

وَاعْتَصِمُوا بِاللَّهِ هُوَ مَوْلَاكُمْ فَنِعْمَ الْمَوْلَى وَنِعْمَ النَّصِيرُ ﴿٧٨﴾ (حج)
و به پناه خدا روید او مولای شماست چه نیکو مولایی و چه نیکو یآوری

آشنایی با ابزار مانتورینگ تصویری و کنترل دسترسی و هشدار دهنده اماکن و سنسور و بیومتریک

مهندس یحیی نجفیان

CV

تایستان 1402

سیستم های مدار بسته

تاریخچه

امروزه در مراکز صنعتی و اداری جهت نظارت بر محیط فیزیکی و نظارت بر کارکنان یا کارگران در جهت کنترل و مدیریت بهتر و کارآمدتر به وفور از سیستمهای تلویزیونی مدار بسته (cctv) closed circuit TV استفاده می شود. این سیستمها به عنوان سیستمهای کنترل تصویری نیز نامیده می شوند. گاهی نیز از این سیستمها با مخفف (CCVE) تجهیزات ویدئویی مدار بسته یاد می شود. در محلهایی مانند بانکها - ادارات - دانشگاهها - کارخانجات - فروشگاههای بزرگ - فروشگاههای فروش اجناس گرانقیمت مانند طلافروشیها - در سوپرمارکتهای بزرگ و در کنترل ترافیک خیابانها و چهارراهها این سیستمها را میتوان نصب و مورد استفاده قرار داد.

لنز دوربين

لنز دوربین مداربسته

لنز دوربین مداربسته (CCTV Lens) به ترکیبی از عدسی ها گفته می شود که از آن برای تنظیم و ارسال نور محیط بر روی چپ تصویر استفاده می شود. لنز دوربین مداربسته از اصلی ترین جزء تجهیزات سیستم نظارتی است.

چپ تصویر چرا به لنز نیاز دارد؟

تصویر محیط بسیار بزرگ است، و چپ تصویر دوربین مداربسته معمولا اندازه ای کمتر از یک سانتیمتر مربع دارد. پس در صورتی که بخواهید یک تصویر را بدون لنز ثبت کنیم باید یک چپ تصویر به اندازه خود تصویر بسازیم. به دلیل این که این کار غیرممکن است از لنز استفاده می شود. لنز دوربین، کل نور محیط را دریافت کرده و در یک بخش متمرکز می کند، به این صورت تصویر کل محیط در یک فضای کوچک ساخته می شود.



لنز دوربین مداربسته سه مشخصه مهم دارد:

- فاصله کانونی لنز

- فاصله کانونی به فاصله بین لنز و سنسور تصویر زمانی که سوژه دوربین در فوکوس است، اشاره دارد. در واقع فاصله کانونی تعیین می کند که دوربین چقدر می تواند ببیند و اغلب بر حسب میلی متر بیان می شود. بسته به اینکه فاصله کانونی یک لنز چقدر است زاویه دید دوربین مدار بسته متفاوت خواهد بود.

- واحد اندازه گیری فاصله کانونی با میلیمتر بیان می شود. هر چه فاصله کانونی کمتر باشد، زاویه دید دوربین بیشتر بوده و برعکس هر چه فاصله کانونی بزرگتر، زاویه دید دوربین کوچکتر است. پس از طریق تغییر فاصله کانونی لنز، می توان زاویه دید تصویر را تغییر داد.



HIKVISION

WWW.Hikvision.Cent402



- انواع لنزها بر اساس ساختار کانونی

نوع ساختار کانونی لنزها می تواند بسیار متفاوت باشد. در دوربین های مداربسته معمولا لنزها از نظر فاصله کانونی به صورت زیر هستند:

- ثابت (Fix)
- تنظیم دستی (Vari-focal)
- تنظیم خودکار یا موتوردار (Motorized).



لنز ثابت:

لنزهای ثابت همیشه فاصله کانونی ثابتی دارند. این یعنی اینکه پس از نصب، زاویه دید دوربین ثابت است و نمی توان آن را تغییر داد. در کاربری های معمولی لنزهای ثابت به دلیل قیمت مناسب آن معمولا پرکاربردتر هستند.

لنزهای متغییر دستی:

لنزهای وریفوکال امکان تغییر فاصله کانونی به صورت دستی، آن هم در یک بازه مشخصی را دارند. لنز وریفوکال دارای زوم اپتیکال می باشند.

لنزهای وریفوکال موتوردار:

لنزهای موتوردار یا موتورایز را می توان از راه دور، فاصله کانونی شان را تغییر داد و اصطلاحا زوم دار هستند. این نوع لنزها به دلیل اینکه موتور در آنها تعبیه شده است معمولا نسبت به بقیه لنزها گرانتر است. ترجیحا این نوع لنزها برای محیط هایی که محدودیت نصب دارند بسیار پرکاربرد هستند.



مشخصه مرتبط با ضریب عبور:



در دوربین های مدار بسته معمولا خیلی وارد جزئیات فنی مرتبط با لنزها نمی شوند. همه مشخصه های فنی دیگر لنز به صورت مگاپیکسل آن نوشته می شود. مثلا لنزی که 3 مگا پیکسل است برای استفاده در دوربین هایی تا این رزولوشن مناسب است. اگر رزولوشن دوربین بالاتر باشد باید از لنز بهتری استفاده کرد.

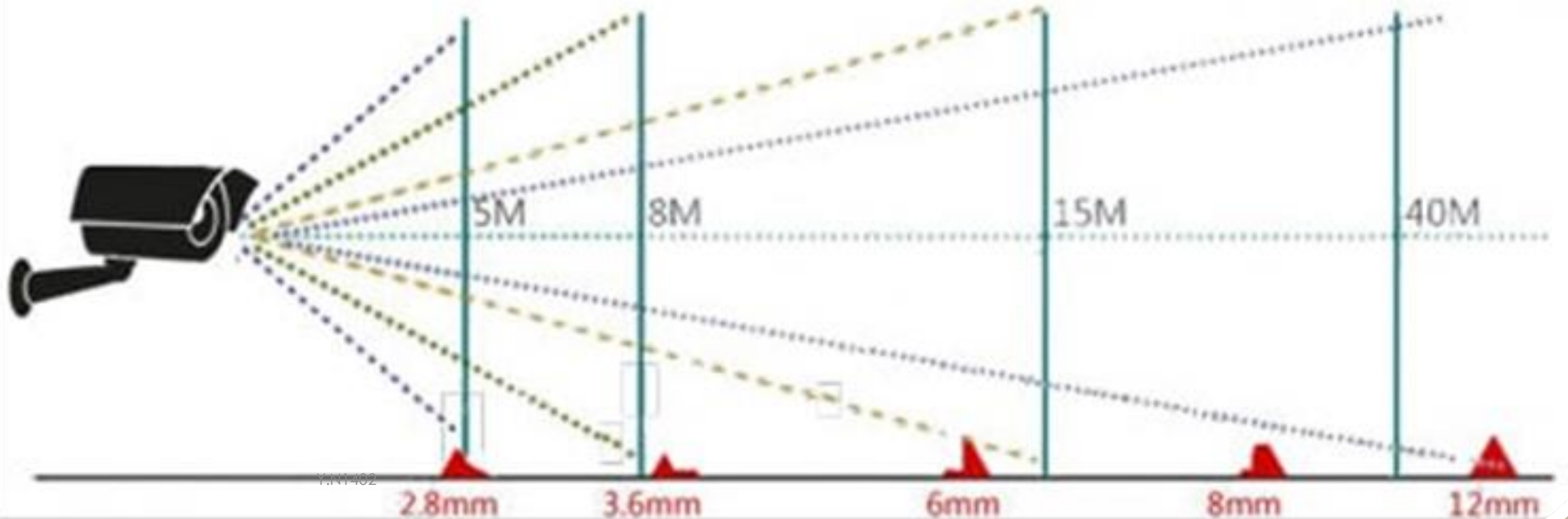


لنز خودکار دوربین مداربسته (Auto Iris) چیست؟

به منظور کنترل میزان نور عبوری از لنزهای Auto Iris (اتو ایریز)، استفاده می شود. هرچه نور بیشتر باشد، عدسی بسته تر خواهد شد و هر چه نور محیط کمتر شود، عدسی بازتر می شود تا نور بیشتری به روی تراشه تصویر برداری منتقل شود.

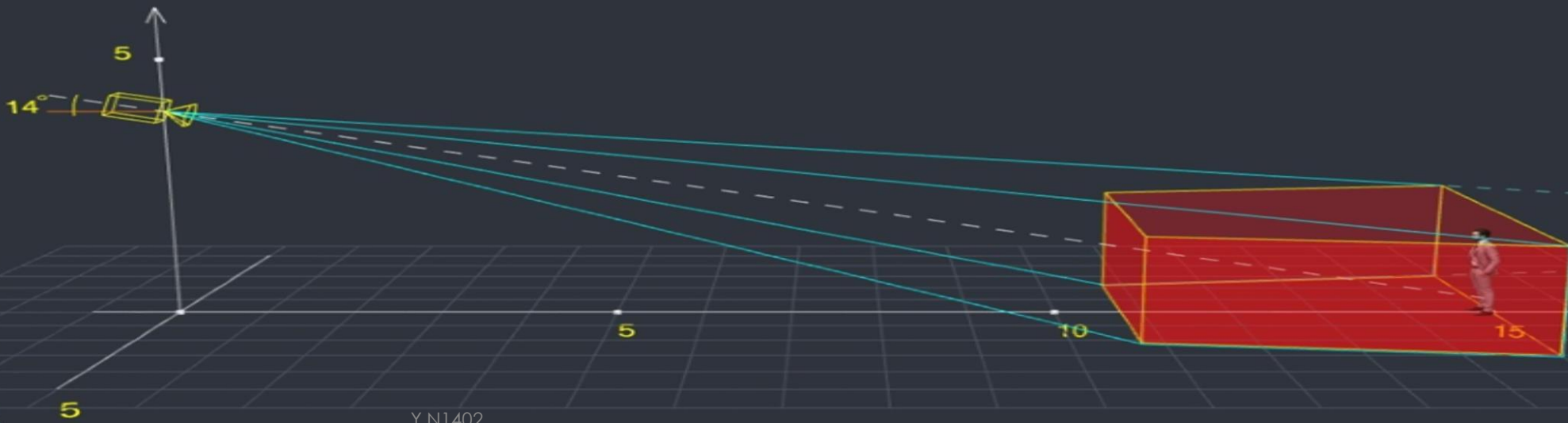
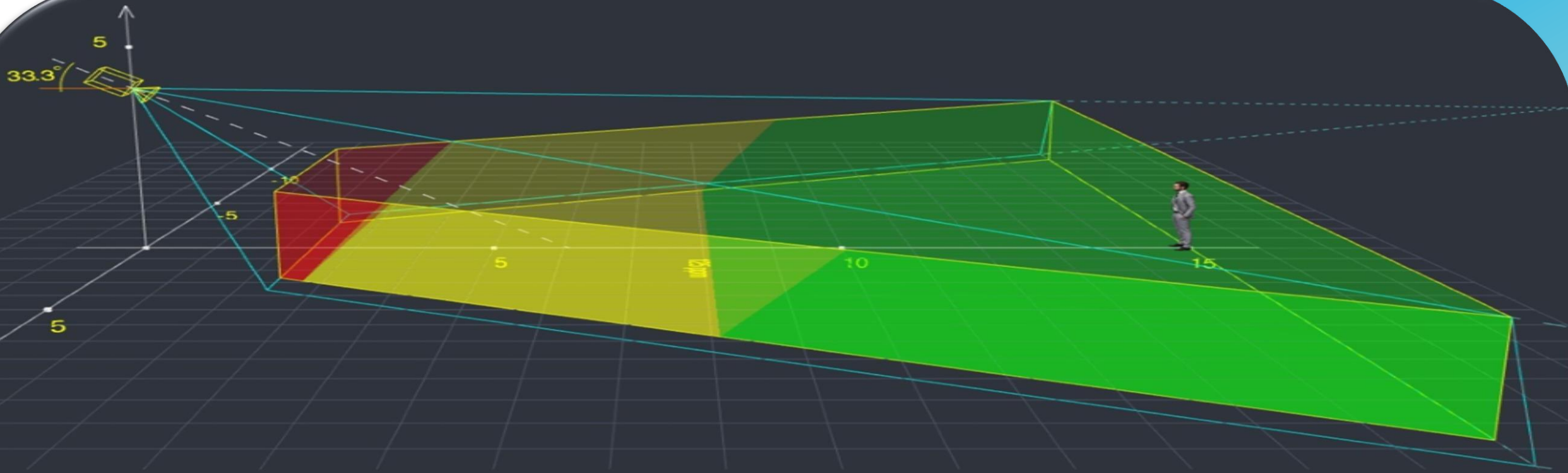
لنز دوربین مداربسته و زاویه دید آن

لنز دوربین مداربسته	2.8mm	3.6mm	6mm	8mm	12mm	16mm
زاویه دید	90°	69°	50°	33°	22°	18°
فاصله	3~5 M	8 M	15 M	20~30 M	40~50 M	70~80 M





تصویر اسلاید بعد تفاوت بین دو دوربین مداربسته با دو لنز واید و غیر واید را نشان می دهد. در بخش بالای تصویر دوربین مداربسته واید با لنز 2.8 است که فضای تحت پوشش آن از جهت جزئیات تصویر به سه بخش تقسیم شده است. بخش قرمز رنگ اشیاء به طور واضح دیده شده و قابل شناساییست. در محدوده زرد رنگ جزئیات اشیاء کمتر از محدوده قرمز قابل رویت است. در فضای سبز رنگ تصویر مقابل که وسعت زیادی را نیز در بر می گیرد دوربین نظارت کلی بر محیط را فراهم می کند. اما در بخش پایینی عکس، محدوده تحت پوشش دوربین مداربسته با لنز 12 به نمایش گذاشته است. طبق تصویر محدوده کمی از فضا تحت پوشش دوربین است اما همان محدوده را با جزئیات ارائه می کند.





HIKVISION

WWW.Hikvision.Center

Y.N1402

یکی از مهمترین قابلیت هایی که لنز دوربین مداربسته می تواند داشته باشد، قابلیت بزرگنمایی تصویر (زوم) است. لنز زوم جهت مشاهده بسیار مفید است. لنز زوم دوربین در دو نوع اپتیکال و دیجیتال می باشند. در زوم اپتیکال یا زوم واقعی کیفیت تصویر هنگام بزرگنمایی کاهش پیدا نمی کند. اما در زوم دیجیتال هنگام بزرگنمایی کیفیت کاهش خواهد یافت.

لنز 2.8 میلی متر زاویه ی دید بیشتری به نمایش می گذارد. اما در عوض جزئیات تصویر به خوبی در آن مشخص و واضح نیست. به بیان ساده تر اشیایی که در نقاط دورتری قرار دارند وضوح کمتری دارند.

لنزهای 12 میلی متری زاویه دید محدودتری دارند اما وضوح جزئیات تصاویر در آن بیشتر است. پس شما زاویه دید محدودتری دارد اما جزئیات بهتری خواهید دید.

دوربین

دوربین های صنعتی Box Cameras

این دوربین ها در مارک ها و نوع ها و قیمت های متفاوت در بازار موجود می باشد. اکثرا دوربین بدون لنز می باشد که لنز مربوطه بنا به نیاز باید تهیه و نصب گردد.

کیفیت دوربین از تعداد خط تصویر که ایجاد می کند مشخص می گردد. که به TVline گفته می شود که کیفیت های مورد قبول از TVL 350 شروع شده و بهترین کیفیت TVL 600 می باشد دوربین های فوق منهای سیستمی که در داخل آن وجود دارد که دیجیتال و یا آنالوگ باشد خروجی تصویر آنالوگ 75 hertz برای ما می دهد که سیگنال های تولید شده توسط کابل Coaxial (تصویر) به محل ضبط تصاویر انتقال داده می شود. برخی از دوربین های پیشرفته خود دارای منوی تنظیمات نیز می باشند که بصورت دیجیتالی روشنایی وضوح و رنگ و ... قابل تنظیم در دوربین نیز می باشد. البته این نوع دوربین ها به مراتب گرانتر می باشند.

این دوربین ها کاربرد زیادی دارند که در محیط های داخلی و تمیز از پایه کوچک دوربین و در محیط های بزرگ و بیرونی جهت محافظت از گرد و غبار و رطوبت داخل کاور قرار داده می شود. دوربین های جدید قابلیت دید در شب را نیز دارا می باشند دید در شب با علامت D/N نشان داده می شود. دید در شب به حالتی اطلاق میگردد که با حداقل نور و یا با کمک نور مادون قرمز (نامرئی) در محل های کاملاً تاریک قابلیت تصویر برداری را دارا می باشند (بصورت سیاه و سفید)



HIKVISION

WWW.Hikvision.Center

دوربین های سقفی Dome Cameras

این دوربین ها دارای محفظه شیشه ای جهت جلوگیری از گرد و غبار بصورت حبابی طراحی شده است این دوربین ها بر روی سقف نصب میگردند و در انواع مدل های معمولی و دید در شب در بازار موجود می باشد. از این دوربین ها در محیط اداری و منازل بیشتر کاربرد دارد. این دوربین ها ثابت بوده و قابل تنظیم بصورت 360 درجه افقی و 90 درجه عمودی می باشند. این دوربین ها نیز در کیفیت های متفاوتی در بازار موجود می باشد.



