مجله رویکردهای نوین در تحقیقات علوم پایه، فنی و مهندسی
سال دوم، شماره ۵، تابستان ۱۳۹۸
ISSN: ۲٦٤٥-٥٤٣٩
www.jonarbset.ir

کشف تقلب در اثر انگشت با استفاده از روش های ترکیبی داده کاوی

منصوره سادات موسوی[۱] ، حسین جعفر کریمی[۲]

[۱] کارشناس ارشد مهندسی کامپیوتر-نرم افزار دانشگاه آزاد اسلامی واحد علوم تحقیقات تهران(دماوند)
[۲] استادیار دانشگاه آزاد اسلامی واحد دماوند

چکیده

اثر انگشت انسان دارای قابلیت های فراوانی است و استفاده از آن در سیستم های بیومتریک روز به روز گسترده تر می شود چرا که نمونه برداری از آن راحت و دسترسی به آن سریع می باشد. همچنین احتمال دستکاری شدن و صدمه دیدن نمونه های آن بسیار کم است. در این تحقیق، به ارائه روشی مبتنی بر تکنیک های داده کاوی پرداخته شده است و هدف از آن تشخیص اثر انگشت تقلبی از اثر انگشت زنده در سیستم های احراز هویت با دقت بالا می باشد. علاوه بر تشخیص تقلب به بررسی نوع مواد تقلبی که در ساخت اثر انگشت از آن استفاده شده است، پرداخته شد. تا بر اساس نوع مواد، ارزیابی های لازم صورت گیرد و به کشف دانش در خصوص حساسیت حس گر ها نسبت به نوع مواد تقلب رسید. مواد استفاده شده در این پژوهش شامل ژلاتین، اکو فلکس، چسب چوب و لاتکس میباشد. مراحل مورد بررسی در این تحقیق به شرح ذیل است: در مرحله استخراج ویژگی از روشهای آماری مرتبه اول بر روی هیستوگرام تصویر استفاده شد. سپس برای طبقه بندی از الگو ریتم ترکیبی ماشین بردار پشتیبان و درخت تصمیم بهره گرفته شد. در مرحله آخر ، با استفاده از نرم افزار Rapid Miner و پایگاه داده Livdet۲۰۱۵، داده کاوی بر روی اثر انگشتها صورت پذیرفت .با توجه به نتایج حاصل از این تحقیق اثر انگشت های تقلبی که با ژلاتین ساخته شده بود ، دارای کمترین میزان خطا و چسب چوب دارای بیشترین خطا، در طبقه بندی عنوان شد.

واژه‌های کلیدی: درخت تصمیم، بیومتریک، اثر انگشت، ماشین بردار پشتیبان.

۱. مقدمه

شاید اولین گام در پیدایش سیستم های بیومتریک را انسانهای نخستین برداشته اند. آنها صرفا از طریق حس بینایی یکدیگر را شناسایی می کردند. بدیهی است با گذشت زمان و پیشرفت بشر، نیاز به شاخصه های دقیق تری برای شناسایی انسانها احساس می شد. ازین جهت، نام و نام خانوادگی، نام پدر و دیگر شاخصه ها بوجود آمد.

هنگامیکه کامپیوتر در زندگی انسانها شروع به نقش آفرینی کرد همین داده های سنتی به صورت طبقه بندی شده وارد دنیای دیجیتال گردید. با پیشرفت رایانه و همچنین نیاز به اتوماسیون، ضرورت پرداختن به سیستم های بیومتریک برای پیشگامان این تکنولوژی احساس شد. برخی از روش های بیومتریک، سوابقی بسیار کهن تر از تاریخچه ایجاد رایانه دارند. مانند شناسایی چهره که احتمالا به پیدایش انسان بر می گردد و یا شناسایی اثر انگشت که در قرن ۱۸ میلادی بوجود آمد.

امروزه سیستم های بیومتریک کاربردهای بسیار گسترده ای دارند به طوریکه بسیاری از مهمترین امور جوامع بر این اساس پایه گذاری شده اند. بطور مثال در برخی از کشورها، سیستمهای کنترل تردد از طریق اسکن عنبیه چشم انسان عمل می کنند و در بعضی جاهای دیگر ، امور بانکی از طریق شناسایی صدای افراد انجام می شود. همچنین در برخی کشورها ، شناسایی از طریق ورید صورت می گیرد. موارد استفاده در سیستم های بیومتریک عبارت اند از: - شناسایی اثر انگشت - شناسایی اجزای چهره شامل: چشم، گوش و بینی - شناسایی اسکلت بدن - شناسایی بوی بدن و بسیاری موارد دیگر .

همانطور که می دانیم "امنیت" یکی از مهمترین فاکتورهایی است که همواره در دنیای فناوری اطلاعات مطرح بوده و همچنین از عمده ترین مشکلاتی است که همیشه در سیستم های بیومتریک اثر انگشت مطرح می شود. در مورد این سیستم ها، مقصود از امنیت، تشخیص درست اثر انگشت زنده است. مشکل دیگری که دراینجا مطرح می شود مساله سرعت تشخیص اثر انگشت و به عبارت کلی تر، کارایی سیستم تشخیص اثر انگشت می باشد. برای برآوردن این مهم، باید از الگوریتم ها و تکنیکهایی استفاده شود که امنیت سیستم را از نظر "بالا بردن درصد تشخیص درست" و "پایین آوردن درصد تشخیص غلط" بهبود بخشد اما در عین حال از کارایی سیستم نکاهد. این مساله نیاز ضروری دنیای بیومتریک می باشد و ما هنوز در ابتدای راه هستیم. حتی در دقیق ترین سیستم بیومتریک یعنی "سیستم کنترل دی ان ای" ممکن است احتمال خطا از ۱ به ۱۰۰۰۰ برسد! البته این خطاها بطور کلی در ماهیت هر تبدیل آنالوگ به دیجیتالی نهفته است اما با توجه به افزایش سرعت پردازش ها و حافظه ها و کارایی الگوریتم ها و همچنین با اتکا به تجربیات مفید درباره سیستم های موجود و دانستن نواقص آنها ، لازم است به طور مستمر در بهبود روش ها و نیز نوآوری در این زمینه تلاش شود. یکی از معضلات بزرگی که در سیستم های بیومتریک اثر انگشت وجود دارد، بحث تقلب در این سیستم هاست. هدف از این پژوهش، طبقه بندی اثر انگشتهای زنده از اثر انگشت هایی است که به صورت تقلبی ساخته شده و به سیستم معرفی شده اند. جهت شناسایی این اثر انگشت ها از تکنیک های داده کاوی استفاده شده است. از آنجاییی که کلاس های مورد نظر مشخص میباشد از تکنیک طبقه بندی در این پژوهش بهره برده شده است. در بخش اول به پیشینه پژوهش پرداخته شد.درگام دوم، به استخراج ویژگی های اثر انگشت پرداخته شد. پس از استخراج و بررسی اثر انگشت های زنده و تقلبی، بارز ترین ویژگی ها که اثر انگشت زنده را از تقلبی متمایز میکرد، انتخاب گردید. سپس جهت طبقه بندی، از ماشین بردار پشتیبان و درخت تصمیم استفاده شد. از آنجایی که اثر انگشتهای تقلبی با مواد مختلف ساخته میشود جهت بررسی این مواد و همچنین کارایی سیستم در مواجهه با این مواد به داده کاوی پرداخته شد و نتایج قابل توجهی در ارزیابی ها کشف گردیدکه در فصل انتهایی نتایج ارزیابی نمایش داده شده است.

۲. پیشینه پژوهش

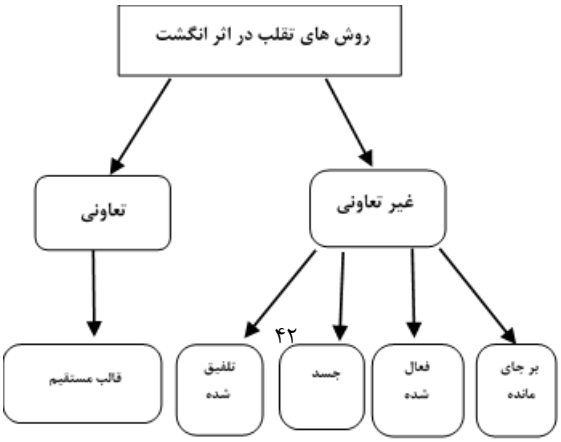
در این فصل به بررسی پژوهش هایی که تا کنون بر روی "سیستم های تشخیص تقلب" صورت گرفته است، می پردازیم. ابتدا مروری بر تاریخچه شناخت اثر انگشت خواهیم داشت و سپس انواع روش های تقلب در آن را معرفی خواهیم کرد. سپس به شناخت ویژگیهای اثر انگشت پرداخته و بعد، کلاسهای یک اثر انگشت را مرور می

کنیم. در ادامه به بررسی معماری"سیستم تشخیص تقلب اثر انگشت" و روش های شناسایی اثر انگشت می پردازیم و دو روش "سخت افزاری" و "نرم افزاری" را مورد بحث قرار می دهیم. در نهایت، پژوهش هایی را که تا کنون در زمینه شناسایی تقلب به روش نرم افزاری انجام شده، ارائه خواهیم داد.

