بسم الله الرحمن الرحيم

دانشگاه شاهد

دانشکده فنی و مهندسی

پایان‌نامه دوره کارشناسی ارشد مهندسی برق – مخابرات

بهبود تشخیص هویت بر اساس اطلاعات شکل وبافت چهره

مصطفی الحسینی

استاد راهنما:

دکتر رسول خیاطی

زمستان ۱۳۹۰

چکیده

انسان از دیر باز برای شناسایی و تشخیص هویت افراد از ویژگی‌های بیومتریک (زیست سنجی) آنان مانند صورت، صدا یا دست‌خط استفاده می‌کرده است. با وجود اینکه انسان‌ها قادرند حتی در شرایط نامطلوب مانند نور ضعیف و چرخش صورت، چهره فرد مورد نظر را شناسایی کنند، اما سیستم‌های خودکار شناسایی چهره در این شرایط با مشکل روبرو می‌شوند. این امر سبب شده است که مسئله شناسایی چهره همچنان چالش‌انگیز باقی بماند. پیشرفت‌های علمی در زمینه ابزارهای محاسبات دیجیتال در دهه اخیر فصل جدیدی را در تشخیص و شناسایی چهره گشوده است.

در این پایان نامه به ارائه روشی پرداخته خواهد شد که با وجود چرخش صورت و تغییر در شدت روشنایی تصاویر مورد نظر، کارِ شناسایی چهره را با دقت خوبی انجام دهد. در روش پیشنهادی در گام اول توسط روش تبدیل هاف تصادفی[۱] چهره فرد مورد نظر از تصویر ورودی جدا می‌شود. در گام بعد برای تصویر مربوط به هر چهره، یک بردار ویژگی با استفاده از روش فیلتر گابور[۲] و روش مقادیر ویژه چهره[۳] تولید می‌شود. سپس به کمک روش تحلیل مولفه های اصلی[۴] ابعاد بردارهای ویژگی کاهش می‌یابد و در گام آخر با استفاده از یک شبکه عصبی پرسپترون چندلایه[۵] شناسایی چهره در فضای ویژگی تولید شده انجام می‌گیرد.

نتایج حاصل از پیاده‌سازی روش فوق توسط داده‌های پایگاه FEI مورد ارزیابی قرار گرفت، آنچه در این پایان نامه بیان می‌شود به معرفی یک روش شناسایی چهره با دقتی در حدود ۹۱٪ می‌پردازد. امید است در ادامه این کار بتوان گام‌های دیگری را در راستای مقاوم سازی سیستم های شناسایی چهره نسبت به تغییرات مختلف محیطی برداشت.

کلمات کلیدی: مقادیر ویژه چهره، فیلتر گابور، تشخیص چهره[۶]، شناسایی چهره[۷].

[1] Randomized Hough Transform
[2] Gabor Filter
[3] EigenFace
[4] Principle Components Analysis
[5] Multi-Layer Perceptron
[6] Face Detection
[7] Face recognition

فهرست مطالب

عنوان صفحه

فصل ۱- کلیات تحقیق ۱

۱-۱- مقدمه ۱

۱-۲- نیاز به سیستم بیومتری در دنیای مدرن ۱

۱-۳- اهداف شناسایی چهره ۳

۱-۳-۱- تصدیق هویت ۴

۱-۳-۲- شناسایی هویت ۴

۱-۳-۳- فهرست بررسی ۵

۱-۴- رویکرد این پایان نامه ۶

فصل ۲- روش های تشخیص هویت مبتنی بر تشخیص چهره ۷

۲-۱- مقدمه ۷

۲-۲- مروری بر روش‌های تشخیص چهره ۸

۲-۲-۱- تشخیص چهره بر اساس اطلاعات هندسی شکل ۹

۲-۲-۲- تشخیص چهره با شبکه‌های عصبی در تصاویر رنگی ۱۲

۲-۲-۳ روش تشخیص چهره مبتنی بر پردازش مورفولوژیک و تخمین پلک زدن چشم به طور زنده ۱۴

