

مروری بر کاربرد شبکه های عصبی در بیومتریک¹

محمد قاسمی قره‌بلاغ
گروه مهندسی برق - کنترل
حسین پناهی
گروه مهندسی برق - قدرت
هادی رزمی
گروه مهندسی برق - کنترل
دانشکده مهندسی برق و کامپیوتر دانشگاه تبریز
sthadirazmi@yahoo.com mhosseinpanahi@yahoo.com mggh60@yahoo.com

چکیده: در این مقاله ابتدا به تعریف بیومتریک و طبقه عملکرد آن می پردازیم و با معرفی انواع روش های بیو متریک و کار بردهای آنها با سیستم های تشخیص هویت و تایید هویت آشنا می شویم. با معرفی سیستم ها تشخیص الگو کاربرد شبکه های عصبی در بیومتریک را مورد بررسی قرار خواهیم داد و در نهایت با معرفی چند روش مهم و پر کاربرد از بیومتریک و توضیح مختصری در مورد آنها شبکه های عصبی استفاده شده در آنها را نام خواهیم برد. در ضمن در هر مورد از روش های بیومتریک خواص منحصر به فرد آنها را ذکر کرده و به طور مختصر این روش ها را با هم مقایسه خواهیم نمود.

کلمات کلیدی: شبکه های عصبی، بیومتریک، تشخیص الگو، بردار ویژگی.

۱- مقدمه

روشهای به کار رفته در بیومتریک متنوع بوده و روز بروز نیز توسعه بیشتری می یابند، یکی از این روش ها استفاده از شبکه های عصبی مصنوعی می باشد که در انواع مختلف بیومتریک مورد استفاده قرار می گیرند. بیومتریک یک تکنولوژی نوین برای تشخیص خودکار هویت افراد می باشد که از ویژگی های منحصر به فردی از قبیل اثر انگشت، صوت، چهره، عنبیه، شبکیه چشم، کف دست، امضا، سیاهرگ مچ دست، هندسه دست می باشد. همچنین بیومتریک راه حلی است برای افزایش امنیت جوامع اطلاعاتی نسبت به امنیت حاصله از روش های تشخیص هویت جاری از قبیل کلمه عبور²، Pin code³، کارتهای نوار مغناطیسی.

مزایای تکنولوژی بیومتریک نسبت به روش های تشخیص هویت قدیمی عبارتند از:

- ضرورت حضور فیزیکی فرد در محل شناسایی
- عدم نیاز به یاد آوری کلمه عبور، PIN و یا حمل کارت شناسایی.
- کاهش شدید امکان تقلب و دسترسی غیر مجاز و صرفه جویی میلیاردی در اقتصاد.

¹ -Biometrics

² -Password

³ - Personal Identification Number

۲- یک سیستم بیومتریک چگونه کار می کند ؟

سیستمهای بیومتریک از اجزای زیر تشکیل شده اند: ۱- خواننده یا وسیله اسکن عضو مورد نظر ۲- نرم افزار تبدیل کننده اطلاعات جمع آوری شده به شکل دیجیتال. ۳- پایگاه داده که داده های بیومتریک را برای مقایسه با موارد از پیش ضبط شده فراهم می کند، می باشد.

۲-۱- انواع روش های بیومتریک

روشهای بیومتریک به دو نوع فیزیکی و رفتاری تقسیم می شوند. بیومتریک فیزیکی برای تشخیص هویت و بیومتریک رفتاری برای تایید هویت مورد استفاده قرار می گیرند. و اما ویژگی های مورد استفاده در بیومتریک فیزیکی عبارتند از: شکل دندان، طول اعضای بدن، اثر انگشت، چهره و صورت، هندسه دست، عنبیه، شبکیه، DNA، دندان، نوع راه رفتن، بوی بدن، شکل گوش، اثر کف دست، ورید های مچ دست و ویژگی های مورد استفاده در بیومتریک رفتاری عبارتند از: سخن گفتن، امضا، سرعت و ریتم کلمات تایپ شده. با توجه به اینکه سیستمهای تایید هویت، که از یک نوع نمایشگر و تشخیص دهنده بیومتریک استفاده می کنند اغلب مجبورند که با داده های نویزدار، و درجه خطای نامحدود مواجه شوند بنا بر این به منظور بهبود اجرای عمل تطابق، در چنین وضعیت هایی سیستمهای بیومتریک مرکب مورد استفاده قرار می گیرند [28].

