دانشکده‌ی علوم ریاضی

گروه علوم کامپیوتر

پایان‌نامه

جهت دریافت درجه‌ی کارشناسی ارشد در رشته‌ی مهندسی کامپیوتر گرایش هوش مصنوعی

موضوع

ساخت کلید رمزنگاری بر مبنای تئوری فازی با استفاده از ویژگی‌های آماری نمونه‌های بیومتریک

استاد راهنما

دکتر محمدرضا فیضی درخشی

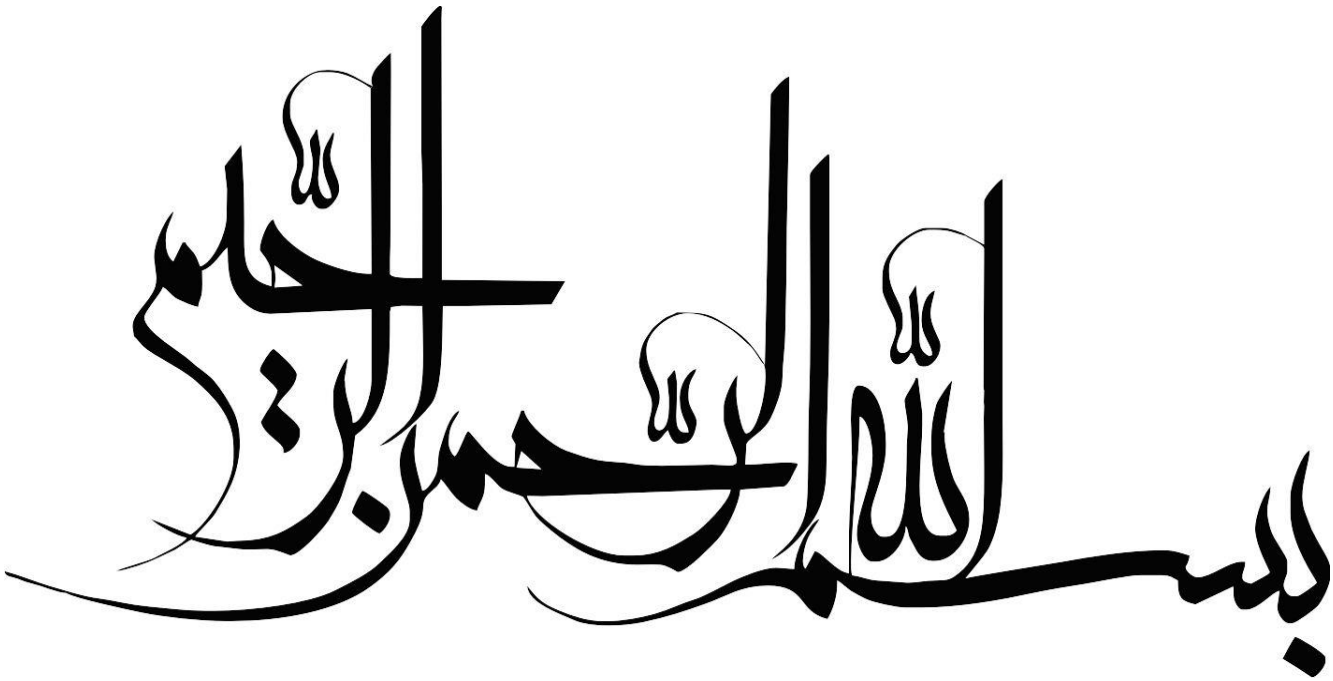
استاد مشاور

دکتر محمد شهریاری

پژوهشگر

سعید حیدرزاده جزی

شهریور ۱۳۹۲


بسم الله الرحمن الرحيم

نام خانوادگی : حیدرزاده جزی **نام**: سعید

عنوان پایان‌نامه: ساخت کلید رمزنگاری بر مبنای تئوری فازی با استفاده از ویژگی‌های آماری نمونه‌های بیومتریک

