احراز هویت مبنی بر رمزنگاری متقارن برای سیستم‌های پرداخت الکترونیک

نگارش:

سجاد سروش

چکیده

بانکداری آنلاین و سیستم‌های پرداخت الکترونیکی در اینترنت به‌طور فزاینده‌ای پیشرفت می‌کنند. در سطح ماشین، تراکنش‌های بین مشتری و سرور میزبان از طریق یک کانال امن محافظت شده با SSL / TLS انجام می‌شود. احراز هویت کاربر معمولا براساس دو یا چند عامل است. با این وجود، توسعه بد افزارها مختلف و حمله‌های مهندسی اجتماعی کاربران کامپیوتر را به یک وسیله مورد اعتماد تبدیل می‌کند در نتیجه احراز هویت کاربر آسیب‌پذیر است. در این پایان نامه احراز هویت کاربر با بیومتریک در بانکداری آنلاین با استفاده از اثرانگشت را پیشنهاد می دهیم. در این پایان نامه نیاز دارد تا تأیید اعتبار نه تنها توسط کاربر (یا دستگاه شخصی) بلکه توسط بانک طبق استاندارد سیستم‌های بانکداری انجام شود. بنا به بیانی دقیق‌تر، یک پروتکل جدید برای تولید رمز عبور یک‌بار مصرف از داده‌های بیومتریک ارائه شده است، تا اطمینان حاصل شود امنیت و حریم خصوصی حفظ شده است. نتایج نشان می‌دهد با توجه به مثبت کاذب بودن نتایج عملکرد بهتری نسبت به روش های دیگر احراز هویت دارد. تجزیه و تحلیل امنیتی پروتکل نیز مزایای مربوط به تقویت امنیت را با بکارگیری روش های رمزنگاری کلید متقارن در این روش پیشنهادی نشان می‌دهد. روش پیشنهادی در مقابل انواع حملات بانکداری الکترونیکی همانند حملات سرقت گذر واژه و فیشینگ بسیار مقاوم می باشد.

مقدمه

در ابتدا برای حفظ امنیت سه مولفه محرمانگی، صحت و در د سترس پذیر بودن مطرح شد و برای ار ضای هریک از این مولفه‌ها راهکارهایی ارائه گردید و باعث به وجود آمدن پروتکل‌های رمزنگاریی گردید که امروزه از آن‌ها اســـتفاده می‌گردد ولی با گذ شت زمان مولفه‌های دیگری به این موارد ا ضافه گردید که از جمله عدم انکار، احراز هویت و احراز ا صالت که در این زمان با توجه به ر شد محیط‌های ارتباطات شبکه‌ای از اولویت‌های بالایی برخوردارند و در کنار سه مولفه قدیمی باید به ارضای آن‌ها نیز پرداخته شود[۱و۲].

حال جالب آن اســت که طیف بزرگی از پروتکل‌های رمز نگاری که در گذشــته طراحی شــدند قابلیت‌هایی فراتر از اهدافی سنتی محرمانگی، صحت و در د سترس بودن اطلاعات را دارا بودند ولی از آن‌ها به این صورت ا ستفاده نمی‌گردید ولی با ترکیب مدل‌های مختلف رمزنگاری مانند رمزنگاری متقارن با رمزنگاری نامتقارن به این پروتکل‌های پی‌شرفته د ست یافتند و امروزه به طور گســترده از آنها در کنار هم اســتفاده می‌شــود. مثلا امضــاهای دیجیتالی در پرداخت‌های الکترونیکی، شنا سنامه‌های دیجیتال که برای ن شان دادن هویت فرد و م شخ صات وی می‌با شد از کاربردهای پی شرفته این پروتکل‌ها می‌باشد.در این فصل به بررسی کلیات تحقیقات ،اعم از بیان مسئله،ضرورت و اهداف و فرضیات پرداخته خواهد شد.

بیان مسئله

در این تحقیق از رمزنگاری متقارن ا ستاندارد رمزنگاری داده (DES) یک الگوریتمی ریا ضی ا ست که برای رمزنگاری و رمزگ شایی اطلاعات کد شده باینری به کار می رود. رمزنگاری داده ها را تبدیل به داده های نامفهومی به نام cipher می کند. رمزگ شایی از cipher آن را به داده های ا صلی بازمی گرداند. الگوریتم مذکور هر دو عملیات رمزنگاری و رمزگ شایی را بر ا ساس یک عدد باینری به نام کلید م شخص می سازد. داده ها تنها در صورتی قابل بازیابی از cipher ه ستند که دقیقاً از کلیدی که برای رمزنگاری ا ستفاده شده برای رمزگ شایی نیز ا ستفاده شود. در DES طول قطعات ۶۴ بیت ا ست. کلید نیز شــامل ۶۴ بیت اســت ولی در عمل تنها از ۵۶ بیت آن اســتفاده می‌شــود و از ۸ بیت دیگر فقط برای چک کردن parityاستفاده می‌شود.

الگوریتم AES بایت به بایت کار می کند و ورودی اصــلی را با کلید رمزنگاری در یک ماتریس ۴×۴ جفت می کند. کلید، به طریقی تقسیم یا برنامه ریزی شده ا ست که بتواند در مراحل مختلف تکرار به تدریج تزریق شود. اولین قسمت کلید قبل از شروع پروسه ۱۰ مرحله ای تزریق می شود. در هر کدام از این مراحل، بایت ها جابجا می شوند، ردیف ها شیفت پیدا می کنند و ستونها ترکیب می شوند.

DES از نظر محا سباتی ساده‌ا ست و براحتی می‌تواند تو سط پردازنده‌های کند (بخ صوص آنهایی که در کارتهای هو شمند وجود دارند) بکار گرفته شوند. این روش ب ستگی به مخفی‌بودن کلید دارد. بنابراین ا ستفاده از این روش در دو ضعیت زیر مناسب است:

هنگامی که کلیدها می‌توانند با یک روش قابل اعتماد و امن توزیع و ذخیره شوند.

زمانی که کلید بین دو سیستم مبادله می‌شود، قبلا هویت همدیگر را تایید کرده باشند.

عمر کلیدها بی‌شتر از مدت تراکنش آنها طول نمی‌کشد. رمزنگاری DES عموما برای حفاظت دیتا از شنود در طول انتقال ا ستفاده می شود. کلیدهای DES ۴۰بیتی امروزه در عرض چندین ساعت تو سط کامپیوترهای معمولی شکسته می شوند و بنابراین نباید برای محافظت از اطلاعات مهم و جهت اعتبار طولانی مدت از آنها ا ستفاده شود. کلید ۵۶ بیتی عموما تو سط سخت‌افزار یا شبکه‌های بخ صو صی شکسته می شوند. AES جانشین DES می با شد. الگوریتمی که تو سط AES

توصیف می شود ، یک الگوریتم کلید متقارن است. به این معنا که از یک کلید مشابه برای رمز کردن و گشودن اطلاعات استفاده می شود AES.اولین رمزنگار رمز باز و قابل دسترس برای عموم است که توسط آژانس امنیت ملی NSA برای اطلاعات فوق محرمانه پذیرفته شد.

اهمیت و ضرورت تحقیق

بحث های زیادی شده که کدام یک از این الگوریتم‌ها بهترند اما جواب مشخصی ندارد. البته بررسی هایی روی این سوال شده به طور مثال دونفر به نام های Needham و Schroeder بعد از تحقیق به این نتیجه رسیدند که طول پیغامی که با الگوریتم‌های متقارن میتواند رمزنگاری شود از الگوریتم‌های نامتقارن کمتر است و با تحقیق به این نتیجه رسیدند که الگوریتم‌های متقارن الگوریتم‌های بهینه تری هستند. اما وقتی که بحث امنیت پیش می آید الگوریتم‌های نامتقارن کارایی بیشتری دارند. به طور خلاصه می‌توان گفت که الگوریتم‌های متقارن دارای سرعت بالاتر و الگوریتم‌های نامتقارن دارای امنیت بهتری هستند. در ضمن گاهی از سیستم ترکیبی از هر دو الگوریتم استفاده می‌کنند که به این الگوریتم‌ها الگوریتم های ترکیبی (hybrid) گفته می‌شود. اما اگر به طور دقیق تر به این دو نگاه کنیم آنگاه متوجه خواهیم شد که الگوریتم‌های نامتقارن و الگوریتم‌های کلید متقارن دارای دو ماهیت کاملاً متفاوت هستند و کاربردهای متفاوتی دارند به طور مثال در رمزنگاریهای ساده که حجم داده‌ها بسیار زیاد است از الگوریتم متقارن استفاده می شود زیرا داده‌ها با سرعت بالاتری رمزنگاری و رمزگشایی می شوند. اما در پروتکل هایی که در اینترنت استفاده می شود، برای رمز نگری کلید هایی که نیاز به مدیریت دارند از الگوریتم‌های نامتقارن استفاده می‌شود.با توجه به مباحث فوق می توان بیان داشت که لازم و ضروری است تا تحقیقات گسترده تری در حوزه مرتبط با موضوع انجام گیرد.

اهداف تحقیق

ایجاد امنیت در بستر بانکداری الکترونیکی جهت انجام تراکنش ها با حداکثر سرعت و دقت لازم

فرضیات تحقیق

۱. طول کلیدهای اولیه انتخاب شده p , q حداقل ۱۰ رقمی می باشد.
۲. احراز هویت در دو فاز ثبت نام و فاز بررسی انجام می گیرد.
۳. اطلاعات محرمانه ایجاد شده در حافظه کارت هوشمند ذخیره می گردد
۴. از توابع درهمسازی استاندارد SHA استفاده می کنیم.

