وزارت علوم، تحقیقات و فناوری

موسسه آموزش عالی پارسا

عنوان پروژه

پردازش تصویر اثرانگشت در فناوری بیومتریک

پروژه برای دریافت درجه کارشناسی

در رشته کامپیوتر گرایش نرم افزار

استاد راهنما:

سرکار خانم الهام حسن زاده

دانشجو:

زهرا عبداله پور

بهار 1392

1392

تقدیم به

کسانی که حقیقت بر

دل و جانشان تجلی کرده است

اگر چه از این

اوراق بی بها هستند

Dalan_z32@yahoo.com

فهرست مطالب

عنوان **صفحه**

فهرست شکلها

عنوان

اقرا باسم ربک الذی خلق

خلق الانسان من علق

اقرا و ربک الاکرم

الذی علم بالقلم

قرآن کریم

چکیده

سیستم بیومتریک یکی از فناوریهای برترجهان است و پردازش تصویر در اثرانگشت هم یکی از مشخصه های فیزیکی از این تکنولوژی می باشد. در این پروژه ابتدا در مورد سیستم بیومتریک و متدها و بخش های آن بیان شده است. در میان سیستم های تعیین هویت، سیستم هایی که از ویژگی های فیزیولوژی یا رفتاری افراد استفاده می کنند، از قابلیت اعتماد و سطح امنیت بیشتری برخودارند که نمونه ای از آن تشخیص هویت از طریق اثرانگشت می باشد که به دلیل دقت بالا و سادگی، متداو ل ترین و پرکاربردترین روش شناسایی افراد براساس تکنولوژی بیومتریک است. در ادامه به روش تحلیل اثرانگشت و نحوه ی بدست آوردن اثرانگشت ارائه گردیده است. در نتیجه به شناسایی از طریق اثرانگشت و کلاس بندی های آن را پرداخته و مورد بررسی قرار داده شده است. به دنبال آن، مزایای سیستم انگشت نگاری و خطاهای سیستم خودکار اثرانگشت نگاری و همچنین اشتباهات در سیستم انگشت نگاری را ارائه داده و کاربردهای آن در صنایع مختلف و زمینه های گوناگون مثال زده شده است. در نهایت به پردازش اثرانگشت و کارایی آن در نرم افزار متلب پرداخته، که به بررسی عملیات باینری و ساختاری آن بر روی اثرانگشت را همراه با کدهای متلب ارائه گردیده شده است.

کلمات کلیدی: بیومتریک–پردازش اثر انگشت– تشخیص هویت

1-1 : مقدمه

"امروزه، استفاده از سیستم های بیومتریک علاوه بر کاربردهای جرم شناسی، در خدمات شهروندی و دولتی نیز بسیار متداول شده است. درسیستم های بیومتریک از ویژگی های حیاتی و رفتاری افراد به منظور تشخیص هویت آنان استفاده می شود. ویژگی های حیاتی و رفتاری متعدی به منظور استفاده در سیستم های تشخیص هویت مبتنی بربیومتریک ارایه شده است. سیستم های بیومتریک مبتنی بر اثر انگشت از خصوصیات مهمی نظیر امنیت بالا، ارزان بودن ادوات اخذ اثرانگشت، کوچک بودن و نیز سهولت کار با آنها برخوردار هستند. این خصوصیات سبب شده تا سیستم های تشخیص هویت مبتنی براثرانگشت، نسبت به سایر سیستم های تشخیص هویت، بیشتر مورداستفاده قرار گیرند. در حالت کلی، سیستم های بیومتریک به دوروش تایید و یا شناسایی، عمل تشخیص هویت را انجام می دهند."[1]

2-1: تعریف بیومتریک[1]

بیومتریک از کلمه یونانی bios به معنای زندگی و کلمه metrikos به معنای اندازه گیری و تخمین تشکیل شده است و با عنوان زیست سنج معرفی می شود. 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 می‌توان گفت که همه افراد در زندگی روزمره خود، ناخودآگاه از بیومتریک استفاده می‌کنند. به عنوان مثال هویت افرادی که با آنها سرو کار داریم را می‌توان از روی صدا، چهره و حتی طرز راه رفتن‌شان تشخیص دهیم بنابراین می‌توان تاریخچه استفاده از بیومتریک را به قدمت تاریخ بشر دانست. فناوری بیومتریک به عنوان یکی از ده فناوری جدید جهان است که آینده را تغییر خواهد داد.

یک سیستم بیومتری اساسا یک سیستم تشخیص الگو است که یک شخص را بر اساس بردار ویژگی های خاص، فیزیولوژیک خاص، یا رفتاری که دارد باز شناسی می کند. بردار ویژگی ها پس از استخراج معمولا در پایگاه داده ذخیره می شود. یک سیستم بیومتری بر اساس ویژگی های فیزیولوژیک اصولا دارای ضریب اطمینان بالایی است.

3-1: سیستم های تشخیص هویت

اولین نوع سیستم های شناسایی چیزایی است که کاربران به همراه دارند. توکن معمولاً چیزی است که شما به همراه خود دارید و می توان 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.

[1] biometric

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

دسته سوم سیستم های مبتنی بر بیومتریک یعنی چیزایی که مربوط به کاربران است. این سیستم ها از خصیصه‌های فیزیولوژیکی و رفتاری انسان جهت شناسایی استفاده می کنند. این روش دیگر معایب روش های قبل را ندارد و امنیت و دقت را تا حد بسیار زیادی افزایش داده است.

سیستم شناسایی بیومتریک و تشخیص هویت در بسیاری از موارد با هم اشتراک دارند اما به طور کامل شبیه هم نیستند. در واقع بیومتریک از ویژگی ها و مشخصه های رفتاری و فیزیکی فرد استفاده می کند و سپس تصمیم می گیرد که آیا این همان کسی است که ادعا می کنید یا خیر. درحالی که تشخیص هویت تنها از برخی ویژگی های فیزیکی فرد استفاده می کند و اغلب در تحقیقات جنایی کاربرد دارد. امنیت سیستم های شناسایی بیومتریک از مشخصه های فیزیکی فرد همانند اثر انگشت الگوی دست، ساختار عنبیه، رگ های دست فرد یا از مشخصه های رفتاری مانند: صدا دست خط یا حتی آهنگ و ریتم نوشتن استفاده می کند. سیستم بیومتریک به جای مقایسه تصویرهای واقعی از الگوریتم ها و کدهای عددی برای تحلیل اطلاعات استفاده می کند. این اطلاعات فضایی بسیار کم و در حد چند بیت اشغال می کند.

