پایان نامه دوره کارشناسی ارشد برق

گرایش مخابرات

ادغام در پارامترهای بیومتریک اثرانگشت، صدا و چهره برای تشخیص هویت

حسین سبزعلی زنجانخواه

استاد راهنما:

خانم دکترغزاله سربیشه‌ای

اسفند ماه 1390

بسم الله الرحمن الرحيم

تقدیر و تشکر

هم اکنون که با یاری و استعانت باری تعالی، این طرح تحقیقاتی را با موفقیت به اتمام رسانده‌ام، وظیفه خود می دانم از زحمات استاد ارجمندم **خانم دکتر غزاله سربیشه ای** که در تهیه و تنظیم و ارائه این پایان نامه استاد راهنمای اینجانب بوده‌اند و در تمامی مراحل با سعه‌ی صدر و بزرگواری ابهامات وارده را برطرف نمودند، کمال تشکر و قدردانی را داشته باشم.

ضمنا بر خود لازم می دانم از کمک های بی دریغ دوست و همسر عزیزم **سرکار خانم حانیه ساداتی** و نیز حمایت های **جناب آقای دکتر محمدرضا سبزعلی زنجانخواه** و **آقای دکتر مهدی پورروح الامین** که در کلیه مراحل انجام و سرانجام این پروژه همواره مشوق اینجانب بوده‌اند، سپاسگزاری نمایم.

حسین سبزعلی زنجانخواه

اسفند ماه 1390

چکیده

با توجه به تمام پیشرفت های صورت گرفته در زمینه سیستم‌های تشخیص هویت مبتنی بر پارامترهای بیومتریک هنوز استفاده از این سیستم ها محدود به محیط‌های کوچک اداری و امنیت در دسترسی‌های فیزیکی می باشد. عمده مشکل پیش روی سیستم های بیومتریک برای استفاده‌های تحت شبکه‌ی اینترنت نبود سخت افزارهای مناسب بر روی سیستم‌های شخصی و اداری است. سیستم‌های بیومتریک به طور معمول از سنسورهای گران قیمتی برای دریافت پارامترهای بیومتریک استفاده می کنند که نصب آن‌ها بر روی کامپیوترهای شخصی سبب افزایش قیمت نهایی این محصولات و عدم استقبال کاربران می شود.

در این پروژه (تا حد امکان) سعی شده به کمک سخت افزارهای موجود بر روی برخی از رایانه‌های شخصی، سیستمی با کارایی و امنیت بالا، مبتنی برادغام در سه پارامتر اثرانگشت، صدا و چهره ی کاربران برای کاربردهای آنلاین ارائه شود. نتایج به دست آمده از شبیه سازی های صورت گرفته به روشنی نشان می دهد که تنظیم سیستم برای FRR=0، FAR بسیار ناچیزی ر ا پس از ادغام در پارامترها به همراه دارد که سبب سخت شدن دسترسی برای افراد سودجو بدون قطع خدمات برای افراد حقیقی می شود. همچنین با توجه به این نتایج و احتمال رخ دادن تطابق‌های غلط، شاید هنوز تا طراحی سیستم های بدون نقص مبتنی بر پارامترهای بیومتریک برای کاربردهای آنلاین فاصله ی زیادی باقی مانده باشد، اما هم اکنون هم استفاده از ادغام در پارامترهای بیومتریک به همراه استفاده از نام کاربری و گذرواژه (تنظیم برای FRR=0) به صورت سیستم‌های ترکیبی می تواند امنیت مضاعفی را برای کاربران در دسترسی‌های حساس تحت شبکه فراهم کند.

فهرست:

فهرست اشکال:

فهرست جداول:

