International Conference on
RESEARCH IN ELECTRICAL AND COMPUTER ENGINEERING
کنفرانس بین‌المللی پژوهش در مهندسی برق و کامپیوتر
15 December 2016 Singapore www.receconf.com سنگاپور ۲۵ آذر ۱۳۹۵

رمزنگاری اثر انگشت برای احراز هویت ایمن‌تر از رمزنگاری مبتنی بر ویژگی

سمیرا قاسمی
گروه کامپیوتر،دانشکده فنی و مهندسی،واحد ساوه، دانشگاه آزاد اسلامی،ساوه، ایران
smrghasemi@gmail.com

چکیده
واضح است که سرویس‌دهنده ابر از روش‌های مختلف احرازهویت، اعتبارسنجی و کنترل دسترسی استفاده کند، اما این‌که چه فرآیند و رویه امن و قابل اطمینانی را انتخاب کند، اهمیت بیشتری دارد. از آنجایی که اطلاعات بیومتریک همیشه همراه فرد است، از روش‌های دیگر احراز هویت که ممکن است فراموش شده، دزدیده شده و یا از دست برود، کارآمدتر است. یکی از قدیمی‌ترین و رایج‌ترین مشخصه‌ها، جهت کنترل دسترسی و احراز هویت، اثرانگشت می‌باشد. از اثر انگشت در کاربردهای مختلف برای احراز هویت و کنترل دسترسی استفاده شده است. در این پژوهش یک روش برای احراز هویت ایمن ارائه شده است. برای تطبیق و استخراج اثر انگشت از نقاط مینوشیا به همراه ویژگی‌های محلی و سراسری و نقاط برآمدگی استفاده شده است. تمام داده‌ها در آزمایشگاه FVC onGoing تولید شده است و نتایج نشان می‌دهد که سرعت، دقت و امنیت بالاتری نسبت به رمزنگاری مبتنی بر ویژگی دارد.

واژگان کلیدی: بیومتریک، مینوشیا، کنترل دسترسی، رمزنگاری مبتنی بر ویژگی

مقدمه

امروزه روش‌های متفاوتی برای تشخیص[۱] و تصدیق[۲] هویت اشخاص وجود دارد که قدیمی‌ترین و در عین حال پرکاربردترین و عملی‌ترین آنها روش شناسایی اشخاص بر اساس اثر انگشت می‌باشد. که به دلیل یکتایی، عدم تغییر در طول عمر و پردازش کم هزینه و سریع، در حدود یک قرن است که توجه دانشمندان و نیروهای امنیتی را به خود جلب کرده است. بیومتریک‌های مبتنی بر دست نه فقط به دلیل عملکرد ممتازشان که الزام برنامه‌های با امنیت بالا هستند بیشترین تصدیق برای احراز هویت‌های شخصی بودند. شناسایی با اثر انگشت یکی از روش‌های بیومتریک شناسایی افراد است و نسبت به ویژگی‌های دیگر تحت تاثیر حوادث فیزیکی و یا حالات روحی شخص تغییر نمی‌کند. در روش‌های سنتی جهت تعیین هویت افراد از اطلاعاتی که فرد در اختیار داشت مانند رمز عبور و یا شماره شناسایی استفاده می‌شد. اما با وجود اهمیت بسیار رمز عبور هنوز هم بسیاری از کاربران از رمز عبورهایی مانند مجموعه اعداد یک تا ۹، نام و نام‌خانوادگی، نام مکان‌های مهم، تاریخ تولد، شماره تلفن همراه، کدملی و بسیاری از اعداد و عبارات استفاده می‌کنند. در صورتی‌که این نوع رمزهای عبور براحتی قابل حدس زدن است و افراد خرابکار با استفاده از روش‌های نرم‌افزاری خیلی راحت می‌توانند این رمزها را کشف کنند. یک چالش بزرگ برای امنیت و حفظ حریم خصوصی است. اطلاعات بیومتریک نمی‌تواند لغو شود، پس برای داده‌هایی که دارای اهمیت بالایی هستند، بیومتریک یک راه امن در نظر گرفته است. هنگامی که اطلاعات حساس باشند، حفظ نیازمندی‌های امنیتی اطلاعات، به یک چالش اساسی تبدیل می‌شود. کنترل دسترسی به عنوان یک راه‌حل امنیتی سنتی و البته مهم و اساسی، بنا به دلایلی همچون دور زدن مکانیزم‌های کنترل دسترسی و عدم اعتماد به اعمال کننده‌ی خط‌مشی‌های کنترل دسترسی، به تنهایی ضمانتی برای حفظ نیازمندی‌های امنیتی اطلاعات نیست. مهاجمان و بدخواهان نیز در هر سناریویی می‌توانند به عنوان تهدیداتی مهم، امنیت اطلاعات را با چالش روبرو کنند. بنابراین نیاز است تا با استفاده از مکانیزم‌هایی همچون رمزنگاری به مقابله با این چالش‌ها پرداخت.

با رشد شبکه‌ها و تعداد کاربران،IBAC برای مبنای دفاع از چنین رشد زیادی ضعیف عمل کرده است. مفاهیم پیشرفته در کنترل دسترسی شامل مالک/گروه/عمومی، معرفی شده است. که IBAC نشان داد که برای سیستم‌های توزیع شده مشکل ساز است. مدیریت دسترسی به سیستم ومنابع، سخت و آسیب‌پذیر در مقابل خطا شده است. یک روش جدید شناخته شده به عنوان کنترل دسترسی مبتنی بر نقش(RBAC) معرفی شده است(Ferraiolo DF and Kuhun DR,1992). کنترل دسترسی مبتنی بر نقش، دسترسی کاربر به سیستم را بر اساس نقش کاری آن تعیین می‌کند. نقش با حداقل مجوز و یا ویژگی‌های لازم برای انجام کار تعریف می‌شود و سپس این مجوزها می‌تواند کم و یا اضافه شود. با این حال، مشکلات RBAC زمانی آشکار شد که در سراسر دامنه‌های اجرایی گسترش یافت. و نشان داد که برای رسیدن به توافق سطح دسترسی در ارتباط با نقش دشوار است. بر این اساس، کنترل دسترسی مبتنی برسیاست که به عنوان کنترل دسترسی مبتنی بر ویژگی ABAC شناخته شده، به وجود آمد(A. Pimlott and O. Kiselyov,2006 , M. Blaze and J Feigenbaum). در ABAC دسترسی بر روی ویژگی واگذار شده که می‌تواند اثبات شود، مانند تاریخ تولد یا شماره ملی.

تاریخچه

[۱] Identification

[۲] Verification

رمزگذاری مبتنی بر ویژگی

مفهوم ABE برای اولین بار توسط(A. Sahai and B. Waters,2005) به عنوان یک روش جدید برای رمزگذاری مبتنی بر هویت فازی معرفی شد. کاربر تنها در صورتی که کلید رمزگشایی کاربر با متن رمز منطبق باشد، قادر به رمزگشایی است. در یک سیستم رمزنگاری مبتنی بر ویژگی کلیدهای کاربران و متن‌های رمز شده با مجموعه‌ای از ویژگی‌های توصیفی برچسب گذاری شده‌اند. در این سیستم یک کلید خاص می‌تواند یک متن رمز شده‌ی خاص را باز کند، اگر و تنها اگر بین ویژگی‌های متن رمز نشده و کلید کاربر مطابقت وجود داشته باشد. در کنترل دسترسی مبتنی بر ویژگی، تصمیم‌گیری کنترل دسترسی بر اساس ویژگی‌های گرفته شده درخواست کننده، سرویس‌ها، منابع و محیط آن است. کنترل دسترسی مبتنی بر ویژگی گسترش یافته‌ی کنترل دسترسی مبتنی بر نقش است، با مشخصات زیر:

- مجوز اختیارات ویژگی
- تمرکز زدایی از ویژگی‌ها
- تداخل ویژگی‌ها

کنترل دسترسی مبتنی بر ویژگی از چهار نهاد زیر تشکیل شده است:

درخواست کننده(Req[۳]): درخواست را به ابر می‌فرستد و اقدام به فراخوانی سرویس‌ها می‌کند.

سرویس (Serv[۴]): نرم‌افزار و سخت‌افزار با شبکه مبتنی بر واسط و عملیات از پیش تعریف شده است.

منابع (Res[۵]): برای یک یا چند عمل سرویس‌های ابر، با یک مجموعه خاص از حالت داده‌ها در سند XML است.

محیط (Env[۶]): حاوی اطلاعاتی است که امکان دارد، در گرفتن تصمیم دسترسی مفید باشد، مانند تاریخ و زمان.