1-3-1 : انواع سیستم تشخیص هویت مبتنی بر بیومتریک

- **سیستم تایید هویت (تطابق ۱:۱)**

"در این سیستم ها شخص مدعی داشتن یک هویت خاص است. سیستم به منظور تایید یا رد این ادعا، ویژگی بیومتریک مورد نظر شخص مدعی را دریافت و با نمونه ی واقعیِ موجود در پایگاه داده، مقایسه می کند."[2]

- **سیستم شناسایی هویت (تطابق 1:n)**

"در این سیستم ها، شخص یک ویژگی بیومتریک خود را در اختیار سیستم قرار می دهد. سیستم پایگاه داده خود را به منظور یافتن نمونه ی مشابه با ویژگی اخذ شده، جستجو می کند. در صورت یافتن نمونه ی مشابه، هویت شخص مورد نظر شناسایی می شود. در هر دو سیستم اشاره شده در بالا، سرعت سیستم به زمان لازم بر ای تشخیص هویت بستگی دارد. در این سیستم ها ابتدا ویژگی های مربوط به نمونه ی اخذ شده، استخراج و سپس با ویژگی های موجود در پایگاه داده مقایسه می شود. از این رو زمان لازم برای تشخیص هویت، برابر مجموع زما ن های لازم برای استخراج ویژگی ها و تطابق است. زمان لازم جهت استخراج ویژگی ها در سیستم های تایید و شناسایی یکسان است. از آنجا که تعداد عملیات تطابق در این دو سیستم متفاوت است، زمان لازم برای تطابق در آنها یکسان نیست. از این رو زمان لازم برای تایید هویت به صورت زیر بیان می شود."[3]

$$tv = t\,fe + tm$$

4-1: طبقه بندی متدهای بیومتریک

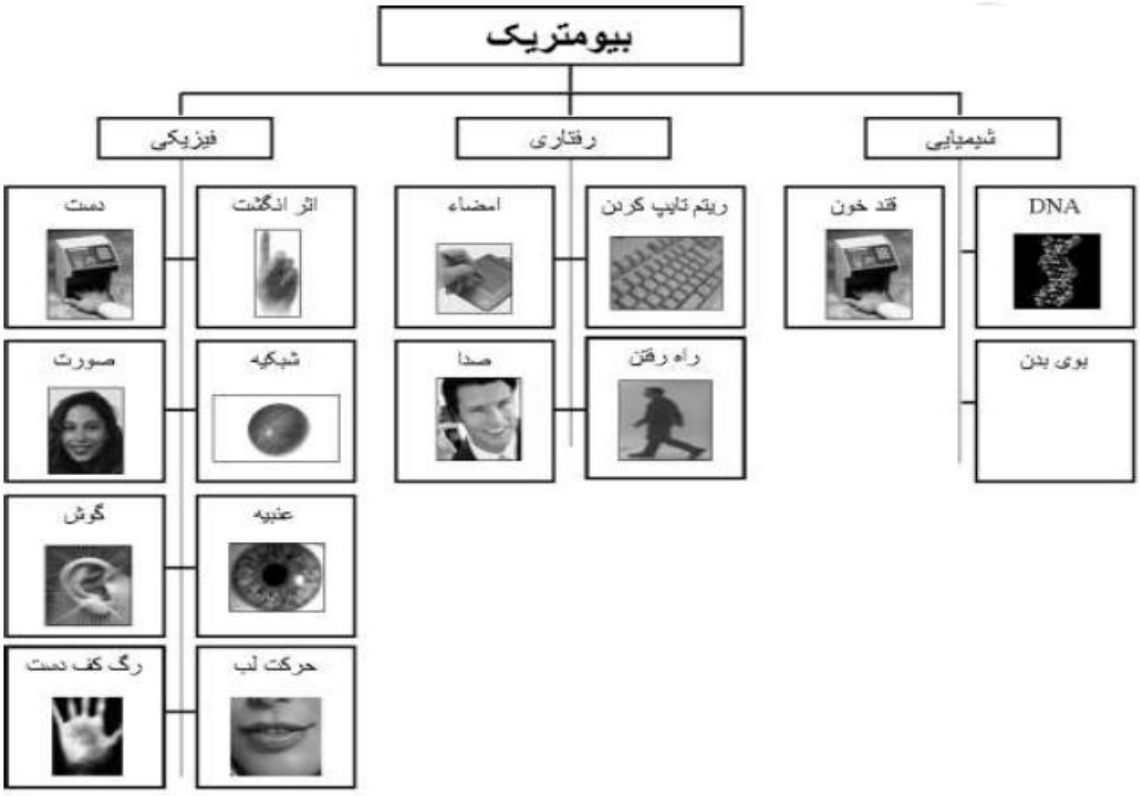
عموما در سیستم های بیومتریک از دو نوع ویژگی مختلف افراد جهت شناسایی استفاده می شود که در ذیل به آنها اشاره می کنیم.

- **پارامترهای فیزیولوژیکی**[1]: "اساس شناسایی در این کلاس، اندازه گیری و انالیز مشخصه های ثابت یک شخص می باشد. این دسته از ویژگی ها به مجموعه ای از خصوصیات همراه انسان اعم از اثر انگشت، عنبیه چشم، چهره، DNA و غیره اشاره دارد،این ویژگی ها عمدتاً از بدو تولد انسان و گهگاه قبل از تولد انسان شروع به شکل گیری نموده و تا آخر عمر در بدن انسان ثابت و غیرقابل

[1] Physiometric

تغییر (گهگاه تغییرات اندک) می مانند." [4] سنجش های مشخصات فیزیکی به ابزار سنجش بزرگتر و نرم افزار پیچیده تری احتیاج دارند.

- **پارامترهای رفتاری**[1]: "شناسایی الگوهای رفتاری مشخص یک فرد است. این ویژگی ها در حقیقت خصوصیات ناشی از رفتارهای انسان هاست نظیر راه رفتن انسان، نحوه فشردن دکمه ها (مثلا موبایل) و غیره که می تواند بیانگر مشخصات یک انسان خاص باشد نظیر راه رفتن یک انسان که گاهی با نگاه کردن آن از پشت سر می توان تشخیص داد که وی چه کسی است."[5] رفتار با زمان و حال شخص تغییر می کند. تکنیکهای سنجش رفتاری هنگامی به بهترین نحو عمل می کنند که مرتبا استفاده شوند، و به این ترتیب سطوح تغییرات هر فرد مورد توجه قرار می گیرد. مدلهای سنجشهای رفتاری باید این تغییرات را لحاظ کنند.



شکل1: طبقه بندی کلی متدهای بیومتریک

[1] Behavioral

5-1: سیستم های بیومتریک

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

6-1: بخش های بنیادی سیستم بیومتریک

یک سیستم بیومتریک شامل چهار بخش بنیادی است:

- Sensor Module : قسمت نمونه برداری که اطلاعات خام مورد نیاز را جمع آوری می کند. مانند تصویر اثرانگشت.

- extraction Module Feature : قسمت پردازش برای استخراج ویژگی ها از اطلاعات مرحله قبل می باشد.

- Module Matching : قسمت مطابقت که بررسی می کند آیا اطلاعات جمع آوری شده با اطلاعات الگو مطابقت می کند یا خیر؟ مثلا 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 اینکه 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.