"اثر انگشت" یک مشخصه فیزیولوژیکی بیومتریک برای شناسایی یک فرد است. همان طور که از نامش پیداست، به "چاپ" یا تصویر ساخته شده توسط انگشت فرد، اثر انگشت می گویند که از بدو تولد بر روی کف دست و انگشتان وجود دارد و با افزایش سن، واضح و برجسته تر می شود اما از نظر الگو و ساختار تفاوتی نمی کند و در طول زمان تغییر نمی یابد. این اثر درواقع بر روی لبه های برجسته پوست وسطوح بی موی دست و پا وجود دارد. اثر انگشت و الگوهای اثر دست برای هزاران سال به عنوان وسیله ای جهت شناسایی شخصی استفاده می شده و با توجه به پیشرفت چشمگیر سالهای اخیر در قابلیت های محاسباتی، امروزه این شناسایی به صورت خودکار انجام می گیرد. در سال ۱۶۸۴، دکتر نحیمیا گرو به توصیف برآمدگی ها و خلل و فرج انگشتان دست و پا پرداخت[۱]. پس از چندین سال، پروفسور ژوهانش به ایجاد یک سیستم طبقه بندی از اثر انگشت پرداخت[۲].

او، نه الگو را برای طبقه بندی اثر انگشت پیاده سازی نمود و هر کدام را با جزئیات مربوطه نام گذاری کرد و با این طبقه بندی ثابت کرد که اثر انگشت هر فرد منحصر به فرد می باشد. در سال ۱۸۹۲، یک انسان شناس معروف به نام سر گالتون ، نتایج قطعی فعالیت های خود را منتشر کرد و اثر انگشت را با هدف استفاده در شناسایی هویت معرفی نمود[۳]. به طور کلی سه اصل اساسی در ارتباط با اثر انگشت وجود دارد. نخست آنکه اثر انگشت یک مشخصه منحصر به فرد می باشد. دوم، اثر انگشت با طول عمر تغییر نخواهد کرد و سوم اینکه اثر انگشت ها دارای الگوهای رایج عمومی می باشند که بر این اساس می توانند در گروههایی خاص طبقه بندی شوند .

با ظهور اثر انگشت تقلبی، تهدید بزرگی در سیستمهای "تشخیص خودکار احراز هویت" به وجود آمد. به طور کلی روش های تقلب روی اثر انگشت را میتوان به دو دسته "تعاونی" و"غیر تعاونی" تقسیم نمود[۴] .در روش تعاونی، انگشت فرد به طور مستقیم تاثیر گذار می باشد به این معنی که می توان از اثر انگشت، جهت نمونه برداری قالب و به منظور ساخت اثر انگشت تقلبی استفاده کرد. در روش غیر تعاونی، از انگشت فرد مورد نظر به طور مستقیم استفاده نمی شود بلکه از اثرانگشت های به جا مانده بر روی سطوح (جهت ساخت قالب اثر انگشت تقلبی) استفاده می گردد . نمودار ۱ این طبقه بندی را نمایش می دهد.



نمودار ۱. طبقه بندی روش های تقلب در اثر انگشت

همانطور که در نمودار ۱ قابل مشاهده است، در روش تقلب به صورت تعاونی، از اثرانگشت فرد به طور مستقیم و بر روی خمیر، قالبی تهیه کرده و سپس با ریختن موادی مایع مانند ژلاتین ، لاتکس و چسب مایع ، تصویر اثر انگشت را ایجاد نموده و از آن استفاده می کنند. از جمله ی بهترین موادی که در ساخت قالب از آن استفاده می شود میتوان به خمیرهای دندانپزشکی ، خاک رس و خشت وبلوتک اشاره کرد[۵, ۶]. شکل ۱ مراحل قالب گیری و ساخت یک اثر انگشت تقلبی به روش تعاونی (با استفاده از قالب پلاستیک و مایع ژلاتین) را نشان می دهد.

		
۱.قرار دادن پلاستیک در آب گرم	۲.قراردادن انگشت روی قالب	۳.قالب آماده شده
		
۴..قرار دادن ژلاتین در آب	۵.جوشاندن ژلاتین در آب	۶.مخلوط کردن آب با ژلاتین
		
۷.ریختن مایع درقالب	۸. قرار دادن در محل خنک	۹.اثرانگشت ژلاتینی

شکل ۱- نمونه ای از قالب گیری جهت تقلب اثر انگشت به روش تعاونی [۷]

بر اساس تحقیقات پیترز[۸]، در روش غیر تعاونی حالتهای مختلفی برای انجام تقلب وجود دارد که ازآن جمله می توان به روش اثر انگشت بر جای مانده روی سطوح اشاره کرد . این روش نیز به طرق مختلف قابل انجام است که در این تحقیق به سه مورد از آنها اشاره میکنیم. در روش اول با استفاده از ریختن نوعی پودر مخصوص نمونه برداری بر روی آثارباقی مانده روی سطوح، اثر انگشت را یافته وسپس پودر را با قلمو پاک می کنند. آثاری که باقی می ماند اثر انگشت مورد نظر است که بوسیله ی یک چسب نواری میتوان آنرا بر داشت و بر روی سنسور، استفاده نمود. در روش دوم که بر اساس لیتوگرافی انجام می شود از "بردهای مدار چاپی" استفاده میکنند. در این روش، اثر انگشت موجود روی سطح شفاف را توسط پودری سیاه و با استفاده از یک قلمو برس میزنند و پس از آشکار شدن، بوسیله ی یک دوربین دیجیتالی از آن عکس گرفته و بر روی سطحی شفاف، چاپ می کنند(به منظور درست کردن ماسک). سپس ماسک ایجاد شده روی مدار قرارگرفته و در معرض نور ماورا بنفش قرار می گیرد و بعد با سیلیکون مایع پر می شود. پس از آماده شدن، آنرا بر روی اثر انگشت یک فرد زنده قرار می دهند و از آن جهت تقلب استفاده میکنند. در روش سوم که روش جدید و پیشرفته ای می باشد، اثر انگشت بر جای مانده روی سطوح مختلف را با استفاده از تکنولوژی "الکتروریسی نانو" و در کمتر از ۳۰ ثانیه تصویر برداری می کنند[۹]. شکل ۲، نمونه ای از ساخت اثر انگشت تقلبی به روش غیر تعاونی را نشان می دهد.

۱ .ژلاتین مایع شده

۲. ریختن ژلاتین بر روی قالبی که از اثر انگشت بر جای مانده ایجاد شده است

۳. قراردادن آن در جای خنک و ایجاد اثر انگشت تقلبی

		
۱.ژلاتین مایع شده	۲.ریختن ژلاتین بر روی قالبی که از اثر انگشت بر جای مانده ایجاد شده است	۳.قرار دادن آن در جای خنک و ایجاد اثر انگشت تقلبی

شکل ۲- نمونه ای از قالب گیری جهت تقلب اثر انگشت به روش غیر تعاونی [۷]

سه نوع مختلف از اثر انگشت های تقلبی که می توانند سیستم "شناسایی خودکار اثر انگشت" را تهدید نمایند، عبارتند از: - تغییر اثر انگشت - اثر انگشت مصنوعی - تصویر اثر انگشت.از این بین، روش سوم، بدلیل ساده و کم هزینه بودن به طور گسترده تری مورد استفاده قرار می گیرد. در این روش از موادی مانند خمیر بازی ، لاتکس، سیلیکون ، مومداسیل و چسب چوب استفاده میکنند و تصویر واقعی اثر انگشت بسادگی روی آنها نقش می بندد[۱۰]. در این تحقیق، تمرکز ما روی این نوع تقلب در اثر انگشت می باشد.

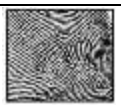
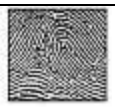
ویژگی های اثر انگشت بر اساس آنچه در FBI بیان شده است برای هر ده اثر انگشت متفاوت می باشد[۱۱]. به طور کلی، ویژگی های اثر انگشت، به دو دسته "ویژگی های محلی" و "ویژگیهای عمومی" تقسیم می شود. ویژگی های عمومی با چشم غیر مسلح نیز قابل روئیت می باشند مانند نوع خطوط، شیارها ، هسته، مناطق الگوها، دلتا، تعداد برآمدگی ها و غیره. اما ویژگی های محلی که به آن "مینوتیا" نیز گفته می شود ویژگی های منحصر به فردی هستند که از طریق شیارهای موجود در انگشت بررسی می شوند[۱۱] .

کلاسهای اثر انگشت بر اساس الگوهای بصری، به سه دسته ی منحنی ، مارپیچی و حلقوی تقسیم میشوند. بر اساس مقاله آبهیشک[۱۲]، الگوی منحنی، خود به دو دسته تقسیم می شود که شامل "منحنی با افزایش تند" و "منحنی با افزایش ملایم" است. الگوی حلقوی نیز به دو دسته تقسیم می شود: "حلقوی متمایل به سمت چپ" و "حلقوی متمایل به سمت راست" و یا به عبارتی: حلقوی متمایل به سمت انگشت شصت و حلقوی متمایل به سمت انگشت کوچک. ویژگیهای استخراج شده از تصویر برآمدگی یک اثر انگشت، به طور کلی به ۳ دسته تقسیم می شود.

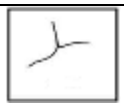
سطح اول: کمانی،حلقه، مارپیچ

سطح دوم: پایان برآمدگی ، انشعاب ، چشم ، قلاب ، خط واحد ، خط قطع بندی ،

سطح سوم: روزنه ، اشکال خط ،برآمدگیهای اولیه ، چینها ، زگیلها ، خراشها .شکل۳ نمونه ای ازسطح اول طبقه بندی اثر انگشت را نشان می دهد. شکل ۴ نمونه ای از سطح دوم طبقه بندی اثر انگشت را نشان می دهدو شکل ۵ نمونه ای از سطح سوم طبقه بندی اثر انگشت را نشان می دهد.