هر یک دارای ویژگی‌های تعریف هویت و خصوصیات نهاد مربوطه است. ویژگی‌های هویت در(B. cha, J Seo and J. Kim. 2011) به شرح زیر تعریف می‌شود:

$Attr(Req) = \{ReqAttr_i \mid i \in [1, I]\}$

$Attr(Serv) \{ServAttr_j \mid j \in [1, J]\}$

$Attr(Res) \{ResAttr_k \mid k \in [1,K]\}$

$Attr(Env) \{EnvAttr_l \mid l \in [1, L]\}$

که در آن I، J، K و L اعداد صحیح هستند و نشان دهنده حداکثر تعداد ویژگی برای هر یک از موجودیت‌ها است.

درخت دسترسی

برای تعریف کنترل دسترسی در سیستم‌های رمزنگاری مبتنی بر ویژگی، از یک درخت کنترل دسترسی استفاده می‌شود. درخت دسترسی به صورت زیر تعریف می‌شود:

تعریف: فرض کنید یک درخت باشد که یک ساختار دسترسی را نمایش می‌دهد. هر گره غیر برگ از این درخت یک گیت آستانه‌ای است. این گره با بچه‌هایش و یک مقدار K_x توصیف می‌شود. اگر num_x تعداد بچه‌های گره x بوده و K_x مقدار آستانه‌ای این گره باشد آنگاه $0 \le K_x \le num_x$. واضح است که اگر $K_x=1$ آنگاه گیت آستانه‌ای یک OR است و وقتی $K_x=num_x$ باشد گیت آستانه‌ای یک AND خواهد بود. همچنین هر گره x که برگ این درخت است، با یک ویژگی توصیف می-

[۳] Requestor
[۴] Service
[۵] Resource
[۶] environment

شود و مقدار آستانه‌ای آن $K_x=1$ می‌باشد. در این صورت به درخت □ یک درخت دسترسی می‌گوییم. صدق کردن در درخت دسترسی نیز به صورت زیر تعریف می‌شود:

فرض کنید □ یک درخت دسترسی با ریشه‌ی r باشد. زیردرختی از این درخت با گره ریشه‌ی x با T_x نمایش داده می‌شود. در واقع □ با □ یکی است. عبارت $T_x(Y)=1$ □ یعنی مجموعه ویژگی‌های Y در درخت □ صدق می‌کنند.$T_x(Y)$ به صورت بازگشتی محاسبه می‌شود. یعنی اگر x یک گره غیر برگ باشد، ابتدا مقدار $T_{x'}(Y)$ را برای هر فرزند 'x از گره x حساب می‌شود. □ $(Y)_x$ برابر ۱ است اگر و تنها اگر حداقل k_x فرزند مقدار ۱ برگردانند. اگر x یک گره برگ باشد، آنگاه □ $(Y)_x$ مقدار ۱ برمی‌گرداند اگر و تنها اگر $att(x)\in Y$.

درطرح(محفوظی،۱۳۹۲) با استفاده از رمزنگاری مبتنی بر ویژگی روشی برای اعمال کنترل دسترسی توسط سرویس‌دهنده غیر قابل اعتماد ارائه داده است. که در این روش قابلیت پویایی در تغییر کنترل دسترسی در کنار راهبری خط‌مشی‌های دسترسی دیده شده است. به این معنی است که مالک داده ضمن امکان تغییر در خط‌مشی‌های دسترسی می‌تواند حق اعطا و ابطال را نیز به کاربران بدهد. نتایج مقایسه و تحلیل نشان می‌دهد این روش برای تعیین حقوق دسترسی کاربران انعطاف‌پذیری بیشتری داشته و امکان اعطای حقوق مختلف دسترسی به مجموعه‌ای از کاربران در این روش ساده‌تر است. همچنین این روش محافظ حریم خصوصی کاربران است و سرویس‌دهنده غیر قابل اعتماد از الگوی دسترسی کاربران مطلع نمی‌شود.

هدف(Jun Yan et al, 2011)، کمک به صاحب داده برای دستیابی به کنترل دسترسی ریزدانه و انعطاف‌پذیر در برون‌سپاری داده‌ها در ابر است. همچنین برای جلوگیری از یادگیری محتوای داده‌ها و اطلاعات کاربر توسط ارائه دهنده ابر است، و صاحب داده مجوز تعریف دسترسی کاربران به فایل داده‌ها را خواهد داشت. در(Jin Li et al,2010)، یک راه برای پیاده‌سازی مقیاس‌پذیر و سیستم کنترل دسترسی ریز دانه بر اساس رمزنگاری مبتنی بر ویژگی بیان کرده‌اند. برای کنترل دسترسی ایمن در رایانش ابری، از توطئه به‌اشتراک‌گذاری کلید در میان کاربران جلوگیری کرده‌اند. که با توجه به آزمایشات انجام شده این طرح کارآمد و عملی و بدون محدودیت است.

رمزنگاری مبتنی بر ویژگی با سیاست کلید

رمز گذاری کلید عمومی ابتدایی برای ارتباطات یک به چند است(V. Goyal et al,2006). در KP-ABE[۷]، داده‌ها همراه با ویژگی که هر یک از آنها یک جزء کلید عمومی هستند، تعریف شده است. رمزگذار، مجموعه‌ای از ویژگی‌های مرتبط با پیام را، با تطابق اجزای کلید عمومی رمزنگاری می‌کند. در این سیستم کلید هر کاربر وابسته به یک ساختار درخت دسترسی است که در آن برگ‌ها همان ویژگی‌ها هستند. یک کاربر می‌تواند متنی را رمزگشایی کند اگر ویژگی‌های مربوط به متن رمز شده در درخت دسترسی موجود در کلیدش صدق کند. طرح KP-ABE از چهار الگوریتم تشکیل شده است:

راه اندازی. در این الگوریتم پارامتری را به عنوان ورودی می‌گیریم، که این پارامتر امنیتی k نام دارد. و یک مجموعه ویژگی U داریم $U=\{1,2,\ldots,N\}$ با درجه‌ی N. یک گروه G_1 دو خطی، سفارش اولیه P با تعریف مولد g، یک نگاشت دوخطی $e: G_1\times G_1\rightarrow G_2$ است که خواص دوخطی، محاسبات و عدم انحطاط را دارد. یک سیستم کلید عمومی PK و کلید اصلی MK را در بر می‌گیرد، که به شرح زیر است:

$PK=(Y,T_1,T_2,\ldots,T_N)$ (۱)

$MK=(y,t_1,t_2,\ldots,t_N)$ (۲)

که در آن $T_i\in G_1$ و $t_i\in Z_P$ و برای ویژگی $1\leq i\leq N$، $Y\in G_2$ یکی دیگر از اجزای کلید عمومی است. که $T_i=g^{t_i}$, $Y=e(g,g)^y, y\in Z_P$.

در حالی که PK به طور عمومی در سیستم شناخته شده، کلید مخفی MK فقط در اختیار صاحب داده است.

[۷] Key Policy Attribute-Based Encryption

رمزگذاری. این الگوریتم یک پیام M،کلید عمومی PK و مجموعه ای از ویژگی I را به عنوان ورودی می‌گیرد. خروجی متن رمز E با فرمت زیر است:

$E=(I,\hat{E},\{E_i\}\ i\in I)$ (۳)

$\hat{E}=MY^s\ ,\ E_i=T^{s_i}$ (۴)

و S به طور تصادفی از Z_p انتخاب می‌شود.

ایجاد کلید. ورودی این الگوریتم یک درخت دسترسیT، کلید اصلی MK و کلید عمومی PK است.خروجی کلید مخفی کاربر SK است، که به شرح زیر است:

اول آن را با چند جمله ای تصادفی $P_i(x)$، برای هر گره i از T از روش بالا به پایین با شروع از گره ریشه r تعریف می-کند. برای هر گره غیر ریشه j، $P_j(0)= P_{parent(j)}(idx(j))$ که در آن parent(j) نشان دهنده والدین j و idx(j) شاخص منحصر به فرد داده شده توسط والدین j است.برای هر گره ریشه r، $P_r(0)=y$ آنگاه خروجی SK: $SK= \{sk_i\}_{i\in L}$، که در آن L نشان دهنده مجموعه ای از ویژگی متصل به گره برگ از T و $SK_i=g^{p_i(0)/t_i}$ است.

رمز گشایی.این الگوریتم ورودی متن رمز E در مجموعه ویژگی I، کلید مخفی کاربر SK برای درخت دسترسی T و کلید عمومیPK است. اولین محاسبات $e(E_i,sk_i)= e(g,g)^{p_i(0)s}$ برای گره برگ است.

سپس نتایج جفت شدن به صورت پایین به بالا با استفاده از چندجمله ای درون یاب است.در نهایت، چند فاکتور ناپیدا بازیابی می‌شود.