۲-۳- مروری بر روش‌های شناسایی چهره ۱۹

۲-۳-۱- روش مقادیر ویژه چهره ۱۹

۲-۳-۲- روش فیشرفیس ۲۴

۲-۴- خلاصه ۳۰

فصل ۳- بهبود تشخیص چهره بر اساس اطلاعات شکل وبافت چهره ۳۱

۳-۱ مقدمه ۳۱

۳-۲- سیستم تشخیص چهره با استفاده از تبدیل هاف تصادفی ۳۲

۳-۲-۱- تبدیل هاف تصادفی و تشخیص بیضی ۳۲

۳-۲-۲- شرح الگوریتم تبدیل هاف تصادفی ۳۳

۳-۳- سیستم شناسایی چهره با استفاده از EF و فیلتر گابور ۳۹

۳-۳-۱- شناسایی چهره با استفاده از تحلیل مولفه های اصلی(PCA) یا EF ۳۹

۳-۳-۲- شناسایی چهره با استفاده از فیلتر گابور ۴۱

۳-۴- روش شناسایی چهره به روش ترکیبی فیلتر گابور با EF ۴۴

فصل ۴- نتایج ۴۵

۴-۱- مقدمه ۴۵

۴-۲- پایگاه های داده ۴۵
۴-۲-۱- پایگاه داده CMU ۴۵
۴-۲-۲- پایگاه داده FEI ۴۶
۴-۳- پیاده سازی سیستم آشکارسازی چهره ۴۶
۴-۳-۱- پیش پردازش تصویر برای آشکارسازی چهره ۴۷
۴-۳-۲- لبه یابی و اتصال لبه ۴۸
۴-۳-۳- تشخیص بیضی چهره با استفاده از تبدیل هاف تصادفی ۴۸
۴-۴- پیاده سازی سیستم شناسایی چهره ۵۰
۴-۴-۱- پیش پردازش تصویر برای شناسایی چهره ۵۰
۴-۴-۲- استخراج بردارهای ویژگی ۵۰
۴-۵- ساختار شبکه عصبی و ارزیابی نتایج شناسایی چهره ۵۴
۴-۵-۱- ساختار پایه‌ی شبکه های عصبی مورد استفاده ۵۴
۴-۵-۲- شناسایی چهره با به کارگیری ویژگی هایEF ۵۵
۴-۵-۳- شناسایی چهره با به کارگیری ویژگی های GF ۵۵
۴-۵-۴- شناسایی چهره با به کارگیری روش پیشنهادی ۵۶
فصل ۵- بحث نتیجه گیری وپیشنهادات ۵۷
فهرست مراجع ۶۰

فهرست اشکال

شماره شکل صفحه

شکل ۱-۱- اصلی ترین سوال مطرح در تصدیق هویت در شناسایی چهره ۴
شکل ۱-۲- شناسایی هویت در شناسایی چهره. ۵
شکل ۲-۱- بلوک دیاگرام روش تشخیص چهره بر اساس اطلاعات شکل. ۹
شکل ۲-۲- اثر متعادل سازی هیستوگرام بر لبه یابی تصاویر... ..... ۱۰
شکل ۲-۳- تاثیرات فیلتر میان گذر... ..... ۱۱
شکل ۲-۴- اتصال لبه ها بطور پیوسته... ..... ۱۱
شکل ۲-۵- تشخیص چهره با شبکه عصبی ۱۳
شکل ۲-۶- نتایج بکارگیری شبکه عصبی برای تشخیص چهره از روی تصاویر رنگی. ۱۴
شکل ۲-۷- فلوچارت الگوریتم ۱۵
شکل ۲-۸- نمونه‌های آموزشی مثبت و منفی ۱۷
شکل ۲-۹- اندازه گیری فاصله میان چشم ها و شدت بازشدن چشم‌ها ۱۸
شکل ۲-۱۰- مولفه های اصلی نقاط دو بعدی ۲۰
شکل ۲-۱۱- نمونه‌ی ۲۰ نفری. ۲۳
شکل ۲-۱۲- تصویر میانگین. ۲۳
شکل ۲-۱۳- بردارهای ویژه به ترتیب از بزرگترین به کوچکترین. ۲۳
شکل ۲-۱۴- دسته بندی با کمک PCA , LDA ۲۵
شکل ۲-۱۵- جدا ساز فیشر. ۲۵
شکل ۲-۱۶- توزیع غیرگوسی ۲۹
شکل ۲-۱۷- حالتی که داده‌ها در پراکندگی هستند نه در مرکز ۲۹
شکل ۳-۱- بلوک دیاگرام مربوط به سیستم تشخیص چهره. ۳۲
شکل ۳-۲- آناتومی بیضی ۳۵
شکل ۳-۳- یافتن مختصات مرکز بیضی با تعیین محل تقاطع نیمساز های حاصل از... ..... ۳۷
شکل ۳-۴- چرخش محور (x,y) حول مبدا مختصات به اندازه θ و وتشکیل..... ..... ۳۸
شکل ۳-۵- بلوک دیاگرام مربوط به روش PCA برای استخراج بردارهای ویژگی از تصویر. ۳۹
شکل ۳-۶- نمایی از اعمال فیلترهای گابور پنج کانال به تصویر ورودی. ۴۳
شکل ۳- ۷- بلوک دیاگرام مربوط به روش ترکیبی فیلتر گابور با EF. ۴۴
شکل ۴-۱- نمونه‌های از تصاویر پایگاه داده ی FEI برای یک نفر. ۴۶
شکل ۴-۲- تصاویر ورودی به سیستم آشکارسازی چهره ۴۷
شکل ۴-۳- تصاویر حاصل از عملیات پیش پردازش. ۴۸
شکل ۴-۴- تصاویر ورودی به سیستم آشکارسازی چهره پس از لبه یابی و اعمال اتصال لبه ها... ۴۹

