نشریه علمی «نوآوری‌های فناوری اطلاعات و ارتباطات کاربردی»
سال اول، شماره ۲، تابستان ۱۴۰۰؛ ص ۵۰- ۳۵

علمی – تخصصی

بهبود احراز هویت مبتنی بر عنبیه چشم با ارائه معماری شبکه حسگر بیسیم با هدف حفظ حریم شخصی در اینترنت اشیاء صنعتی

کیوان برنا[1*]، امید مهدی عبادتی[2]، شایان زینلی[3]

۱- استادیار دانشکده علوم ریاضی و کامپیوتر، دانشگاه خوارزمی، ۲- استادیار دانشکده مدیریت دانشگاه خوارزمی

۳- دانش‌آموخته کارشناسی ارشد دانشکده مدیریت، دانشگاه خوارزمی

(دریافت: ۱۴۰۰/۰۴/۰۲، پذیرش: ۱۴۰۰/۰۶/۰۱)

چکیده

اینترنت اشیاء صنعتی امکان دسترسی سریع به اطلاعات درباره جهان فیزیک و اشیاء درون آن را فراهم می‌کند که منجر به خدمات جدید و افزایش کارایی و بهره‌وری می‌شود مخصوصاً در محیط‌های صنعتی و نظامی. شبکه حسگر بیسیم زیرساخت شبکه‌ای مهمی در اینترنت اشیاء به شمار می‌رود و تائید هویت کاربر برای تائید اعتبار کاربر برای WSNها، به‌عنوان ساز و کار امنیت پایه‌ای مورداستفاده قرار می‌گیرد. در این مقاله سعی بر آن است برای بهبود امنیت احراز هویت ارائه‌شده با استفاده از پردازش تصویر روشی جدید ارائه گردد. تجزیه‌وتحلیل توسط نرم‌افزار متلب انجام گرفته است. نتایج ارائه‌شده در این مقاله که شامل هفت مرحله است در شناسایی مردمک دارای درصد تشخیص صحیح ۹۳٪ می‌باشد. این هفت مرحله به ترتیب عبارتند از: ۱. کاهش نویز، ۲. یافتن مرز خارجی مردمک، ۳. جداسازی مژه‌ها، ۴. پیدا کردن مرز پلک‌ها، ۵. یافتن مرز خارجی عنبیه، ۶. جداسازی محدوده‌ی عنبیه، ۷. استخراج ویژگی و رمزگذاری پیکسل‌ها به روش رمزنگاری خم‌های بیضوی. با اندازه‌گیری‌ها و آزمایشات انجام‌شده مشخص گردید که روش پیشنهادی در شناسایی مرز پلک به روش معادله درجه دوم نسبت به معادله درجه سوم و روش تبدیل‌هاف سهمی از نظر زمانی بهینه و سریعتر می‌باشد. جهت استخراج ویژگی پارامترهای موثر در الگوریتم استخراج ویژگی سیفت موردبررسی و اندازه‌گیری قرار داده‌شده و پارامترهای بهینه انتخاب گردیدند. بدین‌صورت که پارامتر سیگما با مقدار ۲,۵ و پارامتر اکتاو با مقدار ۴ به‌عنوان بهترین مقادیر در نظر گرفته شوند. همچنین به‌منظور بررسی مقاومت روش پیشنهادی نسبت به عوامل ایجاد خطا مثل زاویه، روشنایی و مقیاس، روش پیشنهادی مورد آزمایش قرار گرفت و ثابت گردید که روش مذکور دارای مقاومت مناسب جهت تشخیص در شرایط مختلف می‌باشد.

کلید واژه‌ها: احراز هویت، شبکه حسگر بیسیم، حریم شخصی، اینترنت اشیاء صنعتی، پردازش تصویر

۱- مقدمه

امروزه، امنیت در هر سامانه که داده‌ها را ذخیره می‌کند بسیار مهم است؛ بنابراین آماده‌سازی امنیت مؤثر و قدرتمند یکی از عوامل مهم در هر سامانه می‌باشد. در سال‌های اخیر، دستگاه‌های محاسبات کوچک مانند تلفن همراه، دستیاران دیجیتال شخصی (PDA) سامانه‌های جاسازی‌شده، حسگرها و کارت‌های هوشمند نقش کلیدی در زندگی بشر به‌دست آورده‌اند و آن‌ها را به یک جزء جدایی‌ناپذیر از جهان مدرن تبدیل کرده است. این دستگاه‌ها به شدت در قدرت محاسباتی، حافظه و عمر باتری منابع محاسباتی، محدود هستند. چنین محدودیت‌هایی می‌تواند دستگاه‌ها را در برابر بسیاری از حملات امنیتی آسیب‌پذیر کند و نقص امنیتی را به وجود آورد. علاوه بر این، قابل‌اطمینان بودن خدمات و قابلیت اطمینان از فن‌آوری‌ها هنگامی‌که با اطلاعات حساس در ارتباط هستند نگرانی‌هایی را به وجود می‌آورد. کارت‌های هوشمند یکی از ابزارهایی است که برای امنیت بسیار مورداستفاده قرار می‌گیرد [۱ و ۲].

اینترنت اشیاء صنعتی[1] یا به اختصار IIoT امکان دسترسی سریع به اطلاعات درباره جهان فیزیک و اشیاء درون آن منجر به خدمات جدید و افزایش کارایی و بهره‌وری می‌شود، مخصوصاً در محیط‌های صنعتی و نظامی [۳]. محیط IoT یک محیط مقید است؛ زیرا اشیاء دارای محدودیت‌هایی مانند قدرت پردازش، مقدار حافظه محدود و مصرف انرژی کم می‌باشند [۴ و ۵]. شبکه

* رایانامه نویسنده مسئول: borna@khu.ac.ir

[1] Industrial Internet of Things

حسگر بیسیم (WSN)، زیرساخت شبکه‌ای مهمی در اینترنت اشیاء (IIoT) به شمار می‌رود و می‌توان آن را به‌طور گسترده‌ای در بسیاری از زمینه‌های صنعتی با ترکیب فناوری محاسبات ابری [۶] برای جمع‌آوری داده‌ها برای کارکردهایی مانند نظارت و مدیریت فرآیند صنعتی، نظارت بر صحت کارکرد ماشین و تشخیص خطا به‌کار گرفت [۷]. چگونگی شناسایی اعتبار هویت کاربران چالش کلیدی برای امنیت IIoT یا WSN به شمار می‌رود. علاوه بر مدیریت کلیدی، تائید هویت کاربر برای تائید اعتبار کاربر برای WSNها، به‌عنوان ساز و کار امنیت پایه‌ای مورداستفاده قرار می‌گیرد [۸]. محققان بسیاری پروتکل‌های تائید هویت کاربر را برای WSNها پیشنهاد کرده‌اند. استاندارد عمومی استانداردی است که کاربر، درگاه و حسگر باید احراز هویت متقابل را دریافت کنند. کاربر می‌تواند ارتباط را با ارسال یک پیام ورود به درگاه آغاز کند [۹] و سپس درگاه ارتباطی با حسگر خاص برای جمع‌آوری اطلاعات درخواست شده توسط کاربر برقرار می‌شود. در انتها کاربر پیام را از درگاه دریافت می‌کند. بااین‌حال، WSN به‌دلیل ویژگی باز بودن کانال بیسیم از حملات مخرب اشباع می‌شود. علاوه بر این، محدودیت منابع گره‌های حسگر باعث می‌شود که الگوریتم‌های رمزنگاری کلیدی عمومی مانند RSA برای محیط WSN مناسب نباشند [۱۰]. این الگوریتم در کنار الگوریتم رمزنگاری منحنی بیضوی ECC از شناخته‌شده‌ترین الگوریتم‌های رمزنگاری می‌باشد و به علت اینکه RSA در اینجا مناسب نمی‌باشد از الگوریتم ECC بهره می‌گیریم. رمزنگاری منحنی بیضی (ECC) یک روش رمزگذاری مبتنی بر نظریه منحنی بیضوی است که می‌تواند برای ایجاد سریع‌تر، کوچک‌تر و کارآمدتر کلیدهای رمزنگاری استفاده شود. ECC از طریق خواص معادله منحنی بیضوی به‌جای روش تولید سنتی به‌عنوان محصول اعداد اول بسیار بزرگ تولید می‌کند. این فنّاوری را می‌توان در ارتباط با بیشتر روش‌های رمزنگاری کلید عمومی مانند RSA و Diffie-Hellman استفاده کرد. به گفته برخی از محققان، ECC می‌تواند سطح امنیت را با یک کلید ۱۶۳ بیتی تولید کند که سایر سامانه‌ها نیاز به کلید ۱،۰۲۴ بیتی برای دستیابی به آن دارند. ازآنجاکه ECC به ایجاد امنیت معادل با استفاده از توان کم محاسبات و باتری کمک می‌کند، به‌طور گسترده‌ای برای برنامه‌های تلفن همراه مورداستفاده قرار می‌گیرد. در [۱۲] نویسندگان به مسأله به‌کارگیری شبکه‌های مبتنی بر نرم‌افزار جهت ارتقای امنیت در اینترنت اشیاء پرداختند.

در این مقاله قصد داریم برای بهبود امنیت احراز هویت ارائه‌شده با استفاده از الگوریتم ECC (که در رمزنگاری قوی عمل می‌کند) و الگوریتم‌های پردازش تصویر روشی جدید ارائه دهیم. برای بهبود عملکرد احراز هویت قصد داریم در این پژوهش شبیه‌سازی را با استفاده از شبیه‌ساز متلب انجام دهیم و الگوریتم کلی را بهینه کنیم، همچنین با استفاده از زبان برنامه‌نویسی PHP روندی دومرحله‌ای برای احراز هویت مبتنی بر رمز برای کاربر ایجادشده. پیش از این کارهای مشابه با نرم‌افزارهایی مانند NS3 شبیه‌سازی انجام داده‌اند و الگوریتم‌های دیگر مانند RSA و سایر محیط‌ها استفاده‌شده است که به نظر می‌رسد با این نوآوری نتیجه بهبودیافته در زمینه احراز هویت در محیط IoT حاصل شود.

نتایج ارائه‌شده در این مقاله شامل هفت *مرحله ذیل* است: ۱. کاهش نویز، ۲. یافتن مرز خارجی مردمک، ۳. جداسازی مژه‌ها، ۴. پیدا کردن مرز پلک‌ها، ۵. یافتن مرز خارجی عنبیه، ۶. جداسازی محدوده‌ی عنبیه، ۷. استراج ویژگی و رمزگذاری پیکسل‌ها به روش رمزنگاری خم‌های بیضوی. روش پیشنهادی در شناسایی مرز پلک به روش معادله درجه دوم نسبت به معادله درجه سوم و روش تبدیل‌هاف سهمی ازنظر زمانی بهینه و سریع‌تر می‌باشد و دارای درصد تشخیص صحیح ۹۳٪ می‌باشد. به‌منظور بررسی مقاومت روش پیشنهادی نسبت به عوامل ایجاد خطا مثل زاویه، روشنایی و مقیاس، روش پیشنهادی مورد آزمایش قرار گرفت و ثابت گردید که روش مذکور دارای مقاومت مناسب جهت تشخیص در شرایط مختلف می‌باشد.

