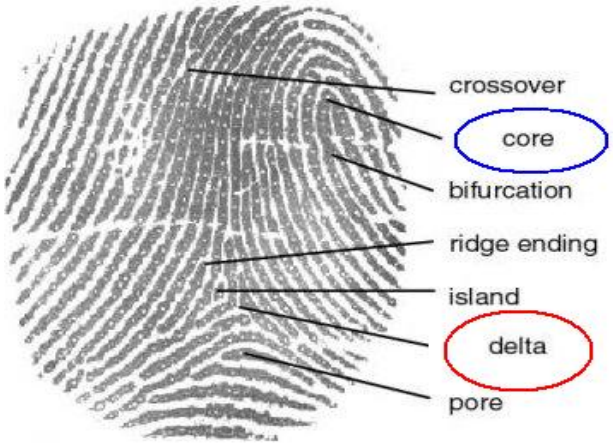
2- کمان مایل

3- حلقه چپ

4- حلقه راست

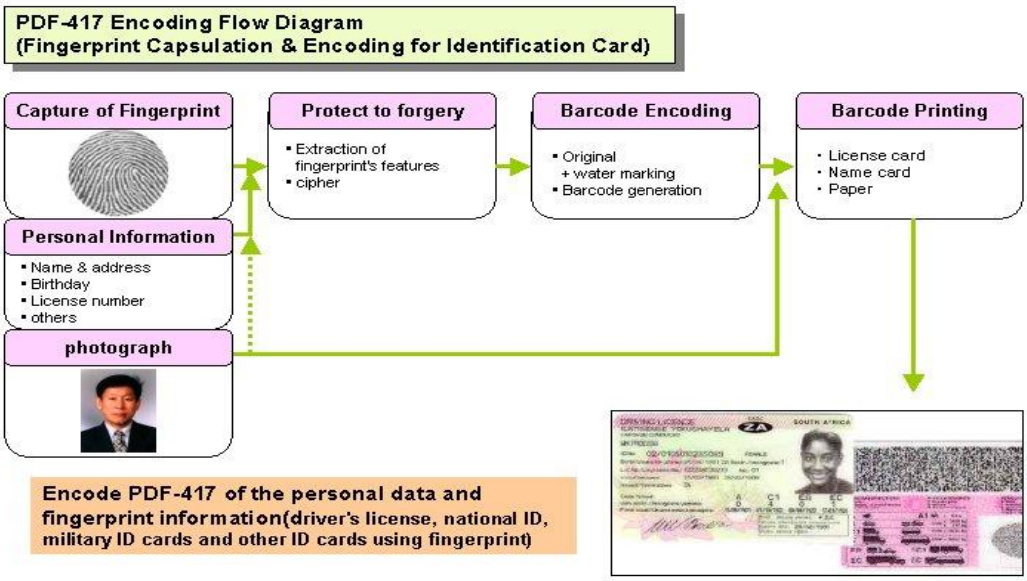
5- مارپیچ

در تصاویر نویز دار و جزئی ممکن است کلاس الگو نامشخص باشد، که در اینصورت از یک ویژگی سطح بالاتری به نام چگالی برآمدگی ها به جای کلاس الگو استفاده می شود که بیانگر تعداد برآمدگی ها در واحد طول تعریف می شود. به منظور مستقل کردن چگالی برآمدی ها از جهت تصویر، تعداد برآمدگی ها بین دو نقطه منفرد محاسبه می شود. نقاط منفرد در اثر انگشت هسته و دلتا می باشند.هسته بالاترین نقطه در داخلی ترین برآمدگی و دلتا یک نقطه سه شاخه است که سه برآمدگی از کنار آن عبور می کند. در شکل زیر این نقاط نمایش داده شده است:




**شکل 2 : محل نقاط هسته و دلتا بر روی اثر انگشت**

یک سیستم اتوماتیک تشخیص اثر انگشت دارای مراحل نشان داده شده در شکل 3 می باشد:

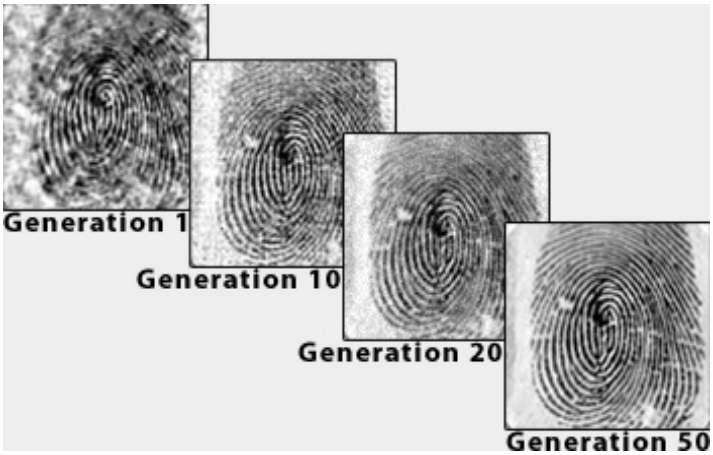



**شکل3: بلوک دیاگرام نحوه کد کردن اطلاعات اثر انگشت**

در ادامه به بررسی مختصری از مراحل فوق می پردازیم:

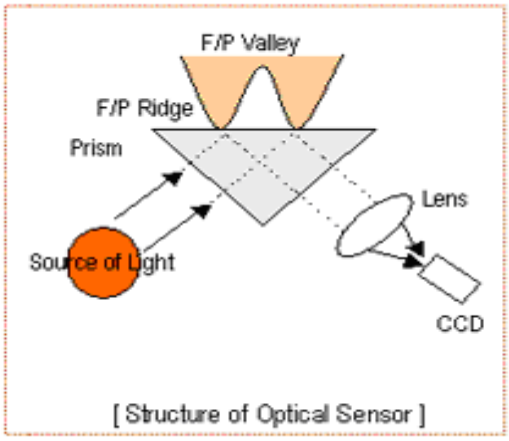
1- **نحوه به دست آمدن تصویر اثر انگشت:**

1-1- **کاغذ و مرکب** : در سالهای گذشته بیشتر از روش کاغذ و مرکب استفاده می شد به این ترتیب که در ابتدا اثر انگشت فرد با استفاده از مرکب بروی کاغذ ثبت و سپس تصویر اثر انگشت اسکن شده و فایل تصویری آن آماده می شد، که این روش اکنون به علت مشکلات خاص خود و البته پیشرفت تکنولوژی کم کم منسوخ می شود. معمولا چون کیفیت تصویر به دست آمده پایین است با استفاده از تکنیک های پردازش تصویر این نقیصه تا حدی مرتفع می گردد، در شکل 4 نمونه هایی از این عمل دیده می شود:




**شکل4: نمونهای از پردازش اولیه تصویر به دست آمده از اسکن اثر انگشت**

2-1- **روش اسکن مستقیم نوری**: روشهای گوناگونی برای انجام این نوع تصویر گیری وجود دارد. نمونه ای از آن در شکل زیر آمده است:

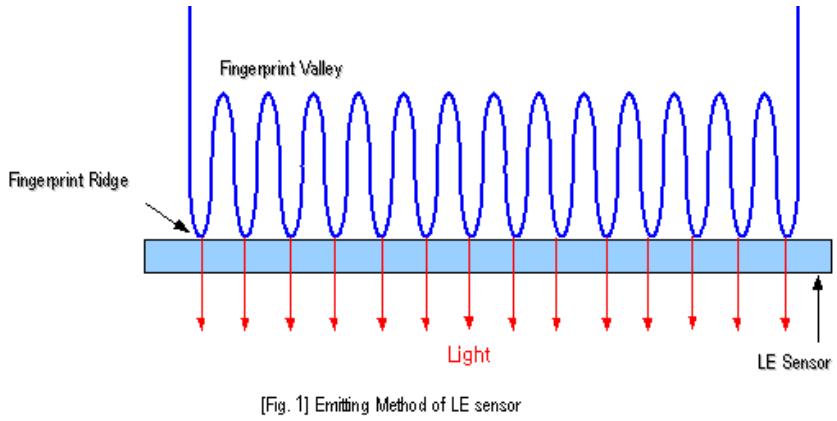



**شکل5 : روش اسکن مستقیم نوری**

### 3-1- با استفاده از سنسور LE

در این روش از تکنولوژی نیمه هادی ها استفاده می گردد. به این ترتیب که انگشت شخص بر روی سنسور LE که از جنس نیمه هادی می باشد، قرار گرفته (شکل6) و در نتیجه در محل های

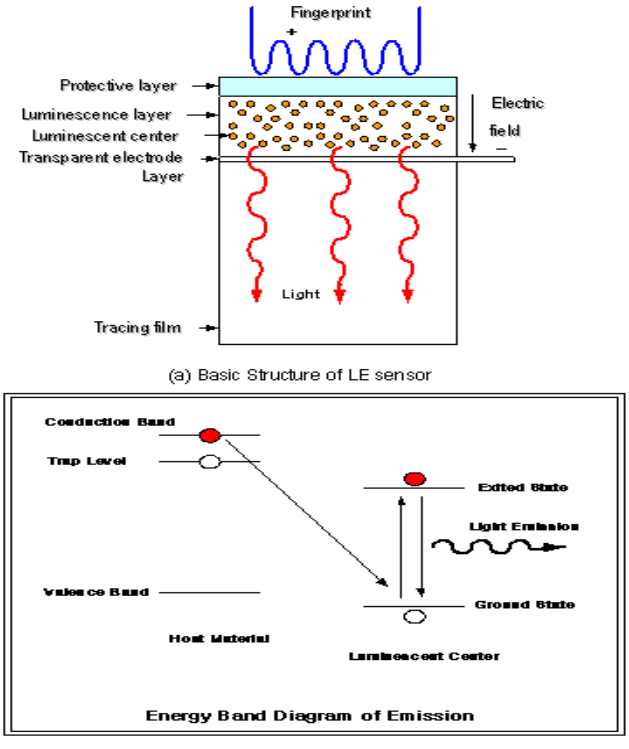
برآمدگی پوست انگشت که در تماس با سنسور می باشند، فوتون آزاد شده و به این ترتیب اثر انگشت ثبت می گردد.