استاد راهنما: دکتر محمدرضا فیضی درخشی **استاد مشاور: دکتر محمد شهریاری**

مقطع تحصیلی: کارشناسی ارشد **رشته**: علوم کامپیوتر

دانشگاه: تبریز **دانشکده**: علوم ریاضی

تاریخ فارغ التحصیلی: شهریور ۱۳۹۲ **تعداد صفحه**: ٦٦

واژه‌های کلیدی: بیومتریک، کلید رمزنگاری، تشخیص عنبیّه، بیومتریک نویزی

چکیده

در سامانه‌های امنیتی برای ساخت کلیدهای رمزنگاری متفاوت برای کاربران مختلف، عموماً از گذرواژه‌ای که کاربر انتخاب می‌کند، استفاده می‌شود. امّا معمولاً گذرواژه‌های کاربران ضعیف، کوتاه و قابل حدس هستند؛ از این رو کلید حاصله از چنین گذرواژه‌هایی نیز چندان قدرتمند نخواهد بود. از سوی دیگر امکان دارد این گذرواژه‌ها فراموش شوند و یا لو بروند. روش دیگر برای ساخت کلیدهای رمزنگاری مختلف تولید گذرواژه‌هایی طویل و قوی به روش‌های خودکار می‌باشد؛ امّا کاربران نمی‌توانند چنین گذرواژه‌هایی را به یاد بسپارند و یادداشت کردن نیز مخاطرات امنیتی دارد. یکی از راه‌های پیشنهادی برای حلّ این مسئله این است که کلیدی قدرتمند را به روش‌های رمزنگارانه تولید کرد و آن را به صفت بیومتریکی از کاربر مقیّد ساخت. در این حالت کاربر تنها در حالتی می‌تواند به کلید دسترسی داشته باشد که صفت بیومتریک مورد استفاده بتواند کلید را از قید ایجاد شده برهاند. در این پایان‌نامه برای انقیاد کلید رمزنگاری به بیومتریک عنبیّه، سامانه‌ای بر مبنای طرح امانت فازی پیشنهاد شده است. این سامانه به گونه‌ای طراحی شده است که برای بیومتریک عنبیّه‌ی نویزی نیز مناسب باشد. نویز موجود در عنبیّه از منابع متعددّی از قبیل تکان خوردن سر، مسدود شدن با پلک‌ها و مژگان، بازتاب آینه‌وار ایجاد می‌شود. برای مقابله با هر یک از این اختلالات راهکاری پیشنهاد شده تا دقّت و کارایی قابل‌قبول به دست آید. با آزمایش سامانه‌ی پیشنهادی روی دادگان عنبیّه‌ی نویزی CASIA نه تنها به کلیدهای ۲٦۰ بیتی دست یافته بلکه دقّت و محرمانگی بیومتریک هم حفظ شده است. سامانه توانسته میزان پذیرش نادرست کاربران را به صفر برساند و برای هر نام نویسی به طور میانگین به ٤۰۳۳ بیت پایا دست یابد که افزایش محسوسی نسبت به کارهای پیشین دارد. میزان شکست در نام‌نویسی نیز به ۱/۹۳٪ کاهش یافته است.

فهرست

فهرست تصاویر

فصل ۱

مقدّمه

۱-۱ مقدّمه

با گسترش استفاده از فنّاوری اطّلاعات و ارتباطات، می‌توان از طریق سامانه‌های رایانه‌ای به بسیاری از منابع مالی و اطّلاعاتی دسترسی داشت. چون بسیاری از اطّلاعات موجود خصوصی و محرمانه است، باید دسترسی به آن‌ها را محدود و کنترل کرد. برای کنترل دسترسی به اطّلاعات می‌توان از روش‌های تأیید هویّت[1] بهره گرفت. یکی از امن‌ترین و در دسترس‌ترین روش‌ها برای تأیید هویّت استفاده از بیومتریک[2]ها است. امّا نمونه‌های بیومتریک هر فرد به‌ندرت دقیقاً یکسان است یعنی وجود تفاوت‌هایی اندک در نمونه‌های گوناگون هر فرد امری رایج است. از این رو نمی‌توان از آن‌ها در روش‌های مرسوم رمزنگاری، که بر اساس دانش دقیق پایه‌ریزی شده، بهره گرفت. برای حلّ این مشکل باید از روش‌های تصحیح خطای ویژه‌ای بهره جست؛ به‌گونه‌ای که اگر نمونه‌ی ارائه شده به نمونه‌ی اصلی نزدیک بود، هویّت فرد تأیید گردد.

