"روشی نوین جهت تشخیص هویت بمنظور کنترل تردد با استفاده از ترکیب دو روش RFID و بیومتریک"

نویسنده: طلایه قدسی زاد، دانشجوی دکتری مهندسی پزشکی (بیوالکتریک)، از کارشناسان ارشد شرکت مهندسین مشاور گروه ۴

چکیده:

مدیریت امنیت در سازمان‌های مختلف متفاوت است. هنگامیکه در مورد مکان‌هایی که نیاز به حفاظت و کنترل دسترسی دارند صحبت می‌شود، معمولا در ذهن عموم مردم، بیمارستان‌ها در اولویت قرار نمی‌گیرند و مراکز مالی، شرکت‌های امنیتی، ساختمان‌های دولتی و مکان‌های مشابه به ذهن می‌آیند، این درحالیست که بیمارستان‌ها در مقابل مسائل امنیتی بسیار آسیب پذیر هستند و امنیت یکی از اصلی‌ترین سرویس‌های پشتیبانی برای ایجاد یک محیط درمانی ایمن است. اهمیت این موضوع ممکن است در بیمارستان های کوچک کمتر حائز اهمیت باشد درصورتیکه در بیمارستان‌های بزرگ، کنترل دسترسی از جمله موارد امنیتی بسیار حیاتی بشمار می‌رود.

سیستم‌های کنترل دسترسی در تمامی حرفه‌ها برای حفاظت از افراد و امکانات ضروری است. برخلاف سیستم‌های دسترسی در دیگر سازمان‌ها، سیستم‌های کنترل دسترسی بیمارستان‌ها منحصر به فرد هستند زیرا باید قادر به محدود کردن دسترسی به مناطق حساس، جلوگیری از گسترش بیماری، ردیابی و جلوگیری از سرقت تجهیزات و داروهای حیاتی و حفاظت از هر دو نوع از کارکنان و بیماران باشد. بنابراین، در انتخاب نوع سیستم کنترل دسترسی بیمارستان و ویژگی‌های خاص آن باید به این نگرانی‌های امنیتی توجه شود.

RFID یکی از رایج‌ترین سیستم‌های کنترل دسترسی است. با این حال، فناوری RFID فعلی، هویت دارنده کارت RFID (یا برچسب) را شناسایی نمی‌کند در نتیجه، هر فرد غیر مجازی که یک کارت RFID مجاز بهمراه داشته باشد می‌تواند به منطقه امن دسترسی پیدا کند. در نتیجه، تکنیک‌های محاسباتی هوشمند برای جبران این خلا بکار گرفته می‌شوند. برای مقابله با این مشکل، شناسایی بیومتریک برای کار با RFID برای کنترل دسترسی پیشنهاد شده است. شناسایی اثر انگشت، شناسایی کف دست، شناسایی قرنیه، شناسایی صدا، برخی از روش‌های شناسایی بیومتریک هستند. اثر انگشت و اثر کف دست با تغییری در پوست دست شخص بشدت تحت تاثیر قرار می‌گیرند. صدای افراد نیز ممکن است توسط افراد غیر مجاز تقلید یا حتی ضبط شود. این درحالیست که صورت و چهره منحصر به فرد هستند و در مقایسه با سایر روش‌های بیومتریک امکان به سرقت رفتن و تقلید آن تقریبا غیر ممکن می‌باشد.

با توجه به موارد ذکر شده در مورد سیستم‌های معمول RFID، یک سیستم کنترل دسترسی که ترکیبی از فناوری RFID و شناسایی چهره بر اساس شبکه عصبی است در این مقاله ارائه شده است. این سیستم چهره فردی که کارت RFID در اختیار دارد را شناسایی می‌کند و در صورت تناقض اطلاعات این دو، دسترسی را غیرممکن می‌کند. در این سیستم، یک شبکه عصبی پایه شعاعی (RBFNN) برای یادگیری چهره صاحبان مجاز کارت بهمراه مدل خطای تعمیم محلی (L-GEM) برای آموزش RBFNN به کار می‌رود که داده‌های آموزش شبکه عصبی Eigenface های بدست آمده از الگوریتم PCA هستند و بمنظور صرفه جویی در حافظه سیستم زمانی که تعداد دارندگان کارت‌ها زیاد می‌شود، فقط پارامترهای RBFNN ذخیره می-شوند.

مقدمه:

سازمان‌هایی با امکانات بهداشتی–درمانی مثل بیمارستان‌ها بصورت ۲۴ ساعت در روز و ۷ روز در هفته باز هستند. در نتیجه، صدها مراجعه کننده از قشرهای مختلف جامعه در یک روز در بیمارستان رفت و آمد می‌کنند. بخش های امنیت و حفاظت بیمارستان همیشه درصدد این بوده‌اند که یک محیط ایمن برای کارکنان، بیماران و ملاقات کنندگان ایجاد کنند و این امر باید با ماهیت در دسترس بودن بیمارستان برای عموم مردم در تعامل باشد [۱].

سیستم‌های کنترل دسترسی امکان کنترل، مانیتور و محدود کردن حرکت افراد، تجهیزات، اسناد و وسایل نقلیه داخل خارج و اطراف ساختمان یا محوطه را فراهم می‌کنند [۲].

برای اینکه تسهیلات خاص، بعنوان مثال بیمارستان‌ها، از سوی استانداردهای کمیته مشترک[1] (TJC) تایید شوند، نیاز به آشنایی با استانداردهای اعتباربخشی آنها برای مراقبت از بیمار، فرد و ساکنین وجود دارد. تعدادی از این استانداردها بر محدود کردن امکانات در مراکز مراقبت بهداشتی تاکید دارند. همچنین TJC دارای شامل استانداردهای دیگری نیز است که امکانات و کارمندان امنیتی باید آنها را درنظر بگیرند. این استانداردها به سه دسته استانداردهای شناخته شده (Known standards)، استانداردهای ناشناخته های شناخته شده (Known Unknowns)، و استانداردهای ناشناخته/ناشناخته (Unknown Unknowns) تقسیم می‌شوند.