[Fig. 1] Emitting Method of LE sensor

**شکل 6: شناسایی محل های برآمدگی اثر انگشت بوسیله سنسور LE**

در شکل زیر اصول اولیه این روش آمده است.




(a) Basic Structure of LE sensor

(b) Energy band diagram

[Fig. 2] Principle Emission of LE sensor at half cycle

**شکل 7: نحوه عملکرد سنسور LE با استفاده از نمودار نوار انرژی**

امروزه اسکنر هایی که برای ارتباط با کامپیوتر طراحی شده اند، به راحتی اطلاعات تصویراثر انگشت را تهیه و از طریق درگاه های کامپیوتر در اختیار نرم افزارهای مربوطه قرار می دهند

**نحوه استخراج ویژگی ها**:

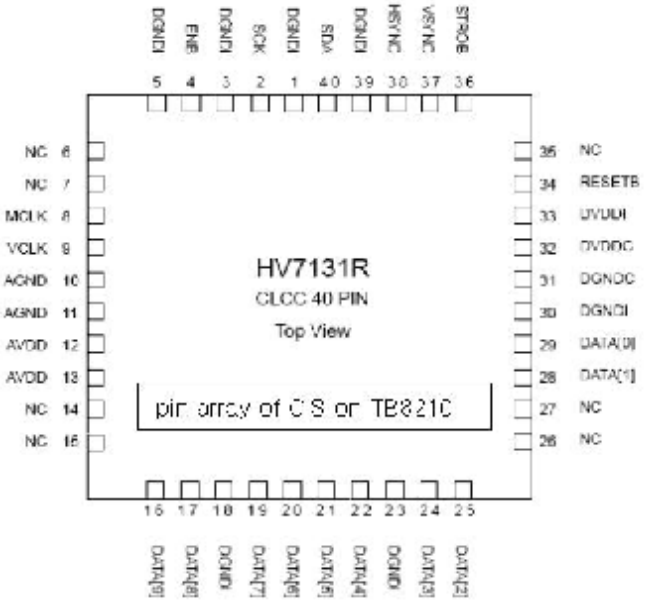
در اکثر سیستم ها از روشهای ساختاری که بر مبنای مینوتا هستند برای استخراج ویژگی ها استفاده می شود. در این سیستم ها در ابتداپیش پردازشهای اولیه ای مانند یکنواخت کردن هیستوگرام، تشخیص برآمدگی ها و نازک کردن آنها روی تصویر اعمال میگردد. سپس با استفاده از روشهای زیر به استخراج ویژگی ها و شناسایی اثر انگشت مبادرت می ورزند:

1 – روش فازی

2- روش شبکه های عصبی

3- ساختن گراف مربوطه به هر تصویر با استفاده از میدان جهت دار و الگوریتم راتا

پیاده سازی این روشها یا با استفاده از کامپیوتر انجام گرفته و یا از مدارات مجتمعی که به همین منظور ساخته شده است، انجام می گیرد. نمونه ای از مدارات مجتمع در شکل 11 آمده است:

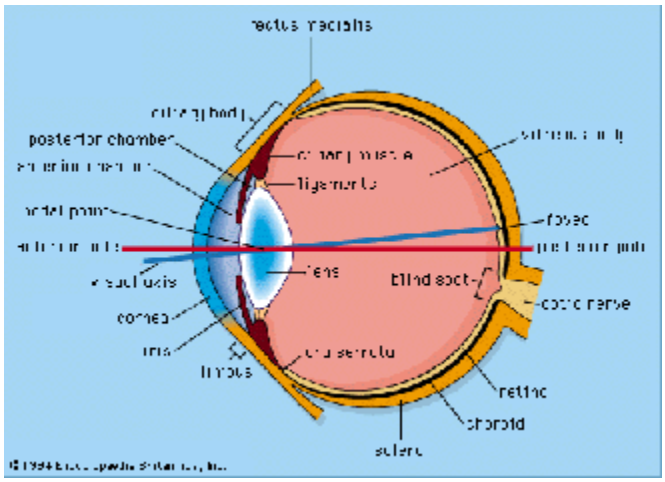



**شکل 8: نمونه ای از مدارات مجتمع برای پردازش اطلاعات اثر انگشت به دست آمده ازسنسور**

## آناتومی و یکتایی شبکیه

نسبت شبکیه و چشم همانند  نسبت فیلم به دوربین میباشد. شبکیه از بافت های گیرنده ای است که از لایه های مختلفی تشکیل شده است. همچنین شبکیه از میلیونها گیرنده نوری تشکیل شده است که عملکرد آنها عبارت است از جمع آوری اشعه های نوریی است که به آن فرستاده می شود و تبدیل این نورها به پالسهای الکتریکی  است که با عبور از عصب نوری به مغز رسیده و در آنجا این پالسهای الکتریکی به تصویر تبدیل می شود. دو گونه مختلف گیرنده های نوری در شبکیه وجود دارند، گیرنده های میله ای و گیرنده های مخروطی. گیرنده های مخروطی که تقریبا 6 میلیون از آنها وجود دارند در دیدن رنگهای مختلف به ما کمک کرده و گیرنده های میله ای که تقریبا 125 میلیون از آنها وجود دارند در دید در شب و محیط پیرامون به ما کمک می کنند. این الگوی رگهای خونی موجود در شبکیه است که تشخیص هویت از این طریق قرار گرفته است.

شکل زیر نشان دنده موقعیت شبکیه است. همانطور که مشاهده می شود قرنیه در جلوی چشم قرار گرفته است و شبکیه در انتهای چشم قرار دارد. به علت اینکه شبکیه در مکانی درون چشم قرار گرفته است و در مقابل محیط خارج از چشم نیست به عنوان یک روش تشخیص هویت پایدار قلمداد می شود.




**شکل 9 نشان دهنده شمای نزدیکی از الگوی رگهای خونی درون چشم می باشد.**

خطهای قرمز نشان دهنده رگهای خونی و قسمت زرد رنگ نشان دهنده مکان دیسک نوری(مکانی است که عصب نوری به شبکیه متصل می گردد و اطلاعات در این مکان از چشم به مغز ارسال می شود) است. دایره ای که در شکل وجود دارد مکان است که توسط دستگاه برای استخراج ویژگی اسکن شده است.

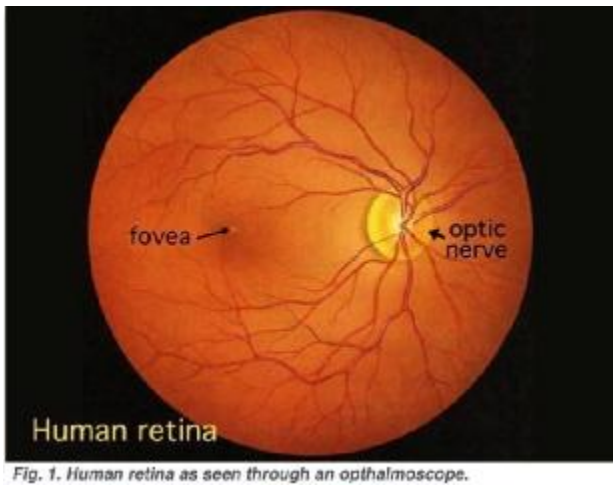


Fig. 1. Human retina as seen through an opthalmoscope.

## تکنولوژی دستگاههای اسکن

دستگاه های اسکن شبکیه از 3 بخش عمده تشکیل شده اند:

1- **قسمت تصویر برداری و پردازش سیگنال**:

این بخش شامل دوربینی جهت تصویر برداری و سپس تبدیل تصویر اسکن شده از شبکیه به فرمت دیجیتال می باشد.

2- **قسمت تطبیق دهنده**:

این بخش شامل یک سیستم کامپیوتری اعتبارسنجی و تشخیص هویت استفاده کننده می باشد.

3- **قسمت نمایش دهنده**:

در این بخش ویپگی های یکتای شبکیه به صورت یک قالب نمایش و ذخیره می شود.

قسمت اخذ تصویر و بخش پردازش آن مشکلترین بخش برای انجام بصورت کاملا صحیح می باشد و به این دلیل است که شخص مورد نظردر طی انجام این پروسه باید همکاری کامل داشته باشد.

استفاده کننده ابتدا باید چشم خود را در مقابل لنز دستگاه اسکن شبکیه در فاصله بسیار نزدیک قرار دهد. در این هنگام بسیار مهم است که برای اخذ تصویری خوب شخص کاملا بی حرکت روبروی دستگاه قرار گیرد. همچنین استفاده کننده باید هرگونه عینکی که به چشم دارد را قبل از اخذ تصویر برداشته تا از انعکاس نور توسط عینک و یا لنز و تداخل آنها با سیگنالهای شبکیه جلوگیری شود.

در این لحظه استفاده کننده از درون لنزمتوجه نور سبز رنگی که درون پشت زمینه سفید قرار دارد خواهد شد. هنگامی که دستگاه فعال می شود، نور سبز در درون مسیر دایره ای رنگ شروع به حرکت می کند و تصویری از شبکیه از درون مردمک چشم تهیه می کند. معمولا 3 تا 5 تصویر از شبکیه گرفته می شود. با توجه به همکاری استفاده کننده این مرحله می تواند بیشتر از 1 دقیقه به طول کشد. که نسبت به اخذ و پردازش تصویر روشهای دیگر تشخیص هویت زمان بسیار زیادی به حساب می آید. این زمان برای دستگاه اسکن قرنیه تقریبا برابر 2 ثانیه می باشد.