رمز گذاری

در رمزنگاری هدف ساختن طرح‌ها یا پروتکل‌هایی است که بتوان با کمک آنها حتی در حضور دشمن نیز کارهای خاصی را انجام داد. یک هدف اساسی در رمزنگاری این است که به افراد این امکان را بدهند که روی یک کانال ناامن با حفظ حریم خصوصی و اصالت داده‌هایشان به صورت کاملاً امن با هم ارتباط برقرار کنند. به عنوان مثال فرض کنید که آلیس بخواهد از طریق اینترنت پیامی را برای باب ارسال کند. در حالت ایده‌آل می‌خواهیم که هیچ حمله کننده‌ای نتواند هیچ اطلاعاتی درباره پیام آلیس به‌دست آورد و همچنین نتواند هیچ تغییری در پیام آلیس بدون اینکه باب متوجه شود، ایجاد کند.

با وجود اینکه حفظ حریم خصوصی و اصالت داده‌ها یک هدف اصلی برای پروتکل‌های رمزنگاری است علاوه بر این امروزه علم رمزنگاری در موضـــوعات بســـیار زیاد دیگری مانند رأی‌گیری الکترونیکی، پول‌های الکترونیکی و مزایده‌های امن پیشرفت‌های قابل توجه‌ای کرده است و مسائل زیادی در این زمینه‌ها نیز مطرح شده است. در ادامه توضیح می‌دهیم که رمزنگاری چیست و چگونه می‌توانیم یک توجیه علمی برای امنیت طرح‌های رمزنگاری داشته باشیم.

سیستم های پرداخت

سیستم های پرداخت بخش حیاتی زیرساخت اقتصادی و مالی یک کشور هستند. عملکرد خوب آنها در انتقال امن و به موقع وجوه مهمترین اثر آنها در عملکرد کلی نظام اقتصاد می باشد. اما سیستم های پرداخت می‌توانند ریسک جدی برای مشترکین داشته باشند. به این ترتیب که این سیستم ها می توانند به صورت یک کانال، مشکلات را از یک قسمت از اقتصاد به بخش های دیگر منتقل کنند. این ریسک سیستماتیک دلیل اصلی توجه و علاقه بانک های مرکزی در طراحی و اپراتوری این سیستم ها می باشد[۲۸ الی ۳۰].

یک نظام پرداخت در واقع یک سری ترتیباتی است که اجازه می دهد که استفاده کنندگان پول را انتقال دهند. در حال حاضر در بسیاری از کشورهای پیشرفته پول عبارت است از سکه و اسکناس چاپ بانک مرکزی و طلب از موسسات اعتباری به شکل سپرده.

برای انجام پرداخت، پرداخت کننده می بایست درخواست خود را به بانکی که پول را در اختیار دارد، بدهد. این درخواست ممکن است به صورت کاغذی باشد مثل چک و یا به صورت الکترونیکی باشد مثل کارت های پلاستیکی.

در مرکز هر سیستم پرداخت ترتیباتی هست که انتقال پول را بین اعضای سیستم تسهیل می کند (واسطه هایی که مستقیم به سیستم و یا به یکدیگر متصل می شوند). بنابراین سیستم های پرداخت تشکیل شده اند از تعدادی از شبکه ها که اعضا را به هم پیوند می دهد، سوئیچ ها جهت توزیع پیغام ها و قانون و رویه جهت استفاده از این زیر ساخت به عبارت دقیق تر هر سیستم پرداختی شامل:

۱- استانداردهای فنی توافق شده و روش های انتقال پیغام ها بین اعضا

۲- یک ابزار توافق شده جهت تسویه طلب های اعضا از یکدیگر (مثل حساب در بانک مرکزی)

۳- یک مجموعه از قوانین و رویه های اجرایی

اهمیت سیستم های پرداخت

ســـالهای متمادی نحوه عملکرد و کارکرد نظام پرداخت به عنوان نگرانی و دغدغه بانکهای مرکزی مطرح نبود. عملیات این نظام بیشتر به عنوان یک فعالیت مکانیکی و پشت پرده مطرح بود که سیاست گذاری خاصی را نمی طلبید. این تفکر در حال حاضر تغییر پیدا کرده است. اقتصادهای مدرن در ۱۵ سال اخیر شاهد دو اتفاق بوده اند:

الف) رشد چشمگیر گردش پول در سیستم های پرداخت، هم از لحاظ تعداد مبادلات انجام شده و هم از لحاظ مقدار ارزش پول جابجا شده. این امر به علت رشد سریع فعالیت بازارهای مالی در سراسر جهان می باشد که پرداخت های مربوطه به تبع آن رشد کرده است.

ب) رشد چشمگیر تکنولوژی. از طریق این تکنولوژی وجوه می توانند از خلال سیستم های پرداخت بسیار سریع تر حرکت کنند.

در کشور انگلستان گردش نظام پرداخت ۴۲ برابر تولید ناخالص داخلی (GDP) سالانه این کشور می باشد. به بیان دیگر تنها شش روز کاری کافیست تا نظام پرداخت انگلستان ارزشی برابر با GDP کشور را پردازش نماید.

بنابراین هم اکنون توجه زیادی به نقش سیستم های پرداخت در اقتصاد بازار مبذول می شود. این اقبال جهانی از چند وجه قابل توجه می باشد:

۱. به عنوان بخش حیاتی زیرساخت مالی و اقتصاد
۲. به عنوان کانال لازم جهت مدیریت موثر اقتصادی، خصوصاً از لحاظ سیاست های پولی.
۳. به عنوان یک ابزار جهت ارتقا کارایی اقتصادی

انواع سیستم های پرداخت الکترونیکی

برخی از سیستم‌های پرداخت الکترونیکی که امروزه روی اینترنت استفاده و یا پیشنهاد شده‌اند، عبارتند از: سیستم های مبتنی بر کارت اعتباری، سیستم های مبتنی بر چک الکترونیکی، سیستم های مبتنی بر پول الکترونیکی، سیستم های ریز پرداخت، سیستم های مبتنی بر مزایده

ارزیابی ویژگی های سیستم های پرداخت الکترونیک

از ویژگی های سیستم های پرداخت الکترونیک، برای توصیف و ارزیابی سیستم های پرداخت الکترونیک استفاده شده است. ویژگی هایی که در این بررسی مورد بحث قرار گرفته به عنوان چارچوبی در جهت ارزیابی سیستم های پرداخت الکترونیک در نظر گرفته شده است. برخی از ویژگی های مزبور در ارائه تصویر مناسبی از معیارهای سیستم پرداخت الکترونیک موثر بوده و بهبود آنها کمک می نماید. اطلاعاتی که از این جنبه به دست می آید در حقیقت به عنوان ورودی‌های طراحی سیستم های پرداخت الکترونیک مورد استفاده قرار می‌گردد .

احراز هویت

شناسایی و احراز هویت دو هسته اصلی در بیشتر سیستم‌های کنترل دسترسی هستند. شناسایی عملی است که یک کاربر برای معرفی خود به یک سیستم اطلاعاتی استفاده می‌کند و که معمولاً در قالب یک نام کاربری و کلمه عبور است. احراز هویت اولین گام در فرایند اتصال است. هر سازمان یا شخصی نیاز به اتصال قابل اعتماد به سیستم و برنامه‌های کاربردیش دارد پس یک منبع تعیین هویت واحد و قابل اعتماد برای مدیریت دسترسی‌ها لازم است. بعد از فرایند احراز هویت اتصال برقرار می‌شود.

شناسایی در حقیقت برای پاسخگویی کاربر به اعمالی است که بر روی سیستم انجام می‌دهد. احرازهویت روشی است که براساس آن بررسی می‌شود که آیا طرف مقابل ارتباط همانی است که باید باشد یا یک نفوذگر است که خود را به جای طرف واقعی جازده است. بررسی هویت واقعی طرف مقابل ارتباط، عملی دشوار است.

در واقع حراز هویت یعنی تشخیص هویت فردی که می‌خواهد از امکانات یک سیستم یا شبکه استفاده کند و این اطمینان را می‌دهد که موجودیتی که در یک ارتباط شرکت کرده مجاز است یا نه. یکی بودن هویت کاربر با چیزی که ادعا کرده یعنی مجاز شناخته شدن آن کاربر. تنها از این طریق است که کاربر می‌تواند از سرویس‌ها و امکانات یک شبکه یا

سیستم استفاده کند. احراز هویت، هویت فرد را بوسیله مقایسه یک یا چند عامل با پایگاه دادهایی از هویت‌های معتبر، بررسی می‌کند. (یگانگی،۱۳۹۰).

در کل از۳ روش برای احراز هویت استفاده می‌شود. امروزه این ۳ روش را ۳ فاکتور احراز هویت گویند البته یک متدچهارم هم به آنها اضافه شده ولی می‌توان آن را در دسته‌های دیگر هم جای داد:[۱و۲]

1. **چیزی که شما می‌دانید. (رمز)**
2. **چیزی که شما دارید. (کارت شناسایی)**
3. **چیزی که شما هستید. (بیومتریک: اثرانگشت)**
4. **جایی که شما هستید. (محل شما را مشخص می‌کند)**

پیشینه تحقیقات

خرابی بالقوه شبکه های کامپیوتری بدلیل اعتماد روز افزون به اینترنت و ارتباطات وسیع تر در حال افزایش می باشد. سیستم های تشخصیص نفوذ (IDS) تبدیل به جزیی ضروری از امنیت شبکه برای تشخیص حملاتی که علیرغم وجود بهترین اقدامات محافظتی رخ می دهند، شده اند. مشکلی که سیستم های تشخیص نفوذ فعلی دارند این است که رویدادهای منفی و مثبت کاذب زیادی دارند. بیشتر سیستم های تشخیص نفوذ موجود بکار گرفته شده امروزی به سیستم‌های خبره مبتنی بر قاعده وابسته اند که حملات جدید در آنها قابل شناسایی نیستند.