در میان استانداردهای شناخته شده، استاندارد محیط مراقبت است که یک بیمارستان باید برنامه‌های لازم برای مدیریت امنیت هر فرد در این مرکز داشته باشد. این برنامه ها باید سالانه بررسی و به روز شوند. Warren یادآور می شود که بسیاری از ناشناخته های شناخته شده "از قوانین مربوط به امنیت و ایمنی هستند که با هم روبرو هستند که با حوزه امنیت و ایمنی عمومی همپوشانی دارند مانند مدیریت بحران. یک نمونه از استاندارد ناشناخته بخش منابع انسانی است که "بیمارستان توانایی های مورد نیاز کارکنان خود که مراقبت های بیمار، درمان یا خدمات را تامین می کنند را با استفاده از روش های ارزیابی برای تعیین شایستگی فرد در مهارت های مورد نظر بررسی میکند و صلاحیت یک فرد با زمینه تحصیلی، تجربه یا دانش مربوط به مهارت هایی که مورد نظر است، را ارزیابی می کنند

امنیت لایه ای[2]، یک اصل پیشگیری کننده جرم از طریق طراحی محیطی[3] (CPTED) است و به عنوان لایه های متمرکز اقدامات امنیتی تعریف می شود که از دارایی های ارزشمند پشت چندین مانع محافظت می کند. کارکرد این سیستم از محیط بیرونی شروع شده و بسمت داخل حرکت می کند و در هر یک از لایه های امنیتی طراحی بگونه ایست که تا زمانی که ممکن است زمان را برای نفوذ و ورود جعلی طولانی کند.

انجمن بین المللی امنیت و ایمنی بهداشت و درمان[4] (IAHSS)، ۵ سطح ایمنی را بصورت زیر تعریف می‌کند:

[1] The Joint Commission
[2] Layered security
[3] Crime prevention through environmental design
[4] The International Association of Healthcare Security and Safety's

- محوطه اموال
- محوطه ساختمان
- داخل ساختمان- جدا کردن بازدید کنندگان مجاز و غیر مجاز
- داخل ساختمان- جدا کردن مناطق عمومی و بیماران از مناطق مختص کارکنان
- داخل ساختمان- محدود کردن بیشتر دسترسی کارمندان به مناطق بسیار حساس

- محوطه اموال:

داشتن یک سایت که برای عموم مردم در دسترس است، چالش هایی را برای کارمندان امنیتی ایجاد می کند. نشانه های سایت یک روش ساده و ارزان برای هدایت بازدیدکنندگان به مناطق مختلف سایت برای تخلیه بیمار، پارکینگ بازدید کننده و دسترسی به بخش اورژانس (ED) می باشد. علاوه بر این، بازدیدکنندگان هنگام ورود به پارکینگ یک بلیط می گیرند، حتی اگر مجبور به پرداخت وجه نباشند، یک منطقه نیمه خصوصی را در نظر عموم ایجاد می‌کند. مجرمان احتمالی ممکن است از ورود به نواحی نیمه خصوصی بنسبت مناطق دیگر که به نظر کمتر ایمن هستند (مکان‌های عمومی) امتناع کنند.

در حالی که دستگاه های امنیتی الکترونیکی یک سایت یا تسهیلات را امن تر نمی کنند، آنها می توانند یک نیروی ضربتی برای تیم امنیتی باشند، به این معنی که یک منطقه بزرگ تر می تواند نظارت شود و کارهای امنیتی بیشتری با کارکنان کمتری انجام شود. یک مثال اصلی از این سیستم، استفاده از تکنولوژی نظارت تصویری است. با استفاده از این سیستم، در یک سایت که برای عموم مردم در دسترس است، اینکه چه کسی دسترسی به آن را دارد حائز اهمیت است و به پرسنل امنیتی قبل از رسیدن خطر به محیط ساختمان هشدار می دهد. مکان های نصب دوربین باید به تیم امنیتی یک دید کلی از سایت ارائه دهد در حالی که بتواند برچسب نصب شده مجوز تردد خودرو ها را شناسایی کند.

- محوطه ساختمان:

محوطه ساختمان اولین خط دفاع است که هدف آن ورود عموم مردم و کارکنان به نقاط موردنظرشان است. تمامی درهای بیرونی به غیر از ورودی های عمومی اصلی باید شامل کنترل دسترسی و در تمامی لحظات نظارت بر آنها بطور کامل انجام شود. درهایی که فقط برای خروج درنظر گرفته شده اند نباید سخت افزار بیرونی داشته باشند و تمام درهای اطراف باید تحت نظارت قرار بگیرند، بنابراین درب ها برای اجازه دسترسی غیر مجاز باز نخواهند شد.

- داخل ساختمان- جدا کردن بازدید کنندگان مجاز و غیر مجاز

مناطق پر خطرتر، مانند مناطق درمان اورژانس، بخش های مراقبت ویژه، واحدهای اطفال و نوزادان، باید مجهز به سیستم کنترل دسترسی باشند. اگر چه علامت هایی مانند "تنها مجوز کارکنان" در حفظ دسترسی عمومی به مناطق کنترل شده یا دسترسی محدود بسیار موثر است، اما مانع نفوذ مزاحمان نخواهد شد. داشتن کارت و نشان کنترل دسترسی فعال معتبر برای بازدیدکنندگان یک رویکرد جدی است که محبوبیت فراوانی در مسائل امنیتی به دست آورده است. به عنوان مثال، کارکنان

امنیتی می توانند برای پدر نوزاد یک تگ کنترل دسترسی صادر کنند که به وی اجازه داده شود فقط در مناطق زایمان تردد کند.

