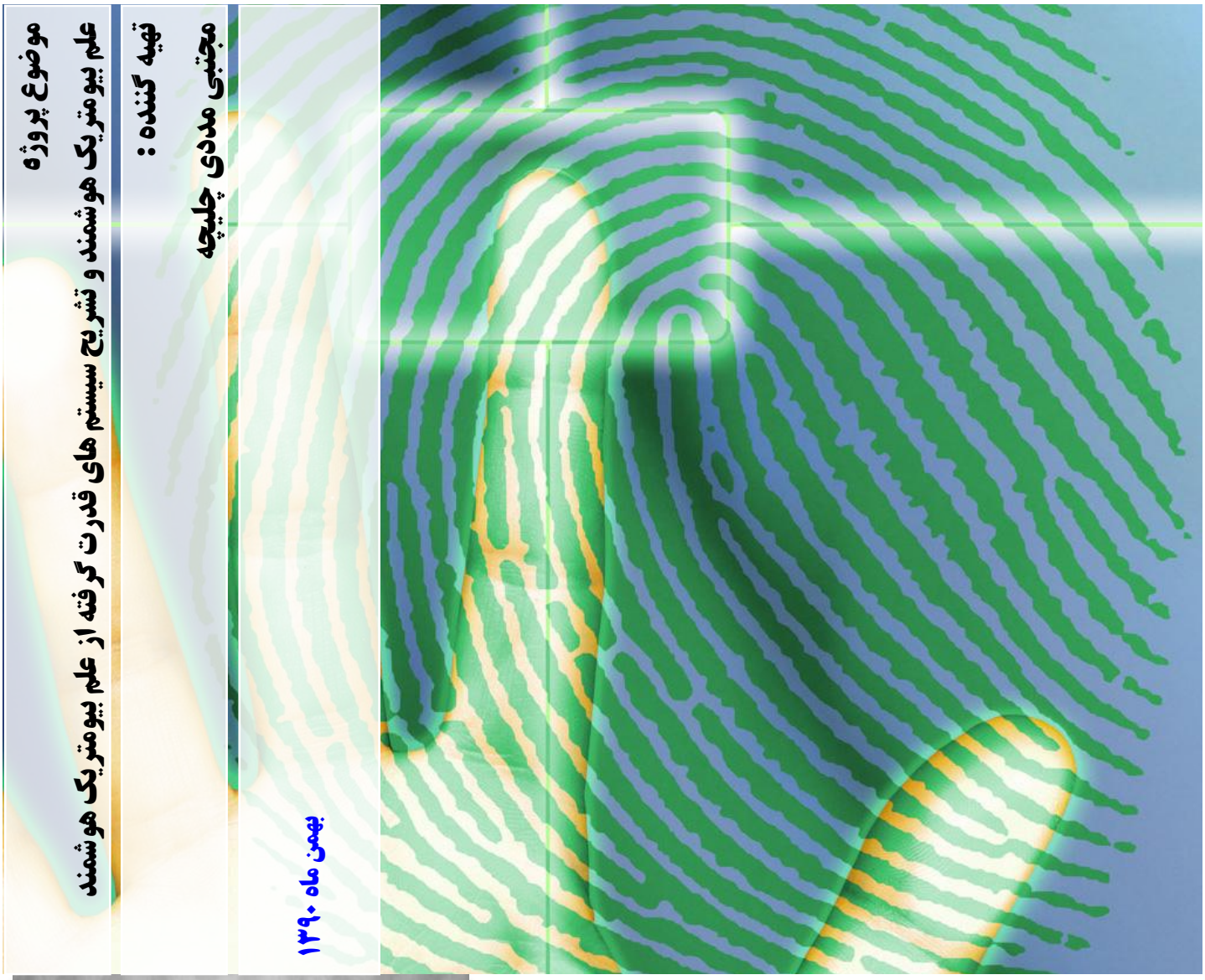
www.prozhe.com



موضوع پروژه

علم بیومتریک هوشمند و تشریح سیستم های قدرت گرفته از علم بیومتریک هوشمند

تهیه کننده :

مجتبی مددی چلیچه

بهمن ماه ۱۳۹۰

از دیر باز انسان برای بقا، نیاز به تشخیص دوست از دشمن داشته است و تشخیص هویت برای وی امری حیاتی بوده و هست، لذا امروزه سعی در مکانیزه سازی سیستمهای شناسایی یا تشخیص هویت شده است. "این پیشرفتها دلیل بر نیاز جامعه و جهان است".[۱] نیازی که پیشرفت در آن باعث کاهش تخلفات، افزایش امنیت، تسریع در امور روزمره و ... شده است. در گذشته جهت شناسایی جرم و جنایتکار، از روال شناسایی اثر انگشت و چهره نگاری استفاده می شده، اما اکنون سیستمهای مکانیزه ای ایجاد شده است.

مرکز آموزش عالی جهاد دانشگاهی
شهرکرد – خیابان حافظ شمالی – خیابان یاسر
۰۳۸۱-۳۳۴۰۹۶۴

www.prozhe.com

www.prozhe.com

مرکز آموزش عالی جهاد دانشگاهی

شعبه شهرکرد

علم بیومتریک هوشمند و تشریح سیستم های قدرت گرفته از علم بیومتریک هوشمند

Biometric smart power systems ranging from science to explain the science and biometric smart

www.prozhe.com

www.prozhe.com

موضوع پروژه : علم بیومتریک هوشمند

استاد راهنما : جناب آقای مهندس عبدالهیان

بسم الله الرحمن الرحیم

www.prozhe.com

www.prozhe.com

مرکز آموزش عالی جهاد دانشگاهی

شعبه شهرکرد

موضوع تحقیق :

علم بیومتریک هوشمند و تشریح سیستم های قدرت گرفته از علم بیومتریک هوشمند

Biometric smart power systems ranging from science to explain the science and biometric smart

تکلیف تحقیق درس شیوه ارائه مطالب علمی و فنی

استاد مربوطه :

جناب آقای مهندس عبدالهیان

تهیه کنندگان :

مجتبی مددی چلیچه

شماره دانشجویی :

****

بهمن ۹۰

www.prozhe.com

www.prozhe.com

فهرست مطالب

معرفی علم بیومتریک..... ٦

مقدمه..... ٦

سیستمهای تشخیص هویت..... ٦

بیومتریک چیست؟..... ٧

طبقه بندی متدهای بیومتریک..... ٧

معماری سیستمهای بیومتریک..... ٧

پارامترهای مهم در سیستم‌های بیومتریک..... ٨

تکنولوژیهای بیومتریک..... ٩

شناسایی از طریق اثر انگشت..... ٩

مراحل پردازش تصویر در شناسایی بر اساس اثر انگشت..... ٩

شناسایی از طریق چهره..... ١١

شناسایی از روی عنبیه چشم..... ١١

شناسایی از روی شبکیه چشم..... ١٢

شناسایی از روی نمودار حرارتی چهره..... ١٢

شناسایی از روی نحوه راه رفتن..... ١٣

شناسایی از روی هندسه دست..... ١٣

ترکیبات بیومتریک..... ١٣

اثر انگشت هم جایزالخطاست!..... ٢٠

اثر انگشت..... ٢١

کاربردهای بیومتریک..... ٢٧

آزمایشگاه سیستم های بیومتریک – SfinGe..... ٣٩

کارت شناسایی بیومتریک چیست؟..... ٤١

بیومتریک ؛ عبور بدون رمز..... ٤٤

منابع..... ٥٥

www.prozhe.com

www.prozhe.com

معرفی علم بیومتریک

این مقاله به معرفی سیستمهای تشخیص هویت که مهمترین و دقیق‌ترین آنها بیومتریک است خواهد پرداخت. پس از تعریف بیومتریک به تعریف معماری سیستم های بیومتریک می پردازیم و درمی یابیم که هر سیستم بیومتریک با چه معماری ای کار می‌کند. در این مقاله همچنین در مورد چند تکنولوژی بیومتریک هم توضیح داده می شود مانند اثر انگشت، عنبیه چشم، نحوه راه رفتن، چهره و ... اما به دلیل اینکه سیستم اثر انگشت از اهمیت بیشتری نسبت به دیگر سیستم ها برخوردار است بیشتر به تجزیه و تحلیل این سیستم خ واهیم پرداخت و ابتدا به معرفی خطوط و نقاط مشخصه انگشت که در اصطلاح به آنها ریزه کاری گفته می شود می پردازیم و سپس روش های پردازش این نقاط برای رسیدن به الگویی برای شناسایی هویت را بیان خواهیم نمود . پس از آن سنسورهای مختلف که همگی همراه با شکل برای فهم بیشت ر مطرح شده اند مورد بحث قرار خواهند گرفت و سپس این سنسورها با هم مقایسه می‌شوند و مزیت هر یک بیان می‌شود. سپس به معرفی سایر سیستم‌ها خواهیم پرداخت و در انتها به معرفی مفهوم ترکیبات بیومتریک و روش های متنوع آن خواهیم پرداخت .استفاده از روش ترکیب بیومتریک کارایی، امنیت، دقت سیستم را افزایش می‌دهد.

مقدمه

از دیر باز انسان برای بقا، نیاز به تشخیص دوست از دشمن داشته است و تشخیص هویت برای وی امری حیاتی بوده و هست، لذا امروزه سعی در مکانیزه سازی سیستمهای شناسایی یا تشخیص هویت شده است . "این پیشرفتها دلیل بر نیاز جامعه و جهان است ".[۱] نیازی که پیشرفت در آن باعث کاهش تخلفات، افزایش امنیت، تسریع در امور روزمره و ... شده است. در گذشته جهت شناسایی جرم و جنایتکار، از روال شناسایی اثر انگشت و چهره نگاری استفاده می شده، اما اکنون سیستمهای مکانیزه ای ایجاد شده است.

سیستمهای تشخیص هویت

توکن معمولاً چیزی است که شما به همراه خود دارید و میتوان گفت سند هویت شماست، مانند : کارتهای هوشمند، کارتهای مغناطیسی، کلید، پاسپورت، شناسنامه و ... این اشیاء دارای نواقصی هستند همچون : گم شدن، عدم همراه بودن شخص، فرسوده شدن و جعل شدن.

دومین نوع سیستمهای شناسایی دانش نام دارد، یعنی چیزی که شما بخاطر میسپارید مانند :پسورد و پین کد . البته این سری نیز دارای نواقصی هستند مانند: فراموش کردن و لو رفتن.

www.prozhe.com

www.prozhe.com

دسته سوم سیستمهای مبتنی بر بیومتریک است . این سیستمها از خصیصه های فیزیولوژیکی و رفتاری انسان جهت شناسایی استفاده می کنند . این روش دیگر معایب روشهای قبل را ندارد و امنیت و دقت را تا حد بسیار زیادی افزایش داده است.

بیومتریک چیست؟

• اندازه گیری و تحلیل آماری داده های بیولوژیکی • بیومتریک اشاره دارد به تکنولوژیی برای اندازه گیری و آنالیز مشخصات بدن افراد جهت تشخیص هویت شخص • شناسایی اتوماتیک یک شخص با استفاده از ویژگیهای اختصاصی (مشخصات فیزیولوژیکی یا رفتاری)(تعریف در کنسرسیوم بیومتریک)

دو اصطلاح مهم در بیومتریک: تطابق یک به یک، عمل تطابق الگوهای کاربر با داده‌های ذخیره شده . تطابق یک به چند، یافتن یک الگو از میان الگوهای ذخیره شده جهت شناسایی کاربر.

طبقه بندی متدهای بیومتریک

عموما در سیستمهای بیومتریک از دو نوع ویژگی مختلف افراد جهت شناسایی استفاده می شود که در ذیل به آنها اشاره می کنیم . • (پارامترهای فیزیولوژیکی) اساس شناسایی در این کلاس، اندازه گیری و آنال یز مشخصه های ثابت یک شخص می باشد. • (پارامترهای (اثرΥرفتاری) شناسایی الگوهای رفتاری مشخص یک فرد پارامترهای فیزیولوژیکی : (شناسایی از Υ (شناسایی از طرق عنبیه چشم) Υ (شناسایی از روی شبکیه چشم) Υانگشت) (شناسایی از طریق Υ (شناسایی از طریق امضاء) Υروی هندسه دست) پارامترهای رفتاری: (شناسایی از روی شدت ضربه شخص بر روی کیبورد) در این مقاله ما سعی بر معرفیΥصدا) این سیتمها داریم.

معماری سیستمهای بیومتریک

تمامی سیستمهای بیومتریک دارای یک معماری کلی یکسان در ساخت هستند که به آنها فضای Υ تصمیم گیری Υ تطبیق Υ پردازش سیگنال Υ درخواست داده‌ها Υاشاره میکنیم. محیط انتقال داده ها زیر سیستم درخواست داده در این زیر سیستم Υذخیره سازی داده های خام، که از یک فرد، توسط یک سنسور ویژه اسکن شده است، وارد سیستم می شود. فرایندی که در این زیر سیستم انجام می شود:

- دریافت داده‌ها توسط سنسور

www.prozhe.com

www.prozhe.com

- تبدیل داده های(سیگنالها) دریافتی از سنسورها به فرم مناسبی(A/D) جهت ارسال به زیر سیستم پردازش سیگنال

زیرسیستم پردازش سیگنال عملیات این زیر سیستم به شرح ذیل می باشد : ۱- دریافت داده‌های خام از زیر سیستم جمع آوری داده ۲- استخراج خصیصه ۳- عملیات فیلترینگ جهت حذف نویز ۴- اصلاح داده ها ۵- تبدیل داده‌های دریافتی به فرم لازم(تولید الگو) برای زیر سیستم تطبیق. لازم بذکر است که از داده‌های دریافت شده در این زیر سیستم، پس از پردازش، یک الگو از برخی ویژگیهای موجود تولید و ذخیره می شود. در واقع این الگوی تولید شده مورد مقایسه و شناسایی قرار می گیرد . ماهیت این الگو که از روی یک شابلون از پیش تعریف شده تولید می شود(یک استاندارد ثابت)، ماتریسی از صفر و یک می باشد . در واقع این شابلون قسمتهای مورد اندازه گیری از یک نمونه را بر می گرداند. زیرسیستم تطبیق خروجی این زیر سیستم از مقایسه دو الگو بدست می آید . فرایند این زیر سیستم شامل : دریافت داده‌های پردازش شده(الگو) از زیر سیستم قبل و دریافت الگوهای ذخیره شده مقایسه الگوی تولید شده در زیر سیستم قبل، با الگوهای موجود زیر سیستم تصمیم گیری این زیر سیستم پس از اجرای زیر سیستم قبل فراخوانی می شود که وظیفه آن تصمیم گیری بر روی تطابق انجام شده متناسب با درخواست است. در این مرحله یک حد یا آستانه در نظر گرفته شده است . اگر امتیاز بیشتر یا برابر این آستانه باشد، کاربر تائید می شود در غیر اینصورت کاربر پذیرفته نمی شود . زیر سیستم فضای ذخیره سازی شامل الگوهایی است که در هنگام ثبت نام از کاربران بدست آمده است . ممکن است برای هر کاربر یک یا چند الگو ذخیره شده باشد. زیر سیستم محیط انتقال وظیفه این بخش انتقال داده ها، بین اجزاء یک سیستم بیومتریک است.