۲-۲- کاربردهای سیستمهای بیومتریک

کاربردهای سیستمهای بیومتریک را میتوان به ۳ گروه زیر طبقه بندی نمود:

- **تجاری:** از قبیل دخول به شبکه های کامپیوتری، امنیت اطلاعات الکترونیکی، دستیابی اینترنتی، سیستمهای خود گردان بانک، کارتهای اعتباری، کنترل دستیابی فیزیکی، تلفن های سلولی، آموزش از راه دور
- **دولتی:** از قبیل شماره شناسایی ملی، گواهینامه رانندگی، امنیت اجتماعی، کنترل مرزها
- **دادگاهی:** از قبیل شناسایی جسد، شناسایی قاتل، شناسایی تروریست، تعیین والدین کودکان گمشده

۲-۳- سیستم های بیومتریک

یک سیستم بیومتریک اساساً یک سیستم شناسایی الگو میباشد که توسط کسب اطلاعات Biometric کار می کند. بسته به زمینه استفاده و کارکرد، یک سیستم بیومتریک می تواند هم در حالت تایید هویت و هم در حالت تشخیص هویت کار کند.

- در حالت تشخیص سیستم با جستجوی الگوی همه کاربران در پایگاه داده های خود، یک فرد خاص را تشخیص می دهد. تشخیص در واقع یک امر خطیر در کاربردهای تشخیص منفی می باشد. تشخیص منفی بدین معنی است که سیستم تشخیص می دهد که آیا فرد مورد نظر فردی حقیقی است یا خیر.
- در حالت تایید، سیستم هویت یک شخص را با مقایسه داده های بیومتریک اخذ شده و پایگاه داده های خود تأیید می کند. این نوع تحقیق و بازبینی هویت عموماً برای تشخیص مثبت به کار برده می شود. به این معنی که هدف سیستم جلوگیری از استفاده چندین کاربر از هویت یکسان می باشد.

۳- شبکه های عصبی در بیومتریک

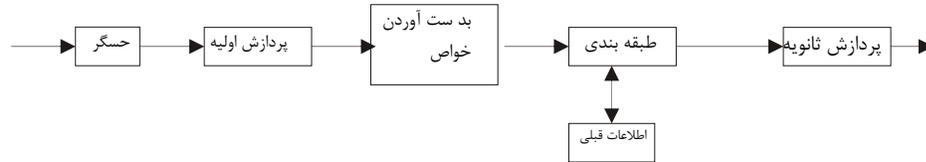
برای طراحی شبکه عصبی مورد نیاز لازم است که اطلاعات دقیق از ابعاد و ساختار آن داشته باشیم. تمامی شبکه های عصبی از هر نوع که باشند - اگر در بیومتریک مورد استفاده قرار گیرند - عمل تشخیص الگو را انجام می دهند.

۳-۱- Pattern Recognition

یک دسته الگو عبارتند از دسته ای از اشیاء که دارای چندین خاصیت و ویژگی اساسی و مجزا به صورت متداول می باشند که در نهایت می تواند یک اسم باشد. PR عبارتست از علم نامگذاری به اشیای طبیعی در جهان واقعی و یا در اصطلاح فنی: "فرآیندی که به موجب آن یک الگو یا یک سیگنال دریافت شده به یکی از کلاسهای از پیش تعریف شده ارجاع داده می شود."

۳-۲- طرح کلی یک سیستم تشخیص الگو

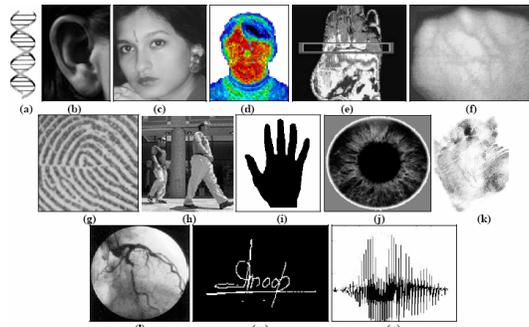
وظیفه اساسی یک سیستم که عمل تشخیص الگو را انجام می دهد، بدست آوردن اطلاعات مفید از شیئی سپس عمل کلاسبندی توسط یک مقایسه با برخی نتایج معلوم می باشد. در شکل(۱) مراحل مختلف تشخیص یک الگو نشان داده شده است: [2]