- داخل ساختمان- جدا کردن مناطق عمومی و بیماران از مناطق مختص کارکنان

لایه چهارم کنترل دسترسی باید مناطق عمومی و مناطق بستری بیماران را از مناطق "فقط کارکنان"، از جمله دفاتر پرستاری، اتاق های قفل کارکنان، مکان های ذخیره سازی و توزیع، راهروهای استریل و آزمایشگاه های تحقیقاتی، جدا کند.

- داخل ساختمان- محدود کردن بیشتر دسترسی کارمندان به مناطق بسیار حساس

لایه نهایی حفاظت به معنای محدود کردن دسترسی کارکنان به مناطق بسیار حساس است - مواردی که به طور خاص به کارکنان مجاز خدمات بهداشتی محدود می شود که شامل داروخانه و فضای ذخیره سازی مواد مخدر، مواد خطرناک، زیر ساخت فناوری اطلاعات (IT) و مناطق دربرگیرنده اطلاعات شخصی بیماران است. قانون پاسخگویی و مسئولیت بیمه سلامت[1] (HIPAA) دارای مقرراتی در خصوص حفظ حریم اطلاعات شخصی است. در نتیجه، دسترسی به سوابق فیزیکی یا سوابق الکترونیکی بیماران باید کنترل شود.

بطور کلی سیستم‌های کنترل دسترسی شامل ۳ جزء هستند:

۱- موانع فیزیکی

- درب‌ها: حفاظت شده با قفل‌های مغناطیسی یا الکتریکی
- گیت‌ها: برای محدود کردن عبور یک فرد به ازای یک کارت
- موانع برای وسایل نقلیه: برای محدود کردن دسترسی وسایل نقلیه به دارندگان مجوز عبور

۲- سیستم های تشخیص هویت

تعداد زیادی از تکنولوژی‌های متفاوت برای شناسایی کاربران در سیستم‌های کنترل دسترسی وجود دارد که شامل:

- کارت خوان‌های RFID با قابلیت شناسایی در فواصل نزدیک یا دور
- کارت خوان‌های هوشمند
- صفحه کلید
- سیستم‌های بیومتریک

۳- نرم افزار کنترل کننده درب فضاها

[1] Health Insurance Portability and Accountability Act

نرم افزارهای کنترل کننده درب قلب سیستم هستند و برای تصمیم‌گیری اینکه چه کسی در چه محلی و در چه زمانی اجازه تردد دارد استفاده می‌شوند که این تصمیم‌گیری وابسته به سایز سیستم و تعداد قرائت کنندگان (readers) یا محوطه‌های نیازمند کنترل از یک نقطه خاص تغییر می‌کند. برخی گزینه‌های موجود بصورت زیر است:

- کنترل کننده مستقل نصب شده روی یک درب و بدون نرم افزار
- مجموعه تعدادی کنترل کننده درب مستقل و لینک شده به یک کامپیوتر برای کنترل یک محوطه
- لینک شدن تعدادی محوطه کنترل شده برای بوجود آوردن یک شبکه وسیع

حفاظت ۲۴ ساعته در بیمارستان‌ها از مهمترین موضوعات چالش برانگیز در بیمارستان‌ها است [۳]. از جمله ویژگی‌های استفاده از سیستم‌های کنترل دسترسی در بیمارستان‌ها می‌توان به موارد زیر اشاره کرد که هدف اصلی مقاله در ارتباط با ارائه راهکاری جدید جهت کنترل دسترسی پرسنل بیمارستان است:

۱- ایمنی و امکان کنترل بیماران

هنگامیکه بیماران به بخش پذیرش بیمارستان مراجعه می‌کنند، برای هر بیمار یک کد شناسایی یا Identification Card صادر می شود که برای وی منحصر به فرد است. این کد شناسایی حاوی اطلاعات بیمار، سابقه بیماری وی، پزشک معالج، بخش بستری تعیین شده و ... است. این ID بصورت ذخیره شده در یک تگ یا دستبند که دارای یک IC جهت ذخیره اطلاعات است در اختیار بیمار قرار می‌گیرد. بدین ترتیب با حرکت بیمار در هرلحظه امکان ردیابی وی وجود خواهد داشت. یکی دیگر ار ویژگی‌های کاربرد این سیستم برای بیماران، محافظت از نوزادان در برابر ربوده شدن است که متاسفانه از گذشته تا به امروز موارد بسیار از ربوده شدن نوزاد در بیمارستان گزارش شده است. با توجه به مچ بندهای RFID بر روی دستهای نوزادان، به محض خارج شدن آنها از فضای خود، درب های تعریف شده بسته شده و دوربین های آن فضا شروع به تصویربرداری خواهند کرد و از دزدی نوزادان جلوگیری خواهد شد.

۲- مانیتورینگ ملاقات کنندگان

در یک محیط با تعداد زیادی از بیماران و ملاقات کنندگان زودگذر، استفاده از کامپیوتر و شبکه‌های کامپیوتری باید در نظر گرفته شوند. بدین منظور می‌توان از سیستم Self sign-in استفاده کرد. این سیستم‌ها می‌توانند ID ای بصورت یک عکس پرینت کنند و اجازه دسترسی به محدوده‌های مجاز برای آنها را صادر کنند. استفاده از سیستم نرم افزاری ملاقات کنندگان راهی آسان برای حفاظت است. ملاقات کنندگانی که از قبل (یا در محل بیمارستان) در سیستم ثبت نام و اطلاعات مورد نظر را ثبت کرده اند، با استفاده از کیوسک‌های موجود در بیمارستان می‌توانند اطلاعات خود را ویرایش کنند و بطور اتوماتیک یک نشان و ID پرینت شده از دستگاه دریافت کنند که بوسیله آن شخص می‌تواند در محل‌ها و زمان‌های خاصی که در اطلاعت ثبت شده تعیین می‌شود تردد کند.