فصل اول

مقدمه

مقدمه

امروزه با پیشرفت‌های صورت گرفته در زمینه‌ی انتقال آنلاین داده‌ها، لزوم احراز هویت آنلاین افراد جهت محدود کردن دسترسی افراد غیر مجاز و امنیت انتقال داده‌ها از اهمیت بسیار زیادی برخوردار شده است. همانگونه می‌دانیم، استفاده از روش سنتی گذر واژه و نام کاربری به علت ضعف‌های ذاتی این روش خطرات زیادی را به همراه دارد. لو رفتن گذر واژه‌ها، انتخاب گذر واژه‌های قابل حدس زدن، سختی بخاطر سپردن گذر واژه‌های امن و احتمال فراموشی آن‌ها و در نتیجه قبول ریسک یادداشت کردن این گذر واژه‌ها، همه و همه تنها بخشی از ضعف‌های سیستم‌های مبتنی بر گذر واژه است. حال آنکه در سیستم‌های مبتنی بر پارامترهای بیومتریک به علت آن که نام‌های کاربری و گذر واژه‌ها در واقع بخشی جدا ناشدنی از هویت افراد هستند، غیر قابل سرقت، فراموشی و انتقال می‌باشند.

یک سیستم بیومتریک آنلاین سعی بر آن دارد که با بخاطر سپردن ویژگی‌های منصر به فرد و قابل استخراج مجدد از کاربر بدون تحت فشار قرار دادن فرد برای بخاطر سپردن گذر واژه و یا حمل هر گونه نشانه (کارت‌های مغناطیسی) به نحوی مطمئن و با حداقل احتمال خطا، امکان دسترسی به اطلاعات و خدمات مجاز را فراهم سازد. یکی از مشکلات پیش روی سیستم‌های بیومتریک برای گسترش و متداول شدن (چه در کاربردهای آنلاین و چه در دسترسی‌های فیزیکی) مسأله‌ی سخت افزار است. سیستم‌های بیومتریک برای جمع آوری اطلاعات و پارامترهای بیومتریک احتیاج به سخت افزارهایی دارند که به طور معمول در سیستم‌های کامپیوتر شخصی یافت نمی شوند. همچنین افزودن این امکانات موجب بالا رفتن قیمت تمام شده‌ی محصولات شده و سبب عدم استقبال کاربران از این محصولات می‌گردد.

در این پروژه سعی شده با استفاده از سخت افزارهای متداول و به کمک ادغام در پارامترهای بیومتریک، سیستم بیومتریکی با کارایی بالا و حداقل احتمال خطای ممکن (با توجه به الگوریتم‌ها و سخت افزارهای موجود) ارائه شود. در ادامه فصل دوم را با معرفی اجزای تشکیل دهنده‌ی یک سیستم بیومتریک آغاز کرده و سپس نحوه‌ی مقایسه سیستم‌ها و لزوم ادغام در پارامترهای بیومتریک را مورد بررسی قرار می‌دهیم، در این فصل با توجه به محدودیت‌های موجود سیستمی با کارایی بالا که به حداقل سخت افزارهای جانبی نیازمند باشد را معرفی کرده و در

فصل‌های سوم تا پنجم به طراحی آن می‌پردازیم. در فصل سوم اثر انگشت را به عنوان یکی از پارامترهای انتخاب شده در فصل دوم در دو مرحله‌ی افزایش کیفیت و تطابق مورد بررسی قرار داده و میزان عملکرد چنین سیستمی را در حالت پیش از ادغام و پس از آن مورد مقایسه قرار می‌دهیم. در فصل چهارم به پارامتر بعدی یعنی صدا پرداخته و میزان خطای این سیستم را نیز در حالت قبل از ادغام و پس از آن بیان می‌کنیم. در ادامه و در فصل پنجم به آخرین پارامتر یعنی چهره می‌رسیم و با بیان نکاتی در مورد پایگاه داده‌ی مورد استفاده قرار گرفته به بیان عملکرد سیستم قبل و بعد از ادغام می‌پردازیم. همچنین راه کارهایی را برای گسترش استفاده از این روش و تعمیم به سایر پایگاه‌های داده ارائه می‌کنیم.

در پایان و در فصل ششم و در آخرین مرحله، سه پارامتر اثر انگشت، صدا و چهره را برای ایجاد ده هویت فرضی به یکدیگر متصل کرده و میزان صحت عملکرد سیستم را در شرایط ادغام سه پارامتر مورد بررسی قرار می‌دهیم و نتایج حاصل را به صورت نتیجه گیری و پیشنهاداتی در پایان ارائه می‌کنیم.