			
حلقوی راست	حلقوی چپ	کمانی بلند	کمانی ساده
			
مارپیچ تصادفی	مارپیچ دو حلقه ای	مارپیچ بسته شده در مرکز	مارپیچ ساده

شکل۳- سطح اول طبقه بندگی اثر انگشت[۱۲]

			
انشعاب	برآمدگی کوتاه	پایان برآمدگی	هسته
			
جزیره	چشم	قلاب	دلتا

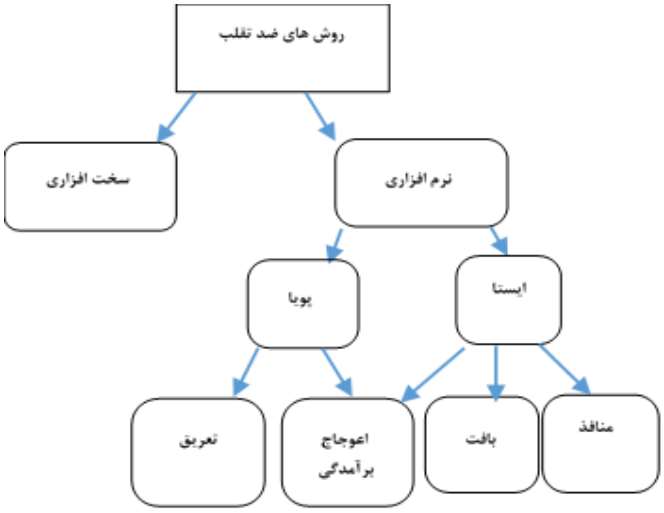
شکل۱-سطح دوم طبقه بندگی اثر انگشت [۱۳]

			
برامدگیهای اولیه	زخم	اشکال خط	روزنه

شکل۲- سطح سوم طبقه بندی اثر انگشت[۱۳]

در حقیقت، اثر انگشت، تصویری از برآمدگیهای روی سطح انگشت می باشد و منحصر به فرد بودن و عدم تغییر آن در طول زمان باعث شده که احراز هویت و شناسایی از این طریق، به عنوان یکی از مهمترین و محبوبترین

روش ها در تکنولوژی بیومتریک به حساب آید. وجود فاکتورهایی مانند متمایز بودن اثر انگشتها، استقامت، سهولت در استفاده و بالا بودن نرخ تطبیق پذیری از دلایل اصلی تسلط سیستمهای بیومتریک اثر انگشت بر بازار می باشد. به طوریکه بیش از ۵۲ درصد از سیستمهای احراز هویت در دنیا بر اساس سیستم بیومتریک اثر انگشت می باشد[۱۲]. در سالهای اخیر، روش های متعددی جهت کشف تقلب در سیستمهای احراز هویت پیشنهاد شده است که به طور کلی میتوان آنها را به دو روش سخت افزاری و نرم افزاری تقسیم بندی نمود[۱۶]. نمودار ۲ طبقه بندی روش های کشف تقلب در سیستمهای احراز هویت را نشان می دهد[۱۷].



نمودار ۱-طبقه بندی روش های کشف تقلب در سیستمهای احراز هویت بر اساس اثر انگشت

در روش های سخت افزاری از سیستمهای تعبیه شده در سنسورها استفاده میکنند که توانایی اندازه گیری فاکتورهای سرزندگی از جمله اندازه گیری تعریق، درجه حرارت، رایحه ، ضربان قلب و میزان اکسیژن خون را دارد[۱۴و۱۵]روش های سخت افزاری به دلیل در اختیار داشتن منابع زیادی از اطلاعات، دارای تضمین وقابلیت اطمینان بسیار بالایی هستند که جزو مزایای این روش می باشد. اما بدلیل هزینه بالا و انعطاف پذیری پایین از محبوبیت کمتری نسبت به روش نرم افزاری برخوردار می باشند[۱۶]. در این پژوهش، تمرکز ما بر روی روش های نرم افزاری است. همانطور که در نمودار ۲ قابل مشاهده است روش های نرم افزاری به دو دسته "پویا" و "ایستا " تقسیم میشوند. در روش های نرم افزاری، برای تشخیص اثر انگشت زنده، از تحلیل ویژگیهای ترکیبی یک اثر انگشت که به راحتی در اثر انگشت تقلبی قابل ایجاد نیست، استفاده می کنند. در برخی از این روشها از مطالعه دقیق فیزیک اثر انگشت الهام گرفته شده و در برخی از آنها از تجزیه و تحلیل آماری ایده گرفته شده است.
روش های نرم افزاری که بر اساس تکنیکهای پردازش سیگنال عمل میکنند، به دلیل هزینه پایین و انعطاف پذیری بالا، دارای جذابیت و محبوبیت بیشتری نسبت به روش سخت افزاری میباشند[۱۶]. میزان اطمینان و تضمین روش های نرم افزاری با توجه به انتخاب نوع ویژگی، نوع موادی که جهت تقلب از آن برای ساخت اثر انگشت تقلبی استفاده شده است، نوع الگوریتم طبقه بندی، نوع سنسور استفاده شده و حجم اطلاعات پایگاه داده متفاوت می باشد[۱۶]. در این پژوهش، روش استفاده شده بر اساس روش های نرم افزاری می باشد و در

ادامه پژوهش های انجام شده ارائه می گردد. جین و همکارانش در سال ۲۰۰۴، از تکنیک اندازه گیری تعریق و موجک جهت کشف اثر انگشت تقلبی استفاده کردند [۲۳]. سنسورهای مورد استفاده آنها سه نوع سنسور نوری[۱]، خازنی[۲] و الکترو نوری بودند. آنها بدون استفاده از الگوریتم یادگیری ماشین، تقلب را تشخیص دادند و نتیجه نهایی ویژگیهای ارزیابی شده را با میزان آستانه از قبل تعیین شده مقایسه کردند. میزان آستانه ای که آبهینکار در سنسور خازنی، نوری و الکترو نوری در نظر گرفته بود، به ترتیب برابر با ۴۰/۷۴، ۴۴/۵۵، ۳۱/۶۰ بوده است که با این میزان آستانه، میزان رد غلط اثر انگشت زنده و پذیرش غلط اثر انگشت زنده برابر با صفر بوده است[۲۳]. آنتونلی و همکارانش در سال ۲۰۰۶ از تکنیک اعوجاج و انتشار نور جهت کشف تقلب برروی اثر انگشت استفاده کردند. سنسور مورد استفاده آنها در ارزیابی، سنسور نوری بود. پایگاه داده مورد استفاده آنتونلی به "BSL" معروف است. آنتونلی، توالی داده های یک تصویر واقعی از اثر انگشت را با یک اثر انگشت دچار اعوجاج به منظور بررسی سطح تشابه آنها مقایسه کرد. معیار ارزیابی آنتونلی "درصد اشتباه برابر" بود که نسبت رد غلط اثر انگشت زنده به پذیرش غلط اثر انگشت زنده را در نظر گرفته بود که میزان این درصد را ۱۱/۲۴ عنوان کرده بود[۲۴, ۲۵]. جیا و همکارانش در سال ۲۰۰۷ از تکنیکهای اعوجاج، تعریق و آمارشناسی استفاده کردند. سنسور مورد استفاده آنها در ارزیابی، سنسور خازنی بود. او به بررسی خاصیت کششی پوست انسان زنده که در هنگام فشار دادن بر روی سنسور، آثار بارزی را از خود به جا میگذارد پرداخت. مشاهدات بدست آمده، تفاوت قابل توجه بین اثر انگشت زنده و تقلبی را نشان دادند. طبق تحقیقات او، فشار وارد شده از اثر انگشت زنده بر روی هر دو قسمت از ناحیه اطراف اثر انگشت، آثاری بر جای میگذارد و ضریب همبستگی در اثر انگشت زنده مقداری مثبت می باشد. معیار ارزیابی جیا ، "درصد اشتباه برابر" بود که میزان این درصد ۴/۷۸ عنوان شده است[۲۶].

ژانگ و همکارانش در سال ۲۰۰۷ از تکنیک اعوجاج، جهت کشف تقلب استفاده کردند. آنها، اعوجاج اثر انگشت زنده و تقلبی را با استفاده از تکنولوژی تی پی اس ۳(برای اندازه گیری میزان زبری از سطح بسیار نازک از یک صفحه نازک) مدلسازی کردند. سنسور مورد استفاده آنها سنسور نوری بود. با توجه به تحقیقات آنها در این زمینه، اثر انگشت زنده نسبت به اثر انگشت تقلبی میزان زبری و سختی کمتری دارد. (به دلیل خاصیت کششی پوست). علاوه بر آن، اگر فشار وارد شده روی سنسور، همجهت با اثر انگشت زنده باشد در شرایط مساوی، میزان تغییر شکلی که بر اثر فشار بر جای میماند در اثر انگشت تقلبی کمتر از اثر انگشت زنده می باشد. اعوجاج ها با تغییر شکل "مینوتیا" قابل نمایش می باشد و محاسبه پارامتهای تی پی اس، از طریق محاسبه سری جفت مینوتیاهای قرار داده شده، قبل و بعد از اعوجاج صورت می گیرد. طبقه بندی این تمایز از طریق خمیدگی بردار انرژی در تی پی اس می باشد. کارایی این روش متکی بر درصد استخراج جفت مینوتیا ها می باشد که بر اساس درصد اشتباه برابر، میزان آن ۴/۵ درصد عنوان شد که نسبت به روش جیا دارای کارایی بهتری بود[۲۷].