ساختار این مقاله به شرح ذیل است: در بخش ۲ به بررسی روش تحقیق و مرور تاریخچه مسأله پرداخته می‌شود. بخش ۳ به مطالعه روش پیشنهادی طی هفت گام اختصاص یافته است. بخش ۴ به شبیه‌سازی روش پیشنهادی و ارزیابی کارایی آن می‌پردازد. نهایتاً در بخش ۵ به نتیجه‌گیری و کارهای آتی تخصیص‌یافته است.

۲- روش تحقیق

عنبیه مجموعه‌ای پیچیده از ماهیچه‌ها در جلوی چشم می‌باشد، که دیدن و اندازه‌گیری آن آسان می‌باشد و به‌وسیله قرنیه و پلک چشمان به‌شدت مورد محافظت قرار می‌گیرد و احتمال آسیب رسیدن به آن در طول عمر هر فرد بسیار پایین است. شاکله بافت عنبیه در طول عمر هر فرد قابل‌تغییر نبوده و پایدار تعریف شده است و میزان بالایی از توانمندی ساختاری و تقریباً وابستگی بسیار کمی به نوع ژن فرد را داراست. به همین دلیل می‌شود از

بافت عنبیه که منحصرا برای هر شخص است برای تشخیص شناسایی انسان‌ها استفاده کرد. اما مکان‌یابی، تشخیص و مستخرج کردن مشخصه‌های عنبیه در نوع خود چالشی بزرگ محسوب می‌شود.

۲-۱- مرور تاریخچه مسأله

در سال ۱۹۸۱ لمپورت [۱۳] اولین پروتکل احراز هویت را ارائه کرد که مبتنی بر توابع درهم‌ساز[1] هست، سرویس‌دهنده مقدار درهم‌سازی شده‌ی رمز عبور کاربران (تصدیق‌کننده‌ی هویت کاربران) را درون جدولی به نام جدول کاربران ذخیره می‌کند و هویت کاربران را بر اساس این مقادیر بررسی و احراز می‌کند. هرچند پروتکل لمپورت یک پروتکل بسیار ساده و سبک وزن است ولی محققین زیادی از جمله لنون و همکاران [۱۴] و همچنین ین و لیائو [۱۵] نشان داده‌اند که این پروتکل در مقابل حمله دزدیدن تصدیق‌کننده‌ی کاربران[2] آسیب‌پذیر است. این حمله بیانگر این موضوع است که یک دشمن با حمله و نفوذ به پایگاه داده سرویس‌دهنده می‌تواند به اطلاعات محرمانه تصدیق‌کننده‌ی کاربران دست یابد و از آن‌ها برای فریب دادن و جعل هویت کاربران و همچنین سرویس‌دهنده استفاده کند. علاوه بر این، هر یک از این محققین پروتکل‌های احراز هویت دیگری ارائه داده‌اند. درواقع این نوع پروتکل‌های احراز هویت که فقط بر اساس دانش کاربر (داشتن یک رمز عبور) هستند در دسته پروتکل‌های احراز هویت تک عاملی قرار می‌گیرند. در پروتکل‌های احراز هویت تک عاملی، سرویس‌دهنده مجبور به نگهداری تصدیق‌کننده‌ی هویت کاربران در پایگاه داده خود است تا بر اساس آن‌ها کاربران را احراز هویت کند؛ اما همان‌طور که گفته شد یک دشمن می‌تواند به پایگاه داده‌ی سرویس‌دهنده نفوذ کند و این اطلاعات را به‌دست آورد. از این رو، کارهای متعددی برای نگهداری تصدیق‌کننده‌ی کاربران به‌صورت امن و محافظت‌شده در پایگاه داده سرویس‌دهنده انجام‌شده است.

در سال ۲۰۰۴ کومار [۱۶] امنیت پروتکل احراز هویت بهبود یافته ارائه‌شده توسط چن و همکاران [۱۷] را تحلیل کردند و نشان دادند که این پروتکل نسبت به حمله نشست موازی[3] و همچنین حمله عامل خودی[4] آسیب‌پذیر است. سپس جهت افزایش امنیت، یک پروتکل احراز هویت جدید ارائه دادند. متاسفانه در همان سال یون و همکاران [۱۸] نشان دادند که پروتکل کومار [۱۶] نیز در مقابل حمله نشست موازی و حمله منع سرویس[5] آسیب‌پذیر است و برای غلبه بر این مشکلات یک پروتکل احراز هویت جدید ارائه کردند و ادعا کردند که پروتکل پیشنهادی‌شان در برابر حملات مختلف امنیتی امن و مقاوم است. بااین‌وجود در سال ۲۰۰۷ ونگ و همکاران [۱۹] امنیت پروتکل-های ارائه‌شده توسط کومار [۱۶] و یون و همکاران [۱۸] را تحلیل کردند و نشان دادند که این پروتکل‌ها نسبت به حملات جعل هویت، حدس رمز عبور به‌صورت برون خط[6] و منع سرویس[7] آسیب‌پذیر هستند. علاوه بر این، آن‌ها یک پروتکل احراز هویت جدید جهت بهبود امنیت پروتکل‌های قبلی ارائه کردند.

در سال ۲۰۱۱ آواسی و همکاران [۱۹] نیز یک پروتکل احراز هویت بهبودیافته ارائه کردند و ادعا کردند که پروتکل پیشنهادی‌شان در برابر حملات مختلف امنیتی امن هست. اما کوماری و همکاران [۲۱] نشان دادند که پروتکل احراز هویت ارائه‌شده توسط آواسی و همکاران [۲۰] نسبت به حمله حدس رمز عبور به‌صورت برون خط آسیب‌پذیر است و همچنین محرمانگی رو به جلو[8] را نیز فراهم نمی‌کند. علاوه بر این نشان دادند که در پروتکل ارائه‌شده توسط آواسی و همکاران کاربر و سرویس‌دهنده روی هیچ‌گونه کلیدی توافق نمی‌کنند، یعنی پروتکل آواسی و همکاران توافق کلید را فراهم نمی‌کند. سپس جهت غلبه بر این مشکلات، یک پروتکل احراز هویت و توافق کلید جدید ارائه دادند.

در سال ۲۰۱۳ چانگ و همکاران [۲۲] نشان دادند که پروتکل احراز هویت و توافق کلید ارائه‌شده توسط ونگ و همکاران [۱۹] نسبت به حمله منع سرویس آسیب‌پذیر است. آن‌ها همچنین ادعا کردند که ازآنجایی‌که این پروتکل شناسه کابر در تمام پیام‌های درخواست ورود کاربر ثابت و بدون تغییر است، فعالیت‌های کاربران در آن پروتکل قابل ردیابی است و درواقع این پروتکل غیرقابل ردیابی بودن[9] را فراهم نمی‌کند. چند سال بعد ژیناگ و همکارانش [۲۳] مورد بهبودیافته از [۲۲] را پیشنهاد دادند که البته بار محاسباتی نسبتا بالایی دارد. اخیرا، گوپ و همکاران [۲۴] پروتکل احراز هویت، سبکی را با ناشناس‌سازی کاربر برای شبکه‌های حسگر بیسیم استفاده کردند که در واقع تطابقی بین امنیت و بازدهی است بدین معنا که یک پروتکل دوعاملی رمزگشایی را برای این شبکه‌ها طراحی‌شده است.

[1] Hash functions
[2] Stolen verifier attack
[3] Parallel session attack
[4] Insider attack
[5] Denial-of-Service attack
[6] Off-line password guessing attack
[7] Denial of Service attack
[8] Perfect forward secrecy
[9] Untraceability

در همین راستا در این مقاله قصد داریم برای بهبود امنیت احراز هویت ارائه‌شده با استفاده از الگوریتم ECC که در رمز نگاری نسبت به RSA مزایایی را از جهات طول کلید و پردازش‌ها و فضای ذخیره‌سازی فراهم می‌سازد، روشی جدید ارائه دهیم. درواقع از مزایای الگوریتم RSA که کارایی زیادی در رمزنگاری نامتقارن دارد در کنار ECC استفاده می‌کنیم. بخصوص در مواردی که اندازه پیام ها متوسط و طرف رمزنگاری قدرت محاسباتی محدودی دارد یا رمزگشایی به ندرت رخ می‌دهد سبب بهبود نتایج در زمینه احراز هویت در محیط IoT می‌شود. قصد داریم با استفاده از الگوریتم ECC و مشخصات بیومتریک تعدادی نمونه به شبیه‌سازی با نرم‌افزار متلب بپردازیم. برگ خریدهای مؤثر در بهبود امنیت در پژوهش حاضر مواردی مانند تشخیص ورود اشتباه رمز عبور، مقاومت در برابر حمله و تائید هویت کاربر می‌باشد.

۳- روش پیشنهادی

روش پیشنهادی پژوهش حاضر شامل ۷ مرحله می‌باشد که پس از دریافت تصویر ورودی به شرح مندرج در شکل (۱) باید اعمال گردند:

۱. کاهش نویز،

۲. یافتن مرز خارجی مردمک،

۳. جدا سازی مژه‌ها،

۴. پیدا کردن مرز پلک‌ها،

۵. یافتن مرز خارجی عنبیه،

۶. جداسازی محدوده‌ی عنبیه،

۷. استخراج ویژگی و رمزگذاری پیکسل‌ها به روش ECC.

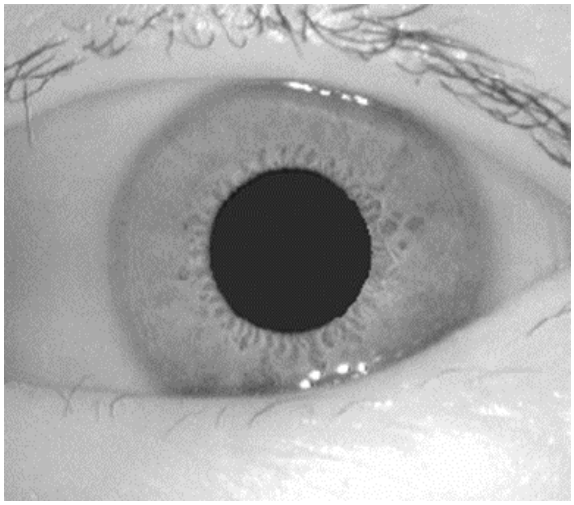
شکل (۱): مراحل هفت‌گانه روش پیشنهادی

از همین رو در ادامه به تشریح مراحل روش پیشنهادی پژوهش حاضر پرداخته خواهد شد.