شکل ۴-۵- نتیجه پیاده سازی الگوریتم تبدیل هاف تصادفی برای دو تصویر نمونه ورودی. ۴۹
شکل ۴-۶- بلوک دیاگرام سیستم شناسایی چهره. ۵۰
شکل ۴-۷- بیست تصویر نمونه از پایگاه دادهی FEI. ۵۱
شکل ۴-۸- بردارهای ویژه به ترتیب از بزرگترین به کوچکترین. ۵۱
شکل ۴-۹- یک تصویر نمونه از پایگاه دادهی FEI. ۵۲
شکل ۴-۱۰- اندازه پاسخ فیلتر گابور برای ورودی شکل بالا. ۵۳
شکل ۴-۱۱- هیستوگرام تصویر خروجی فیلتر گابور. ۵۳
شکل ۴-۱۲- ساختار یک شبکه عصبی MLP با یک لایه پنهان. ۵۴

فهرست جداول

شماره جدول صفحه

جدول ۲-۱- نتایج دنباله های زنده ۱۹
جدول ۲-۲- مقایسه نتایج پیاده سازی روش‌های صورت ویژه، فیشرفیس و ICA ۳۰
جدول ۴-۱- نتایج شناسایی را با روش EF با تغییر دو پارامتر مذکور نشان می دهد. ۵۵
جدول ۴-۲- نتایج شناسایی را با روش GF با تغییر دو پارامتر مذکور نشان می دهد. ۵۶
جدول ۴-۳- نتایج شناسایی را با روش پیشنهادی با تغییر دو پارامتر مذکور نشان می دهد. ۵۶
جدول ۵-۱- نتایج شناسایی را با روش GF با تغییر دو پارامتر مذکور نشان می دهد. ۵۸

فصل ۱– کلیات تحقیق

۱–۱– مقدمه

از گذشته‌های دور، تفاوت و تمایز میان انسان‌ها به دلایل گوناگون همواره مورد توجه بوده، به طوری که در کتب مختلف به این نکته اشاره شده است. قرآن کریم تفاوت انسان‌ها را از نظر رنگ، لهجه، زبان و چهره را به عنوان نشانه ای برای اهل تفکر و خرد دانسته است.
این تفاوت‌ها که از ویژگی‌های رفتاری و جسمی انسان ها نشأت گرفته است، از دیرباز به شیوه نیمه آگاهانه برای شناسایی افراد مورد استفاده قرار گرفته است. این توانایی در طی قرون و اعصار بر اثر تکامل نوع بشر، در انسان ایجاد و از نسلی به نسل دیگر انتقال و بهبود یافته است. در قرن اخیر که به قرن دیجیتال مشهور است، پژوهشگران کوشیده‌اند تا این توانایی را مکانیزه نمایند. حاصل این تلاش‌ها و تحقیقات منجر به کشف ویژگی‌های زیست سنجی دیگری نیز شده، که پیش از آن بشر توانایی درک آن را نداشت. این ویژگی ها در سیستم‌های مدرن امروزی که شامل حسگر و سیستم‌های پردازنده می‌باشد، مورد استفاده قرار می‌گیرند. امروزه سیستم‌های زیست سنجی در زندگی روزمره کاربردهای گسترده‌ای در زمینه های مختلف پیدا کرده اند.

۱–۲– نیاز به سیستم بیومتری در دنیای مدرن

در نگاهی گذرا به دنیای مدرن می‌توان دریافت، که محدوده‌ها و فضاهای اختصاصی که برای هر شخص به طور مجزا تعریف شده، به وفور در پیرامون ما وجود دارد. از این قبیل، می‌توان به محدوده‌هایی مانند منازل، ادارات، حساب‌های بانکی و ... اشاره نمود که مکانیزه شدن دسترسی به آن، موجب آسانی و تسهیل امور گشته است. با این حال، یکی از بزرگ‌ترین دغدغه‌های مدیران این سیستم‌ها موضوع امنیت در این مکانیزم‌ها می‌باشد. ایجاد نام کاربری و اسم رمز برای کارت‌های مختلف، یکی از راهکارهای پیشنهادی برای حل این مشکل است؛ هرچند این راه حل دسترسی را محدود می‌کند، اما امکان رمزگشایی این کارت‌ها وجود دارد. به عبارت دیگر، مسئله ای که این سیستم ها با آن مواجه اند، مساله امنیت سیستم است و لذا این سیستم‌ها چندان قابل‌اطمینان