در مرحله استخراج ویژگی های منحصر به فرد مزیت روش شبکیه در این است که فاکتورهای ژنتیکی تایین کننده الگوی شبکیه نیستند. این موضوع باعث می شوند که شبکیه دارای ویژگی های منحصر به فرد قوی باشد. از شبکیه تا 400 نقطه منحصر به فرد اطلاعاتی می توان استخراج کرد که نسبت به اسکن اثر انگشت که 30 تا 40 نقطه است بسیار روش دقیقتری است.

در مرحله تولید قالب، ویژگی های استخراج شده منحصر به فرد از الگوی رگهای خونی شبکیه اساس تشکیل این قالب می باشند که 96 بایت می باشد. لذا یکی از کوچکترین قالب های تشخیص هویت در نظر گرفته  می شود. این حجم برای دستگاه اسکن قرنیه بین 256 تا 512 بایت می باشد.

## منابع خطاها

مشکلات متفاوتی می توانند در اخذ تصویری دقیق از شبکیه نقش داشته باشند و لذا درعدم تشخیص دقیق نقش داشته باشند. در زیر به تعدادی از این خطاها اشاره شده است:

1- عدم همکاری شخص استفاده کننده با دستگاه. هر گونه حرکت از سمت استفاده کننده در مرحله اخذ تصویر می تواند باعث خطا شود.

2- عدم رعایت فاصله مشخص شده توسط دستگاه.

3- لنز کثیف دستگاه اسکن شبکیه.

4- تداخل نوری توسط محیط خارجی

5- ابعاد مردمک استفاده کننده. روشنایی زیاد محیط باعث کاهش نوزی می شود که از طریق مردمک به شبکیه و بالعکس می شود. این امر باعث افزایش تعداد عدم پزیرش توسط دستگاه می شود.

## استانداردهای عملکردی روشهای تشخیص هویت

تمامی دستگاههای تشخیص هویتی توسط یک سری معیارهای استانداردی مقایسه می شوند. در زمینه تصویر شبکیه دو معیارقابل بررسی هستند و عبارتند از:

1- ضریب عدم تشخیص اشتباه:

نسبت به تمامی استانداردهای قابل بررسی، روش شبکیه از این استاندارد بیشترین تاثیر را می پذیرد. بدین علت که فاکتورهای زیادی در کیفیت تصویر نقش دارند و در صورت عدم کیفیت مناسب دچار خطای عدم پذیرش اشتباه می شود.

2- نسبت توانایی بررسی:

این استاندارد بیانگر احتمال تمام افرادی است که توسط سیستم اسکن شبکیه در روز می توانند مورد بررسی قرار گیرند. برای روش شبکیه این نسبت برابر مقدار کم 85% است. که عمدتا مربوط به نگرانی استفاده کنندگان از دستگاه اسکن شبکیه و اسکن از فاصله بسیار نزدیک است.

## مزایا و معایب تشخیص هویت از طریق شبکیه

همانند سایر روشهای تشخیص هویت این روش نیز به نوبه خود دارای معیب و مزایایی می باشد.تعدادی از مزایای این روش در زیر آمده است:

- الگوی رگهای خونی شبکیه به ندرت در طی دوران زندگی تغییر می کنند. به غیر از مواردی که افراد دچار بیماری چشمی می شوند مانند اب مروارید ،...
- حجم قالب اصلی 96 بایت است که بسیار کوچک است و باعث کاهش زمان در انجام مراحل بررسی و تشخیص هویت نسبت به قالبهای بزرگتر می شود که ممکن است باعث افزایش زمان انجام این پروسه شود.
- تا حدود 400 نقطه دارای ویژگی های منحصر به فرد را می توان از الگوی رگهای خونی شبکیه به دست آورد.
- شبکیه درون چشم قرار دارد و در مقابل صدمات محیط خارجی مصون است.

**معایب عمده این روش عبارتند از:**

- تهدید سلامت چشم، این شایعه وجود دارد که اسکن از شبکیه باعث تخریب چشم می شود.
- عدم راحتی استفاده کننده به علت نزدیکی زیاد لنز با چشم.
- میزان انگیزه شخص استفاده کننده، بر خلاف روشهای دیگر کیفیت یکس گرفته شده بستگی مستقیم با میزان همکاری شخص دارد.
- استفاده کننده باید عینک و یا لنز چشمی خود را بردارد.
- در حال حاضر دستگاههای اسکن شبکیه بسیار گرانقیمت هستند.

# فصل دوم

## باز شناسی  هویت با استفاده از عنبیه

در سال 1936 چشم پزشکی به نام frank Burch پیشنهاد تشخیص افراد از طریق الگوی قرنیه را عنوان کرد. اما تا سال 1985 بود که توسط دو چشم پزشک بنامهای Leonard Flom و Aran Safir این مطلب بیان شد که قرنیه های افراد مختلف کاملا با هم متفاوت است. ودر سال 1987 موضوع تشخیص هویت از طریق قرنیه افراد به نام آنها ثبت شد. در 1993 سازمان دفاع هسته ای برای ساخت و آزمایش اولین دستگاه تشخیص هویت از طریق الگوی قرنیه آغاز به کار کرد که این طرح در سال 1995 کاملاً موفقیت آمیز به انجام رسید.

کوششهای بشر برای تعبیه ابزار مکانیکی قابل اطمینان جهت شناسایی خصوصیات رفتاری و فیزیولوژیکی اشخاص، تاریخچه ای بس طولانی و رنگین دارد. به طور مثال در دوران ویکتوریا با الهام از پیدایش جرم شناسی و میلی که برای شناسایی زندانیان وتبهکاران وجودداشت، سرفرانسیس گالتون فهرست های مختلفی از خصوصیات برجسته صورت تهیه کرده بود. همچنین وی تعدادی انتخاب کنندگان خودکار مکانیکی برای اندازه گیری خصوصیات صورت تهیه کرده و یک آزمایشگاه اندازه گیری خصوصیات بدن انسان در کنزینگتون جنوبی تاسیس نموده بود تا بر اساس سیستم پزشک فرانسوی به نام آلفونس برتیلون هر یک از مجرمین را در یکی از 81 طبقه ای که او ایجاد کرده بود قرار دهد. از دیگر مشخص کنندگان خصوصیات فیزیولوژیکی و رفتاری که در طول تاریخ به کارگرفته شده اند میتوان ابعاد جمجمه، طول انگشت، اندازه گیری خصوصیات مختلف  هندسی صورت و غیره را نام برد.

امروزه نیاز به وسایل قابل اطمینان، سریع وغیر تهاجمی برای تشخیص خودکار هویت اشخاص به شکل قابل توجهی وجود دارد. تکنیک های کامپیوتری که برای شناسایی ویژگیهای افراد مانند صورت، اثر انگشت، شبکیه، صوت، هندسه کف دست، چشم و غیره به کار می روند، کاربردهای فراوانی در زمینه های امنیتی، نظارتی و مالکیت دارند. اما بسیاری از روشهای موجود توانائیهای محدودی در

زمینه شناسایی ویژگیها در موارد عملی و واقعی دارند؛ برخی از روشها مستلزم تماس با بدن شخص می‌باشند، برخی به صورت تهاجمی عمل می‌نماید، تعدادی از روش‌ها مستلزم تنظیم نهایی توسط یک شخص می‌باشند و برخی دیگر از آنها هزینه های بالایی دارند. روشی که اخیراً بیشتر از سایر روش‌ها مورد توجه قرار گرفته است، شناسایی افراد از روی خصوصیات موجود در عنبیه آنهاست.

ایده استفاده از الگوهای عنبیه برای شناسایی افراد ابتدا توسط چشم پزشکی به نام فرانک برچ در سال 1936 پیشنهاد شد. در دهه 1980 این ایده در یکی از فیلمهای جیمزباند به نام Never Say Never Again ظاهر شد و بدین طریق به افکار عمومی راه یافت، اما در آن زمان هنوز به عنوان حدس و افسانه علمی باقی مانده بود. در سال 1987 دو چشم پزشک دیگر به نامهای آرن سفیر و لئونارد فلوم این ایده را ثبت نموده و در سال 1989 از جان داگمن (که در آن زمان در دانشگاه هاروارد به تدریس مشغول بود) خواستند تا برای خلق الگوریتمهای واقعی برای شناسایی افراد بر اساس عنبیه کوشش نماید. الگوریتمهایی که داگمن در سال 1994 به ثبت رساند، پایه ای برای تمامی سیستمها امرزوی شناسایی افراد بر اساس عنبیه می‌باشد.

الگوریتمهای داگمن به شرکت تکنولوژیهای Iridian تعلق گرفته است و فعالیت بر روی آن تحت امتیاز کمپانی‌های متعدد دیگر در آمده است که به عنوان سیستمهای کامل کننده و پیشرفت دهنده شناسایی افراد بر اساس عنبیه عمل می‌نماید. در سالهای اخیر محصولات متعددی برای بدست آوردن تصاویر عنبیه از فواصل مشخص و کاربردهای متنوع توسعه داده شده اند. در سال 1996 یک سیستم تصویر برداری فعال که توسط مجوز شرکت Sensar توسعه داده شده بوداز دوربین‌های خاصی برای بدست آوردن تصاویر عنبیه در فاصله تا یک متر استفاده می کرد. این سیستم تصویر برداری فعال در ماشینهای خودپرداز در آزمایشهای عملی موفقیت آمیزی توسط دو کمپانی به نامهای NCR وِDiebold در کشورهای متعددی در طول سالهای 1999-1997 کار گذاشته شد.

یک وسیله تصویر برداری کوچکتر جدید و کم هزینه، Authenticam، دوربینی دیجیتالی برای استفاده دستی، رومیزی، تجارت الکترونیکی و دیگر کاربردهای امنیتی اطلاعات می باشد. برای ایمنی فیزیکی، دوربینی با متمرکز کننده و تنظیم کننده خودکار به نام IrisAccess برای کنترل مدخل و درب ورودی ساختمان توسط شرکت زنجیره ای کره‌ای به نام Ticketless air travel توسعه داده شد. روشهای ایمنی و کنترل ورودی بر پایه باجه های شناسایی افراد براساس عنبیه در فرودگاهها توسط شرکت Eye Ticket توسعه داده شده است. سیستمهای دیگری که الگوریتمهای شناسایی افراد بر اساس عنبیه را در خود جای می‌دهند توسط شرکتهای Oki ، LG و Panasonic در حال توسعه می‌باشند.