1-7: بیومتریک های متداول

1. استفاده از اثر انگشت
2. استفاده از تصاویر صورت
3. استفاده از تصاویر عنبیه چشم
4. استفاده از هندسه دست
5. استفاده از بو یا خواص شیمیایی
6. استفاده از تصاویر شبکیه
7. استفاده از امضا
8. استفاده از صدا
9. استفاده از اثر کف دست

1-7-1: اثرانگشت[1]

تعیین هویت افراد با استفاده از اثر انگشت نسبت به سایر روش های بیومتریک تعیین هویت، به طور گسترده ای مورد استفاده قرار می گیرد. به برآمدگی ها و فرو رفتگی های موجود در پوست نوک انگشت اثر انگشت گویند.

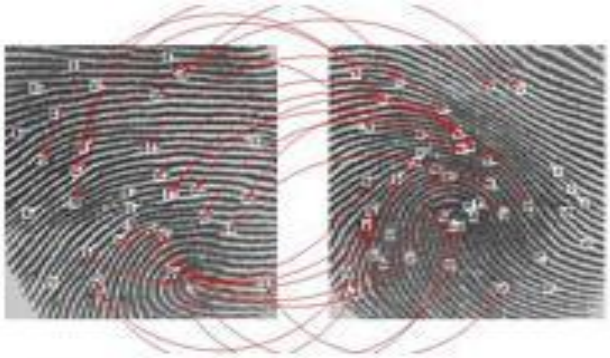
بزرگترین دلیل استفاده گسترده و عمومی از اثر انگشت بعنوان ابزار تعیین هویت این است که اثر انگشت افراد منحصر به فردند و در طول عمر فرد تغییر نمی کنند. اثرانگشت از قدیمی‌ترین و شناخته شده‌ترین روشهای شناسایی بیومتریک افراد است. اما شناسایی افراد با استفاده از اثرانگشت در سالهای اخیر تغییرات عمده‌ای داشته است. در روشهای جدید به جای استامپ و کاغذ از اسکنرهای خاص که قابلیت بررسی و تطبیق سریع اثرانگشت را با نمونه ضبط شده دارند، استفاده می‌شود.

این روش از معمول ترین روشهای تشخیص هویت به شمار می‌رود؛ تا حدی که حتی در سیستم‌های حضور و غیاب کارمندان و برخی لپ تاپ های جدید نیز از این روش به عنوان یکی از روشهای مطمئن و سریع استفاده می‌شود. تکنیک های شناسایی اثر انگشت اطمینان و ثبات در تشخیص هویت را تضمین می کنند و بدین ترتیب در کاربردهای مختلف مورد استفاده قرار می گیرد. از جمله اثر انگشت در صنایع کامپیوتری مانند Software licensing, Network, business و وسایل جانبی مانند ماوس و صفحه کلید کاربرد دارد. همچنین در روشن کردن اتومبیل، قفل گاو صندوق یا درب ها یا کارت های اعتباری استفاده می شود. از طرف دیگر مشکلات عملی زیادی در سیستم های شناسایی اثر انگشت وجود دارد. هر دفعه که یک اثر انگشت گرفته می شود ممکن است به دلیل قابلیت کشسانی پوست، تحریفاتی در شکل و محل اثر انگشت ایجاد شود. علاوه بر این اطمینان بالا و پردازش بلادرنگ، فاکتورهای مهم مورد نیاز در سیستم خودکار

[1] fingerprint

شناسایی اثر انگشت هستند. برای حل این مشکلات، استخراج دوشاخه ها از تصاویر اثر انگشت و کاربرد آن ها در تطبیق اثر انگشت مورد بررسی قرار می گیرد.

1-8: روش‌های تحلیل اثر انگشت



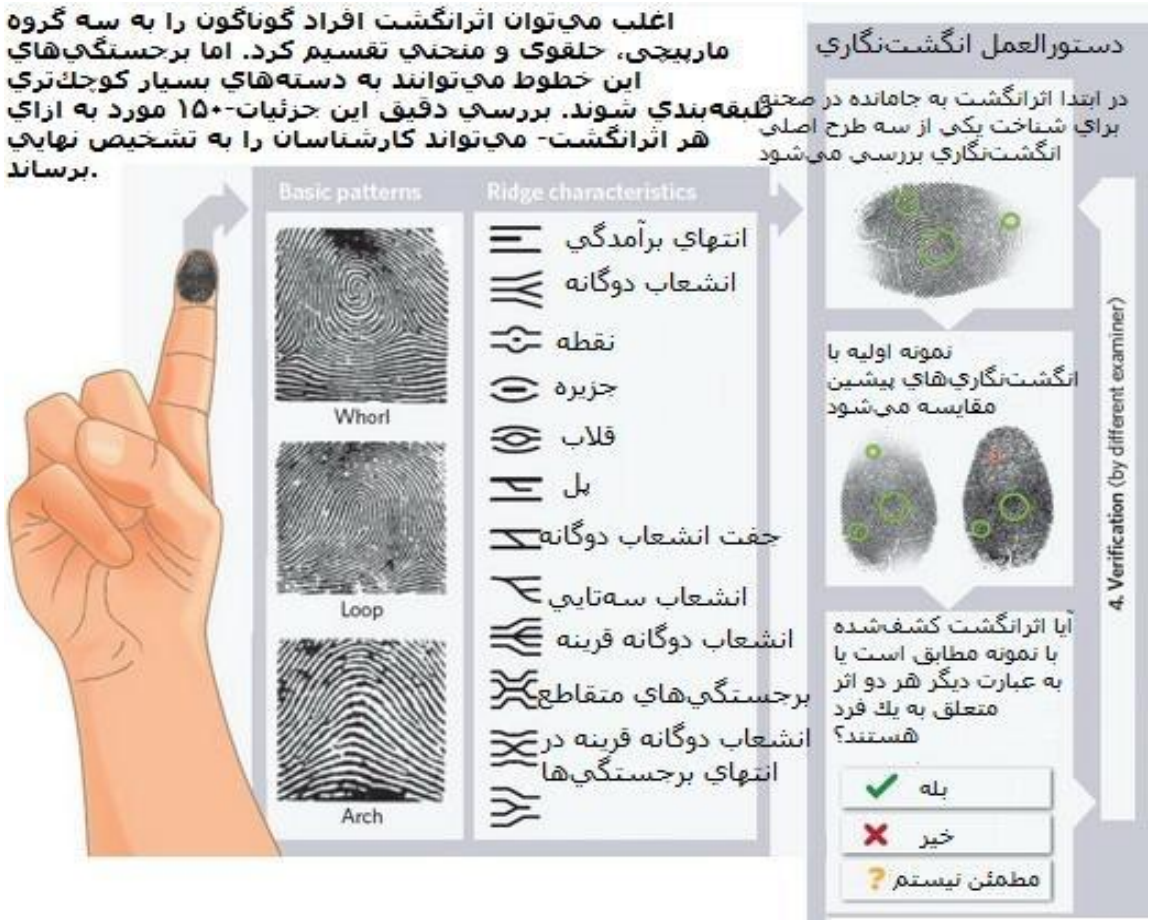
شکل 2: تحلیل نقاط در اثر انگشت

برای به حداقل رساندن داده‌های یک اثر انگشت در بانک اطلاعاتی، همه تصویر به طور کامل نگهداری نمی‌شود. نخست کل تصویر تحلیل شده و سپس نقاط کلیدی آن ذخیره می‌شود. این کار نقش بسیار مهمی برای جستجوی سریع در بانک‌های اطلاعاتی دارد. در مجموع هر تصویر اثرانگشت حدود 35 ویژگی مهم مانند نقاط تقاطع، نقاط پایانی، انشعاب و ... دارد. برای تشخیص هر اثر انگشت و اعلام آن با قطعیت بررسی 8 تا 22 ویژگی کافی است. مشخصات اثر انگشت یا به طور مستقیم روی ایستگاه یا روی کارت‌های هوشمند یا روی یک سرویس دهنده ذخیره می‌شود و در صورت تطابق مشخصات دریافتی با مشخصات ذخیره شده نسبت به صدور مجوز تصمیم‌گیری می‌شود.