یکی از مهمترین مؤلّفه‌های رمزنگاری، کلید رمزنگاری است. کلید رمزنگاری کاربران، که به منظور تأئید هویّت آنان به کار می‌رود، معمولاً از روی گذرواژه[3]هایی، که آنها انتخاب می‌کنند، به

[1] authentication
[2] biometric
[3] password

دست می‌آید. امّا گذرواژه‌ها مشکلات متعدّدی به بار می‌آورند که یکی از راه‌های حلّ این مشکل استفاده از بیومتریک‌ها برای ساخت کلید رمزنگاری است. روش‌های گوناگونی برای تولید کلید از روی بیومتریک‌های مختلف وجود دارد که هر یک مزایا و امنیّت خاصّ خود را ارائه می‌دهند.

۱-۲ بیان مسئله و اهداف پایان‌نامه

مسئله‌ی مورد بحث این پایان‌نامه انقیاد[1] کلید رمزنگاری به داده‌ی بیومتریک است. انقیاد کلید به بیومتریک مسائل خاصّ خود را دارد؛ مسائلی مانند تصحیح خطا[2]ی ذاتی بیومتریک، کمّی‌سازی[3] مقادیر بیومتریک، حفظ محرمانگی[4] کاربر، قابلیّت فسخ[5] کلیدهای حاصله، امنیّت حاصله و . . . . در این پایان‌نامه سامانه‌ای را برای انقیاد کلید رمزنگاری به داده‌ی بیومتیک عنبیّه ارائه خواهیم داد. سامانه‌ی پیشنهادی قابلیّت کار با داده‌های نویزی را داشته و می‌تواند وجود نویز در عنبیّه را اداره نماید. دو مسئله‌ی حائز اهمّیّت برای این سامانه طول کلید تولیدی و همچنین مسئله‌ی امنیّت سامانه‌ی خواهد بود که در جای خود بررسی خواهد شد.

۱-۳ ساختار پایان‌نامه

فصل دوم به آشنایی با مفاهیم اوّلیّه اختصاص دارد. ابتدا مفاهیم پایه‌ای رمزنگاری، مانند کلید رمزنگاری و الگوریتم رمزنگاری ارائه می‌شود. سپس انواع رمزنگاری از نظر نوع کلید، یعنی متقارن و نامتقارن معرفی می‌گردد و نشان داده می‌شود که مهمترین عامل ایجاد امنیت، کلید است. ادامه‌ی فصل، بیومتریک یا همان صفات مشخّصه‌ی رفتاری و زیستی فرد را معرّفی می‌کند. خواهیم دید

[1] binding
[2] error correction
[3] quantization
[4] privacy
[5] revocability

سامانه‌ی بیومتریک سامانه‌ای برای تشخیص افراد با استفاده از صفات بیومتریک است. این فصل توضیح مختصری از انواع بیومتریک را در بر خواهد داشت.

در فصل سوم سامانه‌ی پیشنهادی ارائه شده و کلیّات آن مطرح می‌گردد. ابتدا با اساس سامانه آشنا شده و سپس به ترتیب مراحل نام‌نویسی و وارسی شرح داده خواهد شد.

در شرح مرحله‌ی وارسی روش‌های پیشنهادی مقابله با نویز عنبیّه، روش پایایی‌سنجی و کدکردن کلید با روش کدینگ BCH آورده خواهد شد. در انتها نیز سامانه‌ی پیشنهادی ارزیابی می‌گردد. این ارزیابی شامل مقایسه‌ی آن با سامانه‌های مشابه موجود و همچنین ارزیابی امنیّت خواهد بود. در ارزیابی با روشی غیر صوری امنیّت سامانه را نشان داده و خواهیم دید کلید حاصله می‌تواند در کاربردهای معمول رمزنگاری به کار رود.

در فصل چهارم نتیجه‌گیری از مطالب ارائه شده انجام می‌گیرد. بررسی ویژگی‌های سامانه‌ی پیشنهادی انجام شده و برتری‌ها و کاستی‌های آن ذکر می‌گردد. در بخش بعدی این فصل نیز به کارهای آینده پرداخته و زمینه‌های پیش‌رو برای ادامه‌ی کار را خواهیم دید.