پیش‌بینی می شود که شناسایی افراد بر اساس عنبیه در محدوده وسیعی از کاربردهایی که شناسایی افراد در آنها می بایست ایجاد شده و یا تصدیق گردد، گسترش یابد. این ایده، کنترل گذرنامه، تجارت الکترونیکی، خدمات درمانی، پرداخت‌های استحقاقی، حق دستیابی به اطلاعات ویژه، اختیارات، خدمات دولت، کاربردهای نیروی انتظامی و قانونی، سفر هوایی، ورود به کامپیوتر و یا هر تعامل دیگری که درآن شناسایی شخصی بر دارائی یا رمز خاصی(کلیدها، کارت ها، مدارک، کلمات عبور، شماره های شناسایی فردی) تکیه می کند، را شامل می‌گردد.

برای الگوریتمهای شناسایی افراد بر اساس عنبیه، مدال و جایزه IT جامعه کامپیوتر انگلستان در سال 1997 به داگمن تعلق گرفت. تکنولوژی توسط شورای طرح انگلستان در سال 1998 به محصول هزاره دوم تخصیص داده شد و در طول سال 2000 میلادی در گنبد هزاره استفاده گردید. این سیستم همچنین در نمایشگاه سال 2000 در هانوفر آلمان به نمایش گذاشته شد. در حال حاضر کمپانی‌ها در کشورهای متعدد این الگوریتمها را در انواع مختلف محصول به کار می‌برند.

## کاربردهای شناسایی افراد بر اساس عنبیه:

برخی کاربردهای ممکن شناسایی افراد بر اساس عنبیه عبارتند از:

- ورود به کامپیوتر؛ به عنوان یک رمز عبور زنده.

- کنترل مرزهای ملی؛ عنبیه به عنوان یک گذرنامه زنده.

- پرداخت هزینه تلفن بدون استفاده از پول نقد، کارت و یا شماره های شناسایی شخصی.

- دستیابی مطمئن به ماشین خودپرداز در بانک.

- سفر هوایی بدون بلیط.

- کنترل دستیابی به اموال(خانه، اداره، آزمایشگاه و غیره).

- گواهینامه‌های رانندگی و دیگر مدارک شخصی.

- موارد قانونی، شناسنامه، یافتن گمشده یا اشخاص تحت تعقیب

- اعتبار سودها و القاب

- سندیت کارتهای اعتباری

- گشودن قفل اتومبیل و جلوگیری از سرقت.

- ضد تروریسم (مانند بازرسی افراد مشکوک در فرودگاهها).

- معاملات مالی ایمن(تجارت الکترونیکی، بانکداری).

- ایمنی اینترنت؛ کنترل دستیابی به اطلاعات ویژه

- کلید بیومتریک به صورت رمز در آمده برای پنهان ساختن وآشکار نمودن پیامها.

- هر استفاده موجود از کلیدها، کارت‌ها، شماره‌های شخصی و یا کلمات عبور.

در حال حاضر بعضی از شرکت‌های استفاده کننده این الگوریتمها عبارتند از:

- شرکت Iridian Technologies ایالات متحده آمریکا

- شرکت LG کره

- صنایع الکتریکی OKI ژاپن

- شرکت NCR انگلستان

- شرکت Diebold ایالات متحده آمریکا

- جامعه The Nationwide Building انگلستان

مزایا و معایب عنبیه برای شناسایی افراد:

**برخی از مزایای عنبیه برای شناسایی افرادعبارتند از**:

- از اعضاء داخلی بسیار محافظت شده چشم است.

- قابل دید از خارج است؛ الگوهایی که می‌توانند از یک فاصله تصویر شوند.

- الگوهای عنبیه از 244 درجه آزادی برخوردار هستند.

- منحصر به فرد بودن به دلیل پیچیدگی ترکیبی

- تغییر اندازه مردمک طبیعی بودن فیزیولوژی را تایید می‌نماید

- دارای ساختار شکل گرفته قبل از تولد(ماه هفتم از دوران بارداری).

- الگوهای عنبیه قابلیت نفوذ ژنتیکی محدود دارند

- الگوهای در طول دوران زندگی پایداری می‌باشند

- به رمز در آوردن وتصمیم‌گیری روی تصاویر عنبیه مشکل نیست.

**برخی از معایب عنبیه برای شناسایی افراد عبارتند از**:

- کوچک بودن هدف(یک سانتیمتر) برای دستیابی از فاصله‌ای حدود یک متر

- متحرک بودن هدف

- قرار گرفتن عنبیه در پشت سطحی منعکس کننده، مرطوب و منحنی

- تاثیر مژه ها، عدسی‌ها و انعکاسات بر روی آن.

- عدم وضوح تصویر به دلیل فروافتادگی پلک‌ها.

- تغییر شکل غیرارتجاعی به دلیل تغییرات اندازه مردک

- تابش نباید مرئی یا روشن باشد.

**علم عنبیه**:

یک اعتقاد مشهور در مورد تغییرات سیستماتیک درظاهر عنبیه وجوددارد که مطابق آن عنبیه قادر است سلامتی ارگانهای مختلف بدن، خلق و یا شخصیت فرد را معلوم سازد. اشخاص شاغل و ماهر در تفسیر نمود الگوهای عنبیه برای تشخیص سلامتی، شخصیت و مهارتهای درونی آیریدولوژیست نامیده می‌شوند. علم عنبیه در کشور رومانی و ایالت کالیفرنیا متداول‌تر از دیگر نقاط می‌باشد.

سه نوع تغییر در ظاهر عنبیه از نظر علمی می‌تواند وجود داشته باشد:

1) در اولین ماههای زندگی پوششی از سلولهای کروماتوفور در لایه‌های قدامی عنبیه رنگ چشم را مشخص می‌سازد.

2) گزارش شده است که برخی معالجات دارویی برای درمان بیماری گلوکما(آب سیاه) که درگیر پروستوگلاندین هستند، ملنین و در نتیجه تجمع رنگدانه‌های بافت عنبیه را تحت تاثیر قرار می‌دهند. البته این تغییرات رنگ عنبیه به روشهای شناسایی عنبیه ارتباطی پیدا نمی‌کند زیرا تصویر برداری از عنبیه با دوربینهای مونوکروم و با تابش مادون قرمز در باند 700-900nm صورت می‌گیرد که ملنین تقریباً غیر جاذب این طول موجهاست.

3) در چشم افراد مسن گاهی یک حلقه سفید عنبیه را محاصره می‌نماید.

**خصوصیات بیومتریک ژنتیکی و اکتسابی**:

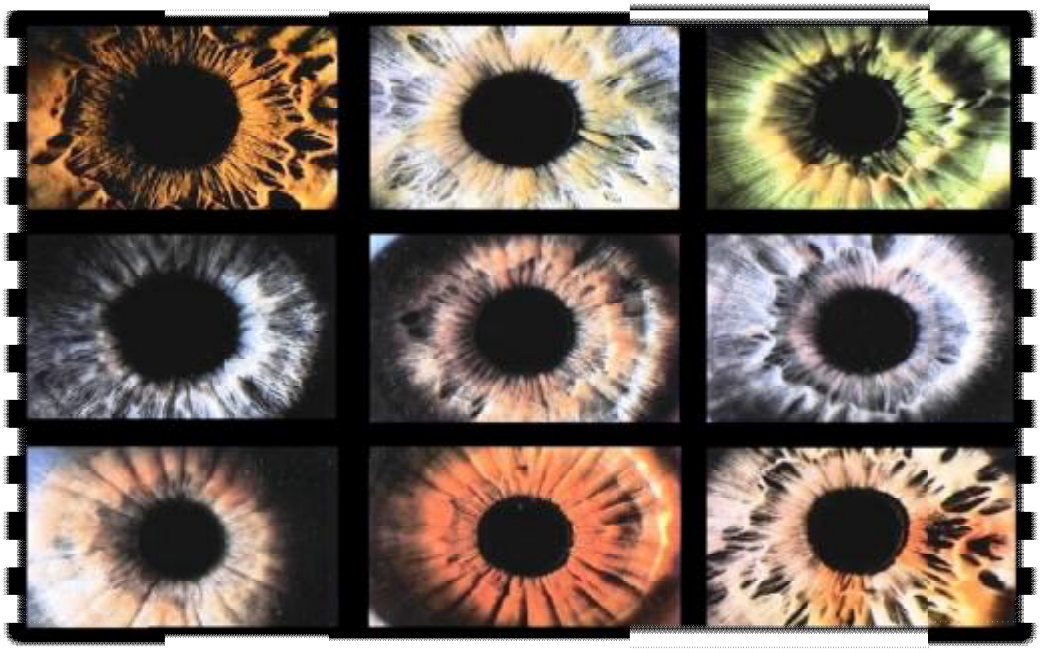
خصوصیات ژنتیکی به ساختمان ژنتیکی و یا اشتراک یک گروه در یک خصوصیت گفته می‌شود وخصوصیات اکتسابی به تجلی حقیقی یک ویژگی به واسطه تعامل با نوع ژنتیکی و محیط اطراف گفته می‌شود. نفوذپذیری ژنتیکی قابلیت توارث عوامل مختلف را توضیح می‌دهد. در این بحث به خصوصیاتی مانند گروه خون و توالی DNA ویژگیهای ژنتیکی و به اثر انگشت و الگوهای عنبیه

ویژگیهای اکتسابی ژنتیکی ثانویه گفته می‌شود. اشخاصی که از نظر ژنتیکی مساوی هستند دارای خصوصیات ژنتیکی برابر مانند خصوصیات جنسیت، گروه خون، نژاد و توالی DNA هستند. بعضی از خصوصیات مانندسیمای کلی صورت هم فاکتور ژنتیکی(شبیه به نظر رسیدن دوقلوهای مساوی) و هم فاکتور ژنتیکی ثانویه(تغییر ظاهر صورت به مرور زمان) را آشکار می‌سازند. اهمیت این خصوصیات بیومتریک این است که دو نوع خطای پایه را تحت تاثیر قرار می‌دهند: تطابق نادرست و رد نادرست. میل به ویژگیهای بیومتریکی که به مرور زمان تغییر می‌کنند(مانندصورت) می‌نیمم نرخ خطای رد نادرست را ایجاد می‌کند که به آن نرخ خطای بیومتریک اکتسابی هم گفته می‌شود.