نیستند. راهکار دیگر، به‌کارگیری هویت اشخاص است. بر اساس این روش، ویژگی‌های بدن اشخاص در بازشناسی آنان به کار می‌رود که به این ویژگی‌ها، ویژگی‌های بیومتری[1] گفته می شود.
در توضیح عبارت بیومتری به این نکته می‌توان اشاره کرد که افراد برای شناسایی یکدیگر، از مجموعه‌ای از ویژگی‌های منحصر به فرد استفاده می‌کنند که این ویژگی‌ها از شخصی به شخص دیگر متفاوت است. از آن جمله می‌توان به شکل صورت، گفتار، طرز راه رفتن و ... اشاره کرد.
یک سیستم بیومتری اساساً یک سیستم تشخیص الگو است، که شخص را بر اساس بردار ویژگی-های فیزیولوژیک یا رفتاری، بازشناسی می‌کند. بردارهای ویژگی پس از استخراج معمولاً در پایگاه داده ذخیره می‌گردد. معمولاً سیستم‌های بیومتری که بر اساس ویژگی‌هایی فیزیولوژیک عمل می‌کنند، دارای ضریب اطمینان بالایی هستند. سیستم‌های بیومتری می‌توانند به دو گونه عمل کنند: شناسایی و تأیید. شناسایی یعنی مقایسه اطلاعات کسب شده با تمام کاربران و تأیید یعنی مقایسه اطلاعات با کاربر مورد نظر.
چهره نقشی اساسی در شناسایی افراد و نمایش احساسات آن‌ها درسطح جامعه دارد. توانایی انسان در تشخیص چهره‌ها قابل توجه است؛ ما می‌توانیم هزاران چهره به یاد سپرده شده در طول عمرمان را تشخیص دهیم و در یک نگاه چهره‌های آشنا را حتی پس از گذشت سال‌ها شناسایی کنیم. این مهارت در مقابل تغییرات شرایط دیداری، مانند حالت چهره، سن و همچنین تغییراتی در عینک، ریش یا مدل موها همچنان پابرجا می‌ماند.
اگر چه درست است که انسان‌ها در تشخیص چهره توانا هستند، اما نحوه رمزگذاری و رمزگردانی چهره‌ها در مغز انسان کاملاً آشکار نیست، تشخیص چهره انسان برای بیش از بیست سال مورد مطالعه قرار گرفته است. توسعه یک مدل محاسباتی برای تشخیص چهره بسیار دشوار است و دلیل آن، پیچیدگی چهره ها و ساختار چند بعدی بینایی است. بنابراین تشخیص چهره یک فعالیت سطح بالا در مبحث بینایی ماشین است و می‌تواند بسیاری از تکنیک‌های پایه اولیه را در این زمینه دربرگیرد.
در سال‌های اخیر شناسایی چهره در عرصه تحقیقات بیومتریک، شناسایی الگو و بینایی ماشین مورد توجه بسیاری از محققان قرار گرفته است [۱، ۲]. همچنین روش‌های شناسایی چهره در برخی امور تجاری و امنیتی نیز کاربرد دارد. این کاربردها شامل کنترل امنیتی افراد[2] (مثلاً برای کنترل گذرنامه)، کنترل دسترسی[3] ، شناسایی[4] افراد مجرم می‌شود. به دلیل اهمیت خاص مباحث امنیتی، انتظار می‌رود سامانه‌های پردازشی تشخیص چهره بدون خطا عمل کنند، اما هیچ یک از سامانه‌هایی که تا کنون ارائه شده‌اند، بهره‌وری ۱۰۰ درصد نداشته‌اند. بنابراین همیشه باید عامل انسانی در طول فرآیند پردازش این نوع سامانه‌ها دخیل باشد. چندین روش برای تشخیص رایانه‌ای چهره وجود دارد. روش صورت مشخصه با استفاده از روش‌های آماری، اجزاء اصلی مجموعه تصاویر

[1] Bio-metric
[2] Automated crowd surveillance
[3] Access Control
[4] Identification

چهره‌های داده شده را استخراج می‌کند. از آنجا که شناسایی با کمک تصاویر چهره کمتر نیازمند دخالت انسان ها می باشد، مورد توجه شرکت‌های امنیتی قرار گرفته است.
تشخیص چهره یک عمل تشخیص الگو است، که به طور خاص بر روی چهره‌ها انجام می‌شود. این عمل عبارت است از مقایسه چهره‌های ذخیره شده افراد شناخته شده با چهره جدید و پس از آن، دسته‌بندی چهره‌ها به دو گروه شناخته شده و ناشناس. مدل‌های محاسباتی تشخیص چهره بایستی پاسخگوی چندین مسئله‌ی دشوار باشند. این دشواری ازآنجا ناشی می شود که چهره‌ها باید به گونه‌ای ارائه شوند، که اطلاعات موجود در چهره را برای تشخیص یک چهره‌ی خاص از دیگر چهره-ها به بهترین نحو به کاربرند. در این مورد، یکسانی مؤلفه های موجود در چهره‌ها (چشمان، بینی و دهان) باعث دشواری می‌شود.
در سال ۱۹۹۳ Chow and Li [۳] و در سال ۱۹۹۴ Yang and Huang [۴]، در تحقیق خود روش«تطبیق الگو»[1] را که متداول‌ترین روش در مباحث مربوط به تشخیص چهره است، به کار گرفتند. در این روش کانتور یا منحنی چهره به شش قسمت تقسیم می شود:

۱. با استفاده از سه تای آن‌ها (دو چشم و دهان) ویژگی های اصلی چهره به دست می‌آید.

۲. با استفاده از گونه‌ها و چانه کانتور چهره استخراج می شود. اما در صورت کمبود نور، سایه و چرخش صورت این روش قادر به تشخیص چهره نیست.