شکل(۱)- مراحل مختلف تشخیص الگو

۴- چند نوع مهم سیستمهای بیومتریکی و کاربرد شبکه های عصبی در آنها

هر سیستم بیومتریکی دارای قدرت و ضعف خاص خودش می باشد و انتخاب هر روش خاص بسته به کاربرد آن می باشد. از هیچ روش بیومتریکی به تنهایی انتظار نمی رود که به صورت کاملا موثر نیازهای یک کاربرد را برآورده سازد. به عبارت دیگر هیچ بیومتریکی بهینه نیست. در شکل(۲) تعدادی از روشهای مختلف بیومتریکی با کاربرد های مختلف مشاهده می شود:



شکل (۲): نمونه هایی از انواع بیومتریکی: (a) DNA (b) شکل گوش (c) چهره (d) گرمای صورت (e) گرمای دست (f) رگ دست (g) اثر انگشت (h) راه رفتن (i) هندسه دست (j) عنبیه (k) اثر کف دست (l) شبکه (m) امضاء (n) صوت [1]

در ادامه با معرفی چندین روش بیومتریکی شبکه های عصبی مورد استفاده شده در هر یک را نام برده و اطلاعات مورد نیاز در هر مورد برای استفاده در شبکه های عصبی را به طور اجمال مورد بررسی قرار خواهیم داد.

۴-۱- شناسایی اثر انگشت (FID)

تشخیص هویت از طریق اثر انگشت به دلیل دقت بالا متداول ترین و پر کاربرد ترین شکل شناسایی بر اساس تکنولوژی بیومتریکی می باشد در گذشته اثر انگشت توسط جوهر و فشار انگشت روی کاغذ ایجاد می شد ولی امروزه این عمل با تکنولوژی لیزر انجام پذیر گشته است.

به منظور استفاده از شبکه های عصبی در شناسایی اثر انگشت ابتدا تصویری که از اثر انگشت بدست آمده را به صورت یک ماتریس نمایش می دهند و با انجام اعمالی چون افزایش وضوح تصویر، اصلاح جهت تصویر، آن را به یک بردار از مختصات نقاط موجود در تصویر تبدیل کرده از این بردار به عنوان بردار ویژگی استفاده می شود. [7]

شبکه های عصبی که در این مورد استفاده شده اند عبارتند از: شبکه های [7]SOM, [9,10] MLP برای ایجاد داده مورد نیاز یک شبکه عصبی در این روش بایستی دانست که نقاط خاص و منحصر به فردی وجود دارند که مکان آنها برای اثر انگشت در هر فرد متفاوت است. بدین ترتیب مختصات این چند نقطه خاص را می توان به صورت یک داده ورودی برای هر شبکه عصبی مورد استفاده قرار داد.

این روش دارای نقایص جزئی نیز هست که می تواند برای تشخیص هویت خودکار نامناسب باشد. چون اثر انگشت میتواند تحت تأثیر عواملی چون: فاکتور های ژنتیک، سالخوردگی، دلایل محیطی و کار (از قبیل کارگر هایی که با دست کار می کنند و مقدار زیادی بریدگی و سوختگی در دستهای آن ها وجود دارد) قرار بگیرد.

۴-۲- هندسه دست (Hand Geometry)

این روش حتی قدیمی تر از اثر انگشت دیجیتالی است. این روش برای اولین بار بیش از ۲۰ سال پیش برای اهداف امنیتی در Wall street استفاده شد.

هندسه دست بر این حقیقت استوار است که دست هر فرد به طور بالقوه دارای شکلی متفاوت با دیگران است و این شکل (البته بعد از یک سن خاص) تغییر مهمی نمی کند.

در این روش وقتی که یک کاربر دست خود را روی دستگاه قرار می دهد یک تصویر سه بعدی از دست بدست می آید. سپس شکل و طول انگشت ها و بند انگشت ها در محل های مختلف اندازه گیری می شوند و به صورت تصویر در پایگاه داده ها ذخیره می گردند. این تصویر به صورت ماتریس تعریف شده و به عنوان بردار ویژگی در شبکه عصبی مورد استفاده قرار می گیرد.