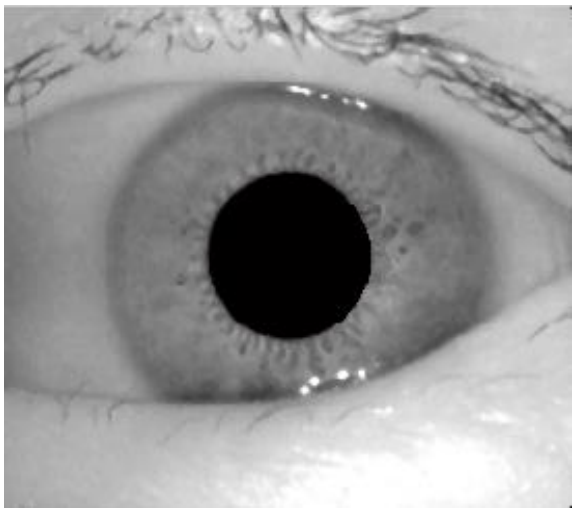
۳-۱- کاهش نویز

به‌طورکلی در مسائلی همچون یافتن لبه‌های یک تصویر، نویز موجب تخریب لبه‌ها خواهد شد و باعث می‌شود که لبه‌ها به‌صورت دقیق و شفاف تشخیص داده نشوند. لذا با توجه به شکل‌های (۲ و ۳) جهت کاهش نویز در تصاویر ورودی اول کانال‌های RGB تصاویر از یکدیگر جدا خواهند شد. پس از آن فیلتر میانه باهدف کاهش نویزهای احتمال داده شده‌اند، مورداستفاده قرارگرفته است. فیلتر میانه یک نوع فیلتر آماری است و به‌صورت معمول از یک طرح مرکز نقطه مناسب مورد ارزیابی و محاسبه قرار می‌گیرد. طرح مدنظر درروش پیشنهادی پژوهش حاضر ۳×۳ می‌باشد. لذا نیازمند پردازش ۹ پیکسل در طرحی مرکزی با مختصات (x,y) می‌باشد.

پس از اعمال فیلتر وسطی بر روی هریک از کانال‌های RGB و پس از آن دوباره هر سه کانال را با یکدیگر یکی کرده و یک تصویر مجموع به‌دست می‌آوریم تا در مرحله بعد فاز لبه‌یابی انجام شود.



شکل (۲): تصویر ورودی اول کانال‌ها



شکل (۳): تصویر خروجی فیلتر شده جهت کاهش نویز

Canny algorithm

// Finding the edges of the input picture

1-Compute f_x and f_y

$$f_x = \frac{\partial}{\partial x}(f * G) = f * \frac{\partial}{\partial x} G = f * G_x$$

$$f_y = \frac{\partial}{\partial y}(f * G) = f * \frac{\partial}{\partial y} G = f * G_y$$

$G(x,y)$ is the Guassian function

$G_x(x,y)$ is the derivate of $G(x,y)$ with respect to x: $G_x(x,y) =$

$$\frac{-x}{\sigma^2} G(x,y)$$

$G_y(x,y)$ is the derivate of $G(x,y)$ with respect to y: $G_y(x,y) =$

$$\frac{-y}{\sigma^2} G(x,y)$$

2- Compute the gradient magnitude

$$magn(i,j) = \sqrt{f_x^2 + f_y^2}$$

3-Apply non-maxima suppression.

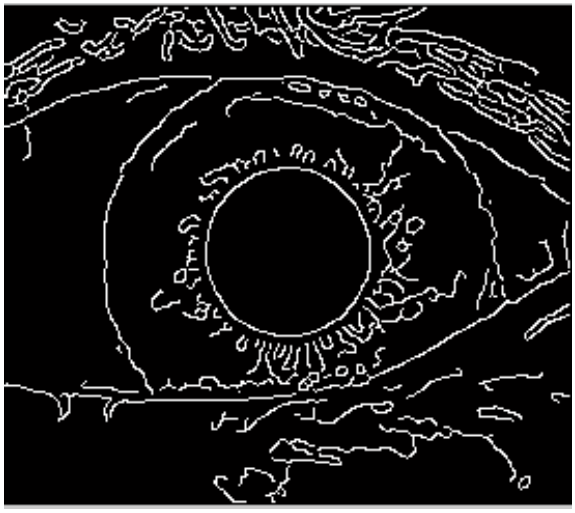
4- Apply hysteresis thresholding/edge link

//Threshold of the edge is found

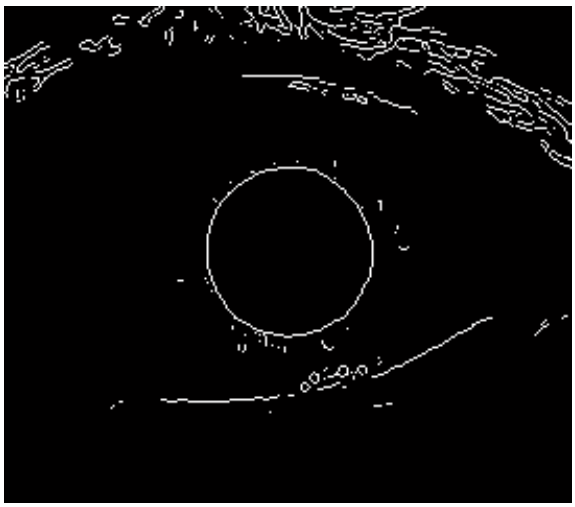
۳-۲- یافتن مرز خارجی مردمک چشم

بعد از حذف کامل نویز یک مرحله پیش از تخمین اولیه از نقاطی که می‌توان آن‌ها را به‌عنوان لبه تلقی کرد انجام می‌شود. در ابتدا تصویر از فضای رنگی[1] به فضای خاکستری‌رنگ[2] تغییر وضعیت داده خواهد شد و پس از آن الگوریتم لبه‌یاب کانی[3] با هدف پیدا نمودن لبه‌های تصویر مورداستفاده قرار خواهد گرفت. از این‌رو شکل (۴) خروجی نهایی لبه‌یابی شده توسط الگوریتم مورداستفاده را نمایش می‌دهد.

همان‌گونه که در خروجی شکل (۴) قابل مشاهده است الگوریتم مورداستفاده تمامی لبه‌های تصویر را مورد شناسایی قرار داده است. ولی نقاط زیادی از نقاط شناسایی‌شده در خروجی به‌دست‌آمده جز لبه‌ها نبوده و الگوریتم دچار اشتباه شده و آن‌ها را به‌عنوان لبه شناسایی کرده است که درواقع ناراستی یا انحنا هستند. جهت حذف این لبه‌های ضعیف در خروجی به‌دست‌آمده، الگوریتم لبه‌یابی سوبل[4] مورداستفاده قرارگرفته است. الگوریتم مدنظر شبیه به فیلتر میانه از یک طرح جهت استخراج لبه‌های تصویر ورودی استفاده می‌کند. الگوی جهت استفاده در این پژوهش الگوی ۳×۳ می‌باشد. شکل (۵) خروجی لبه‌یابی شده حاصل از الگوریتم سوبل را به معرض نمایش قرار می‌دهد



شکل (۴): خروجی نهایی لبه‌یابی به وسیله الگوریتم کانی



شکل (۵): خروجی لبه‌یابی شده حاصل از الگوریتم سوبل

همان‌گونه که در خروجی (۵) قابل مشاهده است. هیچ اثری از لبه‌های ضعیف در تصویر خروجی مشاهده نمی‌شود و لبه‌های قوی‌تر به‌جای مانده است. از همین رو در مرحله بعد جهت تقویت لبه‌های قوی باقی‌مانده در خروجی حاصل از مرحله قبل یک فیلتر لاپلاسین به خروجی وارد خواهیم کرد. با اعمال این

[1] RGB
[2] gray style
[3] canny
[4] Sobel

فیلتر به خروجی، خروجی جدیدی به‌دست می‌آمد که پس از انجام این عمل در آن اندازه نقطه‌هایی که شامل لبه هستند افزایش و اندازه نقطه‌هایی که شامل لبه نیستند صفر شده است. شکل (۶) خروجی فیلتر شده با ماسک لاپلاسین را نمایش می‌دهد.

Sobel algorithm

// Finding more accurate edges of the input picture to remove outlier edges

1- Implementing sobel mask

$$G_x = (z_7 + 2z_8 + z_9) - (z_1$$

2- Find the y-direction derivative: Substract the first column from the third column usingthe mask

$$G_y = (z_3 + 2z_6 - z_9) - (z_1 - 2z_2 + z_7)$$

3- Find the Gradient magnitude

$$G$$

4- Finding the gradient direction

$$\theta$$

// Unnecessary and outlier edges of the eyes are removed

Laplacian algorithm

// Boosting the remained edges of the input picture for a faster and more accurate detection

$$\nabla^2 f = \frac{\partial^2 f}{\partial^2 x} + \frac{\partial^2 f}{\partial^2 y}$$

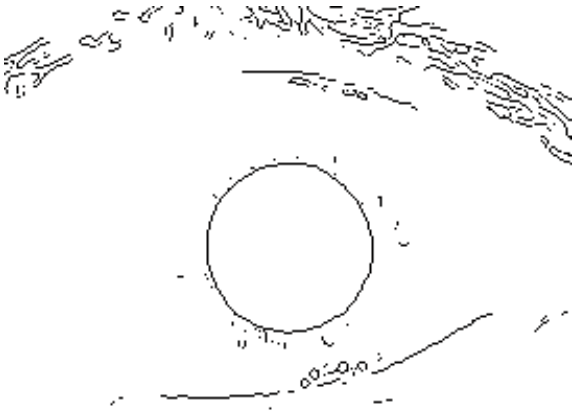
Where the second order derivative in the x direction is defined as follow

$$\frac{\partial^2 f}{\partial^2 x} = f(x+1, y) + f(x-1, y) - 2f(x, y)$$

And the y direction as follows

$$\frac{\partial^2 f}{\partial^2 y} = f(x, y+1) + f(x, y-1) - 2f(x, y)$$

// Filtered the unnecessary edges and have a boosted required part of the eyes for better detection



شکل (۶): واردکردن فیلتر لاپلاسین بر روی خروجی به‌دست‌آمده از مرحله قبل

در مرحله بعد نیز با اجرای فرمان امفایل[1] تمامی چاله‌هایی که در خروجی وجود دارد را پر نموده تا در مرحله آتی جهت شناسایی مرز مردمک از مبدل‌هاف استفاده کنیم. شکل (۷) خروجی به‌دست‌آمده از پرکردن چاله‌ها را نشان می‌دهد.

شکل (۷): خروجی به‌دست‌آمده از پرکردن چاله‌ها

در مرحله بعدی جهت شناسایی مرز مردمک یک تبدیل هاف دایره‌ای را می‌توان اجرا کرد.

تبدیل هاف[2] یک فن معروف است که به‌وسیله آن می‌توان خطوط راست و حتی اشکال دایره‌ای را در یک تصویر تشخیص داد. درواقع جهت شناسایی و پیدا کردن یک شکل ویژه در خروجی به‌دست‌آمده با تبدیل‌هاف نیاز است که شکل موردنظر دارای فرم پارامتری ویژه و مشخصی باشد. همین دلیل مهمی

[1] M.fill
[2] Hough Transform

هست که از تبدیل‌هاف جهت شناسایی و پیدا کردن شکل‌هایی مثل سهمی، دایره و خط در خروجی‌های به‌دست‌آمده استفاده می‌شود. یکی از مهم‌ترین مزایای تبدیل هاف در یافتن خط و دایره در تصویر این است که نسبت به همپوشانی حساس نیست. کیفیت نهایی خروجی و تشخیص تا حد زیادی به کیفیت تشخیص لبه بستگی دارد. همچنین عامل مهم دیگر در کیفیت خروجی این است که چه مقدار دانش پیشین درباره اندازه دایره‌ای در اختیار است که قصد تشخیص آن در تصویر را داریم. با اعمال تبدیل‌هاف بر روی خروجی به‌دست‌آمده از مرحله قبلی مرکز و شعاع دایره مرکزی مردمک مشخص خواهد شد. شکل (۸) خروجی حاصل از اعمال الگوریتم تبدیل‌هاف بر روی خروجی به‌دست‌آمده از مرحله قبل را به نمایش می‌گذارد.