یک برنامه ممکن از شبکه های عصبی به عنوان بخشی از یک سیستم تشخیص نفوذ معرفی شده است. یک سیستم تشخیص نفوذ بنام رد خدمات تشخیص هوشمند (DoSID) توسعه داده می شود. نوع شبکه عصبی بکار گرفته شده برای اعمال DoSID پیشخوری است که از الگوریتم آموزشی پس انتشار استفاده می کند. داده های بکار رفته برای آموزش و آزمون، داده های جمع آوری شده توسط آزمایشگاه لینکلن در دانشگاه ام آی تی برای ارزیابی یک سیستم تشخیص نفوذ تحت حمایت آژانس پروژه های تحقیقات پیشرفته دفاعی آمریکا می باشد. ویژگی های خاص سوابق اتصال برای استفاده در حملات رد خدمات (Dos) شناسایی شده اند. چندین آزمایش برای تست قابلیت شبکه های عصبی در متمایز کردن حملات شناخته شده و ناشناس از ترافیک معمولی انجام شده است. نتایج نشان می دهند که ترافیک عادی و حملات شناس به نسبت ۹۱ درصد و ۱۰۰ درصد تشخیص داده شده اند. همچنین در آخرین آزمایش نشان داده شد که منفی کاذب سیستم بطور قابل توجهی کاهش یافته است.

بیماران بدلیل رشد سریع فن آوری کامپیتوری می توانند بسیاری از خدمات طبی آنلاین را از طریق سیستم های اطلاعاتی مراقبت راه دور طبی (TMIS) در اختیار داشته باشند. بنابراین امنیت ارتباطات از طریق شبکه بین کاربر و سرور بسیار حائز اهمیت می باشد. احراز هویت نقش مهمی را در حفظ اطلاعات در برابر حملات مخرب برعهده دارد. اخیرا، جیانگ و همکارانش یک طرح بهبودی حریم خصوصی برای TMIS با استفاده از کارت های هوشمند ارائه داده اند و ادعا نموده اند که طرح آنها از طرح چن و همکارانش بهتر است. با این وجود، ما نشان دادیم که طرح جیانگ و همکارانش ضعف بی ثمر بودن ID را

داشته و در برابر حمله حدس زدن کلمه عبور آفلاین و حمله جعل هویت کاربر اگر مهاجم کارت هوشمند کاربر قانونی را به خطر بیاندازد. همچنین در مقابل حمله DoS در دو حالت نمی تواند مقاومت نماید: پس از یک حمله موفق جعل هویت و پسورد ورودی اشتباه در فاز تغییر پسورد. سپس یک طرح احراز هویت دوجانبه بهبود یافته مورد استفاده برای سیستم های اطلاعاتی مراقبت راه دور ارائه نمودیم. در حالتی که اطلاعات از طریق اینترنت انتقال می یابد، مراقبت راه دور، بررسی تاریخچه سابقه پزشکی قبلی بیمار و مشاوره راه دور را می توان بکار برد. در نهایت، تحلیل ما مشخص می نماید که طرح پیشنهادی بر نقات ضعف طرح جیانگ و همکارانش غلبه نموده و برای سیستم های اطلاعاتی مراقبت راه دور نیز عملی می باشد.

یک دهه و نیم است که اساس احراز هویت موضوعی برای تحقیق و مطالعه شده است. تلاشهای اولیه در تجزیه و تحلیل رسمی پروتکل های احراز هویت از منطق ذاتی استفاده نمی کردند اما یقینا منطقی نبودند. بازپرسی میلن پرولوگی مبتنی بر ابزار بود که بطور خاص برای تجزیه تحلیل پروتکل احراز هویتی طراحی شده که لزوما بعنوان مدل بررسی کننده برای مقاصد خاص عمل کرده است. کمرر از هدف کلی زبان مشخصات رسمی Ina Jo و یک ابزار سمبلیک همراهی کننده بنام Inatest برای مشخص کردن و تحلیل پروتکل ها استفاده نمود.

ما برروی منطق های احراز هویت که با BAN شروع می شود، تمرکز می کنیم. با این وجود ما تنها برروی منطق های ذاتی بحث نمی کنیم. همچنین به قافیه و دلیل احراز هویت، تلاش برای رسمی کردن و تعریف مفاهیم احراز هویت برای اعمال اینها را نیز در نظر خواهیم گرفت. در نتیجه ما منطق احراز هویت را در یک مفهوم گسترده تر بررسی می کنیم.

ما درباره روش های رسمی دیگر (بجز موارد اتفاقی) که برروی احراز هویت اعمال شده اند، بحث نمی‌کنیم. بطور خاص، ما فرایند جبری، ماشینی و ابزارهای اتوماتیک همانند تحلیلگر قضیه ها یا بررسی کننده مدل ها را شرح نخواهیم داد. برخی از این دیگر روش ها در جایی دیگر در این دوره بحث و بررسی شده اند. باقیمانده این قسمت پس زمینه ای بر پروتکل‌های احراز هویت ارائه نموده و یک مثال در حال اجرا را معرفی می نماید.

سیستم اطلاعاتی مراقبت راه دور طبی، خدمات تحویل مراقبت سلامتی را فعال یا حمایت می نماید. در سالهای اخیر، افزایش دسترسی سیستم های راه دور کم هزینه و دستگاه های نظارت فیزیولوژیکی سفارشی ساز برای بیماران این امر را ممکن ساخته است که مزایای پزشکی از راه دور را به مستقیما به خانه بیماران بیاورد. این سیستم ها به سمت محیطی حرکت می کنند که مدارک پزشکی خودکار بیمار و امکانات مراقبت راه دور پیوسته الکترونیکی در آنجا مرسوم است. بنابراین یک طرح احراز هویت ایمن برای محافظت از یکپارچگی داده ها، محرمانه بودن و در دسترس بودن، لازم است. طرح های بسیاری بر مبنای رمزنگاری برای این اهداف ارائه شده اند. با این وجود، بسیاری از این طرح ها در مقابل حملات مختلف آسیب پذیر بوده و نه موثراند و نه کاربردوست. بویژه در زمینه بهره وری، بسیاری از این طرح ها به محاسبات نمایی نیاز دارند که منجر به هزینه زمان بالا می شود. بنابراین ما طرح احراز هویت جدیدی را ارائه می نماییم که ایده پیش محاسبه را در طول فرایند

ارتباط برای جلوگیری از محاسبات نمایی زمان گیر ارائه می نماید. در نهایت، نشان داده شده است که برای محیط های مراقبت راه دور طبی ایمن و عملی است.

تضمین حریم خصوصی و امنیت کاربران در سیستم اطلاعاتی مراقبت راه دور طبی مهم است. اخیرا، وو (Wu) و همکارانش طرح احراز هویتی برای دستگاه های موبایل در سیستم اطلاعاتی مراقبت راه دور طبی ارائه نموده اند. آنها ایده پیش محاسبه را در طول فرایند ارتباط برای جلوگیری از محاسبات نمایی زمان گیر ارائه نموده اند. آنها همچنین ادعا می نمایند که طرح شان در برابر حملات مختلف می تواند مقاومت نماید. ما نشان خواهیم داد که طرح آنها متحمل حمله جعل هویت در حمله خودی است برای مقابله بر این نقاط ضعف ها ما طرح بهبود یافته ای ارائه می نماییم که این نقطه ضعف را از بین ببرد. طرح ما نه تنها از طرح آنها ایمن تر است بلکه عملکرد بهتری نیز دارد. و طرح ما کارا تر بوده و برای مرتب کردن دستگاه های موبایل با شارژ کم برای سیستم اطلاعاتی مراقبت راه دور طبی مناسب تر است.

سیستم اطلاعاتی مراقبت راه دور طبی، خدمات تحویل مراقبت سلامتی را فعال یا حمایت می نماید. بمنظور محافظت از حریم خصوصی بیمار، مانند شماره تلفن، شماره مدارک پزشکی، اطلاعات سلامت و ... یک طرح احراز هویت ایمن لازم است. اخیرا وو (Wu) و همکارانش طرح کارت هوشمند مبتنی بر تصدیق کلمه عبور در سیستم اطلاعاتی مراقبت راه دور طبی ارائه نموده اند. سپس هی و همکارانش اشاره نمودند که طرح وو (Wu) و همکارانش نمی تواند در مقابل حملات جعل هویتی و حملات خودی ها مقاومت نماید و طرح جدیدی ارائه نمودند. در این مقاله ما نشان خواهیم داد که هر دوی آنها در دستیابی به احراز هویت دو عامله آنچنان که طرح های کارت هوشمند مبتنی بر تصدیق کلمه عبور باید به آن برسند، شکست می خورند. همچنین طرح احراز هویت بهبود یافته ای برای سیستم اطلاعاتی مراقبت راه دور طبی ارائه می نماییم و نشان می دهیم که این طرح بهبود یافته، نیازهای امنیتی احراز هویتی دو عامله را بدست آورده و همچنین کارا است.

در این مقاله [۷]، برای تضمین حریم خصوصی بیمار مانند شماره تلفن، شماره مدارک پزشکی، اطلاعات سلامت و ... طرح های احراز هویت برای سیستم اطلاعاتی مراقبت راه دور طبی بصورت گسترده مورد مطالعه قرار گرفته است. اخیرا، ویی و همکارانش یک طرح احراز هویت کارا برای TMIS ارائه نموده و ادعا می نمایند که طرح شان در مقابل حملات مختلف مقاوم است. با این حال در این مقاله ما نشان خواهیم داد که طرح آنها در مقابل حمل حدس کلمه عبور آفلاین هنگامی که کارت هوشمند کاربر گم شده، آسیب پذیر است. برای افزایش امنیت، یک طرح امنیتی جدیدی برای TMIS ارائه نموده ایم. نتایج نشان داده است که طرح ما می تواند بر نقاط ضعف طرح ویی و همکارانش غلبه کرده و عملکرد بهتری نسبت به طرح آنها از خود نشان می دهد.