این روش در علم بیومتری MBFM[1] نامیده می‌شود. در این شیوه پردازش سنگینی روی تصویر برای استخراج مشخصات کلیدی انجام می‌گیرد. اما روش دیگری نیز با نام CBFM [2] وجود دارد که در آن به جای

[1] Minutiae-Based Fingerprint
[2] Correlation Based Fingerprint Matching

مقایسه تک تک نقاط کلیدی با داده‌های اصلی، بخش‌هایی از تصویر با بخش‌های متناظر از شکل اصلی مقایسه می‌شود.



"با توجه به این که اغلب متخصصان انگشت نگاری سال ها آموزش دیده اند، 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 ACE-V نام دارد،که مراحل متوالی تحلیل، مقایسه، ارزیابی و تایید نهایی است. خط فاصله نشان می دهد تایید نهایی باید توسط شخص دیگری انجام بگیرد."[6]

"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 روی نکات ظریف تری مانند انشعاب های گرفته شده از

برآمدگی ها و نقاط پایانی آنها خواهد بود. در بسیاری از موارد مرحله دوم تعیین کننده است. اگر احتمال خطا وجود داشته باشد، می شود در مرحله سوم شکل لبه برآمدگی ها یا طرح پرزها را نیز بررسی کرد.

پس از اتمام مرحله تحلیل، مقایسه با نمونه های پیشین آغاز می شود که شامل باز بینی برای تعیین شباهت ها یا تفاوت ها با نمونه هایی است که پیش از این وجود داشته، از بایگانی استخراج شده یا متعلق به مظنون هستند."[7]

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

1. شناسایی که به معنی تشخیص اثرانگشت است.
2. مردود شدن اثر که باید حداقل یک تفاوت آشکار با نمونه اولیه وجود داشته باشد.
3. غیرقاطع که نشان می دهد اثر به اندازه کافی برای تشخیص و اعلام نظر واضح نبوده است.

در واقع سیستم به شکلی طراحی شده که خطاها بیشتر به سمت تشخیص منفی نادرست بروند تا اینکه بی گناهی گناهکار تشخیص داده شود."[8]

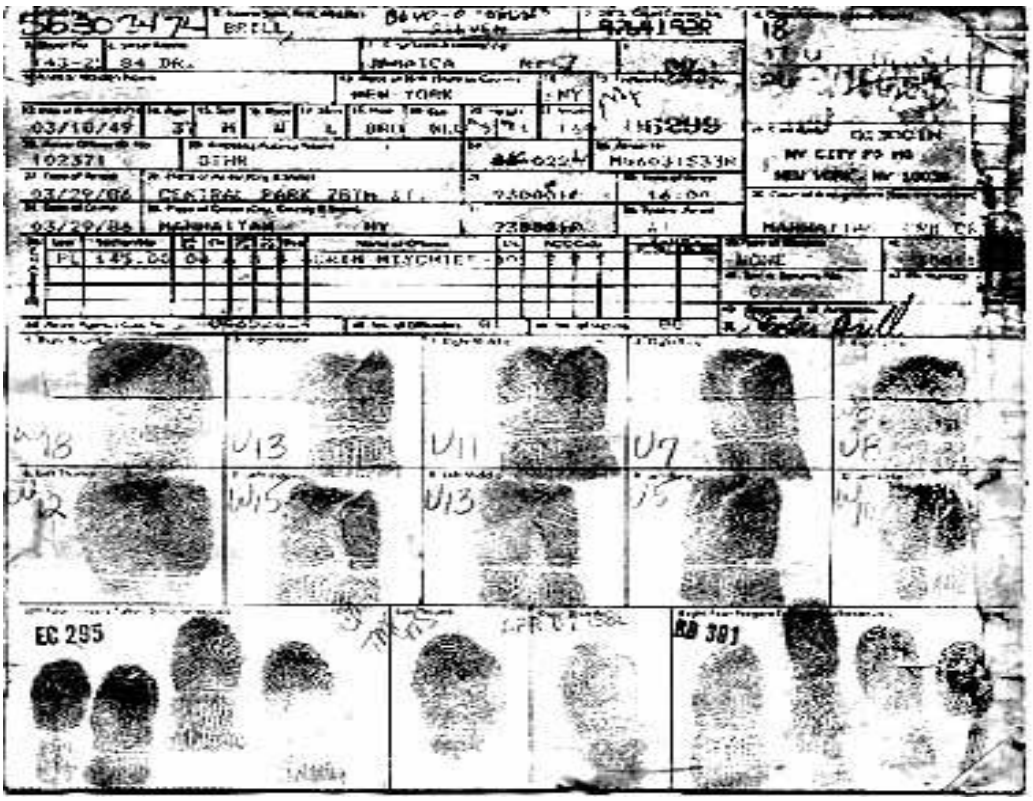
با این وجود، پرونده های نادری نیز وجود دارند که بیشتر حاصل مجموعه ای از اشتباهات بوده اند. پرسش اصلی اینست که چرا اصلا چنین اشتباهاتی رخ می دهند؟

در کتاب «چالش ها در انگشت نگاری» یکی از علل خطای انسانی، تخلف از دستورالعمل ذکر شده و انجام هم زمان مرحله تحلیل و مقایسه با یکدیگر به دلیل کاهش زمان این فرایند ذکر شده است.

1-8-1: نحوه بدست آوردن تصویر اثر انگشت

1-1-8-1: اخذ تصویر از طریق کاغذ و مرکب

قدیمی ترین روش همان روش استفاده از کاغذ و جوهر است در این شیوه ابتدا سطح انگشت را به جوهر اغشته کرده و سپس روی کاغذ می غلتانند. برای وارد کردن تصویر به دست امده به یک سیستم کامپیوتری از یک پویشگر تخت استفاده می شود .تصویر بدست امده از این روش بسیار اعوجاج داشته و حتی در تشخیص بصورت دستی نیز نیازمند یک فرد خبره است. که این روش به علت مشکلات خاص خود و البته پیشرفت تکنولوژی کم کم منسوخ می شود.