Finding circles by hough transform

// Finding the circle of the iris for detection of the specific person

For all x

For all y

If edge point at (x,y)

For all θ

rho = $x * \cos(\theta) + y * \sin(\theta)$

Increment (add 1 to) the cell in H corresponding to (θ, rho)

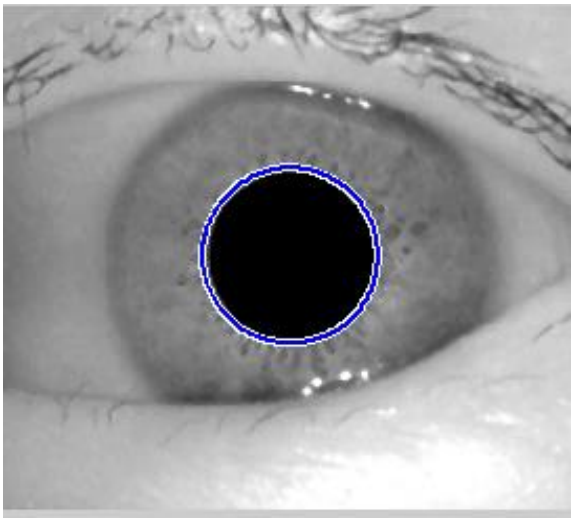
End

End

End

End

// The specific part of the eye (Iris) is detected. This will help to detetct a specific person

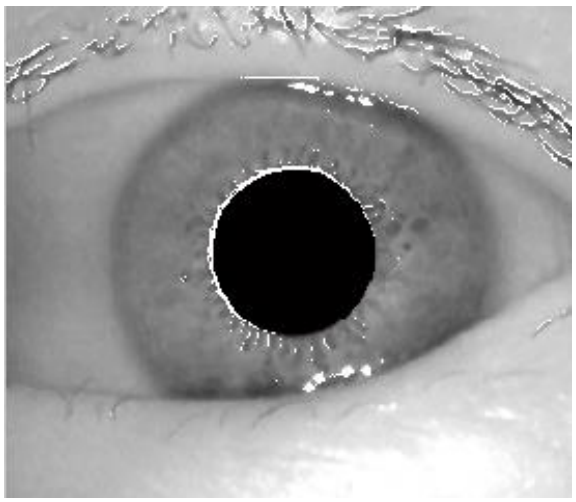


شکل (۸): تشخیص مرز داخلی مردمک خروجی

همان‌گونه که در خروجی شکل (۸) قابل‌مشاهده است. مرز داخلی مردمک چشم به‌وضوح قابل‌مشاهده است. پارامترهای (x,y,r) که به ترتیب بیانگر مختصات افقی، عمودی و شعاع مرکز مردمک چشم است ذخیره خواهند شد تا در ادامه برای تشخیص مرز خارجی عنبیه استفاده شوند.

۳-۳- تفکیک مژه‌ها

مژه اندامی بلند و نازک می‌باشد که دارای ضخامتی به اندازه ۱ یا ۲ پیکسل می‌باشد. به‌دلیل اینکه مژه‌ها عمدتا دارای رنگی تیره هستند و نسبت به سایر نقاط شدت نور کمتری دارند، نقاطی از خروجی را که اندازه اختلاف میزان نور هر پیکسل با پیکسل سمت پایینی و یا با پیکسل سمت راستی خودش بالاتر از بیست باشد را مژه در نظر خواهیم گرفت و جهت از بین بردن آن نقطه اندازه رنگ آن پیکسل را مساوی با ۲۵۵ در نظر خواهیم گرفت. شکل (۹) خروجی به‌دست‌آمده از مرحله تفکیک یا جداسازی مژه‌ها را نشان می‌دهد.



شکل (۹): خروجی به‌دست‌آمده از مرحله تفکیک یا جداسازی مژه‌ها

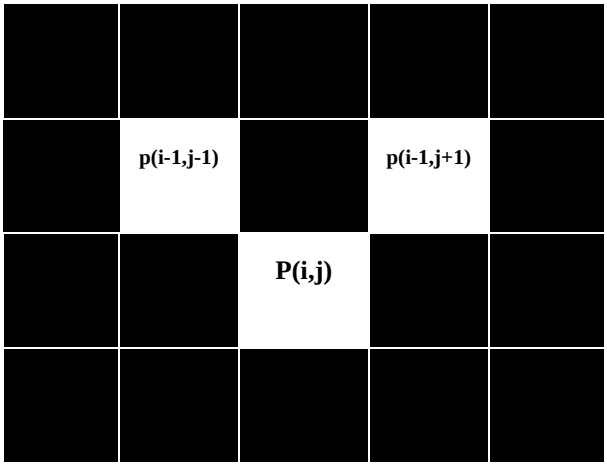
۳-۳-۱- تعیین مرز پلک‌ها

همان‌گونه که در خروجی شکل (۴) قابل مشاهده است. با در نظر گرفتن پلک‌ها به‌صورت یک سهمی و جهت تشخیص آن‌ها می‌توان نقطه‌های لبه مدنظر را به‌دست آورد و با استفاده از تبدیل‌هاف سهمی ویژگی‌های سهمی گذرا از لبه‌ها را به‌دست آورد. اما به‌دلیل اینکه حل معادله به‌دست‌آمده که شامل ۴ پارامتر است زمان‌بر می‌باشد و نیاز به محاسبات سنگین هست، هر پلک با یک معادله درجه سوم تخمین زده خواهد شد. جهت انجام این کار ابتدا می‌بایست نقاطی از پلک را تعیین کنیم. به صورتی که اول با به‌کار بردن از لبه‌یاب سوبل و در جهت محور افقی خروجی را لبه‌یابی خواهیم کرد. و پس از آن در راستای

بهبود لبه‌های به‌دست‌آمده از عملگر مورفولوژی Dilation با یک ساختار خطی با اندازه ۵ و جهت ۲۵- درجه استفاده خواهیم کرد. شکل (۱۰) خروجی به‌دست‌آمده از عملگر Dilation بر روی خروجی را نشان می‌دهد.

شکل (۱۰): نتیجه به‌دست‌آمده از عملگر **Dilation** بر روی خروجی

با توجه به اینکه پلک پایین همیشه در منطقه پایین‌تر از مرکز عنبیه واقع‌شده است، لیکن در نقطه پایین‌تر از خط افقی گذرا از مرکز محدوده چشم که در مرحله تشخیص مردمک حاصل‌شده است در جستجوی نقطه‌های تشکیل‌دهنده‌ی پلک خواهیم بود. به همین ترتیب ازآنجایی‌که پلک پایین یک سهمی رو به بالا هست لذا نقطه‌هایی که بر روی لبه‌ها شامل شرط موجود در خروجی (۱۱) باشد را به‌عنوان نقطه‌های متشکل پلک در نظرخواهیم گرفت:

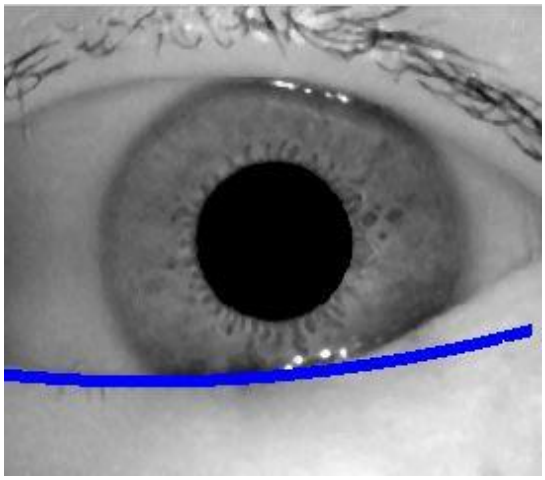


شکل (۱۱): نتیجه به‌دست‌آمده از عملگر **Dilation** بر روی خروجی در بعدهای کوچک‌تر

هر پیکسل مثل P(i,j) که اندازه آن ۱ پیکسل و مقادیر پیکسل‌های اطرافی آن p(i-1,j+1) و p(i-1,j-1) نیز مساوی ۱ باشد می‌تواند به‌عنوان نقطه‌ای از یک سهمی محسوب شود. از همین رو نقاط ذکرشده به‌عنوان نقطه‌های منتخب سهمی در نظر گرفته می‌شوند به‌عبارت‌دیگر:

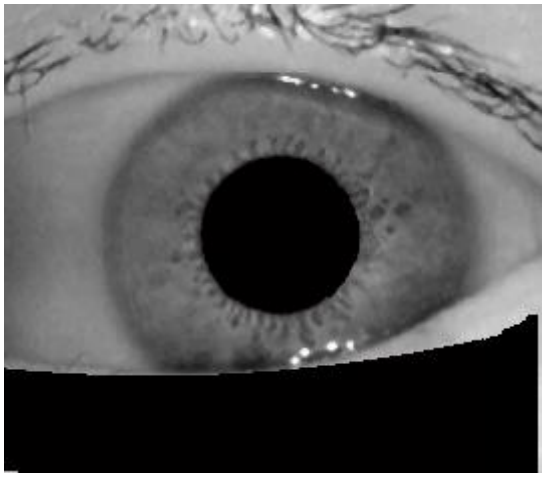
If P(i , j) ==1 && P(i-1, j+1)==1 &&
P(i-1, j-1)==1
Then P(i , j) is a Candidate Point

پس از آن مختصات همه نقطه‌های منتخب در خروجی حاصل‌شده و با فرمان polyfit (x,y,2) ضریب‌های معادله درجه ۲ گذرا از نقطه‌های منتخب حاصل می‌شود و با داشتن ضریب‌های معادله می‌توان سهمی گذرا از نقطه‌های منتخب را ترسیم کرد. شکل (۱۲) یک نمونه از مشخص شدن پلک را نشان می‌دهد.



شکل (۱۲): مشخص شدن مرز پلک به شکل سهمی درجه ۲

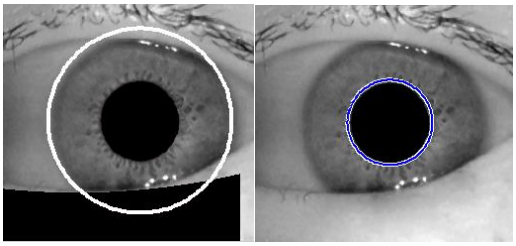
در مرحله بعد جهت جدا کردن محدوده پلک زیرین همه پیکسل‌های زیر سهمی به‌دست‌آمده را به صفر تبدیل نموده تا در مرحله استخراج ویژگی از این ناحیه که جز عنبیه نیست ویژگی استخراج نشود. شکل (۱۳) یک نمونه از حذف پیکسل‌ها را به ما نشان می‌دهد.