سیستم اطلاعاتی مراقبت راه دور طبی قصد دارد خدمات راه دور را بنا ساخته و عموم مردم را قادر سازد تا به خدمات یا اطلاعات پزشکی از سایت های دور دسترسی داشته باشند. احراز هویت و توافق کلیدی برای اطمینان از یکپارچگی داده، محرمانه بودن و در دسترس بودن برای TMIS ضروری است. اخیرا، چن و همکارانش یک طرح احراز هویت کارا و ایمن پویای مبتنی بر ID برای TMIS ارائه نموده و مدعی هستند که طرح آنها به هدف ناشناس بودن کاربر دست یافته است. هرچند ما مشاهده نمودیم که طرح آنها نه به ناشناس بودن کاربر و نه به غیر قابل ردیابی بودن دست یافته و در معرض حمله حدس هویت و ردیابی می باشد. بمنظور حمایت از حفظ حریم خصوصی کاربر ما یک طرح احراز هویت پیشرفته را ارائه می

نماییم که هم به ناشناس بودن کاربر و هم به غیرقابل ردیاب بودن دست می یابد. این طرح احراز هویت، طرحی کارا و ایمن با حفظ حریم خصوصی کاربر بوده که برای TMIS کاربردی می باشد.

جهت اطمینان از تنها دسترسی مجاز به خدمات پزشکی، چندین طرح احراز هویت برای TMIS بصورت نوشته ارائه شده اند. بدلیل عملکرد بهتر آن نسبت به رمزنگاری سنتی، هائو و همکارانش یک طرح احراز هویت برای TMIS با استفاده از نقشه بی نظمی مبتنی بر رمزنگاری ارائه نمودند. آنها مدعی هستند که طرح شان می تواند در مقابل حملات گوناگون من جمله حمله کارت هوشمند به سرقت رفته مقاومت نماید. با این وجود ما تشخیص دادیم که طرح آنها در برابر حمله کارت هوشمند به سرقت رفته آسیب پذیر می باشد. دلیل بوجود آمدن حمله کارت هوشمند به سرقت رفته این است که این طرح بر مبنای این فرضیه طراحی شده که خود طرح به هدف غیر قابل ردیابی بودن کاربر دست یافته است. پس ما یک طرح احراز هویت قوی و توافق کلیدی ارائه نمودیم. در مقایسه با طرح های گذشته، طرح ما نه تنها شامل ویژگی های امنیتی بیشتری می شود بلکه بهره وری بهتری نیز دارد. تحلیل ما نشان می دهدکه طراحی یک طرح احراز هویت دو عامله بر مبنای اینکه حفظ حریم خصوصی در خود طرح بدست آمده ممکن است خطرات امنیتی بالقوه ای را وضع نماید. درسی که ما آموختیم این است که باید از این وضعیت در طرح های آینده طرح های احراز هویت دو عامله پیشگیری نماییم.

سیستم اطلاعاتی مراقبت راه دور طبی، ارائه خدمات مراقبت های پزشکی را ممکن می سازد. با این وجود، دسترسی این خدمات از کانال های عمومی مشکلات امنیتی و حریم خصوصی را بالا می برد. در سال های اخیر، چندین طرح احراز هویت مبتنی بر کارت هوشمند برای اطمینان از ارتباط ایمن و مجاز بین نهادهای راه دور از طریق کانال های عمومی برای TMIS معرفی شده اند. ما امنیت برخی از طرح های احراز هویت ارائه شده در این مدت اخیر لین، ژی و همکارانش، چائو و ژای، و وو و ژوو را برای TMIS تجزیه و تحلیل می کنیم. برای ما مشخص گردید که این طرح ها در دستیابی به ویژگی‌های امنیتی مورد دلخواه شکست خوردند. در این مقاله ما بطور خلاصه چهار طرح پویای احراز هویت مبتنی بر ID را مورد بحث قرار داده و ضعف آنها در دستیابی به ویژگی های امنیتی را نشان خواهیم داد. هدف این تحقیق این است که نشان دهد چطور مرحله تغییر کلمه عبور ناکارآمد می تواند به رد سناریوهای سرور برای یک کاربر مجاز منجر شده و چطور مرحله ورود به سیستم ناکارآمد منجر به بروز ارتباطات و محاسبات سربار شده و عملکرد سیستم را کاهش می دهد. علاوه براین ما آسیب پذیری طرح چائو و ژای در برابر حمله اطلاعات موقت خاص دور شناس، آسیب پذیری طرح وو و ژو به حمله تشخیص کلمه عبور آفلاین و آسیب پذیری طرح ژی و همکارانش به حمله حدس پسورد آنلاین غیر قابل ردیابی نشان خواهیم داد.

طرح های احراز هویت برای سیستم اطلاعاتی مراقبت راه دور طبی TMIS تلاش می کنند تا از دسترسی ایمن و مجاز مطمئن گردند. طرح های احراز هویت مبتنی بر ID ارتباطات ایمن را هدف گرفته اما حریم خصوصی به درستی هدف گرفته نشده است. اخیرا، برای TMIS طرح های احراز هویت کاربر راه دور پویای مبتنی بر ID جهت حمایت از حریم خصوصی کاربر ارائه شده است. طرح های احراز هویت پویای مبتنی بر ID بطور موثری از حریم خصوصی کاربر محافظت می نمایند. متاسفانه، بیشتر طرح های احراز هویت پویای مبتنی بر ID موجود برای سیستم TMIS شرط تأیید ورودی را نادیده می‌گیرند. این امر مراحل ورود به سیستم و تغییر کلمه عبور را ناکارآمد می سازد. ناکارآمدی مرحله تغییر کلمه عبور می تواند به حمله DoS در صورت ورودی اشتباه در مرحله تغییر کلمه عبور منجر گردد. برای غلبه بر این نقاط ضعف ما طرح احراز هویتی پویای مبتنی بر ID با استفاده از کارت هوشمند ارائه نموده ایم. این طرح ارائه شده می تواند بسرعت ورودی داده اشتباه را شناسایی نموده که موجب می گردد مرحله ورودی به سیستم و تغییر کلمه عبور کارآمد گردند. ما این طرح را با هدف محافظت از حریم خصوصی و مراحل کارآمد ورودی به سیستم و تغییر پسورد بکار گرفتیم. این طرح همچنین در برابر حمله

تشخیص کلمه عبور آفلاین و حمله DoS مقاوم است. ما همچنین اعتبار طرح ارائه شده را با استفاده از منطق BAN (بوروز، آبادی و نیدهام) که بطور گسترده پذیرفته شده نشان می دهیم. علاوه براین، طرح ما به لحاظ سربار ارتباطات و محاسبات با طرح های مربوطه برای TMIS قابل مقایسه می باشد.

مقایسه تکنولوژی های زیست سنجشی

قبل از مقایسه تکنولوژی های بیومتریک،نیاز به تعریف پارامتر های اندازه گیری برای این تکنولوژی ها داریم. این پارامترها عبارتند از:

- عمومیت یا فراگیری: تعداد افرادی که شامل این ویژگی هستند را مشخص می کند.
- یکتایی: احتمال اینکه دو فرد متفاوت دارای یک ویژگی برابر نباشند توسط این ویژگی بیان می شود.هر چه قدر میزان این ویژگی بیشتر بیان شده باشد میزان یکتایی افراد بر اساس این ویژگی بیشتر است.
- دوام و بقا: تغییر نکردن ویژگی را با گذر زمان مشخص می کند.
- جمع آوری : راحتی جمع آوری و اندازه گیری ویژگی را بیان می کند.این ویژگی را قابلیت ارزیابی نیز نامیده اند.
- کارایی : میزان دقت و مقبول بودن نتایج سیستم ما را نشان می دهد.
- مقبولیت: میزان علاقه مردم به استفاده از تکنولوژی مورد نظر را نشان می دهد.
- دور زدن: پایین بودن امکان تقلب و دور زدن سیستم را توسط فرد غیرمجاز نشان می دهد.

دلایل فراگیر شدن تشخیص اثر انگشت

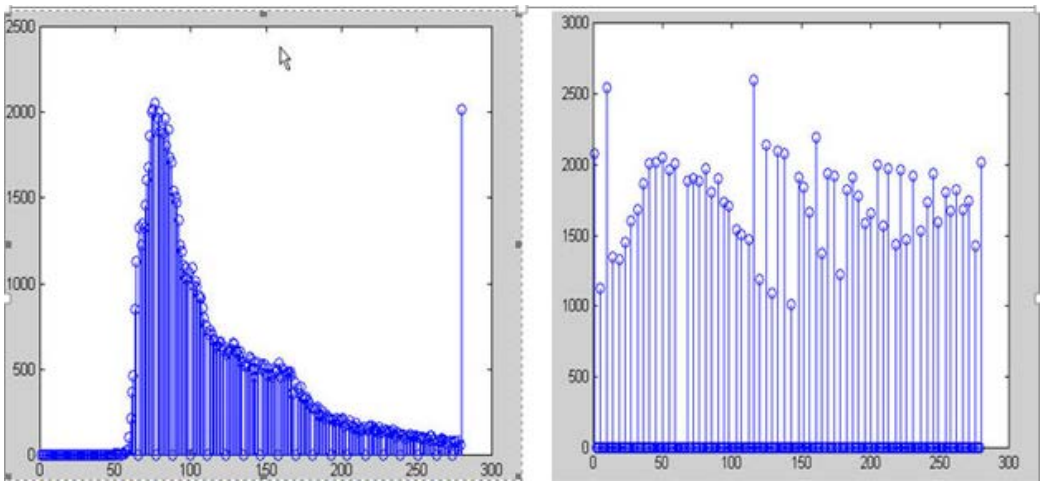
مهم ترین دلایل فراگیر شدن تشخیص اثر انگشت عبارت است از:

- موفقیت این شیوه در کاربرد های مختلف قضایی،دولتی،تجاری و... در حدی که حتی در تلفن های همراه جدید نیز استفاده می شود.
- باقی ماندن اثر انگشت مجرمان در صحنه جرم دلیل دیگر استفاده از این روش است .
- وجود پایگاه داده کاملی از آثار انگشت(به طوری که تا سال ۲۰۰۰ بیش از ۷۰ میلیون اثر انگشت مختلف در پایگاه داده FBI موجود بوده است) .
- وجود دستگاه های ثبت اثر انگشت ارزان قیمت و کم حجم آزمایش‌ها

قبل از توضیح در مورد روش پیاده سازی،به معرفی مجموعه دادگان می پردازیم.مجموعه دادگانی که در اینجا استفاده می شود، FVC نام دارد. این دادگان توسط دانشگاه بلونیا ایتالیا تهیه شده است و هر دو سال نسبت به بهبود آن اقدام میگردد.برای تهیه این دادگان، از ۱۰ انگشت و به ازای هر انگشت،هشت اثر انگشت استفاده شده است.این آثار انگشت،توسط حسگر نوری و وضوح بالای ۵۰۰dpi تهیه شده است. اولین مرحله پس از بارگذاری عکس،پیش پردازش است.این مرحله خود از دو زیر مرحله زیر تشکیل شده است:

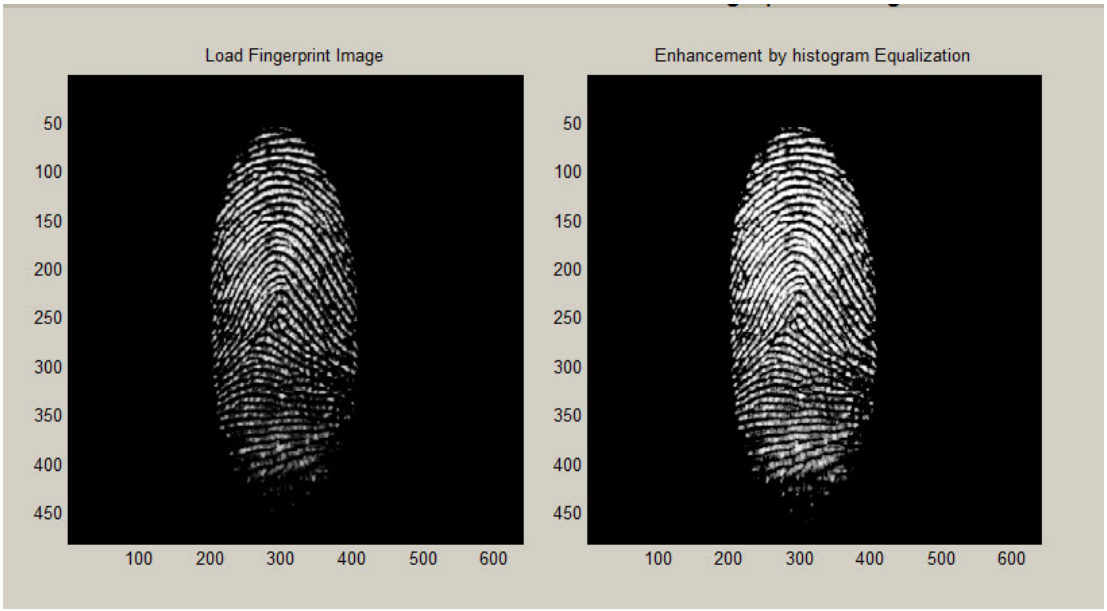
برابر سازی

در این مرحله با تبدیل مقادیر کم،به صفر و افزایش مقادیر زیاد باعث افزایش تفاوت(کنتراست)در عکس می شویم که باعث بهبود تشخیص خطوط اصطکاکی نسبت به زمینه سفید عکس می شود.



شکل (۳-۱) هیستوگرام

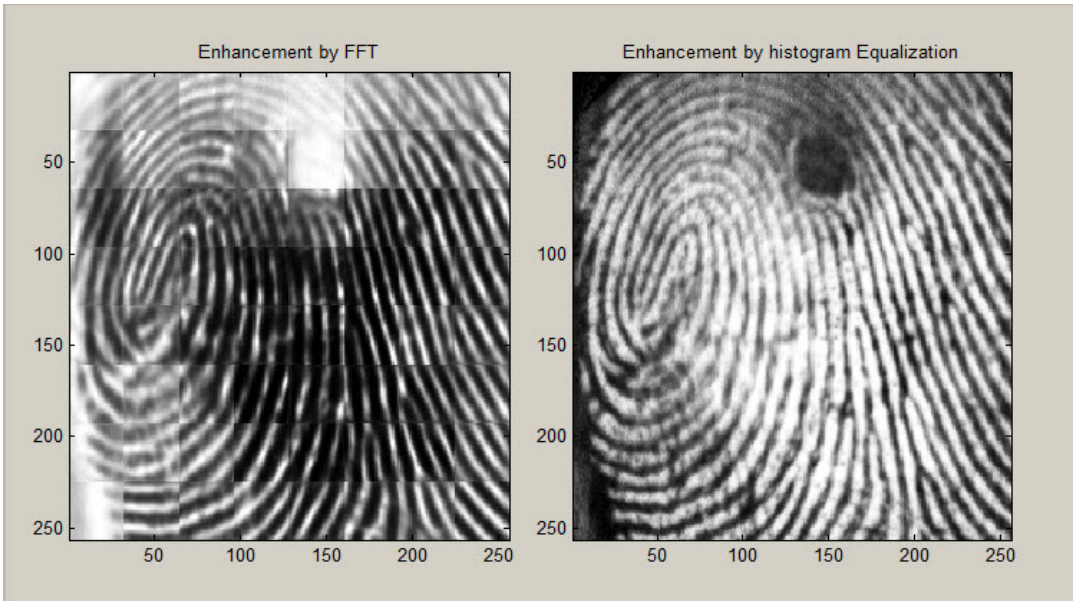
شکل(۳-۲) تفاوت عکس قبل و بعد از اجرای این مرحله را نمایش می دهد.



شکل (۳-۲) بهبود اثر انگشت با متعادل سازی هیستوگرام

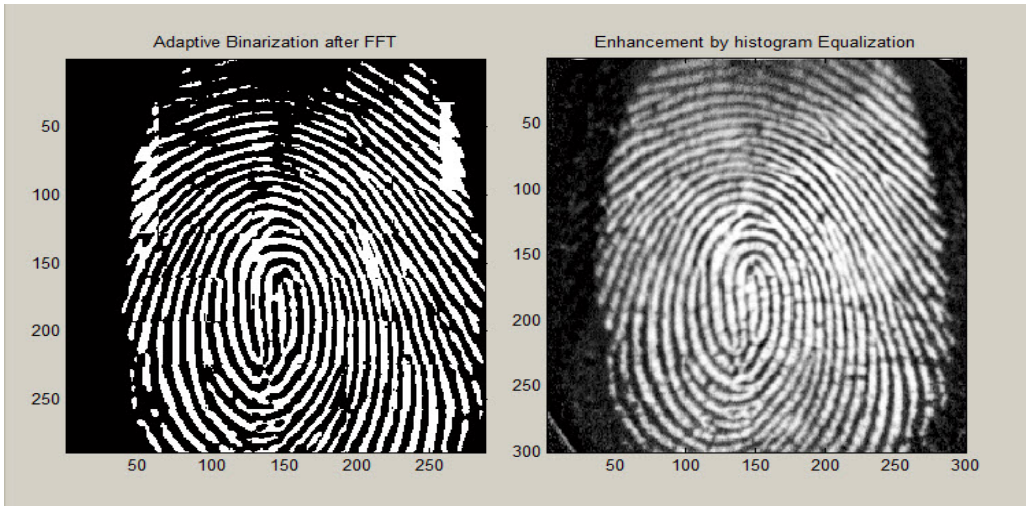
تبدیل سریع فوریه

توسط این مرحله،عکس تبدیل به قسمت های ۳۲ در۳۲ پیکسلی شده،سپس پردازش بر روی هر قسمت به صورت موازی اجرا می شود. مقدار k در بازه مابین صفر تا ۱ اختیار می شود که طبق محاسبات تجربی بهترین نتایج با مقدار k=۰,۴۵ به دست آمده است. در شکل (۳-۴) تفاوت ایجاد شده پس از اجرای این مرحله در عکس، نمایش داده شده است:



شکل (۳-۳) بهبود سازی اثرانگشت به کمک تبدیل فوریه

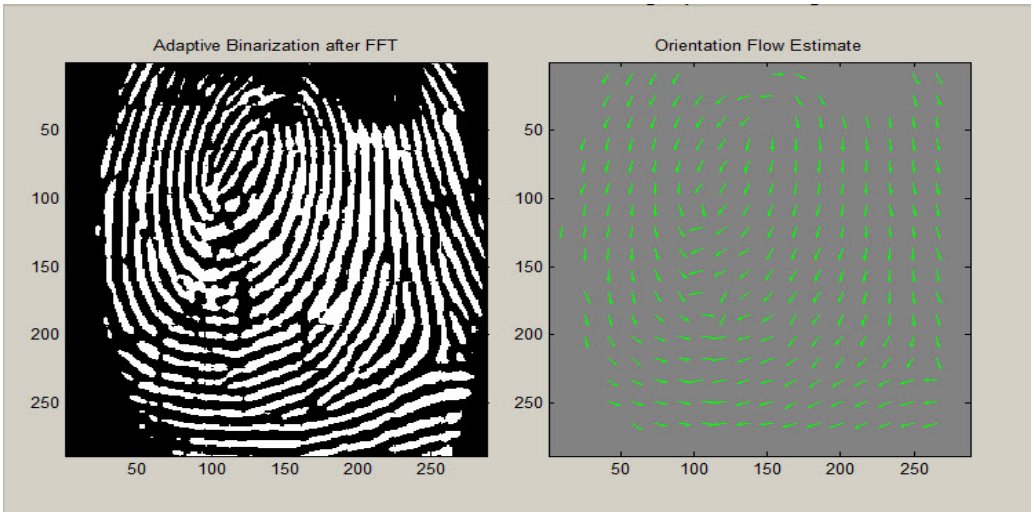
پس از پیش پردازش، نوبت به باینری کردن تصاویر می رسد.در این فاز تصویر را به بلاک های ۱۶در۱۶ پیکسلی تقسیم می کند.سپس مقدار هر پیکسل را با میانگین هر بلاک مقایسه می کند، اگر مقدارپیکسل، بیشتر از میانگین باشد مقدار آن پیکسل تبدیل به ۱ و اگر کمتر باشد مقدار آن پیکسل تبدیل به صفر می شود. شکل (۳-۵) تاثیر این قسمت را نمایش می دهد:



شکل (۳-۴) بهبود سازی اثر انگشت به کمک باینری سازی تطبیقی

پس از باینری کردن،نوبت به بخش بندی تصاویر می رسد.در این قسمت،سعی می شود به نواحی مورد علاقه توجه شود.به این معنا که این نواحی حاوی رگه شناسایی، و سایر نواحی که فقط حاوی تصویر زمینه هستند حذف می شوند. این قسمت خود تقسیم به دو زیر مرحله می شود:

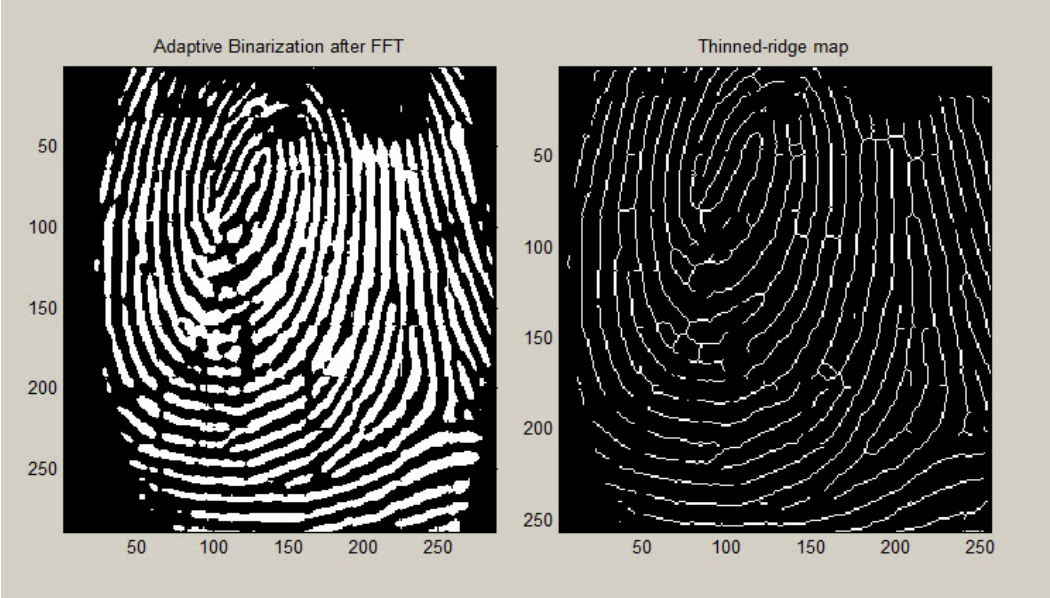
پیش بینی جهت بلاک : ابتدا یک بلاک wدرw پیکسلی (با مقدار پیش فرض۱۶در۱۶) انتخاب شده و مقادیر گرادیان محور x و y برای آن محاسبه می شود. برای این منظور از دو فیلتر سوبل استفاده می شود. سپس برای هر بلاک،حداقل مربعاتِ جهت بلاک محاسبه می شود. با محاسبه گرادیان های محور افقی و عمودی،می توان توسط این فرمول، مقدار E را حساب کرد و مقداری که کمتر از حد آستانه هستند را به عنوان تصویر پشت زمینه در نظر گرفته و حذف نمود. شکل زیر،تاثیر این قسمت از پروژه را نمایش می دهد:



شکل (۳-۵) تخمین جهت های اثر انگشت

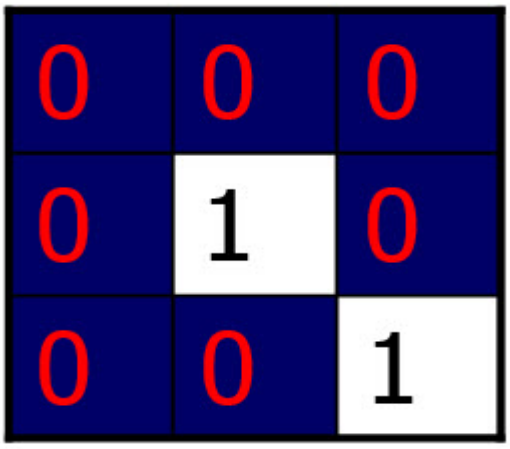
اجرای عملگرهای مورفولوژیک

این عملگر ها به دو عملگر باز که وظیفه حذف نویز پشت زمینه و عملگر بسته که برای یک دست کردن ناحیه استفاده می شود تقسیم می شوند. پس از بخش بندی تصاویر،استخراج مینوشیا آغاز می شود.مرحله اول در استخراج مینوشیا، نازک سازی تصاویر است برای این منظور عرض خطوط اصطکاکی را تا زمانی که عرض آنها برابر با یک پیکسل شود کم می‌کنیم. برای این منظور عکس را به بلاک ها ۳ در۳ پیکسلی تقسیم می کنیم. پیکسل های درون این بلاک را بررسی کرده و پیکسلی که نسبت به بقیه پیکسل ها بی ربط باشد را حذف می‌کنیم(برای درک بهتر می توان گفت پیکسلی که خارجی ترین پیکسل سیاه است حذف می شود) شکل زیر تاثیر این قسمت را بر روی عکس نمایش می دهد:



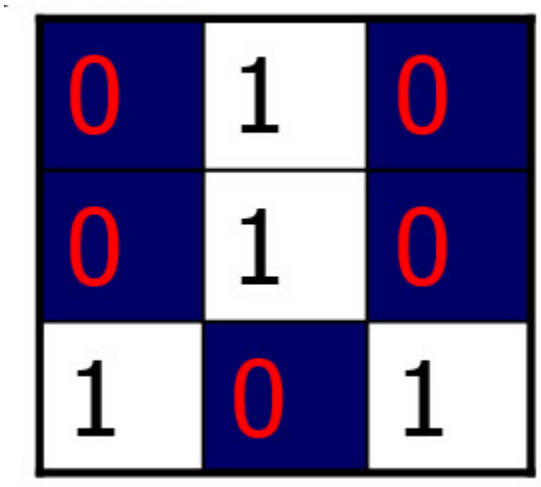
شکل (۳-۶) نگاشت thinned - ridge

سپس مینوشیا های استخراج شده را علامت گذاری می کنیم.برای این منظور،تصویر را به بلاک های ۳*۳ تقسیم کرده،اگر مقدار نقطه میانی یک و مقدار یک پیکسل دیگر نیز یک باشد،شکل حاصل نقطه پایانی است:



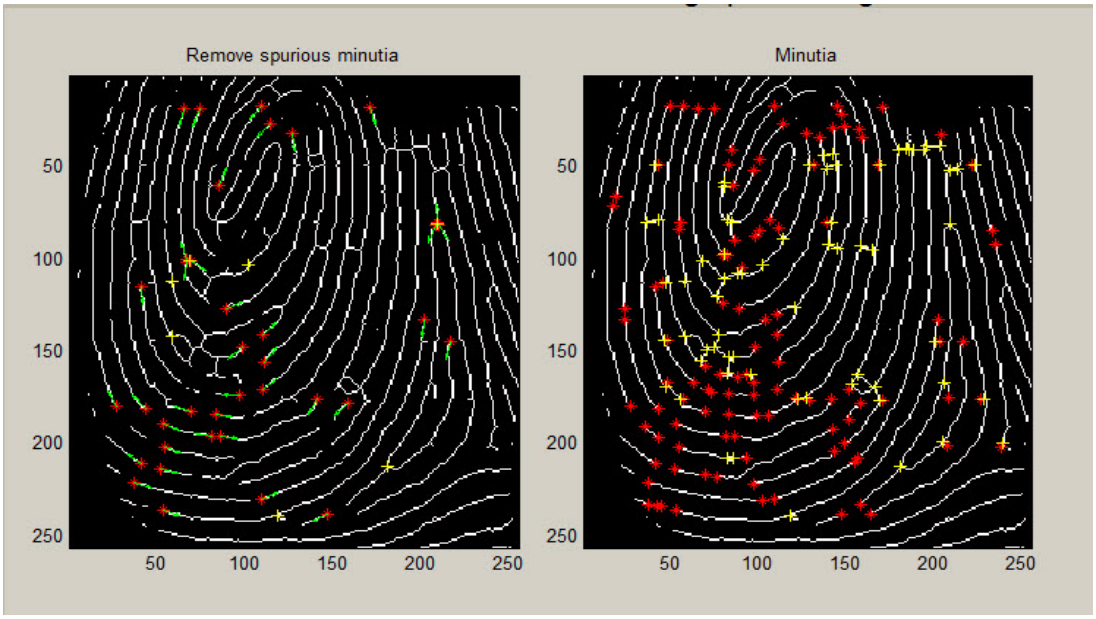
شکل (۳-۷) ماسک ۳×۳

اگر نقطه میانی مقدار یک و دقیقا سه پیکسل دیگر نیز با مقدار یک نیز وجود داشته باشد، شکل حاصل نشانگر دوشاخگی است:



شکل (۳-۸) دوشاخگی در یک ماسک ۳×۳

علاوه بر این تابع،فاصله بین دو نقطه پایانی محاسبه می شود. اگر مقدار آن کمتر از مقدار آستانه D باشد، فقط یکی از نقاط به عنوان نقطه انتهایی در نظر گرفته می شود و نقطه دیگر حذف می شود. شکل زیر این کاهش را نمایش می دهد:



شکل (۳-۹) جداسازی مینوشیا اصلی

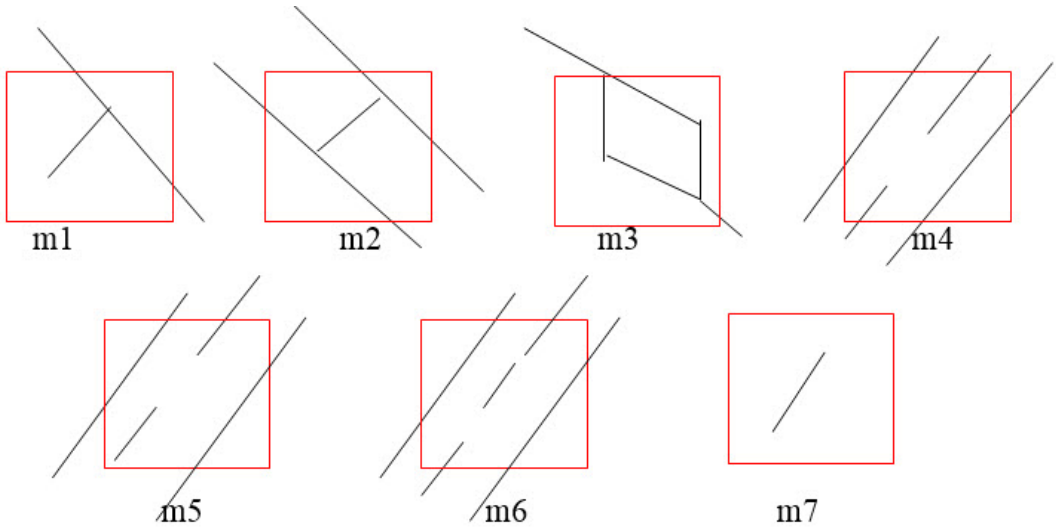
در نتیجه توسط این الگوریتم علامت گذاری،تمام نقاط پایانی با یک شناسه منحصر به فرد مشخص می‌شود. این شناسه توسط تابع BWLABEL به هر کدام از این نقاط اختصاص داده می شود. نقاط به دست آمده، در یک فایل با پسوند .dat ذخیره می شوند.برای عملیات تطبیق دو اثر انگشت،فایل مربوط به هر اثر انگشت توسط تابع match_end خوانده و با یکدیگر مقایسه می شود.

پس پردازش مینوشیا

پیش پردازش داده ها به تنهایی نمی تواند تمام عیوبی که هنگام ثبت اثر انگشت به وجود آمده است را از بین ببرد. به همین دلیل نیاز به یک پردازش مجزا بعد از یافتن مینوشیای اثر انگشت احساس می شود.این مرحله در دو قسمت اجرا می شود:

حذف مینوشیای اشتباه

با توجه به اینکه ساز و کار احراز هویت در این پروژه،توسط مینوشیا مشخص می شود.تشخیص و از بین بردن مینوشیا های اشتباه بسیار حیاتی به نظر می رسد.حالات مختلفی می تواند باعث تشخیص اشتباه مینوشیا شود.مثلا ایجاد بریدگی و زخم و...شکل زیر تعدادی از این حالات را مشخص می کند.



شکل (۳-۱۰) حالات مختلف مینوشیا

در این پروژه حذف مینوشیا به صورت زیر انجام می شود:اگر فاصله یک دوشاخگی و یک نقطه پایانی کمتر از مقدار آستانه D بود ،هر دوی آنها در راستای یک رگه هستند و هر دو حذف می شوند.

اگر فاصله دو دوشاخگی کمتر از D باشد و هر دو روی یک لبه قرار داشته باشند هر دو حذف می شوند.

اگر دو نقطه پایانی در فاصله کمتر از D باشند و جهت آنها تقریبا با یکدیگر در یک راستا باشدهمانندm4، m5 وm6 مینوشیای به دست آمده به دلیل خراشیدگی یک لبه به وجود آمده و تمام این نقاط حذف می شوند.

اگر فاصله دو مینوشیا کمتر از مقدار D باشد یعنی طول لبه ای که حاوی این دو مینوشیا است کمتر از D باشد،هر دو مینوشیا حذف می شوند. شکل m7 .

۲-۴-۴-۳- یکی کردن نقاط پایانی و دو شاخگی

با توجه به اینکه کوچکترین تغییری در وضعیت اثر انگشت یا حسگر ها،نوع مینوشیای تشخیص داده شده را تغییر می دهد،توصیه می شود نقاط پایانی و دوشاخگی با یکدیگر یکی شده و مینوشیا ها توسط مکانشان (x,y) و جهت آنها شناسایی شوند. بیان این نکته لازم است که محاسبه جهت یک دوشاخگی چالش های خاص خود را دارد که بیان آن در این مطلب ضروری نیست.

۵-۴-۳- انطباق مینوشیا

آخرین قسمت برای احراز هویت،انطباق مینوشیاهای اثر انگشت با مینوشیاهای آثار انگشت درون پایگاه داده است. انطباق دو اثر انگشت در اینجا توسط تطبیق مینوشیا های تراز شده انجام می شود و دو مرحله دارد.

۱-۵-۴-۳- مرحله تراز کردن

از هر تصویر یک مینوشیا انتخاب می شود و شباهت میان رگه های این مینوشیا با رگه مینوشیای دیگر مقایسه می شود . اگر میزان شباهت از یک حد آستانه بالاتر باشد،این دو مینوشیا منتخب شده و در اصل یکی در نظر گرفته می شوند و دو تصویر توسط این دو مینوشیا تطبیق داده می شوند.منظور از تطبیق تغییر محور مختصات و زاویه های مینوشیای دو عکس است به طوریکه این دو مینوشیای منتخب دو عکس بر روی هم کاملا منطبق شوند.

۲-۵-۴-۳- مرحله تطبیق

پس از تراز کردن،از یک عکس یک مینوشیا انتخاب شده و مینوشیای با x,y نزدیک به آن در عکس دیگر نیز انتخاب می شود.اگر زاویه مابین جهت این دو مینوشیا کمتر از یک حد آستانه باشد،این دو مینوشیا یکسان در نظر گرفته می شوند. سپس نسبت تعداد مینوشیای یکسان را به تعداد کل مینوشیای درون تصاویر بر حسب درصد حساب کرده و آنرا به عنوان امتیاز برمیگرداند.امتیاز حاصل با حد آستانه مقایسه می شود و اگر مقدار آن بالاتر باشد دو اثر انگشت یکی در نظر گرفته می شوند.

تجزیه و تحلیل عملکرد

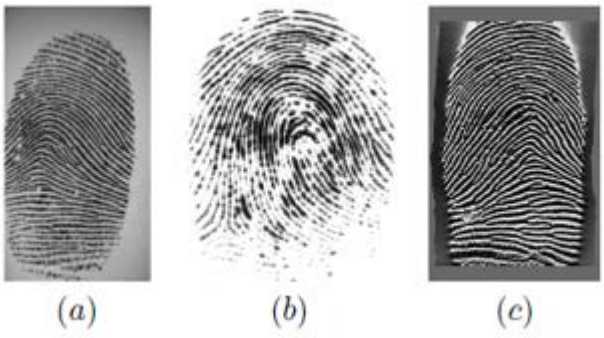
در این بخش، عملکرد پروتکل را برای جلوگیری از رد اشتباه و نادرست تجزیه و تحلیل می‌کنیم. با تعریف تجربی پروتکل شروع می‌کنیم.

۱) پروتکل تجربی: در این مطالعه، از سه پایگاه داده اثر انگشت استفاده شده است که، هر کدام از ۸۰۰ عکس از ۱۰۰ نفر با ۸ نمونه از هر کاربر تشکیل شده است:

- پایگاه داده معیار FVC2002 DB2: وضوح تصویر ۲۹۶ × ۵۶۰ پیکسل با حسگر نوری "FX2000" توسط Biometrika؛
- پایگاه داده معیار FVC2004 DB1: وضوح تصویر ۶۴۰ × ۴۸۰ پیکسل با سنسور نوری "V300" توسط CrossMatch؛
- پایگاه داده معیار FVC2004 DB3: وضوح تصویر ۳۰۰ تا ۴۸۰ پیکسل با سنسور حرارتی فراخوانی است "FingerChip FCD4B14CB" توسط Atmel.

شکل (۶-۱) یک تصویر از هر پایگاه داده ارائه می‌دهد. ما می‌توانیم ببینیم که اثرانگشت‌ها کاملا متفاوت و نمایشی از انواع مختلف اثرانگشت (به دست آمده از سنسورها با استفاده از فن‌آوری‌های مختلف) است.