**مقایسه بین الگوهای عنبیه مساوی از نظر ژنتیکی**:

اگر چه شباهت دوقلوهای مساوی ناشی از نفوذپذیری ژنتیکی ظاهر صورت است مقایسه بین عنبیه-های مساوی نشان می‌دهد که بافت عنبیه یک ویژگی اکتسابی ژنتیکی ثانویه است نه یک ویژگی ژنتیکی. یک مثال ساده برای عنبیه‌های مساوی ژنتیکی، چشم راست وچپ هر شخص می‌باشد که رابطه ژنتیکی مساوی دارند.

رنگ چشم ناشی از خصوصیات ژنتیکی است ولی جزئیات بافت عنبیه حتی در جفتهای مساوی ژنتیکی، مستقل و ناهمبسته است. بنابراین روش شناسایی با عنبیه مانند سایر روشهای شناسایی مثل شناسایی چهره، DNA و غیره به وسیله نرخ تولد دو قلوهای مساوی و یا وجود روابط ژنتیکی محدود نمی‌شود. شکل (11) تفاوتهای موجود در بافت عنبیه افراد را به خوبی نشان می‌دهد.



**شکل (10) تفاوتهای موجود در بافت عنبیه افراد**

## باز شناسی  هویت از طریق چهره

یکی ازروشهای مورد بررسی برای تعیین هویت انسان، بازشناخت چهره توسط کامپیوتر می‌باشد، که معمولا با عنوان شناسایی چهره و یا بازشناخت چهره بیان می‌گردد. در باز شناخت تصویر یک چهره تصویر ورودی با توجه به اطلاعات موجود در بانک اطلاعات، مورد شناسایی قرار می‌گیرد. این بانک شامل مشخصاتی از تصویر چهره افراد شناسایی شده می‌باشد. بازشناخت چهره استفاده‌های فراوانی در شناسایی بزهکاران، کارتهای اعتباری، سیستمهای امنیتی و موارد متعدد دیگر داشته و بدلیل کاربردهای فراوان، در سال‌های اخیر، مورد توجه قرار گرفته است. این بازشناخت چهره در تصویر دردو مرحله انجام می‌شود:

1- موقعیت و حدود چهره یا چهره ها، در تصویری که دارای اشیاء و زمینه های مختلف است، مشخص می شود

2- از چهره مشخص شده در تصویر، ویژگی‌های لازم استخراج شده و بازشناخت انجام می‌شود. که از جمله آن مشخص کردن اجزاء چشم و تعیین حالت و موقعیت آنها می‌باشد.

کارهای انجام شده برای استخراج خصوصیات از تصویر بر روی دو نوع تصویر (تصاویر تمام رخ و نیمرخ) بوده است و بدلیل اینکه تصاویر نیمرخ حاوی اطلاعات کمتری از تصاویر تمام رخ است، بررسی‌های انجام شده، بیشتر بر تصاویر تمام رخ متمرکز شده است. در دهه‌های اخیر روشهای متعددی برای باز شناخت چهره پیشنهاد شده است، ولی به دلیل مشکلاتی رسیدن به این هدف به طور کامل میسر نشده است.

**مشکلات اساسی در بازشناخت**:

اساساً اختلاف و تنوع زیاد در چهره افراد به گونه‌ای است که نمی‌توان چهره‌ها را در دسته‌ها وگروههای مشخصی طبقه‌بندی کرد. علاوه بر آن، ممکن است تغییراتی شبیه بلندی یا کوتاهی موی سر و صورت یا نحوه مرتب کردن آن و نیز تغییر سن باعث تغییر چهره گردد. در ضمن ممکن است، تغییر در چهره به دلیل شرایط تصویر برداری باشد. این شرایط می‌تواند شامل تغییرات در شدت نور و نیز چگونگی قرار گرفتن (زاوه و چرخش چهره) یا زاویه تصویر برداری از چهره باشد، که به هر صورت، باعث مشکلات اساسی در باز شناخت تصویر چهره می‌گردد. به دلایل ذکر شده، استخراج ویژگی‌های ثابتی از یک چهره، که با ویژگی‌های استخراج شده از تصویر یک شخص با تغییر شرایط تصویربرداری تغییر می‌کند، و گاهی نیز بر عکس آن ویژگی استخراج شده از چهره اشخاص متفاوت (به دلیل شباهت و تعدد چهره‌ها)، بسیار شبیه بوده و در باز شناخت تصویر مشکل آفرین می‌گردد.

**روشهای استخراج خصوصیات از چهره**:

در سالهای اخیر روشهای مختلفی برای استخراج ویژگیهای مهم وموثر جهت شناسایی چهره، مورد بررسی قرار گرفته است، این روش‌ها به سه دسته کلی تقسیم‌بندی می‌شوند:

### الف- ویژگیهای ظاهری

ویژگی‌های ظاهری شامل مختصات اجزاء چهره، مانند چشم‌ها، بینی، حلقه‌ها، بافت‌ها ونواحی مختلف چهره می‌باشد که همان خصوصیات ظاهری چهره هستند. در استخراج این خصوصیات از تصویر محدودیت‌های فراوانی وجود دارد. این روش در فصل سوم مورد بررسی قرار گرفته است.

### ب- ویژگیهای جبری

هر تصویر می‌تواند بصورت یک ماتریس تلقی شده و سپس عملیات جبری و تبدیلات ریاضی مختلف بر روی آن اعمال گردد. ویژگیهای جبری، حاصل این فرایند بود و عموما نشانگر خواص ذاتی یک تصویر می‌باشد. ازعملیات مهم بر روی ماتریس تصویر، تحلیل مولفه‌های اساسی (تبدیل PCA) می-باشد. این تبدیل یکی از روشهای مهم برای استخراج ویژگیهای جبری از تصویر چهره می‌باشد، که بر مبنای بردارهای ویژه ماتریس کواریانس بنا نهاده شده است. بردارهای ویژه ماتریس، بیان کننده توزیع جبری ماتریس وثابت‌های هندسی بوده و می‌تواند برای استخراج ویژگی از تصویر بکاربرده شود.

از دیگر روشهای جبری، روش تجزیه مقادیر منفرد SVD می‌باشد. می‌توان نشان داد که تجزیه مقادیر منفرد ماتریس یکی از روشهای موثر برای استخراج ویژگی ازماتریس تصویر است. تجزیه مقادیر منفرد در فشرده‌سازی و پردازش سیگنال نیز مورد استفاده قرار می‌گیرد.

روش تجزیه مقادیر منفرد و تحلیل مولفه‌های اساسی در فصول چهار و پنج مورد بررسی قرار گرفته-اند.

### ج- ویژگیهای آماری نقاط تصویر

با توجه به دو بعدی بودن تصاویر و در نظر گرفتن نقاط تصویر به صورت داده‌های آماری، می‌توان از مشخصات آماری نقاط، برای توصیف تصویر استفاده کرد. در این روش معمولا از خصوصیاتی استفاده می‌شود که دارای توانائی کافی برای توصیف تصویر بوده وضمن غنای اطلاعاتی، از پایداری خوبی نیز

برخوردار باشد. یکی از روش‌های آماری مهم استفاده از روش خود بستگی موضعی با درجه بالا می-باشد که در فصل ششم مورد بررسی قرار گرفته است.

ویژگیهای استخراج شده از تصویر بصورت بردار در نظر گرفته می‌شود. اگر بردارهای استخراج شده از تصاویر دارای ابعاد زیادی باشند، باید کاهش بعد داده شوند تا جداپذیری و طبقه‌بندی کلاس‌ها بهتر گردد. روش کاهش بعد و جداپذیرتر کردن کلاسها نیز در فصل دوم ارائه شده است.

## روش اخذ تصاویر و تهیه بانک تصویر

تعداد افراد قابل بازشناخت را روش مورد استفاده در استخراج ویژگی از تصویر و دقت لازم برای بازشناخت تعیین می‌کند و هر قدر روش استخراج ویژگی از چهره کاراتر باشد، می‌توان تعداد بیشتری افرادرا مورد شناسایی قرار داد. اما عموما در تمام روشهای موجود، باز شناخت برای تعداد محدودی از افراد انجام می‌گیرد.

تصاویر چهره دارای ابعاد 128*128 نقطه بوده و هر نقطه توسط یک بابت بیان می‌گردد. به عبارتی تصاویر دارای 256 سطح روشنایی می‌باشند. فاصله دوربین تا چهره تصویربرداری شده تقریبا ثابت در نظر گرفته شده است و اختلاف در فاصله تصویر برداری از افراد، حداکثر 40 سانتیمتر می‌باشد. البته برای تصاویر گرفته شده از یک شخص، این تقریب به 20 سانتیمتر محدود می‌شود.

در مورد شدت نور تصاویر و تغییرات نور در تصویربرداری، چون تصاویر در روزهای مختلفی گرفته شده، نور تمامی تصاویر دقیقا یکسان نیست. اما برای تصاویر گرفته شده از یک نفر، به دلیل اینکه تصاویر در یک محیط ثابت ودر فاصله زمانی کم گرفته شده است، تغییرات نور کم بوده ومی‌توان از آن صرف نظر کرد(در گرفتن تصاویر از نور فلاش استفاده شده است).