HIKVISION

WWW.Hikvision.Center

دوربین های مادون قرمز IR Cameras

این دوربین ها در انواع محیط ها کاربرد دارند از خصوصیات این دوربین ها به دید در شب بودن آنها می توان اشاره کرد و نیاز به لنز ندارند ... برخی از مدل ها قابلیت تنظیم لنز و زوم کردن سه برابر اپتیکال را نیز دارا می باشند ولی مدل های کوچک آن از قبل تنظیم شده می باشند. تعداد LED های موجود بر روی آن قدرت پروژکتور آن را نشان می دهد که حداکثر تا 30 متر را می توانند پوشش دهند ... این پروژکتور هیچ گونه نور مرئی (قابل دیدن نیست) ندارند ولی برای دوربین بسیار کاربرد دارد.

این دوربین ها بطور اتوماتیک در هنگام شب و یا تاریکی به حالت دید در شب سوئیچ می شوند و در روز و روشنایی بصورت رنگی تصاویر را نشان خواهد داد . این دوربین ها خود در برابر آب و خاک و گرد و غبار عایق می باشند و بطور پیش فرض نیازی به کاور محافظ ندارند منبع تغذیه این دوربین 12 ولت 2 آمپر و خروجی تصویر 75هرتز می باشد. این دوربین ها هم در کیفیت های متفاوتی در بازار وجود دارد. TVL 500 کیفیت خوبی می باشد.

به دید در شب بودن آنها می توان اشاره کرد و نیاز به لنز ندارند ... برخی از مدل ها قابلیت تنظیم لنز و زوم کردن سه برابر اپتیکال را نیز دارا می باشند ولی مدل های کوچک آن از قبل تنظیم شده می باشند. تعداد LED های موجود بر روی آن قدرت پروژکتور آن را نشان می دهد که حداکثر تا 30 متر را می توانند پوشش دهند ... این پروژکتور هیچ گونه نور مرئی (قابل دیدن نیست) ندارند ولی برای دوربین بسیار کاربرد دارد.

این دوربین ها بطور اتوماتیک در هنگام شب و یا تاریکی به حالت دید در شب سوئیچ می شوند و در روز و روشنایی بصورت رنگی تصاویر را نشان خواهد داد . این دوربین ها خود در برابر آب و خاک و گرد و غبار عایق می باشند و بطور پیش فرض نیازی به کاور محافظ ندارند منبع تغذیه این دوربین 12 ولت 2 آمپر و خروجی تصویر 75هرتز می باشد. این دوربین ها هم در کیفیت های متفاوتی در بازار وجود دارد. TVL 500 کیفیت خوبی می باشد.



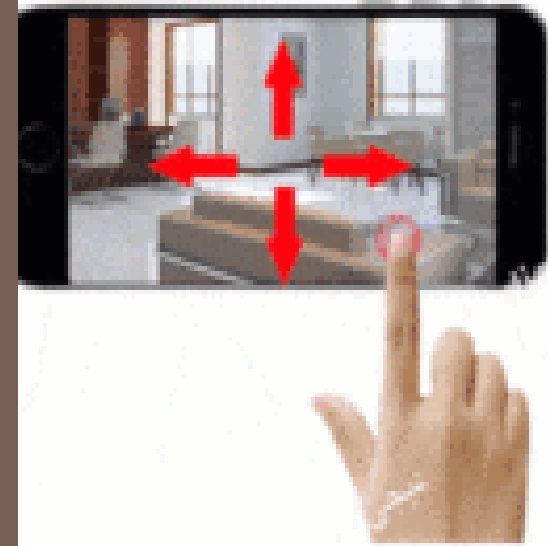
انواع دوربین های تحت شبکه:

➤ - دوربین های تحت شبکه ثابت

➤ Fixed Network Cameras

➤ این دوربین ها که شامل یک بدنه و یک پایه هستند از نظر شکل ظاهری شباهت بسیاری به دوربین های آنالوگ سنتی دارند. در بعضی از کاربرد ها دیده شدن دوربین و جهت دید آن امری مطلوب است. در چنین کاربردهایی بهترین گزینه استفاده از دوربین های ثابت است. مزیت دیگر این دوربین ها این است که اغلب آنها لنزهای قابل تعویض دارند و می توان لنز دوربین را متناسب با کاربرد آن انتخاب کرد.

➤ برای حفاظت از دوربینهای ثابت می توان از Housing و پوششش مناسب استفاده کرد.



-دوربین های تحت شبکه PTZ

این دوربینها قابلیت حرکت افقی ، عمودی و همچنین زوم اپتیک و دیجیتال بصورت کنترل دستی و اتوماتیک دارند. در حالت کنترل دستی، یک دوربین PTZ می تواند به عنوان مثال در یک محیط فروشگاهی برای تعقیب یک فرد مورد استفاده قرار گیرد این دوربینها جهت دید مشخص دارند و فاقد امکان حرکت 360 درجه کامل هستند و برای حرکت اتوماتیک دائمی ساخته نشده اند. زوم اپتیک این دوربینها معمولا بین 18 تا 26 برابر است.





دیجی وی



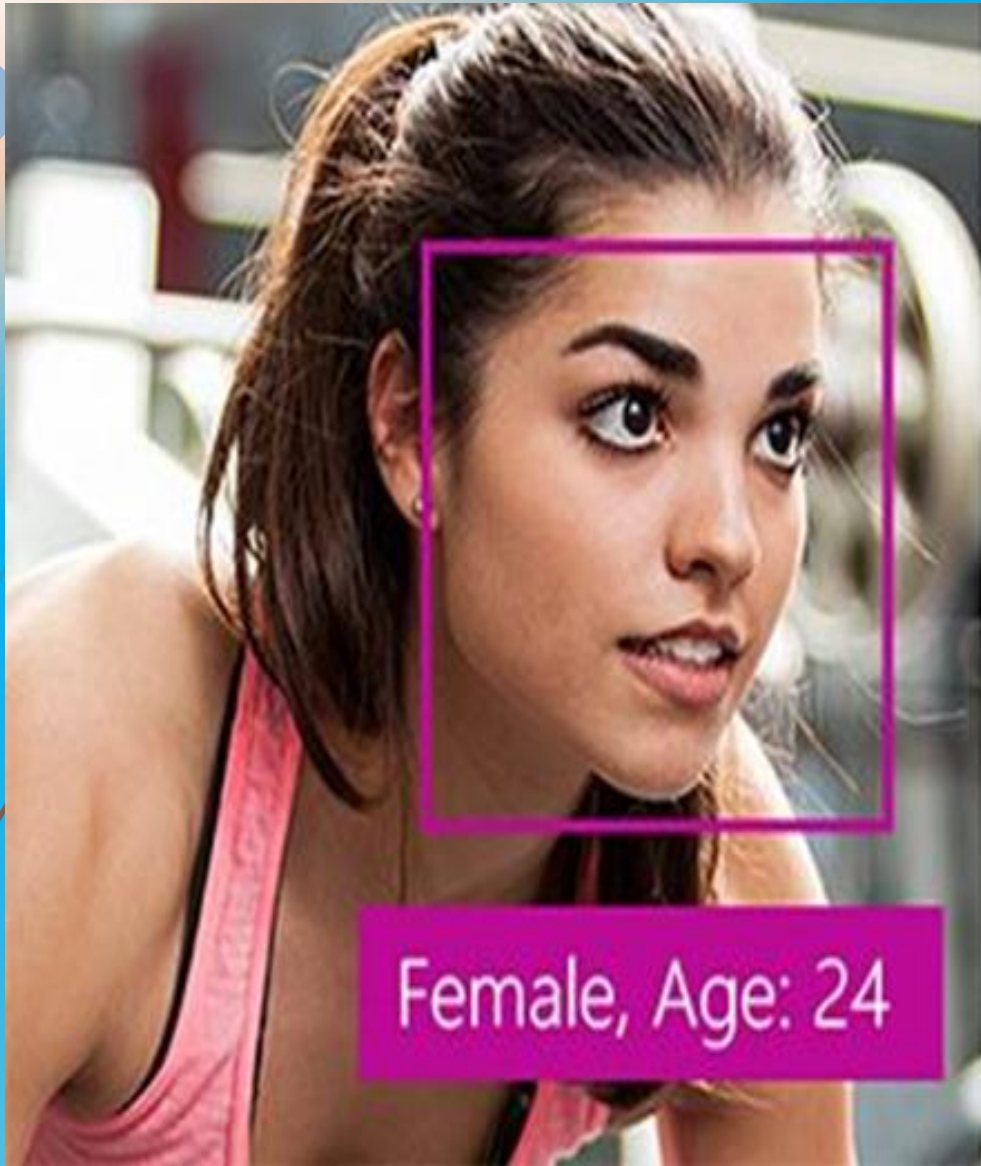
HIKVISION Y.N1402
WWW.Hikvision.Center

دیجی وی

HIKVISION
WWW.Hikvision.Center

تشخیص چهره در دوربین های مداربسته چگونه عمل می کند ؟

دوربین های مدار بسته با قابلیت تشخیص چهره با استفاده از الگوریتم های خاصی که در نرم افزار آنها تعریف شده است (مانند فاصله میان چشم ها، ابروها، بینی، خطوط صورت و ...) می توانند چهره افراد جلوی دوربین را تشخیص دهند. همچنین در زوایای مختلف، تشخیص چهره از جمله روبرو یا نیم رخ انجام می شود که این قابلیت به نرم افزار دوربین مدار بسته بستگی دارد. ولی معمولا تا زاویه ۴۵ درجه را از روبرو تشخیص می دهند. در بخش پردازش تصاویر ، دوربین از چهره افراد مورد نظر عکس گرفته و در بایگانی دستگاه ضبط یا سرور ذخیره می کند و شما می توانید به تمام تصاویر به همراه سایر جزئیات اعم از روز و ساعت ورود افراد دسترسی داشته باشید.



Female, Age: 24



Male, Age: 32





یک سیستم تشخیص چهره در دوربین مدار بسته به چه تجهیزاتی نیاز دارد؟

- دوربین مدار بسته: دوربین مدار بسته باید دارای رزولوشن تصویر بالایی باشد. هرچه رزولوشن تصویر بالاتر باشد امکان تشخیص دقیق تر چهره بیشتر خواهد شد.
- سرور: از آنجا که تمام پردازش های نرم افزاری باید در سرور انجام شود، هرچه از سیستم پیچیده تری برای پردازش تصویر استفاده کنید، نیاز به سرور قوی تری نیز دارید.
- نرم افزار پردازش تصویر: نرم افزار بخش اصلی کار را انجام می دهد. نحوه نوشته شدن نرم افزار نقش بسیار زیادی در دقت نرم افزار شما دارد، پس انتخاب اصلی شما در این بخش خواهد بود.

نحوه عملکرد دوربین های پلاک خوان

پلاک خودرو یکی از بهترین اقلام اطلاعاتی برای احراز هویت خودروهاست، دوربین های مدار بسته پلاک خوان با سرعت بالا عکس های متوالی و با کیفیت بالا میگیرند و سپس نرم افزار بهترین تصویر را انتخاب کرده و پردازش می کند. این دوربین های هوشمند با دریافت و شناسایی کاراکترهای اپتیکی و با اخذ تصاویر از دوربین های نصب شده در هر یک از نقاط ورودی خودرو ها با الگوریتم های وروش های پیشرفته متن مربوط به پلاک (شماره پلاک) را استخراج نموده، با دقت بسیار بالا می خواند و ثبت می کند تا در قسمت های دیگر نرم افزار به منظور مشاهده سوابق و احراز هویت خودرو مورد استفاده قرار بگیرد.

تفاوت LPR و ANPR

- دوربین پلاک خوان دوربین مداربسته ایست که می تواند پلاک خودرو را ثبت کند. شناسایی به صورت استخراج اعداد و حروف درج شده در پلاک انجام می شود. در شرایط نوری خاص این دوربین نیاز به قابلیت هایی است که بتواند اثر منفی بی نوری یا نور شدید را خنثی کند. اما تفاوت دو عبارت LPR و ANPR در چیست؟ در واقع LPR و ANPR هر دو اصطلاح مختلف برای توصیف سخت افزار و نرم افزار مورد استفاده در تشخیص و ضبط پلاک خودرو توسط دوربین مداربسته هستند.
- LPR مخفف (License Plate Recognition) و به معنای مجوز تشخیص پلاک خودرو است. اصطلاحی است که معمولاً برای توصیف دوربین های مداربسته تخصصی استفاده می شود. این دوربین ها قادر به مقابله با چالش های مربوط به ثبت پلاک هستند. این چالش ها می توانند سرعت خودرو، مه، دید در شب و مواد بازتابنده روی پلاک باشند.
- ANPR مخفف (Automatic Number Plate Recognition) و به معنای تشخیص خودکار شماره پلاک است. اصطلاحی است که معمولاً در توصیف نرم افزاری استفاده می شود که ورودی دوربین LPR را می گیرد. سپس با استفاده از نرم افزار نوشته های عددی و حرفی روی یک پلاک را تشخیص می دهد. مرحله بعد ذخیره شماره پلاک و یا مطابقت آن با سوابق پایگاه داده است.



سیستم پلاک خوانی معمولا از نورهای مادون قرمز بهره می برد که امکان تصویر برداری برای دوربین در هر زمانی از شبانه روز را فراهم می کند. تکنولوژی ANPR باید قادر باشد تا شماره پلاک را رقم به رقم بخواند.

ویژگی های مهم نرم افزار دوربین ANPR

- ▶ ثبت پلاک خودرو های در حال تردد
- ▶ تعریف مالکین همچون: نام، توضیحات و تصویر مالک به تعداد بالا
- ▶ تعریف خودرو به تعداد دلخواه
- ▶ اتصال خودکار به دوربین های نظارتی
- ▶ پردازش خودکار جریان (stream) دوربین و شناسایی پلاک به محض قرارگیری خودرو در مقابل دوربین مداربسته
- ▶ ذخیره سازی اطلاعات تردد شامل: تاریخ و ساعت ورود، مجاز بودن خودرو، شماره و تصویر پلاک و تصویر کامل خودرو
- ▶ اتصال به انواع آلارم
- ▶ اتصال به راه بند یا گیت ورودی
- ▶ بازکردن خودکار راهبند برای خودروهای مجاز
- ▶ تعیین زمان مجاز تردد برای هر خودرو

فنس مجازی، راهکاری مدرن برای حفاظت پیرامونی

مناطق حساس و مهم و وجود دارند که محافظت از آنها در برابر حملات تروریست-ها، خرابکاریها، دزدها و یا خسارت-های اتفاقی بسیار اهمیت دارد. وجود سامانه هایی مدرن برای بهبود شرایط نظارت بر این مناطق و توجه به تهدیدات واقعی، بیشتر احساس می گردد.

ما با سیستم های مدرن نظارت تصویری و فنس مجازی که ترکیبی از دوربین-های مدار بسته حرارتی و متداول، آنالیز هوشمند و دوربین های (PTZ دوربینهای مدار بسته گردان با قابلیت تراکینگ هوشمند) است، به کارفرمایان خود یک روش موثر برای تشخیص هوشمند، تایید و اقدام سریع در محیط-های حساس ارائه می-نماییم. این سامانه حتی در شرایط بسیار سخت و دشوار نیز بسیار کارآمد و با عملکرد بالا موجب رضایتمندی می گردد.