از معایب این روش میتوان به عوامل زیر اشاره کرد:

- غیر قابل استفاده بودن در کودکان.
- افزایش احتمال خطا بدلیل استفاده از زیور آلات نظیر انگشتر، انگو.
- به علت بزرگ بودن دستگاه دست خوان غیر قابل استفاده بودن در دستگاههای کوچک نظیر Lap top ها در این مورد نیز خواص منحصر به فردی که می توانند بعد از تبدیل شدن به بردار عددی خاص به عنوان یک داده برای شبکه عصبی مورد استفاده قرار گیرند عبارتند: پهنای کف دست، درازای دست، درازای بند انگشت های خاص، کلفتی بند انگشت ها

۴-۳- اسکن چشم (Eye Scanning)

بیومتریک هایی که ویژگی های منحصر به فرد و پیچیده چشم را تجزیه و تحلیل می کنند به دو گروه تقسیم می شوند: سنجش عنبیه، سنجش شبکیه.

عنبیه عبارتست از یک باند از بافت رنگی که اطراف مردمک چشم را احاطه کرده است. یک سیستم شناسایی عنبیه از یک دوربین ویدیویی برای بدست آوردن نمونه ها استفاده می کند و از طرف دیگر یک نرم افزار که می تواند از الگوریتم یک شبکه عصبی خاص استفاده کرده باشد نتایج داده ها را با الگوهای ذخیره شده مقایسه می کند.

و اما شبکیه لایه ایست از مویرگها که در پشت چشم قرار دارند. اسکن شبکیه توسط یک نور مستقیم مادون قرمز و با شدت کم انجام می شود تا ویژگی های منحصر به فرد شبکیه بدست آید. در اسکن شبکیه یک ناحیه معروف به Face واقع در مرکز شبکیه وجود دارد که از آن الگوی منحصر به فرد ورید های خونی بدست می آید. تشخیص کاربر از طریق شبکیه در علم بیومتریک به عنوان بهترین روش مطرح شده است علی رغم دقت خوب این تکنیک بدلیل ضرورت ثابت ماندن فرد در حین اسکن و افتادن نور در چشم کاربر اغلب کاربران از آن ناراضی می باشند و کسب مقبولیت عمومی برای این تکنیک دشوار است.

از معایب اسکن چشم آن است که فرد بایستی در حین خواندن اطلاعات ساکن بایستد. در ضمن این روش در مورد کسانی که از لنز استفاده می کنند غیر قابل استفاده است.

در روش سنجش عنبیه نمونه مورد نظر می تواند رنگ و شکل خاص عنبیه باشد. با توجه به اینکه هر رنگی ترکیبی است از سه رنگ اصلی آبی، قرمز و سبز. با استفاده از رنگ عنبیه می توان برداری سه بعدی تولید کرد که عدد هر مؤلفه بردار، شدت هر یک از این سه رنگ را نشان می دهد.

در مورد شبکیه بزرگی و کوچکی مویرگ های روی شبکیه می توانند مورد بررسی قرار گیرند و به عنوان یک داده استفاده گردند.

شبکه های عصبی که بیشتر در این روش استفاده شده اند عبارتند از: HMM [12]، MLP [13]، RBF [14]

۴-۴- تشخیص چهره (Face Recognition)

سیستم های شناسایی چهره، یک فرد را توسط تجزیه و تحلیل شکل و ریخت منحصر به فرد صورت هر فرد را شناسایی می کنند. دو روش اساسی برای پردازش داده های بدست آمده از عمل تشخیص چهره وجود دارد: تجسم ویدیویی و تجسم حرارتی. تکنیک های استاندارد ویدیویی بر اساس تصویر صورت بدست آمده از یک دوربین ویدیویی می باشند. تکنیک های تصویر برداری گرمایی و حرارتی، الگوی گرما ساز رگهای خونی زیر پوست را تجزیه و تحلیل می کنند. جذابیت این سیستم در این است که قادر است بدون تماس فیزیکی کار کند. در هر حال این سیستم ها غیر قابل اعتماد و پرهزینه می باشند. برای مثال این سیستم قادر به تمییز دادن ذوقلو ها و کاربران بعد از عمل جراحی صورت نمی باشد. شبکه های عصبی مورد استفاده در این روش عبارتند از: HMM [13]، (Embedded HMM) EHHM [14]، MLP [15,16]، Bayesian MLP [15,16]، KNN [16]، ART [17]، RBF [18]

۴-۵- صدا و گفتار (Voice & Speech identification)