دسته تصاویر مربوط به یک نفر، شامل تصویر چهره در حالت تمام رخ، چرخش چهره به اطراف، چشمهای بسته، لبخند و حالتهای مختلف چهره می‌باشد. درتهیه بانک تصویر سعی شده از انواع چهره و افراد مختلف استفاده شود.

پس از تهیه بانک تصویر، از تصاویر اشخاص موجود در بانک تصویر، ویژگیها استخراج شده وکاهش بعد داده می‌شوند. واضح است که ویژگیهای استخراج شده و کاهش بعد یافته، در بانگ دیگری، که بانک ویژگیهای استخراج شده نامیده می‌شود، ذخیره می‌گردد.

**تغییرات اعمال شده بر روی تصاویر**:

هدف پروژه شناسایی یک چهره است.بنابراین در مرحله اول این شناسایی که پروژه فعلی بر اساس آن تعریف گشته است، از مرحله تفکیک که چهره را از میان اجزاء دیگر موجود درتصویر منفک می‌نماید صرف نظر می‌گردد. این موقعیت مشابه با وضعیتی است که فردی به یک در بسته نزدیک می‌شود و قرار است قبل از رسیدن به در مورد شناسایی قرار گیرد. دوربین از چهره وی تصویر برداری کرده تا بازشناخت را بوسیله سیستم انجام دهد، سپس دستورات بعدیمثلا باز شدن در ورودی انجام شود، دراین حالت تصاویر پشت سر فرد می‌تواندسفید در نظر گرفته شود. این محدودیت در تعریف بازشناخت باعث می‌گردد که در تصویر برداری از چهره محدودیتهای اعمال گردد. از جمله این محدودیتها ثابت بودن زمینه تمام تصاویر می‌باشد، لذا پس از تصویر برداری زمینه تصویر سفید و اطلاعات اضافی از قبیل شانه‌ها و گردن تا حد ممکن حذف میگردد. واضح است هر قدر اطلاعات اضافی وناخواسته در تصویر چهره کمتر باشد، ویژگی استخراجی دارای پایداری بیشتری می‌باشد.

**مدل سیستم بازشناخت**:

برای بازشناخت یک تصویر ورودی، ابتدا از تصویر بردار ویژگی استخراج می‌شود(باید ویژگی استخراج شده، با روش استخراج ویژگی از تصاویر موجود در بانک ویژگی مطابقت داشته باشد). سپس بردارهای استخراجی کاهش بعد داده می‌شود. در کاهش بعد جداپذیری کلاس‌ها و طبقه‌بندی آنها بهتر میگردد. سپس ویژگی دسته موجود دربانک ویژگی مشخص می‌شود. حال یکی از دسته‌های موجود در بانک ویژگی انتخاب شده، باید مشخص کرد که آیاتصویر ورودی متعلق به همین کلاس است(شخصی که ویژگی‌های موجود دربانک متعلق به آن شخص است) یا اینکه تصویر ورودی اصلا در بانک تصاویر

نبوده وکاملا جدید است. لذا یک سطح آستانه برای فاصله و متناسب با ضریب اطمینان لازم برای باشناخت تصویر جدید بکار برده شده و به این صورت عمل می‌گردد که اگر فاصله بردار ویژگی استخراج شده از تصویر جدید تا نزدیکترین بردار ویژگی موجود در بانک، در حد قابل قبولی بود، تصویر جدید متعلق به آن کلاس تشخیص داده می‌شود. و در غیر اینصورت تصویر جدید قابل شناسایی(باز شناخت) نمی‌باشد. اگر برای ویژگی مربوط به فردی که تصویر ورودی متعلق به وی است. در بانک باشد و باز شناخت انجام نشود. به این معنی است که ویژگی‌های استخراجی از تصویر جدید، با ویژگی استخراجی از تصاویر آموزشی متفاوت است.

با تغیر تصویر چهره یک شخص ویژگی‌های استخراجی تغییر می‌کند، اما اگر روش استخراجی به گونه‌ای باشد که تغییرات در تصویر فرد، تاثیر زیادی بر بردار ویژگی مربوط به وی نداشته باشد. ویژگی استخراجی موثرتر و پایدارتر بوده و می‌توان حالت‌های متفاوت‌تری از چهره را مورد باز شناخت قرار داد.

## پارامترهای مهم در تعیین نرخ بازشناخت:

نرخ باز شناخت در تمامی روش‌های موجود، به چند عامل مهم وابسته است، که به آنها اشاره می‌شود:

### الف- اندازه تصاویر چهره

هر چند تصاویر بزرگتر باشند، حاوی اطلاعات بیشتری از چهره بوده واین فراوانی اطلاعات در بردار استخراجی نیز صدق می‌کند، ولذا طبقه‌بندی و جداپذیری کلاسها بهتر انجام گرفته و نرخ بازشناخت افزایش می‌یابد. البته اگر تصاویر بزرگ و تعداد آنها زیاد باشد، حجم و حافظه زیادی برای پردازش و نگهداری تصاویر، لازم خواهد بود.

**ب- تغییرات تصاویر آموزش هر شخص**

اگر تغییرات تصاویر آموزشی در هر کلاس کم باشد، تغییرات بردار استخراجی و تداخل بین کلاسها کمتر بوده و نرخ شناسایی افزایش می‌یابد. اما باید توجه داشت که در این صورت، حالت‌های محدودی از چهره (شبیه تصاویر آموزشی) قابل بازشناخت خواهد بود.

**ج- تعداد اشخاص (کلاسها) در بانک تصاویر**

با افزایش تعداد کلاسها، تداخل بین کلاس‌ها بیشتر شده و از جداپذیری آنهاکاسته می‌گردد ونرخ شناسایی نسبت به تعداد کمتر کلاسها، پایین می‌آید.

**د- بکار بردن سطح آستانه**

با بکار بردن سطح آستانه، برای فاصله کلاسها می‌توان فاصله کلاسها می‌توان دقت و نرخ بازشناخت را افزایش داد و این دقت را برای هر شخص(کلاس) به مقدار دلخواهی تعیین کرد، اما باید توجه کرد که با افزایش دقت در بازشناخت، تنوع چهره در بازشناخت کاهش می‌یابد.

در این تحقیق روشهای موجود برای بازشناخت چهره مورد بررسی قرار گرفته و کارایی و توانایی آنها در بازشناخت چهره مقایسه شده است.

# فصل سوم

## باز شناسی  هویت از طریق گفتار

باز شناسی گفتار یکی از مهمترین مباحث تحقیقات گفتاری است که در طول پنج دهه گذشته، یعنی از زمانی که چنین تحقیقاتی در اوایل دهه 50 میلادی آغاز شد، پیشرفتهای زیادی داشته است.

فرایند بازشناسی گوینده[1] که در اینجا به شاخه عمومی مسائلی از قبیل تعیین هویت گوینده[2]، تصدیق گوینده[3] و طبقه بندی گوینده اطلاق می شود، اولین بار توسط آتال[4] در این زمینه مطرح شد. این اولین قدم در معرفی این زمینه تحقیقاتی بود که البته در ابتدا از موفقیت کمی برخوردار بود.

تعیین هویت گوینده به این صورت تعریف می شود که از میان N مدل گوینده مرجع، آن مدل گوینده ای که نزدیکترین و بیشترین شباهت را به گوینده نا مشخصی ورودی دارد پیدا می کند. از آنجایی که الگوهای گفتار با تک تک مدلهای مرجع مقایسه می شوند و همچنین از آنجایی که برای هر تصمیم گیری نادرست احتمال معینی برای هر مقایسه وجود دارد، بنابراین واضح است که احتمال تصمیم گیری کلی تابعی از N بوده و در نتیجه هر چه تعداد مدل ها بیشتر باشد احتمال خطا یا تصمیم گیری نادرست در تعیین هویت گوینده بیشتر می شود.

مسئله تصدیق گوینده به این صورت مطرح می شود که گفتار یک هویت گوینده نامشخص و مدل گوینده ای که وی ادعا می نماید داده شده است و بایستی مشخص شود که آیا گفتار این گوینده به اندازه کافی به مدل گوینده ادا شده شباهت دارد یا نه. بنابراین در این حالت تعداد مقایسه یکی است و معمولاً مستقل از تعداد جمعیت مدل مرجع است.

در یک تقسیم بندی، بسته به اینکه مدلی که برای شناسایی مورد آزمون قرار می گیرد جزو مدلهای مجموعه باشد یا نباشد، دو تعریف زیر ارائه می گردد:

---

[1] Speaker Recognition
[2] Speaker Identification
[3] Speaker Verification
[4] Atal

1- تعیین هویت در مجموعه بسته: که در این حالت مدل مورد آزمون جزو N مدل موجود در شبکه می باشد.

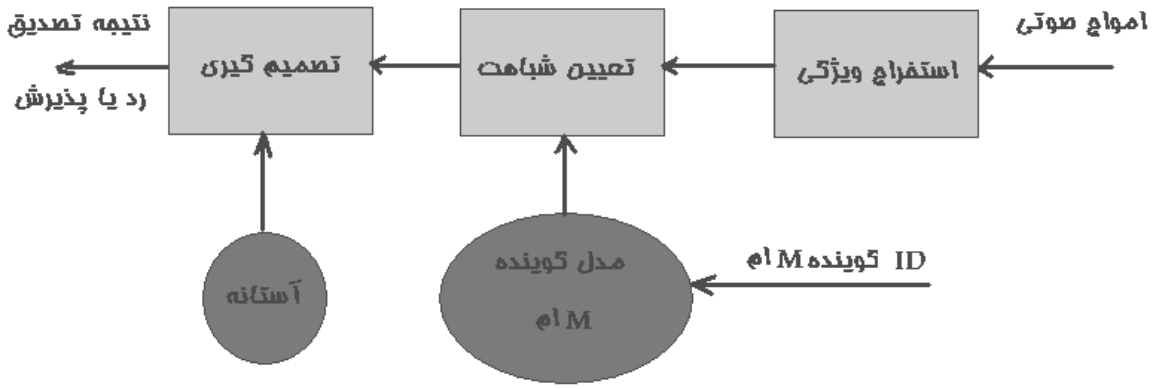
2- تعیین هویت در مجموعه باز: که در این حالت گفتار ورودی نامشخص متعلق به هیچ کدام از اعضای مدلهای گویندگان مرجع موجود در سیستم نمی باشد.