 SAT
شباب آرا تک

Y.N1402

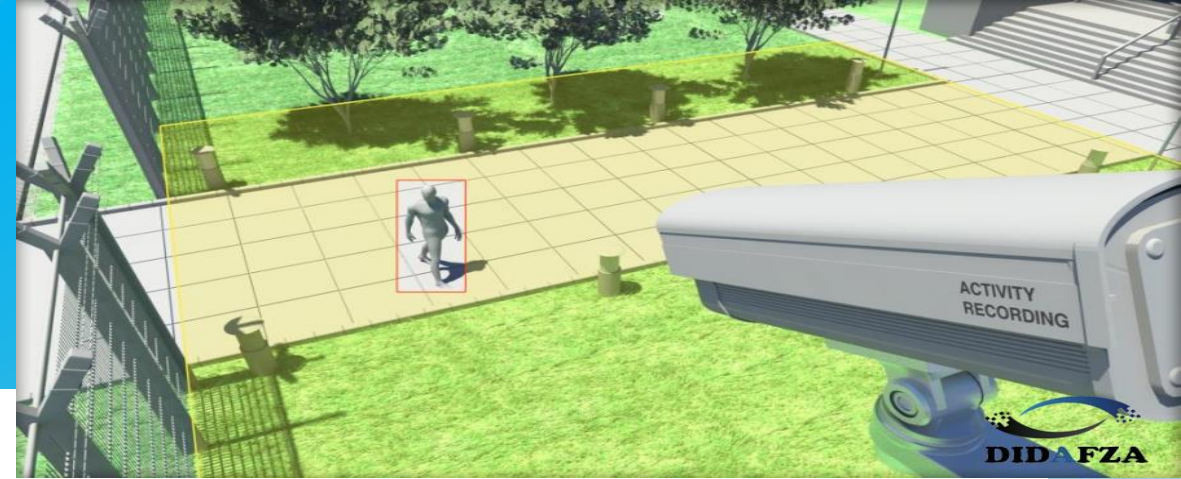


 KDT
شماره 66
Networking & Communication
© Out. 201

2019 04 16 13:20:50

AKITAN | دوربین مدار بسته

 ipmcctv.com  021-66126233





دی وی آر سیستم ضبط کننده (DVR)
ی دیجیتالی تصویر است که از یک یا دو
هارد با ظرفیت بسیار بالا برای ذخیره
سازی تصاویر استفاده می کند و بیش از
2000 ساعت تصویر را به صورت فشرده
ضبط می کند علاوه بر این تمامی قابلیت
های سوئیچر، کواد و مالتی پلکسر را به
صورت یکجا دارد و از طریق منوی مربوطه
می توان سیستم را برای شرایط مختلف
برنامه ریزی کرد.

سرویس دهنده ویدئویی تحت شبکه

- می توان محصولات ارائه شده مرتبط با این مبحث را به چند بخش زیر دسته بندی نمود:
- شبکه Network Video Server سیستم های سرویس دهنده ویدئویی تحت شبکه
- Network Camera Server دوربین های تحت شبکه
- NVR(Network Video Recorder) Server سیستم های ضبط تصویر شبکه ای
- DVR(Digital Video Recorder) Server سیستم های ضبط تصویر بصورت دیجیتال
- Network Media Decoder سیستم صوتی تحت شبکه ای
- Network DVR Software نرم افزارهای تخصصی ضبط و کنترل تصاویر تحت شبکه
- AOIP(Always-On-IP Dynamic) Server سیستم نمایش و کنترل از طریق اینترنت



سیستم های سرورس دهنده ویدئویی تحت شبکه Network video Server

ویدئو سرورها سیستم هایی هستند که امکان اتصال انواع دوربینهای آنالوگ به شبکه های کامپیوتری و نیز کنترل آنها و ارسال تصاویر گرفته شده بصورت Real Time را دارند. انواع این سیستم های دارای ورودیهای ویدئویی استاندارد BNC و نیز خروجیهای تصویری بصورت آنالوگ برای اتصال به سیستمهای دیگر می باشند.

سیستم های ویدئو سرور می توانند با استفاده از ورودی ها و خروجی های استاندارد (RS232,RS485,DI/DO,...) با سیستمهای جانبی دیگر مانند: انواع مودمها و روترها، کنترل کننده های حرکتی دوربین ها (PTZ) ، سیستمهای ایمنی و... ، ارتباط برقرار نموده و همرا با ضبط تصاویر از طریق انواع شبکه های کابلی و بیسیم (WireLess) آنها را بصورت همزمان کنترل و وقایع را ثبت نماید.

اساس کار این سیستمها بر پایه پروتکل TCP/IP و بصورت WebBase می باشد. سیستمهای فوق با استفاده از نرم افزار تخصصی خود می تواند مدیریتی کامل را بر سیستم تصویر برداری ، ضبط ، کنترل ، امنیت و ... در مدیریت به مدیران و کاربران ارائه دهد. لازم به ذکر است این سیستمهای بصورت External امکان اتصال به تجهیزات جانبی ضبط صدا را نیز دارند. بطور کلی ویدئو سرورها سیستمهای Stand-alone با امکانات شبکه ای جهت کنترل سیستمهای تصویری هستند. سیستمهای ویدئو سرور میتوانند بصورت تک کانال یا چند کاناله وحتى بصورت USB کار کنند. لازم به ذکر است سیستمهای ویدئو سرور تفاوتهای زیادی با کارتهای Capture تصویری دارند . گرچه هردو یک عملیات را انجام میدهند ولی سیستم های متفاوتی دارند.

دوربین های تحت شبکه Network Camera Server



دوربین های تحت شبکه در اصل یک مجموعه کامل از سخت افزارهای مختلف شامل دوربینهای CCD ویدئو سرور IP Base و سیستم کنترل و... می باشند . استفاده از این دوربین ها در طراحی سیستم های نظارت تصویری باعث صرفه جویی در هزینه ها ، زمان اجرا ، کیفیت بهره برداری ، دسترسی آسان و... می شود.

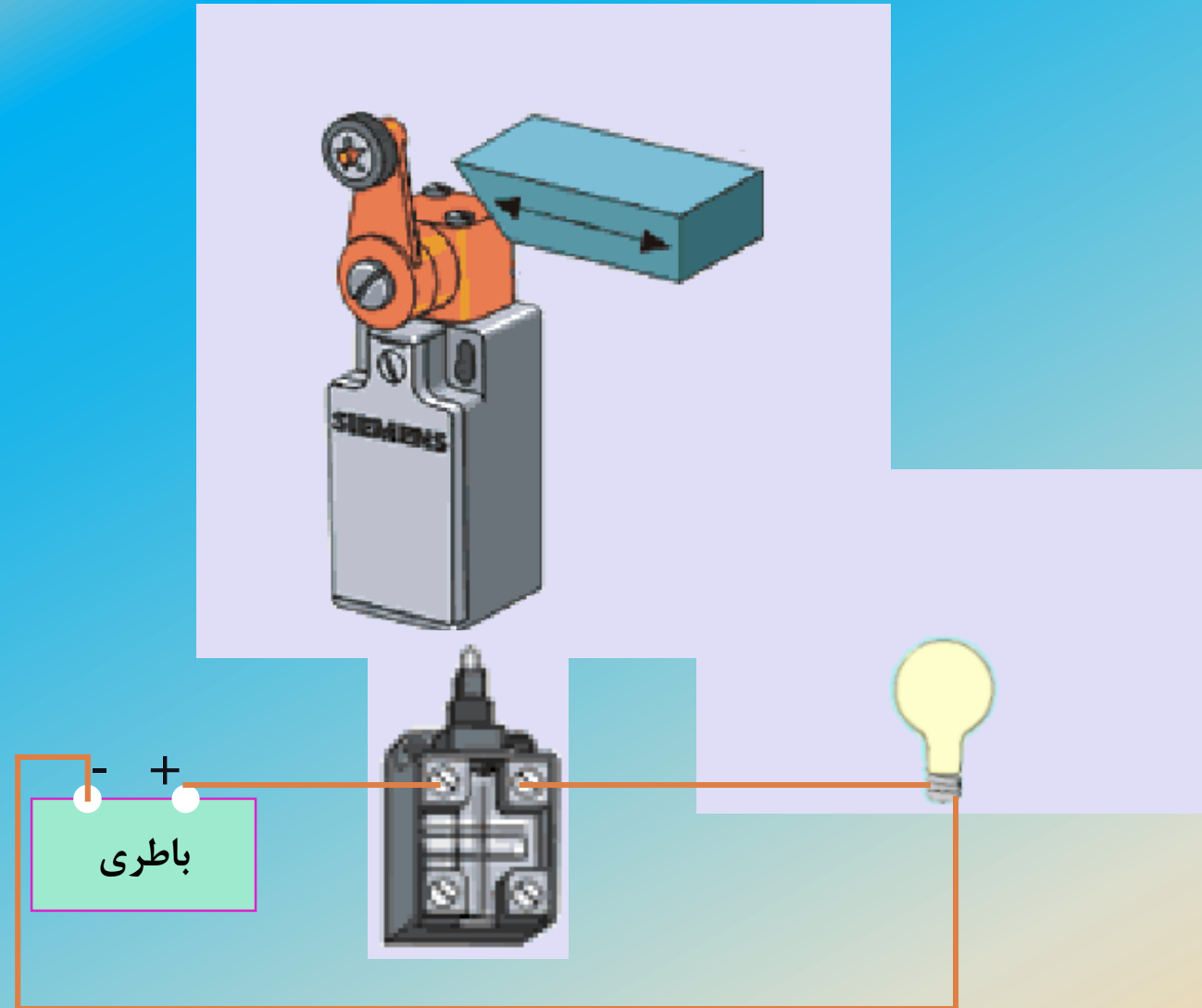
قابلیت اصلی این دوربینها ارسال تصاویر و کنترل سیستم به صورت همزمان یا Real Time از طریق خروجی RG45 و شبکه های LAN می باشد این قابلیت باعث شده دسترسی به اطلاعات تصویری از طریق اینترنت یا حتی سیستم های Dial-up به سادگی امکان پذیر بوده و بدون احتیاج به تجهیزات ویدئویی و شبکه ای گران قیمت از طریق PC های معمولی یا PDA ها تصاویر را مشاهده ، ضبط و سیستم را کنترل نمود .

سری های مختلف این دوربین ها قابلیت اتصال چندین دوربین آنالوگ دیگر را با استفاده از ورودی های استاندارد BNC را داشته و می توانند به صورت همزمان تا 3 دوربین جانبی را پشتیبانی و از طریق شبکه و خروجی استاندارد ویدئویی تصاویر را مشاهده نمود. مشاهده کنترل و ضبط تصاویر نیاز به نرم افزار جانبی نداشته و فقط یک مرورگر اینترنتی استاندارد مانند Internet Explorer یا Netscape ،... کافی می باشد.



سنسور ها

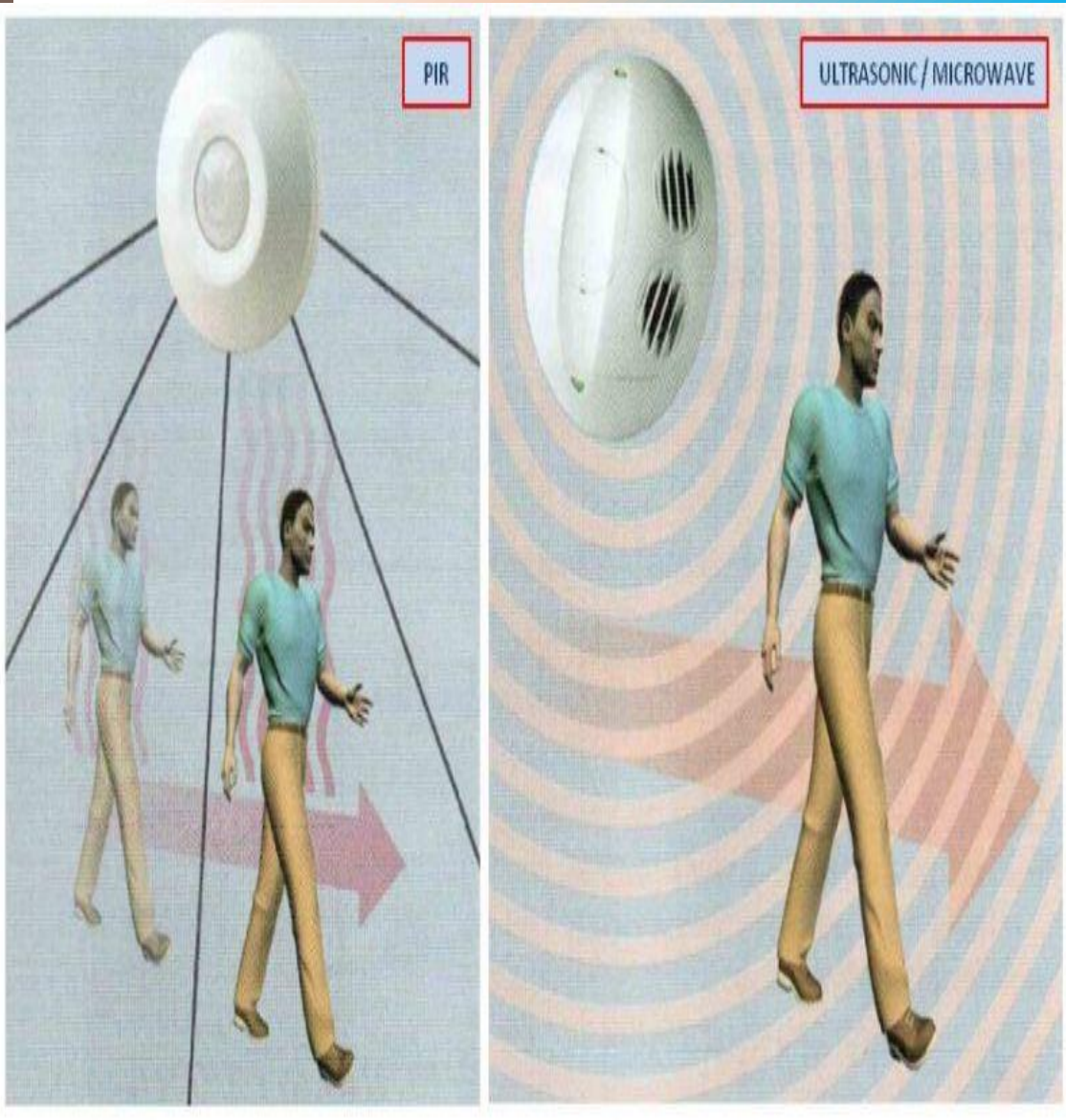
اتصال لامپ به لیمنت سویچ



سنسور یا حسگر چیست؟

سنسور الکتریکی (که سنسور الکترونیکی نیز نامیده می‌شود) وسیله‌ای است که پارامتر فیزیکی مورد نظر (مانند گرما، نور، صدا) را تشخیص می‌دهد و آن را به سیگنال الکتریکی تبدیل می‌کند که می‌تواند توسط یک سیستم الکتریکی یا الکترونیکی اندازه‌گیری و استفاده شود.

کمیت شناسایی شده معمولاً نوعی انرژی است که ماهیت آنالوگ (پیوسته) دارد و با استفاده از مبدل به انرژی الکتریکی تبدیل می‌شود (مثلاً میکروفون مبدلی است که انرژی صوتی را به انرژی الکتریکی تبدیل می‌کند).



کاربرد سنسور ها

سیگنال تولید شده در خروجی یک سنسور الکتریکی معمولاً به منظور اندازه گیری استفاده می شود که سپس می تواند برای ایجاد پاسخ بعدی مورد استفاده قرار گیرد. به عنوان مثال، یک سنسور دما می تواند برای اندازه گیری دمای یک اتاق و تبدیل آن به سیگنال الکتریکی استفاده شود. اگر دمای اتاق اندازه گیری شده خیلی پایین باشد (زیر آستانه از پیش تعیین شده) این اطلاعات می تواند توسط یک سیستم الکترونیکی استفاده شود که به طور خودکار یک بخاری را روشن می کند تا دمای اتاق را به آستانه از پیش تعیین شده افزایش دهد. از طرف دیگر، اگر اندازه گیری از سنسور نشان می دهد که اتاق خیلی گرم است (بالتر از آستانه از پیش تعیین شده)، سیستم می تواند به طور خودکار یک واحد تهویه مطبوع را برای کاهش دمای اتاق روشن کند. نام رایج سنسور مورد استفاده برای اندازه گیری دما دماسنج است.



دسته بندی انواع سنسورها

انواع مختلفی از سنسورها وجود دارد که دسته بندی های اصلی عبارتند از:

سنسورهای موقعیت

سنسورهای فشار

سنسورهای دما

سنسورهای نیرو

سنسورهای لرزش

سنسورهای پیزو

سنسورهای ویژگی سیالات

سنسورهای رطوبت

فشار سنج

حسگرهای نوری

سوئیچ های جریان و سطح



دزدگیر اماکن چیست؟

دزدگیر اماکن یکی از ملزومات ضد سرقت است که در خانه‌ها، دفاتر کار و حتی اداره‌ها استفاده می‌شود. دزدگیر اماکن یک پکیج الکترونیکی نیمه هوشمند است که با ورود افراد غیرمجاز به منزل یا محل کار، اعلام هشدار می‌کند. به زبان ساده با ورود فرد غیرمجاز، دزدگیر شروع به آژیر کشیدن می‌کند.

زمانی که این دزدگیرها تولید شد، ابتدا یک سیستم ساده امنیتی ایجاد شد که تنها می‌توانست علامت هشدار را در چندمتری محل خود اعلام کند؛ اما گذر زمان و رشد تکنولوژی سبب شد کاربرد دزدگیر اماکن بیشتر شده و اعلام سرقت را برای کیلومترها دورتر نیز اعلام کند. دزدگیرها چه خودرو و چه اماکن از یک تکنولوژی استفاده می‌کنند





کاربرد دزدگیر اماکن

اعلام سرقت و پیام هشدار در زمان سرقت از جمله وظایف دزدگیر اماکن است اما می‌توان این جمله را بهتر توضیح داد.

○ جلوگیری از سرقت: هرگونه احساس سنسورهای الکترونیکی، موجب می‌شود دزدگیر اماکن یا خودرو به صدا درآید. هر ساختمانی و خودرویی می‌تواند از دزدگیر استفاده کند.