در این روش خصایص منحصر به فرد صدای افراد، فرکانس بین آواها، دیجیتالی شده و با نمونه های ذخیره شده در پایگاه داده ها، مقایسه می شود. این عمل با تشخیص گفتار متفاوت است، چون این تکنولوژی، کلمات فرد سخنگو را تشخیص نمی دهد بلکه یک سخنگو را با تجزیه و تحلیل ویژگی های گفتاری خاص، شناسایی می کند. تکنولوژی تشخیص سخنگو با صدا به فرد این امکان را می دهد تا به سرویس های محدود و منحصر به فردی از قبیل: راه یابی تلفنی به بانکها، پست ها ی صوتی و دستیابی به تجهیزات امنیتی راه یابد. اما تشخیص گفتار چگونه انجام می شود؟

در این روش ابتدا صدای کاربر ضبط و دیجیتالی شده و تعدادی آوا از گفتار فرد جمع آوری میشود. سپس این آوا ها با هم ترکیب و به یک یا چند کلمه خاص تبدیل می شوند نهایتا توسط یک نرم افزار که می تواند از انواع مختلفی از شبکه های عصبی باشد این کلمات را با کلمات از پیش ضبط شده قبلی مقایسه می نماید و هویت ادعا شده توسط کاربر تایید یا مردود اعلام می شود.

در این نوع از تشخیص کاربر از شبکه های عصبی مصنوعی HMM، MLP بیشتر استفاده شده است. [19,20,21,22,23] این روش با وجود راحتی، به دلیل امکان تقلید صدا قابل اطمینان نیست. یک فرد با صدای سرما خورده یا تازه از خواب بیدار شده نیز با این سیستم مشکل خواهد داشت.

۴-۶- تشخیص امضاء (Signature Recognition)

در این روش کاربر امضای خود را روی یک لوح گرافیکی دیجیتالی می کشد. مشخصه های پویای امضاء از قبیل سرعت، سرعت نسبی، ترتیب حرکات و فشار، مورد تجزیه و تحلیل قرار می گیرند. تشخیص امضاء به دو صورت انجام می شود: دینامیکی و استاتیکی.

کلید امضای دینامیکی تفاوت بین قسمت هایی از امضا است که همیشگی هستند و قسمت هایی که تقریبا با هر امضایی فرق می کنند می باشد.

همانطور که گفته شد در حالت دینامیکی کاربر امضای خود را روی یک لوح گرافیکی دیجیتالی می کشد. پویای امضاء از قبیل سرعت، سرعت نسبی، ترتیب حرکات و فشار، مورد تجزیه و تحلیل قرار می گیرند و در نهایت این خصوصیات جمع شده و در غالب یک بردار یا نوع دیگری از داده به ورودی شبکه عصبی استفاده شده اعمال می شود.

در روش دیگر که تأیید امضای استاتیکی است. ابتدا امضاء روی یک شیء خاص کشیده می شود و سپس شکل کلی آن به صورت یک ماتریس مورد بررسی قرار می گیرد که تعداد درایه های این ماتریس برابر پیکسل های هر شکل امضاء می باشد که البته از قبل این اندازه به صورت پیش فرض تعیین شده است. [30]

۴-۷- پویایی شناسی حرکت یک کلید روی صفحه کلید رایانه (Key Stroke)

یک سیستم تایپ بیومتریک عبارتست از سیستم Password یا شماره PIN با یک بعد اضافی دینامیک فشار کلید ها. در این سیستم یک کاربر نه تنها باید کلمه رمز را بداند بلکه او بایستی قادر باشد که سرعت تایپ و فواصل زمانی بین هر فشار کلید را بداند تا به اطلاعات دسترسی پیدا کند.

بنا بر این حتی اگر کسی کلمه رمز را بداند وی قادر نخواهد بود بدون داشتن ریتم تایپ مناسب به سیستم راه یابد. بیومتریک تایپ که بر اساس تاخیر زمانی بین هر فشار کلید می باشد یکی از اقتصادی ترین بیومتریک هایی است که می تواند بدون کوچکترین کشف رمز اجرا شود و معمولا نیاز به سخت افزار اضافی هم ندارند. علاوه بر آن تشخیص هویت بر پایه ریتم تایپ قابل تقلید نمی باشد.

در این مورد برای ایجاد یک داده ورودی برای شبکه عصبی می توان از مواردی چون: کلمه تایپ شده، فاصله زمانی بین فشار هر کلید، سرعت نسبی و کلی تایپ کلمه عبور استفاده کرد.