فصل ۲

مفاهیم پایه و روش‌های پیشین

۲-۱ مقدمه

در این فصل به مفاهیم پایه‌ای مورد نیاز برای درک بهتر مطالب می‌پردازیم. مفاهیم این فصل حول دو موضوع کلّیِ رمزنگاری و بیومتریک خواهد بود. ابتدا با مفاهیم رمزنگاری آشنا شده امّا بیشتر روی آشنایی با کلید رمزنگاری تمرکز می‌کنیم. سپس بیومتریک را معرّفی می‌کنیم و با انواع آن آشنا خواهیم شد. در پایان نیز جمع‌بندی مطالب را ارائه می‌کنیم.

۲-۲ رمزنگاری

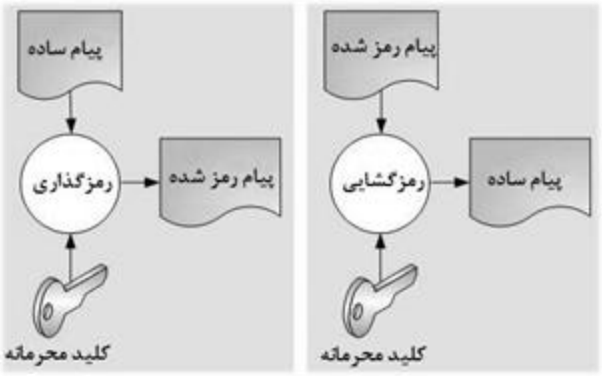
رمزنگاری دانش تغییر دادن پیام یا اطّلاعات است به گونه‌ای که این پیام یا اطّلاعات را تنها فرد مجاز بتواند بخواند و از دید سایرین ناخوانا باشد. برای نمونه تکه پیام رمزشده‌ی شکل ۲-۱، موسوم به مردان رقصان، برای کسی که از نحوه‌ی کد شدن پیام ناآگاه باشد ناخوانا و حتّی بی‌معنی می‌نماید.

شکل ۲-۱ تکه پیام رمز شده (به معنای Biometric Key) با مردان رقصان [8]

در رمزنگاری برای پنهان‌سازی اطّلاعات، پیام یا متن ساده را با استفاده از الگوریتمی به نام الگوریتم رمزگذاری[1] به صورت پیام رمزشده[2] درآورده و برای بازخوانی اطّلاعات از متن رمز شده

[1] encryption algorithm
[2] cipher text

هم الگوریتمی به نام رمزگشایی[1] به کار می‌رود. این الگوریتم‌ها معمولاً ثابت، عمومی و شناخته شده هستند و آن‌چه ایجاد امنیّت و محرمانگی می‌کند عاملی است که در این الگوریتم‌ها به کار رفته و باید محرمانه نگه داشته شود. این عامل چیزی جز کلید رمزنگاری نیست [25]. این اصل، که آن را «اصل کِرکهُف[2]» می‌نامند، می‌گوید: «تنها محرمانگی کلید است که امنیت ایجاد می‌کند.» در تعریف دقیق (مطابق با استاندارد ISO/IEC 10116:2006) کلید را دنباله‌ای از نشانه‌ها که عملیات تبدیل رمزنگارانه (رمزگذاری و رمزگشایی) را کنترل می‌کند، تعریف کرده‌اند. معمولاً محافظت از کلید آسان‌تر از الگوریتم رمزنگاری است و اگر لو رفت نیز، تغییر دادن آن آسان‌تر است. از این رو در طرح رمزنگاری خوش‌ساخت[3]، امنیّت طرح تنها به امنیّت کلیدهای مورد استفاده بستگی دارد. در شکل ۲-۲ شمایی کلّی از عملیات رمزگذاری و رمزگشایی می‌بینید.