آبهینکار و شاکرز در سال ۲۰۰۹ پیشنهاد روش تشخیص تقلب بر اساس تغییر الگوی تعریق ایزوله شده از اثر انگشت از طریق تحلیل موجک را دادند. در این روش آنها دو تصویرگرفته شده متوالی از اثر انگشت را که توسط

---

۱. Optical. سنسورهای نوری،با اسکن اثر انگشت و تهیه عکس از روی آن، و پردازش تصویر، کار میکنند.

۲. Capacitive سنسورهای خازنی، با استفاده از پستی و بلندی اثر انگشت و تغییر ظرفیت خازنی آن، در مقابل یک آرایه خازنی از روی اثر انگشت، تصویری تهیه میکنند که با پردازش آن سیستم کار میکند.

۳. TPS

سنسور نوری با فاصله ۲ ثانیه نمونه برداری شده بود توسط فیلترینگ متعادل و نمودار هیستوگرامی برابری، تقویت کردند. سپس تحلیل موجک توسط بسته موجک با تمرکز بر روی مولفه هایی با فرکانس بالا که ازانتقال دایره ای اطراف منافذ از نقاط تاریک به سمت نقاط روشن گرفته شده بود و تحلیل تفکیک پذیری چند گانه با تمرکز بر روی اجزایی با فرکانس پایین که به صورت متناوب از مکان منافذ گرفته شده بود، انجام شد. برای هر زیر باند، تغییر ضرایب موجک، از تصویر اول به تصویر دوم در نظر گرفته شد و اندازه گیری سر زندگی، بر اساس محاسبه انرژی کل بدست آمد. ضرایبی که بیشتر از ۴۰ درصد تغییر نکرد جزو اثر انگشت زنده، در نظر گرفته نشد. میزان درصد اشتباه برابر، ۶/۷ درصد اعلام شده است [۲۸].

۱-۲-پژوهش های انجام شده نرم افزاری در استخراج ویژگیهای پویا

۲-۱-۱-ویژگی تعریق[۴]

"تعریق" یکی از شاخصه های عمومی و طبیعی اثر انگشت زنده می باشد. عرق از منافذ شروع می شود و در طول برآمدگیها منتشر می شود و محدوده ای را بین حفره ها ایجاد میکند که در تصویر تیره تر دیده می شود. الگوی فضایی به جا مانده از رطوبت با مشاهده چند تصویر اثر انگشت در طول زمان مشخص، بدست می آید. یک اثر انگشت زنده، تصویر غیریکنواختی[۵] از سطحی خاکستری در طول زمان از خود به نمایش میگذارد. این سطح خاکستری به دلیل پدیده تعریق که در حفره ها شروع شده و در طول برآمدگیها پیشرفت داشته بوجود می آید که در طول زمان قابل اهمیت است. در مقابل، یک اثر انگشت تقلبی هم در طول زمان، تصویر یکنواختی[۶] از خود بر جای میگذارد. از آنجایی که تعریق یک پدیده فیزیولوژیکی می باشد، در هر فرد متفاوت است. علاوه بر این، میزان تعریق، به محیط، فشار انگشت، فاصله زمانی و میزان رطوبت اولیه پوست نیز وابسته می باشد. برای اینکه بتوان از پدیده تعریق جهت استخراج ویژگی استفاده کرد، باید میزان تعریق را در طول زمان بر روی برآمدگیها با استفاده از سیگنالی که از خود بر جای میگذارد، محاسبه کرد. تغییرات سطح خاکستری در یک توالی زمانی از تصویر اول تا آخرین تصویر با توجه به حداکثر و حداقل محلی در طول برآمدگی، قابل اندازه گیری می باشد. به طور کلی، نوسان در اثر انگشت زنده بالاتر از اثر انگشت تقلبی می باشد. در آخرین تصویر در مقایسه با اولین تصویر، زمانیکه میزان رطوبت به بالاترین حد خود رسیده است، میزان سیگنال برآمدگی کوچکتر می باشد. الگوی زمانی از میزان رطوبت، بوسیله محاسبه ویژگی هایی مانند "درصد تغییر در انحراف معیار استاندارد" از سیگنال اولین تا آخرین اثر انگشت قابل محاسبه می باشد و در فرمول ۱ [۲۹] نمایش داده شده است.

$$\Delta = \frac{\sum_{i=1}^{m} c_{1i} - c_{1i-1}}{\sum_{i=1}^{m} c_{2i} - c_{2i-1}} \quad (۱)$$

که در آن m نشان دهنده طول سیگنال، $c_{1}i$ و $c_{2}i$ به ترتیب، نشان دهنده مقدار سطح خاکستری پیکسل i ام در تصویر گرفته شده اول و دوم می باشد.

فرمول شماره ۲[۲۹]میزان رشد سیگنال حداقل به حداکثر را نمایش می دهد.

$$\Delta = \frac{\sum_{j=1}^{m} Cmin_{2j} - Cmin_{1i}}{\sum_{j=1}^{m} Cmax_{2j} - Cmax_{1i}} \quad (۲)$$

۴. Perspiration Based
۵. No uniformity
۶. Uniformity

از دیگر ویژگیهای پویای قابل محاسبه در پدیده تعریق، تغییرات درصد اشباع خشکی و رطوبت می باشد که میزان سرعت ناپدید شدن اشباع خشکی و سرعت پدیدار شدن اشباع رطوبت را اندازه گیری میکند. این اندازه ها برای زمان مصرف شده جهت انتشار رطوبت از منافذ حساب می شود[۲۹]. فرمول شماره۳، ویژگی تغییرات درصد اشباع خشکی و فرمول ۴، ویژگی تغییرات درصد اشباع رطوبت را نمایش می دهد[۳۰].

۳) $\Delta=\frac{\sum_{i=1}^{m}\delta(C_{1i}\text{-}LT)-\delta(C_{2i}\text{-}LT)}{0.1+\sum_{i=1}^{m}\delta(C_{2i}\text{-}LT)}$

۴) $\Delta=\frac{\sum_{i=1}^{m}\delta(C_{2i}\text{-}HT)-\delta(C_{1i}\text{-}HT)}{0.1+\sum_{i=1}^{m}\delta(C_{1i}\text{-}HT)}$

۲-۱-۲. ویژگی اعوجاج برآمدگی[۷]

همانطور که در بخش اول نیز اشاره شد، زمانیکه یک اثر انگشت زنده بر روی سنسور، فشار وارد میکند و حرکتی را روی سنسور انجام می دهد، اعوجاج تولید شده بارز تر از اعوجاج تولید شده از اثر انگشت تقلبی می باشد. اعوجاج پوست توسط پردازش دنباله ای از فریم ها در نرخ بالای فریم حاصل می شود. زمانیکه کاربر، انگشت خود را بر روی سنسور میچرخاند و فشاری بر سنسور وارد میکند، اعوجاج بدست می آید. در ابتدا، فرض می شود اثر انگشت هیچ گونه اعوجاجی ندارد. جنبش بلوکهای تک تشخیص داده شده و توسط جریان نوری مدلسازی میشوند و سپس توالی کد اعوجاج مقایسه می شود[۳۱]. یک اثر انگشت زنده با افزایش فشار، باعث افزایش شدت سیگنال در نواحی و اطراف آن می شود. مقدار مثبت ضریب همبستگی، یک شاخص و ویژگی خوب جهت تشخیص زنده بودن اثر انگشت می باشد. فرمول شماره **۵**، ویژگی ضریب همبستگی و فرمول شماره ۶ شدت سطح سیگنال را نشان می دهد[۳۰] .

۵) $Si= Ni \times W \times W$

که در آن S_i نشان دهنده محدوده اثر انگشت از فریم i_{th} ***می باشد و*** N_i تعداد بلوک هایی است که واریانس بیشتر از حد آستانه دارند. واریانس برای هر بلوک با سایز ۱۶ * ۱۶ $(W\times W)$ محاسبه می شود.

۶) $Int_i=\frac{\sum_{I(x'y')\in S}I(x'y')}{s_i}$

که در آن Int_i شدت سیگنال فریم i_{th} می باشد.$I(x,y)$ شدت محیط اثر انگشت Si می باشد.$\in$ آستانه مورد استفاده برای جداسازی پیکسلهای اثر انگشت مربوطه از پس زمینه می باشد[۲۶].

در این فصل به بررسی پژوهشهای انجام شده در زمینه سیستم های احراز هویت، انواع روشهای تقلب در سیستم های مذکور، انواع روشهای کشف تقلب بر اساس طبقه بندی های موجود، پرداخته شد.در بخش بعد، به استخراج ویژگی اثر انگشت و انتخاب بهترین ویژگی پرداخته میشود.