شبکه هایی که در این روش مورد استفاده قرار گرفته اند عبارتند از: [24]KNN، [25]MLP، [26]LVQ

۴-۸- DNA

چون ساختار DNA در هر فرد منحصر به فرد است تجزیه آن یک راه بسیار دقیق برای اثبات هویت می باشد. به دلیل نیاز به تکنولوژی پیشرفته و آزمایشات پر هزینه این روش زیاد به صرفه نیست ولی هرگاه تشخیص قطعی مورد نیاز باشد این روش مطمئن ترین روش می باشد.

و اما شبکه هایی نظیر [5]LVQ و [6]Time delay در این نوع از بیومتریک استفاده شده اند.

۴-۹- تشخیص هویت با رادیوگرافی دندان (Dental Biometrics)

بر خلاف سایر روش های بیومتریک تشخیص هویت از طریق دندان بسیار پیچیده است. زیرا دندان ها با گذشت زمان تغییر می کند. یک دندان می تواند در اثر یک عمل جراحی یا تصادف از دست برود. به همین دلیل در مجامع قانونی این روش تشخیص هویت کمتر قابل قبول است ولی در برخی موارد (مثل قتل در یک آتش سوزی) تنها وسیله تشخیص هویت همین روش می تواند باشد.

در این روش از بیومتریک عکس های رادیولوژی که از دندان افراد مختلف گرفته می شود به عنوان اطلاعات اولیه پایگاه داده ها مورد استفاده قرار می گیرد. سپس پس از مرگ یک فرد به طوری که نشود او را از طرق دیگر تشخیص داد از دندان های او عکس گرفته و با داده های قبلی تطابق داده می شود تا هویت فرد مورد نظر تعیین شود. [3,4].

۴-۱۰- ترکیب چند روش بیومتریک (Fusion) یا Multimodal Biometrics

سیستم های تایید کاربر که از یک روش بیومتریک استفاده می کنند اغلب مجبورند که با داده های نوین دار و درجات خطای نامحدود مواجه شوند. به منظور بهبود اجرای تطابق های ویژه در چنین وضعیت هایی سیستم های بیومتریک ترکیبی مورد استفاده قرار می گیرند.

لازم به ذکر است که سطح تلفیق روش های بیومتریک خود سه دسته اند:

- **تلفیق در سطح به دست آوردن اطلاعات:** چندین بردار ویژگی از روش های بیومتریک مختلف استخراج شده و سپس به روش های مختلف با هم ترکیب می شوند
- **تلفیق در سطح حوزه تطابق:** هر تطبیق بیومتریک یک درجه شباهت (Similarity score) ایجاد می کند که نشان دهنده نزدیکی بردار ویژگی ورودی با بردار الگو (Template vector) است که حوزه تطابق نام دارد. در این سطح از تلفیق این حوزه ها می توانند با هم ترکیب شوند و در شناساندن کاربر به ما کمک کنند.
- **تلفیق در سطح تصمیم گیری:** در این حالت هر بیومتریک بر اساس اطلاعات و تکنیک های خود عمل تشخیص را انجام می دهد سپس بر اساس رای گیری عمل تشخیص نهایی انجام می شود. [1]

شبکه های عصبی مصنوعی مورد استفاده در این مورد در واقع تمامی شبکه هایی اند که در روش های قبل مورد استفاده قرار گرفته اند. در واقع در این جا نیز می توان از ترکیبی از چند شبکه عصبی مصنوعی استفاده کرد.

۵- نتیجه:

در این مقاله با چند نوع پرکاربرد از روش های بیومتریک آشنا شدیم و شبکه های عصبی استفاده شده در آنها را نام بردیم. در جدول (۱) ویژگی های این روش ها جمع آوری شده و شبکه های عصبی متداول استفاده شده در آنها نام برده شده است.