○ ارسال پیامک هشدار: یکی از مشکلاتی که دزدگیرهای ابتدایی داشتند، عدم اطلاع به موقع صاحب اماکن یا خودرو بود. در حال حاضر، دزدگیرها این تکنولوژی را دارند که با اتصال یک سیم‌کارت به دستگاه در زمان سرقت به صاحب مکان یا خودرو پیامک هشدار ارسال کنند.

○ اتصال به سیستم حفاظت: امروزه اماکن حفاظتی در سطح شهر بسیار دیده می‌شود که وظیفه محافظت از اماکن خاص را برعهده دارند؛ یکی از مزایای دزدگیر اماکن این است که می‌تواند به سیستم‌های حفاظتی متصل شده تا در صورت آلام، مأموران خود را فوراً به آن مکان برسانند. مغازه‌های طلافروشی، ساختمان‌های لوکس از این دزدگیرها می‌توانند استفاده کنند. بانک‌ها و صرافی‌ها نیز می‌توانند دزدگیر خود را به مراکز پلیس متصل کنند تا در صورت سرقت، مأموران خود را به بانک برسانند.



Vita

Y.N1402

اجزاء دزدگیر اماکن عبارت‌اند از:

۱. پنل دزدگیر: پنل یا بدنه دزدگیر که تمام اجزاء الکتریکی درون آن جمع می‌شود، البته بعضی‌ها اعتقاد دارند پنل قلب دزدگیر اماکن است. روی پنل دزدگیر یک کانکتور وجود دارد که به آن زون می‌گویند. برای اینکه دزدگیر اماکن به درستی کار کند، نیاز به سنسورهای قوی است. این سنسورها توسط بردهای الکتریکی کنترل می‌شود که این بردهای سنسور روی زون نصب می‌شوند؛ پس در واقع اتاق فرمان دزدگیر، درون پنل وجود دارد.

۲. چشمی دزدگیر: سنسور مادون قرمز دزدگیر یا چشمی دزدگیر است. کار چشمی تشخیص حرکت است؛ چشمی‌ها محیط را هر لحظه اسکن می‌کنند و هر حرکت کوچکی را ثبت می‌کنند. با هر حرکت مشخصی چشمی یک هشدار به پنل می‌دهد تا پنل اعلام سرقت کند. امروزه دزدگیرهای اماکن مجهز به چشمی‌های بی‌سیم هستند که توسط وایرلس به پنل وصل می‌شوند. البته چشمی‌های ارزان‌تر از چشمی بی‌سیم نیز وجود دارد که این چشمی‌ها توسط دو سیم به دزدگیر متصل می‌شوند.





3-مگنت دزدگیر(مغناطیسی): یکی از اجزاء مهم دزدگیر قسمت مگنت است، به خصوص برای ساختمان‌هایی که سارقین می‌توانند از پنجره وارد شوند. مگنت از دو قطب مثبت و منفی تشکیل شده است. زمانی که قصد نصب مگنت را دارید، باید قطب مثبت و منفی را مقابل هم و با فاصله ۱/۵ سانتی‌متری از یکدیگر قرار دهید. یعنی یک جزء را روی قسمت بازشوی پنجره و جزء دیگر را بر قاب پنجره قرار دهید. به دلیل وجود بردهای الکتریکی روی هر دو قسمت مگنت با کوچک‌ترین حرکت پنجره و فاصله گرفتن مگنت‌ها از همدیگر، سنسور فرمان آژیر را به صدا در می‌آورد.

۴.تلفن‌کننده دزدگیر اماکن: تلفن‌کننده یک نوع حافظه داخلی است که به محض آنکه سنسور حرکت یا اعلام سرقت فعال شود، تلفن با استفاده از شماره‌های درون حافظه، شماره‌گیری کرده و به افراد تلفن می‌زند.

این حافظه می‌تواند از ۴ تا ۱۶ شماره را در خود جای دهد و بسته به اولویت با افراد تماس بگیرد. در دزدگیرهای پیشرفته حتی امکان ارسال پیامک نیز وجود دارد و می‌توان برای افراد پیامک‌های از پیش تعیین شده را ارسال کرد. این تلفن‌کننده‌ها به دو صورت شماره‌گیری کارتی و ثابت وجود دارد.





۵. بلندگوی دزدگیر: دزدگیر اماکن نیازمند یک بلندگوست تا سرقت را به دیگران اطلاع دهد. کار بلندگوی دزدگیر اماکن نیز همان است و در زمان لازم با پخش آژیر دیگران را مطلع می‌کند. بلندگوی دزدگیر دارای وات‌های متفاوت است که هرچه وات بلندگو بیشتر است برد صدا هم بیشتر می‌شود و افزایش قیمت را به دنبال خواهد داشت.

۶. پدال دزدگیر: پدال قطعه‌ای است که روی زمین و در مکان‌های خاص نصب می‌شود تا با فشار و لمس آن، فرمان به پنل دزدگیر داده شده و دزدگیر اعلام سرقت می‌کند. از آنجاکه سنسور چشمی، مگنت در دزدگیر وجود دارد و حساسیت زیادی به حرکت هم دارند؛

۷. ریموت دزدگیر: ریموت یک کنترل است که در دست مالک یا صاحب دزدگیر اماکن قرار دارد تا با فعال و غیرفعال کردن، دزدگیر اماکن را در مدار قرار داده یا خاموش کند. برد این ریموت بسته به قدرت ریموت ۵۰ تا ۱۵۰ متر است.

۸. ریپیتر دزدگیر اماکن: برای اینکه ریموت در فاصله بیشتر نیز کار کند و دزدگیر اماکن را قطع کند از ریپیتر استفاده می‌شود. ریپیتر نه تنها برد ریموت را افزایش می‌دهند، بلکه باعث می‌شوند قدرت سنسور چشمی نیز افزایش پیدا کند. یکی دیگر از مزایای استفاده از ریپیتر افزایش قدرت پنل دزدگیر است. در مواقعی که پنل دزدگیر با فاصله زیادی از اجزاء قرار گرفته است، ریپیتر موجب افزایش قدرت پنل شده و ارتباط اجزاء را با پنل بهتر می‌کند.



انواع سنسور

سنسور حرکتی : سنسورهای حرکتی باید در ورودی اصلی یا راهرو در طبقه همکف خانه قرار داده شوند تا بتوانند حرکت را تشخیص دهند و در صورت فعال بودن دزدگیر هشدار دهند. برخی از سنسورهای حرکتی به حیوانات حساس نیستند یعنی دزدگیر را می توان فعال کرد و حیوان در خانه پرسه بزند

سنسور درب ورودی : به سنسور مگنت یا درب و پنجره معروف می باشند. دوقسمت دارد : یکی روی پنجره یا درب نصب می شود و دیگری بر روی قاب یا چهارچوب آنها نصب می شود. اگر این 2 قطعه از هم جدا شوند به این معناست که در یا پنجره باز شده است . دراین صورت دزدگیر اماکن به ما هشدار می دهد

سنسور دود : این سنسور با تشخیص دود ناشی از حریق شما را در جریان این موضوع قرار میدهد و باعث آژیر کشیدن دزدگیر منزل نیز میشود.





■ سنسور نشت آب : این سنسور زمانی که آب نشت کند و بر روی زمین جاری شود این نشتی را تشخیص داده و سریعاً به شما اطلاع میدهد و دزدگیر را به صدا در می آورد

■ سنسور نشت گاز: سنسور نشت گاز: این سنسور زمانی که گاز شهری یا کپسول نشت کند به شما اطلاع میدهد و دزدگیر به صدا در می آید.

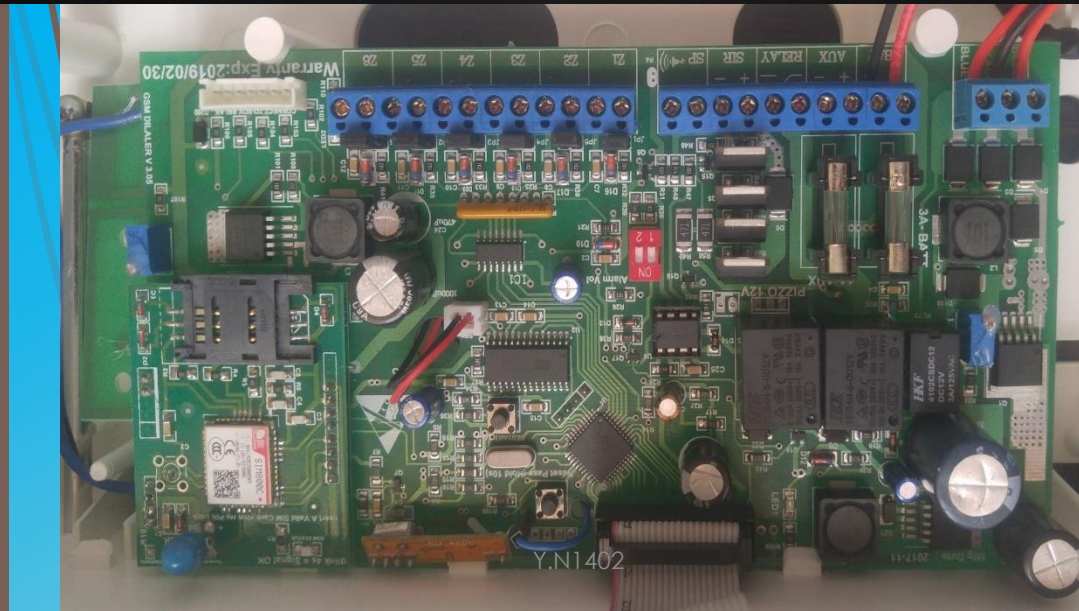


تشخیص
نشتی آب

Y.N1402

Water Leak Detector www.linkap.net





بیومتریک

روش‌های تشخیص هویت بیومتریک (Biometric Methods)



اثر انگشت در آیات قرآن کریم

بحث اثر انگشت به طور ضمنی در آیه ۳ و ۴ سوره قیامت مورد اشاره قرار گرفته است. خداوند متعال در این دو آیه می‌فرماید: "أَيُّحْسِبُ الْإِنْسَانُ أَنْ نَجْمَعَ عِظَامَهُ. بَلَىٰ قَادِرِينَ عَلَىٰ أَنْ نُسَوِّيَ بَنَانَهُ"

آیا انسان گمان می‌برد استخوان‌های او را پس از مردن و متلاشی شدن جمع‌آوری نخواهیم کرد؟ آری ما قادریم که حتی انگشتان (خطوط سرانگشتان) او را دوباره به صورت اول، موزون و مرتب کنیم.

اشاره

یکی از مباحث مهم در جامعه امروزی که دغدغه بسیاری از کارشناسان و همچنین کاربران می باشد بحث امنیت و تشخیص و تایید هویت است.

امروزه در امور مربوط به امنیت اماکنی مانند دانشگاه ها، فرودگاه ها، وزارتخانه ها و حتی شبکه های کامپیوتری استفاده از روش های بیومتریک در تشخیص هویت یا تایید هویت افراد بسیار متداول شده است. سیستم های پیشرفته حضور و غیاب ادارات، سیستم های محافظتی ورود خروج اماکن خاص، نوبت بوک های مجهز به Finger Print و ... از روش های مختلف تشخیص هویت بیومتریک استفاده می کنند. در این مقاله سعی می کنیم به صورت مختصر، مروری بر روش های مختلف بیومتریک داشته باشیم.



مقدمه

کلمه Biometric از ترکیب دو کلمه یونانی **bios** (زندگی) و **metrikos** (تخمین) شکل گرفته است.

بیومتریک عبارت است از، تشخیص هویت افراد با استفاده از ویژگی های فیزیولوژی و رفتاری آنها.

این یک تعریف کلی از واژه بیومتریک است. با استناد به این تعریف می توان گفت که همه افراد در زندگی روزمره خود، ناخودآگاه از بیومتریک استفاده می کنند. به عنوان مثال هویت افرادی که با آنها سرو کار داریم را می توان از روی صدا، چهره و حتی طرز راه رفتن شان تشخیص دهیم بنابراین می توان تاریخچه استفاده از بیومتریک را به قدمت تاریخ بشر دانست.

سیستم های بیومتریک

سیستم های بیومتریک باید با درصد قابل توجهی قابل اعتماد باشند تا سیستم در تشخیص افراد و اجازه دسترسی آنها اشتباه نکند.

در مقایسه با روش های سنتی تشخیص هویت مانند رمز عبور و کارت شناسایی می توان به این مزایای بیومتریک اشاره کرد:

- قرض داده نمی شوند.
- دزدیده نمی شوند.
- گم و یا فراموش نمی شوند
- خراب نمی شوند.

معمولا یک سیستم بیومتری به کمک الگوریتم های تشخیص الگو (Pattern Recognition)

سعی در استخراج ویژگی های (features) از رفتار یا ساختار فیزیولوژی فرد می کند و سپس این ویژگی ها را در دیتابیس (برای تشخیص و تایید هویت) ذخیره می کند. سیستم هایی که بر اساس علائم فیزیولوژی عمل می کنند بسیار مطمئن تر از سیستم های رفتاری هستند.

یک سیستم بیومتریک شامل ۴ بخش بنیادی است :

• **Sensor Module** : قسمت نمونه برداری که اطلاعات خام مورد نیاز را جمع آوری می کند. مانند تصویر اثر

انگشت.

• **Feature extraction Module** : قسمت پردازش برای استخراج ویژگی ها از اطلاعات مرحله قبل.

• **Matching Module** : قسمت مطابقت که بررسی می کند آیا اطلاعات جمع آوری شده با اطلاعات الگو

مطابقت می کند یا خیر؟ مثلاً تشخیص می دهد که آیا اطلاعات بدست آمده می تواند متعلق به یک اثر انگشت باشد یا

خیر، در صورت مطابقت بر حسب نیاز آن را ذخیره می کند و یا به مرحله بعدی برای تشخیص هویت می رود.

• **Decision-making Module** : قسمتی که اطلاعات ورودی (ویژگی ها) را با اطلاعات ذخیره شده

مقایسه می کند و اگر شباهت از درصد معلومی بالاتر بود به فرد اجازه دسترسی می دهد در غیر اینصورت پیغام خطا

می دهد.

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.

متدهای امروزی در بیومتریک

در این قسمت متدهای متداول و غیر متداول بیومتریک را معرفی خواهیم کرد و از بیان جزئیات وسایل و الگوریتم‌های پردازشی خودداری خواهیم کرد و 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:

تشخیص هویت (Identification):

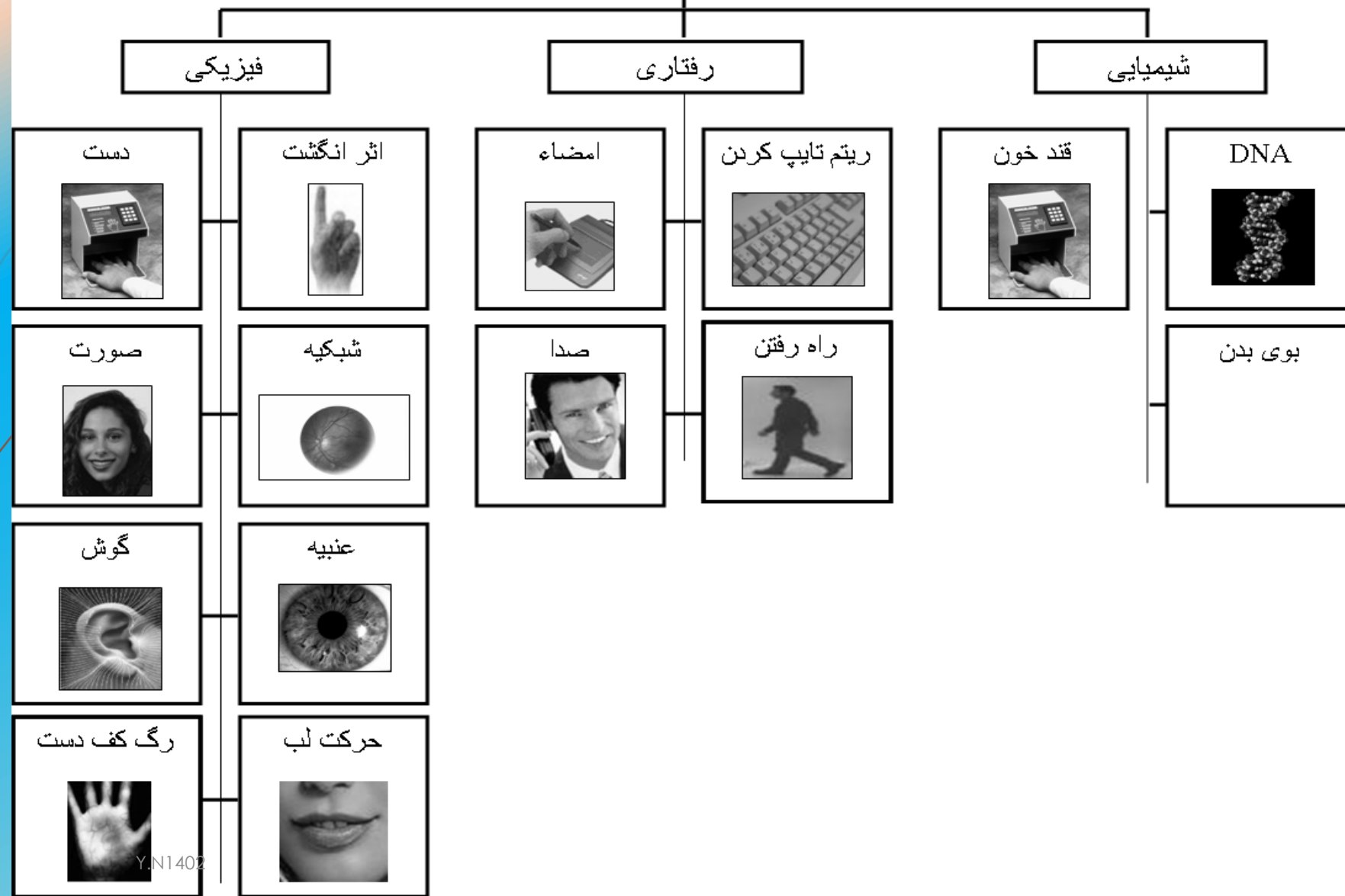
در این فیلد سعی می شود که هویت شخص دقیقا مشخص گردد.