شکل (۱۳): از بین بردن پیکسل‌های زیر سهمی

۳-۳-۲- تشخیص مرز خارجی عنبیه

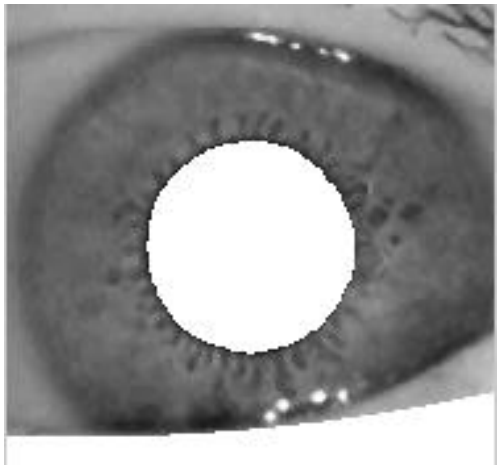
اصلی‌ترین و ویژه‌ترین مرحله قطعه‌بندی و شناختن عنبیه مرز خارجی بین عنبیه و صلبیه است. چون در وحله اول در این منطقه مرز مشخص و تعیین شده‌ای وجود ندارد و اختلاف میزان اندازه نور عنبیه و صبلیه در مرز بسیار ناچیز است و در وحله دوم نقطه‌های لبه دیگر که اختلاف میزان نور در آن‌ها خیلی زیادتر از مرز عنبیه و صلبیه است در تصویر چشم موجود نیست. لذا نتیجه می‌گیریم الگوریتم‌های لبه‌یاب که توانایی مشخص کردن لبه‌های مربوط به مرز خارجی عنبیه را دارند آن‌ها را به‌عنوان لبه تشخیص می‌دهند. که این تشخیص خود موجب به وجود آمدن خطا می‌شود. از همین رو جهت مشخص شدن مرز عنبیه از مختصات به‌دست‌آمده‌ی مرکز مردمک چشم که در مرحله مشخص شدن مردمک به‌دست‌آمده استفاده می‌شود. به این صورت که مرکز مردمک و عنبیه به یک اندازه می‌باشد. سپس مختصات (x,y) به‌دست‌آمده جهت مرکز مردمک چشم همان مختصات دایره عنبیه خواهد بود. از آن جهت که به‌طورمعمول شعاع عنبیه چشم حدود ۵۰ پیکسل هست، شعاع مردمک چشم (r) را با ۵۰ پیکسل جمع می‌کنیم و به‌عنوان شعاع عنبیه مدنظر قرار خواهیم داد. بدین ترتیب مشخصه‌ها (x,y,r+50) به‌عنوان مشخصه‌ها و شعاع عنبیه چشم در نظر گرفته می‌شود و دایره گذرا از این مشخصه‌ها نیز مرز بین عنبیه و صلبیه در نظر گرفته‌شده است. شکل (۱۴) یک نمونه از تشخیص مرز عنبیه را نشان خواهد داد.



شکل (۱۴): تشخیص مرز خارجی مردمک و عنبیه

۳-۳-۳- تفکیک محدوده عنبیه

باهدف استخراج خصوصیت‌های مفید از عنبیه باید در وحله اول محدوده‌ی عنبیه از خروجی بریده شود و استخراج ویژگی فقط از این ناحیه صورت پذیرد از همین رو جهت انجام این مرحله بعد از مراحل تشخیص مرز بین عنبیه و صلبیه ناحیه مردمک و سطح زیر پلک پایین از خروجی حذف خواهند شد و یک ناحیه مربعی به طول شعاع عنبیه از خروجی اصلی بریده خواهد شد تا در مرحله استخراج ویژگی فقط از ناحیه عنبیه ویژگی استخراج شود. شکل (۱۵) نتیجه‌های به‌دست‌آمده از این مرحله‌ها را نشان می‌دهد.

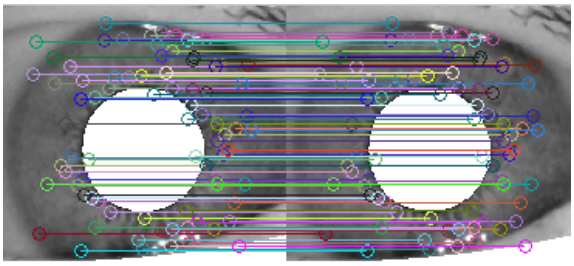


شکل (۱۵): حذف محدوده مردمک و زیر سهمی پلک پایین و بریدن محدوده عنبیه

۳-۳-۴- مرحله استخراج ویژگی

به‌منظور واکشی خصوصیات مقاوم و مناسب در برابر عوامل به وجود آورنده خطا معرفی‌شده (فاصله، شرایط روشنایی، زاویه و ...) از الگوریتم‌های استخراج خصوصیات سیفت استفاده خواهد شد.

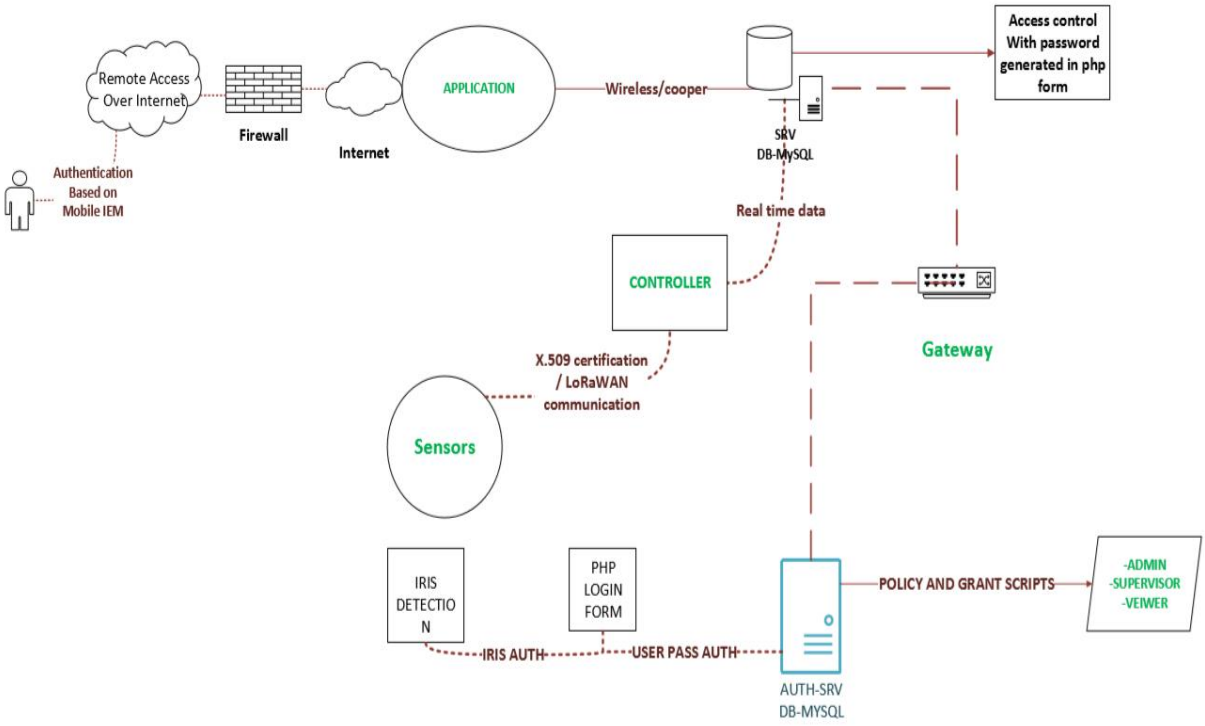
الگوریتم تبدیل ویژگی مستقل از مقیاس (SIFT) یک راهبرد تناظریابی عارضه مبنا است که به‌منظور انجام فرایند شناسایی الگو در تصاویر اپتیکی مدنظر قرار گرفته‌شده است. درواقع این الگوریتم برای استخراج ویژگی‌های مشخص از تصاویر، برای به‌کارگیری در الگوریتم‌های تطبیق نماهای مختلف یک جسم و شناسایی اجسام به‌کار می‌رود. مشخصه‌های به‌دست‌آمده در این الگوریتم جدا از تغییرات روشنایی، دوران، پایدار در مقابل نویز، تغییر موقعیت گرفتن تصویر و مقیاس می‌باشد. به‌منظور پیاده‌سازی الگوریتم سیفت، توابع متلب مورداستفاده قرارگرفته است. الگوریتم سیفت شامل مولفه‌هایی می‌باشد که بر روی کارکرد الگوریتم تأثیرگذار است و مولفه‌های مناسب موردراندازه‌گیری قرارگرفته‌اند. مولفه سیگما در فیلتر گوسین به‌عنوان یک فیلتر (low pass) عمل خواهد کرد و هر چه میزان شدت و اندازه آن بالاتر باشد خروجی مات‌تر خواهد شد و خصوصیات و عارضه‌های به‌دست‌آمده کمتر خواهند شد. مقدار در نظر گرفته‌شده برای این مولفه ۲/۵ می‌باشد. یکی دیگر از مولفه‌های تأثیرگذار و دارای اهمیت در کارایی الگوریتم‌های سیفت مولفه اکتاو هست که تعداد در نظر گرفته شده ۴ اکتاو می‌باشد. به‌علاوه تعداد تصویرهای در نظر گرفته‌شده در هر اکتاو نیز در این الگوریتم سه تصویر می‌باشد. خروجی الگوریتم سیفت برای هر نقطه بیانگر عارضه یک بردار ۱۲۸تایی خواهد بود. همین‌طور جهت تناظریابی و تشخیص نقطه‌های متناظر از فاصله اقلیدسی به‌منظور بردارهای ویژگی حاصل‌شده استفاده‌شده است. نمونه‌ای از تناظریابی به‌دست‌آمده در شکل (۱۶) نشان داده‌شده است.



شکل (۱۶): تناظریابی خصوصیات سیفت به‌دست‌آمده در دو خروجی

۳-۴- ساختار مدل احراز هویت دو مرحله ای

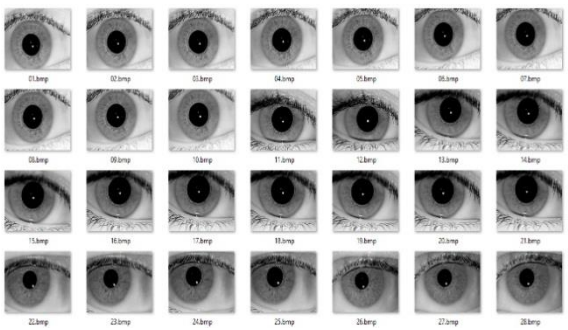
این مدل با توجه به اهمیت برقراری امنیت در برابر حملات و حفظ حریم خصوصی ارائه شده است. به این صورت که با طراحی یک فرم php که در تمامی فیلدها کنترل اطلاعات ورودی برقرار است و در برابر حمله Sql Injection با استفاده از توزیع PDO جهت محافظت Sql Database مقاوم می‌باشد، طراحی شده است.



شکل (۱۷): احراز هویت دو مرحله ای

۴- شبیه‌سازی

در این پژوهش، به‌منظور صحت‌سنجی و تست مناسب‌تر روش پیشنهادشده داده‌های پایگاه CASIA مورداستفاده قرارگرفته است. در این آزمایش‌ها پایگاه داده عنبیه CASIAVersion1.0[1] نام‌گذاری می‌شود، که ۷۵۶ تصویر به‌صورت خاکستری گرفته‌شده است؛ که داده‌های ۱۰۸ کاربر مختلف می‌باشد. برای هر کاربر ۷ تا ۱۰ تصویر خاکستری در نظر گرفته‌شده، که در دو بازه زمانی متفاوت گرفته‌شده است به صورتی که به فواصل زمانی یک‌ماهه می‌باشند. این تصویرها به‌صورت ویژه جهت شناسایی هویت بر اساس عنبیه به‌وسیله دوربین‌های ویژه که به‌منظور این کار طراحی و ساخته‌شده‌اند گرفته شدند. نمونه‌هایی از تصویرهای این پایگاه داده در شکل (۱۸) آمده است.لازم به ذکر می‌باشد که شبیه‌سازی الگوریتم ارائه‌شده توسط نرم‌افزار MATLAB R2015B و روی سیستم‌عامل ویندوز ۸/۱ بر روی دستگاه لپ‌تاپ SONY svf143 با مشخصات RAM:16GB-20307MHz, CPU: corei7-1.80GHz انجام‌گرفته است.