شکل ۱: سیستم کنترل دسترسی ملاقات کنندگان

۳- کنترل آسانسورها

با توجه به وجود طبقات مختلف در ساختمان و فضاهایی ماند اتاق های عمل، بخش‌های بستری بیماران، بخش‌های مراقبت‌های ویژه و ... این مسئله بسیار حائز اهمیت است که پزشکان، پرسنل و مراجعه کنندگان فقط در زمان‌های خاص و طبقات مجاز دسترسی داشته باشند. توسط این سیستم می‌توان بگونه‌ای برنامه ریزی نمود که طبقات عمومی برای کلیه افراد فعاال باشند و برای طبقات خاص، در صورت مجاز بودن فرد برای تردد به آن طبقه، کلید مربوط به آن طبقه فعال شود.

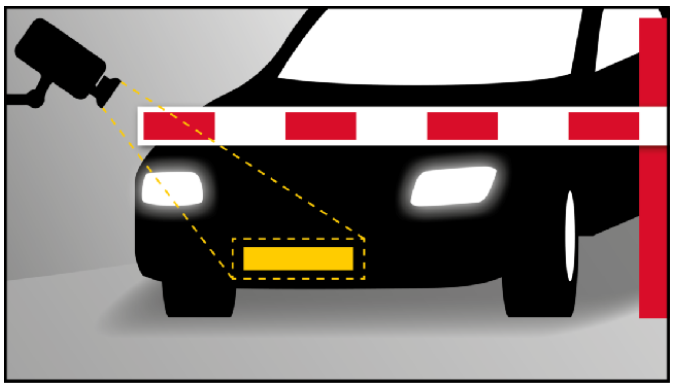
۴- کنترل درب پله های فرار

پله‌های فرار در ساختمان‌های بلند مرتبه و همچنین بیمارستان‌های بزرگ بمنظور خروج افراد در زمان‌های بحران از داخل به خارج ساختمان درنظر گرفته می‌شود. اما این پله‌ها می‌توانند بعنوان راهی جهت تردد افراد غیر مجاز به محل‌های خاص باشند. بدین منظر کنترل آنها بعنوان دروازه ورود به بخش‌ها از نکات کلیدی کنترل دسترسی است. این درب‌ها باید همیشه در جهت مسیر فرار باز شوند (از داخل بخش به راه پله) و در مقابل برای حرکت در جهت مخالف از راهرو به طبقات کنترل دسترسی بکمک سیستم RFID درنظر گرفته شود.

۵- ارتباط با سیستم تشخیص پلاک (ANPR[1])

برای بیمارستان‌ها که حجم زیادی از پرسنل، بیماران و ملاقات کنندگان که با خودرو وارد می‌شوند و در محوطه پارک می-کنند، ANPR گزینه مناسبی است. برای مانیتور کردن ورود وسایل نقلیه به محوطه، دوربین‌های CCTV و نرم افزار کامپیوتری برای شناسایی پلاک اتومبیل‌ها استفاده می‌شود. برخی سیستم‌ها همچنین می‌توانند تصاویر راننده و خودرو را برای بررسی‌های احتمالی در آینده ذخیره کنند. این نرم افزار پیچیده، اطلاعات مهم و کلیدی را چهت ارسال به پلیس برای کمک به پیدا کردن مجرمین ارسال می‌کند.

[1] Automatic Number Plate Recognition



شکل ۲: سیستم تشخیص پلاک

۶- امکان کنترل موجودی و جابجایی داروها و تجهیزات

با توجه به حجم انبوهی از داروها و تجهیزات گران قیمت که در بیمارستان وجود دارد، می توان برای برخی یا همه آنها یک برچسب ID درنظر گرفت. بدین ترتیب می‌توان موقعیت هریک از آن‌ها را تعیین نمود. بعنوان مثال برای تجهیزات سیار و مشترک بین بخش‌ها، بعنوان مثال دستگاه رادیولوژی سیار، می‌توان با الحاق سیستم ID به آن، در مواقع اورژانس نزدیک‌ترین دستگاه رادیولوژی سیار را به بخش مورد نظر انتقال داد که این امر باعث صرفه‌جویی در زمان و نیروی پرسنل و کاهش مفقود شدن وسایل و تجهیزات بیمارستان می‌شود.

۷- ارتباط با سیستم های دیگر

بیمارستان‌های بزرگ که در بیش از یک طبقه و حتی در چند ساختمان طراح شده‌اند، نیازمند سیستم امنیتی یکپارچه شامل CCTV، سیستم اعلام حریق، BMS و ... هستند. یکی از راه‌های دستیابی به این هدف، استفاده از تکنولوژی IP است که امکان برقراری ارتباط این سیستم‌ها با یکدیگر برای افزایش بازده را فراهم می‌کند. سیستم کنترل دسترسی بهتر است بصورت شبکه ای مجزا از سایر شبکه های ذکر شده طراحی شود، این در حالیست که باید ارتباطی بین سیستم شبکه های بیمارستان با سیستم کنترل دسترسی نیز وجود داشته باشد. بعنوان مثال، با درنظرگیری ارتباط بین شبکه اعلام حریق و شبکه کنترل دسترسی، در مواقع اضطراری وقوع آتش، سیستم کنترل دسترسی بصورت Local و یا Global غیرفعال شود.