Sobottka و همکارانش[۵] Tang و همکارانش [۶] نشان دادند که شکل کلی صورت و تمام سر بسیار شبیه به بیضی می‌باشد، ولی با این روش نیز نمی‌توان چهره را به‌طور کامل شناسایی کرد. آن‌ها با انجام آزمایش‌های گسترده نشان دادند که سیستم جدید در هنگام چرخیدن تصاویر با یک زمینه ساده صرف نظر از تغییرات در اندازه سر، قادر به تشخیص چهره است.
در سال ۲۰۰۷ Liu و Bhuiyan و همکاران [۷]، تشخیص چهره را با استفاده از خصوصیات فیلتر گابور از منظر کامپیوتر، پردازش تصویر و تشخیص الگو انجام دادند. انگیزه اصلی جهت استفاده از فیلترهای گابور، ارتباط زیستی‌ای است که خصوصیات عصبی میدان پذیرنده در قشر اصلی بینایی پستانداران جهت‌دار است و دارای مشخصات فرکانسی-مکانی می‌باشد. فیلترهای گابور ویژگی‌های نمایان بصری مانند نقطه تمرکز فاصله‌ای، انتخاب جهت و خصوصیات فرکانسی-مکانی را به‌کارمی-گیرند. در فصل سوم روش فیلتر گابور را به تفصیل توضیح داده خواهد شد.

۱-۳- اهداف شناسایی چهره

به طور کلی شناسایی چهره به سه منظور انجام می‌گیرد:
الف) تصدیق چهره یا احراز هویت[2]
ب)شناسایی چهره

[1] Template matching
[2] Face Verification or Authentication

ج)فهرست بررسی[1]

۱-۳-۱- تصدیق هویت

تصدیق هویت یک شناسایی یک به یک است، به این معنی که تصویر شخص مورد نظر، با تصویر شخصی که هویت آن ادعا شده، مقایسه می‌شود. این سیستم‌ها در محل‌هایی کاربرد دارد، که دسترسی به آن‌ها فقط برای افراد خاصی مجاز می‌باشد و باید از ورود افرادی غیر از افراد مجاز جلوگیری شود. برای بررسی میزان دقت سیستم‌ها، میزان تأیید صحیح[2] بر حسب تأیید اشتباه[3] محاسبه شده و منحنی آن رسم می‌گردد. یک سیستم کارآمد باید بتواند با انتخاب یک حد آستانه مناسب بین این دو مقدار، کارایی را به میزان بهینه‌ای برساند. در صورتی که میزان شباهت تصویر ورودی با تصویر موجود در این سیستم‌ها از حد معینی کمتر باشد، سیستم فرد مورد نظر را رد می‌کند. حالت ایده‌آل برای این سیستم‌ها زمانی است که کلیه افراد مجاز تأیید و کلیه افراد غیر مجاز رد شوند. در صورتی که شخص مجاز، رد شده[4] و یا شخص غیرمجاز، تأیید شود[5] سیستم دچار خطا شده‌است. شکل (۱-۱) سوال مطرح در این روش را به تصویر کشیده است.

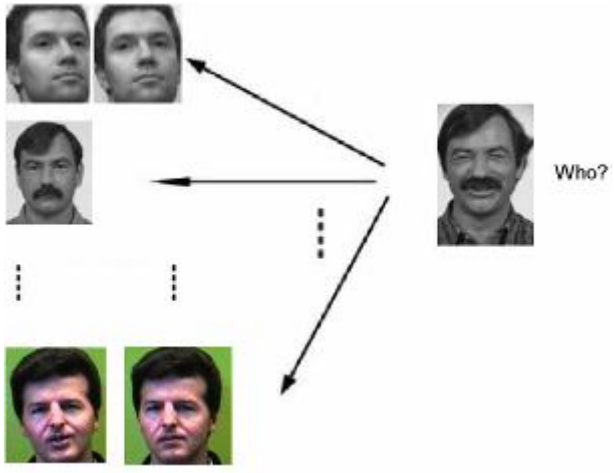
شکل ۱-۱- اصلی ترین سوال مطرح در تصدیق هویت در شناسایی چهره[۱].

۱-۳-۲- شناسایی هویت

شناسایی هویت یک روش تطبیقی یک به چند است که در آن یک تصویر ورودی با تمامی تصاویر موجود مقایسه می‌شود و شبیه ترین تصویر به عنوان تصویر شناسایی شده انتخاب می‌شود. برای این کار ابتدا یک تصویر از شخص مورد نظر گرفته می‌شود و ویژگی های آن با ویژگی های داده‌های موجود مقایسه می‌شود، تصاویر به ترتیب بیشترین شباهت مرتب می‌شوند و شبیه ترین تصویر به عنوان شخص شناسایی شده در نظر گرفته می‌شود. مثالی از کاربرد این سیستم در شکل (۱-۲) آمده است.

---

[1] Watch List
[2] Verification Rate
[3] False Acceptance
[4] False rejection
[5] False acceptance



شکل ۱-۲- شناسایی هویت در شناسایی چهره[۱].

۱-۳-۳- فهرست بررسی

در این حالت یک سری تصاویر از افرادی موجود است که به دنبال آن‌ها می‌گردیم، بنابراین تصویری که برای شناسایی به سیستم داده می‌شود ممکن است که در داده‌ها موجود باشد و ممکن است تصویری از او در لیست نباشد. برای این کار سیستم شباهت بین تصویر ورودی و تصاویر موجود را بررسی می‌کند و بر اساس شباهت به ترتیب از بیشترین شباهت تا کمترین شباهت مرتب می‌کند. در صورتی که شباهت از یک حد آستانه بیشتر باشد، سیستم حضور شخص را تایید میکند. در اینجا دو پارامتر تعریف می‌شود.