فصل دوم

سیستم‌های بیومتریک و ادغام

1-2 مقدمه

سیستم‌های مبتنی بر گذر واژه در مقایسه با سیستم‌های بیومتریک از ساختارهای پیچیده‌ای برای تشخیص هویت استفاده نمی‌کنند. در سیستم‌های مبتنی بر گذر واژه، واژه‌ی رمز باید به طور کامل با واژه‌ی موجود در پایگاه داده‌ی سیستم مطابقت داشته باشد تا امکان دسترسی به اطلاعات و یا خدمات فراهم شود. حال آن که در سیستم‌های بیومتریک به ندرت اتفاق می‌افتد که نتایج حاصل از دریافت دوباره‌ی یک پارامتر به طور کامل مطابق با نتایج قبلی باشد. در واقع یک سیستم بیومتریک باید بتواند تفاوت‌های درون کلاسی (تفاوت‌های ناشی از جمع آوری دوباره‌ی اطلاعات از یک هویت) و برون کلاسی (تفاوت‌های ناشی از جمع آوری اطلاعات از هویت‌های دیگر) را به خوبی از یکدیگر تشخیص دهد.[1]

در ادامه با بررسی ساختار یک سیستم بیومتریک به بررسی نحوه‌ی تایید و یا رد هویت در آن خواهیم پرداخت.

2-2 ساختار یک سیستم بیومتریک

به طور کلی یک سیستم بیومتریک از چهار بخش سخت افزاری و نرم افزاری زیر تشکیل شده است.

1-2-2 بخش سنسور

بخش سنسور بخشی از یک سیستم بیومتریک است که اطلاعات بیومتریک افراد را به کمک سخت افزارهای جانبی از ورودی می‌خواند. مانند: سنسور اثر انگشت، میکروفن برای دریافت صدا و دوربین برای تصویر برداری از چهره و سایر انواع دریافت کننده‌های بیومتریک.

2-2-2 بخش استخراج کننده‌ی ویژگی ها

این بخش که به طور معمول یک بخش نرم افزاری است، ویژگی‌های منحصر به فرد و متمایز کننده‌ی از هویت افراد را به کمک الگوریتم‌هایی از نمونه‌های دریافت شده توسط بخش سنسور استخراج کرده و برای پردازش و ذخیره در پایگاه داده‌ی سیستم آماده می‌کند.

3-2-2 بخش انطباق دهنده

این بخش جزئیات و ویژگی‌های استخراج شده از نمونه (هویت تست) را با اطلاعات و ویژگی‌های موجود در پایگاه داده‌ی سیستم مقایسه کرده و برای این انطباق یک نمره‌ی انطباقی در نظر می‌گیرد. مانند: تعداد و یا درصد انطباق نقاط ویژه[1] در نمونه‌ی اثر انگشت و الگوی ذخیره شده در پایگاه داده‌ی یک سیستم بیومتریک مبتنی بر شناخت اثر انگشت.

4-2-2 بخش تصمیم گیرنده

این بخش با توجه به نمره‌ی انطباقی و یک حد آستانه[1] (که در ادامه به توضیح آن می‌پردازیم.) در مورد تایید انطباق و یا رد آن تصمیم گیری می‌کند.[2]

3-2 نحوه‌ی مقایسه‌ی عملکرد سیستم‌های بیومتریک و تعیین حد آستانه

کارایی سیستم‌های تشخیص هویت مبتنی بر پارامترهای بیومتریک را به طور کلی می‌توان با گزارش میزان تصدیق‌های اشتباه FAR[1] و میزان تصدیق‌های صحیح GAR[1] یا میزان رد کردن‌های اشتباه FRR[1] با هم مقایسه کرد. به طور معمول این فاکتورها را در یک منحنی ROC[1] رسم می‌کنند، سپس با بررسی عملکرد سیستم در قبال افراد حقیقی و افراد سوء استفاده‌گر (به کمک مقایسه‌ی نمره‌های انطباقی این دو دسته) حد آستانه‌ای را برای رد یا قبول انطباق در نظر می‌گیرند.[2]

---

[1] Minutiae Points
[1] Threshold Value
[1] False Acceptance Rate
[1] Genuine Acceptance Rate
[1] False Rejection Rate
[1] Relative Operating Characteristic