پارامترهای مهم در سیستم‌های بیومتریک

در همه سیستمهای بیومتریک پارامترهایی موجودند که ویژگیها و قابلیتهای سیستم شما را معرفی میکنند . ۱- نرخ پذیرش اشتباه این پارامتر تعیین کننده امکان پذیرش کاربر جعلی از کاربر اصلی می باشد. این پارامتر باید تا جای ممکن کوچک باشد. ۲- نرخ عدم پذیرش اشتباه این مقیاس نمایانگر اینست که تا چه اندازه شخص اصلی اشتباها پذیرش نمی شود (حساسیت بسیار بالا). این پارامتر نیز باید تا حد مورد نیاز کم باشد . ۳- نرخ خطای مساوی : کاهش نرخ پذیرش اشتباه باعث افزایش غیر تعمدی نرخ عدم پذیرش اشتباه میشود . نقطه ای که میزان نرخ عدم پذیرش اشتباه با نرخ پذیرش اشتباه برابر می‌شود نقطه نرخ خطای مساوی است. هرچه میزان این پارامتر کمتر باشد نمایانگر اینست که سیستم دارای یک حساسیت بهتر و توازن خوبی است . ۴- نرخ ثبت نام نادرست احتمال خطایی که در هنگام نمونه بردای جهت ثبت در پایگاه داده، در خصوص تشخیص صحیح ممکن است رخ هد.

www.prozhe.com

www.prozhe.com

تکنولوژیهای بیومتریک

(اثر انگشت) (هندسه دست) (اندازه گیری شبکیه چشم) (اندازه گیری عنبیه) (تشخیص چهره) (تشخیص امضاء) (تشخیص صدا) (آزمایش دی- ان-ای) (تشخیص از روی سی هرگ دست) (نمودار حرارتی چهره) (شدت ضربه بر روی صفحه کلید) (شکل گوش) (بوی بدن)

شناسایی از طریق اثر انگشت

بدلیل اهمیت این سیستم، بیشتر به تجزیه و تحلیل آن خواهیم پرداخت . یکی از قدیمی ترین روشهای تشخیص هویت، روش شناسایی از طریق اثر انگشت می باشد .نوک انگشت دارای یکسری خطوط است که از یک طرف انگشت به طرف دیگر ادامه دارد.این خطوط دارای یکسری نقاط مشخصه می باشند که به آنها ریزه کاری گویند. این ریزه کاریها شامل کمانها، مارپیچها، حلقه ها، انتهای لبه ها، انشعابها، نقطه ها (شیارهای نزدیک به لبه ها)، جزایر(دو انشعاب نزدیک به هم)، تقاطع (نقطه تلاقی دو یا چند لبه)، منفذها می باشند. در واقع ما در این سری از سیستمها الگوهای تولید شده از این ریزه کاریها را مورد مقایسه قرار می دهیم

در تشخیص اثر انگشت دو روش عمده وجود دارد: در روش اول یک شابلون از محل قرار گیری ریزه کاریهای : "انتهای لبه‌ها، انشعابها، کمانها، مارپیچها و حلقه ها" تهیه می‌شود و الگوها بر این اساس تولید می شوند. در حالت دیگر مابقی ریزه کاریهای ذکر شده نیز الگو برداری می شوند ."با مقایسه نوع، راستا (جهت) و ارتباط(موقعیت) ریزه کاریها عمل شناسایی انجام می شود . " در روش دوم از مقایسه نواحی در برگیرنده همه ریزه کاریهای ذکر شده و نیز علامت‌های مجزای دیگر و داده های حاصل از مقایسه مجموعه لبه ها در این نواحی، استفاده می شود . عموما سایز الگو در روش دوم دو الی سه برابر بزرگتر از روش اول می باشد . در روش اول تقریبا امکان ندارد که بتوان تصویر اثر انگشت را از الگوی مبنا بدست آورد بدلیل اینکه از تعدادی از ریزه کاریها الگوبرداری مشود و مابقی ترتیب اثر داده نمی شوند، ولی از روش دوم می توان به اثر انگشت نیز رسید

مراحل پردازش تصویر در شناسایی بر اساس اثر انگشت

حالت اول شمای یک اثر انگشت پردازش نشده را نمایش می دهد . در مرحله دوم جهت خطوط اثر انگشت توسط متدهای خاصی تولید می شود تا از آن بتوان در شناخت جهت هر ریزه کاری استفاده کرد . در حالت سوم نویزهای موجود در تصویر اول را حذف کرده سپس مرز بین لبه ها و شیارها مشخص می شود. در مرحله چهارم میزان رنگ تصویر حاصله را کاهش می دهند تا نویزهای کوچک باقیمانده نیز حذف شوند و نیز حجم تصویر نیز

www.prozhe.com

www.prozhe.com

کاهش یابد.در مرحله پنجم ریزه کاریها علامت گذاری می شوند و در مرحله آخر نیز این ریزه کاریها بیکدیگر متصل میگردند که ماتریس حاصل از شکل بد ست آمده از این نواحی و ماتریس حصل از جهتها در شکل دوم و نیز ماتریس شامل نوع ریزه کاریهای در نظر گرفته شده، الگوی ما را تولید میکند .مراحل در شکل زیر به نمایش گذاشته شده اند : سنسورهای مورد استفاده در روش شناسایی با استفاده از اثر انگشت : ۱-سنسور نوری در این تکنولوژی کاربر انگشت خود را بر روی یک سطح پلاستیکی یا شیشه ای تمیز قرار می دهد، سپس یک اسکنر (CCD (شروع به اسکن کردن و تصویر برداری از انگشت می کند . این اسکنرها دارای تعدادی گیرنده نوری هستند که بصورت سطری در کنار یکدیگر قرار گرفته اند، که نوسانات و تغیرات شدت نور دریافتی را اندازه گیری می کنند . با تابش یک دسته شعاع نوری با شدت ثابت به انگشت، بازتاب این شعاع نوری توسط این دوربینهای CCD اندازه گیری می شود . این آرایه‌های CCD تصویری با رزولوشن ۶۰۰-۷۲dpi را نمایش می دهند. که البته قابلیت تصویر برداری تا ۱۰۰۰dpi را دارا می باشند. تصویر اثر انگشت تولیدی بصورت یکسری لبه‌های تاریک و شیارهای روشن نشان داده می شود که در ابتدا نامفهومند و با عملیات پردازش تصویر، تصویر واضحی از اثر انگشت تولید می شود ۲-سنسور خازنی عملیات این سری از سنسورها بصورت جوشن خازنی است (یک ماتریس از خازنهای کنار هم). با تماس انگشت بر سطح سنسور، بین لبه‌های اثر انگشت و سنسور، یک ظرفیت خازنی مطابق با شکل ایجاد می شود که با اندازه گیری این سطوح خازنی و پردازش این سیگنالها، یک تصویر دیجیتالی بصورت ترکیبی از رنگهای مشکی، سفید و خاکستری (روشن و تیره) ۸بیتی بدست می آید . شکل زیر بیانگر این موضوع است . همانطور که در شکل مشاهده میکنید، انگشت باعث برقراری ارتباط بین دو الکترود می‌شود که این امر باعث بوجود آمدن فضای خازنی در بین این دو الکترود شده است. تغییرات فاصله ای که بین لبه ها و شیارهای انگشت وجود دارد، باعث پیدایش یک سیگنال ولتاژی در فضای خازنی می شود که در شکل دوم نشان داده شده است . با توجه به اینکه فاصله بین پیک لبه و شیار از یک نقطه به یک نقطه دیگر تغییر می کند، داده خام برگردانده شده توسط سنسور به یک تصویر درهم که دارای یکسری سایه های خاکستری است، تبدیل می شود. که از یک الگوریتم دیگر جهت تکمیل و تصحیح این تصویر استفاده می شود رزولوشن این تصویر توسط اندازه و تقسیم بندی سلولهای سنسور تعیین می گردد. بعنوان مثال برای یک رزولوشن ۵۰۰dpi به یک سنسور با اندازه سلول ۵۰۰ میکرون نیاز است. عموما این سری سنسورها رزولوشن ۵۰۰-۲۵۰dpi را تولید می کنند. دقت این سنسورها تا اندازه ای پایین است و نیاز به بازسازی تصویر بیشتری دارند . ۳-سنسور آلتراسوند این سنسورها از یکسری فرستنده- گیرنده‌های صوتی استفاده می کنند . آنها امواج آلتراسوند را به شئ ساطع می کنند، سپس به حالت گیرنده رفته و امواج بازگشتی را ذخیره می کنند. (مطابق شکل) این امواج توسط تکنیکهای ویژه تصور صوتی پردازش می شوند . نحوه الگو برداری از یک سطح کثیف توسط سنسورهای آلتراسوند

www.prozhe.com

www.prozhe.com

فرکانس ارسالی و دریافتی این سنسورها قابل تنظیم است . این ویژگی باعث می شود که فرکانسهای ناهمگن دریافتی را حذف کند. فرکانسهای این سنسورها را می توان طوری تنظیم نمود که از سلولهای بیجان عبور کنند که این یک مزیت بزرگ سنسورهای آلتراسوند است . 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

شناسایی از طریق چهره

فرم هندسی یک چهره نیز از پارامترهای مورد اندازه گیری در سیستمهای بیومتریک است ولی نمی توان گفت که جزء خصیصه‌های منحصر بفرد افراد است لذا این سیستمها در جاهایی که تعداد کاربران کم است و نیز زمانهای الگوبرداری درازمدت نیست، این سیستمها مناسبند. از دیگر کاربردهای این سیستمها، استفاده در سیستمهای مالتی بیومتریک جهت افزایش دقت است . تصویر چهره یک کا ربر می تواند توسط یک دوربین سیاه و سفید با استاندارد که یک رزولوشن ۲۴۰*۳۲۰ و اقلا ۳ تا ۴ فریم را تولید کند، گرفته می شود . دو روند اصلی برای تشخیص چهره انجام می شود i روند کلی یا کل چهره i خصوصیات پایه ای چهره خصوصیات پایه ای چهره بر شناسایی و تشخیص نقاط ثابت و معین در چهره که با مرور زمان کمترین حساسیت و تغییری را از خود نشان می دهند شامل: قسمتهایی از چشم، اطراف بینی و دهان و بخشهایی که استخوان گونه را احاطه کرده اند تکیه دارد. یا روند کلی یا کل چهره در این روش یک تصویر کامل و یکجا از چهره، بدون لوکالیزه کر دن نقاط ویژه مورد پردازش قرار می گیرد . این متد از تکنولوژیهای زیرجهت پردازش چهره بهره می شبکه های عصبی در کل سیستمهای این چنینی دارای دقت بالایی Υ تحلیل آماری Υگیرد: نیستند بدلیل اینکه چهرها کاملا منحصر بفرد نیستند و گاه اتفاق می افتد که دو نفر(مخصوصا دو قلو ها) از نظر چهره با هم مشابهند. لذا از اینگونه سیستمها فقط در مکانهایی استفاده می شوند که امنیت تا حد بسیار زیاد مورد نظر نباشد.

شناسایی از روی عنبیه چشم

عنبیه قسمت رنگی چشم است که ترکیبی است از نوعی ماهیچه به شکل دایره با یکسری خطوط شعاعی، لایه ای یا توری مانند که در پیش از تولد انسان شکل گرفته است و تا زمان مرگ تقریبا هیچ تغییری نمیکند . این ماهیچه شامل یکسری کارکترها مانند : خطوط، حلقه ها، حفره ها، شیارها، تارها، لکه ها و... است که قابل تفکیک می باشند. می توان گفت که عنبیه چشم همه افراد با یکدیگر متفاو ت است. تصویر عنبیه معمولاً توسط یک دوربین

www.prozhe.com

www.prozhe.com

تک رنگ مادون قرمز (۹۰۰-nm۷۰۰) که مجهز به سنسور CCD است گرفته می شود. معمولاً فاصله دوربین تا چشم باید چیزی در حدود ۱۸ اینچ باشد.(تابش نور به عنبیه سپس اندازه گیری بازگشت آن) فرایند پردازش بدین شکل است که ابتدا مکان و اندازه مردمک در تصویر مشخص شده و سپس با به دست آوردن مکان و اندازه عنبیه، کلیه تصویر عنبیه که در میان این دو دایره قرار دارد به شکل مستطیلی با ابعاد معین تبدیل میشود، این تکنیک باعث میشود تا با کوچک یا بزرگ شدن مردمک تصویر مستطیل شکل تقریبا ثابت بماند ت ا در انجام فرآیندهای بعدی مشکلی نباشد . تصویر موجود در مستطیلی با ابعاد معین دارای مشخصه های قابل تبدیل به کدهای باینری است، در این تبدیل ها روشهای مختلفی وجود دارد که هر یک مزایا و معایب خودرا دارند . پس از بدست آوردن الگوی باینری، با استفاده از بدست آوردن فاصله همینگ بین الگوی موجود با الگوی بدست آمده می توان نتیجه تطبیق را بدست آورد . در روشهای دیگری مانند نمونه یابی در مکانهای مشخص با برداشت چند نمونه از قسمتی از تصویر عنبیه که مشخصات قابل توجهی دارد، در زمان تشخیص با استفاده از نمونه های ذخیره شده و مکان یابی نمونه ها، عنبیه افراد قابل تشخیص است . این سیستم دارای قابلیت خوبی در تشخیص افراد است بدین دلیل که عنبیه هم منحصر بفرد است و هم در برابر گذشت زمان مقاوم، ولی متاسفانه حجم الگوها در این روش بسیار بالا است، این تکنولوژی بسیار گران است، کاربر پسند نیست و بدلیل اینکه در حین نمونه برداری لازم است که چشم کاملا بی حرکت باشد لذا الگو برداری ممکن است دقیق نباشد.

شناسایی از روی شبکیه چشم

شبکیه چشم در منتهی الیه کره چشم قرار دارد که شامل یکسری رگهای خونی است که این مویرگها داری اشکال مختلفی هستند، این خصیصه در افراد منحصر بفرد است . با قرارگیری چشم کاربر در یک مکان مشخص، یک دسته نور ماوراء قرمز یا نور سبز با طول موج کوتاه به شبکیه چشم تابیده می‌شود و بازتاب آن توسط یک دوربین CCD اندازه گیری میشود. این روش تقریبا مشابه شناسایی از طریق عنبیه می باشد.

شناسایی از روی نمودار حرارتی چهره

نمودار حرارتی چهره نیز یکی دیگر از پارامترهایی است که در تمامی افراد حتی دوقلوها نیز متفاوت است. نمودار ترموگرام در برابر گذشت زمان [تا مدت محدودی]، آرایش و اصلاح کردن مقاوم است، حتی جراحی پلاستیک نیز باعث بروز آسیب به نمودار ترموگرام نمی شود . جهت تصویر برداری از چهره از یک دوربین مادون قرمزبا

www.prozhe.com

www.prozhe.com

طول موج ۳ الی ۵ میکرون یا ۸ الی ۱۲ میکرون بدین صورت که تا عمق ۴ سانتی متر زیر پوست را حس کند استفاده می شود.

شناسایی از روی نحوه راه رفتن

معمولا این روش در جاهایی که ارتباط مستقیم با افراد میسر نیست کاربرد دارد خصوصا در فرودگاهها و معابر امنیتی. (این سیستم شناسایی تقریبا یک سیستم شناسایی مخفی است) در این روش یک تصویر از شخص در هنگام راه رفتن بدست می آید که معرف نمودار جابجایی و زمان برای وی است .در هنگام راه رفتن افراد حرکت پاها و سر افراد با یکدیگر متفاوت است (البته حرکت دستان نیز در برخی موارد کاربرد دارد) که الگوی بدست آمده از این قسمتها می باشد.

شناسایی از روی هندسه دست

دراین سیستم دست در یک مکان مشخص مطابق شکل قرار می گیرد . سپس با استفاده از یک دوربین دیجیتال CCD با کیفیت مطلوب ۳۲۰۰۰ پیکسل تصویر دست از دو نمای فوقانی و کناری گرفته می شود. که یک تصویر ۳بعدی از دست تولید می کند . از تصویر بدست آمده حدودا ۱۷ قسمت دست اندازه گیری می شود، منجمله: انگشتان(طول، پهنا، ضخامت، انحنا) و پارامترهای هندسی دیگر که در شکل آمده است . معمولا حجم داه بدست آمده ۹بایت است.

ترکیبات بیومتریک

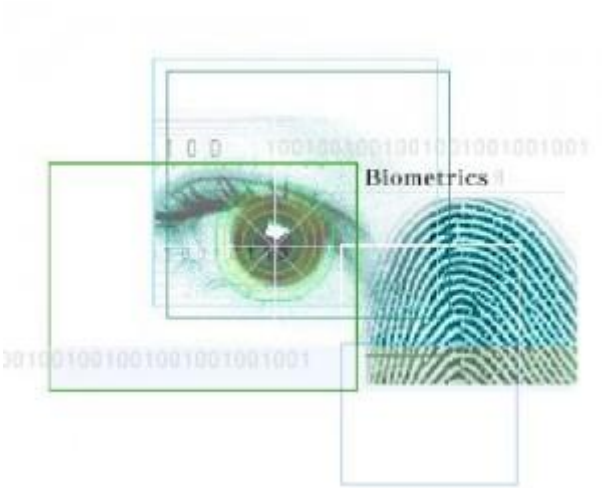
با ترکیبات بیومتریک می توان کارایی، امنیت و دقت سیستم را تا حد قابل ملاحظه ای افزایش داد، که در ذیل به تعدادی از روشهای ممکن اشاره خواهیم کرد : ترکیب سنسور در این مدل ما برای یک متد از بیومتریک، از چندین سنسور استفاده میکنیم. بعنوان مثال در اثر انگشت از سنسورهای نوری، خازنی، آلتراسوند و یا سنسورهای دیگر استفاده کنیم. این کار باعث افزایش دقت در امر نمونه برداری خواهد شد . ترکیب واحد نمونه برداری در این روش ما از چند واحد نمونه برداری میکنیم . بعنوان مثال در روش اثر انگشت از دو انگشت اشاره و انگشت وسط ویاانگشتان دیگر نیز عمل نمونه برداری را انجام میدهیم ویا از انگشت دست چپ و راست نمونه برداری میکنیم. ترکیب نمونه برداری در این روش چندین بار از مشخصه مورد نظر نمونه برداری میکنیم و ممکن است دو یا چند الگو از یک کاربر داشته باشیم. بعنوان مثال از انگشت کاربر دوبار نمونه برداری میکنیم و در حافظه ذخیره میکنیم. ترکیب روش‌های بیومتریک در این روش مااز ترکیب دو یا چند روش بیومتریک استفاده میکنیم . بعنوان

www.prozhe.com

www.prozhe.com

مثال : اثر انگشت + هندسه چهره + هندسه دست نتیجه گیری و جمع بندی علم بیومتریک اشاره دارد به تکنولوژیی برای اندازه گیری و آنالیز مشخصات بدن افراد جهت تشخیص هویت شخص . همه سیستم های بیومتریک دارای معماری ویژه ای برای پردازش نمونه مورد بررسی و احراز هویت می باشند. روش‌های مختلفی برای تشخیص هویت در بیومتریک وجود دارد که هر یک با توجه به دقت و کارایی مورد استفاده قرار می گیرند. اثر انگشت به دلیل اینکه برای هر فرد منحصر به فرد است و با گذشت زمان هیچ گونه تغییری نمی کند، در میان سیستم‌های بیومتریک بیشتر مورد استفاده قرار می گیرد. البته سیستم های دیگر مانند : عنبیه چشم، شبکیه چشم و نمودار حرارتی چهره هم از فردی به فرد دیگر متفاوت هستند. برای افزایش کارایی و امنیت و دقت سیستم می‌توانیم از ترکیبات بیومتریک استفاده کنیم.

