**دانشگاه صنعتی خواجه نصیرالدین طوسی**

**دانشکده مهندسی صنایع**

# بهبود سرعت شناسایی گوینده در سیستم‌های با تعداد گوینده بالا با استفاده از خوشه‌بندی سلسله مراتبی

**امین پروانه**

**استاد راهنما:** دکتر رضا بشیرزاده

**پایان نامه برای اخذ درجه کارشناسی ارشد**

**در رشته مهندسی فناوری اطلاعات گرایش تجارت الکترونیکی**

**مهر ۱۳۹۰**

**دانشگاه صنعتی خواجه نصیرالدین طوسی**

**دانشکده مهندسی صنایع**

# بهبود سرعت شناسایی گوینده در سیستم‌های با تعداد گوینده بالا با استفاده از خوشه‌بندی سلسله مراتبی

**امین پروانه**

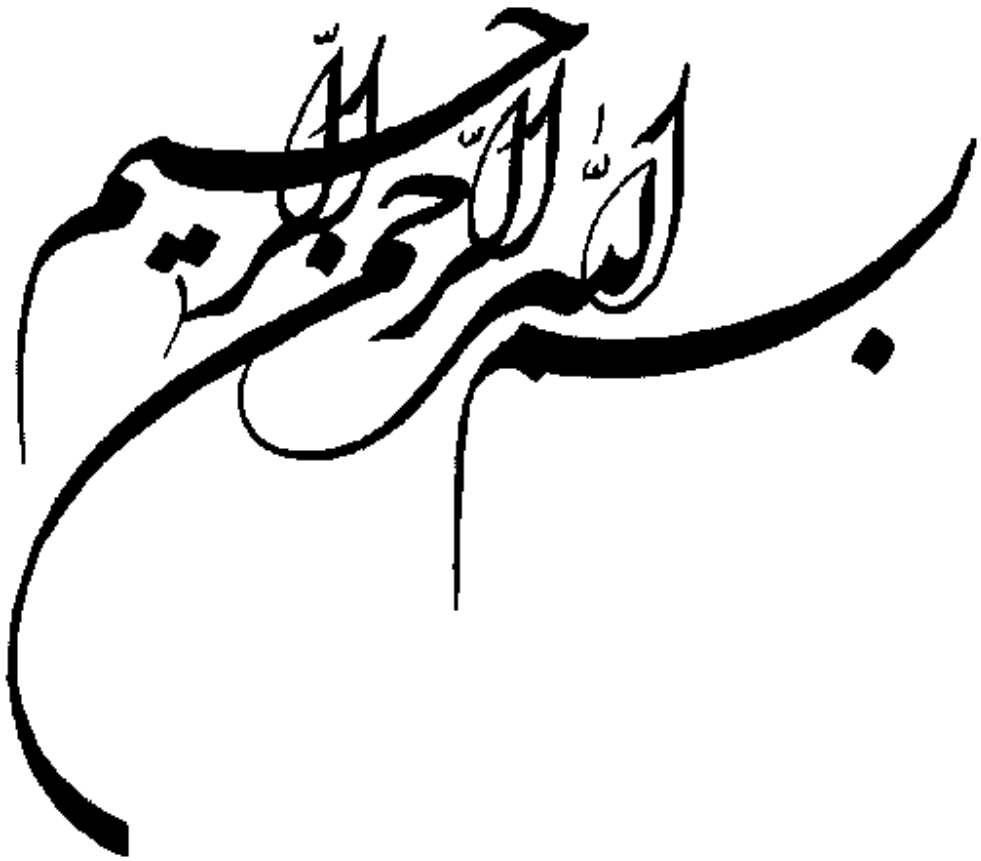
**استاد راهنما:** دکتر رضا بشیرزاده

**استاد مشاور**: دکتر شهریار محمدی

**پایان نامه برای اخذ درجه کارشناسی ارشد**

**در رشته مهندسی فناوری اطلاعات گرایش تجارت الکترونیکی**

**مهر ۱۳۹۰**


بسم الله الرحمن الرحيم

**تقدیم به پدر و مادر عزیزم**

# اظهار نامه دانشجو

**موضوع پایان نامه: بهبود سرعت شناسایی گوینده در سیستم‌های با تعداد گوینده بالا  با استفاده از خوشه‌بندی سلسه مراتبی**

**استاد راهنما: دکتر رضا بشیرزاده**

**نام دانشجو: امین پروانه**

**شماره دانشجویی: ۸۸۰۶۹۹۴**

اینجانب **امین پروانه** دانشجوی دوره کارشناسی ارشد مهندسی فناوری اطلاعات گرایش تجارت الکترونیکی دانشکده  مهندسی صنایع  دانشگاه صنعتی خواجه نصیرالدین طوسی گواهی می نمایم که تحقیقات ارائه شده در این پایان نامه توسط شخص اینجانب انجام شده و صحت و اصالت مطالب نگارش شده مورد تائید می‌باشد و در موارد استفاده از کار دیگر محققان به مرجع مورد استفاده اشاره شده است. به علاوه گواهی می‌نمایم که مطالب مندرج در پایان‌نامه تاکنون برای دریافت هیچ نوع مدرک یا امتیازی توسط اینجانب یا فرد دیگری در هیچ جا ارائه نشده و در تدوین متن پایان‌نامه چارچوب مصوب دانشگاه رعایت شده است.

**امضاء دانشجو:**

**تاریخ**

# حق طبع و نشر و مالکیت نتایج

# تقدیر و تشکر

خداوند بزرگ را سپاسگزارم که به من توفیق داد تا انجام این تحقیق را به پایان برسانم.

آنچه در ادامه می آید، تلاشی است که بی شک بدون کمک و همراهی بزرگوارانی میسر نمی گشت:

از استاد گرامی جناب آقای دکتر رضا بشیرزاده به علت رهنمود های ارزشمندشان در مسیر انجام این تحقیق قدردانی می کنم.

از استاد ارجمند جناب آقای دکتر شهریار محمدی به پاس رهنمود های بی شائبه شان در طول انجام این تحقیق تشکر می کنم.

# چکیده

شناسایی هویت مطمئن یک اصل اساسی برای شروع یک تراکنش تجاری می‌باشد. استفاده از بیومتریک‌ها می‌تواند باعث بالارفتن امنیت، سرعت و سادگی سیستم‌های شناسایی هویت شود. صدا به عنوان یک بیومتریک با دقت نسبتا بالا، سادگی استفاده و پیاده‌سازی بالا، هزینه کم و پذیرش بالای کاربر، یک گزینه مناسب برای این منظور می‌باشد که تا کنون به شکل گسترده‌ای مورد استفاده قرار گرفته است. یکی از مشکلات سیستم‌های شناسایی گوینده معمول، سرعت کم این سیستم‌ها در زمان شناسایی می‌باشد که با افزایش تعداد گوینده‌ها به صورت خطی کاهش می‌یابد. علت این امر این است که در این سیستم‌ها یک مقایسه‌ی 1:N بین گوینده‌ی ناشناس و گویندگان ثبت شده در سیستم صورت می‌پذیرد. استفاده از خوشه-بندی برای قرار دادن گوینده‌های شبیه به هم در یک خوشه و چند مرحله‌ای شدن شناسایی (ابتدا شناسایی نزدیکترین خوشه در یک یا چند مرحله و سپس شناسایی نزدیکترین گوینده قرار گرفته در آن خوشه) یکی از مهمترین کارهایی است که در این زمینه صورت گرفته است. در این تحقیق یک سیستم شناسایی گوینده طراحی شده است و نتایج آن در حالت معمول با کارهای مشابه تطابق داده شده است. پس از آن برای بهبود سرعت سیستم از روش خوشه‌بندی سلسله مراتبی تجمعی پایین به بالا به شکلی جدید استفاده شده است. در این روش برای ساختن یک گوینده مجازی به عنوان نماینده یک خوشه، از داده‌های همه‌ی گویندگان عضو آن استفاده می‌شود. ۵ الگوریتم متفاوت بر اساس روش خوشه‌بندی پیشنهادی طراحی و مورد استفاده قرار گرفته‌اند. تفاوت اصلی این الگوریتم‌ها در نحوه محاسبه‌ی فاصله‌ی بین دو خوشه و نیز در نحوه‌ی ایجاد ساختار سلسله مراتبی (نحوه‌ی انتخاب خوشه‌ها برای ترکیب) می‌باشد. نتایج این تحقیق، با توجه به طراحی در شرایط مشابه، با نتایج الگوریتم K-Means، که از کاراترین الگوریتم‌های مورد استفاده در این زمینه تاکنون به شمار می‌رود، مقایسه شده است که نشان‌دهنده‌ی بهبود دقت در سرعت یکسان می‌باشد.