4-2 بررسی خصوصیات پارامترهای بیومتریک

در انتخاب یک پارامتر برای طراحی یک سیستم بیومتریک باید به ویژگی‌ها و موارد خاصی توجه کرد که امنیت (به معنای سخت بودن ایجاد یک الگوی دروغین به اندازه‌ی کافی متشابه با الگوی اصلی)، کاربر پسندی (به معنای میل و رغبت کاربر برای ایجاد ارتباط و استفاده از سیستم)، قابلیت جمع آوری (به معنای سهولت نمونه برداری از پارامتر بیومتریک موردنظر)، کارایی (به معنای عملی بودن ا ستفاده از آن در تشخیص هویت)، دوام (به معنای عدم تغییر پارامتر در کاربر با گذشت زمان) و قابلیت ایجاد تمایز (به معنای اینکه پارامتر تا چه اندازه‌ای می‌تواند میان کاربران تفاوت ایجاد کند.) از آن جمله هستند. گذشته از ویژگی‌های ذکر شده برای کاربردهای آنلاین و جهت متداول شدن استفاده از سیستم‌های بیومتریک به جای سیستم‌های مبتنی بر گذر واژه لازم است که این سیستم‌ها با حداقل سخت افزارهای جانبی مورد نیاز کار کنند.

از میان پارامترهای بیومتریک متداول، چهره[1] (دریافت از طریق دوربین‌های موجود بر روی برخی از سیستم‌های شخصی و اکثر لپ تاپ ها)، صدا[2] (دریافت از طریق میکروفن) و اثر انگشت[3] (دریافت از طریق سنسورهای موجود بر روی برخی از انواع لپ تاپ ها) نسبت به سایر پارامترهای بیومتریک از سنسورهای در دسترس‌تر و متداول‌تری برای جمع آوری اطلاعات استفاده می‌کنند. البته باید این نکته را نیز در نظر داشت، که به علت قابلیت ایجاد تمایز پایین صدا در کنار تغییرات ناشی از خواب آلودگی، احساسات و تغییر لحن، عدم وجود نور مناسب در کنار کیفیت پایین دوربین‌های موجود بر روی سیستم‌های شخصی، همچنین تغییرات ایجاد شده بر اثر خشکی، کثیفی و چرب بودن انگشت‌ها در کنار بریدگی‌ها و سایش خطوط در اثر انگشت، استفاده از پارامتر بیومتریک به تنهایی احتمال خطای بالایی را به دنبال خواهد داشت. به همین علت از تلفیق در پارامترهای بیومتریک که به آن ادغام[4] می‌گویند، استفاده می‌گردد. ادغام در پارامترها در سطوح و اشکال گوناگونی انجام می‌شود که هدف تمامی آن‌ها کاهش احتمال خطا FAR و افزایش صحت عملکرد سیستم GAR می‌باشد.

[1] Face
[2] Voice
[3] Fingerprint
[4] Fusion

5-2 ادغام

شاید مهمترین نقطه ضعف یک سیستم بیومتریک، تغییر مداوم پارامتری باشد که برای تشخیص هویت از آن استفاده می‌شود. به عنوان مثال، در یک سیستم تشخیص هویت مبتنی بر چهره، چهره‌ی فرد به طور مرتب با توجه به نوع آرایش، مدل ریش و ابرو، رنگ، بلندی و کوتاهی مو و استفاده از عینک در حال تغییر است. همچنین صدای فرد می‌تواند بر اثر احساسات و یا بیماری دچار تغییر شود و در مورد اثر انگشت همواره چرخش و تغییر فشار دست بر روی اسکنر در کنار سایش برآمدگی‌ها، کثیفی، چرب بودن و یا خشکی پوست موجب تغییرات عمده‌ای می‌شود. این محدودیت‌ها سبب می‌شود که استفاده از یک پارامتر بیومتریک به تنهایی احتمال خطای فراوانی (در سیستم‌های پرکاربر و در حالت استفاده‌ی مکرر از سیستم، یک خطای کوچک $FAR = 0.001\%$ می‌تواند سبب بروز موارد متعددی از خطای تایید غلط در یک دوره‌ی زمانی شود.) را به همراه داشته باشد. در این شرایط ادغام در پارامترهای بیومتریک این امکان را به وجود می‌آورد که سیستم به سطحی از امنیت و کارایی برسد که دسترسی به آن با استفاده از سیستم‌های مبتنی بر یک پارامتر امکان پذیر نیست.