شکل 3: اثرانگشت با استفاده از کاغذ و مرکب

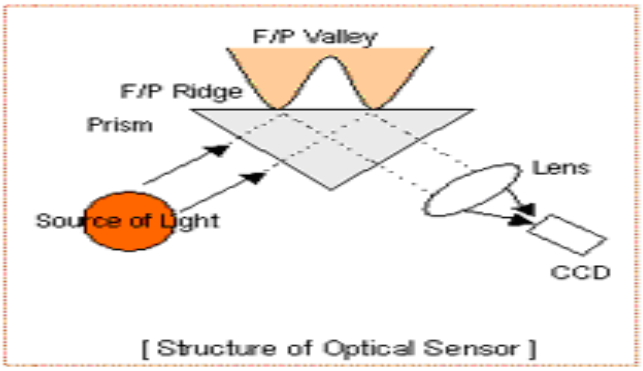
1-8-1-2: اسکن زنده

روش دیگری که امروزه در بسیاری از سیستم ها از ان استفاده می شود بکارگیری دوربین های CCD است. که اصطلاحا اسکن زنده نیز نامیده می شود دستیابی به تصویری با کیفیت خوب امکان پذیر است.

چهار تکنیک برای اسکن زنده وجود داردکه به ان ها اشاره می کنیم :

1. **تکنیک نوری**
2. **ماورا صوت**
3. **میدان الکتریکی**
4. **تکنیک حرارتی**

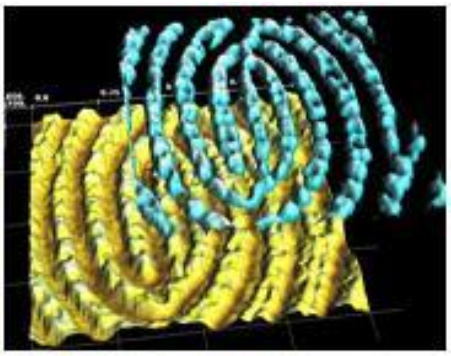
تکنیک نوری: برای خواندن اثر انگشت، سیستم‌های زیادی که از فناوری های گوناگون بهره می‌برند، وجود دارد. اما سیستم‌هایی که اثر انگشت را بر پایه روش‌های نوری ثبت می‌کنند، بیشتر گسترش پیدا کرده‌اند. در این شیوه، نور از سوی یک چشم به انگشت تابانده می‌شود. سپس یک دوربین CCD، پرتوهای باز تابیده را دریافت کرده و از روی آنها یک عکس سیاه و سفید می‌سازد. این عکس مشخصات بارز اثر انگشت را نشان می‌دهد وضوح این سیستم به میزان اهمیت و نوع کاربرد بستگی دارد. برای نمونه برای تشخیص اثر انگشت کودکان که پیچیدگی بیشتری دارد از وضوح 1000dpi استفاده می‌شود در حالیکه برای بزرگسالان، وضوح 500 dpi کافی است.



ماوراء صوت: در روش ماورا صوت با توجه به میزان انرژی صوتی منعکس شده از سطح انگشت برای اشکار سازی لبه ها و شیارها استفاده می شود.

میدان الکتریکی: بر اساس اندازه گیری اختلاف ظرفیت الکتریکی سطح انگشتی که حسگر را لمس می کند عمل می کنند و در نهایت حسگر های حرارتی با اندازه گیری اختلاف دمای سطح پوست شیارها و لبه های اثر انگشت را نمایان می سازد.

تشخیص اثر انگشت با روش‌های حرارتی و مافوق اولتراسوند:



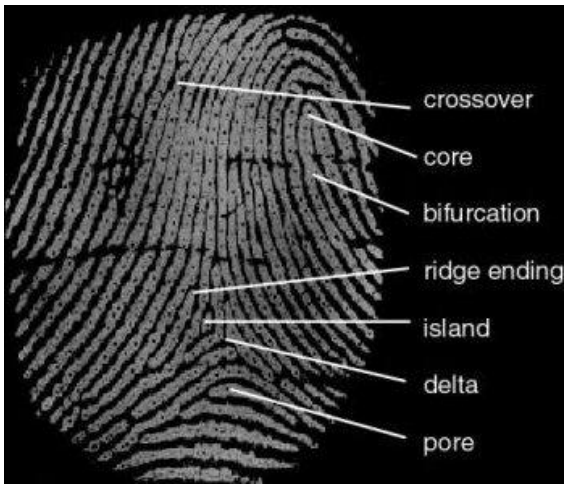
حسگرهای مافوق اولتراسوند و حرارتی نیز برای تشخیص اثر انگشت به کار می‌روند. در روش حرارتی، آرایه‌ای از حسگرها تصویر گرمایی انگشت را می‌سازد. سپس این تصویر بر پایه گرادیان دما به یک نمای سه بعدی از اثر انگشت تبدیل می‌شود روش‌های مافوق اولتراسوند اکنون از دقیق‌ترین و همچنین گران‌ترین

روش‌های تشخیص هویت از روی انگشت هستند. دلیل آن هم این است که آلودگی یا دیگر عوامل مزاحم در کار این روش اختلالی ایجاد نمی‌کند.

در این روش؛ چند حس‌گر امواج مافوق اولتراسوند را به سمت انگشت می‌فرستند. سپس بازتاب این امواج را دریافت کرده و براساس فاصله زمانی بازتاب‌ها یک تصویر سه بعدی از اثر انگشت می‌سازند.

9-1: شناسایی از طریق اثر انگشت

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 (minutiae) 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. ماهیت های قابل اندازه گیری در شکل 4 نشان داده است.



شکل 4: ویژگی های قابل اندازه گیری در اثرانگشت

در تشخیص اثر انگشت دو روش عمده وجود دارد:

- Minutia Matching
- Pattern Matching

در روش اول یک شابلون از محل قرار گیری ریزه کاریهای انتهای لبه ها، انشعاب ها، کمان ها، مارپیچ ها و حلقه ها تهیه می شود 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 علامت های مجزای دیگر و داده های حاصل از مقایسه مجموعه لبه ها در این نواحی، استفاده می شود.

عموما سایز الگو در روش Pattern Matching 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 می شود و مابقی ترتیب اثر داده نمی شوند، ولی از روش دوم می توان به اثر انگشت نیز رسید.

1-9-1: مراحل پردازش تصویر در شناسایی بر اساس اثر انگشت

a) Original
b) Orientation
c) Binarised
d) Thinned
e) Minutiae
f) Minutiae graph

حالت اول شمای یک اثر انگشت پردازش نشده را نمایش می دهد. در مرحله اول جهت خطوط اثر انگشت توسط متد های 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 حالت چهارم میزان رنگ تصویر حاصله را کاهش می دهند تا نویزهای کوچک باقیمانده نیز حذف شوند و حجم تصویر نیز کاهش یابد.

در مرحله پنجم ریزه کاریها علامت گذاری می شوند و در پایان نیز این ریزه کاریها به یکدیگر متصل میگردند که ماتریس حاصل از شکل بدست آمده الگوی مورد نظر ما را تولید می کند.