تایید هویت (Verification):

در این فیلد بررسی می کنند که آیا فرد مطابق با هویت ادعا شده هست یا خیر؟

سیستم هایی که قادر به تشخیص هویت هستند، حتما می توانند تایید هویت را انجام دهند ولی بر عکس آن قطعی نیست.

بیومتریک



تصاویری از تکنولوژیهای بیومتریک



اثر انگشت (finger Print)

این روش متداول ترین مورد استفاده در بیومتریک است و چیزی جز اثر پستی و بلندی های نوک انگشت هر فرد نیست. سابقا اثر انگشت را توسط فشار دادن انگشت جوهری بر کاغذ بدست می آوردند ولی امروزه ، از نوک انگشت تصویری دیجیتالی تهیه می شود.

شکل ۱ : تصویری دیجیتالی از اثر انگشت



مزایای سیستم‌های اندازه گیری اثر انگشت:



۱- هر شخص دارای اثر انگشت منحصر بفردی است .



۲- اثر انگشت در برابر گذشت زمان مقاوم است .



۳- این تکنولوژی به بلوغ خود رسیده است .



۴- استفاده از آن بسیار راحت است .



۵- دارای نرخ خطای مساوی پایینی می باشد .



۶- ارزان است .



۷- عامه پسند است.



برای تهیه تصویر دیجیتالی اثر انگشت از سه نوع اسکنر استفاده می‌شود:

اسکنرهای نوری (optical)، اسکنرهای اولتراسوند (ultrasound) و اسکنرهای نیمه هادی (semiconductor capacitors). 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، سطوح شان چرب و مات می‌شد 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 (Palm Print) و اثر کف پا (Foot print) نیز اشاره کرد. بیومتریک با استفاده از اثر انگشت متداول ترین و در عین ارزانی یکی از مطمئن ترین روش های تشخیص هویت است.



Y.N1402



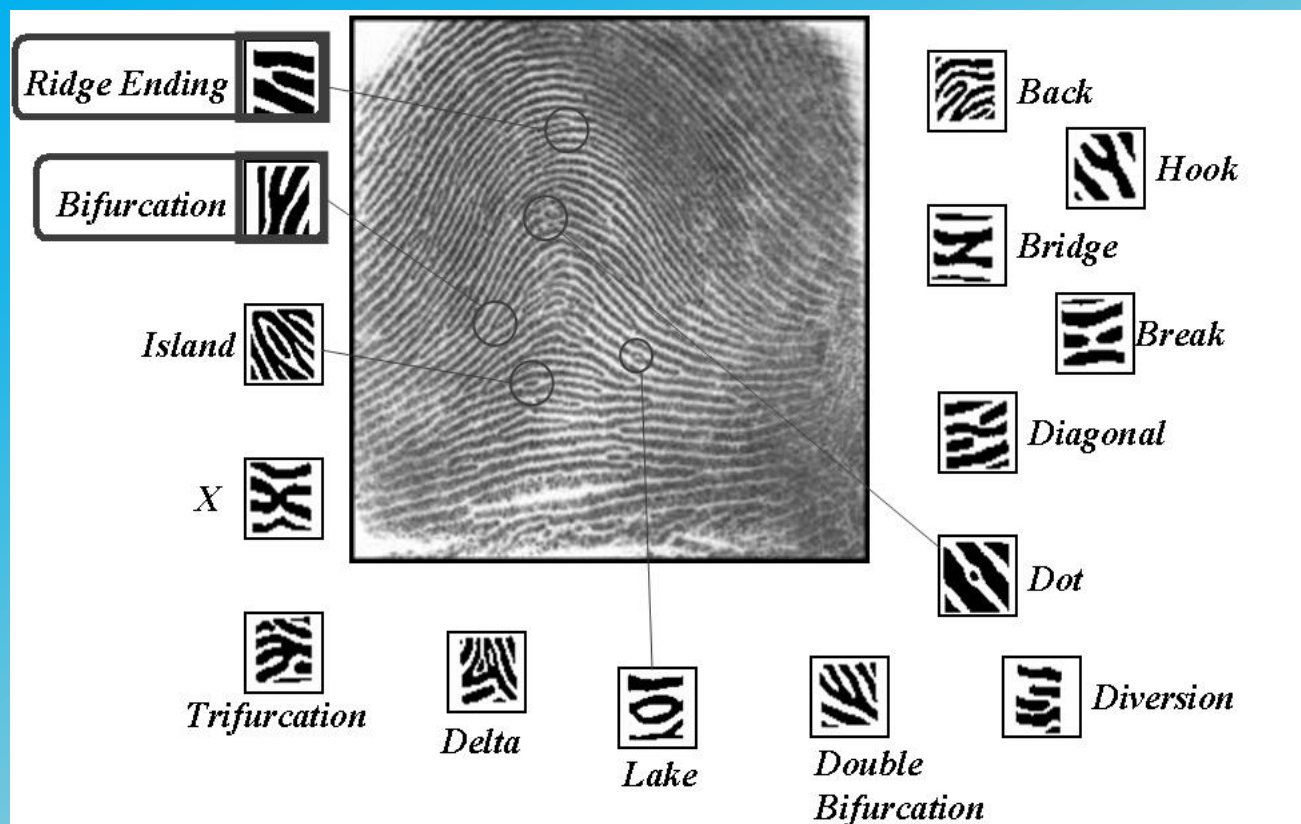
کمان شکسته

کمان

چرخش راست

چرخش چپ

پیچش





شکل ۲: اثر کف دست و اثر کف پا

روش تشخیص زنده بودن انگشت

الگوی دمایی نوک انگشت

تشخیص از طریق تعرق بافت انگشت

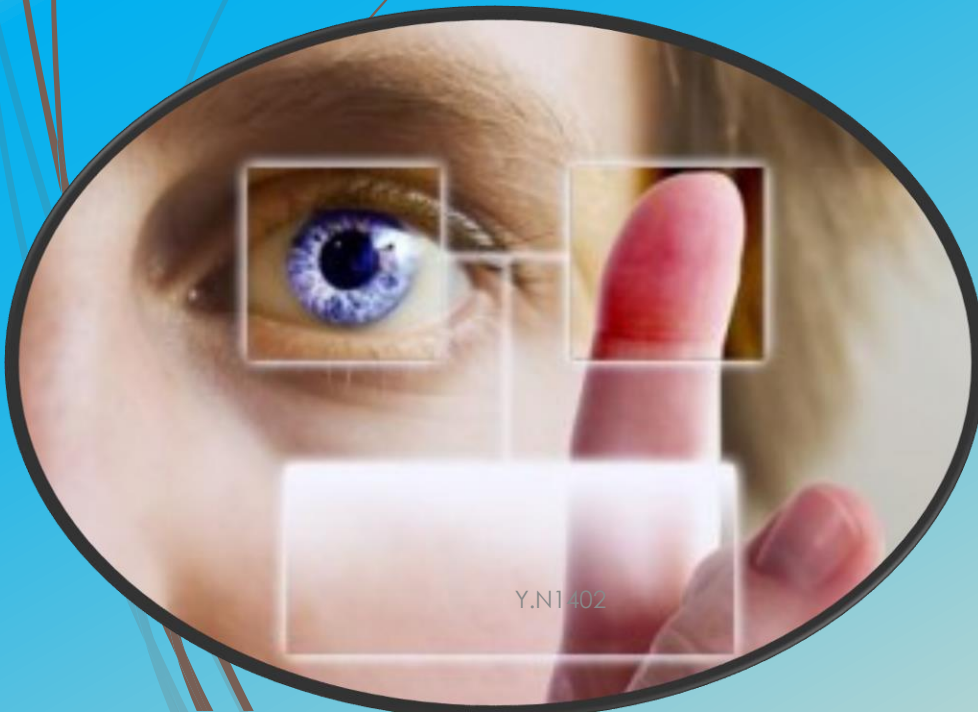
روش های اندازه گیری دمای بافت

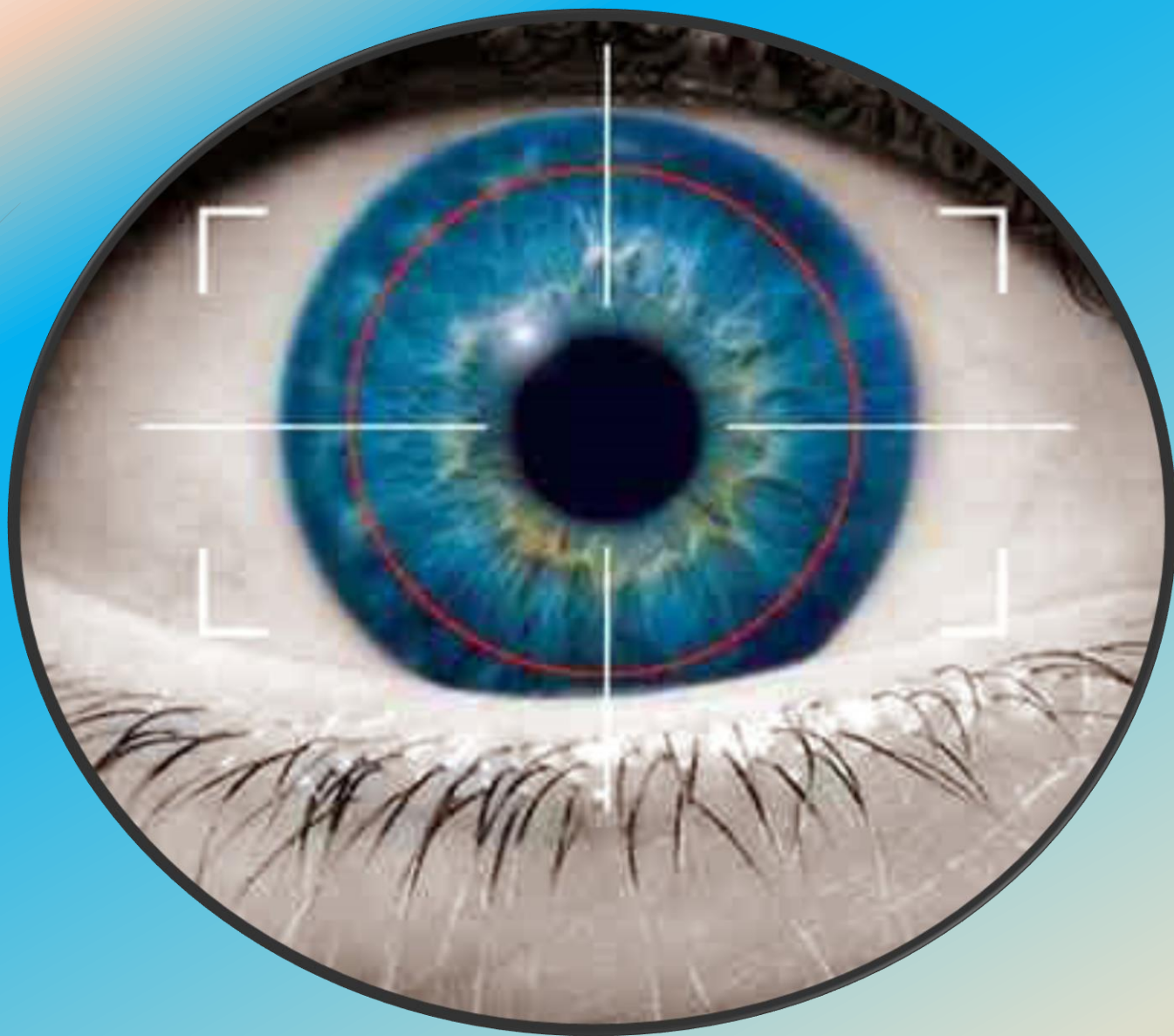
ایجاد گرما در محل قرار گیری انگشت

تشخیص زنده بودن اثر انگشت بر پایه آنالیز ویولت

ساختار شکل گیری عنبیه از ماه سوم جنین آغاز و تا ماه هشتم کاملاً تثبیت می گردد. ظاهر و ساختار (Pattern) 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 در دسر سازی دارد. مثلاً 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.