- ارتباط با سیستم اعلام حریق

این تکنولوژی در بیمارستان‌ها در زمان وقوع آتش بسیار حیاتی است و هنگام آتش بطور اتوماتیک گزارشی حاوی اطلاعات حیاتی در ارتباط با اینکه چه کسانی در کجای ساختمان هستند بدست می‌دهد. این نرم افزار بوسیله کارت‌های هوشمندی که برای کنترل دسترسی در اختیار افراد است کار می‌کند. در مواقع اضطراری، این سیستم افراد حاضر در ساختمان را مطلع می-کند و در عین حال گزارشی از موقعیت افراد در ساختمان نیز تهیه می‌کند.

- ارتباط با سیستم نضارت تصویری (CCTV)

در صورت مشاهده موارد خاص توسط دوربین ها، می توان درب‌های خاصی را بطور اتوماتیک باز یا بسته نمود.

۸- کنترل دسترسی پرسنل بیمارستان

افراد کلیدی بیمارستان شامل پزشکان، پرستاران و پرسنل خدمات هستند. تمامی کاربران بیمارستان دارای شرایط برابر نیستند. پرسنل کادر پزشکی، نظافت کنندگان، بیماران و ملاقات کنندگان آنها و همچنین کارکنان بیشمار موقت و قراردادی، همگی نیازمند دسترسی‌های متناسب با نیازهای متفاوتشان هستند. این سیستم‌ها به مدیران بیمارستان این امکان را می‌دهند تا برنامه حفاظتی را تغییر دهند و سرپرست حفاظت کنترل بیشتری در محوطه داشته باشد (از مانیتورینگ درب‌های داروخانه تا اجازه دسترسی و کار دادن به نظافت کنندگان فقط در محدوده و زمان تعیین شده برای آن‌ها)[۴].

بیمارستان‌ها فقط شامل کارکنان نیستند بلکه شامل بیماران و حجم زیادی از ملاقات کنندگان هستند که در آنجا رفت و آمد می‌کنند. علاوه بر جمعیت گذرا، بسیاری از تجهیزات پزشکی ، تجهیزات IT، داروها و حجم انبوهی از اسناد محرمانه و اطلاعات بیماران بیمارستان‌ها را به مکان‌های مستعد سرقت تبدیل کرده است. درنتیجه سیستم‌های کنترل دسترسی به جهت افزایش ایمنی و حفاظت در بیمارستان‌ها بطور چشمگیری در حال افزایش است تا اجازه دسترسی فقط به افراد با مسئولیت خاص داده شود.

هنگامیکه پرسنل دارای تگ RFID در محیط بیمارستان حرکت می‌کنند، در هر محوطه از تقسیم‌بندی، توسط ردیاب آن قسمت، تگ پرسنل شناسایی می‌شود. حضور و زمان حضور آن پرسنل در آن محوطه، به پنل مرکزی ارسال می‌شود. بنابراین با حرکت پرسنل دارای تگ از محوطه‌های مختلف، رشته‌ای از داده‌ها حاوی شماره شناسایی آن شخص و زمان حضور وی در هر محوطه به پنل مرکزی ارسال می‌شود در نتیجه از طریق پنل مرکزی می‌توان فهمید شخص مورد نظر دز هر لحظه و در زمان جاری در کدام محوطه بیمارستان است. بنابراین دسترسی به آن پرسنل راحت‌تر و سریع‌تر خواهد بود. همچنین برای یافتن پرسنل، نیازی به فراخواندن نام او در کل بخش‌ها و ایجاد مزاحمت صوتی نیست.

بطور کلی مزیای سیستم های هوشمند کنترل دسترسی را می توان بصورت زیر خلاصه کرد:

- امکان مدیریت سطوح دسترسی تمامی افراد(اعم از پرسنل بیمارستان، بیماران، مراجعه کنندگان و ...)
- مدیریت تمامی درب ها و فضاها
- مانیتورینگ تمامی رخدادها
- ارتباط با سیستم های دیگر(اعم از اعلام حریق، CCTV و ...)
- افزایش امنیت فضاها (افزایش امنیت اتاق های دارو، انبار تجهیزات، اتاق سرورها و ...)
- کاهش نیروی انسانی و هزینه ها(حذف نگهبان پارکینگ و ...)
- رضایتمندی بیماران (ایمنی بیشتر در مدت زمان اثامت در بیمارستان، صرفه جویی در زمان و ...)

مطالعه موردی بر اساس نمونه های بیمارستانی داخلی و خارجی که از هریک از سیستم های فوق بهره مند هستند

نمونه های خارجی:

۱. سیستم های یکپارچه- بیمارستان سلامت روان Derbyshire

بیمارستان سلامت روان Derbyshire با مشکالت مکرری مانند سرقت از بیمارستان و همچنین وسایل نقلیه موتوری در سایت های خود مواجه شده است لذا تصمیم به نصب سیستم کنترل دسترسی مجتمع با CCTV در این بیمارستان گرفته شد.

بدین منظور، CCTV در شبکه ای از ۱۱ سایت بیمارستان نصب شد که این مجموعه به ایستگاه نظارت متصل شد. در ۱۱ سایت، تعداد ۳۷ CCTV، آشکارسازهای مادون قرمز و راه حل های Tannoy نصب شد. علاوه بر این، مجموع ۱۷ تنظیم کنترل دسترسی و همچنین ۲۴ خواننده نزدیکی(proximity reader) و دتکتور مادون قرمز را نصب شد.