10-1: کلاس بندی آثار انگشت

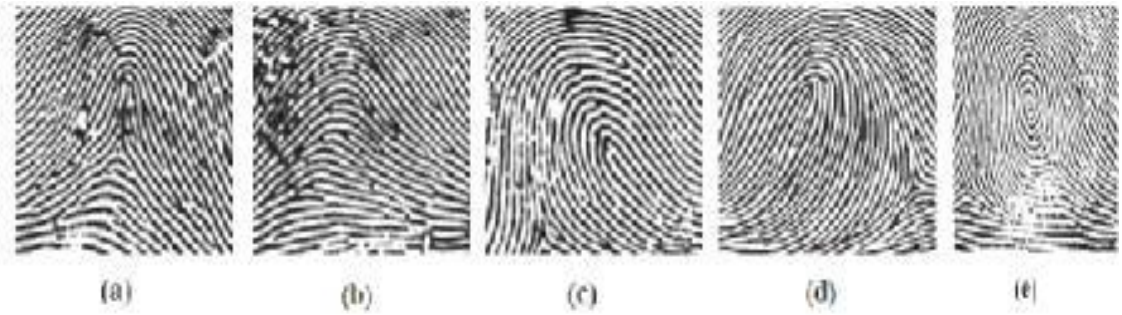
"هنگامی که تعداد نمونه های اثرانگشت در پایگاه داده افزایش یابد، کلاس بندی آنها به منظور کاهش خطای شناسایی و تطبیق سریعتر ضروری می باشد."[9]

"اثرانگشت در دوران جنینی شکل گرفته و تحت تأثیر حوادث روحی و روانی تغییر نمی کند. استفاده از اثرانگشت برای تشخیص هویت، بر اساس خطوط برجسته بند اول انگشتان می باشد. خطوط سر انگشت که توسط کلاف های غدد عرق پوست بوجود می آیند، شامل برجستگی ها و فرورفتگی هایی است. به هر یک از این ها و به فضای خالی بین دو رگه شیار[1] برآمدگی ها رگه می گویند. بعد از تماس سر انگشت با سطوح صاف[2]، اثر نقش رگها بر روی سطح باقی می ماند که به آن اثرانگشت می گویند. رگه ها و شیارها دارای ساختار منظم و شکل ویژه ای هستند که سبب منحصر بفرد بودن آنها می شود. با وجود تنوع نامحدود نقوش اثرانگشت، می توان آنها را به کلاس های محدود و از پیش تعریف شده طبقه بندی نمود. گاهی اوقات اطلاعات مربوط به سن، جنس، نژاد و دیگر خصوصیات فردی در دسترس بوده، که سبب جستجوی سریعتر می شود؛ ولی این اطلاعات در مواردی مانند شناسایی جنایی و اثرانگشت مخفی موجود نمی باشند. روش معمول، تقسیم بندی پایگاه داده به چندین بخش بر اساس خصوصیات یکی از *delta* و *core* و ویژگیهای

[1] Ridge
[2] Valley

ذاتی اثرانگشت است. این دو نقطه که بر اساس جریان رگه ها در اثرانگشت مشخص می شوند، برای کلاس بندی مورد استفاده قرار می گیرند.

کلاس بندی اثرانگشت هنوز هم یکی از مسائل مشکل، چه برای افراد خبره و چه برای سیستم های خودکار بشمار می آید. اثرانگشت علاوه بر داشتن گروه های محدود، دارای توزیع نابرابر در هر گروه نیز می باشد. همچنین آثاری هستند که در هیچ گروهی قرار نمی گیرند. این عوامل طبقه بندی اثرانگشت را دشوار و پیچیده کرده است. "[10] در اغلب روشهای کلاس بندی آثارانگشت، از 5 کلاس کمان[1]، کمان مایل[2]، حلقه چپ[3] ، حلقه راست[4] و مارپیچ [5] استفاده می شود، که در شکل 5، این کلاس ها نمایش داده شده اند.



شکل 5: کلاس های اثرانگشت

11-1: مزایای سیستم های اندازه گیری اثر انگشت:

1. "هر شخص دارای اثر انگشت منحصر بفردی است.
2. اثر انگشت در برابر گذشت زمان مقاوم است.
3. این تگنولوژی به بلوغ خود رسیده است.

[1] *Arch*
[2] *Tented Arch*
[3] *Loop Left*
[4] *Right Loop*
[5] *Whorl*

4. استفاده از آن بسیار راحت است.
5. دارای نرخ خطای مساوی پایینی می باشد.
6. ارزان است.
7. عامه پسند است."[11]

12-1: خطاهای سیستم شناسایی خودکار اثرانگشت

یک سیستم شناسایی اثرانگشت از سیستم های دسته بندی و تطابق تشکیل شده است. از این رو خطاهای سیستم شناسایی به سیستم های دسته بندی و تطابق وابسته است. در حالت کلی در یک سیستم شناسایی، سه دسته خطای پذیرش نادرست، خطای عدم پذیرش نادرست و خطای جابجایی هویت وجود دارد. مفهوم خطاهای پذیرش نادرست و عدم پذیرش نادرست در قسمت مربوط به سیستم تایید هویت ارایه شده است. خطای جابجایی هویت به صورت زیر بیان می شود.

اگر سیستم شناسایی اثرانگشت، یک ادعای درست را با نمونه ی موجود در پایگاه داده که مربوط به شخص دیگری است مشابه در نظر بگیرد، خطای جابجایی هویت روی می دهد. تفاوت این خطا با پذیرش نادرست این است که در خطای جابجایی هویت، اثرانگشت ورودی دارای نمونه ی مشابه در پایگاه داده است. در مورد خطای پذیرش نادرست، اثرانگشت ورودی فاقد نمونه ی مشابه در پایگاه داده می باشد.

در سیستم های شناسایی خودکار اثرانگشت احتمال خطای پذیرش نادرست، احتمال خطای عدم پذیرش نادرست و احتمال خطای نمایش جابجایی هویت را به ترتیب با FARn , EXRn و FRRn می دهند. این سه پارامتر از مهمترین پارامترهای یک سیستم شناسایی خودکار اثرانگشت می باشد.

13-1: اشتباهات در انگشت نگاری

"در این بخش از خطاها به این بر می گردد که دستورالعمل ها گاهی تصریح نشده است، به عنوان مثال مرحله ی تایید نهایی باید توسط فرد دیگری صورت بگیرد ولی در اغلب موارد این فرد در همان بخشی کار می کند که مراحل پیشین صورت گرفته و خواه ناخواه در جریان پرونده قرار دارد.

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

عده دیگری از منتقدان بحث صلاحیت متخصصان انگشت نگاری را مطرح کرده اند. مسئله بسیار پیچیده است، چرا که اغلب این افراد تا سال ها بعد هم نمی دانند آیا درست تصمیم گرفته اند یا نه!