سنسور های اثر انگشت



از نظر دریافت تصویر به دو نوع تقسیم میشوند:

سنسورهای خازنی

سنسورهای نوری

از نظر عملکرد داخلی به دو نوع تقسیم میشوند:

سنسورهای با قابلیت دریافت,ذخیره,مقایسه ,پردازش تصویر

www.prozhe.com

www.prozhe.com

سنسورهای با قابلیت فقط دریافت تصویر از اثر انگشت

مزایا و معایب سنسورهای خازنی:

سرعت بالا

قابلیت روشن بودن بدون ارسال هر بار Request

خش برداشتن در مدت زمان کوتاه

مزایا و معایب سنسورهای نوری:

سرعت متوسط

برای هر بار دریافت تصویر باید عمل Request انجام شود

مقاوم در برابر خش

مزایا و معایب سنسورها از نظر عملکرد داخلی (نوع اول)

دارای حافظه داخلی (مزیت)

نگهداری اطلاعات بصورت محلی (عیب)

سرعت بالا به دلیل پردازش تصویر بصورت داخلی(مزیت)

مزایا و معایب سنسورها از نظر عملکرد داخلی (نوع دوم)

گرفتن اطلاعات و ارسال آن به بیرون از سنسور(مهمترین مزیت)

حافظه داخلی ندارند(عیب)

سرعت به الگوریتم جستجوی نوشته شده توسط برنامه نویس بستگی دارد.(هم میتواند مزیت باشد هم از معایب)

www.prozhe.com

www.prozhe.com

حضور و غیاب

دستگاه کارت خوان

کارت خوان

ساعت حضور و غیاب

ساعت حضور و غیاب انگشتی

کارتخوان دوربین دار

سیستم حضور و غیاب

دستگاه حضور و غیاب

کارتخوان کارتی

دستگاه کنترل تردد کارمندان

اثرانگشت

کارتی

دوربین دار

رمزی

در بازکن

کنترل تردد

سیستم کنترل تردد

اثر انگشتی

www.prozhe.com

www.prozhe.com

کارتی

کدی | دوربین دار | سیستم کنترل تردد اثر انگشتی

زنده بودن اثر انگشت و تشخیص هویت

از سال‌ها پیش از اثر انگشت افراد در جرم شناسی استفاده می شد و امروزه در علم بیومتریک نیز از آن استفاده می شود. مانند تمام دیگر اعضای بدن DNA های هر شخصی الگوی ساخت این خطوط را دارا هستند و در واقعDNA های هر شخص نیز کاملا منحصر به فرد است و این موضوع تقریبا در مورد دیگر اعضای بدن صادق اند . اثر انگشت از قدیمی ترین روش های تشخیص هویت است که با پیشرفت تکنولوژی به تنوع آن افزوده شده است . اگر چه قبلا اثر انگشت تنها در زمینه جرم قابل بحث بوده، تحقیقات در بسیاری کشورها سطحی از پذیرش را نشان می دهد که به این روش اجازه استفاده در برنامه های عمومی را می دهد.خطوطی که بر روی سر انگشتان همه انسان ها نقش بسته از دیرباز مورد توجه همه بوده است، این خطوط نقش های مختلفی دارند، یکی از این وظایف ایجاد اصطکاک بین سر انگشتان و اشیاء متفاوت است مانند قلم که با استفاده از این اصطکاک می توانیم اشیا را برداریم ، بنویسیم یا لمس کنیم . از سوی دیگر این خطوط برای هر شخص منحصر به فرد است.

روش های تأیید هویت موجود با سه فاکتور تقسیم بندی می شوند:

۱ -چیزهایی که کاربران می دانند(برای مثال رمز عبور،PIN)

www.prozhe.com

www.prozhe.com

۲ -چیزهایی که کاربران به همراه دارند (کارت‌های خود پرداز، کارت های هوشمند)

۳ -چیزهایی که مربوط به خود کاربران است (بیومتریک ها شامل:اثر انگشت، الگوی شبکیه، عنبیه) و...

دسته سوم (بیومتریک ها) امن ترین و ساده ترین فاکتور تأیید هویت در دنیای اطلاعات و ارتباطات هستند. بیومتریک به روش های خودکار تشخیص یا تایید هویت یک شخص زنده از طریق اندازه گیری مشخصه های فیزیولوژیک یا رفتاری وی اطلاق می شود . بدین ترتیب بیومتریک یک مجموعه فناوری محسوب می شود .

تشخیص اثر انگشت تقلبی

در هر روش احراز هویت دیگر، تشخیص اثر انگشت کاملا ضد کلاه برداری . تهدیدات بالقوه برای سیستم های مبتنی بر اثر انگشت عبارتند از:

حمله به کانال های ارتباطی، از جمله حملات پخش در کانال بین سنسور و بقیه سیستم؛

حمله به ماژول های نرم افزار خاص (به عنوان مثال به جای استخراج ویژگی و یا تطبیق با یک اسب تروا)؛

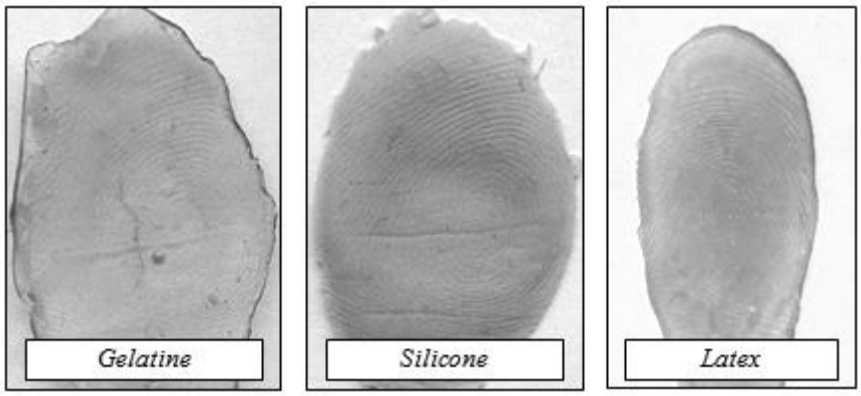
حمله به پایگاه داده از قالب ثبت نام؛

ارائه انگشتان جعلی به سنسور.

امکان سنجی از آخرین نوع از حمله از سوی برخی از محققان گزارش شده است : آنها نشان داد که آن را در واقع ممکن است به کلاه برداری برخی از اثر انگشت سیستم های تشخیص با نوک انگشتان به خوبی ساخته شده است جعلی، ایجاد شده با همکاری صاحب اثر انگشت و یا از اثر انگشت پنهان: در مورد دوم این روش سخت تر است اما هنوز هم ممکن است.

www.prozhe.com

www.prozhe.com



در سال ۲۰۰۵، BioLab دو روش جدید برای تشخیص انگشت جعلی:

تشخیص انگشت جعلی در تجزیه و تحلیل اعوجاج پوست است . کاربر مورد نیاز برای حرکت دادن انگشت خود را در حالی که آن را با فشار دادن در برابر سطح اسکنر، بنابراین عمدا اغراق اعوجاج پوست. هنگامی که یک حرکت انگشت واقعی بر روی سطح اسکنر، آن را به تولید مقدار قابل توجهی از اعوجاج، که مشاهده می شود کاملا متفاوت از آن تولید شده توسط انگشت جعلی است. معمولا انگشتان جعلی از پوست سفت و سخت تر هستند، و سپس اعوجاج است که قطعا پایین تر است، حتی اگر بسیار الاستیک مواد استفاده می شود، آن را بسیار دشوار به نظر می رسد به دقت شبیه سازی خاص انگشت واقعی تحریف شده است، به علت رفتار مربوط ب ه راه خارجی پوست به derma زمینه ای قلاب و متصل شده و تحت تاثیر موقعیت و شکل از استخوان انگشت.

تشخیص انگشت جعلی بر روی تجزیه و تحلیل بو است . بینی الکترونیکی با هدف تشخیص بوی آن دسته از مواد که معمولا مورد استفاده برای ایجاد انگشتان جعلی (مثلا سیلیکون یا ژلاتین) استفاده می شود.

لذا برای نمایش تشخیص اثر انگشت تق لبی دو فیلم از تست انگشت واقعی و انگشت تقلبی در پیوست این پروژه می باشد که به نام های ذیل می باشند.

نمایش دمو از پوست اعوجاج مبتنی بر روش تشخیص جعلی به نام DemoDistortion

نمایش دمو از بوی رویکرد مبتنی بر تشخیص جعلی به نام DemoOdour

www.prozhe.com

www.prozhe.com

اثر انگشت هم جایزالخطاست!

پرونده میفیلد اگر چه روزهای سختی را برای اف.بی.آی رقم زد، اما بدون‌شک نقطه عطفی برای تحقیق و بررسی علمی در زمینه اثرانگشت و میزان ارزش گذاری آن در اعلام حکم نهایی دادگاه های قضایی بود. بررسی‌هایی که نشان دادند از دیدگاه علمی این اثر همیشه قابل‌استناد نیست.

مارس ۲۰۰۴ (اسفندماه ۱۳۸۲): انفجار تروریستی در قطارهای شهری مادرید که بیش از ۱۹۱ کشته و ۲۰۰۰ زخمی برجای گذاشت، دنیا را به تعقیب بین‌المللی عاملان این جنایت واداشت. تنها چند روز بعد پلیس اسپانیا موفق‌شد از چندتایی چاشنی عمل نکرده که درون بسته‌ای در اطراف منطقه انفجار رها شده بودند، یک اثرانگشت ناقص را کشف کند. بلافاصله اثرانگشت مورد نظر در اختیار سایر کشورها نیز قرار گرفت و کمتر از دوماه بعد، اف.بی.آی (پلیس فدرال ایالات متحده)، براندون میفیلد، یکی از وکلای ایالت اورگان را بر پایه مطابقت ا ثرهای انگشت دستگیر کرد.

تنها ۲۰ روز بعد و با دستگیری یک تبعه الجزایر که پش از این هم توسط پلیس اسپانیا به دلیل حملات تروریستی دیگری تحت تعقیب بود، بی گناهی میفیلد اثبات شد . مقایسه اثرانگشت ها هم نشان داد که اثر دوم با نمونه کشف‌شده انطباق بیشتری دارد. در نهایت اف.بی.آی پذیرفت که در تحلیل اثر انگشت نمونه، چندین مورد اشتباه سهوی مرتکب شده است.

اما پرونده میفیلد به مرجعی برای تحلیل هایی از اثرانگشت تبدیل شد که می توانند افراد بی گناه را بی آنکه عمدی در کار باشد گناهکار جلوه دهند . البته این تنها نمونه نیست . ارین موریس، روانشناس و همکار دفتر وکلای تسخیری لوس آنجلس با بررسی پرونده های قضایی ایالات متحده در چندین دهه گذشته، موفق شده فهرستی ۲۵ تایی از تحلیل‌های نادرست را گردآوری کند.

مشاهدات او نشان می دهند تشخیص‌های قدیمی همگی بر پایه فرضیاتی بنا شده اند که هیچ پایه تجربی یی ندارند. آکادمی ملی علوم ایالات متحده (ان.ای.اس) نیز سال گذشته در گزارشی اعلام کرد، با اینکه انگشت نگاری حامل اطلاعات باارزشی است، اما از لحاظ علمی چندان قابل‌استناد نیست.

www.prozhe.com

www.prozhe.com

به گزارش نیچر، پرونده میفیلد، فهرست خطاها و این گزارش اخیر، باعث شد متخصصان انگشت‌نگاری و دولت آمریکا بخواهند حقیقت آشکار شود و به نظر می رسد تنها راه رسیدن به پاسخ نهایی جمع آوری وسیع اطلاعات و دسته‌بندی آنها باشد. به عنوان مثال در آغاز سال جاری میلادی، بخش تحقیقاتی وزارت دادگستری ایالات متحده و مؤسسه ملی دادگستری این کشور اولین برنامه جامع تحقیقاتی برای طبقه‌بندی انگشت‌نگاری‌ها–شامل نمونه‌های کامل، محو یا ناقص را – بر اساس پیچیدگی ظاهری آنها آغاز کرده اند تا میزان خطا در هر دسته ازریابی شود . آیتیل درور، روانشناس ادراکی دانشگاه کالج لندن که در این مطالعه شرکت داشته است، می گوید: «تعداد بسیارزیادی از این آثار مشکل ساز نبودند. اما اگر تنها ۱٪ آنها قابلیت تفکیک کافی نداشته باشند، سالانه امکان هزاران اشتباه بالقوه وجود خواهد داشت».

اثر انگشت

حتی سرسخت‌ترین مخالفان انگشت‌نگاری هم به اینکه این تکنیک از دیگر روش های شناسایی مبتنی بر آزمایش موها، تعیین گروه خون یا هر روش دیگری مگر تعیین دی .ان.ای فرد به مرتب دقیق تر است، اذعان دارند . برجستگی‌ها، فرو رفتگی ها و شکل نهایی خطوط سر انگشتان درون رحم شکل می گیرد و مجموعه ای بسیارپیچیده از وراثت و محیط را تشکیل می دهد، آنقدر که حتی دوقلوهای یک تخمکی هم اثرانگشت یکسانی از خود به جا نخواهند گذاشت . به علاوه این خطوط تا پایان عمر ثابت می مانند و به دلیل چربی طبیعی پوست، همیشه پس از لمس، اثری از خود به جا خواهند گذاشت.

به همین دلیل چیزی که می تواند گمراه‌کننده باشد، باید پس از باقی گذاشتن اثر رخ دهد و با توجه به اینکه اغلب متخصصان انگشت‌نگاری سال‌ها آموزش دیده‌اند، به نظر می رسد، بیش از خطای انسانی باید نگران دستورالعمل چهار مرحله ای شناسایی اثرانگشت که در بسیاری از کشورهای جهان رایج است، باشیم . این دستورالعمل که ACE-V نام دارد، سرنام چهار مرحله متوالی تحلیل، مقایسه، ارزیابی و تأیید نهایی است. خط فاصله نشان می‌دهد تأیید نهایی باید توسط شخص دیگری انجام بگیرد.

در مرحله اول تحلیل سه طرح اصلی که شامل حلقه ها، مارپیچ ها و منحنی ها می شوند، بررسی خواهند شد . با تشخیص طرح اولیه در مرحله دوم تمرکز رو ی نکات ظریف تری مانند انشعاب های گرفته‌شده از برآمدگی ها و

www.prozhe.com

www.prozhe.com

نقاط پایانی آنها خواهد بود. در بسیاری از موارد مرحله دوم تعیین‌کننده است. اگر احتمال خطا و جود داشته باشد، می‌شود در مرحله سوم شکل لبه برآمدگی‌ها یا طرح پرزها را نیز بررسی کرد.

پس از اتمام مرحله تحلیل، مقایسه نمونه با نمونه‌های پیشین آغاز می‌شود که شامل بازبینی برای تعیین شباهت‌ها یا تفاوت‌ها با نمونه هایی است که پیش از این وجود داشته، از بایگانی استخراج شده یا متعلق به مظنون هستند . این بخش از دهه ۱۹۸۰/۱۳۶۰ تاکنون به صورت خودکار انجام شده و در د هه ۱۳۷۰/۱۹۹۰ بهبود پیدا کرده است . البته در مرحله نهایی این متخصص است که به صورت چشمی نمونه ها را تفکیک خواهد کرد .

مطابق دستورالعمل ACE-V در گام سوم، یعنی ارزیابی، متخصص باید به یکی از این سه نتیجه برسد:

۱ –شناسایی که به معنی تشخیص اثرانگشت است

۲ –مردود شدن اثر که باید حداقل یک تفاوت آشکار با نمونه اولیه وجود داشته باشد

۳ –غیرقاطع که نشان می‌دهد اثر به اندازه کافی برای تشخیص و اعلام نظر واضح نبوده است.

www.prozhe.com

www.prozhe.com

در واقع سیستم به شکلی طراحی شده که خطاها بیشتر به سمت تشخیص منفی نادرست بروند تا اینکه بی‌گناهی گناهکار تشخیص داده شود.

با این وجود، پرونده‌های نادری مانند میفیلد نیز وجود دارند که بیشتر حاصل مجموعه ای از اشتباهات بوده‌اند. نمونه دیگری هم در اسکاتلند اتفاق افتاده است: بازرسان در یک صحنه قتل اثرانگشت یکی از مأموران پلیس را پیدا کردند که تنها پس از جلسات متعدد داخلی و بررسی مجدد انگشت‌نگاری‌ها بی‌گناهی او اثبات شد. پرسش اصلی اینست که چرا اصلا چنین اشتباهاتی رخ می‌دهند؟

در کتاب «چالش‌ها در انگشت نگاری» یکی از علل خطای انسانی، تخلف از دستورالعمل ذکر شده و انجام هم‌زمان مرحله تحلیل و مقایسه با یکدیگر به دلیل کاهش زمان این فرایند ذکر شده است . اف.بی.آی نیز این هم‌زمانی را به عنوان یکی از دلایل خطا در پرونده میفیلد پذیرفته است.

وسایل بیومتریک، با اسکن اثر انگشت، آن را به صورت داده های ریاضی ذخیره نموده، سپس با موارد موجود در پایگاه داده ای خود مقایسه می کنند.با کمک این فن آو ری، IBMعضو جدیدی از خانواده نوت بوک های Tink Padرا معرفی کرده است که از فن آوری بیومتریک، برای افزایش امنیت سیستم استفاده می کند. این مدل جدید که ۱۹ اکتبر ۲۰۰۴م. (۲۸ مهر ۱۳۸۳ش.) به بازار عرضه شده است مجهز به سنسور (حس‌گر) پیشرفته ای برای تشخیص اثر انگشت م ی‌باشد و کاربران برای دسترسی به کامپیوتر، بانک های اطلاعاتی، سایت ها و برنامه‌های نرم‌افزاری، باید انگشت خود را از روی این سنسور کوچک و افقی عبور دهند . از آن جا که این حس‌گر جدید، سطح بیشتری از انگشت را اسکن می کند، اطلاعات بیشتری جمع آوری کرده، فرآیند شنا سایی تنها چند ثانیه به طول می‌انجامد .