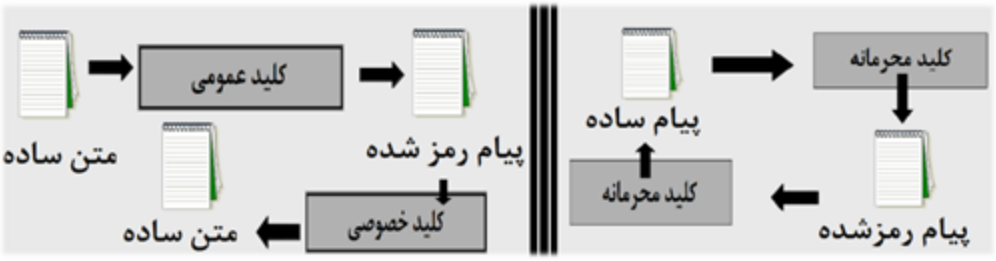


شکل ۲-۲ طرح کلّی عملیّات رمزنگاری و رمزگشایی

کلیدهای مورد استفاده برای رمزگذاری و رمزگشایی می‌توانند یکسان و یا متفاوت باشند. اگر کلیدها یکسان باشد، رمزنگاری را متقارن[4] می‌گویند و در غیر این صورت رمزنگاری را غیر متقارن[5] گویند. رمزنگاری غیر متقارن را رمزنگاری کلید عمومی نیز گویند. زیرا کلید رمزگذاری عمومی است

[1] decryption algorithm
[2] Kerkhoff's principle
[3] well designed
[4] symmetric
[5] asymmetric

یعنی هر شخصی می‌تواند اطّلاعات را رمزگذاری کند، امّا کلید رمزگشایی خصوصی می‌ماند. در شکل ۲-۳ طرح کلّی این دو روش را می‌بینید.



شکل ۲-۳ رمزنگاری متقارن (سمت راست) و رمزنگاری کلید عمومی (سمت چپ)

۲-۳ بیومتریک

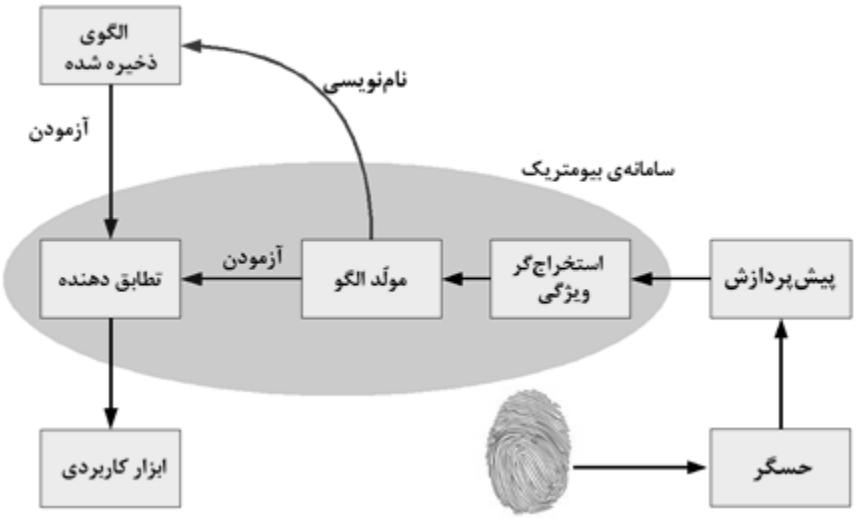
افراد عموماً از ویژگی‌های جسمی مانند چهره، صدا و راه رفتن، همراه با اطّلاعات وابسته‌ی دیگر (مانند مکان و لباس) برای تشخیص فردی دیگر استفاده می‌کنند [12]. تشخیص خودکار شخص بر اساس صفات مشخّصه‌ی رفتاری[1] یا زیستی[2] او را به نام تشخیص بیومتریک یا دانش بیومتریک می‌شناسند (مطابق با استاندارد ISO/IEC JTC1 SC37). به‌صورت دقیق و علمی، هر ویژگی زیستی یا رفتاریِ منحصربه‌فرد و متمایز کننده، پایا و سنجش‌پذیر را که بتواند برای تعیین و یا تأیید هویّت به‌کار رود، بیومتریک گویند.

۲-۳-۱ سامانه‌ی بیومتریک

سامانه‌ی بیومتریک، سامانه‌ی تشخیص الگو[3]یی است که فرد را بر اساس ویژگی‌های زیستی یا رفتاریش بازشناسی می‌کند. همان‌طور که در شکل ۲-٤ می‌بینیم، این سامانه معمولاً دارای حسگری یا حسگرهایی است که مسئول دریافت داده‌ی خام از نمونه‌ی بیومتریک است. این اطّلاعات خام در

[1] behavioural
[2] physiological
[3] template

مرحله‌ی پیش‌پردازش، تصفیه و آماده‌ی استفاده می‌گردد. عمل تصفیه معمولاً شامل حذف نویز و همچنین آماده‌سازی داده‌ی بیومتریک برای استخراج اطّلاعات است.