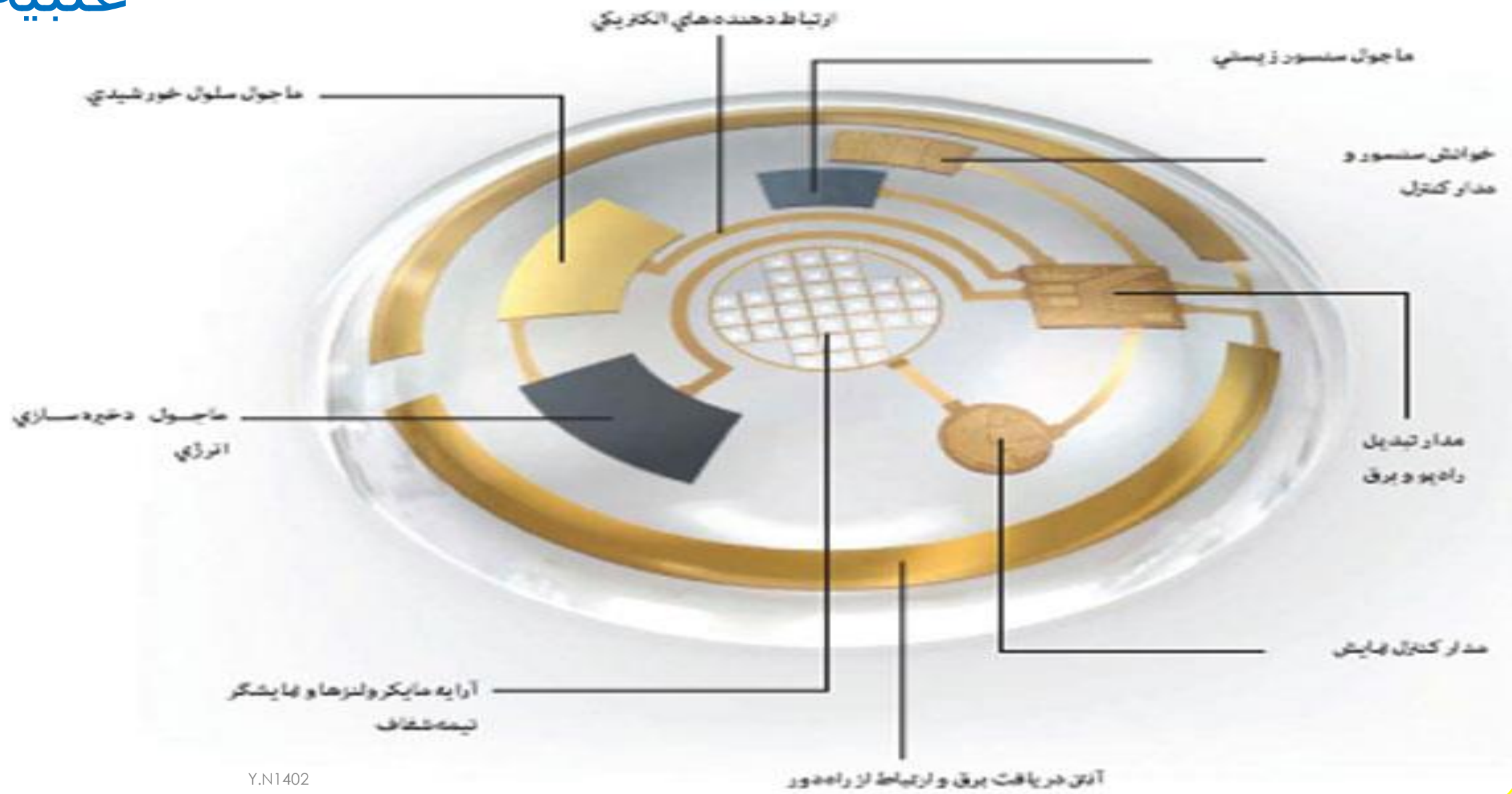




Y.N1402

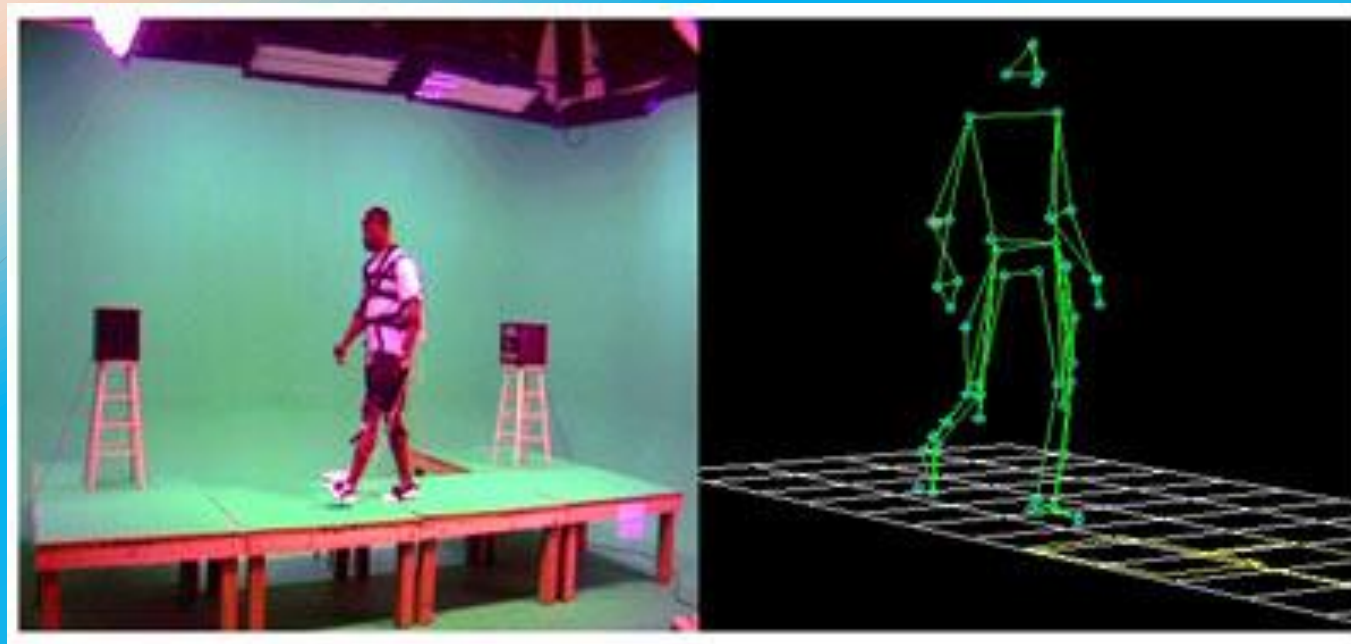
شکل ۳ : تصویربرداری از عنابه

عنبيه



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 های 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.



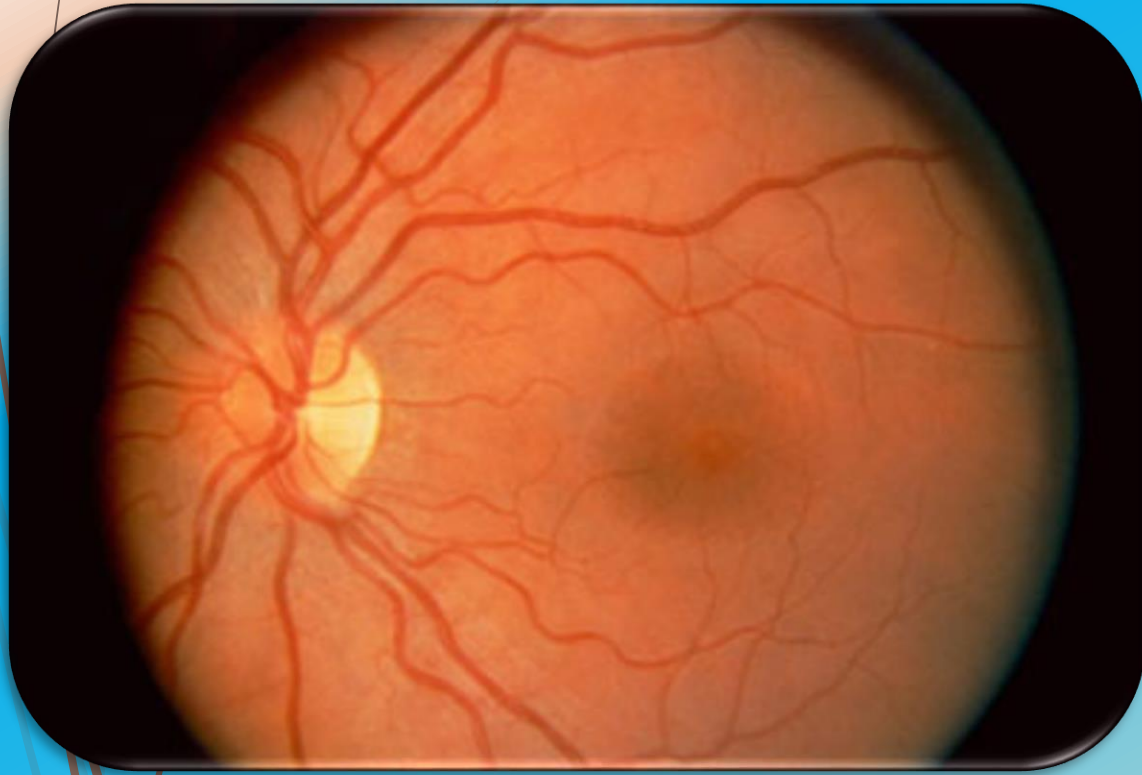
شکل ۴ : بررسی نحوه حرکت اندام های مختلف بدن هنگام راه رفتن

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 گرانبه است. به همین دلایل این روش اصلاً رایج نشده است.

شبکیه (Retina)

در این روش از سطح شبکیه تصویربرداری می شود و ساختار رگ های پشت شبکیه مورد پردازش قرار می گیرد. ساختار این رگ ها 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.

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.



شکل ۵ : ساختار رگ های پشت شبکیه

چگونگی تایپ با کیبورد (KeyStroke)

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 (typing rhythm) نیز گفته می شود. در این سیستم کاربر کلمه خاصی را بطور متناوب وارد می کند و نحوه تایپ (فواصل زمانی بین ضربه زده خودن کلیدها) ثبت و سپس تحلیل می گردد.

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 نوت بوک ها برای افزایش امنیت استفاده شده است.

گوش (Ear)

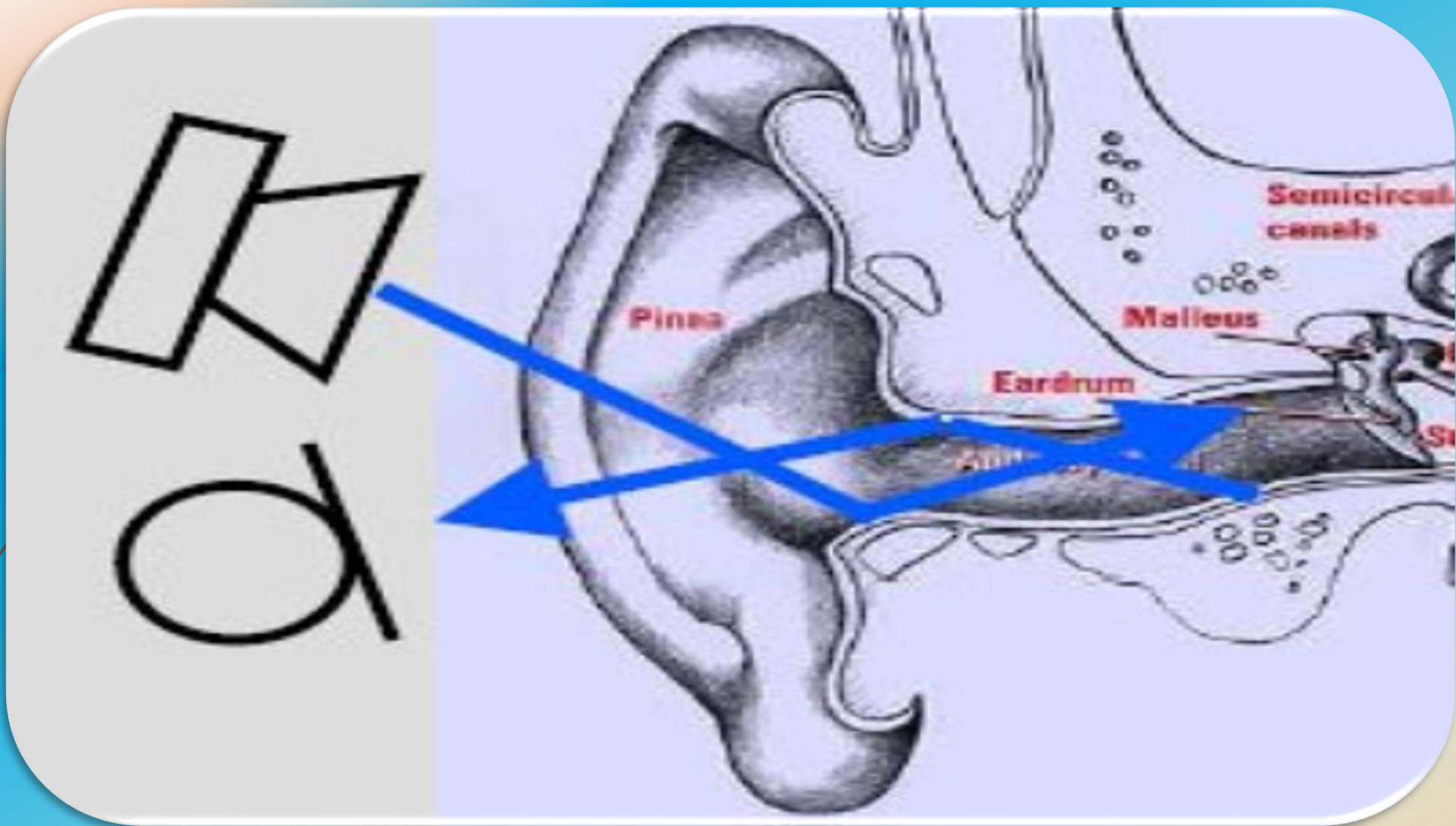
از گوش به دو شکل برای تشخیص هویت استفاده می شود:

شکل و ساختار لاله گوش در افراد مختلف متفاوت است (شکل ۶).

اکوی صدای خروجی از کانال گوش برای هر فرد با فرد دیگری متفاوت است (شکل ۷).

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.





شکل ۷: اکوی صدای خروجی از کانال گوش

شکل هندسی دست و انگشت (Finger Geometry & Hand)

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 دیپارتمان (ورودی دیپارتمان 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 انگشت تغییر یابد و این مسائل به شدت از کارایی این روش می کاهند.



شکل ۸ : تحلیل و مقایسه طول و قطر انگشت ها، مکان مفاصل، شکل و سایز کف دست

Y.N1402

ورید و رگ‌ها (Vascular Patterns & Vein)

در این روش از رگ‌های زیر پوست فرد تصویر تهیه می‌شود و ساختار آنها مورد پردازش و تحلیل قرار می‌گیرند. ساختار این رگ‌ها برای افراد مختلف منحصر بفرد است. روش‌های مختلفی برای تصویربرداری وجود دارد که معمول ترین آنها دوربین‌های مادون قرمز و سنسورهای حرارتی لمسی مادون قرمز است. عموماً از رگ‌های پشت کف دست، کف دست و رگ‌های انگشتان دست برای این نوع بیومتریک استفاده می‌شود. از آن جهت که شکل و حالت پوست در نتیجه این سیستم تاثیر ندارد، این روش نسبت به روش‌های اثر انگشت و شکل هندسی دست دارای امنیت بیشتر است.



Y.N1402

شکل ۹: تصویربرداری از رگ‌های زیر پوست

لب ها (Lips)

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 (Lips Print)** : 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 (Lips Movement)**: 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.

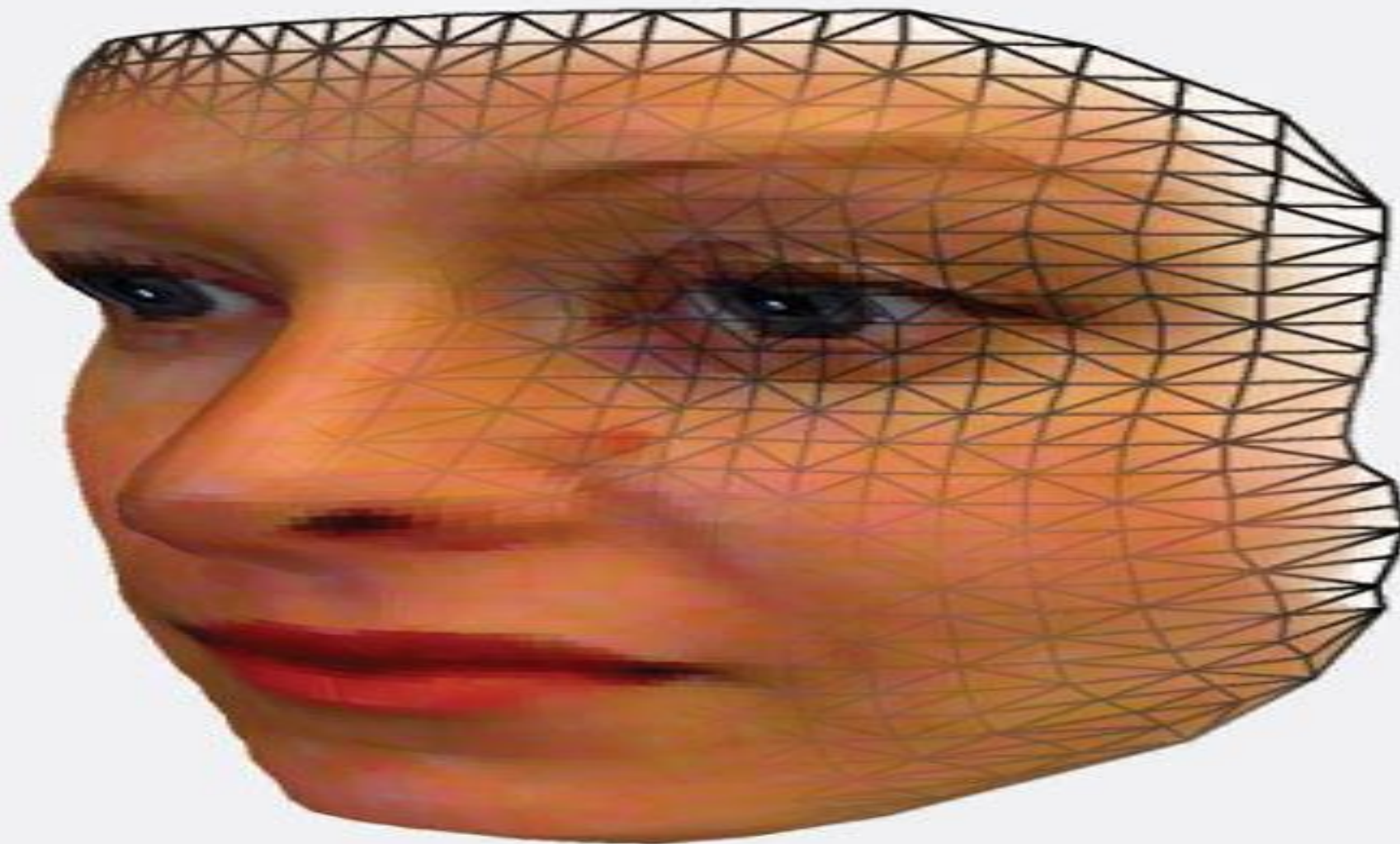
تشخیص چهره (Face recognition)

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 (Facial Geometry Recognition):

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 (شکل ۱۰).

این شیوه بسیار پرکاربردتر از بقیه متدهاست.