پس از حادثه ۱۱ سپتامبر، به کار گیری ابزارهای امنیتی بیومتریک - به خصوص در آمریکا - شکل دیگری به خود گرفت؛ به طوری که طبق مصوبات کنگره این کشور، بعد از تاریخ ۲۶ اکتبر ۲۰۰۴م. (۵ آبان ۱۳۸۳ش.) تمام مسافران خارجی به هنگام ورود به ایالات متحده، بایستی دارای شناسنامه بیومتریک در مدارک خود باشند و در غیر این صورت، از ورود آنها جلوگیری خواهد شد .

از این رو، سفارت خانه‌ها موظف شده اند تا تراشه یا نوارهای بیومتریک از مشخصات افراد متقاضی ویزا را به مدارک آنها ضمیمه کنند . بدین ترتیب، پاسپورت های بیومتریک، دگرگونی اساسی در نظام تهیه پاسپورت و کنترل ورود و خروج مسافران در سراسر دنیا ایجاد خواهند کرد .

www.prozhe.com

www.prozhe.com

جعل پاسپورت بیومتریک، بسیار دشوارتر از انواع کنونی آن خواهد بود . سیستم‌های بیومتریک، هویت هر فرد را در الگوهای ویژه ای خلاصه می کند و ا ثر انگشتان، ویژگی چشم، صورت، صدا و دیگر خصوصیات فیزیکی را در قالب الگوریتم های ریاضی بر روی یک‌تراشه و یا یک نوار ویژه ثبت و ضبط می کند. بدین‌ترتیب، هنگامی که مسافران به مراکز ورودی کشور می رسند، انگشتان خود را در مقابل یک اسکنر ویژه قرار داده، همزمان چهره آنان نیز توسط اسکنر بیومتریک دیگری مورد بررسی دقیق قرار می گیرد و مشخصات به دست آمده، با الگوها و ویژگی‌های ثبت شده در پاسپورت مقایسه می‌شود .

محصولات نرم افزاری و سخت افزاری تولید شده، با تکنولوژی بیومتریک، بازارهای جهانی را متحول ساخته اند.

تعدادی از این محصولات عبارتند از :

-کنترل و مراقبت‌های ویژه .

-کنترل‌های اکتیوکس برنامه‌ها .

BioMetric ActiveX Controls For :BioTools

-کنترل امنیت اینترنت و اینترانت .

BioMetric Internet :BioWeb

-کنترل

Attendance Control and Monitoring Your Program and Interanet Security
دسترسی انحصاری & BioMetric Time :BioTime .

-کنترل دسترسی و مدیریت ساختمان .

BioMetric Building Management and Access :BioAccess

-تصدیق دارنده کارت اعتباری .

BioMetric Smartcard Owner :BioSmatrCard

-شناسایی اعضای گروه به کمک

Stand-Alone BioMetric Access Controls Controls Authentication
بیومتریک :BioDoor .

-پست الکترونیکی مطمئن و امن .

BioMetric Secure Mail :BioMail

دو مورد از جالب‌ترین کاربردهای بیومتریک، به کمک اثر انگشت،

BioMail و BioMetric Group Member Tracking BioSmartcard :BioRegister

می‌باشند .

www.prozhe.com

www.prozhe.com

ترکیبی از اسکن اثر انگشت و پنهان سازی، آخرین ترفند موجود در ایجاد امنیت پست الکترونیکی و راهی برای خصوصی‌سازی ارتباطات است؛ به طوری که به کمک این روش، اسناد و نامه‌های محرمانه شما به هیچ عنوان، در دسترس دیگران قرار نخواهد گرفت .

BioMailیا ایمیل زیستی، به صورت متحد و کاملا نامحسوس، از درون outlook فعالیت می کند؛ به این‌ترتیب که الگوی اثر انگشت شما به صورت محرمانه و همانند یک فایل ضمیمه (Attachment) ، برای آدرس مورد نظر ارسال و به صورت مخفی درAddress Book او ذخیره می‌شود و هر زمانی که لازم باشد از آدرس مورد نظر، پیغام محرمانه ای برای شما ارسال می شود، با افزودن نام شما در قسمت " TO أأ. " و کلیک دکمه مخفی سازی، مندرجات ارسالی به صورت اتوماتیک مخفی شده، سپس ارسال می‌گردد .

در ارسال و دریافت، اسناد همواره مخفی مانده، تنها در صورت مطابقت اثر انگشت دریافت کننده اصلی با الگوی ذخیره شده، در دسترس قرار می‌گیرند .

فن‌آوری جدید، امکان هرگونه سرقت، کپی و یا هک شدن را غیر ممکن می سازد و از آن جایی که رمز عبور شما قسمتی از خود شما خواهد بود، موجب فراموشی نیز نخواهد شد .

در روشی مشابه، بیومتریک برای استفاده کنندگان از کارت‌های اعتباری، ایده جالب‌تری دارد .

کارت‌های اعتباری به دلایلی چون سرقت، تصادف و ... ممکن است مفقود شوند و یا رمز (PIN) آنها فراموش شود و در این صورت توسط هر کس دیگری می‌تواند مورد استفاده قرار گیرد .

BioSmartcardیا کارت‌های هوشمند زیستی ، با ابعاد و اندازه کارت های اعتباری متداول به همراه تراشه‌های پردازش‌گر تعبیه شده در درون آنها ، امکان استفاده از کارت را برای دیگران غیرممکن می‌سازد .

کارت‌های هوشمند زیستی، مشخصه های زیستی افراد را در یافت می کنند و اینها چیزهایی نیستند که فراموش، کپی برداری‌و یا مفقود شوند .

اثر انگشت صاحب اصلی کارت، به صورت دیجیتالی درون کارت قرار داده می‌شود .

هنگام استفاده از کارت، به جای وارد کردن رمز عبور، اثر انگشت شخص توسط یک اسکنر مخصوص، اسکن و در صورت تطابق، استفاده از کارت، مجاز شناخته می‌شود .

اشتباهات در انگشت‌نگاری

بخش دیگری از خطاها به این برمی گردند که دستورالعمل گاهی تصریح نشده است، به عنوان مثال مرحله تأیید نهایی باید توسط فرد دیگری صورت بگیرد ولی در اغلب موارد این فرد در همان بخشی کار می کند

www.prozhe.com

www.prozhe.com

که مراحل پیشین صورت گرفته اند و خواه ناخواه در جریان پرونده قرار دارد . علاوه بر این مطالعات نشان می‌دهند اطلاعات اولیه هر پرونده به طور متوسط می تواند ۱۷ درصد از متخصصان را تحت تأثیر قرار دهد و اطلاعات چیزی نیست که در دستورالعمل فعلی از ارسال آن جلوگیری شده باشد.

اما مهم‌ترین ایرادی که منتقدان این روش به آن وارد می کنند، اینست که تحلیل انگشت نگاری اساسا یک مسئله فردی و ذهنی است، چرا که اغلب اثرهای انگشت کشف‌شده ناقص یا محو هستند و تحلیل آنها پرونده به پرونده و فرد به فرد متفاوت خواهد بود.

عده دیگری از منتقدان بحث صلاحیت متخصصان انگشت‌نگاری را مطرح کرده‌اند. مسئله بسیارپیچیده است، چرا که اغلب این افراد تا سال‌ها بعد هم نمی‌دانند آیا درست تصمیم گرفته‌اند یا نه!

برای کاهش خطای انسانی پلیس منچستر تصمیم گرفته بخش انگشت‌نگاری را از سایر بخش های مرتبط جدا کند تا احتمال درز اطلاعات اولیه پرونده به این بخش به حداقل تقلیل پیدا کند. اما در ایالات متحده هنوز هم در اغلب ایالت ها بخش انگشت نگاری جزیی از اداره پلیس است . علاوه بر این در پلیس منچستر دیگر همکاران بخش انگشت نگاری در جریان نوع پرونده همکارانشان نخواهند بود و در صورت محو یا ناقص‌بودن اثرانگشت، نتیجه را غیرقابل استناد اعلام خواهند کرد.

موضوع دیگری هم وجود دارد که می تواند به خطای انسانی دامن بزند و آن کیفیت چاپ اثرانگشت کشف‌شده در صحنه است . متخصصان معتقدند، هیچ بازآفرینی یی بی‌نقص نیست و این هم می تواند احتمال تشخیص نادرست را افزایش دهد . از دیدگاه آنها اگر ابهامی در تشخیص وجود دارد یا اثرانگشت مشابه دیگری هم شناسایی‌شده، باید به دادگاه اعلام شود.

می‌شود با شناخت بهتری از گستردگی طرح های مورد استناد در مرحله دوم تحلیل اثرانگشت یا «مقایسه» در ملیت های گوناگون، کار را برای متخصصان انگشت نگاری ساده‌تر کرد، اما متأسفانه هنوز چنین تحقیقی در سطح گسترده انجام نشده است.

نکته دیگر ارزش‌گذاری اثر انگشت در تصمیم‌گیری‌های قضایی است. به نظر می‌رسد باید فرهنگ قضایی نیز

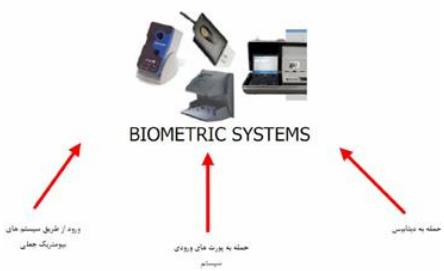
www.prozhe.com

www.prozhe.com

انتظار تغییراتی را داشته باشد. چرا که علم می آید تا به بخش مؤثری از تصمیم های نهایی پرونده‌های قضایی بدل شود.

انواع بیومتریک ها:

بیومتریک های فیزیولوژیک :عنبیه نگاری ، شبکیه نگاری، انگشت نگاری، چهره نگاری، دست نگاری، صوت نگاری



بیومتریک های رفتاری :امضا نگاری ، نحوه تایپ کردن

سایر بیومتریک ها :پارامترهای دیگری هم اخیرا مورد استفاده قرار گرفته است که به علل مختلف هنوز کاربرد وسیعی ندارند. از جمله می توان به بیومتریک های نظیر DNA ، نحوه راه رفتن، الگوی رگ های پشت دست، خطوط کف دست، شکل گوش، بوی بدن و الگوی بافت های زیر پوستی دست اشاره کرد .

راه حل نهایی جهت فایق آمدن بر مشکلاتی که بعضا هر فناوری بیومتریک به همراه دارد استفاده همزمان از چند بیومتریک مختلف در یک سیستم است. به این روش اصطلاحا سیستم چند لایه گفته می شود.

کاربردهای بیومتریک

- **شناسایی مجرمان**

www.prozhe.com

www.prozhe.com

شناسایی مجرمان با استفاده از بیومتریکهای مختلف جهت تعیین یا تأیید هویت افراد مظنون یا بازداشت شده می باشد. تعداد کمی از فناوریها می توانند در این عرصه مؤثر باشند . اثرانگشت و چهره نگاری از جمله این بیومتریکها هستند. درحال حاضر بانک اطلاعاتی AFIS جامع FBI که به IFIS مشهور است دارای ۴۰ میلیون ثبت ۱۰ انگشتی است. چهره نگاری دومین بیومتریک پرکاربرد در این زمینه می باشد. اولین کاربرد عمومی این سامانه‌ها در Newham انگلستان با استفاده از ۱۴۴ دوربین تلویزیونی مدار بسته بود که به منظور ثبت همه فعالیتها در خیابانهای ناامن ایجاد شد . فرودگاه پیرسون در Ontario کانادا هم دارای یک سامانه نظارتی مشابه است که به بانک اطلاعاتی پلیس متصل است. دفاتر پلیس کالیفرنیا و میشیگان هم به سامانه تشخیص چهره مجهز هستند. در زندانهای پنسیلوانیا، نیویورک و فلوریدا از عنبیه نگاری به منظور اطمینان از هویت افرادی که از زندان خارج می شوند استفاده می شود. انتظار می رود در آینده نزدیک DNA سهم عمده ای از این بازار را به خود اختصاص دهد.

- خرده فروشی/ خودپردازها/ پایانه های فروش

تعیین یا تأیید هویت افراد هنگام انجام تراکنشهای مالی، کاربرد بیومتریکها در این عرصه را رقم می زند . این کاربرد که در سالهای اخیر توسعه یافته است جهت تکمیل یا جایگزینی فرایند ورود به سامانه های مالی الکترونیکی به روشی آسانتر و البته مطمئن تر مورد ا ستفاده قرار می گیرد. بانکها و مؤسسات مالی بزرگی در سراسر جهان به استفاده از سامانه های بیومتریکی در این حوزه روی آورده اند. طیف وسیعی از بیومتریکها در این حوزه مورد استفاده قرار می گیرند. انگشت نگاری، عنبیه نگاری، چهره نگاری و اسکن الگوی رگهای دست[۱] از جمله این فناوریها می باشند. فناوری بیومتریکی دربخش بانکداری وخدمات مالی رشد چشمگیری داشته است. این فناوری نه تنها امنیت و ارائه خدمات را افزایش می دهد بلکه امکانات ارزشمند جدیدی از جمله خدمات از راه دور را به ارمغان آورده است . نهایی شدن استانداردهای فرمت داده های بیومتریکی و رمز گشایی آنها شامل BioAPI,BAPI,CBEFF و X9.84 باعث پذیرش بیشتر آن در صنعت شده است . البته هنوز بعلت محافظه کاری بسیاری از مؤسسات و ترس از رخنه افراد سودجو، امکانات بالقوه بسیاری برای توسعه وجود دارد که هنوز توسعه نیافته اند . از اوایل سال ۲۰۰۱ استفاده از فناوریهای مختلف بیومتریکی کاربردهای موفقیت آمیزی در این بخش داشته اند . از مهمترین کاربردها در این بخش می توان به موارد زیر اشاره کرد :

۱- دسترسی به حسابها

یک مثال خوب در این زمینه "وسترن بانک" پورتوریکو است که از اواسط سال ۲۰۰۰ تمامی۳۷ شعبه خود را به سامانه تشخیصی اثر انگشت و اسکن امضا مجهز کرد و مشتریان بانک می توانستند از روشهای قبلی و یا یکی از دو بیومتریک نامبرده استفاده کنند. آمارها نشان می دهد در همان ابتدا ۱۰ تا ۱۵ درصد از ۳۰۰ هزار مشتری بانک

www.prozhe.com

www.prozhe.com

از سامانه بیومتریکی استفاده کردند . هزینه تقریبی راه اندازی این سامانه ۳میلیون دلار برآورد شد . بزرگترین بانک بخش خصوصی برزیل [۲] هم از فناوری صوت نگاری برای اجازه دسترسی تلفنی مشتریان خود به حساب هایشان استفاده کرده است.

۲- خودپردازها

برای بعضی تراکنشها، بیومتریکها می توانند یک گزینه مناسب در خودپردازها باشند . درسال۱۹۹۷ یک موسسه مالی و اعتباری در سوئد و انگلیس طرح آزمایشی Cordless بر پایه سامانه عنبیه نگاری در خودپردازهایش را به اجرا گذاشت. نتیجه موفقیت آمیز این طرح استفاده بیش از ۹۴ درصد از مشتریان و ترجیح این فناوری نسبت به سامانه PIN بود. پروژه های مشابهی در امریکا، هند، آلمان و... اجرا شده که با استقبال فراوانی مواجه شده اند. بانکهای بزرگ جهان از جمله امپریال کانادا با استفاده از فناوری عنبیه نگاری و میتسوبیشی ژاپن با استفاده از فناوری رگ نگاری کف دست از پیشتازان استفاده از خودپردازهای بیومتریکی در دنیا می باشند. بانکداری الکترونیک وبلادرنگ، تراکنشهای تلفنی، دسترسی بهPC و شبکه های کامپیوتری و دسترسی فیزیکی به منابع از موارد دیگر در این زمینه هستند که در امریکا، آلمان، کانادا، مالزی و... بیشترین استفاده مشاهده شده است. با توجه به پروژه های بزرگی که هم اکنون در بخش بانکداری کشور در حال اجراست (از جمله پروژه شتاب) توجه ویژه به قابلیتهای بیومتریکی می تواند حایز اهمیت باشد.

- تجارت الکترونیک / تلفنی

کاربردهای این حوزه بیشتر مربوط به تراکنشهای از راه دور (خصوصاً تلفنی یا اینترنتی) می باشد. در اینجا هم بیومتریکها به منظور تکمیل یا جایگزینی فرایند ورود به سامانه مورد استفاده قرار می گیرند. یکی از مهمترین مزایای استفاده از سامانه بیومتریکی در این فرایندها عدم نیاز به سرپرست یا ناظر ورود و تصدیق هویت افراد می باشد. صوت نگاری از جمله بیومتریکها پرکاربرد در این حوزه می باشد.

- دسترسی به رایانه/ شبکه

تفاوت این کاربرد با کاربرد بیومتریکها در حوزه تجارت الکترونیکی و تلفنی این است که در اینجا تراکنشی انجام نمی گیرد و شناسایی افراد به منظور دسترسی به منابع اطلاعاتی صورت می گیرد. انگشت نگاری و تایپ نگاری از جمله بیومتریکهای پرکاربرد در این عرصه می باشند . در۱۹۹۹ در Oceanside کالیفرنیا پس از طرح آزمایشی که در ۵۰ ایستگاه کاری از ۱۷۰۰ شبکه دولتی انجام شد، ۱۵۰۰ ایستگاه کاری به سخت افزار و نرم افزار تشخیصی اثرانگشت جهت دسترسی به شبکه مجهزشدند. طرح مشابهی

www.prozhe.com

www.prozhe.com

در گلندیل کالیفرنیا برای ۲۱۰۰ کارمند شهر اجرا شد که پیامد آن صرفه جویی ۵۰ هزار دلاری سالانه در هزینه های مدیریتی- بعلت افزایش کارایی و راحتی دسترسی به شبکه بود. برنامه GSA امریکا هم از همین دست می باشد.