شکل (۱۷): نمونه‌هایی از تصویرهای پایگاه داده CASIA

[1]http://biometrics.idealtest.org/findTotalDbByMode.do?mode=Iris

۴-۱- ارزیابی مردمک

برای ارزیابی مرحله تشخیص مردمک ۱۰۰ حالت متفاوت از تصویر ورودی چشم انسان انتخاب‌شده است و الگوریتم پیشنهادی در پژوهش بر روی هر تصویر اعمال‌شده است. نتایج به‌دست آمده بیانگر آن است که از درصد موفقیت بیش از ۹۳٪ تشخیص صحیح و درست مردمک چشم می‌باشد. همین‌طور در ۵٪ از تصاویر دارای خطا و در ۲٪ از تصاویر الگوریتم پیشنهادی توانایی تشخیص مردمک را ندارد (جدول ۱). نمونه‌هایی از تصویرهای تشخیص مردمک در شکل (۱۸) قابل‌مشاهده است.

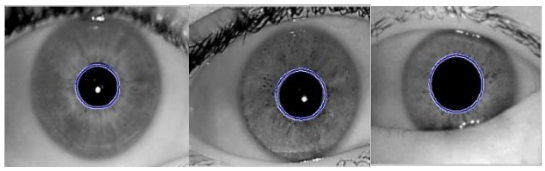
	شخص اول	شخص دوم	شخص سوم	شخص چهارم	شخص پنجم	شخص ششم	شخص هفتم	شخص هشتم	شخص نهم	شخص دهم
میزان تشخیص واقعی (TDR)	0,91	0,87	0,90	0,96	0,89	0,95	0,93	0,95	0,96	0,90

جدول (۱): میزان شناسایی صحیح بر روی ۱۰۰ تصویر چشم افراد مختلف

$$TDR = (\frac{\sum_{i=0}^{100} TDR^i)}{100}$$

$$TDR = 0.93$$

همان‌گونه که در معادله فوق قابل‌مشاهده است، جهت اندازه‌گیری اندازه نرخ تشخیص صحیح کل سیستم، از میانگین‌گیری مقدارهای TDR به‌دست‌آمده برای هر فرد، استفاده‌شده است.



شکل (۱۸): نمونه‌ای از تصویرهای تشخیص مرز مردمک

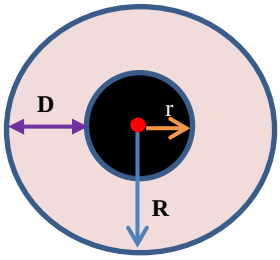
۴-۲- بررسی تشخیص عنبیه

همان‌گونه که در قسمت الگوریتم پیشنهادی شناسایی عنبیه اشاره شد مشخصه‌های مرکز عنبیه و مردمک چشم بسیار مهم می‌باشند. مشخصه مرکز مردمک به‌عنوان مرکز عنبیه نیز در نظر گرفته می‌شود.

ازآنجاکه تبدیل‌هاف دایره‌ای به دنبال مشخصه‌های مرکز مردمک می‌باشد و زمان زیادی را حل معادله‌های این بخش صرف می‌کند از همین رو با توجه به داشتن این مشخصه‌ها و انتخاب یک شعاع درست، می‌توان دایره پوششی عنبیه را بدون نیاز به استفاده از الگوریتم هاف پیدا نمود.

برای انتخاب نمودن شعاع مطلوب در پایگاه داده از ۱۰۰ تصویر متفاوت استفاده شده است. به صورتی که شعاع عنبیه‌ی هر شخص از مرکز مردمک به‌طور دستی اندازه‌گیری شده است و از شعاع مردمک که به‌وسیله تبدیل هاف به‌دست‌آمده کم شده است. به‌عبارت دیگر:

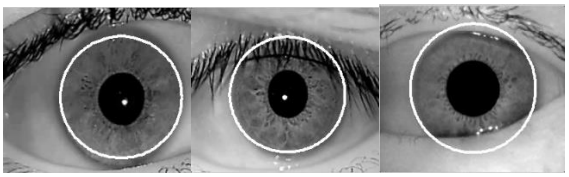
$$D=\| R - r \|$$



پس از آن برای انتخاب کردن شعاع صحیح و مطلوب، میانگین همه مقادیر حاصل شده (D) را حساب کرده و با میانگین ۱۰+ پیکسل به‌عنوان شعاع مفید جهت دایره پوششی عنبیه انتخاب خواهیم کرد. به تعبیر دیگر:

$$R' = \sum_{i=0}^{100} D/100$$
$$R''=R'-10$$

با انجام شدن مرحله‌های فوق ذکر شعاع اثرگذار و متناسب که در نظر گرفته شده است. برای ۱۰۰ تصویر آزمایشی مساوی با ۵۰ پیکسل مورد اندازه‌گیری قرارگرفته شده است. شکل (۱۹) یک مورد از تصاویر تشخیص عنبیه را نشان می‌دهد.



شکل (۱۹): یک نمونه از تصویرهای تشخیص مرز خارجی عنبیه

به همین ترتیب با در نظر گرفتن مرکز برابر جهت مردمک و عنبیه و محاسبه شعاع و پیدا نمودن مرز عنبیه به شیوه بیان‌شده، باعث کاهش قابل‌توجه بار زمانی و محاسباتی شده است. جدول (۲) مقایسه زمان اجرا برای پیدا کردن مرز عنبیه با استفاده از متد تبدیل‌هاف دایره‌ای و روش پیشنهادی پژوهش حاضر را نشان می‌دهد.

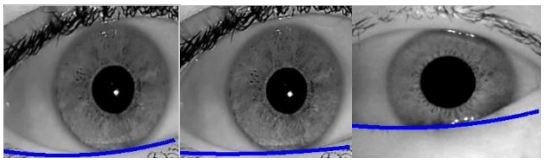
جدول (۲): مقایسه زمان اجرا جهت پیدا کردن مرز عنبیه با استفاده از متد تبدیل‌هاف دایره‌ای و روش ارائه‌شده

زمان (بر حسب ثانیه)		
روش ارائه شده	هاف دایره‌ای	شماره تصویر
۰/۰۰۰۰۰۸	۰/۵۶۳۶۳۲	تصویر اول
۰/۰۰۰۰۱۰	۰/۵۷۸۳۰۲	تصویر دوم
۰/۰۰۰۰۰۸	۰/۶۱۹۴۳۶	تصویر سوم
۰/۰۰۰۰۰۹	۰/۵۶۹۶۲۱	تصویر چهارم
۰/۰۰۰۰۰۷	۰/۵۱۹۶۴۰	تصویر پنجم

همان‌گونه که در جدول (۲) بیان‌شده زمان اجرا روش پیشنهادی پژوهش حاضر نسبت به زمان اجرای متد تبدیل‌هاف کاهش قابل توجهی دارد و همین کاهش زمان، موجب کاهش بار محاسباتی می‌باشد. در روش پیشنهادی پژوهش حاضر برای یافتن مرز مفید عنبیه از مشخصه‌ها و داده‌های حاصل شده در مراحل قبلی استفاده‌شده و نیز شعاع با توجه به معادله اشاره‌شده محاسبه گردیده و الگوریتم مدنظر دیگر نیازی به محاسبه تبدیل‌هاف و به‌دست آوردن چهار مولفه تبدیل‌هاف ندارد.

۴-۳- بررسی الگوریتم شناسایی پلک

از بزرگترین نویزهایی که در تصاویر چشم وجود دارد پلک‌ها می‌باشند. زیرا امکان دارد عنبیه در شرایطی قرار داشته باشد که بخشی از آن در زیر پلک باشد که در این صورت بخشی از پلک به‌عنوان عنبیه چشم در نظر گرفته می‌شود. در مرحله استخراج خصوصیات از این منطقه نیز ویژگی‌های اشتباهی استخراج خواهد شد. به همین دلیل کاهش بار محاسباتی و اجتناب از اعمال الگوریتم تبدیل‌هاف سهمی و همچنین دقت بیشتر، از روش سهمی درجه دوم استفاده‌شده است.

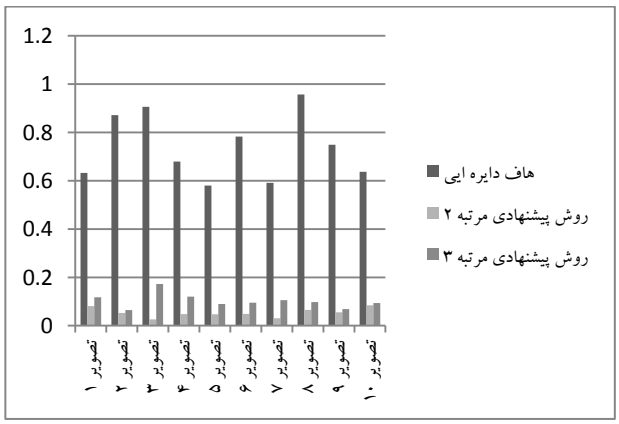


شکل (۲۰): تشخیص پلک به‌وسیله روش پیشنهادشده در پژوهش حاضر (سهمی درجه‌دو)

همچنین در نتایج به‌دست‌آمده مشاهده می‌شود که روش پیشنهادشده در پژوهش حاضر ازنظر زمان اجرا به نسبت تبدیل‌هاف سهمی دارای سرعت بالاتری می‌باشد. جدول (۳) نتایج به‌دست‌آمده از مقایسه زمان اجرا روش پیشنهادشده در پژوهش حاضر به‌صورت معادله‌های درجه دوم؛ درجه سوم و همچنین روش تبدیل‌هاف سهمی را برای ده تصویر نشان می‌دهد (نمودار ۱).