$Y^s=e(g,g)^{ys}$ (۵)

رمزنگاری مبتنی بر ویژگی با سیاست متن رمز شده

در شمای CP-ABE[۸]، کلید خصوصی کاربر با تعداد دلخواهی از ویژگی‌های توصیفی مرتبط است. از طرف دیگر وقتی کاربری یک متن را رمزنگاری می‌کند، یک ساختار دسترسی از روی ویژگی‌ها برای آن مشخص می‌کند. رمزگشا فقط وقتی می‌تواند یک متن رمز شده را باز کند که ویژگی‌های او در درخت دسترسی متن رمز شده صدق کند. در واقع شمای رمز با سیاست متن رمز شده کاملا شبیه شمای رمز با سیاست کلید است با این تفاوت که در آن درخت دسترسی در متن رمز شده و ویژگی‌ها در کلید هر کاربر قرار دارد. یک شمای رمزنگاری مبتنی بر ویژگی با سیاست متن رمز شده شامل چهار الگوریتم اصلی زیر است.

راه‌اندازی. این الگوریتم به عنوان ورودی پارامتر امنیتی دریافت می‌کند. در خروجی پارامترهای عمومی PK و کلید اصلی MK را تولید می‌کند. الگوریتم setup یک گروه دو سویه G_0 از مرتبه‌ی اول ρ با مولد g تولید می‌کند و دو عدد تصادفی $\alpha,\beta \in Z_p$ را انتخاب می‌کند. سپس کلید عمومی و کلید اصلی به صورت زیر محاسبه می‌شوند.

$PK = (G_0,g,h = g^{\beta},f = g^{1/\beta}, e(g,g)^{\alpha})$ (۶)

$MK = (\beta.g^{\alpha})$ (۷)

رمزگذاری(PK,M,T). الگوریتم رمزنگاری به عنوان ورودی پارامتر عمومی PK، یک پیغام M، و یک درخت دسترسی □ دریافت می‌کند. الگوریتم رمزنگاری پیغام را دریافت و رمز می‌کند و پیغام رمز شده،CT، را به عنوان خروجی برمی‌گرداند. این پیغام رمز شده را فقط کاربرانی که صاحب مجموعه‌ی ویژگی‌هایی هستند که در درخت دسترسی □ صدق می‌کند می-توانند رمزگشایی کنند. الگوریتم رمز ابتدا یک چندجمله‌ای q_x یا هر نود x در درخت دسترسی □ انتخاب می‌کند. این چند

[۸] cipher-text policy attribute-based encryption

جمله‌ای‌ها از ریشه‌ی درخت به سمت پایین انتخاب می‌شوند. برای هر نود x از درخت درجه‌ی d_x چندجمله‌ای q_x یکی کمتر از مقدار آستانه‌ای k_x آن نود است، یعنی $d_x = k_x - 1$.

با شروع از نود ریشه R الگوریتم یک عدد تصادفی $s \in Z_q$ را انتخاب کرده و $q_x(0) = s$ قرار می‌دهد. سپس بقیه‌ی d_R نقطه‌ی چندجمله‌ای q_R را به صورت تصادفی انتخاب می‌کند تا این چندجمله‌ای به طور کامل تعریف شود. برای هر نود x غیر ریشه $q_x(0) = q_{parent(x)}(index(x))$ قرار می‌دهد و باز بقیه‌ی d_x نقطه به صورت تصادفی انتخاب می‌شود.

حال اگر Y مجموعه‌ی نودهای برگ در درخت □ باشد. متن رمز شده به صورت زیر محاسبه می‌شود.

$$CT=(T ,\hat{C}=Me(g,g)^{\alpha s},C= h^s,\forall y\in Y: C_y= g^{q_y(0)}, c'_y= H(att(y))^{q_y(0)}). \quad (۸)$$

تولید کلید(MK,S). الگوریتم تولید کلید در ورودی کلید اصلی و یک مجموعه از ویژگی‌ها را دریافت می‌کند. این الگوریتم یک کلید خصوصی،SK، برمی‌گرداند. الگوریتم تولید کلید ابتدا یک عدد تصادفی $r\in Z_p$ را انتخاب و سپس برای هر $j\in S$ عدد تصادفی $r_j\in Z_p$ را انتخاب می‌کند. سپس الگوریتم کلید خصوصی را به صورت زیر محاسبه می‌کند.

$$SK=(D=g^{(\alpha+r)/\beta},\forall\ j \in S : D_j = g^r.H(j)^{r_j},D'_j =g^{r_j}). \quad (۹)$$

رمزگشایی(PK,CT,SK). الگوریتم رمزگشایی در ورودی کلید عمومی PK، یک متن رمز شده CT، که حاوی یک درخت دسترسی □ نیز هست، و یک کلید خصوصی SK، برای مجموعه‌ی S از ویژگی‌ها را دریافت می‌کند. اگر مجموعه‌ی S از ویژگی‌ها در ساختار درخت دسترسی □ صدق کند، الگوریتم پیغام رمز شده CT را رمزگشایی کرده و پیغام اصلی M را برمی‌گرداند.

اثر انگشت

روش‌های بیومتریک از اثر انگشتان، الگوهای رفتاری، خصوصیات چهره‌ای، اسکن شبکیه چشم، دست‌خط بعنوان خصیصه-های قابل شناخت انسان استفاده می‌کنند. به همین نسبت نیز سیستم‌هایی که قادر به تشخیص شاخص‌های بیومتریکی هستند از پیچیدگی بیشتری برخوردارند. اثر انگشت افراد منحصر به فرد است و در طول عمر فرد تغییر نمی‌کند، بنابراین می‌توان از آن به عنوان یک امضا و یا ابزار تشخیص هویت استفاده نمود. سیستم‌های مبتنی بر اثر انگشت مدت طولانی است که مورد بررسی قرار گرفته است(S. Greenberg et al,2000. D. Maio et al,1997,2002). ساختار داخلی اثرانگشت که شامل خطوط برجسته و الگوی حرکتی آنها است، در انطباق و مقایسه تصاویر آن نقش کلیدی دارد. از این رو بسته به کیفیت تصاویر گرفته شده، تا حد توان، ویژگی‌های منحصر به فرد هر اثرانگشت استخراج شده و با دیگر تصاویر مقایسه می‌شود. برای پایگاه‌های داده‌های بزرگ که مقایسه با تک تک عناصر مقرون به صرفه نیست، دسته‌بندی صحیح تصاویر مشابه، بار محاسباتی و زمان مورد نیاز پردازش را تا حد زیادی کم می‌کند. هنری با ارائه‌ی ۵ کلاس کلی، توانست بر اساس نقاط یکتای تصاویر که با گردش ناگهانی منحنی‌های آن ایجاد می‌شوند، این بار محاسباتی را تا حد چشم‌گیری کاهش دهد(S. E. R. Henry,1900). برای تطبیق تصویر گرفته شده با تصاویر موجود در حافظه از الگوریتم‌های انطباقی نظیرPBAیا IBA به‌ترتیب یعنی الگوریتم برمبنای الگوی اثرانگشت PBA[9] والگوریتم بر مبنای تصویرانگشت IBA[10] و الگوریتم پیچیده‌تری به‌نام MBA[11] الگوریتم اجزای ناچیز استفاده می‌شود.

در الگوریتم PBA طرح اثرانگشت شامل خم، پیچش و حلقه با نمونه‌های حافظه مقایسه می‌شود. برای این منظور باید تصاویر در یک جهت معین قرار گیرند که الگوریتم نقطه مرکزی را در تصویر اثر انگشت یافته و آنرا با اثر انگشت ورودی هم مرکز می‌کند. هر الگو در این الگوریتم شامل نوع، اندازه و جهت طرحواره‌های تصویر تراز شده اثر انگشت است.

[9] Pattern-Based-Algorithm
[10] Image-Based-Algorithm
[11] Minutia-Based-Algorithm

درالگوریتم MBA چندین قسمت مختلف از اجزای اثرانگشت موجود در حافظه نظیر لبه‌های انتهایی هر خط موجود در اثر انگشت، انشعابات در خطوط و شیارهای کوتاه بین خطوط با اثر انگشت ورودی مقایسه می‌شوند. این روش همچنین مانند روش قبلی نیاز به تصویری تراز شده از اثر انگشت دارد. تفاوت در این روش این است که بجای انطباق مراکز از یک قاب مرجع Reference Frame استفاده می‌شود. هر نقطه اجزای اثرانگشت در این الگوریتم بصورت یک بردار در طرحواره اثرانگشت ذخیره می‌شود.

در(محمودی, ع., ۱۳۸۴) روشی مؤثر جهت تطابق تصاویر اثرانگشت پیشنهاد شده است. این طرح قابلیت تشخیص اثر انگشت را با استفاده از تنها قسمت کوچکی از آن، دارا می باشد که این مسأله به خصوص در مسائل امنیتی و جنایی از اهمیت به سزایی برخوردار است.