شبکه عصبی رایج مورد استفاده	درجه خطا	مقبولیت	قابلیت اجرا	قابلیت جمع آوری اطلاعات	دوام	درجه تشخیص	عمومیت	
TDNN,LVQ	L	L	H	L	H	H	H	DNA
MLP	M	H	M	M	H	M	M	Ear
MLP,RBF	H	H	L	H	M	L	H	Face
HMM	L	H	M	H	L	H	H	Facial thermo gram
MLP,SOM	M	M	H	M	H	H	M	Fingerprint
MLP	M	H	L	H	L	L	M	Gait
RBF	M	M	M	H	M	M	M	Hand geometry
MLP	L	M	M	M	M	M	M	Hand vein
MLP,RBF,HMM	L	L	H	M	H	H	H	Iris
LVQ,MLP,KNN	M	M	L	M	L	L	L	Keystroke
MLP,KOHONEN	L	M	L	L	H	H	H	Odor
MLP,	M	M	H	M	H	H	M	Palmprint
MLP,RBF,HMM	L	L	H	L	M	H	H	Retina
MLP,RBF	H	H	L	H	L	L	L	Signature
MLP,HMM	H	H	L	M	L	L	M	Voice

جدول (۱) مقایسه تکنیک های بیومتریک H . معادل درصد بالا، M معادل متوسط و L معادل در صد پایین از هر یک از قابلیت های ذکر شده است. [1]

همانگونه که مشاهده می شود شبکه های عصبی پرسپترون چند لایه (MLP) را بی شک می توان مهمترین ابزار مورد استفاده در مسایل تشخیص نمونه ها دانست. البته لازم به ذکر است که استفاده از شبکه های عصبی در همه موارد مفید نبوده و باعث بهبود عملکرد سیستم و یا افزایش سرعت و دقت آن نمی شود و ممکن است که روشهای کلاسیک عملکرد بهتری از خود نشان دهند.

۶- مراجع:

- [1] Anil K. Jain, Arun Ross and Salil Prabhakar: An Introduction to Biometric Recognition, *IEEE Transactions on Circuits and Systems for Video Technology, Special Issue on Image- and Video-Based, Biometrics*, Vol. 14, No. 1, January 2004.
- [2] Vakil.M.T: Farsi Character Recognition using artificial neural networks, Ph. D Thesis, faculty of electrical engineering, university of Ljubljana, October 2002
- [3] Anil K. Jain, Hong Chen: Matching of dental X-ray images for human identification. department of computer science & Engineering, Michigan State University, 3115 Engineering Building, East Lansing MI 48824, USA. *Pattern Recognition* 37 (2004) 1519 – 1532
- [4] Gamal Fahmy, Diaa Eldin M. Nassar, Eyad Haj-Said, Hong Chen, Omima Nomir, Jindan Zhou, Robert Howell, Hany H. Ammar, Mohamed Abdel-Mottaleb and Anil K. Jain: Automated Dental Identification System (ADIS), West Virginia university, Michigan State University, University of Miami
- [5] Vladimir B. Bajic", Suisheng Tang', Hao Han' and Vladimir Brusic ':Artificial Neural Networks Based Systems for Recognition of Genomic Signals and Regions: A Review, *Informatica* 26 (2002) 389-400 389
- [6] Martin G. Reese: Application of a time-delay neural network to promoter annotation in the Drosophila melanogaster genome, Berkeley Drosophila Genome Project, Department of Molecular and Cell Biology, University of California, Berkeley, *Computers and Chemistry* 26 (2001) 51–56