حفاظت از اطلاعات بیماران در شبکه های داخلی کلینیکها و مراکز درمانی و افزایش اهمیت این موضوع علت اصلی ورود بیومتریکها در این عرصه است. کاربردهای بیومتریک در این زمینه بیشتر از نوع کارمند محور است و انتظار می رود کاربردهای مشتری محور از قبیل دسترسی به اطلاعات شخصی و تأیید یا تعیین هویت افراد مرتبط با درمان هم جایگاه خود را پیدا کنند.

از سال ۱۹۹۸ دفتر سلامت روانی نیویورک به ۶۰۰۰ واحد انگشت نگاری جهت تأمین امنیت شبکه خود مجهز شده است. بیمارستان وینسنت و مراکز مراقبتهای بهداشتی در مارس ۲۰۰۱ اقدام به استفاده از فناوری بیومتریکی جهت افزایش امنیت شبکه ۵۰۰۰ کاربره خود نموده اند. اسپانیا و هند هم جزو کشورهای استفاده کننده از سامانه‌های بیومتریکی در بخش بهداشت خود می باشند.

- دسترسی فیزیکی/ زمانی و کنترل حضور و غیاب

دسترسی به اماکن حفاظت شده و کنترل تردد و ورود و خروج افراد، کاربرد دیگر بیومتریک ها می باشد. بسته به سطح امنیت مورد نیاز بیومتریکهای مختلفی به این منظور مورد استفاده قرار می گیرند. شبکیه نگاری، دست نگاری و انگشت نگاری از جمله این بیومتریکها می باشند.

موارد زیر از جمله کاربردهای بیومتریکها در این بخش می باشد:

- اطاق های ویژه
- اماکن و ساختمانهای حساس
- شبکه داخلی یا سازمانی
- گاوصندوق های امن
- صندوق امانات
- اتومبیل شخصی و وسایل نقلیه

www.prozhe.com

www.prozhe.com

- سلاح و کیف حمل اسلحه
- تلفن همراه
- دسترسی به اطلاعات طبقه بندی شده

- شناسایی شهروندان

شناسایی شهروندان در تعامل با نهادهای دولتی کاربرد دیگر بیومتریکها می باشد. این حوزه طیف وسیعی از کاربردها از کارتهای شناسایی بیومتریکی و دسترسی به خدمات و امکانات عمومی تا رأی گیری بیومتریکی را شامل می شود. انگشت نگاری و چهره نگاری از جمله بیومتریکهای پرکاربرد این حوزه می باشند.

۱- شناسایی ملی

تعامل با بدنه دولت جزء زندگی روزمره افراد است . استفاده از بیومتریکها در بخش دولتی امروزه شیوع بسیار زیادی داشته است. برنامه های شناسایی ملی و صدور کارتهای شناسایی با فناوریهای اثر انگشت، چهره نگاری و عنبیه نگاری همراه شده است که البته فعلاً مراحل ابتدایی خود را طی می کند.

ارائه خدماتی جزیی تر در قالب دولت الکترونیک هم بخشی از کاربردهای بیومتریک می باشد که موارد زیر مثالهایی از این دست می باشد:

- آموزش از راه دور در دانشگاههای مجازی
- کنترل و مدیریت حضور و غیاب کارمندان، دانشجویان و دانش آموزان
- خدمات هوشمند کتابخانه ای، آزمایشگاهی و سلف سرویس
- سامانه های خدماتی کارکنان
- کارتها و بلیط های اعتباری مصرفی

۲- مدیریت بحرانهای بزرگ شهری

موارد زیر گوشه ای از خدمات قابل دس‌تیابی به کمک فناوری بیومتریک هنگام بروز بحرانهای بزرگ و غیر مترقبه می باشد:

- تایید هویت بازماندگان و آمارگیری سریع و دقیق

www.prozhe.com

www.prozhe.com

- تعیین هویت مجروحان و آمارگیری سریع و دقیق
- تعیین هویت متوفیان و آمارگیری سریع و دقیق
- ارایه بهینه خدمات توزیع اقلام و کالاهای امدادی
- تایید هویت دقیق مسؤولان و پرسنل فاقد کارت شناسایی و فعال در حین بحران
- تعیین هویت دقیق افراد سابقه دار و مجرمان تحت پیگرد، حاضر در محل بحران
- تشکیل بانک اطلاعاتی اولیه جهت مظنونین افراد فاقد هویت ثبت شده

۳ -رأی گیری

در امر رای گیری تا بحال در چند کشور دنیا از جمله مکزیک (ژولای ۲۰۰۰ با استفاده از چهره نگاری) پرو (انتخابات سال۱۹۹۷ با استفاده از اثر انگشت) ایتالیا، برزیل، دومنیکن، کاستاریکا، پاناما (استفاده از اثر انگشت) انتخابات بیومتریکی داشته اند.

همچنین از ۱۹۹۹ کنگره مکزیک، ۱۹۹۷ مجلس ونزوئلا، و اخیراً مجلس ترکیه از فناوری اثر انگشت برای کنترل رأی گیری داخلی استفاده می کنند.

٤- گواهینامه رانندگی

هم چهره نگاری و هم انگشت نگاری کاربرد موفقیت آمیزی در برنامه های صدور گواهینامه رانندگی داشته است. که هم در زمینه ش ناسایی N:۱ و هم ۱:۱ استفاده می شود. ایلیون، ویرجینیای غربی، جورجیا، کلورادو و تگزاس جزو این دسته از ایالات آمریکا می باشند. در دهلی نو و گجرات هند هم گواهینامه ها مجهز به اثرانگشت در کارتهای هوشمند می باشند.

٥-توزیع امکانات عمومی

پروژه TASS اسپانیا که ازسال ۱۹۹۴ آغاز شده که هدف آن تهیه کارتهای هوشمند دریافت خدمات درمانی و مراقبتهای بهداشتی، تأمین اجتماعی و ... است. در این طرح کارتها به الگوی اثرانگشت افراد مجهزشده اند البته این سامانه فاقد بانک اطلاعاتی است و قادر به شناسایی N:۱ نیست. هدف پروژه، دستیابی شهروندان به خدمات

www.prozhe.com

www.prozhe.com

در کنار امنیت اطلاعات شخصی و جلوگیری از سوء استفاده از کارتهاست . در فیلیپین، افریقای جنوبی و ایالات متحده هم از سامانه‌های مشابه استفاده می شود.

- نظارت

نظارت بر حضور افراد در محیطهای ویژه از جمله قابلیتهای کاربری بیومتریکها می باشد. چهره نگاری مهمترین بیومتریک در سامانه‌های نظارتی می باشد.

ذکر این نکته ضروری است که از ۷ کاربرد ذکر شده، شناسایی مجرمان و شناسایی شهروندان جزء کاربردهای بالغ فناوریهای بیومتریک می باشد و دیگر کاربردها هنوز نوظهور به شمار می روند.

با توجه به زمینه کاربردی، مجموعه های فعال در زمینه های زیر مخاطبان فناوری بیومتریک را تشکیل می دهند:

- صدور کارت شناسایی ایمن (ملی، پرسنلی، بهداشتی، گواهینامه، خدمات شهروندی و...)
- بانکداری الکترونیک
- کنترل دسترسی فیزیکی و اطلاعاتی (منطقی)
- امنیت مرزی
- صدور مدارک مسافرتی و اقامتی
- امنیت ملی و شناسایی مجرمان
- بحران های ملی و حوادث غیرمترقبه
- امنیت شبکه های اطلاعاتی و رایانه ای

کارت هوشمند چیست و چگونه کار می‌کند؟

یک کارت هوشمند از نظر اندازه شبیه به کارت های اعتباری پلاستیکی که یک تراشه در آن کار گذاشته شده است می‌باشد. قرار دادن یک تراشه در کارت به جای نوار مغناطیسی، آن را تبدیل به یک کارت هوشمند با قدرت سرویس‌دهی در مصارف گوناگون می‌نماید...

. این کارت ها به دلیل دارا بودن تراشه، دارای قابلیت کنترل عملکرد بوده و فقط اطلاعات مربوط شخصی و تجاری کاربر واجد شرایط را پردازش می‌نماید.

www.prozhe.com

www.prozhe.com

کارت هوشمند قابلیت استفاده در انواع معاملات بانکی و پشتیبانی مالی را دارد و به دلیل راحتی حمل و نقل و امنیت موجب آسایش خیال کاربر وتامین اطلاعات گوناگون مورد نیاز وی می گردد. استفاده از امکانات متنوع کارت‌های هوشمند به تجار این امکان را می دهد که محصولات و کالاهای خود را در بازارهای جهانی ارائه وفعالیت‌های تجاری خود راگسترش دهند . بانک‌ها، شرکت‌های نرم‌افزاری وسخت افزاری، خطوط هوایی وهمه این شانس را خواهند داشت که به بهره مندی از خدمات نوین محصولات کارتی خود در جهت ارتقاء سطح فعالیت‌ها و ارائه محصولاتشان دست یابند.

ترکیب امکانات نهفته در کارت های هوشمند سبب ایجاد ارتباط نزدیک تر میان طرفین تجاری وآنهایی می گردد که در اقصی نقاط دنیا به نحوی با یکدیگر دارای روابط تجاری می‌باشند.

امروزه در دنیا بیش از ۴/۴ میلیارد کارت اعتباری استفاده می‌شود. فعالیت‌های اقتصادی – مالی مبتنی بر کارت‌های هوشمند به میزان ۳۰ درصد در سال رشد دارد. همچنین تحقیقات انجام شده حاکی از آن است که در سراسر دنیا طی ۵ سال آینده صنعت کارت های هوشمند و وسایل و تجهیزاتی که امکان استفاده از آن را میسر می سازند به طور قابل توجهی رشد خواهد داشت وهمچنین افزایش امکانات وقابلیت های دستیابی با امنیت کافی به شبکه های کامپیوتری وتوسعه رو به رشد استفاده از تجارت الکترونیکی سبب رایج تر شدن بکارگیری کارت های هوشمند می گردد.

با در نظر گرفتن همین میزان مصرف، انتظار می رود کارت های هوشمند برای ۹۵درصد خدمات تلفن بی سیم ودیجیتالی که در تمام دنیا ارائه می شود مورد بهره برداری قرار گیرند . آسیا، آمریکای لاتین وآمریکای شمالی

www.prozhe.com

www.prozhe.com

مناطقی هستند که بالاتر ین پتانسیل را در ۳ سال آینده برای گرایش به استفاده از کارت های هوشمند به خود اختصاص خواهند داد.

اکنون بیشترین زمینه های کاربری از کارت های هوشمند در سطح دنیا مربوط به تلفن های پولی وبی سیم، بانکداری، خدمات بهداشتی و پرداخت آبونمان و لوازم خانگی بوده است.

چرا کارت‌های هوشمند تا این اندازه متداول شده‌اند؟

با وجودی که در حال حاضر میلیاردها کارت هوشمند در دنیای فعلی در دست کاربران قرار دارد، اما ممکن است فردی کارت را از یک کشور خاص تهیه نماید و بخواهد از آن در سایر کشورها استفاده کند

تولیدکنندگان تجهیزات و ارائه‌دهندگان کارت‌های هوشمند برای تامین چنین کاربردهایی، تکنولوژی کارت‌های چند منظوره را ایجاد کرده ودر تلاش هستند تا نوعی سازگاری میان تجهیزات وکارت های توزیع شده در سراسر دنیا به وجود آورند .برای تحقق بخشیدن به این مساله باید اصول تجاری و فنی مورد نیاز واصول استاندارد و هماهنگ با هر کشور، میان کارت‌ها و پایانه‌ها و مشخصه‌های موجود در تجهیزات وسایل ایجاد و مورد آزمایش قرار گیرند. کلید اصلی در دستیابی به این امر جهانی در دست صنعت مربوطه قرار دارد.

استاندارد چه نقشی را در کارآیی کارت‌های هوشمند ایفا می‌کند؟

استانداردها در واقع عواملی هستند که، هماهنگی وتطابق میان کارت ها و وسایل کارت خوان یا پشتیبانی کننده را تضمین می‌نمایند. وجود استانداردهای جهانی و ثابت در این امر باعث می شود تا کارهای تولید و توزیع شده در یک قسمت از دنیا به وسیله دستگاهی در بخش دیگری از دنیا پذیرفته شده و مورد استفاده قرار گیرند.

صنایع، خدمات و فعالیت های بسیاری وجود دارد که از طریق اعمال استانداردها و ضوابط بین المللی می توان عملکرد آنها را تحت پوشش کارت‌های هوشمند قرار داد که دستگاه‌های پمپ بنزین، سیستم‌های پرداخت بانکی و بسیاری موارد دیگر از این قبیل هستند . به همین دلیل سازمان بین المللی استاندارد، اصولی را برای کارت های هوشمند ایجاد و تثبیت کرده است و این اصول همچنان در حال توسعه و همه‌گیر شدن هستند.

www.prozhe.com

www.prozhe.com

همچنین بخشی از صنایع انحصاری موفق شده اند اصول و استانداردهای مشخصی را برای استفاده از کارت های هوشمند به وجود آورده و هم اکنون در حال گسترش و تثبیت آنها در سراسر دنیا می باشند. لذا حضور وسیع حضور نمایی مزیت‌های فراوان موجود درکارت‌های هوشمند صنایع و خدمات مختلف جهانی را بر آن داشته تا با ارائه ضوابط و استانداردهای مدون و قانونی موفقیت آنها را تضمین نمایند.

* مزایای عمده‌ای که کارت‌های هوشمند به مصرف کننده ارائه می‌دهند چگونه ارزیابی می‌شود؟

البته مزایای کارت‌های هوشمند را باید با در نظر گرفتن کاربردها و نحوه مدیریت و ایجاد زیرساخت‌های فرهنگی و تخصصی در هر جامعه بررسی نمود . عموما دستورالعمل ها و استاندارد محلی وضع شده و نحوه برخورد و حمایت قانون از کاربردهای این کارت ها در ارتقاء مزایای آن مؤثر می باشد. شیوه زندگی و اهمیت دستیابی به اطلاعات و چگونگی پردازش آنها و قوانین موجود در تنظیم روابط مالی نیز در تعریف مزایای کارت های هوشمند برای هر منطقه از دنیا حائز اهمیت است که نمی توان آنها را نادیده گرفت . با این وجود مزایای عمده اهداف اصلی ایجاد سیستم‌های بکارگیری کارت‌های هوشمند می‌توان در توانایی اداره یا کنترل مؤثر فعالیت های تجاری کاهش چشمگیر کلاهبرداری، کاهش کاغذبازی وحذف فعالیت‌های زائد و وقت‌گیر خلاصه نمود.

کارت هوشمند چند منظوره چیست؟

کارت هوشمند، برای راحت‌تر شدن و کاهش فعالیت‌های زائد در امور تجاری و غیره تولید گردیده، فعالیت‌هایی از قبیل (خرید و فروش، برنامه های بهداشتی، خدمات بانکی، خدمات مسافرتی و...). اگر قرار باشد برای انجام هر یک از فعالیت های فوق یک کارت هوشمند اختصاص یابد، آنگاه تعداد کارت ها خود مشکل جدیدی می شود که بر تمایلات کاربران تأثیر منفی گذاشته و از کارآیی آن نیز می‌کاهد.

یک کارت چند منظوره پاسخ مناسبی برای این موضوع است زیرا کارت چند منظوره می تواند انواع مختلفی از کارت‌ها را پشتیبانی نماید.

به عنوان مثال کارت چند منظوره "ویزا" کارتی می‌باشد که ترکیبی از اعتبار توسعه یافته ویزا در برگیرنده ستون بدهی و توابع ذخیره مالی و ذخیره‌سازی میزان اعتبار مالی می‌تواند در مسافرت‌ها کارآیی فراوانی داشته باشد.

کارت‌های چند منظوره با تحت پوشش قرار دادن موضوعات متنوعی از عملیات خریدها وخدمات گوناگون مالی موجبات آسایش کاربران را فراهم ساخته است.

کارت اعتباری بدون تماس چیست؟

دو نوع کارت اعتباری بدون تماس وجود دارد . اولی یک کارت بدون تماس از راه نزدیک است که با وارد کردن آن در یک دستگاه جانبی مخصوص خوانده می شود. و دومین کارت بدون تماس از راه دور است که

www.prozhe.com

www.prozhe.com

بدون استفاده از دستگاه جانبی کارت‌خوان قادر است از یک مسافرت معین و به صورت کنترل از راه دور خوانده شود که در دکه‌های دریافت عوارض کاربرد زیادی دارد.

قیمت یک کارت تراشه دار چقدر است؟

در تلاش برای پاسخ دادن به این سئوال که بیشتر مانند پرسیدن قیمت ماشین، بدون در نظر گرفت ن اینکه یک فولکس واگن دسته دوم و قدیمی است و یا یک رولزرویس آخرین مدل، باید گفت بهای کارت های تراشه‌دار ۱۵ الی ۸۰ درصد بستگی به ظرفیت آنها و کمیت اعتباری داشته و در این محدوده متغیر است.