این پایگاه داده‌ها برای مسابقات (رقابت برای تایید اثر انگشت) در سال های ۲۰۰۲ و ۲۰۰۴ استفاده شده است. جدول (۶-۱) عملکرد بهترین الگوریتم‌ها بر روی این پایگاه داده‌ها را نشان می‌دهد. نرخ خطای برابر (EER) نرخ خطای سازش را زمانی که کاربران واقعی به اشتباه رد می‌شوند و فریبکارانه پذیرفته می‌شوند محاسبه می‌کند.



شکل (۵–۱) یک نمونه از اثر انگشت از هر پایگاه داده

ZeroFRM مقدار False Non Match Rate (FNMR) است هنگامی‌که هیچ موردی به‌صورت اشتباه پذیرفته نشده باشد. این مقادیر پیچیدگی هر پایگاه‌داده و برخی از عناصر عملکردی که می‌توانیم در این پایگاه‌داده‌ها انتظار داشته باشیم تعریف می‌کند.

جدول(۵–۱) عملکرد بهترین الگوریتم برای هر پایگاه داده

Database	EER	ZERO FMR
CASIA V3	0.12%	0.23%
CASIA V4	0.31%	0.68%
CASIA V5	1.15%	2.45%

همانند FingerCode، از ویژگی‌های گابور (GABOR) [۱۸] با اندازه n = 512 (۱۶ مقیاس و ۱۶ جهت) به‌عنوان الگو استفاده می‌کنیم. این ویژگی‌ها به خوبی شناخته شده هستند و اجازه می‌دهند تا تجزیه و تحلیل بافت یک اثر انگشت به خوبی انجام شود. برای هر کاربر از اولین نمونه FingerCode به‌عنوان قالب مرجع استفاده کردیم. اثرانگشت‌های دیگر برای تست طرح پیشنهاد شده استفاده می‌شوند. BioCodes به اندازه ۲۵۶ بیت است. برای ارزیابی عملکرد روش بیومتریک یک‌باره، ۱۰۰۰ مقایسه را (با فاصله هامینگ) بین چالش BioCode مرجع و چالش ثبت BioCode برای هر کاربر محاسبه کردیم. ۱۰۰,۰۰۰ امتیاز بین کلاسی و درون کلاسی را برای تجزیه و تحلیل عملکرد طرح پیشنهادی به دست آوردیم.

۲) نتایج تجربی: ما پروتکل قبلی را به راه‌حل پیشنهادی اعمال کردیم. در سه پایگاه‌داده، مقدار EER نزدیک به ۰٪ رسید. که به منظور نشان دادن این کارایی، که در شکل ۷ توزیع امتیازات درون کلاسی و بین کلاسی برای هر پایگاه داده نشان داده شده است. ما به وضوح می‌بینیم که هیچ همپوشانی بین آن دو توزیع و آستانه در نزدیکی ۶۰ (بدین معنی که حداکثر ۶۰ بیت متفاوت بین ثبت و مرجع BioCodes تحمل می‌شود) وجود ندارد و می‌تواند مورد استفاده قرار گیرد. در ستون آخر از جدول(۶–۲) ، ارزیابی مقدار EER را با در اختیار داشتن دستگاه OffPAD و رمز عبور کاربر (بدترین حالت) ارائه می‌دهیم. در این مورد، فریبکار می‌تواند با ارائه بیومتریک خود، تلاش کنید داده‌ها برای جعل هویت کاربر واقعی به کار

ببرد. ما ۱۰۰,۰۰۰ حمله را برای هر پایگاه داده آزمایش کردیم و این حمله در ۱۶٪ تا ۲۵٪ موارد موفقیت آمیز بود. در رویکردهای کلاسیک (تأیید اعتبار با دو عامل)، این حمله همیشه موفق است.

جدول (۵–۲) عملکرد الگوریتم پیشنهادی دشمن هر پایگاه داده

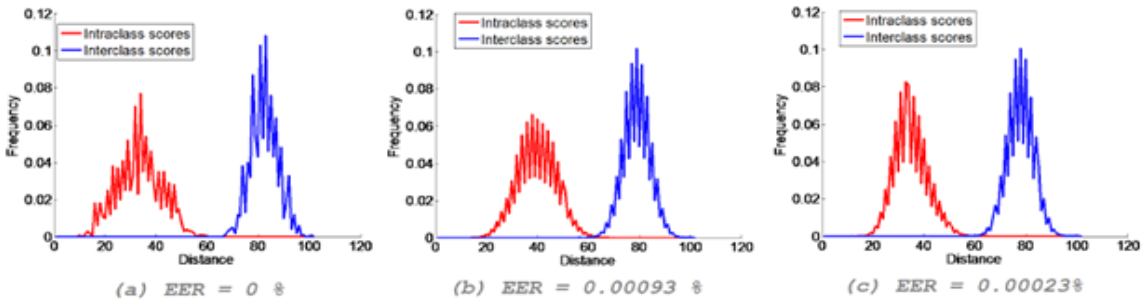
Database	EERwith outattack	EERwith attack
CASIA V3	0.000023%	1.45%
CASIA V4	0.00093%	1.96%
CASIA V5	0.00023%	2.345%

تجزیه و تحلیل امنیت و حریم خصوصی

پروتکل پیشنهاد شده احترام بیشتری برای حریم خصوصی کاربران نسبت به پروتکل D-Secure۳ قائل است. یک تجزیه و تحلیل از پروتکل پیشنهادی در این بخش پیشنهاد می‌کنیم.

۱) امنیت داده‌ها و احراز هویت: کانال امن بین عوامل و طرح‌های رمزنگاری از محرمانه بودن اطلاعات مبادله شده و یکپارچگی داده‌ها در طول پروتکل اطمینان دارد. در نتیجه، الزامات R1 و R2 مورد اطمینان دارند. احراز هویت افراد نیز از طریق SSL برای SP (R6) و بانک‌ها (R7) تحقق یافته است، درحالی‌که تأیید هویت کاربر (R3) به واسطه قدرت قوی به دست آمده از تأیید اعتبار و از طریق الگوریتم درهم سازی است. علاوه براین، با تشکر از چالش‌ها در هنگام تایید هویت کاربر، این احراز هویت یک تایید بیومتریک یک‌باره است. در نتیجه، تراکنش‌های مختلف یک کاربر را نمی‌توان پیوند داد. الزام R8 نیز تضمین شده است. این دستگاه توسط شماره سریال خود و مدرک مالکیت دستگاه کاربر که ارائه شده است تأیید شده است، در نتیجه الزامات R4 و R5 تضمین شده هستند. علاوه براین، برای راه‌حل احراز هویت کاربر، کاربر تنها نیاز به تولید آنچه که او دارد (داده‌های بیومتریک) و آنچه شناخته شده است (رمز عبور) دارد.

۲) تجزیه و تحلیل خصوصی: در طول فرآیند تأیید هویت ما، چندین آیتم اطلاعات حساس مانند داده‌های بیومتریک و رمز عبور مبادله و ذخیره می‌شوند. ذخیره‌سازی آنها نباید متمرکز باشد. با این حال، به لطف استفاده از الگوریتم درهم سازی، قابل لغو می‌باشد. بدین ترتیب، دانش BioCode در مورد اطلاعات شخصی کاربر هیچ چیزی در دست ندارد. در مورد ما، دانش BioCode مرجع با دانش داده‌های بیومتریک مانند اثر انگشت همراه نیست. فقط داده‌های مرتبط و ضروری ارسال و ذخیره می‌شوند. بنابراین اصل کمینه‌سازی (R9) نیز مورد احترام است. علاوه براین، برای احراز هویت هر کاربر، کاربر باید اثر انگشت خود را ارائه دهد و رمز عبور خود را تحویل بگیرد. این اقدامات باعث می‌شود تا کاربر رضایت خود را برای استفاده از این اطلاعات که می‌تواند به لطف محاسبات Capture کنترل شود بیان کند. اصل حاکمیت داده (R10) مورد احترام است.



شکل(۵-۲) اندازه گیری ERR برای سه پایگاه استاندارد اثر انگشت

نتیجه‌گیری و چشم‌اندازهای آینده

راه حل پیشنهادی از یک دستگاه اضافی، که دارای هزینه ناچیزی است استفاده می‌کند. با این وجود، ریسک مالی برای بانکداری و یا پرداخت مهم است و به شدت افزایش می‌یابد. در نتیجه، این دستگاه اضافی برای یک دنیای واقعی مسئله‌ای نمی‌باشد. در این پایان نامه، یک پروتکل احراز هویت جدید "One Time Biometrics" برای بانکداری آنلاین و احراز هویت پرداخت الکترونیکی ارائه شده است. پروتکل شامل دو جزء اصلی است. اولین جزء یک دستگاه خاص به نام OffPAD است که بسیاری از مسائل امنیتی و حفظ حریم خصوصی را تضمین می‌کند. مولفه دوم استفاده از یک الگوریتم حفاظت از قالب بیومتریک برای ذخیره متمرکز داده‌های بیومتریک توسط بانک صادرکننده است. سپس یک پروتکل مبتنی بر چالش برای جلوگیری از حملات مجدد پیشنهاد شده است. طرح احراز هویت کاربر برای کاربران قابل استفاده است زیرا آنها مجبور هستند گذرواژه‌های مختلف را به یاد داشته باشند. پروتکل عملکرد بسیار خوبی در سه پایگاه داده اثر انگشت با توجه به مسائل امنیتی و حفظ حریم خصوصی از خود نشان داده است.

دیدگاه‌های آینده در مورد این مطالعه بسیار زیاد است. ما برنامه‌ریزی می‌کنیم تا از داده‌های بیومتریک چندگانه به منظور اجتناب از استفاده یک رمز عبور در پروتکل پیشنهادی استفاده کنیم و همچنین قصد داریم یک پروتکل معتبر برای داده‌های بیومتریک طراحی کنیم.