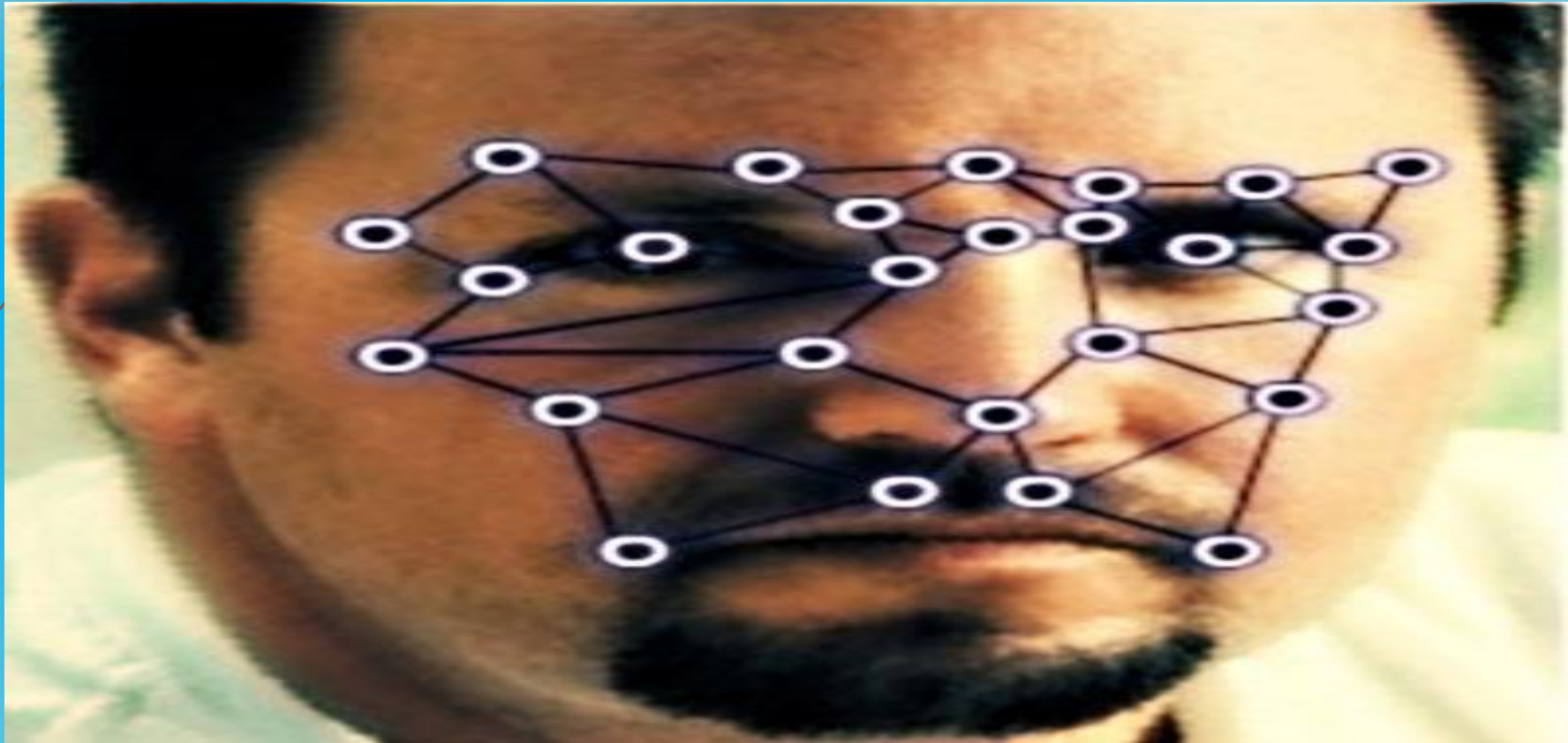


شکل ۱۰ : تحلیل مشخصات فیزیکی صورت مانند مکان چشم، بینی، لب و ...

Y.N1402

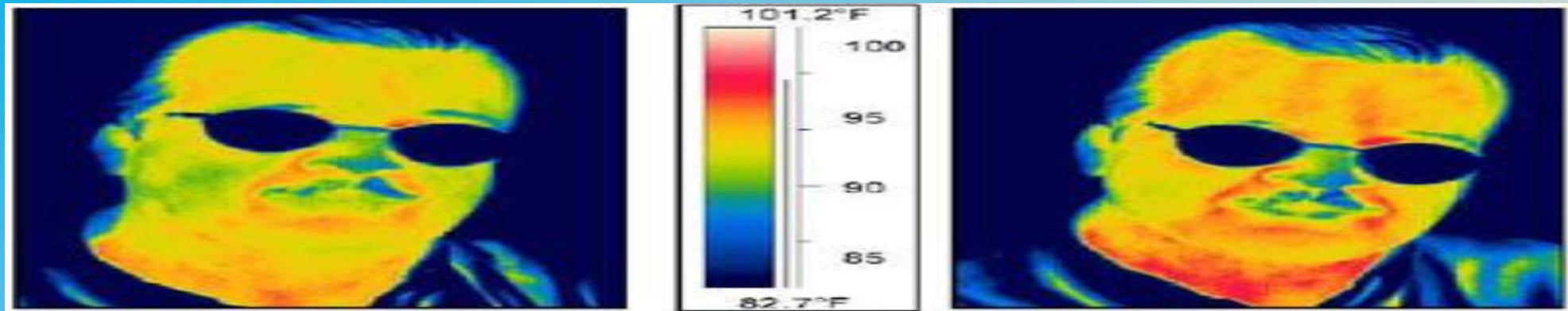
- ساختار ظاهری پوست (Skin Pattern Recognition):

در این روش چین و چروک های صورت بررسی می شود. این ساختار همانند اثر انگشت در افراد مختلف متفاوت است.



شکل ۱۱: بررسی چین و چروک های صورت

- **مشخصه گرمایی صورت (Facial Thermogram):** 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 می شوند (نقشه ای از سطح صورت تهیه می شود). از آنجا که تجمع رگ های زیر پوست صورت در هر فرد شکل متفاوتی دارد، تمایز رنگ بین نقاط مختلف صورت ثابت می ماند. به عنوان مثال در شکل ۱۲ سمت چپ فرد حالت عادی دارد و در سمت راست حالت عصبی دارد، با این حال کاملاً می توان مشاهده کرد که نقاطی که در تصویر سمت چپ قرمز تر از بقیه نقاط بودند باز هم در تصویر سمت راست قرمزتر از باقی نقاط هستند. با این حال تمایز و اختلاف رنگ در نقشه صورت تغییر نکرده است. البته این سیستم به دلیل محدودیت های مختلفی که دارد چندان عمومیت نیافته است.
- **لبخند (Smile):** تفاوت بین چهره در حالت عادی و هنگامی که لبخند می زنیم را تحلیل می کنند.



شکل ۱۲ : سمت چپ فرد حالت عادی و سمت راست حالت عصبی دارد Y.N1402

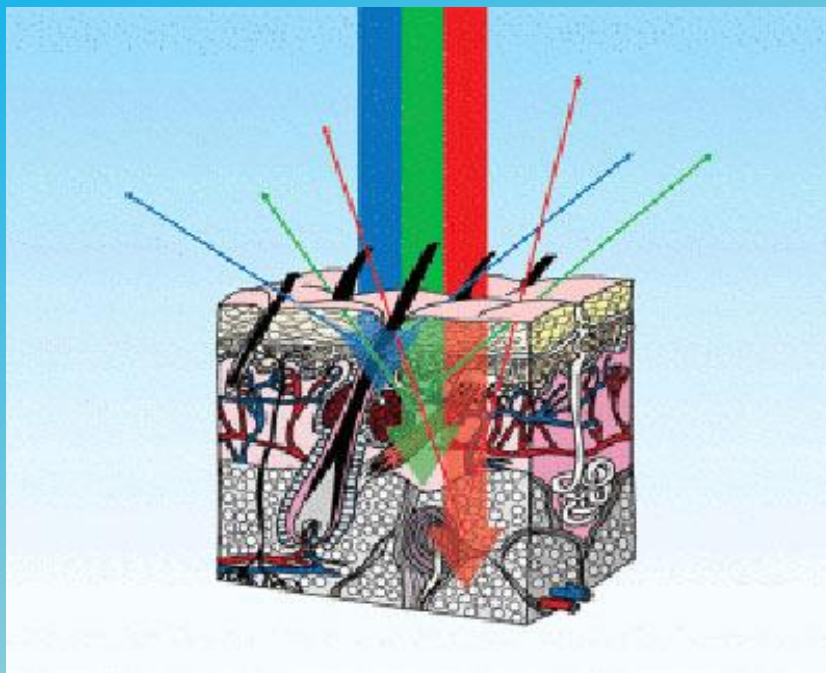
ناخن (Nail)

این متد کاملاً 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 (Nail Bed):** اگر در ابعاد میکروسکوپی به سطح نرم زیر ناخن نگاه کنیم، در می یابیم این سطح دارای برآمدگی هایی موازی و رشته مانند است. این قسمت شامل مویرگ ها، اعصاب و ... است (شکل ۱۶). در طول سن این برآمدگی ها یا رشد طولی دارند یا پهن تر می گردند ولی در هر حال 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 منحصر بفرد است.

طیف الکترو مغناطیسی پوست (Skin Spectrum)

در این روش توسط دیودهای نوری (LED) به سطح پوست یک سری نور خالص با طول موج های مختلف می تابانند و توسط تعدادی فتو دیود (photo diode) 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.



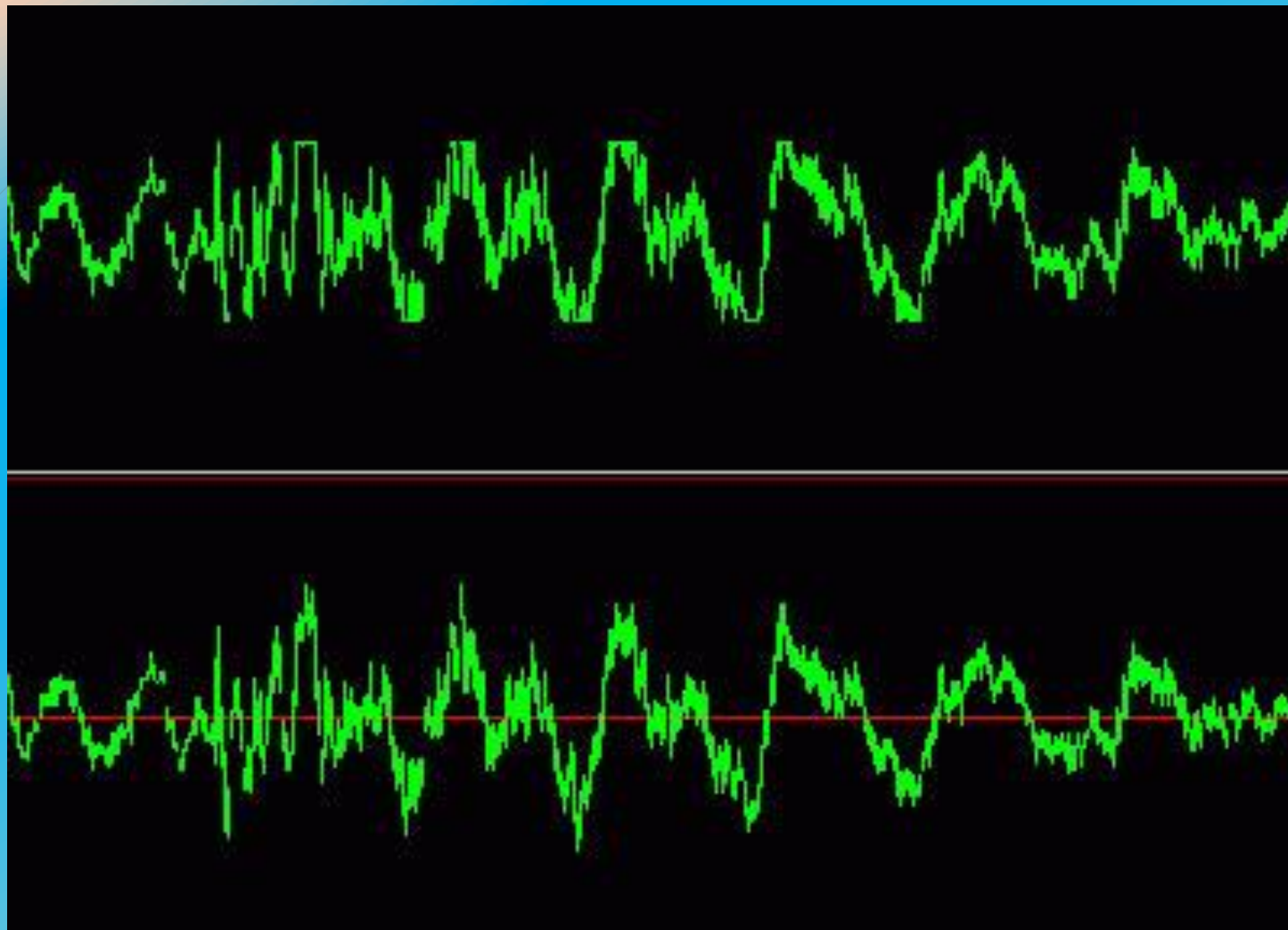
شکل ۱۳ : میزان جذب و انعکاس نور پوست هر فرد متفاوت با دیگران است Y.N1402

صدا (Voice)

این روش هم 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" یا همان Speaker Verification 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.

به خاطر داشته باشید Speaker Verification با Speech Recognition تفاوت زیادی دارد. در Speech Recognition سعی بر اینست که، به طور اتوماتیک دریابیم فرد (مهم نیست چه کسی) چه حرف یا کلمه ای را ادا نموده است. این فیلد پژوهشی در امر دستور دادن، آموزش دادن و درک روبات ها اهمیت بالایی پیدا می کند.



شکل ۱۴ : صدای هر فرد در حالت عادی دارای دامنه های خاصی از فرکانس های مختلف است.

Y.N1402

دست خط و امضا (Signature & Handwriting)

در این روش می توان هم از حالت استاتیک امضا و هم از حالت دینامیک امضا کردن، برای تایید هویت استفاده کرد. روش های دینامیک، از الگوریتم های تشخیص دست خط (Handwriting Recognition) و تشخیص امضا (Signature Recognition) استفاده می کنند. این روش ها، مسیری که قلم فرد برای نوشتن یک کلمه ثابت (امضا) طی آن حرکت می کند، را آنالیز می کنند. از ویژگی های معمول برای مقایسه می توان به سرعت حرکت، مسیر جابجایی و میزان فشار قلم بر کاغذ یا صفحه لمسی اشاره کرد.

حالت استاتیکی امضا (خود شکل نهایی امضا) نیز برای تایید هویت بسیار پرکاربرد و یکی از اولین روش های تایید هویت بوده است ولی در زمینه

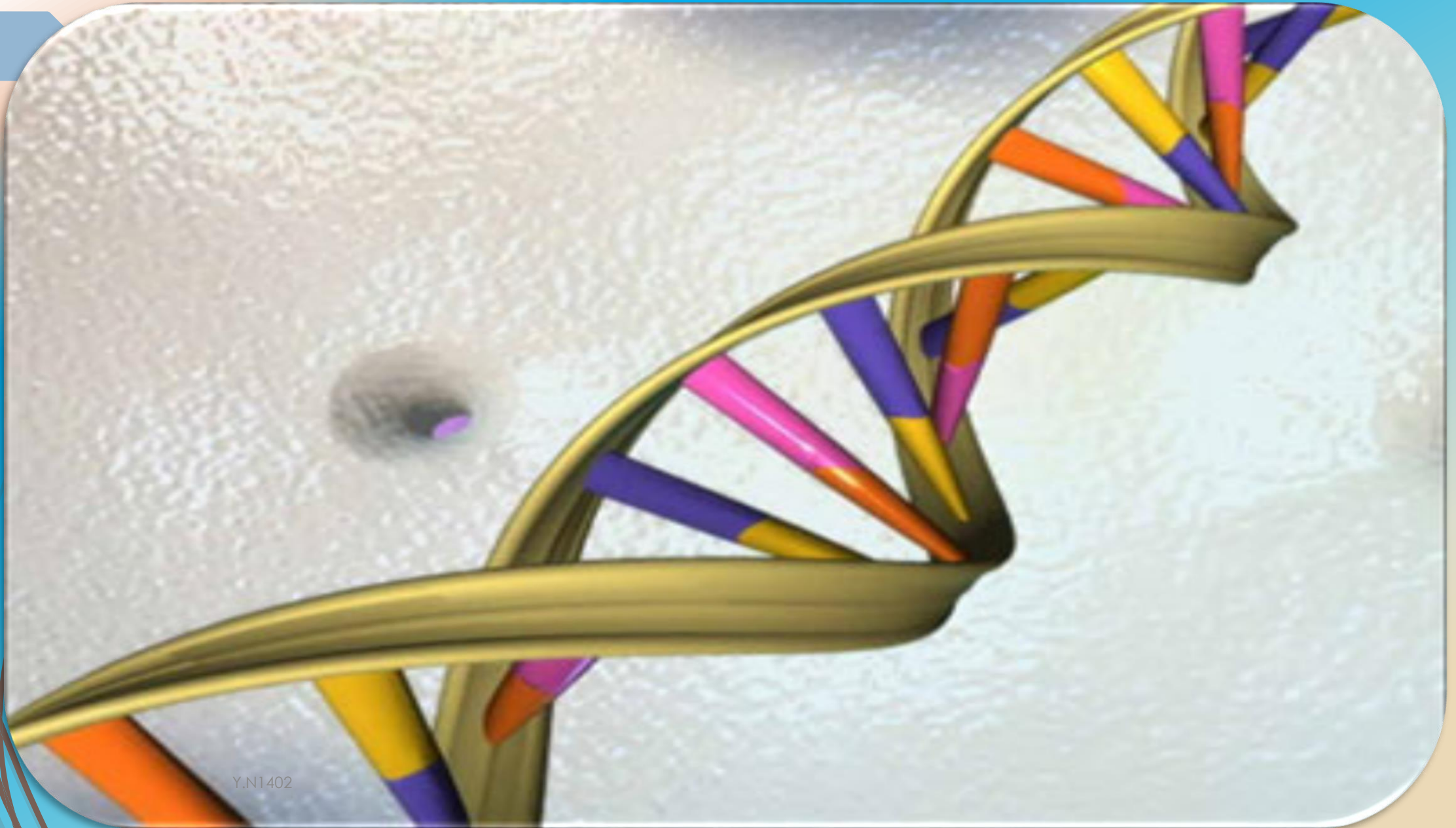
Handwriting Recognition قرار نمی گیرد.