- [7] Raffaele Cappelli, Alessandra Lumini, Dario Maio, Member, IEEE, and Davide Maltoni: Fingerprint Classification by Directional Image Partitioning, IEEE TRANSACTIONS ON PATTERN ANALYSIS AND MACHINE INTELLIGENCE, VOL. 21, NO. 5, MAY 1999
- [8] J. D. Bowen, "The Home Office Automatic Fingerprint Pattern Classification Project," Proc. IEE Colloquium Neural Network for Image Processing Applications, 1992.
- [9] P. A. Hughes and A. D. P. Green, "The Use of Neural Network for Fingerprint Classification," Proc. Second Int'l Conf. Neural Network, pp. 79-81, 1991.
- [10] M. Kamijo, "Classifying Fingerprint Images Using Neural Network: Deriving the Classification State," Proc. Third Int'l Conf. Neural Network, pp. 1,932-1,937, 1993.
- [11] K. Moscinska and G. Tyma, "Neural Network Based Fingerprint Classification," Proc. Third Int'l Conf. Neural Network, pp. 229-232, 1993.
- [12] Waleed Fakhr: HMM- BASED MULTI-MODAL BIOMETRIC AUTHENTICATION SYSTEM WITH NEURAL NETWORK FUSION, Arab Academy for Science and Technology, Cairo – Egypt
- [13] Yunhong Wang, Tieniu Tan, Anil K. Jain: Combining Face and Iris Biometrics for Identity Verification, Center for Biometrics Authentication and Testing, National Laboratory of Pattern Recognition, Institute of Automation, Chinese Academy of Sciences, Department of Computer Science & Engineering, Michigan State University East Lansing
- [14] Yunhong Wang, Tieniu Tan, and Anil K. Jain: Combining Face and Iris Biometrics for Identity Verification, National Lab of Pattern Recognition, Institute of Automation, Chinese Academy of Sciences, Department of Computer Sciences Engineering, Michigan State University East Lansing,
- [15] Dmitry Bryliuk, Valery Starovoitov, : ACCESS CONTROL BY FACE RECOGNITION USING NEURAL NETWORKS AND NEGATIVE EXAMPLES, Institute of Engineering Cybernetics, Laboratory of Image Processing and Recognition, Surganov str. , 6, 220012 Minsk, BELARUS, The 2nd International Conference on Artificial Intelligence, September 16-20, 2002, Crimea, Ukraine, pp. 428-436
- [16] Aki Vehtari and Jouko Lampinen: Bayesian MLP Neural Networks for Image Analysis, Laboratory of Computational Engineering, Helsinki University of Technology, P. O. Box 9400, FIN-02015, HUT, Finland, 14th September 2000
- [17] Zahid raiaz, Arif Gilgiti, Sikander M. Mirza: "Face recognition: A review and comparison of HMM, PCA, ICA, AND neural networks", 0-7803-8655- 8/04/2004IEEE.
- [18] Harkirat S. Sahambi and K. Khorasani, Member, IEEE: A Neural-Network Appearance-Based 3-D Object Recognition Using Independent Component Analysis, IEEE TRANSACTIONS ON NEURAL NETWORKS, VOL. 14, NO. 1, JANUARY 2003
- [19] Trent W. Lewis David M. W. Powers: Audio-Visual Speech Recognition using Red Exclusion and Neural Networks, School of Informatics and Engineering Flinders University of South Australia, South Australia 5001, Journal of Research and Practice in Information Technology, Vol. 35, No. 1, February 2003
- [20] Roberto GEMELLO, Dario ALBESANO, Franco MANA, Loreta MOISA: Multi-Source Neural Networks for Speech Recognition: a Review of Recent Results, CSELT - Centro Studi e Laboratori Telecomunicazioni, 0-7695-0619-4/0, 2000 IEEE
- [21] Hesham Tolba & Douglas O'Shaughnessy: Speech Recognition by Intelligent Machines, IEEE Canadian Review - Summer /2001
- [22] Asterios Toutios, Konstantinos Margaritis: ACOUSTIC-TO-ARTICULATORY INVERSION OF SPEECH: A REVIEW, Parallel and Distributed Processing Laboratory, Department of Applied Informatics, University of Macedonia
- [23] Nalini Vasudevan: A Connectionist Framework For Feature Based Speech Recognition System Using Artificial Neural Networks. R. V. College of Engineering, Computer Science & Engineering, Bangalore
- [24] Fahil Wong Mohd Hasan Wong, Ainil Surfreena Mohd Supian, Ahmad Faris Ismail: "Enhanced user authentication through typing Biometrics with artificial neural networks and K-Nearest neighbor algorithm", 078703-7147-x/01/2001 IEEE
- [25] Fabian Monrose: Keystroke Dynamics as a Biometric for Authentication. Courant Institute of Mathematical Sciences, New York University, New York, NY. , Elsevier Preprint 1 March 1999
- [26] Fabian Monrose, Aviel Rubin: Authentication via Keystroke Dynamics. New York University, Bell Communications Research
- [27] [http://. www. Com p_ai_neural-nets FAQ, Part 1 of 7 Introduction. htm](http://www.com_p_ai_neural-nets_FAQ_Part_1_of_7_Introduction.htm)
- [28] conference 2002 [http://. www. E_court . com](http://www.E_court.com)
- [29] رضا آقایی، حسین نظام آبادی، و احسان ا. . . کبیر. آشکار سازی چهره با شبکه های عصبی و دهمین کنفرانس 10th ICEE MAY 2002. VOL 1
- [30] وحید سلوک، علی آقا گلزاده محمد رضا آشوری، تایید استاتیک امضا های ایرانی توسط شبکه های عصبی MLP 10th Icee may 2002, vol 1
- [31] N. Papamarklos and HBaltzakis. : " Off line Signature verification using multiple NN classification structure". 13th international conference on pattern recognition 1997