جدول (۳): زمان اجرا روش پیشنهادی به‌صورت معادله‌های درجه دوم؛ درجه سوم و همچنین روش تبدیل‌هاف سهمی

زمان (برحسب ثانیه)			
روش پیشنهادشده در پژوهش حاضر درجه سوم	**روش پیشنهادشده در پژوهش حاضر درجه دوم**	**هاف سهمی**	**شماره تصویر**
۰/۱۱۷۶	۰/۰۸۱۳	۰/۶۳۲۵	تصویر اول
۰/۰۶۴۸	۰/۰۵۲۵	۰/۸۷۱۸	تصویر دوم
۰/۱۷۲۶	۰/۰۲۶۱	۰/۹۰۶۱	تصویر سوم
۰/۱۲۰۵	۰/۰۴۸۳	۰/۶۷۹۲	تصویر چهارم
۰/۰۸۹۶	۰/۰۴۷۵	۰/۵۸۰۳	تصویر پنجم
۰/۰۹۴۸	۰/۰۴۸۷	۰/۷۸۳۰	تصویر ششم
۰/۱۰۵۷	۰/۰۳۰۵	۰/۵۹۱۲	تصویر هفتم
۰/۰۹۷۶	۰/۰۶۵۲	۰/۹۵۷۳	تصویر هشتم
۰/۰۶۸۳	۰/۰۵۵۳	۰/۷۴۹۱	تصویر نهم
۰/۰۹۳۷	۰/۰۸۴۵	۰/۶۳۷۲	تصویر دهم



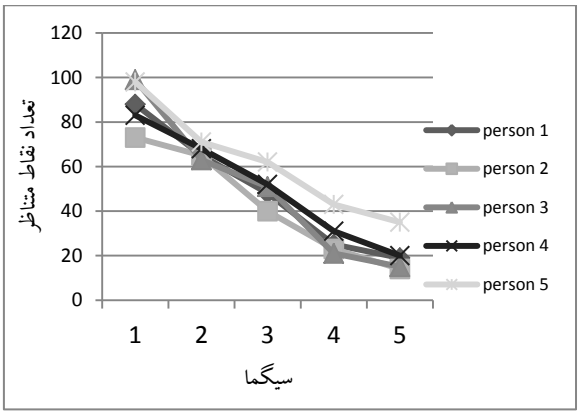
نمودار (۱): زمان اجرا روش پیشنهادی به‌صورت معادله درجه دوم و درجه سوم و روش تبدیل‌هاف سهمی

همان‌گونه که در جدول (۳) و نمودار (۱) قابل‌مشاهده است زمان اجرای روش پیشنهادشده در پژوهش حاضر با معادله درجه دوم از روش پیشنهادشده با معادله درجه سوم و روش تبدیل‌هاف به میزان کمتری می‌باشد زیرا در چنین حالتی تعداد مولفه‌های حساب‌شده به نسبت دیگر روش‌های بیان‌شده کمتر است. ولی ازنظر میزان دقت در تشخیص صحیح مرز پلک‌ها هر سه روش ذکرشده دارای دقت قابل قبولی هستند.

۴-۴- بررسی مولفه‌های مساله

از اساسی‌ترین اقلام در کارکرد مناسب یک سیستم، تنظیم مناسب و درست پارامترهای سیستم می‌باشد. بنابراین در صورت عدم انتخاب پارامترهای صحیح، سیستم دچار خطا خواهد شد و نتایج مناسب و قابل قبولی را ارائه نمی‌کند. مولفه‌های سیگما و تعداد اکتاو در الگوریتم سیفت از جمله مولفه‌های کلیدی و دارای اهمیت می‌باشند که می‌توانند تا حد بالایی بر کارکرد سیستم اثرگذار باشند. از همین رو در این مرحله به ارزیابی و بررسی این دو مولفه پر اهمیت خواهیم پرداخت.

۴-۴-۱- بررسی مولفه سیگما در سیفت

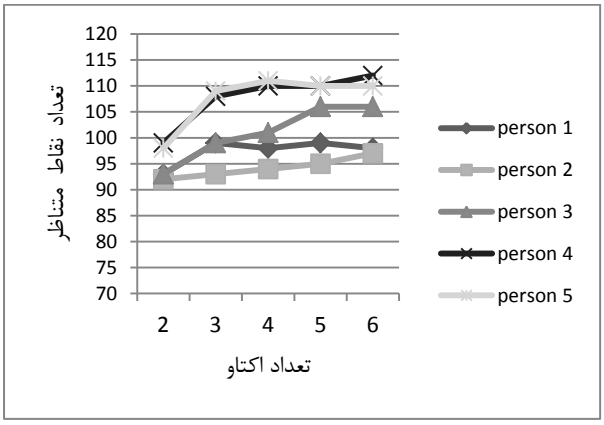


نمودار (۲): نتایج به‌دست‌آمده از اندازه‌گیری سیگما

۴-۴-۲- مشخص کردن تعداد اوکتاو[1] در الگوریتم سیفت

پارامتر اکتاو یکی دیگر از پارامترهای تأثیرگذار و دارای اهمیت در کارایی الگوریتم سیفت می‌باشد. به‌منظور مشخص کردن این پارامتر الگوریتم را با تصاویر ثابتی تست کرده و با توجه به نتایج به‌دست‌آمده در نمودار (۳) تعداد اکتاو مطلوب برای الگوریتم سیفت **۴** اکتاو در نظر گرفته‌شده است. همان‌گونه که در نمودار (۳) قابل‌مشاهده است. نمودار جابه‌جایی تعداد ویژگی‌های یافت شده در الگوریتم بعد از میزان مناسب اکتاو ثابت می‌شود.

[1] Octave



نمودار (۳): تعداد اکتاو مناسب برای الگوریتم سیفت

۴-۵- ماتریس درهمریختگی یا گمگشتگی

ماتریسی که در آن کارکرد الگوریتم‌های مربوطه قابل‌مشاهده است، ماتریس درهمریختگی گفته می‌شود. عمدتا چنین نمایشی جهت الگوریتم‌های یادگیری با ناظر استفاده می‌شود، اگرچه در یادگیری بدون ناظر نیز کاربرد دارد. معمولاً به‌کاربرد این ماتریس در الگوریتم‌های بدون ناظر ماتریس تطابق می‌گویند. هر ستون از ماتریس، نمونه‌ای از اندازه پیش‌بینی‌شده را نمایش می‌دهد. درصورتی‌که هر سطر نمونه‌ای واقعی (درست) را در بردارد. این ماتریس از آنجا بدین نام معروف شده که به کمک آن راحت‌تر می‌توان تداخل بین نتایج و اشتباه را مشاهده نمود.

در این ماتریس هر سطر نشان‌دهنده اندازه فاصله اقلیدسی با هر ستون می‌باشد. به همین صورت که چند تصویر متفاوت از هر شخص با ۹ تصویر دیگر به‌عنوان جفت تصویر به الگوریتم داده‌شده و اندازه فاصله اقلیدسی اندازه‌گیری و درنهایت میانگین‌گیری شده است. همان‌گونه که در جدول (۴) درهمریختگی را نشان می‌دهد، مقدار اندازه‌گیری شده جهت قطر اصلی مساوی با صفر می‌باشد.

۴-۶- اندازه‌گیری میزان دقت روش پیشنهادشـــده در پژوهش حاضر

جهت اندازه‌گیری میزان دقت سیستم در تشخیص اشخاص در حالات متفاوت از یک شخص خاص، معیارهای TP و TN بکار رفته است. معیار TP تعداد نقاط ویژگی است که در ۲ تصویر متفاوت از یک شخص به‌صورت درست متناظر بوده و الگوریتم به درستی شناسایی کرده است (تعداد خطوط صاف در تصاویر تناظریابی شده). معیار TN تعداد نقاط ویژگی است که در ۲ تصویر متفاوت از یک شخص به اشتباه متناظر شده است (تعداد خطوط مورب و غیر صاف). به‌علاوه میزان دقت برای هر دسته از تصویرها با استفاده از معادله زیر محاسبه‌شده است:

$$\text{Accuracy} = \frac{\text{TP}}{\text{TP} + \text{TN}}$$

جدول (۴): ماتریس درهمریختگی به‌دست‌آمده از ۵ شخص (۱۰ جفت عکس)

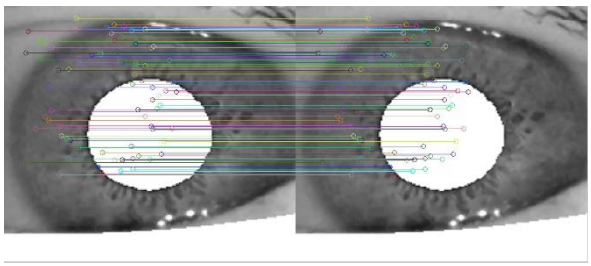
فاصله	شخص اول	شخص دوم	شخص سوم	شخص چهارم	شخص پنجم	شخص ششم	شخص هفتم	شخص هشتم	شخص نهم	شخص دهم
شخص اول	۰	۰/۹۸۳	۰/۷۵۱	۰/۸۵۱	۰/۸۵۰	۰/۶۳۷	۰/۸۴۰	۰/۹۶۱	۰/۹۷۱	۰/۸۴۳
شخص دوم	۰/۹۸۳	۰	۰/۷۳۶	۰/۹۰۴	۰/۵۹۳	۰/۷۳۵	۰/۸۳۵	۰/۷۴۳	۰/۸۴۰	۰/۶۰۶
شخص سوم	۰/۷۵۱	۰/۷۳۶	۰	۰/۷۰۲	۰/۷۳۶	۰/۸۴۷	۰/۵۲۰	۰/۹۵۴	۰/۸۵۴	۰/۶۸۴
شخص چهارم	۰/۸۵۱	۰/۹۰۴	۰/۷۰۲	۰	۰/۵۴۷	۰/۸۲۱	۰/۷۴۲	۰/۵۰۴	۰/۷۳۲	۰/۹۴۳
شخص پنجم	۰/۸۵۰	۰/۵۹۳	۰/۷۳۶	۰/۵۴۷	۰	۰/۷۳۴	۰/۷۵۱	۰/۸۵۷	۰/۷۵۴	۰/۸۵۳
شخص ششم	۰/۶۳۷	۰/۷۳۵	۰/۸۴۷	۰/۸۲۱	۰/۷۳۴	۰	۰/۹۴۳	۰/۷۳۰	۰/۳۵۴	۰/۴۳۰
شخص هفتم	۰/۸۴۰	۰/۸۳۵	۰/۵۲۰	۰/۷۴۲	۰/۷۵۱	۰/۹۴۳	۰	۰/۷۴۵	۰/۸۰۴	۰/۶۸۴
شخص هشتم	۰/۹۶۱	۰/۷۴۳	۰/۹۵۴	۰/۵۰۴	۰/۸۵۷	۰/۷۳۰	۰/۷۴۵	۰	۰/۶۵۳	۰/۸۵۵
شخص نهم	۰/۹۷۱	۰/۸۴۰	۰/۸۵۴	۰/۷۳۲	۰/۷۵۴	۰/۳۵۴	۰/۸۰۴	۰/۶۵۳	۰	۰/۶۰۲
شخص دهم	۰/۸۴۳	۰/۶۰۶	۰/۶۸۴	۰/۹۴۳	۰/۸۵۳	۰/۴۳۰	۰/۶۸۴	۰/۸۵۵	۰/۶۰۲	۰

همان‌گونه که در جدول (۵) قابل مشاهده است، بیشترین میزان دقت اندازه‌گیری شده ۹۶٪ (دقت مقایسه هر تصویر با خودش ۱۰۰٪ می‌باشد) و کمترین میزان دقت ۸۶٪ می‌باشد. همچنین بیشترین میانگین اندازه‌گیری شده دقت ۹۴٪ می‌باشد

جدول (۵): اندازه‌گیری میزان دقت روش پیشنهادشده در پژوهش حاضر

میانگین دقت (ACC)	تصویرها در شرایط متفاوت					تصویر اصلی هر شخص
	تصویر۵	تصویر۴	تصویر ۳	تصویر ۲	تصویر ۱	
۰/۹۲	TP=88 TN=9 Acc=0.9	TP=93 TN=14 Acc=0.86	TP=83 TN=4 Acc=0.95	TP=85 TN=7 Acc=0.92	TP=89 TN=0 Acc=1	شخص اول
۰/۹۲	TP=101 TN=12 Acc=0.89	TP=82 TN=9 Acc=0.90	TP=71 TN=9 Acc=0.88	TP=70 TN=5 Acc=0.93	TP=76 TN=0 Acc=1	شخص دوم
۰/۹۳	TP=93 TN=8 Acc=0.92	TP=91 TN=8 Acc=0.91	TP=86 TN=7 Acc=0.92	TP=88 TN=5 Acc=0.94	TP=92 TN=0 Acc=1	شخص سوم
۰/۹۲	TP=83 TN=6 Acc=0.93	TP=79 TN=11 Acc=0.87	TP=75 TN=8 Acc=0.90	TP=73 TN=7 Acc=0.91	TP=86 TN=0 Acc=1	شخص چهارم
۰/۹۵	TP=84 TN=7 Acc=0.92	TP=80 TN=6 Acc=0.93	TP=88 TN=3 Acc=0.96	TP=78 TN=6 Acc=0.92	TP=89 TN=0 Acc=1	شخص پنجم

در شکل (۲۱) نمونه‌هایی از تناظریابی درست و غلط به‌وسیله الگوریتم نشان داده‌شده است.