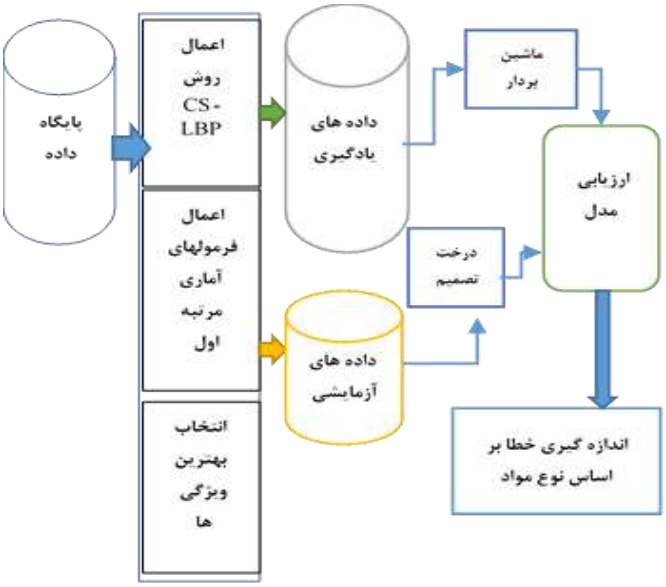
۳. معماری سیستم پیشنهادی

در این طرح پژوهشی، از متدولوژی "CRISP-DM"[۸]، برای انجام پیاده سازی استفاده شده است که یکی از متدولوژی های پر کاربرد در زمینه داده کاوی می باشد. این متدولوژی از شش فاز برای رسیدن به هدف استفاده میکند. در فاز اول، به شناخت سیستم پرداخته می شود. تعیین اهداف پروژه و بررسی وضعیت موجود، از مهمترین وظایفی است که در این مرحله مشخص می شود. فاز دوم، شناخت داده های مورد نظر می باشد. در این فاز به جمع آوری داده های موجود که داده های اولیه نامیده می شوند و همینطور، توصیف و بررسی کیفیت آنها و یکپارچه سازی داده ها ، پرداخته می شود. در فاز سوم، که

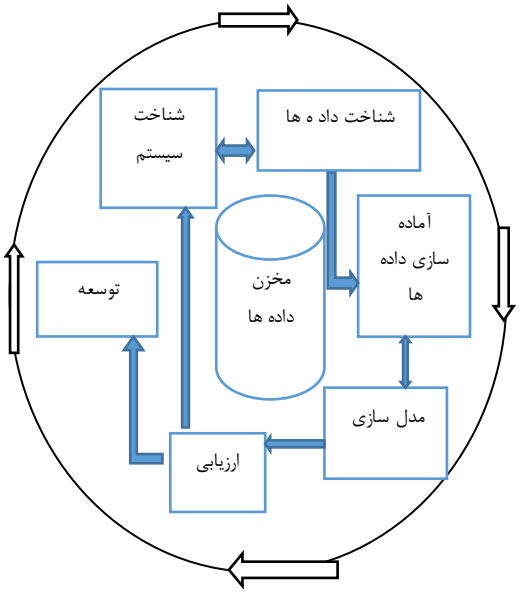
۷. Ridge Distortion

۸. Cross Industry Standard Process for Data Mining

مهمترین فاز در این متدولوژی می باشد، به آماده سازی داده های اولیه پرداخته می شود. در فاز چهارم، مدل مربوطه برای انجام مدل سازی انتخاب شده و بر روی داده های آماده سازی شده اجرا میگردد. در فاز پنجم، پس از اعمال مدل سازی، به ارزیابی مدل و بررسی اعتبار سنجی آن پرداخته می شود و در فاز نهایی(فاز ششم)، در صورتی که تمامی مراحل قبل به درستی انجام شده باشد، از نتایج بدست آمده استفاده خواهد شد. مهمترین وظایف در این فاز، بهبود کارایی و دقت، نظارت و سنجش خروجی ها، آزمون روش ها یا پارامترهای دیگر می باشد که در فاز ششم یا فاز توسعه انجام می شود. نمودار۳ مراحل انجام این متدولوژی را نمایش می دهد[۳۱]. معماری پیشنهادی در این پژوهش در نمودار ۴ قابل نمایش میباشد.



نمودار ۳-متدولوژی CRISP_DM



نمودار۴- معماری طرح پیشنهادی

۴. استخراج ویژگی

انتخاب روش مناسب جهت استخراج ویژگی، یکی از عوامل بسیار موثر و کلیدی در سیستمهای احراز هویت بیومتریک می باشد. با توجه به روش های گوناگونی که در فصل دوم به آن اشاره شد، انتخاب روش موثر و کارا جهت استخراج ویژگی، یکی از چالشهای بحث بر انگیز در این زمینه است. استخراج ویژگی، در حقیقت استخراج اطلاعات حاوی ارزش از داده های خام مسئله می باشد که بتواند ما را به سمت طبقه بندی مناسب سوق دهد. این اطلاعات باید در بین نمونه های کلاسهای طبقه بندی، دارای بیشترین تفاوت و در داخل کلاس مربوطه دارای بیشترین شباهت باشد. از سوی دیگر، انتخاب ویژگی مناسب، برای تصمیم گیری طبقه بندی کننده مورد نظر، جهت یافتن بهترین مرز، برای حصول سهولت و دقت بیشتر، بسیار کارا و موثر می باشد. در طرح پیشنهادی، از روش CS-LBP[۹] برای پردازش تصویر جهت استخراج ویژگی استفاده شده است. در روش های پیشین که در فصل دوم به آن اشاره شد، یکی ازطرح های انتخاب ویژگی، استفاده از روش LBP بود که در آن تصویر به چند زیر تصویر، تقسیم میشد و هر خانه از ماتریس ۳*۳ ،حاوی مقداری بود که نشان دهنده میزان شدت نور در آن

[۹] . Center Symmetric Local binary pattern

پیکسل بود. سپس برای تبدیل تصویر به حالت باینری، نقطه مرکزی ماتریس به عنوان حد آستانه در نظر گرفته میشد و تمامی مقادیر باقی مانده در داخل ماتریس با حد آستانه مقایسه میشد. برای مقادیر کوچکتر از حد آستانه، مقدار صفر و برای مقادیر بزرگتر و مساوی از حد آستانه مقدار یک در نظر گرفته میشد. سپس مقادیر باینری محاسبه میشد و تعداد بین های تصویر جهت رسم هیستوگرام تصویر برای استخراج ویژگی های آماری بدست می آمد. رابطه ریاضی آن در فرمول ۷ قابل مشاهده می باشد.

$$۷)\ LBP(x_m,y_m)=\sum_{i=0}^{p-1} S(g_P-g_m)2^i$$

که در آن g_m مقدار ماتریس مرکزی، g_p مقدار ماتریس پیکسل خانه مورد نظر، p تعداد پیکسل مربوط به تصویر می باشدو تابع S جهت مشخص کردن مقادیر باینری با توجه به میزان آستانه به صورت فرمول ۸ قابل مشاهده می باشد.

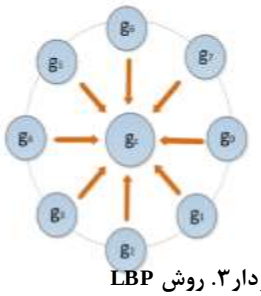
$$۸)S(x)=\begin{cases}0 & x<0\\ 1 & x\geq 0\end{cases}$$

با توجه به فرمولهای ۷و۸ حداکثر میزان نقاط به دست آمده ۲۵۵ می باشد که مقدار قابل توجهی جهت ترسیم هیستوگرام تصویر است. در این طرح پژوهشی، به منظور بهبود کارایی در محاسبات، کاهش تعداد بین های هیستوگرام، با روش "CS-LBP" پیشنهاد شده است. تفاوت روش پیشنهادی با روش باینری محلی در این است که به جای استفاده از تمامی خانه های ماتریس با ماتریس مجاور فقط از ماتریسهای لبه استفاده می شود. نقطه مرکزی ماترس نیز به عنوان حد آستانه در نظر گرفته می شود. این روش نسبت به روش LBP ، دارای بازه محاسباتی کمتری است و قابلیت ارائه جزئیات لبه ها در تصویر، بیشتر است . این روش به جای مقایسه هر پیکسل با پیکسل مرکزی ، دو پیکسل متقارن را باهم مقایسه می کند و با یک مقدار آستانه، اختلاف را بدست آورده و یک نتیجه دودویی ارائه می دهد. رابطه ریاضی آن در فرمول ۹ و ۱۰قابل مشاهده می باشد.

$$۹)\ CS\text{-}LBP(x_m,y_m)=\sum_{i=0}^{(\frac{P}{2}-1)} S\left(g_i-g_{i+p/2}\right)2^i$$

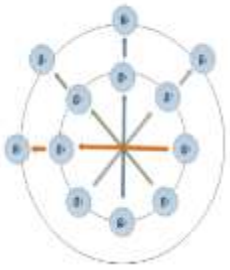
$$۱۰)S(x)=\begin{cases}0 & x\leq 0\\ 1 & x>0\end{cases}$$

نمودار۴و۵ به ترتیب تصویر روش LBP و CS-LBP را به نمایش میگذارد.