۱- درصد تعداد دفعاتی است که شخص شناسایی شده در فهرست وجود دارد و سیستم آن را اعلام می‌کند، که به آن نرخ آشکارسازی و شناسایی[۱] می‌گویند.

۲- تعداد دفعاتی است که با وجود اعلام سیستم، تصویر تشخیص داده شده در لیست وجود ندارد، که به آن نرخ آلارم اشتباه[۲] گفته می شود.

۱-۴- رویکرد این پایان نامه

در فصل دوم روش‌های مختلف تشخیص هویت مورد بررسی قرار می‌گیرد و مزایا و معایب هر روش مطرح می‌شود. سپس در فصل سوم مقدمات لازم برای پیاده سازی یک سیستم تشخیص هویت را که توان شناسایی چهره با وجود چرخش سر در تصویر را داراست معرفی می‌کنیم. سپس در فصل چهارم نتایج شبیه سازی را بررسی کرده و در نهایت در فصل پنجم پس از نتیجه گیری، پیشنهاداتی را برای ادامه کار مطرح می‌نمائیم. این پیشنهادات به این علت مطرح شدند که روش-

[1] Detection And Identification Rate
[2] False Alarm rate

های قبلی قادر به تشخیص چرخش در تصویر نبودند. در ضمن با بهبود الگوریتم شناسایی هویت، دقت شناسایی افزایش یافته است.

فصل ۲– روش‌های تشخیص هویت مبتنی بر تشخیص چهره

۲–۱– مقدمه

ویژگی‌های فردی را می توان به دو دسته ویژگی‌های زیستی مثل اثر انگشت، عنبیه، چهره و ویژگی‌های رفتاری مثل دست خط، صدا و نحوه راه رفتن تقسیم کرد. هر کدام از این ویژگی‌ها قدرت تفکیک‌پذیری متفاوتی را در شناسایی هویت از خود نشان داده‌اند که این تفکیک‌پذیری علاوه بر وابستگی به نوع آن به عوامل دیگری چون الگوریتم، منبع اطلاعات، کیفیت اطلاعات منبع بستگی دارد. با توجه به نحوه جمع‌آوری اطلاعات پایه، ویژگی‌های سیستمی در کاربردهای متفاوت، می توان انتخاب نوع ویژگی مورد استفاده را نیز متاثر از کاربرد دانست. بنابراین در مورد هیچ ویژگی نمی توان ادعا نمود که جوابی کاملا قابل قبول، هم از حیث نتیجه و هم از حیث کاربرد داشته باشد.

چهره انسان راحت‌ترین و در دسترس‌ترین ویژگی انسان برای تمایز انسان‌ها از یکدیگر است. توانایی شناسایی افراد، یک خصوصیت ذاتی است که از هزاران سال پیش در بشر هوشمند به وجود آمده است. امروزه که کامپیوترهای هوشمند پا به عرصه جهان گذاشته‌اند، سعی می‌شود تا این توانایی نیز در آن‌ها ایجاد شود که با مکانیزه کردن شناسایی افراد از طریق چهره بتوان از مزایا و کاربردهای آن بهره برد.

در هر سیستمی شناسایی که بر مبنای اطلاعات بیومتریک انسان کار می کند، لازم است سه گام زیر طی شوند:

۱- دریافت اطلاعات بیومتریک که این درگاه باید منطبق بر نوع ویژگی مورد نیاز باشد که به این دیتا، امضاء زیست سنج[1] اطلاق می شود.

۲- پیش پردازش اطلاعات شامل استخراج ویژگی، تبدیل داده ورودی به فرم قراردادی سیستم که به دیتا خروجی این گام امضا به هنجار شده[2] گفته می شود.

۳- ارسال اطلاعات به هسته بازشناسی برای مقایسه با اطلاعات منبع.

---

[1] Biometric Signature
[2] Normalized Signature

روش‌های شناسایی چهره از دو جهت قابل بررسی هستند. ۱) نوع اطلاعات مورد استفاده، ۲) روش مورد استفاده برای شناسایی چهره. از جهت نوع اطلاعات، روش‌های شناسایی چهره به سه دسته‌ی شناسایی با کمک ۱)تصاویر دو بعدی، ۲)تصاویر سه بعدی و ۳)ترکیبی از تصاویر دوبعدی و سه بعدی تقسیم بندی می‌شوند[۸]. تصاویر دو بعدی چهره‌ی انسان نسبت به تغییرات زاویه‌ی چهره[۱]، زاویه‌ی نور تابشی، حالات چهره[۲]، موهای صورت، پوشش برخی قسمتهای صورت و سن دارای تغییر اطلاعات درونی است. تصاویر سه بعدی چهره نسبت به تغییرات شدت روشنایی و زاویه مقاوم هستند ولی حالت چهره و موهای صورت باعث تغییرات زیادی در این نوع تصاویر می‌شوند و کار شناسایی را با مشکل مواجه می‌کنند.