6-2 سطوح ترکیب در سیستم‌های بیومتریک

سطوح ترکیب در سیستم‌های بیومتریک را می‌توان در سه سطح کلی زیر مورد بررسی قرار داد:

- ترکیب در مرحله‌ی استخراج جزئیات
- ترکیب در مرحله‌ی نمره‌ی انطباقی
- ترکیب در مرحله‌ی تصمیم گیری

1-6-2 ترکیب در مرحله‌ی استخراج جزئیات

هر یک از پارامترهای بیومتریک به طور مستقل از ورودی خوانده می‌شوند، به همین علت هر پارامتر دارای نویز و اطلاعات متفاوتی نسبت به نمونه‌های دیگر است. از این رو در صورت ادغام در مرحله‌ی استخراج می‌توان به داده‌هایی با نویز کمتر و اطلاعات خالص‌تر دست یافت.[2]

2-6-2 ترکیب در مرحله‌ی نمره‌ی انطباقی

پس از خواندن مجزای هر پارامتر (همنوع و یا غیر همنوع) توسط بخش سنسور و پس از استخراج ویژگی‌ها، به هر پارامتریک نمره‌ی انطباقی که نشان دهنده‌ی شباهت میان بردار نمونه[1] و الگو[2] است تعلق می‌گیرد. در این مرحله نمرات انطباقی می‌توانند به اشکال گوناگونی با هم تلفیق شده و با احتمال خطای کمتری تایید و یا رد تطابق را اعلام نمایند.[2]

2-6-3 ترکیب در مرحله‌ی تصمیم گیری

ابتدا هر پارامتر توسط بخش سنسور مربوطه از ورودی خوانده می‌شود. در ادامه و پس از استخراج ویژگی‌ها، این جزئیات با جزئیات موجود در پایگاه داده مطابقت داده می‌شوند و برای این تطابق نمره‌ی انطباقی دریافت می‌کنند. در پایان بر اساس این نمرات انطباقی و حد آستانه‌ی مربوط به آن‌ها، انطباق‌ها به دو دسته‌ی رد یا قبول تقسیم می‌شوند و سرانجام یک برنامه‌ی شمارش اکثریت آرا[3] تصمیم نهایی را در مورد رد یا قبول تطابق اتخاذ می‌کند.[2]

2-7 اشکال ترکیب در بیومتریک

اشکال ترکیب در سیستم‌های بیومتریک را می‌توان در سه شکل کلی زیر مورد بررسی قرار داد:

- نمایش چندگانه از یک پارامتر بیومتریک
- انطباق دهنده‌های چندگانه
- ترکیب بیومتریک چندگانه

[1] Query
[2] Template
[3] Majority Voting

1-7-2 نمایش چند گانه از یک پارامتر بیومتریک

در این شکل از ترکیب به جای استفاده از یک الگو در پایگاه داده، از چندین الگو در پایگاه داده استفاده شده و بـه کمک نمایش چندگانه از یک پارامتر سعی می‌شود احتمال خطا تا حد قابل قبولی کاهش یابد.[2] اصول کار در این روش بدین صورت است که چون احتمـال رخ دادن نـویز شـدیدی کـه موجـب از دسـت رفـتن درک صـحیح از ویژگی‌های واقعی در یک مکان خاص به طور مکرر شود (به عنوان مثال، در یک نمونه‌ی دریافتی از بخش سنسـور و پنج الگوی موجود در پایگاه داده) به مراتب کمتر از احتمال دریافت اطلاعات صحیح با نویز قابل چشم پوشی در همان مکان است. احتمال جمع شدن خطاهای ناشی از نویز کم شده (احتمال اشتباه در رد یا تایید انطباق نمونه بـا حداقل سه الگو از پایگاه داده) و سیستم با اطمینان بیشتری نسبت به انطباق نمونه و الگوها اظهارنظر می‌کنـد. البتـه باید به این نکته نیز در نظر داشت که خطای ناشی از اطلاعات واقعی خارج از الگو (عدم پوشش کامل برآمدگی‌ها و فرورفتگی‌ها در اثر انگشت، تغییر لحن صحبت، استفاده از عینک، آرایش، تغییر حالت مو، ریش و ابرو) بـه مراتـب مشکل سازتر از داده‌های نویزی می‌باشد.