LBP=
S(g۰-gc)۲۰+
S(g۱-gc)۲۱+
S(g۲-gc)۲۲+
S(g۳-gc)۲۳+
S(g۴-gc)۲۴+
S(g۵-gc)۲۵+
S(g۶-gc)۲۶+
S(g۷-gc)۲۷
=(۰:۲۵۵)

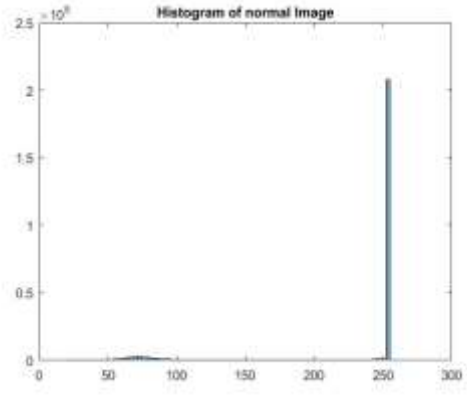
نمودار۳. روش LBP



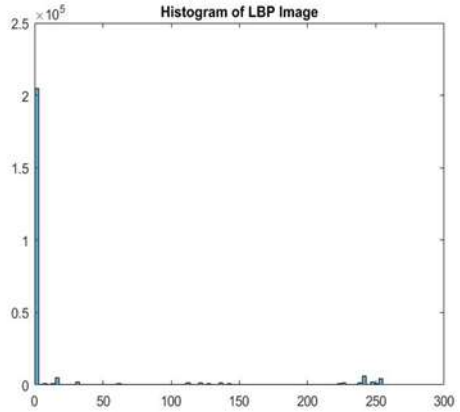
CS-LBP=
S(|g۰-g۴|)۲۰+
S(g۱-g۵)۲۱+
S(g۲-g۶)۲۲+
S(g۳-g۷)۲۳
=(۰:۱۵)

نمودار۴. روش CSLBP

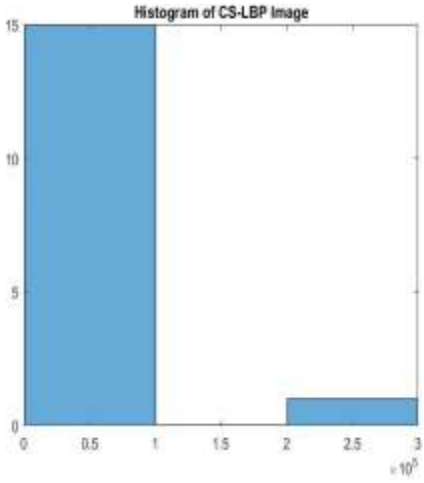
خروجی CS_LBP، ۱۶ بین خواهد بود یعنی در هر مولفه ۱۶ خروجی و خروجی ها بین ۰ و ۱۵ خواهد بود. پس در سه مولفه ۳*۱۶ ویژگی هیستوگرام محاسبه و در ماتریس ذخیره می شود. در حالی که خروجی LBP، ۲۵۶ بین می باشد و تعداد خروجی کاهش میابد و بار محاسباتی را کاهش می دهد. نمودار ۶ تا ۸، هیستوگرام یک تصویر اثر انگشت بصورت عادی، LBP و CS-LBP را نمایش می دهد.



نمودار ۲-هیستوگرام تصویر نرمال



نمودار ۳-هیستوگرام تصویر LBP



نمودار ۴-هیستوگرام تصویر CS-LBP

۴.۱. ویژگیهای آماری مرتبه اول[۱۰]

احتمال مشاهده مقدار سطح خاکستری از یک موقعیت انتخاب شده به صورت تصادفی، میتواند توسط هیستوگرام شدت پیکسل مربوط به تصویر محاسبه شود. اگر H(n) را مقدار نرمال شده هیستوگرام و N را تعدادبین ها در نظر بگیریم، مجموعه ای از فرمولهای آماری به صورت زیرقابل تعریف می باشد[۲۰].

۱۰. First-Order Statistics

– ویژگی میانه [۱۱]

(۱۱) $M=arg\,min\sum_{n}^{n}H(n)|n-a|$

– ویژگی انرژی [۱۲]

(۱۲) $e=\sum_{n=0}^{N-1}H(n)^2$

–ویژگی آنتروپی [۱۳]

(۱۳) $S=-\sum_{n=0}^{N-1}H(n)\log H(n)$

–ویژگی میانگین [۱۴]

(۱۴) $\mu=\frac{1}{N}\sum_{n=0}^{N-1}H(n)$

–ویژگی واریانس [۱۵]

(۱۵) $\sigma^2=\sum_{n=0}^{N}(n-\mu)^2H(n)$

–ویژگی چولگی [۱۶]

(۱۶) $\gamma_1=\frac{1}{\sigma^3}\sum_{n=0}^{N-1}(n-\mu)^3H(n)$

– درجه اوج [۱۷]

(۱۷) $\gamma_2=\frac{1}{\sigma^4}\sum_{n=1}^{N-1}(n-\mu)^4H(n)$

–ضریب تغییرات [۱۸]

(۱۸) $cv=\frac{\sigma}{\mu}$

۵ .طبقه بندی کننده ها

مرحله طبقه بندی، بحرانی ترین مرحله در یک سیستم شناسایی می باشد که در آن ویژگیهای استخراج شده از الگوی ورودی با مدلهای موجود در پایگاه داده مقایسه می شود. سپس طبقه بندی کننده، با توجه به ویژگیهای استخراج شده، الگوی ورودی را به یکی از دو کلاس مورد نظر اختصاص می دهد. به طور کلی، طبقه بندی در دو مرحله انجام می شود. مرحله اول، مرحله یادگیری و مرحله دوم، مرحله آزمایش یا پیش بینی می باشد. از آنجایی که طبقه بندی، یک روش نیازمند به یادگیری می باشد، در مرحله یادگیری، دانش به سیستم تزریق می شود وهمه موارد آن معلوم است. "داده آزمایش"، بعد از یادگیری انجام می شود که کاملا در مقابل "داده یادگیری" است ومقدار آن مجهول است. "داده اعتبار سنجی"[۱۹]، از آنجا که در حین

---

۱۱. Median

۱۲. Energy

۱۳. Entropy

۱۴. Mean

۱۵. Variance

۱۶. Skewness

۱۷. Kurtosis

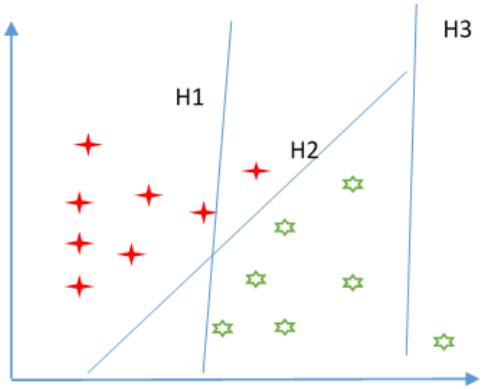
۱۸. Coefficient of variation

۱۹. Validation

یادگیری است شبیه به داده های یادگیری و ازآنجایی که مقادیر آن مجهول است شبیه به داده های آزمایش می باشد. زمانیکه داده ها کم باشند، به جای اعتبار سنجی، از اعتبار سنجی متقابل[۲۰]، استفاده میکنیم. برای اینکه کارایی فرآیند یادگیری را بسنجیم، این روش را بکار می گیریم. با اینکار تکرار را برای یادگیری انجام میدهیم. تکرار را تا جایی انجام میدهیم که به بهترین ارزیابی برسیم. این تکرار در چند طبقه برای هر دونوع داده یادگیری و آزمایش انجام می شود. از این رو به آن اعتبار سنجی متقابل چند لایه ای[۲۱] میگویند. طبقه بندی کننده ها دارای انواع مختلفی میباشند که از انواع آن میتوان به طبقه بندی کننده ساختاری، آماری، شبکه عصبی و ماشین بردار پشتیبان اشاره نمود. در این روش پیشنهادی از هر دو الگوریتم SVM و درخت تصمیم برای بدست آوردن طبقه بندی کننده ای سریعتر، بدون پایین آمدن دقت در طبقه بندی، استفاده شده است.

۵.۱. الگوریتم SVM

کاری که الگوریتم SVM انجام می دهد این است که نزدیکترین عضو از هر کلاس به خط تفکیک کننده را که به آن بردار پشتیبان میگوییم انتخاب میکند. کار بردارهای پشتیبان، دور کردن خط تفکیک از خودشان است. بردارهای پشتیبان با هم همکاری میکنند تا به هدف خود برسند. آنقدر این کار انجام می شود تا به کمترین ریسک عملیاتی برسیم و تا زمانی این کار انجام می شود که بردارهای پشتیبان به جایی برسند که دیگر در خلاف جهت هم کار کنند و هر دو با هم راضی نشوند. در نمودار ۹ ، تفکیک کننده H۲، آخرین وضعیت بهینه موجود می باشد.



نمودار ۵- تفکیک کننده در شبکه عصبی با اضافه کردن داده

۵.۲. الگوریتم ID۳

یک درخت به نام T که یک درخت خالی است، ساخته می شود. اگر همه اعضای D از یک کلاس باشند، یک گره برگ با برچسب کلاس مربوطه ایجاد می شود. اگر فهرست ویژگیهای جدا کننده خالی باشد، یک برگ با برچسب کلاسی که بیشترین عضو را دارد، ایجاد می شود. سپس، بهترین ویژگی جدا کننده پیدا می شود. با توجه به مقادیر بهترین ویژگی تفکیک کننده، انشعابهایی را ایجاد میکنیم و به ازای هر انشعاب j ، مجموعه D(j) شامل همه مقادیری است که در آن انشعاب صدق میکند. سپس، تابع TDT(Dj) را فراخوانی و نتیجه آنرا به درخت اصلی، ملحق میکنیم و در انتها، درخت T را به عنوان نتیجه باز میگردانیم.