از جمله مشخصاتی که برای سیستم شناسایی مورد نظر در نظر گرفته می شود، به حداکثر سرعت عملکرد، ابعاد پایگاه داده، نوع و فرمت اطلاعات ورودی می توان اشاره کرد. بر اساس همین ویژگی-ها الگوریتم‌های بازشناسی مورد دسته بندی قرار می گیرند. دسته بندی تاریخی هم می تواند روند رشد چنین سیستم هایی را نمایش دهد.

در هر سیستم تشخیص چهره لازم است دو گام طی شوند: اول، تشخیص چهره و استخراج ویژگی از چهره و تبدیل ویژگی‌های استخراج شده به فرمت قراردادی و دوم، تطبیق الگوی چهره‌ها. الگوریتم هایی که هر دو گام را انجام می دهند را الگوریتم‌های خودکار[۳] والگوریتم‌هایی که فقط گام دوم را انجام می دهند نیمه خودکار[۴] می نامند.

۲-۲- مروری بر روش‌های تشخیص چهره

در ابتدا لازم به ذکر است که اکثر سیستم های تشخیص چهره مدل دید از روبرو[۵] را پذیرفته‌اند بنابراین می توان انتظار داشت که اکثر توانایی و ضعف‌های این روش‌ها مشابه باشد. این روش‌ها که در خانواده دید از روبر قرار می گیرند، بر پایه مقادیر ویژه چهره[۶] بنا شده‌اند که در این میان به روش های گوناگونی مثل شبکه عصبی[۷]، مدل مخفی مارکوف[۸] و ... می توان اشاره کرد.

مقادیر ویژه به طور اساسی با مفاهیمی چون بردار ویژه[۹]، تصاویر ویژه[۱۰]، مولفه های اصلی[۱۱] و بسط کوهن- لاو[۱۲] مرتبط است. در [۹] و [۱۰] از روش مولفه های اصلی تصویر چهره استفاده شده است.

---

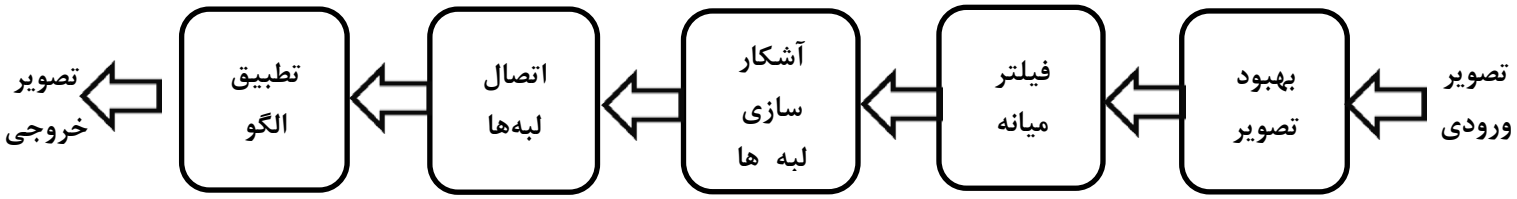
[1] Pose
[2] Facial Expression
[3] Automatic
[4] Partially automatic
[5] Frontal view
[6] Eigenfaces
[7] Neural networks
[8] Hidden markov model
[9] Eigenvector
[10] Eigenpicure
[11] Principal component
[12] Karhunen-Loeve expansion

Majumdar و همکارانش [۱۱] به استفاده موثر از مقادیر ویژه در سیستم‌هایی اشاره کرده که تنها یک نمونه از هر کلاس برای آموزش وجود دارد و عنوان شده که مقادیر ویژه چهره نسبت به سایر روش ها عملکرد بهتری دارد. Yan Yanjung و همکارانش [۱۲] به استخراج مقادیر ویژه با استفاده از روش فیشر[1] برای چهره پرداخته‌اند.

۲-۲-۱- تشخیص چهره بر اساس اطلاعات هندسی شکل

چهره نقشی اساسی را در شناسایی افراد و نمایش احساسات آن‌ها در بر دارد. توانایی انسان در تشخیص چهره‌ها قابل توجه است. انسان قادر است هزاران چهره ای را که در طول عمرش با آنها برخورد کرده است را تشخیص دهد و در یک نگاه چهره‌های آشنا را حتی پس از سالها جدایی شناسایی کند. این مهارت نسبت به تغییرات شرایط دیداری مانند حالت چهره، سن و همچنین تغییراتی در عینک، ریش یا سبک مدل موها پایدار می‌باشد.

این ایده در سال ۲۰۰۰ توسط Wang-Jianguo و همکارانش [۱۳] مطرح شد. بلوک دیاگرام این روش در شکل (۲-۱) نشان داده شده است[۱۳].



شکل ۲-۱-بلوک دیاگرام روش تشخیص چهره بر اساس اطلاعات شکل[۱۳].