بدون شک Deoxyribonucleic Acid یکی از مطمئن‌ترین روش‌های تایید هویت است.

DNA ، کدی یک بعدی و منحصر به هر فرد است. در حالیکه این روش دقیق‌ترین شکل بیومتریک است ولی از آن در تامین امنیت شبکه‌ها و اماکن و... استفاده نمی‌شود، زیرا این روش اصلاً 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 کاملاً یکسان است و عیب بزرگی برای این متد است ولی از دقت و صحت این روش در تشخیص هویت نمی‌کاهد.

شکل ۱۵ : DNA یکی از مطمئن‌ترین روش‌های تایید هویت است



نمایشگر دمای نقاط بدن (Infrared thermogram)

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، رگ های زیر پوست، گوش و ... به کار رود.

در این روش ها الگوی حرارتی تابش شده از صورت فرد، دست ها و یا حتی رگ های فرد را به کمک یک دوربین 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 یقیناً سبب صرف وقت، هزینه، و همچنین عدم راحتی کاربر می شود.

روش های دیگر

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

- سیگنال قلبی و خون (electrocardiogram)
- عطر و بو مربوط به هر فرد (odour)
- انعکاس صوت در مغز (Reflection of acoustic waves in the head)
- مقاومت الکتریکی پوست (Skin impedance)
- شکل ظاهری دست مشت شده (Knuckle creases Articulations)
- چین خوردگی های پوست انگشت (Finger wrinkles)
- چگونگی در دست گرفتن اجسام (Dynamic Grip Recognition)
- صدای منتقل شده از استخوان های انگشت پس از تحریک یک پالس صوتی (Bone sound transmission)
- موج مغناطیسی منتشر شده از انسان (Bioelectric field)
- نحوه رد گیری چشم (Eye movement tracking)
- توپوگرافی سطح قرنیه (Corneal surface topography)
- شکل سه بعدی انگشت (D Finger surface)
- طیف حاصل از سیگنال های مغزی EEG
- شکل سینوس های جلویی سر (Frontal Sinus Recognition)

مقایسه میزان کاربرد متدها

در این بخش، مقایسه ای بین روش های متداول تر بیومتریک انجام می دهیم. ساده ترین و جامع ترین نوع مقایسه را می توان در جداول ۱ و ۲ مشاهده کرد. این دو جدول به گونه ای کامل و واضح مقایسه را نمایش می دهند.

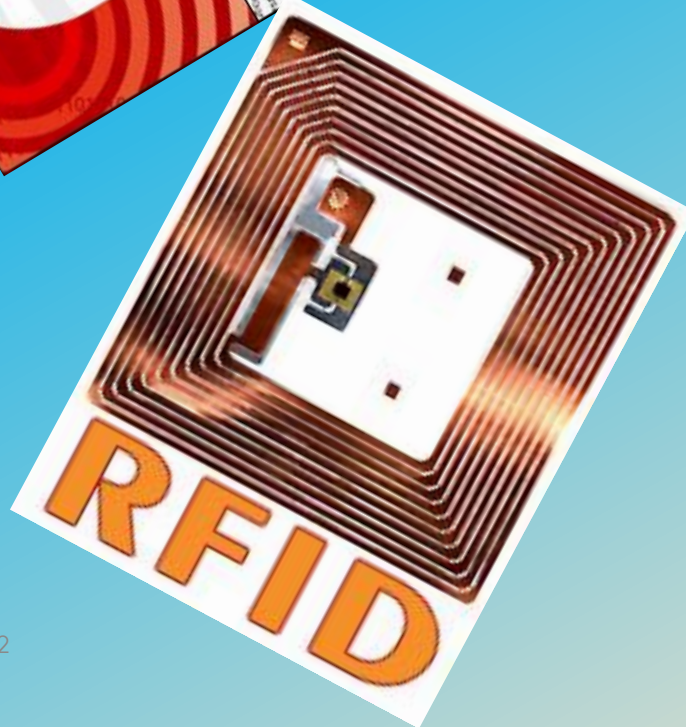
جدول ۱

Biometric	Security Level	Long-term Stability	User Acceptance	Ease of Use	Low Cost	Hardware	Standards
Fingerprint	→→→	→→→	→→	→→→	✓	Special, cheap	Yes
Facial Recognition	→→	→→	→→	→→	✓	Common, cheap	?
Hand Geometry	→→	→→	→→	→→→	✗	Special, mid-price	?
Speaker Recognition	→→	→→	→→→	→→→	✓	Common, cheap	?
Iris Scan	→→→	→→→	→→	→→	✗	Special, expensive	?
Retinal Scan	→→→	→→→	→→	→	✗	Special, expensive	?
Signature Recognition	→→	→→	→→	→→→	✓	Special, mid-price	?
Keystroke Recognition	→→	→	→→→	→→→	✓	Common, cheap	?
DNA	→→→	→→→	→	→	✗	Special, expensive	Yes

Biometric	Verify	ID	Accuracy	Reliability	Error Rate	Errors
Fingerprint	✓	✓	●●●●●	➡➡➡	1 in 500+	dryness, dirt, age
Facial Recognition	✓	✗	●●●●	➡➡	no data	lighting, age, glasses, hair
Hand Geometry	✓	✗	●●●●	➡➡	1 in 500	hand injury, age
Speaker Recognition	✓	✗	●●●	➡	1 in 50	noise, weather, colds
Iris Scan	✓	✓	●●●●●●	➡➡➡	1 in 131,000	poor lighting
Retinal Scan	✓	✓	●●●●●●	➡➡➡	1 in 10,000,000	glasses
Signature Recognition	✓	✗	●●●	➡	1 in 50	changing signatures
Keystroke Recognition	✓	✗	●	➡	no data	hand injury, tiredness
DNA	✓	✓	●●●●●●	➡➡➡	no data	none

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 ارائه 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 ارائه نادیده رفته شد است.

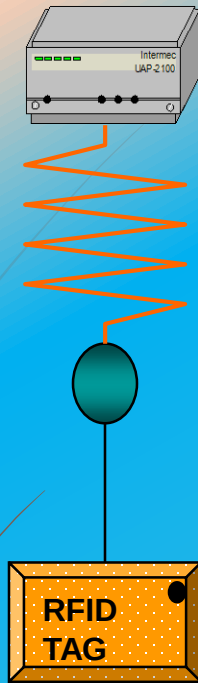
RFID & applications



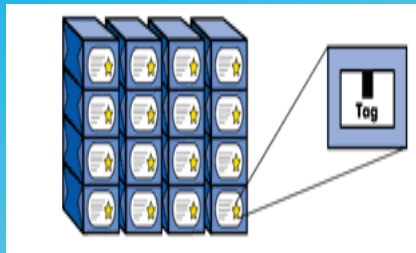
RFID از سه قسمت اصلی تشکیل شده است:

- A Scanning Antenna (آنتن)
- A Transceiver with a decoder (گیرنده با اشکارساز)
- A Transponder(The RFID tag) (فرستنده)

RFID (Radio Frequency Identification)



- ابزار تشخیص امواج رادیویی
- دستگاه های الکترونیکی کوچک شامل یک تراشه و یک آنتن
- تراشه: قادر به ذخیره حداکثر 2000 بایت اطلاعات
- امکان ذخیره سازی، بازیابی و اصلاح اطلاعات بر روی tag های RFID

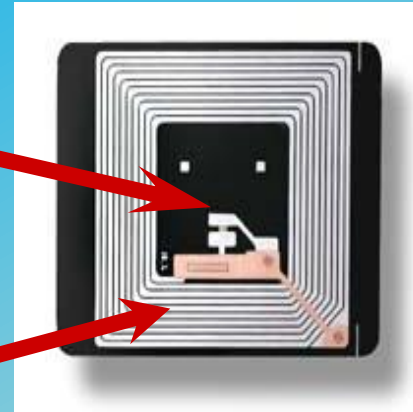


A Transceiver:



A Transponder(The RFID tag)

Chip



Antenna

نحوه انجام عملیات:

- آنتن (Scanning Antenna) امواج رادیویی را منتشر می کند.
- این امواج دو عمل اصلی انجام می دهند:
 - 1) ارتباط با tag (Transponder)
 - 2) تامین انرژی مورد نیاز tag (tag های passive)
- وقتی tag در میدان الکترومغناطیسی ایجاد شده در اطراف آنتن قرار می گیرند، تراشه (chip) روی tag بیدار می شود.
- تراشه اطلاعات موجود در tag را در اختیار آنتن قرار می دهد.
- نقش Transceiver: کنترل خطوط ارتباطی و داده ها

یک دستگاه Reader در واقع ترکیبی است از Scanning Antenna و Transceiver:



شکل زیرچگونگی عملکرد را توضیح می دهد:



انواع RFID

از نظر محدوده فرکانس

RFID در سه محدوده فرکانس مختلف کار می کند:

1- فرکانس پایین (LF) : Low
Frequency

2- فرکانس بالا (HF) : High
Frequency

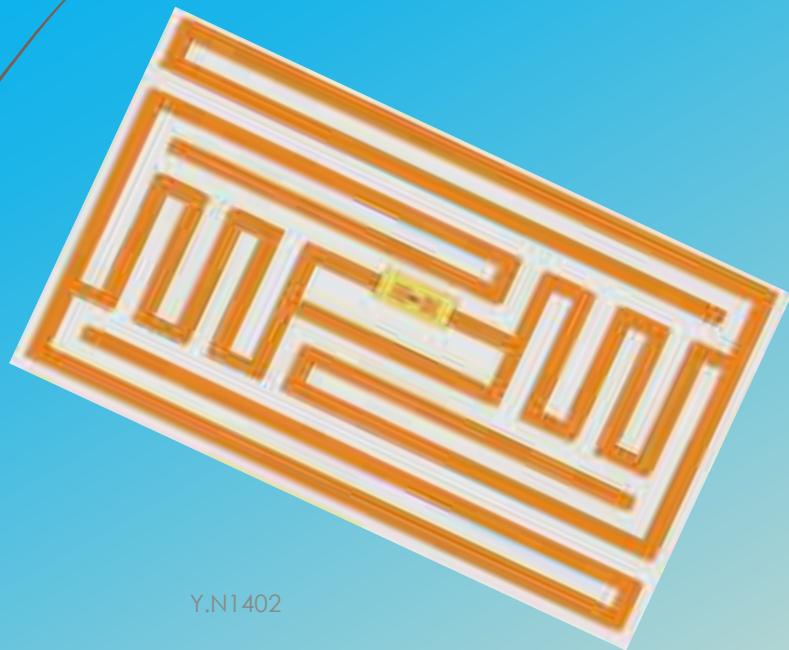
3- فرکانس بسیار بالا (UHF) : Ultra
High Frequency

ویژگی های این سه دسته در جدول زیر خلاصه شده است:

نوع	محدوده فرکانس	توانایی عبور سیگنال از مواد	توانایی خوانده شدن همزمان چند tag	قیمت	کاربرد نمونه
LF	120-134 KHz	زیاد	ضعیف	گران	شناسایی حیوانات در مراکز پرورش حیوانات یا دامداری ها
HF	13.56 MHz	کم	نسبتا خوب	ارزانتر	کتابخانه ها
UHF	902-915 MHz	بسیار کم	بسیار عالی	ارزان ترین	حمل و نقل کالاها و موجودی ها

انواع Tag های

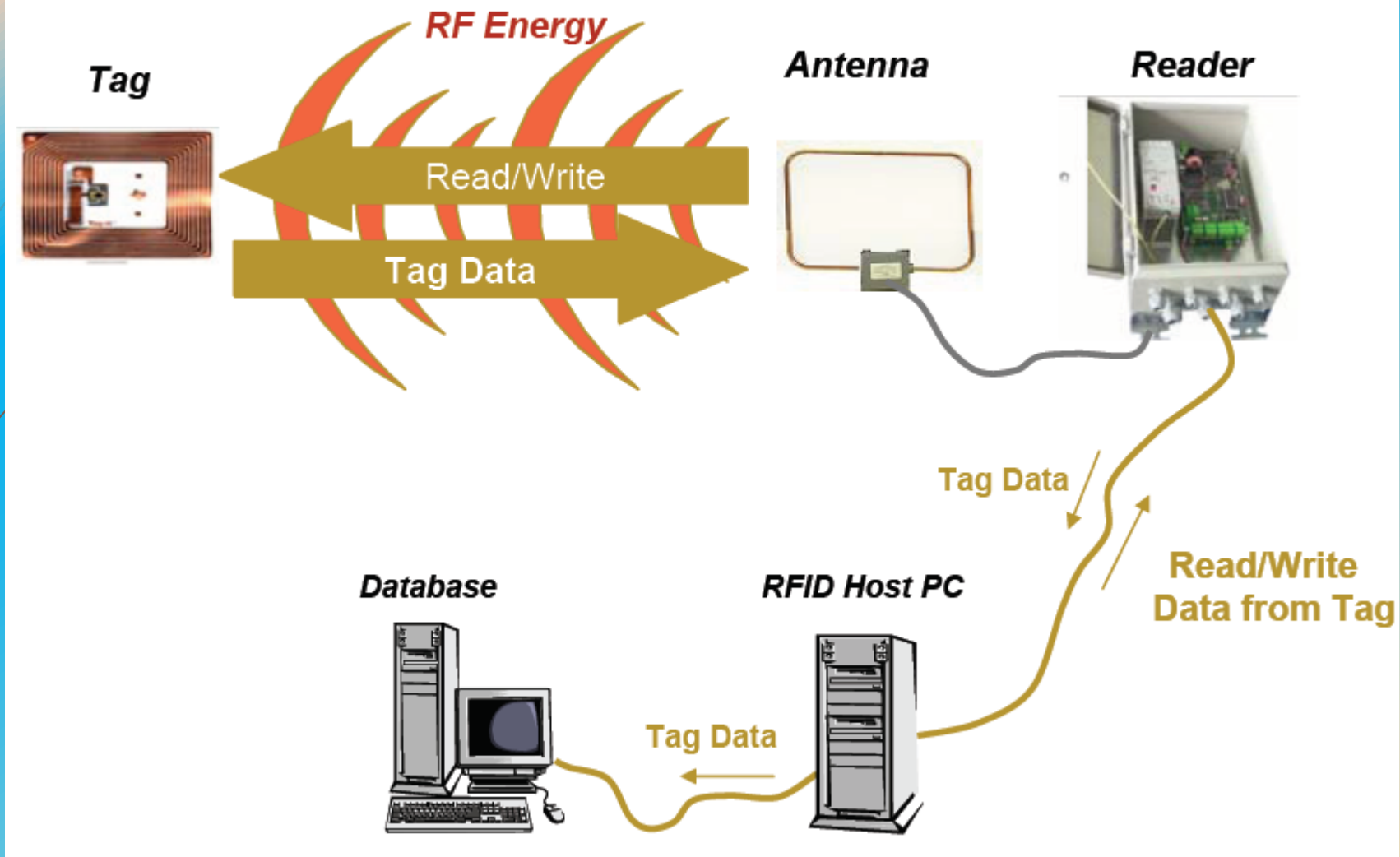
RFID



به طور کلی سه نوع برچسب RFID وجود دارد:

- Passive (غیر فعال) : هیچ منبع تولید انرژی درونی ندارد و انرژی خود را از طریق سیگنال های RF فرستاده شده از سوی دستگاه Reader دریافت می کنند.
- Semi-passive (نیمه فعال) : باتری کوچکی انرژی لازم برای فعال شدن مدار داخل آن را فراهم می کند.
- Active (فعال) : دارای منبع انرژی داخلی است که توانایی انتقال اطلاعات به فواصل دورتر را هم فراهم می سازد.

Passive RFID Illustration



نکات بهداشتی:

- جنس برچسب : سازگار با بافت های بدن
- اندازه برچسب : تقریبا به اندازه یک دانه برنج
- جلوگیری از جابجایی tag در داخل بدن (با تزریق موادی برای احاطه شدن tag توسط بافت های اطراف آن)
- باید بسیار نزدیک به سطح پوست بدن قرار گیرند. (چون فقط از فاصله خیلی نزدیک خوانده می شوند.)