۶-پایگاه داده

یکی از چالشهای بزرگ در زمینه تشخیص تقلب در داده های بیومتریک، داشتن یک پایگاه داده استاندارد می باشد. تا سال ۲۰۰۸، اکثر تحقیقات بر اساس پایگاه داده های شخصی بود که محققین، خود به جمع آوری آن مشغول بودند. در سال ۲۰۰۹ پایگاه داده های استانداردی، جهت بررسی پژوهش، در اختیار محققین قرار گرفت که از آن جمله میتوان به

[۲۰] . Cross Validation
[۲۱] . K-Fold Cross Validation

پایگاه داده "LivDet" و پایگاه داده "ATVS" اشاره نمود. در این پژوهش از پایگاه داده LivDet استفاده شده است. این پایگاه داده، توسط دپارتمان مهندسی الکترونیک و برق دانشگاه کاگلیاری[۲۲] ایتالیا و دپارتمان مهندسی کامپیوتر و الکترونیک دانشگاه کلارکسون[۲۳] آمریکا، از سال ۲۰۰۹، به منظور تحقیقات بر روی تشخیص زنده بودن بیومتریک، سازماندهی شده است. این مجموعه به صورت LivDet۲۰۰۹، LivDet۲۰۱۱ ، LivDet۲۰۱۳ و LivDet۲۰۱۵ قابل دسترسی می باشد. در این پایان نامه از LivDet۲۰۱۵ جهت ارزیابی طرح پروژهشی استفاده شده است. در این پایگاه داده از چندین مجموعه داده استفاده شده است. در مجموعه داده بیومتریک اثر انگشت، دو مجموعه آزمایش و یادگیری موجود می باشد. هر کدام از این مجموعه داده ها، خود به چند زیر مجموعه تقسیم میشوند که در برگیرنده سنسوری می باشد که تصاویر از آنها گرفته شده است. این سنسورها شامل Cross Match، Digital Persona ، Green Bit ، Hi_Scan می باشد و در مجموعه یادگیری، علاوه بر این سنسورها از Time_Series جهت ویژگیهای پویا استفاده شده است. در هر کدام از مجموعه داده های ذکر شده، دو زیر مجموعه دیگر وجود دارد که شامل زیر مجموعه اثر انگشت زنده و اثر انگشت تقلبی می باشد. در زیر مجموعه اثر انگشتهای تقلبی، زیر مجموعه های دیگری نیز وجود دارد که شامل نوع مواد استفاده شده در ساخت اثر انگشت تقلبی می باشد. از جمله می توان به چسب چوب، خمیر بازی، لاتکس، ژلاتین، بادی دابل[۲۴] و اکو فلکس[۲۵] اشاره کرد.

۷. نرم افزار و سخت افزار مورد استفاده

برای پیاده سازی طرح پیشنهادی، از دو نرم افزار متلب"R۲۰۱۵b" با ورژن ۸,۶,۰,۲۶۷۲۴۶ و "Rapid Miner" با ورژن ۷,۲,۰۰۱ استفاده شده است. تمامی ارزیابی ها بر روی سیستمی با مشخصات Intel Corei۷ ، پردازنده با سرعت ۲,۶۰ گیگا هرتز، حافظه ۸ گیگابایت بر روی سیستم عامل ویندوز ۱۰، انجام پذیرفته است.در این فصل، به معرفی طرح پیشنهادی پرداخته شد. در مرحله استخراج ویژگی، از الگوی باینری محلی مقارن مرکزی جهت کاهش بار عملیاتی بهره گرفته شد. در ادامه، روش های آماری مرتبه اول جهت استخراج ویژگی های ایستا ، اعمال گردید. در انتها، جهت مدلسازی، از روش های طبقه بندی ماشین یادگیری، از جمله درخت تصمیم و ماشین بردار پشتیبان و همچنین طرح ترکیبی این دو، در طرح پیشنهادی، استفاده شد، تا در فصل بعد به مقایسه ارزیابی سیستم های پیشین با سیستم پیشنهادی پرداخته شود.

۸. ارزیابی و نتیجه گیری

در این بخش به ارزیابی طرح پیشنهادی پرداخته شد. برای ارزیابی مدل مربوطه، ۵۰ تصویر اثر انگشت، که ۱۰تصویر آن، شامل اثر انگشت های زنده و ۴۰ تصویر، شامل اثر انگشتهای تقلبی (از ۴ ماده مختلف ذکر شده) بودند، انتخاب شد. اندازه C برابر با ۰ و میزان اپسیلن برابر با $\varepsilon=0,48$ انتخاب شد. با این پارامترها، تعداد "support vector" به حداقل خود یعنی ۲ عدد رسید که میزان آلفا در آن برابر با ۰,۱۷۳ بود. در قسمت استخراج ویژگی، از فرمولهای آماری مرتبه اول بر روی هیستوگرام تصاویر که با استفاده از تکنیک باینری محلی متقارن مرکزی بهینه شده بود، بهره گرفته شد.نمودار هیستوگرام مشخصه های آماری در دو شکل نرمال و باینری محلی متقارن مرکزی در نمودار ۱۰ و ۱۱ قابل نمایش میباشد. همانطور که در نمودار مشاهده میشود، از بین ویژگی های آماری، ویژگی های میانگین، آنتروپی و انرژی، که در محاسبات تاثیری نداشتند حذف گردید و ویژگی های چولگی، اوج، انحراف معیار استانداردو واریانس به عنوان بهترین ویژگی انتخاب گردید.

---

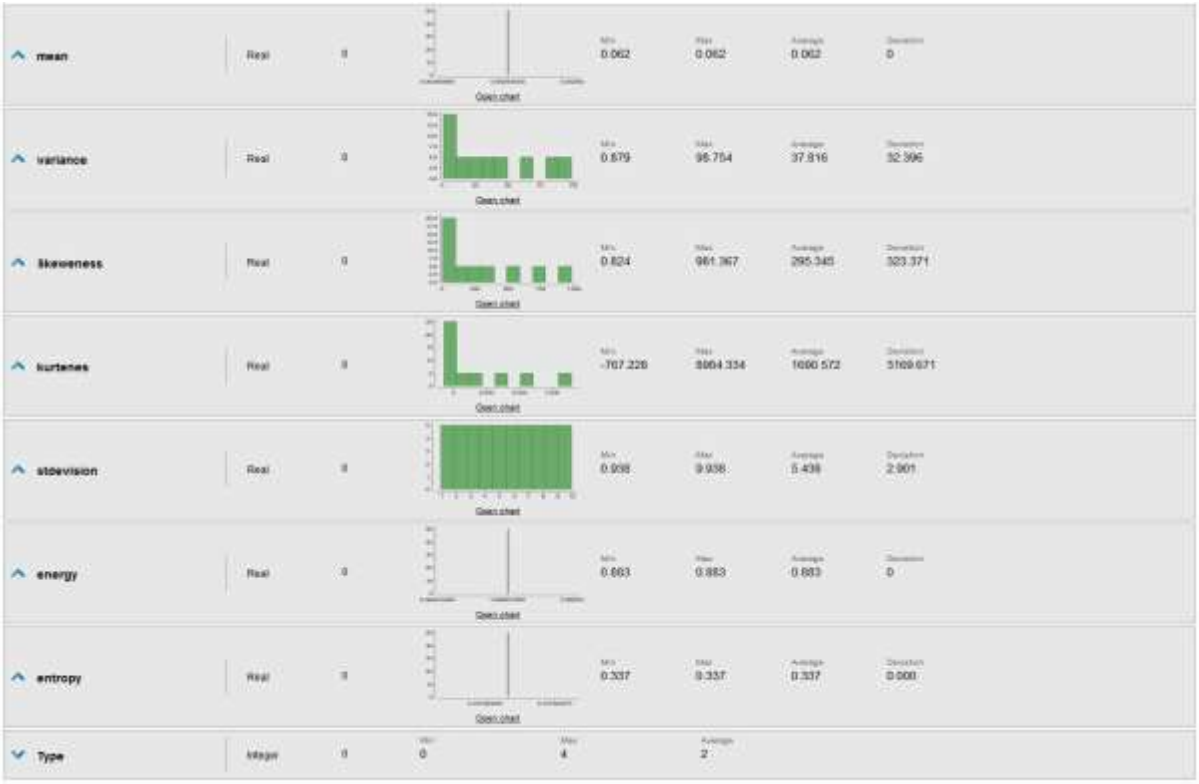
[۲۲] . Cagliari

[۲۳] . Clarkson

[۲۴] . Body Double

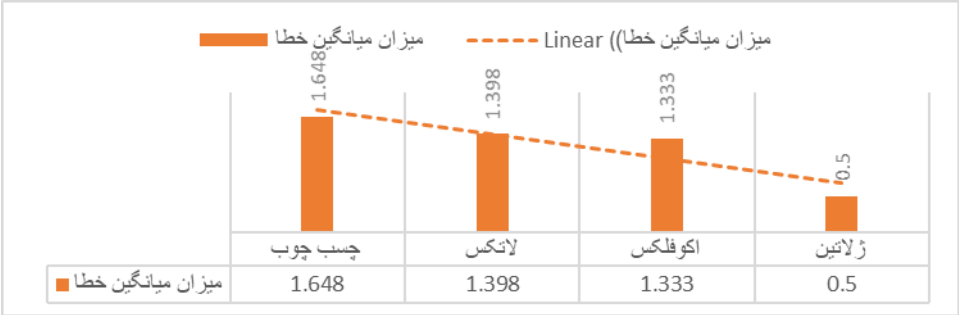
[۲۵] . Ecoflex

نمودار ۶- هیستوگرام نرمال ویژگی های آماری مرتبه اول



نمودار ۷- هیستوگرام باینری محلی متقارن مرکزی ویژگی های آماری مرتبه اول

همانطور که در نمودار مشاهده میشود، از بین ویژگی های آماری، ویژگی های میانگین، آنتروپی و انرژی، که در محاسبات تاثیری نداشتند حذف گردید و ویژگی های چولگی، اوج، انحراف معیار استانداردو واریانس به عنوان بهترین ویژگی انتخاب گردید. پس از استخراج بهترین ویژگی ها جهت دادن ورودی به طبقه بندی کننده به الگوریتم ترکیبی ماشین بردار پشتیبان و درخت تصمیم،دیتا ست مورد نظر آماده گردید. دیتاست مربوطه به طور مجزا برای مواد مختلف مورد ارزیابی قرار گرفت. میزان اعتبار سنجی ، بر اساس متوسط میانگین خطا در طبقه بندی محاسبه گردید. در جدول ۱ و نمودار ۱۲ نتایج ارزیابی قابل مشاهده میباشد.