موضوع دیگری هم وجود دارد که می تواند به خطای انسانی دامن بزند و آن کیفیت چاپ اثرانگشت کشف شده در صحنه است. متخصصان معتقدند، هیچ بازآفرینی یی بی عیب و نقص نیست و این هم می تواند احتمال تشخیص نادرست را افزایش دهد. می شود با شناخت بهتری از گستردگی طرح های مورد استناد در مرحله دوم تحلیل اثر انگشت یا «مقایسه» د رملیت های گوناگون، کار را برای متخصصان انگشت نگاری ساده تر کرد، اما متاسفانه هنوز چنین تحقیقی در سطح گسترده انجام نشده است.

نکته دیگر ارزش گذاری اثر درتصمیم گیری های قضایی است. به نظر می رسد باید فرهنگ قضایی نیز انتظار تغییراتی را داشته باشد.چرا که علم می آید تا به بخش مؤثری ازتصمیم های نهایی پرونده های قضایی بدل شود."[12]

14-1: کاربردها

هم اکنون بسیاری از سازمان های امنیتی مالی و نظامی در کشورهای مختلف جهان از تکنولوژی تشخیص اثرانگشت برای دسترسی به اطلاعات محرمانه و ورود به مکان های خاص استفاده می کنند. ولیکن به تازگی این تکنولوژی به علت قیمت مناسب، کارایی و سرعت بالا کاربردهای تجاری نیز یافته است.

"نمونه هایی از کاربرد های فراوان این تکنولوژی که شرکت هوش مصنوعی رایورز ارائه می دهد در ادامه آمده است: استفاده در جرم شناسی (که مشهورترین کاربرد این سیستم ها می باشد)

- **امنیت در IT**

ورود به کامپیوتر (Computer Logon)

دسترسی به شبکه

تجارت الکترونیکی

امنیت در صفحات وب

رمزگذاری فایل ها

- **شناسایی هویت**

کارت شناسایی / ملی

انتخابات

کارت پایان خدمت

گذرنامه الکترونیک

گواهی نامه رانندگی

- **امنیت در بانکداری**

مکمل و جایگذاری کارت های اعتباری، Debit Card, Prepaid Card

قابل استفاده در دستگاه های کارت خوان، ATM و ...

بانکداری الکترونیکی (تشخیص هویت افراد نقد کننده چک

- **کنترل دسترسی فیزیکی**

درهای ورود و خروج

سیستم حضور و غیاب

دستگاه های هشدار دهنده

گاوصندوق، صندوق امانات و ...

مکان های امنیتی

- **وسایل قابل حمل**

تلفن همراه

PAD

کامپیوترهای Notebook

- **صنایع خودروسازی**

سوئیچ

قفل درهای ماشین

- **صنایع نظامی**

گشت شناسایی

اسلحه های هوشمند و ..."[13]

15-1: پردازش اثر انگشت در نرم افزار متلب

1-15-1: عملیات باینری کردن در پردازش تصویر

تصویر باینری به تصویری گفته می‌شود که پیکسلهای آن تنها دارای یکی از دو مقدار ممکن 0 و 1 یا 0 و 255 باشند. در متلب تصاویر باینری می‌توانند بصورت تصاویر شدت و یا بصورت تصاویر اندیس‌شده ذخیره و معرفی شوند. در حالت دوم ماتریس نقشه رنگ تنها دارای دو سطر خواهد بود. این تبدیل برای کاهش سطوح خاکستری یک تصویر به دو سطح سیاه و سفید بکار می رود. از مزایایی این تبدیل می توان کاهش حجم محاسبات، ساده کردن تصمیم گیری در مورد پیکسل ها و ... را نام برد.

2-15-1: عملیات ساختاری[1]

چهار عملیات بر روی تصاویر باینری می توان انجام داد.

- عملیات افزایش
- عملیات فرسایش
- عملیات گشودن و بازکردن
- عملیات بستن

1-2-15-1: عملیات افزایش [2]

[1] Morphological Operations

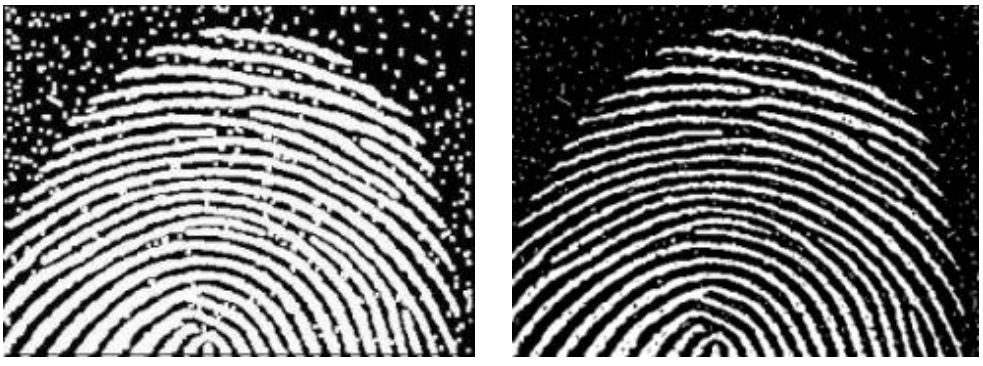
منظور از عملیات افزایش عملیاتی است که باعث افزایش ابعاد اجزا داخل تصویر به اندازه یک یا چند پیکسل می‌گردد. در اثر این عمل ممکن است نقاطی که از یک تصویر باینری در اثر عواملی چون تاثیر نویز یا اعمال حد آستانه نامطلوب جا افتاده است، تصحیح گردند. مثلا ممکن است دو جزء از تصویر به یکدیگر متصل گردند.

الگوریتم اعمال فیلتر افزایش بدین صورت است که تمامی نقاط سیاه تصویر بررسی شده در صورتیکه حداقل یکی از همسایگان انتخابی نقطه مورد بررسی سفید باشند، نقطه مزبور نیز سفید خواهد شد در غیر اینصورت سیاه باقی خواهد ماند. برای عملیات افزایش در متلب از تابع imdilate استفاده می شود وفرمول کلی استفاده از این توابع بصورت زیراست:

```
bw2=imdilate(bw1  , se);
```

همانطورکه ازنام عملگرپیداست ، این عملگر باعث گسترش نقاط در تصویر می شود.

```
>> BW1 = imread('circbw.tif');
>> SE = strel('rectangle',[5  5]);
>> BW2 = imdilate(BW1,SE);
>> imshow(BW1),figure,imshow(BW2)
```



شکل 6: عملیات افزایشی اثر انگشت

[2] Dilation

1-15-2-2: عملیات فرسایش [1]

عملیات فرسایش دقیقا عکس عملیات افزایش است. در این عملیات معمولا نقاط ناخواسته تصویر باینری حذف می‌شوند و سایر اجزا تصویر نیز به اندازه یک یا چند پیکسل نازکتر خواهند شد. عملا تمامی نقاط سفید تصویر بررسی شده در صورتیکه حداقل یکی از همسایگان انتخابی آن سیاه باشد، آن نقطه نیز سیاه خواهد شد.