در(Q. Tang et al,2008) دو مفهوم از حریم خصوصی بیومتریک به نام حریم خصوصی هویت و گمنامی تراکنش توسعه دادند و یک پروتکل احراز هویت با استفاده از اطلاعات خصوصی پروتکل‌های بازیابی که در رمزنگاریElGamal است، ارائه داده‌اند. در هر دو اثر نوع بیومتریک پروتکل‌های خود را تنها می‌توانند در فاصله همینگ بین الگوهای بیومتریک در حوزه رمزنگاری محاسبه کنند. که این طرح باید برروی امنیت سیستم بیشتر کار کند.

در پروتکل(Kai Xi et al,2010)، بیومتریک اثر انگشت کاربر برای تأیید استفاده می‌شود، از نظر محاسباتی توسط کلید عمومی زیرساخت (PKI[۱۲])، منحنی رمزنگاری بیضوی (ECC[۱۳])، است. یک پروتکل زیستی رمزنگاری جدید حفاظت شده، ارائه شده است. در پروسه تأیید هویت، از پروتکل بیومتریک اثر انگشت برای کار با ECC رمزنگاری کلید عمومی استفاده می‌شود. پروتکل بیورمزنگاری شامل دو فاز ثبت نام کاربر و احراز هویت کاربر است. در پایگاه داده NIST 24 نشان می‌دهد که دقت تطابق به دست آمده منطقی است. اجرای شبیه ساز جاوا ME ثابت می‌کند محدودیت منابع و دستگاه‌های تلفن همراه را برآورده می‌کند.

طرح(S.Nagaraju et al,2013) مبتنی بر فن‌آوری اینترنت است، و نظام امن برای ارائه خدمات به ذینفعان فراهم می‌کند. گام اولیه کانال امن بین مصرف کنندگان و خدمات ابری با استفاده از پروتکل امنیتی لایه انتقال است. امنیت بیشتر اینترنت را می‌توان با استفاده از یکی از دنباله‌های رمز داده شده، ایجاد ارتباط امنTLS[۱۴] با استفاده از الگوریتم رمزنگاری نامتقارن (ECDHE,RSA,ect.)، الگوریتم رمزنگاری متقارن(AES,CBC,ect.) و الگوریتم هش کردن(SHA512,MD5,ect.)، فراهم کرده است. که در آن الگوریتم‌های نامتقارن برای احراز هویت، الگوریتم‌های متقارن برای رمزنگاری و الگوریتم‌های هش کردن برای یکپارچگی نهایی موجودیت‌ها، استفاده می‌شود.

روش تحقیق

روش پیشنهادی برای بخش اثر انگشت، تطبیق بخشی از تصویر اثرانگشت با استفاده از مینوشیای تصویر اثرانگشت می-باشد. مینوشیای مورد استفاده، نقطه پایانی و نقطه دوشاخه است. در کنار ویژگی‌های مینوشیا و در بخش تطبیق از ساختار سراسری و ساختار محلی همراه با برآمدگی یا Ridge خطوط اثرانگشت برای افزایش دقت، بهره گرفته شده است.

الگوریتم عمومی تطبیق بر اساس مینوشیا(GMMA[۱۵])

تمام GMMAs از قانون زیر پیروی می‌کنند.

۱.استخراج مینوشیا

[۱۲] Public Key Infrastructure

[۱۳] Elliptic Curve Cryptography

[۱۴] Transport Layer Security

[۱۵] General Minutiae-based Matching Algorithm

۲.تولید پارامترهای مربوط به تست تصویر و تصویر الگو
۳. هماهنگی با پارامترهای برای دریافت تعداد کل تطبیق مینوشیا
۴. تعیین نهایی با توجه به نتیجه مرحله ۳

استخراج ویژگی‌های موجود در اثر انگشت و انطباق اثر انگشت

خصوصیات استخراج شده از یک تصویر اثر انگشت به‌طور معمول به سه سطح تقسیم می‌شوند. سطح اول، شامل برداشت جزئیات مقیاس بزرگ مانند شکل خطوط اصطکاکی، الگوی اصلی خطوط و نقاط منفرد خواهد بود. سطح دوم به مینوشیاهای دوشاخه شدن خطوط و پایانی آن‌ها مربوط است و سطح سوم شامل تمام خصوصیات ابعادی اثر انگشت مانند انحراف خطوط، ضخامت آن‌ها، شکل خطوط، منافذ و خلل و فرج آن‌ها، لبه‌های نهایی خطوط و دیگر جزئیاتی نظیر چین و شکن‌های خطوط و آثار زخم و بریدگی است.

در تطبیق اثرانگشت دو نوع ویژگی می‌توان به کارگرفت: ویژگی‌های سراسری و ویژگی‌های محلی. ویژگی‌های محلی براساس اطلاعات محلی از الگوهای رگه‌ها استخراج می‌گردند مانند نقاط دوشاخه و نقاط پایانی. ویژگی‌های سراسری در برگیرنده ساختار کلی تصویر می‌باشند. نقاط منفرد حلقه و دلتا از ویژگی‌های سراسری محسوب می‌شود. ویژگی‌های محلی نسبت به تبدیلات سراسری، پایدار می‌باشند و در مواردی که اطلاعات مربوط به ساختار کلی اثرانگشت وجود ندارد، مناسب هستند. تطبیق فقط مبتنی بر مشخصه‌های محلی، تأثیر رابطه‌های مکانی ساختار سراسری را که بسیار متمایز کننده می‌باشد، کاهش می‌دهند.

ساختار تطبیق محلی

هر مینوشیا m_i به صورت بردار ۴تایی $m_i = [x_i , y_i , type_i , \theta_i]$ در نظر گرفته می‌شود که x,y، مختصات مکانی مشخصه، type نوع مشخصه و θ_i جهت مینوشیا را در تصویر مشخص می‌سازد. ساختار محلی مینوشیا توسط فاصله، شمارش خط الراس، جهت و زاویه شعاعی مینوشیا نسبت به هر یک از همسایگان مینوشیا محلی و انواع مینوشیا و چرخش تعریف می‌شود.

ساختار تطبیق سراسری

از آنجایی که تنها ساختار محلی استفاده می‌شود برای توصیف ممکن است دو اثر انگشت ساختارهای محلی یکسان داشته باشند در نتیجه باعث پذیرش نادرست می‌شود. باید اطمینان از تطبیق افزایش یابد. همچنین ممکن است تعداد کمی از ساختارهای محلی در توصیف همسایگی وجود داشته باشد. بنابراین ساختار محلی کمتر قابل اعتماد است.یک ایده برای بهبود قابلیت اطمینان اضافه کردن مینوشیا سراسری در تطبیق اثر انگشت است. تغییر شکل غیر خطی که خاصیت ذاتی قالب اثرانگشت است که با درجه بالا ذخیره شده‌اند. این ویژگی سراسری مینوشیا اثرانگشت ورودی کاملا متفاوت از اثرانگشت الگو دیگران است. تطبیق الاستیک با استفاده از یک چهارچوب 3D محدود B_g در ویژگی فاصله به جای تطبیق دقیق است.

برآمدگی خطوط اثر انگشت یا Ridge

این الگوریتم دارای دو مرحله است:
در مرحله اول ناحیه برآمدگی استخراج شده است.نقاط مرکزی را تشخیص داده و برای کاهش محاسبات آن‌را حذف می-کند. در مرحله دوم به جای ردیابی برآمدگی در اطراف نقطه اصلی، برآمدگی در منطقه برآمدگی را پیش‌بینی می‌کند. از

آنجایی که نقطه اصلی در ناحیه برآمدگی نهفته است با دقت طبقه‌بندی نمی‌کنند. هنگامی که برآمدگی ترسیم شد، طبقه-بندی براساس بردار در نقاط پایان و پارامترهای دیگر کشیده شده است. در مرحله تبدیل باینری رگه‌ها یا همان برآمدگی خطوط اثر انگشت با مقدار ۱مشخص می‌شوند، که می‌توان از طریق آن تعداد برآمدگی‌ها را مشخص کرد.

نتایج

تبدیل باینری و کم کردن عملیات

به طور معمول تصاویر اثرانگشت، تصاویر خاکستری است، به همین دلیل اولین مرحله پیش پردازش را، تبدیل تصویر خاکستری به باینری در نظر می‌گیریم که با استفاده از عملیات آستانه به روش زیر است:

$$I_{B(x,y)}=\begin{cases} I(x,y)=255, & \text{if } I(x,y) \geq \theta \\ I(x,y)=0, & \text{otherwise} \end{cases} \qquad (۱۰)$$

که در آن I_B اشاره به تصویر اثر انگشت باینری تولید شده دارد. I(x,y) نشان دهنده مقدار شدت پیکسل در مقیاس خاکستری تصویر اثر انگشت و θ حد آستانه است، که از لحاظ تجربی تعیین شده است. با تبدیل عکس به فرمت باینری، مقادیر عکس به ۰ و ۱ تغییر می‌کند. تصویر باینری اثرانگشت دارای مقدار صفر برای شیارها و مقدار یک برای رگه‌های تصویر می‌باشد.