برای هریک از اعضای این بیمارستان، یک کلید دسترسی صادر شد. استفاده از این کلید، توسط نزدیک ترین واحد CCTV ثبت می شود. اگر یک کارت دسترسی به سرقت رفته باشد و دسترسی به صورت جعلی صادر شده باشد، فیلم برداری از این اتفاق می تواند در پیگیری زمان و محل این رخداد اطلاعات مفیدی حاصل کند.

بلافاصله اجازه می دهد تا برای بازیابی فیلم های تکراری سریع. علاوه بر این، اگر یکی از آشکارسازهای شکن شیشه یا یک هشدار مادون قرمز فعال شود، این نیز به فیلم CCTV وارد می شود، که اپراتورها می توانند بطور مستقیم بررسی کنند. طبق گزارش های اعلام شده از طرف این بیمارستان، افزودن این سیستم یکپارچه به شبکه بیمارستانف موجب صرفه جویی در زمان اپراتورها و همچنین کنترل امنیت کل سایت بیمارستان شده است.

۲- تامین امنیت سایت- بیمارستان های Stobhill و Victoria

این دو بیمارستان از تکنولوژی امنیتی IP بمنظور حفاظت از هریک از بخش های بیمارستان استفاده کرده اند. تمامی نقاط دسترسی در هر دو بیمارستان با استفاده از کارت خوان ها بعنوان پایگاه داده ای برای اعتبارسنجی offline ، صفحه کلید PIN اضافه شده و صفحه نمایش LCD برای نمایش فیدبک سیستم برای دارنده کارت(بعنوان مثال "دسترسی محدود" یا "پایان اعتبار کارت") حفاظت شده اند. همچنین در این دو بیمارستان سیستم کنترل دسترسی برای

. علاوه بر این، سیستم انعطاف پذیر نصب شده در این دو بیمارستان به این معنی است که می تواند دسترسی صاحبان کارت های بازدید کننده موقت را نظارت و کنترل کند. این سیستم یک راه حل جامع امنیتی را فراهم می کند که به محافظت از کارکنان، بیماران و تجهیزات و ساختمان های بیمارستان کمک می کند.

۳- بهبود کنترل دسترسی- بیمارستان Addenbrooke

در بیمارستان Addenbrooke در حال حاضر در برگیرنده بیش از ۶۰۰۰ کارمند از دانشگاه خود و بیش از ۵۰۰۰ کارمند از دیگر سازمان ها است. علاوه بر این، در طول سال، در مجموع بیش از ۲۸۰۰۰۰ بیمار سرپایی، ۲۵۰۰۰ مراجعه روزانه و ۴۴۰۰۰ بیمار بستری در بیمارستان تحت درمان قرار می گیرند. Addenbrooke برای مدیریت محوطه بیمارستان، یک راه حل کنترل دسترسی را در اواخر دهه ۱۹۹۰ برای استفاده در پارک خودروی خود، ساختمان ها و امکانات موقت نصب کرد. Addenbrooke ده سال بعد متوجه شد که آنها نیاز به یک راه حل جدید برای شناسایی و نیازهای کنترل دسترسی خود دارند.

Addenbrooke یک سیستم امنیتی به روز ادغام شده با سیستم های CCTV و زنگ هشدار مدیریت، که ایده آل برای محیط های بزرگ بیمارستانی است، را راه اندازی کرد. تکنولوژی جدید اضافه شده به بیمارستان برای ۲۴ بخش بمنظور پوشش دادن ۵۱۶ خواننده گسترش پیدا کرد، زیرا تعدادی از صاحبان کارت و خوانندگان سیستم میتوانند نامحدود باشند. قبل از نصب سیستم جدید یک بررسی کامل از تکنولوژی کنترل دسترسی فعلی بیمارستان انجام شد و طی آن مشخص شد که سیستم در وضعیت خوبی قرار دارد و قادر به ادغام با سیستم کنترل دسترسی مدرن است. در نتیجه تمام خوانندگان، محوطه ها و کابل ها برای حفظ هزینه ها حفظ شدند. عضو BSIA سیستم خود را به ۲۴ بخش دیگر گسترش داد، با نرم افزار برای حمایت از ۵۱۶ خواننده دیگر. یک پایگاه داده تنها برای تمام فعالیت های اداری از جمله ایجاد کارت، حقوق دسترسی و اصلاحیه های هویت ایجاد شده است.

این دو بیمارستان ده سال بعد نیز توسعه یافت و تاکنون با سیستم های CCTV ادغام شده است و به تکنولوژی کارت های هوشمند تبدیل شده است.

۴- کنترل ملاقات کنندگان- بیمارستان کودکان Sheffield

به عنوان یک بیمارستان کودکان، نگرانی های فراوانی برای کودکان و والدین آنها وجود دارد. امنیت به عنوان یک موضوع حیاتی دراین بیمارستان ها مطرح است؛ والدین مضطرب پس از دیدن کارکنان هنگام وارد کردن کدها در صفحه کلید ، کدها را بخاطر می سپارند و بدین ترتیب افراد غیر مجاز میتوانند وارد مناطق محدود شوند. برای حل مشکل، بیمارستان کودکان شفیلد (SCH) سیستم امنیتی خود را که قبلا شامل صفحه کلید مستقل با قفل در هر درب بود به سیستم جدید ارتقا داد که در آن به هر کارمند یک نشان شناسایی به عنوان کارت دسترسی تعلق گرفت. این سیستم سبب شد که کارکنان فقط اجازه ورود به مناطق محدود شده را داشته باشند. علاوه بر این، این سیستم، بخش های پر خطر بیمارستان مثل مجموعه MRI، داروخانه و ... را حفاظت می کند. نظارت داروخانه بسیار مهم است و در حال حاضر گزارشات به طور منظم برای ردیابی افرادی که در این منطقه و در زمان های مشخص وارد شده اند در دسترس است.