شکل (۲۱): تناظریابی درست دو تصویر یکسان از یک شخص

جدول (۶) حاصل جمع‌بندی نتایج به‌دست‌آمده از آزمایش و مقایسه روش‌های ارائه‌شده می‌باشد

جدول (۶): مقایسه زمان اجرا و دقت

روش	استخراج ویژگی (MS)	تطبیق (ms)	دقت (تا دو رقم)
بولز	**۱۷۰/۳**	**۱۱**	**۹۲**
داگمن	**۶۸۲/۵**	**۴/۳**	**۱۰۰**
تان	**۴۲۶/۸**	**۱۳/۱**	**۹۹**
وایلدز	**۲۱۰/۰**	**۴۰۱/۰**	**۹۳**
روش پیشنهادی	**۱۳۲/۸۷**	**۳/۰۷**	**۹۳**

۵- نتیجه‌گیری

تشخیص، مکان‌یابی و استخراج ویژگی‌های عنبیه یکی از پرچالش‌ترین، مهم‌ترین و البته قابل‌اعتمادترین روش‌های تشخیص هویت بر اساس بیومتریک بدن شخص می‌باشد.چون تصویر چشم شخص مدنظر می‌تواند تحت تأثیر عوامل نویزی فراوانی قرار بگیرد، میزان تغییر فاصله از دوربین، چرخش سر در زمان تصویربرداری، روشنایی نور، پلک‌ها و مژه‌ها از نویزهایی می‌باشند، که توانایی این را دارند که نتایج تشخیص را دچار تغییر کنند. همان‌گونه که در بخش سه به تفصیل بیان شد، روش پیشنهادی در پژوهش حاضر از نظر معیارهای زمان اجرا و دقت موردبررسی قرارگرفته و سپس با روش‌های انجام‌شده قبلی مورد مقایسه قرارگرفته است.

همان‌گونه که در جدول (۶) قابل مشاهده است، روش پیشنهادی پژوهش ازنظر زمان اجرای استخراج و مطابقت با ویژگی‌ها به نسبت دیگر الگوریتم‌های آورده شده بهینه‌تر می‌باشد. همین‌طور روش ارائه‌شده از نظر تشخیص با دقت ۹۳٪ نسبت به دو روش بولز و وایلدز مناسب‌تر بوده ولی از دو روش تان و داگمن از دقتی با درصد پایین‌تر برخوردار می‌باشد که البته روش پیشنهادی زمان تطبیق کمتری دارد.

به‌عبارت‌دیگر روش پیشنهادی توانایی تشخیص و شناخت هویت اشخاص با دقت مطلوب و زمان اجرای بهینه به نسبت روش‌های گذشته می‌باشد. اما از نظر قطعه‌بندی درست عنبیه در تصاویری که عنبیه و مردمک در زیر پلک قرار دارند، الگوریتم‌های تست شده قبلی از درصد موفقیت بیشتری به نسبت روش پیشنهادی برخوردار هستند. به همین دلیل برای ادامه راه این تحقیق پیشنهاد می‌گردد، برای بالا بردن دقت در مرحله قطعه‌بندی عنبیه، اقدام به بهتر شدن الگوریتم قطعه‌بندی نموده و پژوهش‌ها در این زمینه ادامه داشته باشد. به‌طور مشخص پیشنهاد می‌شود در پژوهش‌های آتی ارائه مدل تهدیدات، حملات و آسیب‌پذیری‌ها در شبکه‌های حسگر بیسیم موردبررسی قرار گیرد. به‌علاوه پیشنهاد می‌شود در پژوهش‌های آتی چالش‌ها و مشکلات شبکه‌های WBAN مورد ارزیابی قرار بگیرد.

۶. مراجع

[1] J. Katz, A. J. Menezes, et al., "Handbook of applied cryptography", CRC press, 1996.

[2] W. Rankl and W. Effing, "Smart card handbook", John Wiley & Sons, 2004.

[3] D. Bandyopadhyay and J. Sen, "Internet of things: Applications and challenges in technology and standardization", Wireless Pers. Commun., Vol. 58, no. 1, pp. 49-69, 2011.

[4] K. T. Nguyen, M. Laurent, et al. "Survey on secure communication protocols for the Internet of Things", Ad Hoc Networks, Vol. 32, pp. 17-31, 2015.

[5] Z. Shelby, "Constrained RESTful environments (CoRE) link format", RFC, Vol. 6690, pp. 1-22, 2012.

[6] Y. Kong, M. Zhang, et al. "A belief propagation-based method for task allocation in open and dynamic cloud environments", Knowl-Based Syst., Vol. 115, pp. 123-132, 2017.

[7] Z. Xia, X. Wang, et al. "A privacy-preserving and copy-deterrence content-based image retrieval scheme in cloud computing", IEEE T. Inform. Foren Security, Vol. 11, no. 11, pp. 2594-2608, 2016.

[8] Z. Xia, X. Wang, et al. "A Secure and Dynamic Multi-Keyword Ranked Search Scheme over Encrypted Cloud Data", IEEE T. PARALL DISTR, Trans. Parallel Distrib. Syst., Vol. 27, no. 2, pp. 340-352, 2016.

[9] J. Shen, J. Shen, et al. "An efficient public auditing protocol with novel dynamic structure for cloud data", IEEE T Inform. Foren Security, Vol. 12, no. 10, pp. 2402-2415, 2017.

[10] J. Shen, D. Liu, et al. "A secure cloud-assisted urban data sharing framework for ubiquitous-cities", Pervasive Mob. Comput., Vol. 41, pp. 219-230, 2017.

[11] G. Hsin Lai, Ch. Chen, B. Chiang Jeng, and W. Chao, "Ant-Based IP Traceback", Expert Syst. Appl., Vol. 34, pp. 3071-3080, 2008.

[12] R. Roozbehi, M. Qasemzadeh, "Using Software-Based Networks to Improve IoT Security", Journal of Information Technology and Communication Innovations, Vol. 1, no. 2, pp. 11-16, 2019.

[13] L. Lamport, "Password authentication with insecure communication", Commun. Acm., Vol. 24, no. 11, pp. 770-772, 1981.

[14] R. Lennon, S. Matyas, et al., "Cryptographic authentication of time-invariant quantities", Ieee T. Commun., Vol. 29, no. 6, pp. 773-777, 1981.

[15] Y. Sung-Ming, and L. Kuo-Hong, "Shared authentication token secure against replay and weak key attacks", Inform. Process Lett., Vol. 62, no. 2, pp. 77-80, 1997.

[16] M. Kumar, "On the Weaknesses and Improvements of an Efficient Password Based Remote User Authentication Scheme Using Smart Cards", IACR Cryptology ePrint Archive, Vol. 163, 2004.

[17] H.-Y. Chien, J.-K. Jan, et al., "An efficient and practical solution to remote authentication: smart card", Computers & Security, Vol. 21, no. 4, pp. 372-375, 2002.

[18] E.-J. Yoon, E.-K. Ryu, et al., "Further improvement of an efficient password based

remote user authentication scheme using smart cards", Ieee T. Consum. Electronics, Vol. 50, no. 2, pp. 612-614, 2004.

[19] X.-M. Wang, W.-F. Zhang, et al., "Cryptanalysis and improvement on two efficient remote user authentication scheme using smart cards", Computer Standards & Interfaces, Vol. 29, no. 5, pp. 507-512, 2007.

[20] A. K. Awasthi, K. Srivastava, et al., "An improved timestamp-based remote user authentication scheme", Computers & Electrical Engineering, Vol. 37, no. 6, pp. 869-874, 2011.

[21] S. Kumari, M. K. Khan, et al., "An improved remote user authentication scheme with key agreement", Computers & Electrical Engineering, Vol. 40, no. 6, pp. 1997-2012, 2014.

[22] Y. F. Chang, W. L. Tai, et al., "Untraceable dynamic- identity- based remote user authentication scheme ش with verifiable password update", Int. J. Commun. Syst., Vol. 27, no. 11, pp. 3430-3440, 2014.

[23] Q. Jiang, S. Zeadally, et al., "Lightweight three-factor authentication and key agreement protocol for internet-integrated wireless sensor networks", Ieee Access., Vol. 5, pp. 3376-3392, 2017.

[24] P. Gope, and T. Hwang, "A Realistic Lightweight Anonymous Authentication Protocol for Securing Real-Time Application Data Access in Wireless Sensor Networks", Ieee T Indust Electronics, Vol. 63, no. 11, pp. 7124-7132, 2016.

Journal of "Innovations of Applied Information and Communication Technologies"
Vol. 1, No. 2, 2021 (Serial No. 2)

The Improvement of the Iris-Based Authentication by Presenting the Wireless Sensor Network Architecture to Maintain Industrial Internet of Things Privacy

K. Borna*, A. M. Ebadati, Sh. Zeinali
Kharazmi University, Tehran, Iran

Abstract

The Internet of Things provides instant access to information about the physical world and the objects within it, leading to new services and increasing efficiency and productivity. The wireless sensor network is an important network infrastructure in the Industrial Internet of Things and user authentication is used as a basic security mechanism to authenticate users to wireless sensor networks. In this article, we intend to provide a new way to improve the security of authentication using image processing. The analysis was performed by MATLAB software. The results presented in this article, which includes seven steps, have a 93% correct detection rate in pupil identification. These seven steps are: 1. Noise reduction, 2. Finding the outer border of the pupil, 3. Separating the eyelashes, 4. Finding the border of the eyelids, 5. Finding the outer border of the iris, 6. Separating the iris area and 7. Extracting the feature and encoding the pixels by the elliptic curve cryptography (ECC) method. With the measurements and experiments performed, it was found that the proposed method in identifying the eyelid border by the quadratic equation method is more efficient and faster in terms of time than the third-degree equation and the Huff parabolic conversion method. In order to extract the feature, the effective parameters in the SAIF feature extraction algorithm were examined and measured, and the optimal parameters were selected. The Sigma parameter with a value of 2.5 and the Octave parameter with a value of 4 should be considered as the best values. Also, in order to evaluate the resistance of the proposed method to error factors such as the angle, brightness and scale, the proposed method was tested and it was proved that the method has the appropriate resistance resolution in different conditions.

Keywords: Authentication, Wireless Sensor Networks, Privacy, Industrial Internet of Things, Image Processing

* Corresponding author E-mail: borna@khu.ac.ir