واژگان کلیدی: بیومتریک، شناسایی گوینده، MFCC، مدلسازی GMM، خوشه‌بندی سلسله مراتبی، فاصله KL.

# فهرست مطالب

# فهرست جداول

# فهرست شکل‌ها

# ۱- فصل اول: کلیات

## ۱-۱ مقدمه

با وجود رشد و گسترش تجارت الکترونیکی در سرتاسر جهان، امروزه این تراکنش‌ها به محملی برای انجام سرقت‌ها تبدیل شده است. سازمان‌های زیادی هر ساله در این زمینه مورد حملات قرار می‌گیرند و ضررهای زیادی را متحمل می‌شوند. بسیاری از این خسارات به علت نبود سیستم امنیتی مناسب در سازمان‌ها و نیز نقائص امنیتی شکل می‌گیرند. بسیاری از گزارشگران و مشاوران هزینه خسارات مرتبط با نقائص امنیتی را تا میلیاردها دلار برآورد کرده‌اند (وانگالا و ساسی[1]، ۲۰۰۴). امنیت کم این سیستم‌ها باعث می‌شود که مشتریان نیز از سیستم استفاده ننمایند و سیستم تجاری با شکست مواجه شود.

احراز هویت افراد برای آغاز یک تراکنش تجاری، بسیار مهم است. در ابتدای هر تراکنش تجاری، بایستی حتما هویت فرد مورد نظر شناخته‌شده و سپس تراکنش اصلی انجام شود. یکی از مراحلی که ممکن است یک سیستم تجاری دچار حمله شود، مرحله‌ی احراز هویت می‌باشد که در این صورت سیستم می‌تواند دچار اختلالات اساسی شود. استفاده از ویژگی‌های بیومتریکی برای احراز هویت افراد، به جای رمزهای عبور و کارت‌ها، یکی از کارهایی است که برای احراز هویت مطمئن افراد بکار می‌رود. استفاده از ویژگی‌های منحصربه‌فرد از افراد برای احراز هویت، می‌تواند راهکار مناسبی برای مقابله با حملات مربوط به احرز هویت باشد. صدا به عنوان یک بیومتریک، راه حل مناسبی برای رفع مسئله احراز هویت امن می‌باشد.

در این فصل ابتدا کلیاتی درباره سیستم‌های احراز هویت و سیستم‌های بیومتریکی بیان می‌شود. سپس انواع بیومتریک‌های رایج معرفی شده و ویژگی‌های آن‌ها مورد بررسی قرار می‌گیرد. همچنین هدف و سوالات این تحقیق بیان شده و ساختار کلی پایان‌نامه توصیف می‌گردد.