طبق گزارش های اعلام شده از طرف این بیمارستان، بعد از افزودن این سیستم به بیمارستان کارمندان و بیماران بسیار امن تر هستند و روحیه بیماران و همراهان آنها بدلیل احساس امنیت بیشتر، بهبود یافته است. این رضایت همه جانبه از سیستم امنیتی اضافه شده بیمارستان را بر ان داشته است که این سیستم را تا حد ممکن گسترش دهد.

نمونه های داخل کشور:

در ایران متاسفانه بدلیل محدود بودن بودجه در اکثر پروژه های عمرانی کشور، موضوع امنیت در اولویت هزینه ها قرار نمیگیرد و گاها در پروژه های بیمارستانی برخی از سیستم های کنترلی بصورت مجزا درنظر گرفته می شوند. شایان ذکر است که شاید در ابتدای تصمیم گیری و بودجه بندی پروژه استفاده از سیستم های کنترل تردد و تامین امنیت هزینه های زیادی را دربر داشته باشند اما باید توجه داشت که این سیستم ها می توانند از بسیاری از هزینه های حتی چندین برابری که بدلیل نبود این سیستم حاصل می شود جلوگیری کنند.

در دو پروژه بزرگ بیمارستانی مهدی کلینیک و آتیه غرب تهران که از مجهزترین بیمارستان ها در سطح کشور هستند، زیرساخت های سیستم های هوشمند BMS، CCTV، سیستم اعلام حریق و ... بطور کامل طراحی و تعبیه شده است.

در این مقاله به معرفی یک سیستم کنترل دسترسی که از دو جزء RFID و سیستم تشخیص هویت بیومتریک تشکیل شده است می‌پردازیم که در ادامه هریک از این دو جزء شرح داده شده اند:

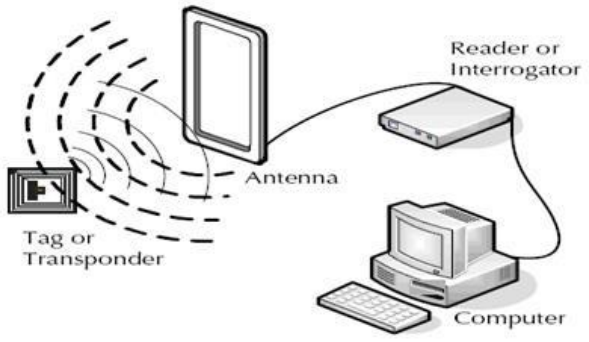
مروری بر تکنولوژی RFID

شناسایی فرکانس رادیویی (RFID) یک تکنولوژی بی‌سیم شناسایی خودکار است که بر اساس ذخیره‌سازی داده و بازیابی آن عمل می‌نماید و می‌تواند برای توسعه سیستم کنترل دسترسی استفاده شود.

سیستم شناسایی اتوماتیک و سیستم کنترل دسترسی برای غلبه بر تهدیدهای امنیتی که در بسیاری از سازمان‌ها در حال حاضر به وجود آمده است، تبدیل شده است. با نصب سیستم در ورودی، افراد مجاز اجازه ورود به سازمان را خواهند داشت. این سیستم همچنین می‌تواند در نقاط مختلف در داخل سازمان نصب شود تا پیگیری حریم شخصی و محدود کردن دسترسی آنها به مناطق حساس در سازمان صورت گیرد. به این ترتیب، افراد مشکوک شناسایی می‌شوند که درنتیجه سطح امنیتی سازمان افزایش می‌یابد.

سیستم RFID شامل سه جزء ترنسپوندر (تگ)، interrogator (reader) و رایانه حاوی پایگاه داده است[۵].

اغلب تگ‌های RFID حداقل از دو قسمت تشکیل شده‌اند: بخش اول از یک IC جهت ذخیره‌سازی و پردازش اطلاعات، مودولاسیون-دمودولاسیون سیگنال‌های RF و سایر عملیات مربوطه و بخش دوم از یک آنتن برای دریافت و انتقال سیگنال‌ها تشکیل شده‌است.



شکل ۳: سیستم RFID

reader اطلاعات تگ را می‌خواند و برای شناسایی به کامپیوتر منتقل می‌کند. اطلاعات پردازش شده و پس از تأیید، اجازه دسترسی داده می‌شود. این سیستم باند فرکانس متنوعی را از فرکانس‌های پایین تا فرکانس‌های مایکروویو ارائه می‌دهد.

برچسب‌های RFID بسته به منبع انرژی الکتریکی به دو دسته فعال یا غیرفعال طبقه بندی می‌شوند. برچسب‌های فعال از یک باتری برای روشن کردن مدار در برچسب و ارسال اطلاعات برچسب بر اساس درخواست reader استفاده می‌کنند. با این

حال، این برچسب ها بسیار گران هستند و به ندرت استفاده می‌شوند. از سوی دیگر، برچسب‌های پسیو انرژی لازم برای راه اندازی مدارشان را از reader می‌گیرند. این برچسب‌ها بسیار مقرون به صرفه هستند و از این رو در اکثر برنامه‌های کاربردی از آنها استفاده می‌شود.

در این مقاله، برچسب‌های RFID پسیو درنظر گرفته شده‌اند. برچسب‌های RFID پسیو هنگامیکه در میدان الکترومغناطیسی تولید شده توسط reader قرار می‌گیرد، اطلاعات را به reader انتقال می‌دهند. این پدیده بر اساس قانون القای الکترومغناطیسی فاراده است. جریان گذرنده از کویل reader میدان مغناطیسی تولید می‌کند که به کویل ترانسپوندر لینک می-شود و موجب تولید جریان در کویل ترانسپوندر می‌شود. سپس کویل ترانسپوندر با تغییر بار بر روی آنتن، این جریان را تغییر می‌دهد. این تغییر در واقع سیگنال مدوله شده است که توسط کوئیل reader از طریق القاء متقابل بین کویل‌ها دریافت می‌شود. کویل reader این سیگنال را رمزگشایی می‌کند و برای پردازش بیشتر به کامپیوتر انتقال می‌دهد.