تبدیل به تصویر اسکلتی

تصویر اسکلتی اثر انگشت با استفاده از الگوریتم نازک‌سازی به‌دست می‌آید. با انجام نازک سازی اقدام به حذف پیکسل‌های مزاحم از تصویر کرده و کار تشخیص را بهتر می‌کند. این الگوریتم با روش تکراری تحت شرایط زیر، نقاط مرزی رگه‌های تصویر اثرانگشت را حذف می‌کند(R. C. Gonzalez, and R. E. Woods, 2002):

الف) نقاط پایانی حذف نشوند. ب) اتصالات قطع نشوند. ج) باعث سایش بیش ازحد نشود.

نازک‌سازی شامل تکرار مراحل زیر می‌باشد:

۱. تعیین نقاط مرزی جهت حذف
۲. حذف نقاط تعیین شده
۳. تعیین نقاط غیرمرزی جهت حذف
۴. حذف نقاط تعیین شده

این مراحل تکرار می‌شوند تا زمانی که دیگر نقطه‌ای برای حذف وجود نداشته باشد.

تعیین نقاط مرزی بر اساس همسایگی هشت‌گانه انجام می‌گیرد. همسایگی هشت‌گانه پیکسل p متشکل از ۸ پیکسل مجاور به p در یک آرایه دیجیتال مستطیل شکل است. هر نقطه p_1 از تصویر که دارای شرایط زیر باشد برای حذف شدن علامت می خورد:

a. $۲ \leq N(P_1) \leq 6$
b. $S(P_1)=1$
c. $P_2.P_4.P_6=0$

d. $P_4.P_6.P_8=0$

که در اینجا $N(P_1)$ تعداد همسایه‌های غیر صفر P_1 می‌باشد و $S(P_1)$ تعداد تغییر حالت از صفر به یک در دنباله مرتب $P_9,\ldots,P_3,P_2$ می باشد. مرحله یک در تمام پیکسل‌های مرزی تصویر اجرا می‌شود، اگر تمام شرایط (a) تا (d)در پیکسلی از تصویر برقرار باشد، آن پیکسل جهت حذف علامت می‌خورد، اما حذف پیکسل‌های تعیین شده، پس از پردازش تمام پیکسل‌ها انجام می‌شود. عقب انداختن حذف پیکسل‌ها، باعث می‌شود تا از تغییر ساختار داده‌ها در حین اجرای الگوریتم جلوگیری شود.

عملیات مورفولوژیک یک نوع عملیات برای نازک‌سازی است. با انجام این کار ضخامت خطوط را به کمترین حد ممکن می‌رسانیم. الگوریتم نازک‌سازی فوق با استفاده از تابع زیر انجام می‌شود.

```
K=bwmorph(~J,'thin','inf');
```

بدین ترتیب تصویر اسکلتی اثرانگشت حاصل می‌گردد.

بهبود تصویر اسکلتی

تصویر اسکلتی ایجاد شده امکان دارد دارای نویز و یا شکستگی شده باشد. این امر به دلیل وجود پیکسل‌های منفرد در پیش‌زمینه و اتصالات کوتاه بین رگه‌ها، موسوم به پیکسل‌های متصلH و رگه‌های کوتاه در تصویر اسکلتی اثرانگشت ایجاد شده و منجر به تولید مینوشیای نادرست می‌شوند، به همین علت این موارد باید حذف گردند. حذف و بهبود تصویر اسکلتی به دست آمده، با به کارگیری متوالی عملگرهای مورفولوژی زیر انجام شده است(R. C. Gonzalez et al,2004).

```
k=bwmorph (j, 'clean');   حذف پیکسل‌های منفرد در پیش‌زمینه
k =bwmorph( j, ' hbreak ' ); H   حذف پیکسل‌های متصل
k = bwmorph( j, ' spur');   حذف رگه‌های کوتاه
```

استخراج نقاط مینوشیا

برای استخراج مینوشیا از تصویر اسکلتی به دست آمده، باید تحلیلی برروی پیکسل‌های همسایگی هر نقطه انجام پذیرد. برای این تحلیل در نظر می‌گیریم که N_8 همسایگی هشت‌گانه پیکسل‌ها را نشان می‌دهد، برای نقاط پایانی و نقاط دوشاخه به ترتیب$N_8=1$ و $N_8>2$ داریم(منیره عبدوس و ناصر مزینی, ۱۳۸۷).

به این ترتیب مینوشیا از تصویر اسکلتی، استخراج می‌گردند. جهت مینوشیا با استفاده از اطلاعات پیکسل‌های مجاور تعیین می‌شود. همان‌گونه که پیش‌تر گفته شد، هر مینوشیا m_i به صورت بردار ۴تایی $m_i = [x_i , y_i , type_i ,\theta_i]$ در نظر گرفته می‌شود. منحصر به فرد بودن ویژگی‌های اثر انگشت بر اساس ویژگی‌های لبه‌های محلی و روابط آن‌ها است. نقاط مینوشیا نشان دهنده ویژگی‌های لبه‌های محلی است که هر دو در پایان لبه یا در دو شاخه لبه ظاهر می‌شود. برای اختلاف بین دو زاویه یا جهت تابع $d\phi(t_1,t_2)$ را تعریف می‌کنیم: با این فرض که $-\pi<t_1$ و $t_2\leq\pi$.

$$d\phi(t_1,t_2)=\begin{cases} t1-t2, & \text{if } -\pi < t1-t2 \leq \pi \\ 2\pi+t1-t2, & \text{if } t1-t2 \leq -\pi \\ 2\pi-t1+t2, & \text{if } t1-t2 > \pi \end{cases} \qquad (11)$$

به منظور به دست آوردن نقاط مینوشیا، از یک صافی در تصویر اثر انگشت استفاده می‌کنیم که پس از تبدیل باینری و کم کردن عملیات است. این فیلتر به دست آوردن یک عدد از یک ارزش از هر پنجره ۳*۳، به شرح زیر است:

۱. پیکسل مرکزی لبه پایانی است، اگر مقدار پیکسل ۱و تنها ۱همسایه یک مقدار باشد.
۲. پیکسل مرکزی دو شاخه است، اگر مقدار پیکسل ۱و ۳ همسایه یک مقدار باشد.
۳. پیکسل مرکزی پیکسل طبیعی است، اگر مقدار پیکسل ۱و۲ همسایه یک مقدار باشد.

کلیه مینوشیاهای صحیح تصویر استخراج گشته و به صورت برداری با چهار عنصر [x_i, y_i , $type_i$,θi] ذخیره می‌شوند. مجموعه M، شامل مشخصه‌های تصویر به صورت زیر می‌باشد:

$$M=\{m_i|m_i=(x_i,y_i,type_i,\theta i)\} \quad (۱۲)$$

سرکوب دورترین نقطه از نقاط مینوشیا

نتایج حاصل از مرحله قبل ممکن است شامل نقاط مینوشیا اثر انگشت نادرست باشد. ممکن است به دلیل وجود لبه-های شکسته رخ دهد. به طور کلی، نقاط مینوشیای جعلی در مرزها، از آنجایی که تصویر به طور ناگهانی به پایان می‌رسد، رخ می‌دهد. برای حل این مشکل، این نقاط کاذب را با استفاده از ماسک تصویر اثر انگشت، حذف می‌کنیم. استخراج ROI[۱۶] یک گام مهم برای حذف دورترین نقطه جعلی از نقاط مینوشیا است. برای این منظور، اول یک عملیات مورفولوژیکی[۱۷] بسته شدن و سپس فرسایش بر روی تصویر باینری، انجام می‌دهیم. فقط آن دسته از نقاط مینوشیا که در حال حاضر در داخل منطقه ROI هستند را در نظر می‌گیریم.

تنها نقاطی از ROI که مقدار Z در آن نقاط ۱ است باقی می‌ماند و بقیه صفر می‌شود و در ZTerm ذخیره می‌شود.