در سیستم های تعیین هویت در مجموعه باز نتایج خروجی N+1 حالت می باشد که N تعداد مدلهای مرجع است. در واقع در این نوع سیستم، ترکیبی از دو نوع سیستم تعیین هویت مجموعه بسته و تصدیق هویت می باشد. دراین سیستم ابتدا نزدیکترین مدل به گفتار ورودی پیدا شده و سپس صحت تعلق گفتار ورودی به آن مدل مورد بررسی قرار می گیرد. بنابراین کارایی این سیستم نسبت به تعیین هویت مجموعه بسته کمتر است.

تصدیق هویت گوینده راحتی و اطمینان بیشتری را برای بسیاری از فعالیتهای روزمره آدمی که نیاز به امنیت دارد ایجاد می نماید. این تکنولوژی بدلیل اینکهاز خصوصیات ذاتی موجود در صدای انسان استفاده می کند، در مقابله با مسئله تقلید و کلاه برداری بسیار مقاوم بوده و از لحاظ ویژگی بازشناسی هویت از راه دور نسبت به برخی روشها از جمله اثر انگشت کارایی بسیار بیشتری دارد.

## روشهای پیاده سازی سیستم های تصدیق گوینده:

شمای کلی یک سیستم تصدیق گوینده در شکل زیر آمده است:




**شکل11: شمای کلی یک سیستم تصدیق گوینده**

سیگنال گفتار گوینده به عنوان ورودی به سیستم انتقال داده می شود. سپس پیش پردازش و نهایتاً استخراج ویژگی ها بر روی آن اعمال می گردد و به این ترتیب به یک فضای جدید منتقل می گردد. ویژگی های استخراج شده از گفتار گوینده با مدل مرجع او مقایسه می شود. عمل مقایسه به این صورت انجام میگیرد که میزان شباهت یا اختلاف این ویژگی ها با مدل مرجع به دست می آید. میزان شباهت به دست آمده با میزان آستانه مقایسه می شود و با توجه به این مقایسه خروجی سیستم مبنی بر تعلق و یا عدم تعلق گفتار ورودی به گوینده ادعا شده مشخص می شود.

قبل از معرفی روشهای پیاده سازی سیستم، به بررسی نکاتی در طراحی سیستم های بازشناسی (اعم از تعیین هویت و یا تصدیق هویت) می پردازیم:

1- **انتخاب ویژگی ها**: برای استخراج ویژگی های گوینده بایستی چند عامل مد نظر قرار گیرد؛ از جمله: این ویژگی ها نبایستی به نویز محیط انتقال مانند کانال های مخابراتی حساس باشند، همچنین این ویژگی ها نبایستی به حالات روانی و فشار های محیط که گوینده در آن در حال صحبت کردن است وابسته باشد. در کل روش بهینه ای برای استخراج ویژگی ها وجود ندارد و معمولاً از طریق تجربه این عمل صورت می گیرد.

لازم به ذکر است که در بازشناسی گوینده از ویژگی های دینامیک که بستگی زیادی به حالات گوینده دارد استفاده می شود، در صورتی که در روشهای دیگر خصوصیات فیزیکی استاتیک و پایدار مورد بررسی قرار می گیرند. بنابراین یک سری محدودیتهای ذاتی در مورد استفاده از این سیگنالها وجود دارد. برای درک این محدودیتها بایستی اطلاعات تمایزدهنده گوینده ها و نحوه قرار گرفتن آنها در سیگنال گفتار مورد بررسی قرار گیرد. سیگنال گفتار از طریق حرکت اندامهای تولید گفتار بوجود می آید و توسط حنجره و سیستم عصبی کنترل می گردد. بنابراین دو منع اطلاعات گوینده در سیگنال صحبت وجود دارد یکی مربوط به خصوصیات فیزیکی و ساختاری مجرای گفتار و دیگری اطلاعات کنترلی از مغز و ماهیچه ها اندام گویایی است. این اطلاعات همراه با اطلاعاتی مربوط به

هنگام حرکت دادن مفصل های اندامهای تولید گفتار، وارد سیگنال صحبت می شود. در کل اطلاعات سیگنال گفتار را به دو دسته سطح بالا (مانند: لحن، محتوای گفتار و استیل گفتار یعنی طریقه استفاده گرامری و نحوی از کلمات) و سطح پایین (مانند: خصوصیات سیگنال گفتار از قبیل دامنه طیف، فرکانی گام واکدار، فرکانس فرمانت، پهنای باند و خصوصیات تناوبی گفتار واکدار) تقسیم بندی می کنند. اطلاعات سطح بالا عملاً در بازشناسی گوینده توسط انسان کاربرد داشته و در عوض سیستم های بازشناسی گوینده اتوماتیک از ویژگی های سطح پایین سیگنال استفاده می شود.

2- **مدل های گویندگان**: در سیستم های بازشناسی گوینده، مدل هر گوینده شامل خصوصیات آماری او است. معمولاً در مدل هی گویندگان از یکی از دو مدل پارامتری (مانند مدل گوسی) و غیر پارامتری (مانند مدل مراکز خوشه ها یا حالات چند گانه) استفاده می شود.

3- **طول گفتار آموزشی**: که با افزایش این زمان نتایج مطلوب تری حاصل می گردد.

4- **انتخاب گفتار مناسب**: پیشنهاد می گردد سکوت وبخشهای غیر گفتاری حذف گردد.همچنین گفتارهای کم انرزی و بی واک در تمایز بین گوینده ها کم اثر بوده و پیشنهاد می گردد که از اطلاعات مدل حذف گردند.

5- **محیط نویزی**: نویز پشت زمینه یک مشکل عمومی است و بهتر است برای تخمین آن از نویز پشت زمینه در زمان سکوت استفاده و با اعمال آن به مدل،تخمینی از مدل بدون نویز داشته باشیم.

6- **تنوع گوینده**: اغلب سیگنال گفتار یک شخص در حالت های خوشحالی، ناراحتی و خستگی متفاوت و به این ترتیب کارایی سیستم را کاهش می دهند.بنابراین خصوصیات آماری یک فرد ثابت نیست.

**معرفی برخی از روشهای بازشناسی گفتار**:

1- **روش پیچش زمانی**[5]: این روش زمانی مناسب است که تعداد افراد مورد بررسی کم باشند. اساس این روش بر پایه الگوریتم برنامه ریزی پویا و روش تطبیق الگو می باشد.

2- روش مدل مخفی مارکوف[6]: این روشی برای مدلسازی آماری فضای صوتی اکوستیکی گوینده می باشد. این مدل نسبت به مدل DTW کارا تر می باشد.

3- **روش شبکه های عصبی**

4- **روش فازی**

## باز شناسی هویت از طریق امضا

بر اساس فرهنگ لغات امریکایی، امضا اینگونه تعریف می‌شود:"اسم شخص که توسّط خود او نوشته شده باشد، عمل نشانه‌گذاری یک اسم".تعاریف دیگر امضا را متشکّل از مجموعه‌ای از حرکات سریع دست که نشانه‌گذاری روی کاغذ می‌شود می‌دانند. بر این اساس، مشخصات فرآیند نشانه‌گذاری سریع(از قبیل سرعت، فشار، خط سیر قلم و غیره)، برای هر شخص منحصر به فرد می‌باشد.در واقع ویژگی‌های این فرآیند از خواص ذاتی سیستم عصبی-عضلانی انسان، که حرکات یاد شده را تولید می‌کنند ، ناشی می‌شود.با آگاهی از عملکرد این سیستم که تشکیل شده از تعداد زیادی نورون و فیبرهای عضلانی می‌باشد و بر اساس تئوری حد مرکزی می‌توان گفت که پروفایل سرعت حرکت‌های تند و بر اثر عادت، به صورت مجانبی به سمت یک معادلهdelta-lognormal میل می‌کند.این امر در واقع پایداری خصویات امضا را تایید می‌کند.بنابراین امضا را می‌توان خروجی سیستمی که در فاصله زمانی معیّنی فعّال و مدل کننده فرد امضاکننده می‌باشد، در نظر گرفت .

روش‌های بازشناسی امضا به دو گروه عمده استاتیک(off-line) و دینامیک(on-line) تقسیم می‌شوند.

---

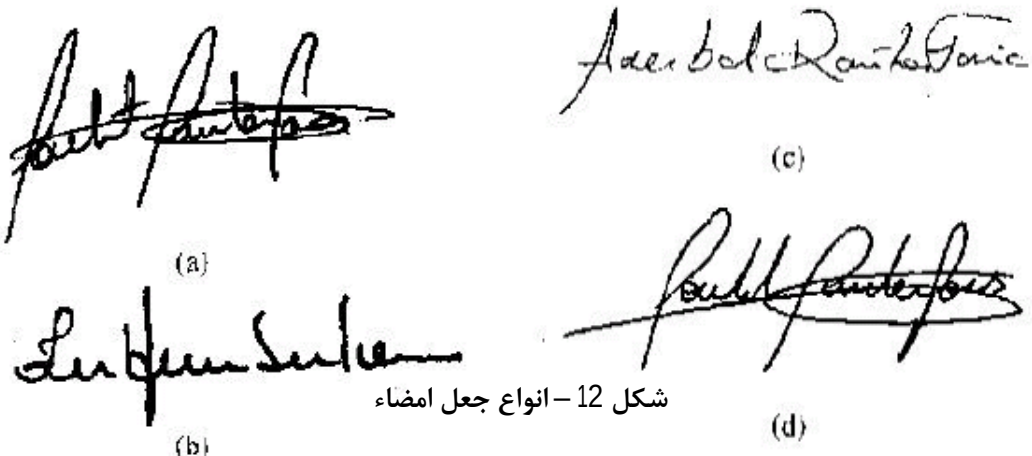
[5] Dynamic Time Warping
[6] Hidden Markov Model

روش استاتیک که بر اساس روش اوّل می‌باشد، امضا را به صورت یک تصویر دو بعدی در نظر می‌گیرد که محتوی هیچگونه اطلّاعات وابسته به زمانی نمی‌باشد.بر این اساس، خصوصیّات استاتیک امضا که نامتغییّر با زمان می‌باشند، برای بازبینی امضا به‌کار می‌روند.در نتیجه عمل بازشناسی امضا به یک فرآیند بازشناسی الگوی عادی تبدیل می‌شود.با توجّه با این نکته که تغییر در الگوی امضا امری اجتناب ناپذیر می‌باشد، فرآیند تصدیق و بازبینی امضا در این روش را می‌توان به تعیین و ترسیم محدوده تغییرات اصلی محدود کرد.