چرا بارگذاری (شارژ) مجدد یک کارت هوشمند اهمیت دارد؟

کارت‌های یکبار مصرف و قابل شارژ مجدد، هر دو از بازارهای مصرف و کاربری برخوردار هستند . کارت‌های یکبار مصرف در مواقعی که کاربر در مسافرت به سر می‌برد و یا به منظور پرداخت ورودیه‌ها و مصارفی شبیه اینها مورد استفاده قرار می گیرند و عمدتا استفاده از آن برای یک زمان مشخص می باشد که پس از اتمام ذخیره، فاقد ارزش و بهره‌برداری می‌باشد و دور انداخته می‌شود.

اگر کارت مورد بحث چند منظوره باشد و مثلا ارزش ها و اعتبارات را ذخیره کرده و حساب های بدهکار و بستانکار کاربر را ثبت نماید، کاربر آن را دور نخواهد انداخت . صحیح‌تر خواهد بود که انرژی (اعتبار) ذخیره شده، قابل شارژ یا بارگذاری مجدد بوده و کاربر مجبور به خرید مکرر کارت‌های یکبار مصرف نگردد.

کارت‌های اعتباری تا چه اندازه ایمن و مطمئن هستند؟

کارت‌های هوشمند عملا امنیت و اطمینان بیشتری نسبت به سایر وسایل ذخیره اطلاعات مالی ارائه می دهند. یک کارت هوشمند مکان امنی برای ذخیره اطلاعات گران بهایی مثل کلیدهای اختصاصی، شماره حساب ها، رمزها یا سایر اطلاعات خصوصی ارزشمند می باشد. کارت‌های هوشمند با قدرت انجام محاسبه‌های پیچیده قابلیت تأمین امنیت بالاتر را دارا هستند و سلامت کاری صاحب کارت را فراهم می‌سازند.

آیا رهنمودهایی برای مصرف‌کننده در استفاده از کارت‌های هوشمند وجود دارد؟

بله، برای اولین بار شرکت های تولیدی کارت هوشمند، اطلاعاتی را در رابطه با صنعت و توزیع کنندگان کارت هوشمند، روش هایی عمومی و قانونی ارائه کردند . درک و شناخت صحیح این رهنمودها بسیار مهم است، خصوصا اینکه برای اولین بار این اطلاعات توسعه صنایع چندگانه به طور داوطلبانه پذیرفته شده و در حال تکامل است.

* انتظارات شخصی مصرف کنندگان را شناسایی کرده و در نظر بگیرید و رهنمودهای شخصی ارائه شده را در مورد آنان اجرا نمایید.

www.prozhe.com

www.prozhe.com

* به منظور تأمین خدمات بهتر و ارائه فرصت های جدید به مصرف کننده، استفاده، جمع آوری و نگهداری اطلاعات مربوطه به آنها را (تا حدی که نیاز است)تهیه و باید کامل شود.

* وسیله‌ای را برای مصرف‌کنندگان تهیه و در محل‌های مختلف تعبیه کنید تا اسامی آنان را به بازار و با شرکت به طور مستقیم یا پست و یا موارد درخواستی دیگر ارسال نماید.

* روش‌های انجام شده و در دسترس، کارمند را از نظر شخصی محدود می‌سازد.

کارمندان را در مورد مسئولیت ها و استانداردهای شخصی جهت حفاظت از منافع مصرف کننده و پاسخ گویی به اعترافات آنان آموزش دهید. و انضباط صحیح و تنبیهات رفتاری را با کارکنانی که نسبت به چنین استانداردهایی بی‌توجه هستند، پیاده کنید

امنیت در سیستم های بیومتریک :

سیستم های بیومتریک همواره به روش های مختلف مورد هجوم قرار می گیرند. این نوع حملات شامل : حمله به دیتابیس ، حمله به پورت های ورودی سیستم و حمله به سیستم تشخیص هویت از طریق بیومتریک های جعلی است .

سارقان معمولا جهت فریب سیستم های تشخیص هویت از روش های مختلفی بهره می برند، از جمله استفاده از عکس چهره یا عنبیه فرد مقابل دوربین ، ضبط با کیفیت صدای شخص در سیستم های بیومتریک صوتی ، استفاده از اثر انگشت ژلاتینی و حتی استفاده از لاشه انگشت ! توسط سارقان جهت ورود به سیستم . فرایند تشخیص هویت می تواند هم از طریق نرم افزاری (خواندن و پردازش اطلاعات بیومتریک) باشد و هم از طریق سخت افزارهایی که در امر تشخیص به ما کمک می کنند .

در روش سخت افزاری از ابزار های مختلفی استفاده می شود : سنسور دما ، پالس اکسی متری انگشت ، هدایت الکتریکی بافت ، ECG ، Matchکردن صدای فرد و حرکت لب با تصویر برداری ، استفاده از اسکن سه بعدی التراسوند و...

www.prozhe.com

www.prozhe.com

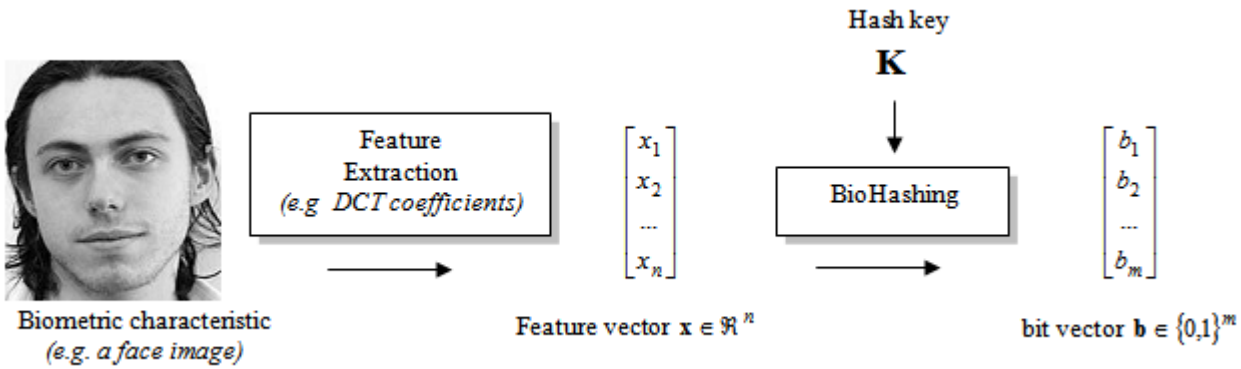
در روش نرم افزاری مولفه های مختلفی مورد بررسی قرار می گیرد. در صورت: جابجایی سر، در عنبیه: جابجایی مردمک

در روش تشخیص زنده بودن انگشت از روش های مختلفی استفاده می شود که در ادامه به بررسی آن ها خواهیم پرداخت.

رمزگذاری بیومتریک

با توجه به انفجار اخیر علاقه به احراز هویت انسان، تایید در tokenised اعداد تصادفی کاذب هستند و بر اساس کاربر خاص از ویژگی های بیومتریک (BioHashing)، توجه زیادی دریافت کرده است . BioHashing دستاوردهای بهبود عملکرد قابل توجه بی‌ش از صرفا بیومتریک (یعنی صفر نرخ خطای برابر)، اشکال اصلی رویکرد پایه BioHashing را متکی در برگزاری نمایشگاه عملکرد پایین "فریبکار" B دزد از کلید هش و او تلاش می کند به عنوان A تأیید هویت در سال ۲۰۰۵، BioLab معرفی برخی از ایده ها برای بهبود روش BioHashing پایه به منظور حفظ نرخ خطای برابر بسیار پایین که هیچکس دزد کلید هش و برای رسیدن به عملکرد خوب زمانی که "فریبکار" دزد کلید هش.

BioHashing تولید بردار بیت با شروع از مجموعه ای از ویژگی های بیومتریک و دانه ای است که نشان دهنده کلید "هش" است.



آزمایشگاه سیستم های بیومتریک – SfinGe

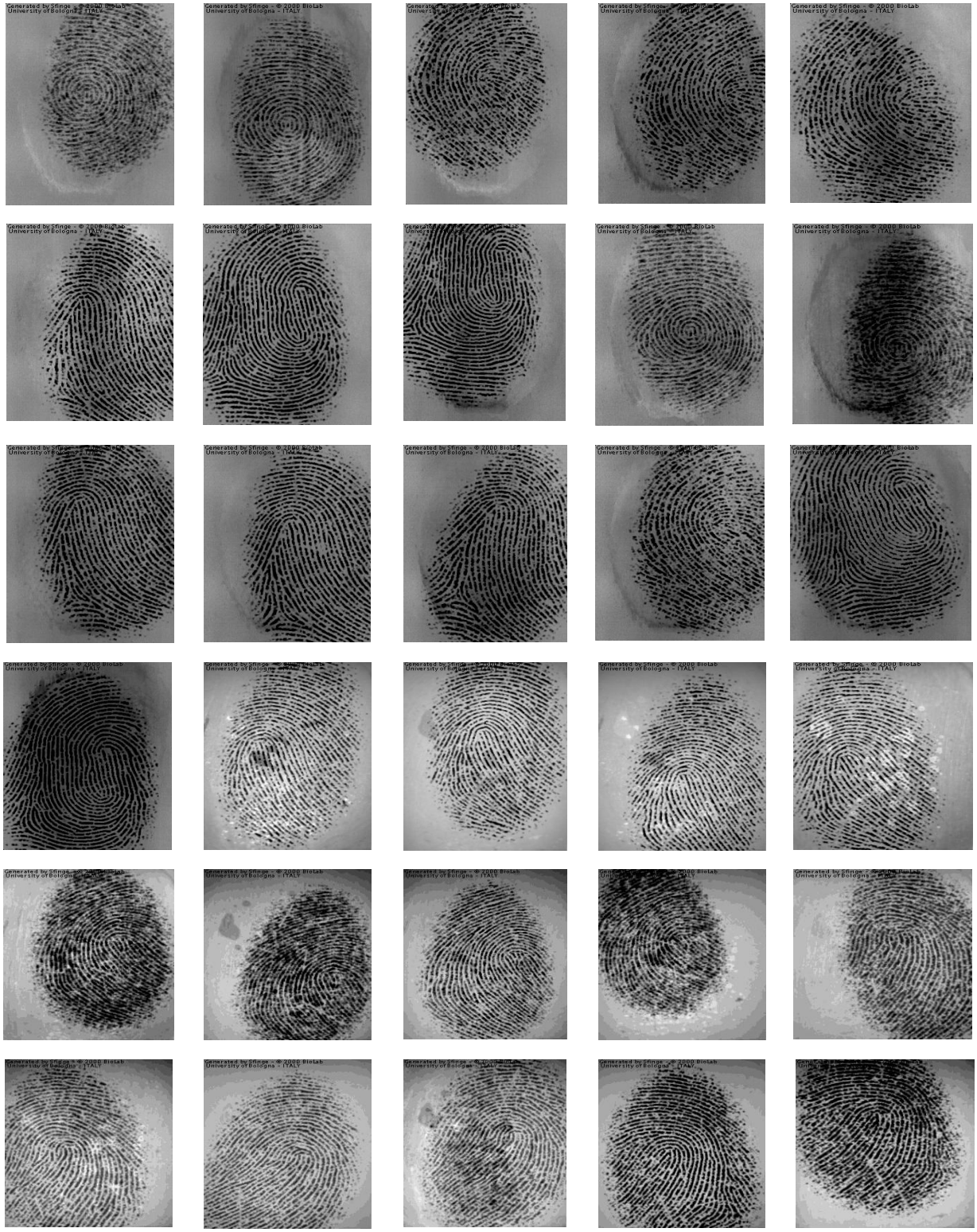
نمونه هایی از اثر انگشت های تولید شده توسط Sfinge v2.5

www.prozhe.com

www.prozhe.com

درضمن نرم افزار Sfinge در پیوست این پروژه می باشد و می توانید با نصب آن خود یک آزمایشگاه اثر انگشت را به صورت مجازی راه اندازی نمایید . که نمونه هایی از آثار انگشت تولید شده توسط این نرم افزار را بررسی نمایید.

توضیحات و ترجمه نحوه ، مدت زمان تولید اثر انگشت در فایل پیوستی پروژه موجود می باشد.



www.prozhe.com

www.prozhe.com

کارت شناسایی بیومتریک چیست؟

امروزه از کارت های شناسائی در ابعاد گسترده و به منظور اهداف مختلفی استفاده می گردد. تشخیص سن افراد ، شناسائی افراد برای اعطای مجوز دستیابی به مراکز داده و یا ارائه خدماتی خاص متناسب با سطح دستیابی تعریف شده به افراد ، نمونه هائی از کاربرد کارت های شناسائی است . هر سازمان و یا موسسه برای ارائه خدمات خاص خود تابع مجموعه سیاست هائی بوده که برای ارائه آنان نیازمند اطمینان از رعایت سیاست های اعلام شده توسط افراد متقاضی می باشد. با استفاده از کارت شناسائی ، هویت افراد بررسی و پس از تائید ، امکان ارائه خدمات به آنان فراهم می گردد . بدیهی است در صورت جع ل کارت های شناسائی ،زمینه استفاده از آنان به منظور انجام عملیات مخرب و خلاف قانون فراهم می گردد .در این راستا لازم است ، مراکز صادر کننده کارت شناسائی بر اساس یک فرآیند معتبر اقدام به صدور کارت شناسائی نموده و در ادامه از مکانیزم های ساده برای بررسی صحت اطلاعات موجود بر روی کارت استفاده نمایند.

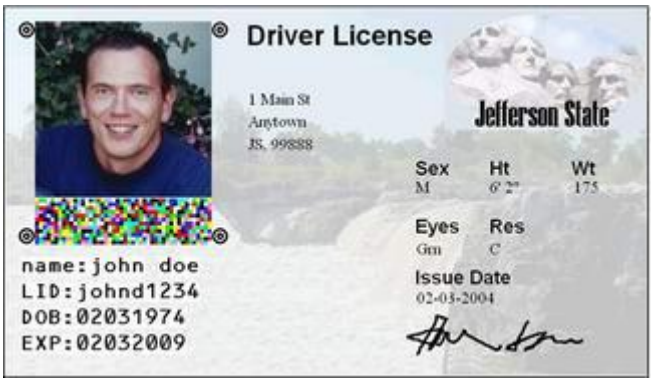
همزمان با تحولات جهانی در عرصه امنیت اطلاعات و فضای جدیدی که اینترنت فراروی مراکز ارائه دهنده خدمات گشوده است ، ضرورت استفاده از کارت های شناسائی هوشمند ، بیش از گذشته احساس می شود . در این نوع کارت ها ، اطلاعات مربوط به صاحب کارت بر اساس یک مدل رمزنگاری ، رمز شده و با استفاده از مکانیزم های خاصی بر روی کارت ذخیره می گردد . با توجه به تجارب موجود در زمینه شناسائی افراد بر اساس امضای دیجیتالی ، سعی شده است که در رویکرد فوق از تجارب فوق استفاده شده و با تلفیق آنان با پارامترهای بیومتریک ، کارت های شناسائی هوشمند ایجاد گردد .

در سیزدهمین کنفرانس RSA که اخیرا" با حضور شرکت های فعال در زمینه امنیت اطلاعات برگزار شده است ، مایکروسافت سیستم کارت شناسائی بیومتریک را که ماحصل تلاش محققین مرکز تحقیقات این شرکت می باشد را معرفی نموده است .کارت های شناسائی بیومتریک بر اساس یک فرآیند خاص ایجاد و بر روی آنان اطلاعات دارنده کارت به صورت رمز شده (استفاده از مدل رمزنگاری کلید عمومی که از آن به منظور ایجاد امضای

www.prozhe.com

www.prozhe.com

دیجیتالی استفاده می گردد) ، ذخیره می گردد . این نوع کارت ها با استفاده از سخت افزارهای ارزان قیمت و کاغذ معمولی تهیه و بکارگیری آنان نیز ساده می باشد .



مزایای کارت های شناسائی بیومتریک

- اطلاعات بر روی کارت های شناسائی بصورت دیجیتال و با استفاده از مدل رمزنگاری کلید عمومی RSA ، رمز و در یک کد میله ای (Bar code) ، ذخیره می گردد. در زمان بررسی کارت شناسائی ، پیوستگی و صحت اطلاعات موجود بر روی کارت بر اساس محتوی کدمیله ای بررسی خواهد شد.
- کارت های شناسائی بیومتریک می توانند بر روی رسانه های فیزیکی نظیر کاغذ معمولی و یا پلاستیک ، چاپ گردند. در این راستا به ویژگی و یا پتناسیل های اضافه ای نیاز نبوده و قیمت آنان مقرون به صرفه خواهد بود.
- بررسی پیوستگی و صحت اطلاعات موجود بر روی کارت شناسائی با استفاده از یک نرم افزار خاص و یک دستگاه اسکنر انجام خواهد شد. برای تطبیق تصویر موجود بر روی کارت با شخص ارائه دهنده کارت ، تمهیدات خاصی پیش بینی شده است.
- در سیستم ارائه شده توسط مایکروسافت برای تشخیص هویت افراد و دارندگان کارت های شناسائی نیازمند استفاده از سایر منابع اطلاعاتی نظیر بانک ها ی اطلاعاتی نخواهد بود .تمامی اطلاعات مورد نیاز به منظور بررسی هویت و شناسائی کارت بر روی خود کارت موجود می باشد . خوشبختانه ، اطلاعات موجود بر روی کارت نمی تواند توسط مرکز صادرکننده تغییر داده شود ، مگر اینکه مجددا" یک کارت شناسائی جدید صادر گردد .
- از کارت های شناسائی بیومتریک می توان به عنوا ن مکمل در کنار سایر سیستم های موجود نیز استفاده نمود (در مواردی که یک سازمان به سطح بالاتری از حفاظت نیاز داشته باشد) . کارت های فوق ، قادر به حمایت و ارتباط با سایر داده های بیومتریک نظیر " اثرانگشت " و یا " پویش چشم "،بوده و می توان از آنان به منظور درج سایر اطلاعات بیومتریک نیز استفاده نمود .

www.prozhe.com

www.prozhe.com

کارت های شناسائی بیومتریک چگونه کار می کنند ؟

سیستم کارت شناسائی بیومتریک ارائه شده توسط مایکروسافت دارای دو فرآیند مختلف برای ایجاد و بررسی ، می باشد. در ادامه به بررسی هر یک از فرآیندهای فوق ، خواهیم پرداخت .