1 Vangala & Sasi

## ۲-۱ سیستم‌های بیومتریک

بر اساس استاندارد X9.49 تعریف شده در استاندارد ANSI، زمانی که یک فرد به سیستم وارد می‌شود، سه راه برای شناخت او در سیستم وجود دارد (ماتیاس جی آر و استاپلتون[1]، ۲۰۰۰):

۱. بر اساس یک چیزی که فرد می‌داند (فاکتور شناخت) مانند رمز عبور و یا یک عدد شناسایی شخصی (PIN)[2].

۲. بر اساس چیزی که فرد در اختیار دارد (فاکتور مالکیت) مانند یک کارت مغناطیسی یا یک کلید ذخیره شده بر روی یک کارت هوشمند.

۳. بر اساس چیزی که فرد هست (فاکتور بیومتریکی) مانند ویژگی‌های قابل اندازه‌گیری رفتاری و یا زیستی که به شکل مطمئنی افراد را از هم متمایز می‌کند و می‌توانند برای تایید هویت افراد استفاده شوند.

به طور کلی هر ویژگی فیزیولوژیکی می‌تواند برای تشخیص هویت بکار رود؛ هرچند که تاکنون بیشتر از ویژگی‌هایی مانند اثر انگشت، صورت، عدسی چشم، شبکیه چشم، هندسه دست، صدا و امضا استفاده شده است (لوئیس-گارسیا[3] و همکاران، ۲۰۰۳). استفاده از فاکتورهای بیومتریکی می‌تواند مزایای امنیت بالای رمزهای طولانی را با سرعت و سادگی رمزهای کوتاه به همراه داشته باشد (راتا[4] و همکاران، ۲۰۰۱). وسایل بیومتریکی از سالهای ۱۹۷۰ وجود دارند و مورد استفاده قرار گرفته‌اند و در حال حاضر نیز در جاهای

1 Matyas Jr & Stapleton
2 Personal Identity Number
3 Luis-Garcia
4 Ratha

مختلف و در کاربردهای متفاوت مورد استفاده قرار می‌گیرند (ماتیاس جی آر و استاپلتون، ۲۰۰۰). برای یک تکنولوژی بیومتریک امن به طور کلی دو کاربرد اساسی وجود دارد (وترو[1] و همکاران، ۲۰۰۹):

۱. **کنترل دسترسی**[2]: در این کاربرد که پیش‌نیاز آن تشخیص هویت بیومتریکی است، به کاربرانی که بیومتریک آنها شناسایی شده است، اجازه دسترسی به مولفه‌های سیستم داده می‌شود. در این کاربرد، ویژگی بیومتریک دریافت‌شده از طریق مقایسه با جدولی از ویژگی‌های بیومتریک‌های اصلی ذخیره‌شده در سیستم، شامل یک بیومتریک مدعی یا همه‌ی بیومتریک‌های ذخیره‌شده، تایید می‌شود (همانند روال سیستم‌های بر اساس کلمه رمز).

۲. **مدیریت کلید**[3]: هدف سیستم بیرون‌کشیدن یک کلید رمزنگاری ماندگار از بیومتریک کاربر است. در این کاربرد بیومتریک دریافت‌شده به عنوان یک رمز مشترک که یک کلید رمزنگاری (رمزگشایی) از آن ایجاد می‌شود، مورد استفاده قرار می‌گیرد.

سیستم‌های تشخیص هویت بیومتریکی می‌توانند به دو شکل مورد استفاده قرار گیرند (لوئیس-گارسیا و همکاران، ۲۰۰۳):

۱. **تایید هویت**[4]: در تایید هویت یک کاربر ادعا می‌کند که شخص خاصی است و سیستم با مقایسه‌ی بیومتریک او با بیومتریک ذخیره شده برای آن شخص در پایگاه داده، این ادعا را می‌پذیرد و یا رد می‌کند.

1 Vetro
2 Access Control
3 Key Management
4 Verification/Authentication

۲. **شناسایی هویت**[1]: در شناسایی هویت کاربر بیومتریک خود را به سیستم ارائه می‌دهد و سیستم با مقایسه‌ی آن با تک‌تک بیومتریک‌های ذخیره‌شده در پایگاه داده، تشخیص می‌دهد که او چه کسی است (در صورتی که قبلا در سیستم ثبت‌نام کرده باشد).