در مقابل، روش دینامیک از خصوصیات دینامیک فرآیند امضا کردن استفاده می‌کند.این روش شامل استخراج ویژگی‌هایی از اطلاعات ثبت شده فرآیند امضا و مقایسه آنها با ویژگی های امضای مرجع می باشد.

## انواع جعل امضا

هدف اصلی بازبینی امضا، تمایز امضای اصلی از امضای جعل شده می باشد.در واقع ابزارها و نتایج بازبینی به نوع امضای جعل شده بستگی پیدا می کند.انواع اصلی جعل امضا در شکل زیر مشاهده می شوند:




**شکل 12 – انواع جعل امضاء**

اولیّن نوع جعل که جعل تصادفی نام دارد(شکل b)، در واقع هیچگونه اطلّاعاتی راجع به امضای اصلی و یا اسم شخص حقیقی در بر نداشته و تنها نمونه ای تصادفی از شخص جعل کننده می باشد.نوع دوم

یا جعل ساده(شکل c) ، تقلیدی ساده از طرز شکل اسم شخص اصلی می باشد و نوع سوم یا جعل امضای تخصصی(شکل d)،تقلیدی هوشمندانه و مناسب از امضای شخص اصلی است.

هرکدام از روش های بازبینی in-line , off-line ، برای گونه خاصی از انواع جعل مناسب است . روش های off-line به طور معمول برای جعل امضاهای تصادفی و ساده به کار می روند ، چرا که این روش ها غالبا با فاکتورهای مربوط به شکل و قالب بندی امضا سروکار دارند و به علت فقدان اطلاعات زمانی و عدم توانایی در مدلسازی خط سیر دستنوشته، تمایز بین امضای اصلی و جعل های تخصصی در این روش مشکل است.

در مقابل برای بازبینی جعل امضاهای تخصصی، که از نظر ظاهری بسیار شبیه امضای اصلی می باشند، روش های on-line که از اطلّاعات زمانی امضا نیز بهره می برند مناسب می باشند.

**نگاهی به روش های استاتیک و دینامیک بازشناسی امضا**:

از میان روش های off-line که برای بازبینی امضا به کار می روند، می توان به موارد زیر اشاره کرد: تبدیل های دوبعدی، هیستوگرام اطلاعات جهت دار،بررسی انحنا، تصویرسازی افقی و عمودی رد امضا و محل یابی نقاط خاص در ساختمان امضا.

یکی از پیشتازان این عرصه ، Ammar در دهه 80 می باشد که از ایده بررسی آماری نقاط پررنگ برای شناسایی ویژگی های شبه دینامیک امضا استفاده کرد.به این معنی که سطح پررنگی و یا میزان خاکستری بودن به طور مستقیم با فشار قلم که یکی از خصوصیات فری هر امضا است بستگی دارد.

از روش های بازبینی دینامیک یا on-line می توان به روش های زیر اشاره کرد:

طبقه بندی کننده های احتمالاتی، time warping، شبکه های عصبی(ANN)، مدل های مخفی مارکف(HMM) ،روش های همبستگی سیگنال، روش های سلسله مراتبی ، فاصله های اقلیدسی و غیره.

در میان روش های مذکور، مدل های مخفی مارکف(HMM) با نرخ خطای کمتر از 1% بهترین نتیجه را در پی داشته است.

**انواع ویژگی های موجود در یک امضا**:

ویژگی های موجود در یک امضا ا می توان به سه گروه ویژگی های عمومی، ویزگی های اطلاعاتی شبکه ای و ویژگی های ساختاری دسته بندی کرد.

ویژگی های عمومی، ویژگی هایی هستند که به طور کلاسیک در مسائل بازشناسی الگو به کار می روند. این ویژگی ها، پس از نرمالیزه سازی و شالوده بندی تصویر امضا مورد استفاده قرار می گیرند.نمونه ای از این ویژگی ها در ادامه آمده است:

مرکز جرم در راستای قائم، مرکز جرم در راستای افق، حداکثر طول تصویر عمودی، حداکثر طول تصویر افقی، پیک های تصویر عمودی(تعداد ماکزیمم های محلی موجود در تصویر عمودی)، پیک های تصویر افقی، زوایای خمیدگی سراسری، زوایای خمیدگی محلّی،تعداد نقاط لبه ای، تعداد نقاط گذر و تعداد حلقه های بسته.

ویژگی های اطلاعاتی شبکه ای به این صورت محاسبه می شوند که تصویر به شبکه ای شامل 96 ناحیه مستطیلی(12*8) تقسیم شده و ویژگی های هر ناحیه به طور جداگانه بررسی می شود.

برای بدست آوردن ویژگی های ساختاری نیز باید از ماتریس وقوع همزمان تصویر امضا استفاده کرد.به عنوان نمونه،در تصاویر باینری، ماتریس های 2*2 توصیف کننده گذار نقاط سیاه و سفید در جهت و فاصله مربوطه می باشند.

**مزایا ومعایب** :

می توان گفت که یک سیستم تشخیص هویت بیومتریک به چهار عامل زیر وابسته است .

- مقبولیت در میان استفاده کنندگان
- صحت
- هزینه و زمان پیاده سازی
- سطح امنیتی مورد نیاز

در این میان روش بازشناسی امضا که در این قسمت مورد مطالعه قرار گرفته است ازمزیت مقبولیت گسترده در میان استفااده کنندگان بهره می برد که این امر به تاریخچه طولانی استفاده از امضا به عنوان عامل اعتبار یک سند مربوط می شود. یکی دیگر از مزایای این روش این است که بیشتر کامپیوتر های قابل حمل جدید از ورودی های دست نووشته ای بهره می برند و بنابر این نیاز به ابداع سیستم های سخت افزاری جدیدی برای جمع آوری اطلاعات نمی باشد. در عین حال باید بیان کرد که سیستم های باز شناسی محدودی وجود دارند که نرخ صحت کافی به همراه بازده مناسب را فراهم می سازند . در هر حال با اینکه باز شناسی امضا یکی از ایمن ترین روش های تشخیص هویت می باشد ، استفاده از آن در فهالیت های تجاری امروزه نیز مورد تایید است که دلیل اصلی همخوانی این روش با اصول قبلی تشخیص هویت پذیرفته شده در میان مردم می باشد.

**کاربردهای بیومتریک**

شناسایی مجرمان: برای شناخت و دستگیری مجرمان کافی است که آثار انگشتان آنها را با اطلاعات موجود در بانک اطلاعات مقایسه کرد.

دسترسی به اطلاعات سیستم ها: برای ورود به اطلاعات مهم و حیاتی هر سازمانی می توان از اسم رمز و نیز اسکن عنبیه به طور همزمان استفاده کرد.

دسترسی فیزیکی و حضور زمانی: در نسل جدید ساعت های حضور وغیاب، از روش های اسکن چهره استفاده می شود.

شناسایی شهروندان: برای شناسایی و ثبت مشخصات شهروندان می توان از انواع سامانه های بیومتریکی اشاره شده استفاده کرد.

تجارت الکترونیک: با استفاده از کارت های اعتباری و شناسه های بیومتریک از امنیت بالاتری نسبت به گذشته برخوردار شده است.

## مزایای فناوری های بیومتریک

1- غیر قابل حدس زدن

2- غیر قابل فراموشی و غیر قابل سرقت

3- سرعت و راحتی استفاده

4- عدم نیاز به هزینه های امنیتی جهت استفاده از نیروی انسانی

5- غیر قابل تقلب

6-امکان تعیین هویت اصلی و واقعی افراد

# فصل چهارم

## نتیجه گیری

فناوری های بیومتریک از جمله فناوری هایی به حساب می آیند که هزینه تمام شده نسبتاً بالایی دارند و بنابراین ممکن است برای افراد و یا سازمان های کوچک استفاده از آنها به صرفه نباشد. اما در یک مقایسه کلی تر، با توجه به امنیت بالای سیستم های بیومتریک نسبت به سیستم های سنتی مانند قفل و زنجیر و نگهبان و غیره شاید بتوان گفت که در دراز مدت استفاده از این فناوری برای سازمان ها به صرفه باشد و در مقابل نیز با توجه به تولید نسخه های جدید تر از این گونه سخت افزار ها و تولید انبوه آنها، صرفه جویی بیشتر شامل حال کاربران شود و قیمت آنها بسیار پائین تر بیاید.

درباره نواقص این سیستم ها نیز می توان عنوان کرد که با توجه به امنیت بالای آنها شاید پس از اتفاقی، خود شما هم نتوانید به حساب بانکی خود وارد شوید و پول برداشت کنید. آیا در آن لحظه هم نظرتان نسبت به فناوری های بیومتریک مثبت است

## منابع و ماخذ


1- http://biometrics.cse.msu.edu/fingerprint.html

2- http://www.diplodock.com

3- http://www.c3.lanl.gov

4- http://www.letsgodigital.org

5- http://www.nsf.gov

6- http://www.geomokit.com

7- http://www.abacus21.com

8- http://www.stormingmedia.us

9- http://www.ispeak.nl

10- http://www.cse.ogi.edu

11- http://www.speechpro.com