اگر بخواهیم بخشی از اثرانگشت را تطبیق دهیم، باید حد آستانه ماکسیمم، برای حذف مینوشیاهایی که فاصله زیادی دارند، در نظر بگیریم تا باعث کاهش محاسبات شود. ویژگی‌ها برای مینوشیاهای m_j و m_i در صورتی که شرط زیر برقرار باشد، محاسبه می‌گردد:

$$d_{ij}=\sqrt{(x_i-x_j)^2+(y_i-y_j)^2} \quad (۱۳)$$

که d_{ij}، فاصله اقلیدسی بین دو مشخصه، T_{min} حد آستانه مینیمم و T_{max}، حد آستانه ماکسیمم برای فاصله دو مشخصه می‌باشد. با استفاده از شرط $T_{min}\leq d_{ij}\leq T_{max}$ فاصله اقلیدسی دو نقطه در تصویر را بدست می‌آوریم.

سیستم تشخیص اثر انگشت در آزمایشگاه FVC 2006، که در واقع همان آزمایشگاه بیومتریک FVC onGoing می‌باشد، اجرا شده است. مجموعه تصاویر DB1 از پایگاه داده FVC 2006، شامل 100 اثر انگشت اسکن زنده است همه‌ی عکس‌ها در یک سنسور نوری با وضوح 500dpi گرفته شده است. در این الگوریتم تنها ویژگی محلی در نظر گرفته شده است. طبق محاسبات انجام شده در FVC 2006 نتایج به صورت زیر است:

جدول ۱:نتایج اجرای الگوریتم مینوشیا

EER	FMR100	FMR1000	ZeroFMR	Avg Enroll time	Avg Match time	Rej_{Enroll}
%۴,۱۸	%۶,۳۶	%۱۱,۲۵	%۱۷,۲۵	sec۰,۱۶	sec۰,۱۶	%۰,۰۰

فاکتورهای مهم برای دقت یک سیستم بیومتریک شامل:EER، FMR100، FMR1000 و ZeroFMR می‌باشد.

[۱۶] Region of Interest

[۱۷] morphological

الگوریتم مینوشیای عمومی بررسی شده و نتایج آن در جدول(۱) آورده شده است. حال برای تطبیق الگوریتم پیشنهادی که تطبیق بر اساس ویژگی‌های محلی و سراسری و برآمدگی خطوط است، را بررسی می‌کنیم.

تطبیق مینوشیا بر اساس ساختارهای محلی و سراسری و برآمدگی خطوط

برای هر مینوشیا M_i فاصله نسبی d_{ki}، زاویه شعاعی φ_{ki} زاویه مینوشیا θ_{ki} بین مینوشیا M_i و L نزدیک‌ترین مینوشیا همسایگی M_k محاسبه شده توسط:

$$d_{ki}=\sqrt{(x_k-x_i)^2+(y_k-y_i)^2} \quad (۱۴)$$

$$\varphi_{ki} = d\phi(\tan^{-1}(y_k - y_i / x_k-x_i)\ \theta_k) \quad (۱۵)$$

$$\theta_{ki} = d\phi(\theta_k , \theta_i) \quad (۱۶)$$

بردار ویژگی مینوشیا محلی با در نظر گرفتن نزدیک‌ترین همسایگی $L=2$ به صورت زیر است:

$$(d_{ki}\ d_{kj}\ \theta_{ki}\ \theta_{kj}\ \varphi_{ki}\ \varphi_{kj}\ n_{ki}\ n_{kj}\ t_k\ t_i\ t_j) \quad (۲۳-۴)$$

محاسبه تعداد برآمدگی بین نقاط مینوشیا n_{ki} و n_{kj} باید در فاز تشخیص مینوشیا باشد.

فرض کنید FL_i^I و FL_j^T ویژگی بردار ساختار محلی مینوشیا i از ورودی اثر انگشت و مینوشیا j از الگوی اثر انگشت است.

$$SL(i,j) = \begin{cases} \frac{bl-W|Fli-Flj|}{bl} & \text{if } W|Fli - Flj| < bl \\ 0, & \text{others} \end{cases} \quad W = (w_d\ w_d\ w_\theta\ w_\theta\ w_\varphi\ w_\varphi\ w_n\ w_n\ w_t\ w_t\ w_t) \quad (۱۷)$$

محاسبه تفاوت بین جهت و زاویه از معادله(۱۷) بدست می‌آید. یک بردار وزن مشخص هم داریم که مرتبط با هر جز بردار ویژگی است. بهترین همسان جفت (b1 ,b2) است که توسط به حداکثر رساندن سطح تشابه بدست آمده:

$$Sl(b1,b2) = \max_{i,j}(sl(I,j)). \quad (۱۸)$$

با توجه به دستگاه مختصات قطبی تمام مینوشیا بر اساس جفت مرجع مینوشیا M_b (b=b1,b2) هم جهت خواهد شد.

$$F_{gk} = \begin{pmatrix} r_{kb} \\ \theta_{kb} \\ \varphi_{kb} \end{pmatrix} =$$

$$d_{ki}=\sqrt{(x_k-x_i)^2+(y_k-y_i)^2}$$

$$\varphi_{ki} = d\phi(\tan^{-1}(y_k - y_i / x_k-x_i)\ \theta_k) \quad (۱۹)$$

$$\theta_{ki} = d\phi(\theta_k , \theta_i)$$

تطبیق سراسری: تطبیق سطح اطمینان (i,j) به صورت زیر است:

$$Ml(i,j)= \begin{cases} 0.5 + 0.5sl(i,j, & \text{if}|Fgi - Fgj| < Bg \\ 0, & \text{others} \end{cases} \quad (۲۰)$$

در نهایت، تطبیق M_s را با توجه به معادله زیر می‌توان محاسبه کرد:

$$M_s=100\times\frac{\sum_{i,j} ml(i,j)}{\max\{M,N\}} \quad (۲۱)$$

که در آن M ,N تعداد مینوشیا برای الگو و اثر انگشت ورودی است. دو اثر انگشت اگر نمره تطبیق‌شان برابر حد آستانه باشد تایید خواهند شد. الگوریتم زیر برای تطبیق برآمدگی اجرا شده است:

۱.اندازه بلوک W×W پیکسل به مرکز (i,j) تصویر اثر انگشت نرمال.

۲.برای هر پیکسل در بلوک، محاسبه شیب در امتداد جهت X,Y را انجام می‌دهد. فراخوانی δ_x و δ_y.

عملگر افقی δ_x به صورت زیر محاسبه می‌شود:

$$\begin{matrix} 1 & 0 & -1 \\ 2 & 0 & -2 \\ 1 & 0 & -1 \end{matrix}$$

عملگر عمودی δ_y

$$\begin{matrix} 1 & 2 & 1 \\ 0 & 0 & 0 \\ -1 & -2 & -1 \end{matrix}$$

۳.جهت محلی در پیکسل (x,y) به صورت زیر محاسبه می‌شود:

$$V_x(i,j) = \sum_{u=i-\frac{w}{2}}^{i+\frac{w}{2}} \sum_{v=j-\frac{w}{2}}^{j+\frac{w}{2}} 2\delta x(u,v)\delta y(u,v) \quad (۲۲)$$

$$V_y=\sum_{u=i-\frac{w}{2}}^{i+\frac{w}{2}}\sum_{v=j-\frac{w}{2}}^{j+\frac{w}{2}}\delta_x^2(u,v)\ \delta_y^2(u,v) \qquad (۲۳)$$

$$\Theta(i,j)=1/2\ \tan^{-1}V_y(i,j)/V_x(i,j)+\pi/2 \qquad (۲۴)$$

۴.بلوک دامنه با ارزش در محدوده ۰تا $\frac{\pi}{2}$ واقع شده است. سپس ردیابی مسیر تا زمانی که به ۰تا $\frac{\pi}{2}$ برخورد کند و بلوک را علامت‌گذاری کند.

تطبیق برآمدگی: با توجه به تصاویر اثر انگشت سیاه و سفید I_1,I_2، تصاویر برآمدگی تصاویر T_1,T_2، و مجموعه مینوشیا M_1,M_2 را بدست می‌آوریم.

ارائه برآمدگی: با توجه به نویز در تصاویر اثر انگشت و نقص در روش استخراج، ساختارهای پیچیده در تصاویر برآمدگی وجود دارد. بنابراین این گام‌ها به پیش پردازش اضافه می‌شود: ۱.برآمدگی نهایی در نقطه دلخواه قطع شود ۲. برآمدگی مرتبط با شاخه به ۳ برآمدگی تقسیم شود ۳.برآمدگی کوتاه حذف شود.