شناسایی هویت نسبت به تایید هویت بیشتر در مقالات مورد توجه قرار گرفته است، چرا که در شناسایی هویت تعداد مقایسه بیشتری باید صورت پذیرد و این باعث افزایش زمان شناسایی شده و احتمال خطای کلی نیز با افزایش گونه ها افزایش می یابد و یکی از موضوعاتی که امروزه توجه زیادی به آن می‌شود، کاهش سرعت شناسایی در این سیستم‌ها می‌باشد (داگمن[2]، ۱۹۹۹).

## ۱-۳ ویژگی‌های سیستم‌های بیومتریکی

یک سری از ویژگی‌هایی که اجازه می‌دهد سیستم‌های تشخیص هویت مختلف را متمایز کنیم و مشخص کنیم که چگونه این سیستم‌ها با زمینه‌های مختلف تطابق می‌یابند، عبارتند از (لوئیس-گارسیا و همکاران، ۲۰۰۳): (۱) دقت و قابلیت اعتماد[3]، یعنی اینکه ارائه‌ی یک کلمه رمز درست در یک سیستم احراز هویت، همواره باعث پذیرش درست یک نفر شود و در غیر این صورت رد شود؛ (۲) سادگی استفاده؛ (۳) پذیرش کاربر؛ (۴) سادگی پیاده سازی؛ و (۵) هزینه. در جدول ۱-۱ این ویژگی‌ها را برای بیومتریک‌های مختلف ملاحظه می‌نمایید.

1 Identification
2 Daugman
3 Reliability

**جدول ۱-۱** ویژگی های بیومتریک های مهم (لوئیس-گارسیا و همکاران، ۲۰۰۳)

| نوع بیومتریک | دقت | سادگی استفاده | پذیرش کاربر | سادگی پیاده سازی | هزینه |
|---|---|---|---|---|---|
| اثر انگشت | بالا | متوسط | پایین | بالا | متوسط |
| هندسه دست | متوسط | بالا | متوسط | متوسط | بالا |
| صدا | متوسط | بالا | بالا | بالا | پایین |
| شبکیه چشم | بالا | پیین | پایین | پایین | متوسط |
| عنبیه | متوسط | متوسط | متوسط | متوسط | بالا |
| امضا | متوسط | متوسط | بالا | پایین | متوسط |
| صورت | پایین | بالا | بالا | متوسط | پایین |

دقت و کاربرپسند[۱] بودن احراز هویت می‌تواند با استفاده از دو معیار اندازه‌گیری نرخ پذیرش اشتباه (FAR)[۲] و نرخ ردکردن اشتباه (FRR)[۳] به صورت کمّی درآید (اولوداگ[۴]، ۲۰۰۶). معیار FAR احتمال پذیرش یک جاعل برای ورود به سیستم است و معیار FRR احتمال عدم پذیرش یک کاربر درست برای ورود به سیستم است. مکمل یک FRR نرخ پذیرش درست (CAR)[۵] و یا نرخ پذیرش کاربر اصیل (GAR)[۶] را بیان می‌کند ($CAR = 1 - FRR$). شکل ۱-۱ هر دو پارامتر را به طور مشخص نمایش می‌دهد. برای سیستم تشخیص هویت بیومتریکی منحنی ویژگی اجرایی دریافت کننده (ROC)[۷] در شکل ۱-۲ توازن بین CAR و FAR را نمایش می‌دهد (لوئیس-گارسیا و همکاران، ۲۰۰۳).

1 User Convenience
2 False Acceptance Rate
3 False Rejection Rate
4 Uludag
5 Correct Acceptance Rate
6 Genuine Acceptance Rate
7 Receiver Operating Characteristic