شکل ۲-٤ نحوه‌ی کار سامانه‌ی بیومتریک

در مرحله‌ی بعد، بسته به نوع بیومتریک، ویژگی‌هایی از اطّلاعات آماده شده استخراج شده و بردار مقدار کمّی آن‌ها به مولّد الگو داده می‌شود. اگر سامانه در مرحله‌ی نام‌نویسی باشد، الگویی از روی این مقادیر تولید شده و در پایگاه داده ذخیره می‌گردد؛ و اگر در مرحله‌ی تأئید هویّت باشد، الگوی تولیدی با الگویی که از قبل ذخیره شده مقایسه می‌گردد و نتیجه‌ی مقایسه به ابزار کاربردی فرستاده می‌شود.

برای کاربردهای گوناگون، صفات مشخّصه‌ی بیومتریک گوناگونی هم وجود دارد که هر یک برتری‌ها و کاستی‌هایی دارد؛ از این رو انتخاب بیومتریک وابسته به نوع کاربرد است. از این گذشته برای استفاده از این صفات مشخّصه باید تعیین کرد که برای کاربرد موردنظر، کدام مناسب‌ترند و چگونه باید از ویژگی‌های این صفات مشخّصه بهره گرفت. از آن‌جایی که هر بیومتریک را با دستگاه خاصّی اندازه‌گیری می‌کنند، فرایند تطابق تأیید هویّت بیومتریک باید بر اساس ویژگی‌های آن

بیومتریک تنظیم گردد. در طول سالیان متمادی صفات مشخّصه‌ی متعدّدی به دست آمده که می‌توان آن‌ها را در دو دسته‌ی زیر جای داد:

- صفات مشخّصه‌ی زیستی (ایستا): ویژگی‌های طبیعیِ جسمی انسان مانند اثر انگشت، چهره، ساختار کف دست یا عنبیّه. این صفات مشخّصه به سختی تأثیر می‌پذیرند و با گذر زمان معمولاً ثابت می‌مانند. تغییر در آن‌ها تحت شرایط ویژه میسّر است؛ مثلاً جراحت می‌تواند ساختار کف دست را تغییر دهد. برخی از بیومتریک‌های زیستی را در شکل ۲-۵ می‌بینید.

شکل ۲-۵ برخی از بیومتریک‌های زیستی (عنبیّه، چهره، اثر انگشت و کف دست)

- صفات مشخّصه‌ی رفتاری (ناایستا): صفات مشخّصه‌ای که مربوط به رفتار شخص و چگونگی انجام کارها است مانند امضاء، صدا یا پویایی شناسی فشردن کلید[1]. این ویژگی‌ها معمولاً با گذر زمان به‌کندی تغییر می‌کنند مثلاً امضای شخص ممکن است با گذر سال‌ها تغییر کند. اکتساب بیومتریک در این دسته به این نیاز دارد که کاربر فعّال باشد یعنی کاری را در جلوی حسگر انجام دهد. سه گونه از بیومتریک‌های رفتاری را در شکل ۲-٦ نشان داده‌ایم.

[1] keystroke dynamics

شکل ۲-٦ برخی از بیومتریک‌های رفتاری (کلیدزنی، امضا و صوت)

در ادامه خواصّ برخی از صفات مشخّصه‌ی زیستی و رفتاری را مختصراً بررسی می‌کنیم. سپس راه‌هایی را که این صفات مشخّصه به‌دست می‌آید و ویژگی‌هایی را که می‌توان از این صفات مشخّصه استخراج کرد، شرح می‌دهیم.