تطابق برآمدگی تراز شده: دو برآمدگی تراز شده $\{a_i\}_{i=1}^{M}$ و $\{b_j\}_{j=1}^{N}$ داده شده است. دو نقطه از نظر فاصله اقلیدسی بررسی می‌شوند: $T(i,j)$,$i=1,\ldots,M;\ j=1,\ldots,N.$

$T(i,j)=1$ a_i , b_j مطابقت دارند

$T(i,j)=0$ a_i , b_j مطابقت ندارند

لیست شاخص جفت‌ها در اینجا $\{(P_l,Q_l)\}_{l=1}^{k}$است. که در آن P_l,Q_l شاخص‌های $\{a_i\}_{i=1}^{M}$ و $\{b_j\}_{j=1}^{N}$ هستند. باید این شرایط را برآورده سازد: ۱. $T(P_l,Q_l)=1$ ۲. P_l,Q_l به طور یکنواخت به ترتیب افزایش و کاهش یابد. ۳.$|P_1-P_{l-1}|\leq 2,|Q_1-Q_{l-1}|\leq 2;\ l=2,\ldots,k.$

شرط آخر به این معنی است که در یک الگوریتم قوی در برابر نویز ناپیوستگی جزئی نقاط همسان مجاز است.

نتایج الگوریتم پیشنهادی

تمامی الگوریتم‌ها و تغییرات آن در آزمایشگاه FVC onGoing، اجرا شده است. در این محک اثر انگشت‌ها با وضوح تصویر 500 dpi و با اندازه تصویر 500×440 توسط سنسور نوری گرفته شده است. برای انجام این محک ۲۸۰واقعی و ۴۵ تلاش فریبکارانه انجام شده است. نتایجی که در آزمایشگاه تخصصی بیومتریک به دست آمده، به صورت زیر است:

جدول ۲:نتایج الگوریتم پیشنهادی

Rej_{Enroll}	Avg Match time	Avg Enroll time	ZeroFMR	FMR10000	FMR1000	FMR100	EER
٪۰,۰۰	sec۰,۹۵۳	۱,۳۴۲ sec	٪۶,۲۳۷	٪۴,۶۱۲	٪۳,۴۹۹	٪۲,۳۲۹	**٪۱,۹۹۴**

همان‌طور که مشاهده می‌شود، درصد خطای کمتری نسبت به الگوریتم مینوشیا عمومی دارد و تمام فاکتورهای مربوط به دقت الگوریتم بالاتر رفته است، اما سرعت آن کمتر شده است، که این مسئله که با بالا رفتن دقت سرعت پایین‌تر می‌رود یک امر بدیهی است چون باید فاکتورهای بیش‌تری را بررسی کند. در اینجا علاوه بر ویژگی‌های محلی و سراسری مینوشیا از برآمدگی خطوط و همچنین شمارش این برآمدگی‌ها استفاده شده است.

بحث و نتیجه‌گیری

آنالیز امنیت

طبق بررسی‌های انجام شده درBIOIDENTIFICATION ویژگی‌های روش‌های مختلف احراز هویت به صورت زیر است:

جدول ۳:ویژگی‌های روش‌های احراز هویت

	بیومتریک	مالکیت شخصی	اطلاعات محرمانه
نمونه	اثر انگشت، چهره،DNA	کلید،کارت شناسایی/ گذرنامه	رمز عبور،PIN
تکثیر	آسان و گاهی دشوار	آسان و گاهی بسیار دشوار	نرم‌افزار
از بین رفتن	خیلی سخت	ساده	فراموش می‌شود
به سرقت رفتن	دشوار	امکان پذیر	جاسوسی
گردش	آسان متمایل به دشوار	ساده	ساده
تغییر	آسان متمایل به بسیار دشوار	ساده	ساده

سیستم‌های بیومتریک به مراتب نسبت به سیستم‌های سنتی قابل اعتمادتر می‌باشند. و از آنجایی که سیستم‌های بیومتریک همیشه همراه فرد است کارآمدتر از روش‌های احراز هویت طبیعی مانند مبتنی بر رمز و یا مبتنی بر دانش است، چون ممکن است فراموش شده، دزدیده شده و یا از دست برود. بیومتریک‌ها امن‌ترین و ساده‌ترین فاکتور تأیید هویت در دنیای اطلاعات و ارتباطات هستند. بیومتریک به روش‌های خودکار تشخیص یا تأیید هویت یک شخص زنده از طریق اندازه‌گیری مشخصه‌های فیزیولوژیک یا رفتاری وی اطلاق می‌شود. طبق جدول(۳) رمزنگاری بیومتریک دارای امنیت بالاتری نسبت روش-های دیگر احراز هویت است. در رمزنگاری بیومتریک امکان دزدیده شدن رمز بسیار مشکل است مخصوصا اینکه از ابزاری برای ارسال اثر انگشت استفاده شود که تشخیص زنده بودن اثر انگشت را داشته باشد. در مقابل رمزهای عبور است، که امکان به سرقت رفتن آنها بیشتر است. همچنین برای امنیت بیشتر نیاز است که چند نکته را در نظر داشته باشید: ۱. کنترل دسترسی ریزدانه ۲. مقاومت در برابر تبانی ۳.ابطال کاربر ۴.محرمانه بودن اطلاعات اما طبق جدول (۴)رمزنگاری مبتنی بر ویژگی ابطال کاربر و محرمانه بودن اطلاعات را پشتیبانی نمی‌کند.

آنالیز عملکرد

بسیاری از الگوریتم‌های تست شده تطبیق مینوشیا نشان می‌دهد هنوز هم یکی از مهم‌ترین روش‌های قابل اعتماد برای تشخیص اثر انگشت است. همچنین طبق بررسی‌هایی که سال۲۰۱۳ درNIST در زمینه اثر انگشت انجام داده است، به این نتیجه رسیده‌اند که با زیاد کردن تعداد نقاط مینوشیا دقت را می‌توان بالاتر برد.

پیاده‌سازی رمزنگاری مبتنی بر ویژگی طرح(Yannis Rouselakis and Brent Waters,2013) بر اساس زبان پایتون است. و روال اجرای آن استفاده از کتابخانه PBC(Ben Lynn) است. زمان سربار تحمیل شده با استفاده از پایتون معمولا کمتر از ۱٪ است. تمام محک‌ها با پردازنده اینتل زئون دو هسته‌ای وCPU W3503@2.40GHz با 2.0GB RAM اجرا شده‌اند. و اجرای آن‌ها در اوبونتو R10.04 و پایتون ۳,۲,۳ است. طرح OT دارای بالاترین امنیت است و طرح LW دارای امنیت انتخابی است.

جدول ۴:نتایج رمزنگاری مبتنی بر ویژگی

	نوع	طرح	Setup	KeyGen	Encrypt	Decrypt
SS1024	KP-ABE	LW	۰,۵۵۵۳۳	۰,۹۲۸۳۸	۰,۶۹۷۸۳	**۰,۱۰۹۸۸**
		OT	۰,۷۹۰۴۳	۰,۱۳۳۸۹۳	۰,۱۳۵۸۲۰	**۰,۱۷۳۵۷**
		Rouselakis, Waters	۰,۰۷۱۵	۰,۶۲۶۳	۰,۳۹۶۸	**۰,۳۲۵۳**
	CP-ABE	OT	۰,۷۸۹۸۹	۰,۱۳۳۹۳۲	۰,۱۳۵۹۸۷	**۰,۱۷۴۰۴**

در اینجا بهترین حالت رمزنگاری مبتنی بر ویژگی، یعنی منحنی فوق العاده منحصر به فرد(گروه جفت شدن متقارن)، را در نظر گرفته شده است. همان‌طور که مشاهده می‌شود زمان اجرای الگوریتم رمزنگاری مبتنی بر ویژگی در بهترین حالت از زمان اجرای الگوریتم مینوشیا بالاتر است. در نتیجه سرعت اجرای تطبیق مینوشیای بسیار بالاتر است.

در بررسی‌های صورت گرفته در زمینه رمزنگاری مبتنی بر ویژگی هیچ یک دقت این رمزنگاری را درنظر نگرفته‌اند. به همین علت دقت این رمزنگاری از جهات دیگر مورد تحلیل قرار داده شده است.

جدول ۵:معیارهای یک طرح ایده‌آل رمزنگاری مبتنی بر ویژگی(**Cheng-Chi Lee et al,2013**)

بخش	ABE	KP-ABE	CP-ABE
محرمانه بودن اطلاعات	N	Y	Y
کنترل دسترسی ریز دانه	Y	Y	Y
مقیاس پذیری	N	N	N
پاسخگویی کاربری	N	N	Y
ابطال کاربر	N	Y	Y
مقاوم در برابر تبانی	Y	Y	Y

تنظیمات اساسی احراز هویت ناشناس برای داشتن بالاترین دقت در شرایط زیر است(**Stefan Rass and Daniel Slamanig, 2014**):

گمنامی[۱۸]، صحت[۱۹]، فراموش نکردن[۲۰]، جلوگیری از تبانی، قابلیت ردیابی[۲۱]، پاسخگویی کاربر و ابطال کاربر.