برای عملیات فرسایش از تابع imerode استفاده کنید و فرمول کلی استفاده از این توابع بصورت زیر است:

```
bw2=imerode(bw1,  se);
```

اعمال عملگر مورفولوژیکی سایش در محیط MATLABبا استفاده تابع imerode انجام می پذیرد.

```
>> BW1 = imread('circbw.tif');
>> SE = strel('rectangle',[5  5]);
>> BW2 = imerode(BW1,SE);
>> imshow(BW1),figure,imshow(BW2)
```

شکل 7: عملیات فرسایشی اثرانگشت

[1] rode

3-2-15-1: عملیات گشودن و بستن[1]

از ترکیبهای مختلف دو عملیات افزایش و فرسایش می‌توان عملیات دیگری ایجاد کرد. مهمترین این عملیات، عملیات گشودن و بستن است. در عملیات گشودن اجزایی از تصویر باینری که از یک اندازه تعیین شده کوچکتر باشند حذف می‌شوند بدون آنکه ابعاد سایر اجزا تغییر کند. در عملیات بستن نیز نواحی جاافتاده تصویر باینری بدون تغییر در ابعاد سایر اجزا ترمیم می‌گردند.

اعمال عملگر بستن بر روی تصویر باینری موجب می شود تا حفره های کوچک تصویر پرشوند.

اعمال عملگر باز کردن بر روی تصویر باینری موجب می شود تا اتصالات باریک تصویر حذف شده و تصویری آرام تر به دست آید.

عملا در صورتیکه ابتدا عملیات فرسایش و سپس افزایش بر یک تصویر باینری اعمال شود، نتیجه، عملیات گشودن خواهد بود اما اگر ابتدا افزایش و سپس فرسایش اعمال گردد، عملیات بستن حاصل خواهد شد.

در متلب برای اعمال عملیات گشودن و بستن و همچنین سایر عملیات مورفولوژی از تابع bwmorph باید استفاده کرد. اگرچه می‌توان این دو عملیات را از عملیات فرسایش و افزایش نیز بدست آورد

اعمال عملگرهای مورفولوژیکی باز کردن و بستن در محیط MATLAB به ترتیب استفاده توابع imopenو imclose انجام می پذیرد.

[1] Open & Close

در این مثال از عملگر بستن استفاده نمودیم.

```
>> originalBW  = imread (‘circles.png’);
>> se = strel (‘rectangle’,[5  5]);
>> closeBW  = imclose  (originalBW,se);
>> imshow  (originalBW),figure,imshow  (closeBW)
```

شکل 8: تصویر اصلی اثرانگشت

شکل 9: باز کردن تصویر اثرانگشت

شکل 10: بستن تصویر اثرانگشت

4-2-15-1: عملیات از پیش تعریف شده

تابع immorph : با استفاده از تابع immorph می‌توان بسیاری از عملیات ساختاری معروف پردازش تصویر را اعمال نمود. شکل کلی استفاده از این تابع بصورت زیر است:

```
bw2 = bwmorph(bw1 , operation , [n]);
```

آرگومان سوم اختیاری بوده و بیانگر ابعاد ماسک مورد استفاده یا فاکتور دیگری با توجه نوع آرگومان دوم در عملیات است. در صورت حذف آرگومان سوم، مقدار پیش فرض آن بکار برده خواهد شد. مقدار آرگومان دوم یکی از رشته‌های زیر است:

fill - hbreak - open - skel - remove - close - dilate erode

در این مثال نتیجه عملیات skel را بر روی تصویر نشان می‌دهد که اسکلت تصویر را بدست می آورد

```
bw1= imread('circbw.tif');
bw2= bwmorph(bw1 , 'skel' , inf)
imshow(bw1); figure;
imshow(bw2);
```

شکل 11: بدست آوردن اسکلت تصویر اثرانگشت با عملیات skel

16-1: نتیجه گیری

فناوری بیومتریک جزء یکی از اصلی ترین فناوری جدید جهان است که آینده را تغییر خواهد داد که با همه گیر شدن می تواند جهان را به سوی یک جهان مطلوب و امن سوق دهد. این فناوری باعث افزایش ضریب امنیت، سرعت وسهولت، کاهش هزینه ها، اطمینان خاطر در تجـارت الکترونیک، افزایش اعتماد عمومی و هزاران اتفاق خوب دیگر می شود و در نهایت پیش بینی می شود تا آینده ای دور، در سراسر دنیا بازاری پایدار و مستحکم برای بیومتریک وجود داشته باشد.

یکی از شاخه های فیزیکی فناوری بیومتریک اثرانگشت می باشد که حتی سرسخت ترین مخالفان انگشت نگاری هم به این تکنیک بیان دارند که از دیگر روش های شناسایی مبتنی بر آزمایش موها، تعیین گروه خون یا هر روش دیگری به غیر از تعیین DNA فرد به مراتب دقیق تر است. برجستگی ها، فرورفتگی ها و شکل نهایی خطوط سرانگشتان درون رحم شکل می گیرند و مجموعه ای بسیار پیچیده 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 پوست، همیشه پس از لمس، اثری از خود به جا خواهند گذاشت. با توجه به اینکه متخصصان انگشت نگاری سال ها آموزش دیده اند، بنظر می رسد، بیش از خطای انسانی باید نگران دستورالعمل چهار مرحله ای شناسایی اثرانگشت که در بسیاری از کشورهای جهان رایج است، باشیم.

فهرست منابع و مآخذ

- [1] هل فروش محمدصادق و محمدپور محسن. (1386)، «ارزیابی یک سیستم شناسایی اثرانگشت با استفاده از پارامترهای سیستم های دسته بندی و تطابق»، ص 1
- [2] «محل مذکور»
- [3]«همان مأخذ»، ص 1-2
- [4] مقاله «بررسی راهکارهای امنیت اطلاعات با استفاده از علم بیومتریک هوشمند»، سال 1391، ص 20-21
- [5] «محل مذکور»
- [6] مددی چلیچه، مجتبی؛ (1390)، «علم بیومتریک هوشمند و تشریح سیستم های قدرت گرفته از علم بیومتریک هوشمند»، ص 21
- [7] «همان مأخذ»، ص 21-22
- [8] «همان مأخذ»، ص 23-23
- [9] وکیل باغمیشه، محمدتقی؛ جعفری موسوی نیا. (1385)، «کلاس بندی اثرانگشت با استفاده از ترکیب روشهای ساختاری و شبکه های عصبی»، ص 1
- [10] «همان مأخذ»، ص 1-2
- [11] «اثرمذکور»، ص 11
- [12] «اثر مذکور»، ص 26-27
- [13] مقاله «بررسی راهکارهای امنیت اطلاعات با استفاده از علم بیومتریک هوشمند»، سال 1391، ص 86-87

فهرست وب سایت ها

www.wikipedia.org

www.matlabonline.com

www.aisthinktank.com

www.traceability.blogsky.com

www.mehdighadamgahi.blogfa.com

www.amir-taghizade.persian.ir