فرآیند ایجاد کارت شناسائی بیومتریک

برای ایجاد یک کارت شناسائی ، نرم افزار مربوطه نیازمند یک عکس و برخی اطلاعات پایه در رابطه با فرد نظیر نام و تاریخ تولد، است. اطلاعات فوق ، توسط نرم افزار و به منظور ایجاد یک امضای دیجیتالی به شکل یک کد میله ای ، پردا زش و در نهایت کد میله ای بر روی کارت شناسائی ، چاپ می گردد . در صورتی که هر یک از اطلاعات موجود بر روی کارت تغییر یابند ، اطلاعات تغییر یافته با امضای دیجیتالی مطابقت پیدا نکرده و اعتبار کارت شناسائی تائید نخواهد گردید.

یک کارت شناسائی بیومتریک دارای اطلاعات زیر است :

- عکس صاحب کارت شناسائی
- اطلاعات متنی (Texttual) در رابطه با دارنده کارت که نوع آنان بستگی به نوع کارت شناسائی دارد . مثلا" در یک گواهینامه رانندگی ، اطلاعاتی نظیر نام ، نام خانوادگی ، تاریخ تولد ، ویژگی های فیزیکی دارنده کارت نظیر قد ، رنگ مو و چشم ، ذخیره می گردد .
- برخی اطلاعات متنی در رابطه با مرکز صادر کننده کارت شناسائی که دارای مجوز انجام این کار می باشد .

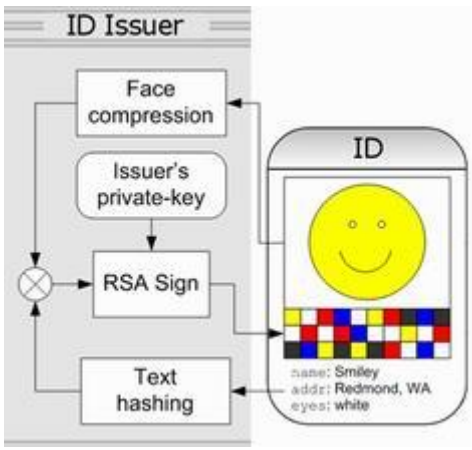
پس از تغذیه اطلاعات فوق به سیستم ، نرم افزار ا یجاد کارت شناسائی بیومتریک عملیات زیر را انجام خواهد داد :

- ایجاد یک مقدار Hash رمزنگاری شده از اطلاعات متنی با استفاده از الگوریتم های استانداردی نظیر SHA1
- فشرده سازی ویژگی های تصویر با توجه به عکس موجود بر روی کارت (پارامترهائی که بر اساس آن منحصربفرد بودن عکس تضمین گردد)
- تائید دیجیتالی Hash و ویژگی های فشرده شده مربوط به تصویر با استفاده از کلید خصوصی مرکز صادرکننده کارت شناسائی
- ایجاد یک کد میله ای که شامل اطلاعات مرحله قبل است .
- چاپ تصویر ، اطلاعات متنی و کد میله ای بر روی کارت شناسائی

شکل زیر مراحل ایجاد یک کارت شناسائی بیومتریک را نشان می دهد :

www.prozhe.com

www.prozhe.com

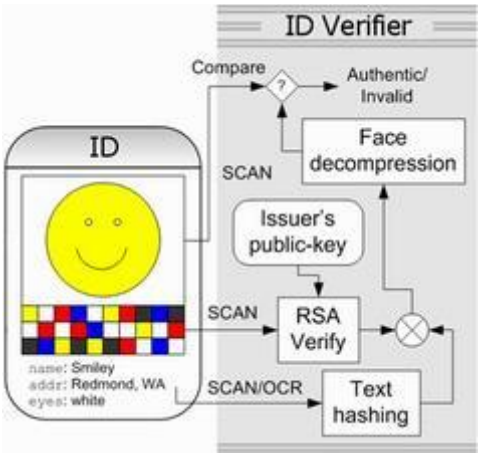


بررسی صحت کارت شناسائی بیومتریک

برای بررسی کارت شناسائی بیومتریک ، کارت از طریق اسکنر متصل شده به کامپیوتر که بر روی آن نرم افزار کارت شناسائی بیومتریک مایکروسافت نصب شده است ، اسکن ودر ادامه نرم افزار مربوطه مراحل زیر را به منظور تائید کارت شناسائی انجام خواهد داد :

- پویش (اسکن) ، سه عنصر تصویر ، متن و کد میله ای موجود بر روی کارت شناسائی
- ایجاد مقدار Hash بر اساس اطلاعات متنی موجود بر روی کارت
- بررسی امضای دیجیتال در کد میله ای با استفاده از کلید عمومی صادر کننده کارت شناسائی

شکل زیر مراحل بررسی یک کارت شناسائی بیومتریک را نشان می دهد :



بیومتریک ؛ عبور بدون رمز

اگر برای کامپیوتر خود رمز عبور تعریف کرده اید، اگر از پست الکترونیکی استفاده می کنید و یا یک بلاگر (وبلاگ نویس) هستید، اگر کارت اعتباری دارید، اگر ... و در هر حال، اگر شهروند دنیای مجازی، آن هم با انبوهی از نام‌های کاربری و رمزهای عبور هستید، به راستی چقدر به رمزهای عبور (password) خود اطمینان دارید و چقدر به حافظه خود برای به خاطر سپردن آنها؟

www.prozhe.com

www.prozhe.com

از آن جا که محیطهای پیچیده، ناامنی های پیچیده تری را به همراه خواهند داشت، محدود شدن به رمزهای عبور، به منظور ایجاد امنیت در چنین فضای متغییر و گسترده ای به لحاظ کیفی و کمی، چندان منطقی و عاقلانه نخواهد بود .

ظهور فن آوری های جدید، گام را از حروف و ارقام فراتر نهاده، جای گزینی مطمئن تر برای آنها یافته اند . موج بعدی در فن آوری امنیت اطلاعات، دانش و فن آوری بیومتریک یا سنجش زیستی می باشد. بیومتریک، در اصل به فراهم سازی ا منیت با استفاده از جنبه های فیزیکی (مانند اثر انگشت) و یا خصوصیات رفتاری مانند (امضای شما) اشاره دارد .

برای وسایل بیومتریک دو نوع کاربرد امنیتی تعریف می‌شود :

1.شناسایی

2.تصدیق هویت

در هنگام شناسایی، وسیله بیومتریک، هویت شما را با کمک داده های بیومتری تشخ یص می دهد؛ اما در مورد تصدیق، شما هویت خود را ارائه می‌دهید و سپس وسیله بیومتری، آن را بررسی می کند .

امضا، اثر انگشت، صدا، چشم و ویژگی های منحصر به فرد چهره افراد، از خصوصیاتی هستند که دستگاه ها و وسایل متداول بیومتریک، برای ایجاد امنیت از آنها استفاده می کنند .

امضا

در این روش، یک اسکنر صفحه ای کوچک، نمونه امضای گرفته شده را با امضاهای موجود در پایگاه داده ای خود مقایسه می کند و در برخی موارد، ممکن است نمونه امضا از نظر شکل، اندازه و خصوصیاتی چون سرعت و زاویه قلم نیز بررسی‌شود .

عنبیه چشم

عنبیه، حاوی اطلاعات بیشتری نسبت به اثر انگشت است و در نتیجه، امنیت بیشتری را تامین می کند. وسایل بررسی عنبیه چشم بدون تماس با چشم می توانند در کمتر از چند ثانیه، پایگاه داده ای بزرگ خود را جست وجو نمایند .

www.prozhe.com

www.prozhe.com

اسکن چهره

در این روش، تشخیص هویت به کمک اسکن چهره انجام می گیرد و جالب این که سیستم‌های بیومتریک در این روش، با وجود عینک و رشد موهای صورت، دچار خطای تشخیص نمی شوند. جالب است بدانیم که در این زمینه، ایران نیز گام‌های نخست خود را برداشته است .

بیستم فروردین امسال، روزنامه شرق به نقل از ایسنا، خبر از ساخت ر ایانه شناسایی چهره، در دانشکده مهندسی برق دانشگاه صنعتی امیرکبیر داد . به گفته دکتر کریم فائز، عضو هیئت علمی دانشکده مهندسی برق دانشگاه صنعتی امیرکبیر، سیستم رایانه رای شناسایی چهره که در قالب یک رساله دکتری طراحی شده، از جمله سیستم‌های شناسایی بیومتریک است که در جرم شناسی، تشخیص هویت و تجهیزات امنیتی کنترل تردد، کاربرد دارد. با استفاده از این سیستم، امکان تشخیص چهره افراد با دقت بیش از ۹۰ درصد فراهم می‌رشود .

صدا

خصوصیات آوایی و صوتی، از دیگر مشخصه های منحصر به فرد، به کار رفته در سیستم های بیومتریک است . برای ورود به یک ساختمان که به ابزارهای بیومتریک مجهز است، کافی است گوشی مخصوص را بردارید و خود را معرفی کنید .

اگر اطلاعات صوتی شما به عنوان فرد، واجد صلاحیت ورود به ساختمان در بانک اطلاعاتی موجود باشد، در آن صورت اجازه ورود به ساختمان را خواهید یافت . نکته مهم در امنیت این روش، آن است که سیستم موجود را نمی‌توان با صداهای‌ضبط شده و یا تقلید صدا فریب داد .

مشکل عمده این سیستم ها، عدم تشخیص در شرایطی چون سرماخوردگی، گرفتگی صدا، آمیختگی با صداهای محیطی و طریقه بیان کلمات همراه با مکث، خنده و سرفه است .

از آن جا که تارهای صوتی انسان، خصوصیاتی غیر خطی دارند و تحت تاثیر عواملی چون جنسیت و حالات عاطفی فرد قرار دارند، سیستم‌های بیومتریک صوتی، نیازمند طراحی دقیق‌تری می‌باشند و مسائلی چون طرز بیان و تلفظ، میزان بلندی لهجه، زیر و بم بودن صدا و سرعت ادای کلمات، بایستی در طراحی آنها مد نظر قرار گیرد .

در هر صورت، ابزارهای بیومتریک، جای‌گزین روش‌های معمول امنیتی خواهند شد و هم اکنون نیز بسیاری از کشورها از فن آوری بیومتریک به صورت‌ترکیبی و همراه با رمزهای عبور استفاده می‌کنند .

افسانه بودن قفل ها و کلیدها و دور ریختن همه کارتهای دست و پا گیر - بی‌هیچ دغدغه ای از ناامنی - هر چند رؤیایی شیرین خواهد بود، اما بدون شک آن زمان، ناامنی تعابیری دیگر و مفهومی گسترده‌تر خواهد یافت .

www.prozhe.com

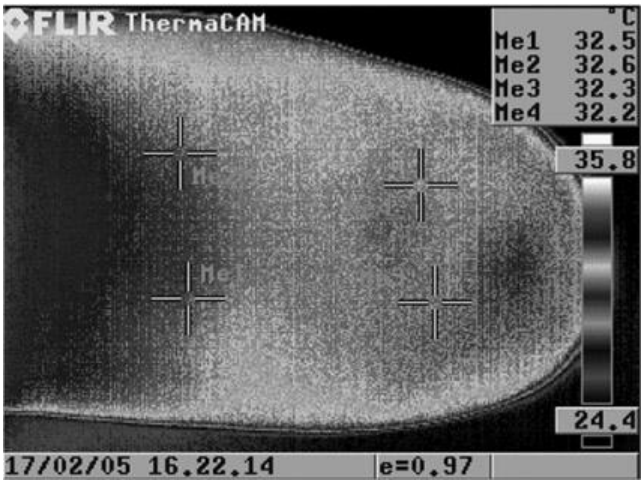
www.prozhe.com

الگوی دمایی نوک انگشت:

یکی از الگوهای متفاوت در تشخیص زنده بودن اثر انگشت بررسی نقاط مختلف گرم شدن آن است ، در شکل ۲ قادر به مشاهده این موضوع خواهید بود:

سارقان به روش های مختلفی اقدام به جعل اثر انگشت می کنند : از جمله استفاده از مواد ژلاتینی که کپی برداری از اثر انگشت فرد است ، استفاده از قالب اثر انگشت که به صورت مواد سفالی و گلی در آمده اند و همچنین استفاده از لاشه انگشت که اثر انگشت فرد دیگری است.

لذا باید روشی به کار گرفته شود تا از میان این حالات ، اثر انگشت زنده و واقعی را تشخیص دهد. در شکل زیر اثر انگشت یک فرد در حالات مختلف ذکر شده نشان داده شده است:



تشخیص از طریق تعرق بافت انگشت :

در تکنیک تشخیص هویت توسط تعرق بافت ، فرد انگشت خود را روی حسگر قرار می دهد بعد از مدتی انگشت عرق کرده و این تعرق در میان لبه های انگشت پخش می‌شود که تصویر متفاوتی از اثر انگشت ثبت خواهد شد. این روش تکنیکی است جهت تشخیص زنده بودن انگشت و جلوگیری از تقلب.

روش های اندازه گیری دمای بافت:

روش های دیگری نیز وجود دارد و آن اندازه گیری دمای بافت است . این دما به راحتی و بدون صرف هزینه زیادی قابل اندازه گیری است. دمای بافت انگشت بین 26تا ۳۰ درجه سانتیگراد قرار دارد. این محدوده دمایی

www.prozhe.com

www.prozhe.com

برای یک انسان سالم است و چنانچه فرد بیمار باشد موجب بالا رفتن دمای بدن و دمای انگشت شده و نمی تواند ارزیابی خوبی برای این تشخیص باشد. در روش فوق کاربر امکان فریب سیستم را نیز خواهد داشت و می شود با سرد یا گرم کردن بافت و نگه داشتن دما در حالت نرمال سیستم را فریب دهد.

ویژگی	اثر انگشت	هندسه دست	عنبیه	چهره	شبکیه	صدا	امضا
سهولت کاربری	بالا	بالا	متوسط	متوسط	پایین	بالا	بالا
عوامل خطا ساز	سن،خشکی، چرک	جراحت، سن	نور کم	نور، سن، عینک، مو	عینک	نویز، بیماری، آب دهان	تغییر امضا
صحت عملکرد	بالا	بالا	بسیاربالا	بالا	بسیار بالا	بالا	بالا
هزینه	بالا	بالا	بسیاربالا	بالا	بسیار بالا	بالا	بالا
میزان پذیرش کاربر	متوسط	متوسط	متوسط	متوسط	متوسط	بالا	متوسط
سطح امنیتی	بالا	متوسط	بسیار بالا	متوسط	بالا	متوسط	متوسط
پایداری	بالا	متوسط	بالا	متوسط	بالا	متوسط	متوسط

ایجاد گرما در محل قرار گیری انگشت:

در این روش فرد انگشت خود را روی سنسور قرار می دهد و دو دکمه نیز در مقابل قرار دارد چنانچه گرما در محل اثر انگشت زیاد شود فرد دکمه قرمز را فشار داده و زمانی که دما کاهش می یابد دکمه آبی را فشار می دهد. پوست انسان نسبت به تغییرات کوچک دما نیز حساس است و برای بدن قابل شناسایی است لذا زمانی که از انگشت های جعلی جهت فریب سیستم استفاده می شود، قابلیت تشخیص کم یا زیاد شدن دما را نداشته و مجوز ورود به سیستم داده نخواهد شد.

www.prozhe.com

www.prozhe.com

تشخیص زنده بودن اثر انگشت بر پایه آنالیز ویولت:

یکی از روش های Liveness Detection استفاده از آنالیز ویولت است. بر پایه این روش می توان اثر انگشت واقعی را از جعلی تشخیص داد.

مواد استفاده شده در انگشت های جعلی معمولا سفالی یا ژلاتینی هستند، این مواد ساختمان متراکمی دارند که سطح نامطلوبی از اثر انگشت را ایجاد می کنند و معمولا سطح چنین مواد سفت تر و زبر تر از بافت واقعی اثر انگشت است. این تفاوت زبری به عنوان یک روش در تشخیص و تفکیک بافت از نوع غیر بافت و جعلی است .

Liveness Detectionتوسط روش Fine Movement در سطح انگشت:

این روش بر پایه آنالیز جابجایی کوچک اثر انگشت و بررسی تغییرات حجمی خون است .در این روش لازم است تا از یک اسکنر نوری اثر انگشت جهت آنالیز تغییرات سیستول و دیاستولی قلب نیز استفاده شود.