نمودار ۸- میزان میانگین خطا بر اساس نوع مواد استفاده شده در اثر انگشت تقلبی

بر اساس این ارزیابی، طبقه بندی کننده ترکیبی توانست اثر انگشتهای تقلبی ژلاتینی را با کمترین میزان خطا، و اثر انگشت تقلبی چسب چوب را با بیشترین میزان خطا طبقه بندی نماید.

جدول ۱- میانگین درصد خطا بر اسا مواد مورد استفاده در اثر انگشت

نوع مواد	چسب چوب	لاتکس	اکوفلکس	ژلاتین
میانگین خطا	۱,۶۴۸	۱,۳۹۸	۱,۳۳۳	۰,۵۰۰

۹. مراجع

۱. Cortes, C., Vapnik, V.: *Support-Vector Networks*. Machine Learning, vol. ۲۰ (۳), pp. ۲۷۳-۲۹۷ (۱۹۹۵)

۲. Wikipedia: *History of Fingerprint by Nehemiah Grew*. Available from: https://en.wikipedia.org/wiki/Nehemiah_Grew (۱٦۸٤)

۳. Harold Cumins , Kennedyt, R.W.: *Purkinje's Observations (۱۸۲۳) on Finger Prints and Other Skin Feature*. Criminal Law and Criminology, vol. ۳۱ (۳) (۱۹٤۰)

٤. Stigler, S.M.: *Galton and Identification by Fingerprints*. (۱۹۹۵)

٥. Emanuela Marasco , Y.D.A.R.: *Combining Match Scores with Liveness Values in a Fingerprint Verification System* IEEE pp. ٤۱۸ - ٤۲٥ (۲۰۱۲)

٦. _۲۰۰۷>*Swb_Vulnerabilitiesrecentadvances_Galbally.Pdf*>.

۷. Javier Galbally, J.F., and Javier Ortega-Garcia: *Vulnerabilities in Biometric Systems: Attacks and Recent Advances in Liveness Detection*. Biometrics Recognition Group (۲۰۰۷)

۸. Bowden-Peters, E., Phan, R.C.W., Whitley, J.N., Parish, D.J.: *Fooling a Liveness-Detecting Capacitive Fingerprint Scanner*. Springer Berlin Heidelberg, vol. ٦۸۰٥, pp. ٤۸٤-٤۹۰ (۲۰۱۲)

۹. Yang, S., Wang, C.F., Chen, S.: *A Release-Induced Response for the Rapid Recognition of Latent Fingerprints and Formation of Inkjet-Printed Patterns*. Angew Chem Int Ed Engl, vol. ٥۰ (۱٦), pp. ۳۷۰٦-۹ (۲۰۱۱)

۱۰. T.Matsumoto, H.M., K.Yamada,S.Hoshino: *Impact of Artificial "Gummy" Finger on Fingerprint System*. vol. ٤٦۷۷ (۲۰۰۲)

۱۱. Huang, Q., Chang, S., Liu, C., Niu, B., Tang, M., Zhou, Z.: *An Evaluation of Fake Fingerprint Databases Utilizing Svm Classification*. Pattern Recognition Letters, vol. ٦۰-٦۱, pp. ۱-۷ (۲۰(۱٥

۱۲. Frassetto Nogueira, R., de Alencar Lotufo, R., Campos Machado, R.: *Evaluating Software-Based Fingerprint Liveness Detection Using Convolutional Networks and Local Binary Patterns*. pp. ۲۲-۲۹ (۲۰۱٤)

۱۳. Abhishek, K., Yogi, A.: *A Minutiae Count Based Method for Fake Fingerprint Detection*. Procedia Computer Science, vol. ٥۸, pp. ٤٤۷-٤٥۲ (۲۰۱٥)

۱٤. Mensvoort, M.v.; Available from: http://www.handresearch.com/diagnostics/fingerprints-sexe-males-females.htm (۲۰۱٦)

۱٥. Gragnaniello, D., Poggi, G., Sansone ,C., Verdoliva, L.: *Local Contrast Phase Descriptor for Fingerprint Liveness Detection*. Pattern Recognition, vol. ٤۸ (٤), pp. ۱۰٥۰-۱۰٥۸ (۲۰۱٥)

۱٦. Marasco, E., Ross, A.: *A Survey on Antispoofing Schemes for Fingerprint Recognition Systems*. ACM Computing Surveys, vol. ٤۷ (۲), pp. ۱-۳٦ (۲۰۱٤)

۱۷. Reddy, P.V., Kumar, A., Rahman, S., Mundra, T.S.: *A New Antispoofing Approach for Biometric Devices*. IEEE Trans Biomed Circuits Syst, vol. ۲ (٤), pp. ۳۲۸-۳۷ (۲۰۰۸)

۱۸. Baldisserra, D., with, A., DEIS, U.d.B., , A.F., , D.M., , D.M.: *Fake Fingerprint Detection by Odor Analysis*. Springer Berlin Heidelberg, vol. ۳۸۳۲, pp. ۲٦٥-۲۷۲ (۲۰۰٦)

۱۹. Jain, A.K., Abhyankar, A.S., Schuckers, S.C., Ratha, N.K.: <*Title*>*a Wavelet-Based Approach to Detecting Liveness in Fingerprint Scanners*</*Title*>. vol. ٥٤۰٤, pp. ۲۷۸-۲۸٦ (۲۰۰٤)

۲۰. A. Antonelli, R.C.D.M.D.M.: *Fake Finger Detection by Skin Distortion Analysis*. IEEE Transactions on Information Forensics and Security, vol. ۱ (۳), pp. ۳٦۰ - ۳۷۳ (۲۰۰٦)

۲۱. Derakhshani, R., Schuckers, S.A.C., Hornak, L.A., O'Gorman, L.: *Determination of Vitality from a Non-Invasive Biomedical Measurement for Use in Fingerprint Scanners*. Pattern Recognition, vol. ۳٦ (۲), pp. ۳۸۳-۳۹٦ (۲۰۰۳)

۲۲. Jia Jia , L.C., Kaifu Zhang , Dawei Chen *A New Approach to Fake Finger Detection Based on Skin Elasticity Analysis*. Springer-Verlag Berlin, Heidelberg, pp. ۳۰۹-۳۱۸ (۲۰۰۷)

۲۳. Yangyang Zhang , J.T., Xinjian Chen , Xin Yang , Peng Shi *Fake Finger Detection Based on Thin-Plate Spline Distortion Model*. Springer-Verlag Berlin, Heidelberg pp. ۷٤۲-۷٤۹ (۲۰۰۷)

۲٤. Aditya Abhyankar, S.S.: *Integrating a Wavelet Based Perspiration Liveness Check with Fingerprint Recognition*. Elsevier Science Inc. New York, NY, USA vol. ٤۲ (۳), pp. ٤٥۲-٤٦٤ (۲۰۰۹)

۲٥. Parthasaradhi, S.T., Jain ,A.K., Derakhshani, R., Hornak, L.A., Schuckers, S.C., Ratha, N.K.: *Improvement of an Algorithm for Recognition of Liveness Using Perspiration in Fingerprint Devices*. vol. ٥٤۰٤, pp. ۲۷۰-۲۷۷ (۲۰۰٤)

۲٦. RezaDerakhshania, S.C.S., LarryA.Hornaka, LawrenceO'Gormanb٥ *Determination of Vitality from a Non-Invasive Biomedical Measurement for Use in Ngerprint Scanner*. pp. ۱-۱٤ (۲۰۰۱)

۲۷. Cappelli, R., Maio, D., Maltoni, D.: *Modelling Plastic Distortion in Fingerprint Images*. vol. ۲۰۱۳, pp. ۳۷۱-۳۷۸ (۲۰۰۱)

۲۸. P.chapman, J.C., R.Kerber,T.Khabaza,T.Reinartzrysler,C.shearer and R.wirth: *Crisp_Dm ۱,۰:Step by Step Data Mining Guid*. (۱۹۹۹)

۲۹. Aditya Abhyankar , S.S.: *Fingerprint Liveness Detection Using Local Ridge Frequencies and Multiresolution Texture Analysis Techniques* IEEE, pp. ۳۲۱ - ۳۲٤ (۲۰۰٦)

۳۰. C.Sansone, E.M.a.: *On the Robustness of Fingerprint Liveness Detection Algorithms against New Materials Used for Spoofing*. International conference on Bio-Inspired System and Signal processing, pp. ۱-۹ (۲۰۱۱)

۳۱. Bozhao Tan , S.S.: *Spoofing Protection for Fingerprint Scanner by Fusing Ridge Signal and Valley Noise*. Elsevier Science Inc. New York, NY, USA vol. ٤۳ (۸), pp. ۲۸٤٥-۲۸٥۷ (۲۰۱۰)