۲-۳-۲ تشخیص اثر انگشت

الگوی خطوط سر انگشتان یکتا و پابرجاست و از این رو می‌توان آن‌ها را نشانه‌ای برای تشخیص هویّت فرد در نظر گرفت. در واقع حتّی می‌توان هویّت دوقلوها را هم بر اساس اثر انگشتشان از هم تمیز داد. اثر انگشت خصیصه‌ای است که بیش از صد سال است از آن استفاده می‌شود. سامانه‌های بیومتریک مبتنی بر اثر انگشت بسیار رایج و موفّق هستند و در نظر عموم معادل مفهوم تشخیص بیومتریک شده است. در سامانه‌های تأیید هویّت اثر انگشت، اکثراً ویژگی‌های مبتنی بر ریزه‌کاری سایشی[1] به کار می‌روند؛ امّا سامانه‌های اندکی نیز طرّاحی شده‌اند که از کلّ تصویر اثر انگشت استفاده می‌کنند. از این رو خروجی و نتیجه‌ی معمول داده‌خوانی سامانه‌ی تائید هویّت اثر انگشت (اسکن)، مجموعه‌ای از نقاط ریزه‌کاری خواهد بود. اصطلاح ریزه‌کاری همان اثر برآمدگی پوست انگشتان است. این نقاط ریزه‌کاری به عنوان ویژگی‌های بیومتریک به کار می‌رود و در طیّ فرایند تطابق با بقیه مقایسه می‌گردد. برخی از ریزه‌کاری‌های اثر انگشت را می‌توان در شکل ۲-۷ دید.

[1] friction minutiae-based features

شکل ۲-۷ ریزه‌کاری‌های اثر انگشت

مشکل اصلی بیومتریک اثر انگشت این موضوع است که داده‌ی اثر انگشت را باید به نوعی نرمال کرد؛ مثلاً با پیدا کردن راستای ویژه‌ی اثر انگشت و مرکز آن. اگر داده‌ی اثر انگشت نرمال شده نباشد، آن‌گاه تمامی محاسباتی که حاصل از ریزه‌کاری‌هاست، وابسته به مکان یا راستا خواهد بود. راه حلّ این مشکل این است که الگوریتم تطابقی داشته باشیم که به تغییر شکل داده‌ی اثر انگشت رسیدگی کند. کارهای بسیاری برای تراز کردن[1] تصاویر اثر انگشت صورت گرفته که شامل استفاده از نقاط با انحنای بالا و خطوط راستا می‌شود. چالش دیگر سروکار داشتن با عکس‌های کیفیت پایین اثر انگشتی است که در بدترین حالت ویژگی‌های مجزّای (نقاط ریزه‌کاری) لازم را برای فرایند تطابق ندارد. دادن این توانایی به سامانه‌ای برای تأیید هویّت شخص حتّی اگر تنها زیرمجموعه‌ای از داده‌ها را هنگام داده‌خوانی اثر انگشت به‌دست آورده باشد، هنوز هم موضوعی است که جا برای پژوهش‌های بیشتر دارد.

۲-۳-۳ تشخیص عنبیّه

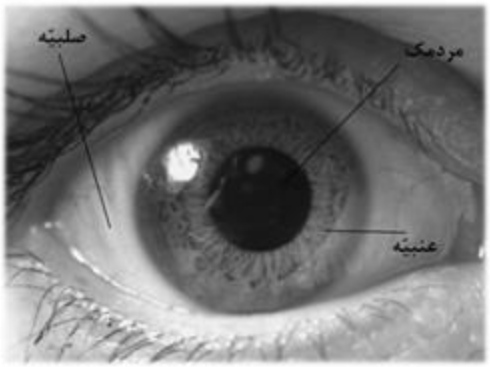
صفت مشخّصه‌ی زیستی دیگر عنبیّه، یا همان ماهیچه‌ی درون چشم برای تنظیم اندازه‌ی مردمک، است. از آن‌جایی که عنبیّه عضو درونیِ محافظت شده‌ای است که بافت و الگوی تصادفی آن، در

[1] aligning

طول عمر بسیار پایدار است، می‌توان آن را به عنوان گذرنامه‌ای زنده یا گذرواژه‌ای که نیاز به یادآوری ندارد و همیشه حاضر است، به‌کار برد. از آن‌جایی که دریافت داده‌های عنبیّه‌ی فرد با استفاده از دوربینی ویژه (اسکنر عنبیّه) انجام می‌گیرد، یکی از کاستی‌های استفاده از عنبیّه برای تأئید هویّت این است که اشخاص باید کاملاً با سامانه کنار آمده و همکاری کنند.