آنالیز Curvelet و Curvelet Co-occurrence جهت تشخیص حمله های اثر انگشت جعلی به سیستم بیومتریک

در این روش بر پایه یک تبدیل کرولت جدید قادر خواهیم بود تا اثر انگشت های جعلی را تشخیص دهیم . اندازه گیری های بافت بر پایه مشخصه های انرژی Curvelet و Curvelet Co-occurrence جهت تشخیص اشکال مختلف اثر انگشت است . ابعاد Feature ها توسط الگوریتم Sequential Forward(SFFS Floating Selection)کاهش داده می شود، سپس دو دسته ویژگی مستقل روی طبقه بندی مختلف تست می‌شود نظیر K-nearest Neighbor , SVM , AddBoost.ML : ، ...سپس همه طبقه بند های ذکر شده توسط الگوریتم Majority Voting Rule به فرم یک طبقه‌بندی کننده ترکیبی در می آیند . استفاده از این روش ساده و بدون نیاز به هیچ گونه سخت افزار اضافی است.

www.prozhe.com

www.prozhe.com

استفاده از آنالیز خطوط برآمدگی انگشت توسط نورهای تابیده شده

این روش بر پایه تشخیص مشخصه های نوری از سطح اثر انگشت (پوست) است، ایده اصلی روش فوق بر اساس جابجا شدن خطوط Papillary Line است.

استفاده از آنالیزTime-Series

در این روش از تکنیکی جدید جهت تشخیص زنده بودن اثر انگشت استفاده شده است به این صورت که کاربر انگشت خود را روی سطح اسکنر فشار داده و سپس در یک سری زمانی مشخص تصاویری از وی ثبت می‌شود. ۵ ویژگی از تصاویر استخراج می شود که دو ویژگی آن نشان دهنده الاستیسیته پوست است . در نهایت توسط روش SVM() انگشت سالم از سایر مواد ژلاتینی تفکیک داده می شود.

استفاده از آنالیز های فرکانسی

یکی دیگر از روش های Liveness Detection استفاده از آنالیز های فرکانسی است . طیف فرکانسی در لبه ها وشیار های اثر انگشت واقعی و غیر واقعی متفاوت است . اثر انگشت زنده و جعلی هر دو طیف هایی را

www.prozhe.com

www.prozhe.com

تولید می کنند اما این طیف های فرکانسی در دامنه و باند های فرکانسی مختلف متفاوتند، در حالت عادی انگشت زنده طیف فوریه قوی تری نسبت به انگشت جعلی دارد . استفاده از این روش نتایج امیدوارکننده ای را در تشخیص حالات زنده و جعلی اثر انگشت داشته است.

تشخیص بر پایه مدل فیلتر گبور

یکی دیگر از روش های تشخیص اثر انگشت واقعی از جعلی است . این روش بر این تکنیک تکیه دارد که اثر انگشت های واقعی و جعلی دارای Texture های متفاوتی هستند. اندازه‌گیری این Textureبر پایه انرژی گبور و مشخصه های co-occurrence texture هستند، فیلتر های استفاده شده بانک گبور چهارتایی هستند.توسط روش gray level co-occurrence matrix) GLCM)جزئیات minute استخراج می شوند. ابعاد این مشخصه ها نیز توسط آنالیز PCAکاهش داده هستند. در این روش از سه تکنیک : neural network, support vector machine and OneRو ترکیب آن ها توسط Max Rule جهت طبقه‌بندی کردن داده ها استفاده شده و به فرم طبقه‌بندی کننده هیبرید درآمده اند.

تشخیص توسط آنالیز بویایی

در این روش تشخیص بر مبنای آنالیز بوی انگشت است ، به این صورت که ضمن ثبت اثر انگشت بو ی آن نیز توسط سنسور های بویایی (electronic nose) ثبت می شود. در این روش به راحتی می توان بین اثر انگشت های جعلی شامل ژلاتینی ، سیلیکنی ، لاستیکی و ... و اثر انگشت واقعی تفکیک داد.

تشخیص بر پایه آنالیز اعوجاج سطح پوست

این روش بر اساس آنالیز الاستیسیته سطح پوست است، کاربر انگشت خود را روی سطح سنسور حرکت داده و اطلاعات از سنسورها ثبت شده و توسط آنالیز های مختلفی اعوجاج سطح پوست سنجیده می شود . در طول جابجایی انگشت روی سطح سنسور عملیات ثبت و پردازش نیز انجام می شوند . این اطلاعات انکد شده و پس از آنالیز مجدد اثر انگشت طبیعی تعیین می شود.

این روش ها همچنان در حال پیشرفت و توسعه هستند و تمام تلاش ها برای افزایش امنیت سیستم های بیومتریک است.

www.prozhe.com

www.prozhe.com

ویژگی های استاتیک چند گانه

در این روش از ویژگی های جدیدی در تصاویر اثر انگشت استفاده شده است ، این ویژگی تحت عنوان ر وزنه های منحصر به فرد بوده و برای هر فرد متفاوت هستند .با بررسی فیزیولوژیک و مشخصه های آماری این روزنه ها می توان تفاوت بین اثر انگشت های جعلی و واقعی را تشخیص داد . تصاویر ثبت شده در این روش باید دارای کیفیت بالایی باشند.

لازم به ذکر است که این پروژه در دانشکده مهندسی پزشکی واحد علوم و تحقیقات تهران و در مقطع کارشناسی ارشد در حال بهینه سازی و بهبود روش های تشخیص جعلی بودن اثر انگشت است.

با تشکر از جناب دکتر معقولی که در تکمیل ایده این پروژه راهنمایی و همکاری داشته اند.

دستگاه اسکنر اثر انگشت همستر با سنسور ضد خش و ضد خرابکاری و جعل با بهترین طراحی و با بهره گیری از جدیدترین تکنولوژی سیستم های Biometric ساخت شرکت NITGEN کره جنوبی است. این دستگاه دارای استحکام فوق العاده در برابر ضربه های فیزیکی و شوک الکتریکی است .

قابلیتهای سیستم تشخیص اثر انگشت (Hamster) :

تغییر ناپذیری : روشن کردن کامپیوتر از طریق شناسایی اثر انگشت کاربر .

ایمن کردن فایلها : ایمن کردن فایلهای محرمانه و ارتقا امنیت برنامه ها

کنترل کردن : گزارشگیری از عملکرد کاربران سیستم

www.prozhe.com

www.prozhe.com

غیر قابل نفوذ : غیر قابل رمزگشایی ، فقط با اثر انگشت کاربر اصلی .

ارتقا عملکرد سیستم : تبدیل رمز Screen saver به سیستم شناسایی اثر انگشت

موارد اضطراری : قابلیت تعریف کردن رمز برای استفاده در موارد ضروری

از این سیستم میتوان برای شناسایی افراد از طریق شبکه و از راه دور در برنامه های مورد نظر استفاده کرد .

رابط نرم افزاری رایگان

قابلیت اتصال به تمامی سنسورهای موجود

پشتیبانی از تمامی زبانهای برنامه نویسی

پشتیبانی از تمامی سیستم های عامل

دارنده تمامی استانداردهای جهانی مرتبط

موارد کاربرد :

امنیت برای کامپیوتر و شبکه

تجارت الکترونیک

ایجاد امنیت برای بانکها و موسسه های مالی برای شناسایی کاربر

سیستم اطلاعات پزشکی

کارهایی که در آن نیاز به شناسایی کاربر است

قابلیت برنامه نویسی جهت استفاده از این دستگاه با سیستم های سخت افزاری و نر م افزاری مختلف

www.prozhe.com

www.prozhe.com

مزایای سیستم تشخیص اثر انگشت : (Hamster)

تغییر ناپذیری : نقشهای اثر انگشت تغییر ناپذیر است .

منحصر به فردی: نقش اثر انگشت هر شخص منحصر به فرد است .

راحت بودن : نیازی به داشتن آگاهی خاص برای استفاده کردن ندارد .

قابل اعتماد :اعتبار امنیت سیستم را ارتقا میدهد .

عمومیت : عمومیترین تکنولوژی بیومتریک است که پذیرفته شده است .

قابل دسترس : در دسترس ترین سیستم بیومتریک .

سیستم همستر از تکنولوژی اسکن نوری و سه بعدی بهره میگیرد ، این نوع اسکن بهترین شیوه تشخیص اثر انگشت میباشد و میزان دقت آن بسیار بیشتر از سیستم خازنی شناسایی اثر انگشت است.

www.prozhe.com

منابع

فهرست کتب

- L. Nanni و A. Lumini ، **"Cancellable بیومتریک: مشکلات و راه حل هایی برای بهبود دقت"**، در هاروی شوستر و ویلفرد Metzger، **بیومتریک: مواد و روش ها، برنامه ها و تجزیه و تحلیل**، نوا انتشارات، ۲۰۱۰. انتزاعی
- L Nanni ، S. Brahnam و A. Lumini ، **"برای یک سیستم احراز هویت اثر انگشت امن به توصیف مبتنی بر جهت گیری minutia Biohashing به کار برده، IET نامه های الکترونیک**، vol.47، no.15، pp.851-853، ژوئیه ۲۰۱۱. انتزاعی
- L. Nanni و A. Lumini ، **"الگوی دودویی محلی برای هیبرید تطبیق اثر انگشت، تشخیص الگو**، vol.41، no.11، pp.3461-3466، نوامبر ۲۰۰۸. انتزاعی
- L. Nanni و A. Lumini ، **"روش چند مودال بر اساس رقبای FVC2004 و بر روی داده های پالم همراه با اعداد تصادفی tokenised"، نامه های تشخیص الگو**، vol.29، no.9، pp.1344-1350، ژوئیه ۲۰۰۸. انتزاعی
- L. Nanni و A. Lumini ، **"شبه تصادفی برای یک BioHashing بهبود یافته برای احراز هویت چهره"، نامه های تشخیص الگو**، vol.29، no.3، pp.295-300، فوریه ۲۰۰۸. انتزاعی
- A. Lumini و L Nanni ، **"بهبود BioHashing برای احراز هویت انسانی"، تشخیص الگو**، vol.40، no.3، pp.1057-1065، مارس ۲۰۰۷. انتزاعی
- L. Nanni ، **"پیشرفته تطبیق چند روش برای تأیید امضای خود را روی خط های ویژگی های جهانی و tokenised اعداد تصادفی"، NeuroComputing**، vol.69، no.16، pp.2402-2406، اکتبر ۲۰۰۶. انتزاعی
- A. Lumini و L Nanni ، **"آزمون تجربی در BioHashing"، NeuroComputing**، vol.69، no.16، pp.2390-2395، اکتبر ۲۰۰۶. انتزاعی

A. Lumini و L. Nanni ، **"پیشرفته چند روش معین برای احراز هویت انسان در داده های بیومتریک ها و tokenised اعداد تصادفی "، NeuroComputing**، vol.69، no.13، pp.1706-1710، آگوست ۲۰۰۶. انتزاعی

L. Nanni و A. Lumini ، **"احراز هویت بشر که امضا و شماره تصادفی tokenised"، NeuroComputing**، vol.69، no.7-9، pp.858-861، مارس ۲۰۰۶. انتزاعی

D. Maio و L. Nanni ، **"MultiHashing، احراز هویت انسان های داده های بیومتریک و tokenised عدد تصادفی : یک مطالعه موردی FVC2004"، NeuroComputing**، vol.69، pp.242-249، دسامبر ۲۰۰۵. انتزاعی

A. فرانکو و D. Maltoni ، **"سنتز و تشخیص اثر انگشت حقه بازی "**، در Ratha NK، V. Govindaraju، **پیشرفت در علم زیست سنجی : سنسور، الگوریتم ها و سیستم ها**، اسپرینگر، ۲۰۰۸. انتزاعی

J. Galbally، R. Cappelli، A. Lumini، گونزالس G. د ریورا، D. Maltoni، J. Fierrez، J. Aguilar اورتگا و گارسیا و د Maio ، **"بررسی حملات مستقیم با استفاده از انگشتان تقلبی تولید شده از قالب ISO"، نامه های تشخیص الگو**، vol.31، no.8، pp.725-732، ژوئن ۲۰۱۰. برنده جایزه مقاله از ۱۹ کنفرانس بین المللی در تشخیص الگوی (ICPR)، کنفرانس ۱۹ بین المللی در تشخیص الگو (ICPR). انتزاعی

D. Maltoni و R. Cappelli ، **"پیشرفت در مدل سازی اثر انگشت "، تصویر و محاسبات چشم انداز**، vol.27، no.3، pp.258-268، فوریه ۲۰۰۹. انتزاعی

A. Antonelli، R. Cappelli ، D. Maio و د Maltoni ، **"تشخیص اثر انگشت جعلی توسط تجزیه و تحلیل پوست تحریف "، معاملات IEEE در پزشکی قانونی اطلاعات و امنیت**، vol.1، no.3، pp.360-373، سپتامبر ۲۰۰۶. انتزاعی

R. Cappelli ، A. فرانکو ، D. Maio و د Maltoni ، **"ladri الکترونیکی Guardie biometrica nell'era"، داروین**، no.13، pp.48-53، مه ۲۰۰۶.

A. Antonelli، R. Cappelli، D. Maio و د Maltoni، " **Apparecchio E metodo در UNA impronta digitale discriminare UNA ورا دا UNA impronta digitale artificiale falsa، L'analisi attraverso دلا distorsione elastica دلا pelle**"، ثبت اختراع N. BO2005A000399، ۲۰۰۵. انتزاعی

D. Baldisserra، A. فرانکو، D. Maio و د Maltoni "**Apparecchio E metodo در UNA impronta digitale discriminare UNA impronta ورا دا dell'odore digitale artificiale attraverso L'analisi دل داغ associato all'impronta digitale discriminare دا**"، ثبت اختراع N. BO2005A000398، 2005. انتزاعی

D. Baldisserra، A. فرانکو، D. Maio و د Maltoni، "**تشخیص اثر انگشت جعلی توسط تجزیه و تحلیل بو**"، در مجموعه مقالات **کنفرانس بین المللی تأیید هویت بیومتریک (ICBA06)**، هنگ کنگ، ژانویه ۲۰۰۶. انتزاعی

A. Antonelli، R. Cappelli، D. Maio و د Maltoni، **رویکرد جدید به تشخیص انگشت جعلی بر اساس اعوجاج پوست**"، در مذاکرات **کنفرانس بین المللی تأیید هویت بیومتریک (ICBA06)**، هنگ کنگ، ژانویه ۲۰۰۶. انتزاعی

[1] A. Maltoni, D. Maio, A.K. Jain, S. Prabhakar, Handbook of Fingerprint Recognition, Springer, New York, 2003, ISBN 0-387-95431-7.

[2] T. Putte, J. Keuning, "Biometrical Fingerprint Recognition: Don't Get Your Finger Burned", Proceedings of 4th Working Conference on Smart Card Research and Advanced Applications, ACM, Bristol, UK, 2002, pp. 289-303, ISBN 0-7923-7953-5.

[3] S. Shuckers, L. Hornak, T. Norman, R. Derakhshani, S. Parthnasardi, "Issues for Liveness Detection in Biometrics", CEMR LDCSEE, West Virginia University, USA, 2006, p. 25.

[4] M. Kluz, "Liveness Testing in Biometric Systems", Master thesis, Brno, Masaryk University, Faculty of Informatics, Brno, CZ, 2005, p. 57.

[5] A. Franco and D. Maltoni, "Fingerprint Synthesis and Spoof Detection", in N.K. Ratha, V. Govindaraju, Advances in Biometrics: Sensors, Algorithms and

Systems, Springer, 2008
[6] A. Antonelli, R. Cappelli, D. Maio and D. Maltoni, "Fake Finger Detection by Skin Distortion Analysis", IEEE Transactions on Information Forensics and Security, vol.1, no.3, pp.360-373, September 2006
[7] J. Galbally, R. Cappelli, A. Lumini, G Gonzalez-de-Rivera, D. Maltoni, J. Fierrez-Aguilar, J. Ortega-Garcia and D. Maio, "An Evaluation of Direct Attacks Using Fake Fingers Generated from ISO Templates", to appear on Pattern Recognition Letters Special issue on ICPR08
[8] Shankar Bhausaheb Nikam and Suneeta Agarwal , " Gabor Filter-Based Fingerprint Anti-spoofing " , J. Blanc-Talon et al. (Eds.): ACIVS 2008, LNCS 5259, pp. 1103-1114, 2008. © Springer-Verlag Berlin Heidelberg 2008
[9] K.-H. Nam and G. Rhee ," A Novel Region Based Liveness Detection Approach for Fingerprint Scanners "(Eds.): ICISC 2007, LNCS 4817, pp. 168-179, 2007. © Springer-Verlag Berlin Heidelberg 2007
[10] Brian DeCann, Bozhao Tan, and Stephanie Schuckers , " A Novel Region Based Liveness Detection Approach for Fingerprint Scanners ", M. Tistarelli and M.S. Nixon (Eds.): ICB 2009, LNCS 5558, pp. 627-636, 2009.c Springer-Verlag Berlin Heidelberg 2009
[11] Y.S. Moon, J.S. Chen, K.C. Chan, K. So and K.C. Woo , "Wavelet based ?ngerprint liveness detection" ELECTRONICS LETTERS 29th September 2005 Vol. 41 No. 20
[12] Denis Baldisserra, Annalisa Franco, Dario Maio, and Davide Maltoni و Fake Fingerprint Detection by Odor Analysis , D. Zhang and A.K. Jain (Eds.): ICB 2006, LNCS 3832, pp. 265 - 272, 2005. © Springer-Verlag Berlin Heidelberg 2005
[13] Heeseung Choi, Raechoong Kang, Kyungtaek Choi, and Jaihie Kim , " Aliveness Detection of Fingerprints using

Smart Card Security and Applications", Mike Hendry , " ۲nd Edition, ©ARTECH House INC.

www.biometrics.co.za/sol_TimeAtten.htm
www.biometrics.co.za/sol_SmartCard.htm
www.sharghnewspaper.com/830120/index.htm
www.ccwmagazine.com/default.asp
www.biometrics.co.za/PDF/biomail.PDF

www.prozhe.com

سایت مایکروسافت www.microsoft.com

www.prozhe.com