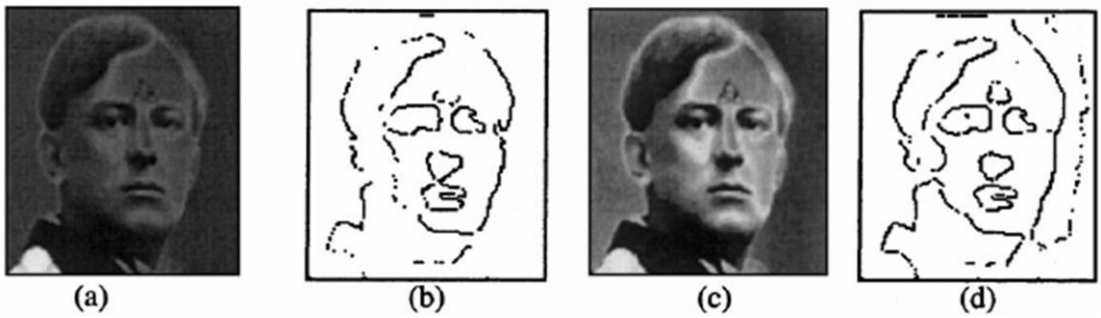
مراحل کار به شرح زیر تقسیم بندی می گردد:

الف: تهیه تصویر ورودی

ب- بهبود تصویر

ممکن است تصاویر ورودی به علت محدودیت شرایط نوری دارای کنتراست ضعیفی باشند. در این سیستم آن‌ها با استفاده از متعادل سازی هیستوگرام تصویر را بهبود دادند. تاثیرات متعادل سازی هیستوگرام در شکل (۲-۲) نشان داده شده است.

[1] Fisher-face Method



شکل ۲-۲- اثر متعادل سازی هیستوگرام بر لبه یابی تصاویر: (a) تصویراصلی دارای تمایز ضعیف، (b) لبه‌های تصویر اصلی، (c) تصویر خروجی متعادلسازی شده (d) لبه‌های تصویر خروجی[۱۳].

ج- فیلتر کردن تصویر با استفاده از فیلتر میانه

معمولا نویزها فرکانس بالا دارند. برای حذف نویز در صورت استفاده از فیلتر پایین گذر بعضی از اطلاعات مفید تصویر مانند لبه‌ها از بین می‌رود. به همین دلیل از فیلتر میانه برای این منظور استفاده گشته تا اطلاعات مفید موجود در تصویر از بین نرود. شکل (۲-۳) تاثیرات استفاده از فیلتر میان گذر را نشان می‌دهد.

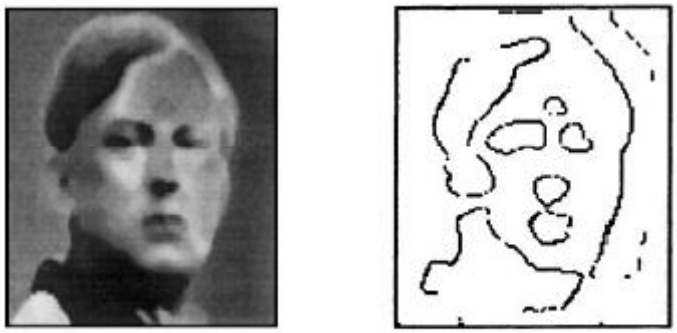
د- آشکار سازی لبه‌ها

در گزارش مذکور با استفاده از آشکار ساز Zero – crossing روی DOE[1] که در سال ۱۹۹۸ توسط MA and Zhang ارائه شد، لبه‌های تصویر را بدست آوردند . DOE یا تفاضل دو تابع نمایی توسط رابطه (۲-۱) تعریف می شود.

$$\boldsymbol{DOE = K_e\left(e^{-\frac{|x|}{t1}} - e^{-\frac{|x|}{t2}}\right)} \qquad (۱-۲)$$

که در آن t_1= 1.5 و t_2=5 در نظر گرفته شده است[۱۴].

[1] Difference of Exponential



شکل ۲-۳- تاثیرات فیلتر میان‌گذر که (a) تصویر خروجی (تصویر C-۲-۲)بعد از فیلتر کردن تصویر با فیلتر میان گذر، (b) لبه‌ها تصویر (a.)[۱۳].

ه- اتصال لبه‌ها

در سال ۱۹۹۶ ke و همکارانش [۱۵]، با معرفی تابع انرژی توسط رابطه ۲-۲ و مینمم کردن آن خطوط لبه‌ها را بدست آوردند.

$$H = 2h_0 + \frac{1}{2}\int k_s(\nabla l_s)^2 ds + \frac{1}{2}\int b_s(\nabla^2 l_s)^2 ds \qquad (۲\text{-}۲)$$

که در آن $\boldsymbol{\nabla^2 l_s} = (\frac{\partial^2 x}{\partial^2 s}, \frac{\partial^2 y}{\partial^2 s})$ ، $\boldsymbol{\nabla l_s} = \left(\frac{\partial x}{\partial s}, \frac{\partial y}{\partial s}\right)$، h_0 ثابت انرژی و K_s و b_s ثابت الاستیک[1] هستند.

شکل ۲-۴- اتصال لبه‌ها بطور بیوسته که (a) تصویر یک چهره طبیعی، (b) تصویر باینری بعد از اعمال اتصال لبه‌ها، (c) نشان دهنده همه نقاط لبه‌ها می باشند[۱۳].

[1] elastic