کار اصلی و راهگشای لازم برای ساخت الگوریتم تشخیص عنبیّه را، که برای به دست آوردن تصویر و تطابق نیاز است، داوگمن [4] انجام داد. الگوریتم داوْگمَن اساس کار تمامی سامانه‌های تشخیص عنبیّه‌ی امروزی است. الگوریتم پالایش اطّلاعات چندین گام دارد که می‌توان آن‌ها را این چنین خلاصه کرد: نخست آن‌که باید عنبیّه را از میان کلّ تصویر چشم جدا کرد. برای این کار باید مرکز عنبیّه و مرزهای درونی و بیرونی آن را تعیین کرد. به دلیل اندازه‌ی پویا و متغیّر مردمک و گشادی پلک این تشخیص عنبیّه باید به دقت انجام گیرد. برای حل این مشکل داوْگمَن روشی به نام گسترش دوایر را پیشنهاد کرد. ایده‌ی اصلی این راهکار وجود تغییرات شدید در درخشندگی تصاویر روی مرزهاست که می‌توان آن‌ها را با انتگرال دایره‌ای[1] تشخیص داد. در ابتدا، مرکز اوّلیّه‌ای از مردمک را تخمین زده و سپس انتگرال دایره‌ای را محاسبه می‌کنند. انحراف معیار این انتگرال در مرزها، که درخشندگی شدیداً تغییر می‌کند، زیاد است. با به کار بردن این روش برای برآورد مرکز، شعاع مرزهای میان مردمک و عنبیّه و میان عنبیّه و صلبیّه[2] (سفیده‌ی سخت چشم) محاسبه می‌گردد. در شکل ۲-۸ این مرزها مشخّص شده‌اند. سپس این شعاع‌ها را برای محاسبه‌ی مرکز بعدی مردمک به کار برده و کلّ روش تا هنگامی که به همگرایی برسد، ادامه می‌یابد.

[1] circular integral
[2] sclera



شکل ۲-۸ جایگاه عنبیّه در چشم

گام بعدی که تحلیل دسته‌ها نام دارد، برای عنبیّه‌ی استخراج شده (شکل حلقه‌وار) تعریف شده است. این دسته‌ها برای جای دادن نقاطی که بعداً فیلترهای گابور[1] دو بعدی پیدا می‌کنند، استفاده می‌شوند. این فیلترهای دو بعدی گابور برای حذف نویز از سیگنال حاصله طرّاحی شده و نباید این فرایند را با هموار کردن سیگنال[2] اشتباه گرفت [19]. حلقه‌ی عنبیّه با نگاشت مختصّات قطبی به مختصّات کارتِزیَن واپیچانده[3] شده و حاصل تصویری مستطیلی خواهد بود. در تصویر مستطیلی شعاع دسته‌های تحلیلی که قبلاً تعریف شده ثابت شده و هر نقطه‌ی پیدا شده یک مرکز از موجک[4] گابور دو بعدی است. برای این موجک ضرایب تعیین شده‌اند که از میان آن‌ها دو بیت پیدا شده است. این روش تا هنگامی که بیت‌های کافی پیدا شود، بار دیگر تکرار می‌شود. تصویر مستطیلی عنبیّه اساساً شامل بخش‌هایی از پلک و مژگان است. مژگان را به عنوان نویز که باید هنگام واپیچانی عنبیّه تشخیص داد، در نظر می‌گیرند. این کار با محاسبه‌ی پوشش بیتی[5] انجام می‌گیرد که در آن هر بیت نشانگر ناحیه‌ای از عنبیّه بوده و در صورت تشخیص هرگونه نویز برابر ۰ و در غیر این صورت برابر ۱ خواهد بود. انواع دیگری از نویز هم، مانند نویز پیکسل دوربین، شاید وجود داشته باشد. نتیجه‌ی کلّی این فرایند را کد عنبیّه می‌خوانند (که مثلاً در روش داوْگمَن رشته‌ای ۲۰۴۸ بیتی است).

[1] Gabor filter
[2] signal smoothing
[3] unwrapped
[4] wavelet
[5] mask-bit