طبق جدول(۵) طرح رمزنگاری مبتنی بر ویژگی بعضی از تنظیمات اساسی احراز هویت را پشتیبانی نمی‌کند. به عنوان مثال پاسخگویی کاربر که باید مشخص کند که فرد متقلب هست یا نه، که ممکن است فرد متقلب نباشد ولی این نوع احراز هویت آن‌را خاطی شناخته و اجازه ورود به سیستم را به او ندهد. مسأله دیگری که می‌تواند به دقت رمزنگاری مبتنی بر ویژگی ضربه بزند نداشتن ابطال کاربر است. ابطال کاربر به این معنی است که، فرد غیر مجاز از مجموعه کاربران مجاز حذف شود. اگر طرح ابطال کاربر وجود نداشته باشد می‌تواند امنیت سیستم را هم دچار مشکل کند.

[۱۸] Anonymity
[۱۹] Correctness
[۲۰] Unforgeability
[۲۱] Traceability

نتیجه‌گیری

رایانش ابری یک چالش جدید را با عنوان سناریو اعتماد باز کرده است. متاسفانه در کنترل دسترسی داده‌های سنتی معمولاً فرض می‌کنیم داده‌ها در سرور قابل اعتماد ذخیره شده است. در جامعه امروز ما تشخیص هویت به صورت خودکار نقش مهمی ایفا می‌کند. بیومتریک که به شناسایی یک فرد بر اساس ویژگی‌های فیزیولوژیکی و یا رفتاری می‌پردازد، نسبت به روش‌های سنتی تعیین هویت مانند شماره رمز، بسیار قابل اعتمادتر می‌باشد. امروزه استفاده از اثر انگشت به عنوان یک تکنیک بیومتریک بسیار رایج است. در این سیستم بیومتریکی، اثر انگشت یک عامل کلیدی برای احراز هویت است. که فضای ذخیره-سازی امن و سرعت پردازش بالاتر را رایانش ابری می‌تواند بدست آورد. بیومتریک از آنجایی که به صاحبان آن‌ها به شدت مرتبط است، نقش مهمی در احراز هویت دارا می‌باشد. با رشد روزافزون تجارت الکترونیک و دولت الکترونیک، می‌توان انتظار داشت که سیستم‌های احراز هویت مبتنی بر بیومتریک در آینده نزدیک بیشتردر شبکه‌های باز مستقر شوند. با این حال، با توجه به باز بودن آن، در اینترنت چالشی بزرگ برای امنیت و حفظ حریم خصوصی و احراز هویت بیومتریک وجود دارد. در این پژوهش یک طرح دستیابی به احراز هویت اثر انگشت و حفظ حریم خصوصی، که در آن الگوریتم تطبیق بر اساس مینوشیا به همراه ساختارهای محلی و سراسری و برآمدگی خطوط اثر انگشت است، ارائه شده است. که کمک می‌کند تا کاهش پیچیدگی محاسباتی و ارتباطی را داشته باشیم. در واقع، مجموعه ویژگی مینوشیا محبوب‌ترین مورد برای استفاده در سیستم‌ها به دلیل تطبیق مبتنی بر مینوشیا است. به این دلیل که در مقابل اعوجاج در کاربردهای تجربی قوی‌تر است. بنابراین این سیستم‌ها طبق بررسی‌های انجام شده دارای دقت و سرعت بالایی در تطبیق هستند. حال آن‌که با این طرح به کارایی بالاتری دست یافته شده است. طبق بررسی‌هایی که از نظر امنیت و کارایی انجام شده، رمزنگاری اثر انگشت که تطبیق آن بر اساس مینوشیا است، برای کنترل دسترسی و احراز هویت نسبت به رمزنگاری مبتنی بر ویژگی دارای سرعت و دقت بیشتری در الگوریتم تطبیق است. و همچنین امنیت بسیار بالایی نسبت به رمزنگاری‌های مبتنی بر ویژگی دارد.

مراجع

محمودی, ع., ۱۳۸۴. *روشی موثر جهت تطابق تصاویر اثر انگشت*, تهران: صنعتی شریف.

محفوظی، .1392 *,استفاده از رمزنگاری تابعی برای مدیریت داده های رمزشده* ,تهران :صنعتی شریف.

منیره عبدوس، ناصر مزینی, ۱۳۸۷. تطبیق بخشی از اثرانگشت با استفاده از ویژگی ترکیبی مبتنی بر مشخصه های اصلی. نشریه علمی پژوهشی انجمن کامپیوتر ایران, 20-12 .pp.

Ferraiolo DF and Kuhun DR. 1992. Role Based Access Control. Proceeding of 15th National Computer Security Conference, Baltimore MD. pp. 554-563.

A. Pimlott and O. Kiselyov. 2006. SOUTEI, A Logic Based Trust Management System. Proceeding of 8th international symposium on Functional and Logic Programming, Springer, Japan. pp. 130-144.

M. Blaze and J Feigenbaum *et al*. The Keynote trust management system. Version 2, IETF RFC 270.

A. Sahai and B. Waters, "Fuzzy identity based encryption," in *Proc. Acvances in Cryptology—Eurocrypt*, 2005, vol. 3494, LNCS, pp. 457–473.

B. cha, J Seo and J. Kim. 2011. Design of Attribute Based Access Control in cloud computing. Proceeding of International conference on IT convergence and Security, Springer. pp. 41-50.

Jun Yan, Miao Zhou, Yi Mu, Willy Susilo, Man Ho Au, 2011. *Privacy-Preserved Access Control for Cloud Computing*, Australia: IEEE.

Jin Li, Gansen Zhao, Xiaofeng Chen, Dongqing Xie,Chunming Rong, Wenjun Li, Lianzhang Tang, Yong Tang, 2010. *Fine-grained Data Access Control Systems with User Accountability in Cloud Computing*, China: 2nd IEEE International Conference on Cloud Computing Technology and Science.

V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in *Proc. Of CCS'06*, 2006.

S. Greenberg, M. Aladjem, D. Kogan, and I. Dimitrov. Fingerprint image enhancement using filtering techniques. In *Pattern Recognition, 2000. Proceedings. 15th International Conference on*, volume 3, pages 322–325. IEEE, 2000

D. Maio and D. Maltoni. Direct gray-scale minutiae detection in fingerprints. *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, 19(1):27–40, 1997

D.Maio, D. Maltoni, J. L. Wayman, and A. K. Jain, "FVC2002:second fingerprint verification competition," in *Proceedings of the International Conference on Pattern Recognition*, pp. 811–814, IEEE, Quebec, Canada, 2002.

S. E. R. Henry, *Classification and uses of finger prints*: George Routledge and Sons, 1900.

Q. Tang, J. Bringer, H. Chabanne, and D. Pointcheval, "A formal study of the privacy concerns in biometric-based remote authentication schemes," in *Information Security Practice and Experience*, vol. 4991 of *Lecture Notes in Computer Science*, pp.56–70, Springer, Berlin, Germany, 2008.

Kai Xi, Tohari Ahmad, Fengling Han and Jiankun Hu, 2010 .*A fingerprint based bio-cryptographic security protocol designed for client/server authentication in mobile computing environment* ,Melbourne: Wiley Online Library.

Mr. S.Nagaraju,Dr. Latha Parthiban,Mr. B.Santhosh Kumar, 2013 .An Enhanced Symmetric Role-Based Access Control Using Fingerprint Biometrics for Cloud Governace .*Parallel and Cloud Computing Research* ,1(2) ,pp. 11-16.

R. C. Gonzalez, and R. E. Woods, *Digital Image Processing*, Prentice Hall, Second Edition, 2002.

R. C. Gonzalez, R. E. Woods, and S. L. Eddins, *Digital Image Processing Using MATLAB*, Pearson Prentice Hall, First edition, 2004.

http://bias.csr.unibo.it/fvc2006/default.asp

https://biolab.csr.unibo.it/FvcOnGoing/UI/Form/Home.aspx

http://www.bromba.com/faq/biofaqe.htm#bioauthentication

http://www.nist.gov/

Yannis Rouselakis,Brent Waters, 2013. *Practical Constructions and New Proof Methods for Large Universe Attribute-Based Encryption*, Berlin, Germany: ACM 978-1-4503-2477-9/13/11.

Ben Lynn. The Stanford pairing based crypto library. http://crypto.stanford.edu/pbc.

Cheng-Chi Lee, Pei-Shan Chung, Min-Shiang Hwang, 2013. A Survey on Attribute-based Encryption Schemes of Access Control in Cloud Environments. *International Journal of Network Security*, 15(4), pp. 231-240.

Stefan Rass,Daniel Slamanig, 2014 .Protection of Identifying Information.*Cryptography for Security and Privacy in Cloud Computing* .Norwood,Massachusetts: U.S. Library of Congress, British Library ,p. 59