2-7-2 انطباق دهنده‌های چندگانه

در این شکل از ترکیب به جای استفاده از یک روش تطابق از چندین (تعداد فرد) روش برای بررسی انطبـاق میـان نمونه و الگو(ها) استفاده می‌شود. سپس نتایج حاصل (که به طور معمول به صـورت رد یـا قبـول تطـابق هسـتند.) توسط یک برنامه شمارش اکثریت آرا شمرده شده و نتیجه جواب سیستم خواهد بود.[2]

به عنوان مثال: دو اثر انگشت را می‌توان به سه روش 1- تطابق نقاط ویژه[1] 2- تطابق الگو[2] و 3- ضرب بـاینری (روش پیشنهادی) با یکدیگر مقایسه کرد و جواب غالب (حداقل دو رای از سه رای) را به عنوان جواب سیستم در نظر گرفت. در این روش امید بر این است که نویزهایی که سبب بروز خطا در روش تطابق نقاط ویژه (تطابق الگو و یا ضرب باینری) می‌شوند بر عملکرد دو روش دیگر بی‌تاثیر باشند.

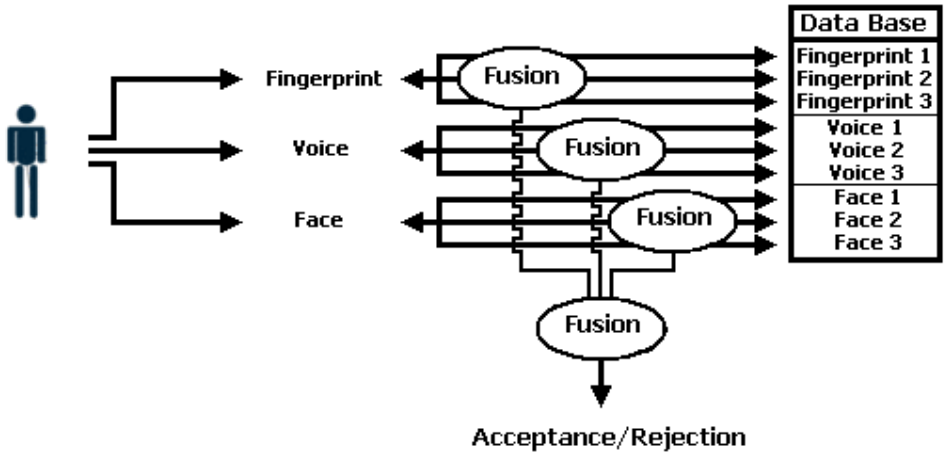
[1] Minutiae Matching
[2] Template Matching

3-7-2 ترکیب بیومتریک‌های چندگانه

در این شکل از ترکیب به جای استفاده از چندین نمونه از یک نوع پارامتر، از یک نمونه از چندین نوع پارامتر (تعداد فرد) استفاده می‌شود. سیستم پس از بررسی مستقل هر یک از پارامترها، مجموعه‌ی جواب‌ها را که به طور معمول به صورت رد یا قبول تطابق هستند، توسط یک زیر برنامه‌ی شمارش اکثریت آرا بررسی کرده و سرانجام بر اساس آن رای به تایید و یا رد تطابق می‌دهد.[2]

همانگونه که پیشتر هم به آن اشاره شد، ادغام در پارامترهای بیومتریک (با افزایش اطلاعات هویتی از کاربران) می‌تواند کارایی و امنیت سیستم‌های بیومتریک را تا حد قابل قبولی ارتقاء دهد. در ادامه یک سیستم تشخیص هویت مبتنی بر ادغام (دو مرحله ای) در پارامترهای بیومتریک را معرفی کرده و در فصل‌های سوم تا پنجم به پیاده سازی عملی آن می‌پردازیم.

طرح کلی سیستم بیومتریک مبتنی بر ادغام پارامترهای اثر انگشت، صدا و چهره برای کاربردهای آنلاین:



شکل شماره‌ی 2-1 : سیستم بیومتریک پیشنهادی برای کاربردهای آنلاین.