تشخیص چهره

سیستم تشخیص هویت بیومتریک پیشنهاد شده در این مقاله بر پایه سیستم تشخیص چهره است.

روش‌های تشخیص چهره

تصویر اساسا یک داده دو بعدی برای بیان یک شیء است. اما برای ذخیره جزئیات شیء، تصویر شامل مقدار زیادی از داده‌ها است. اگر یک تصویر با یک تصویر دیگر با استفاده از مقادیر پیکسل‌هایشان مقایسه شود، از مقدار زیادی از داده باید استفاده شود. بنابراین، تجزیه و تحلیل اطلاعات نقش مهمی در شناسایی اطلاعات یک تصویر دارد. تجزیه و تحلیل الگو یکی از کاربردهای Data mining است. در این زمینه آموزش به منظور کشف اطلاعات معنی دار از داده های موجود انجام می‌شود.

علاوه بر این، برای شناسایی الگوهای تشکیل دهنده داده، از روش‌های انتخاب ویژگی اعمال می‌شود. یک مجموعه ویژگی خوب شامل اطلاعات متمایز کننده است که می‌تواند یک شی را از اشیاء دیگر تشخیص دهد و بتواند از تولید کدهای مختلف برای ویژگی‌های یک کلاس، جلوگیری کند. مجموعه‌ای از ویژگی‌های انتخاب شده باید مجموعه‌ای کوچک باشد که مقادیر آن در میان الگوهای کلاس‌های مختلف تمایز ایجاد کند اما در یک کلاس مقادیر نزدیک بهم داشته باشند بدین منظور باید از روش استخراج ویژگی[1]استفاده کرد. هدف اصلی استخراج ویژگی بدست آوردن اطلاعات مناسب از داده‌های اصلی و بیان این اطلاعات در یک فضا با ابعاد کمتر است. هنگامی که داده های ورودی یک الگوریتم برای پردازش بیش از حد بزرگ و مکرر باشند (داده زیاد باشد اما اطلاعات اضافه‌ای نداشته باشد)، داده‌های ورودی به یک مجموعه از ویژگی‌های نمایشی کاهش یافته (به نام بردار ویژگی) تبدیل می‌شوند که تبدیل اطلاعات ورودی به مجموعه‌ای از ویژگی‌ها، استخراج ویژگی‌ها نامیده می‌شود.

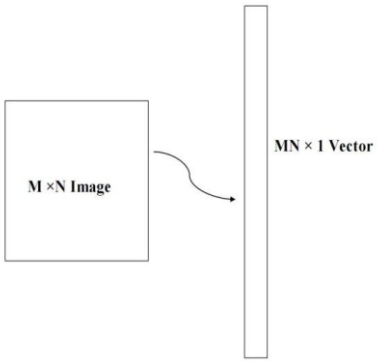
در این مقاله بمنظور تشخیص چهره، از شبکه عصبی RBFNN ومدل خطای تعمیم محلی[۶] (L-GEM[2]) برای آموزش شبکه عصبی استفاده شده است. در این سیستم بمنظور کاهش حجم پایگاه داده و کاربری بهتر سیستم، از ویژگی‌های تصاویر

[1] Feature extraction
[2] Localized Generalization Error Model

بجای ذخیره کردن کل تصاویر پرسنل استفاده شده است که بدین منظور آنالیز اجزاء اصلی(PCA[1]) برای استخراج ویژگی-های چهره بکار گرفته شده است.

آنالیز اجزاء اصلی (PCA)

تجزیه و تحلیل مولفه اصلی (PCA) [۷] یکی از روش‌های استخراج ویژگی از تصاویر است که به طور گسترده برای استخراج ویژگی‌های اصلی برای توصیف یک تصویر استفاده می‌شود. در این الگوریتم، تصاویر به یک فضای جدید متناسب با جهت دو واریانس بیشینه در فضای ورودی نگاشت می‌شوند. درصورتیکه در مجموعه داده آموزش M تصویر متمایز چهره داشته باشیم که ابعاد هریک $m \times n$ باشد، پس هر تصویر را می توان بصورت $X_i = (x_1, x_2, \dots, x_{m\times n})$ نمایش داد.



شکل ۴: تبدیل تصویر $\boldsymbol{m \times n}$ به بردار $\boldsymbol{mn \times 1}$

مجموعه آموزش شبکه با M تصویر نیز بصورت $X = (X_1, X_2, \dots, X_M)$ قابل نمایش است. ماتریس کوواریانس از مجموعه داده آموزش بصورت زیر بدست می آید:

$$\Gamma = \frac{1}{M}\sum_{i=1}^{M}(X_i - \bar{X}) \times (X_i - \bar{X})^T$$

که در آن $\bar{X} = \frac{1}{M}\sum_{i=1}^{M} X_i$ میانگین داده‌های آموزش است. بردارهای ویژه و مقادیر ویژه از Γ قابل محاسبه هستند. اگر $u_1, u_2, \dots, u_n$ و $\lambda_1, \lambda_2, \dots, \lambda_n$ بترتیب بردارهای ویژه و مقادیر ویژه Γ باشند، Γ را می‌توان بصورت $\Gamma = U\Lambda U^T$ نشان داد که در آن $U = (u_1, u_2, \dots, u_n)$ و $\Lambda = (\lambda_1, \lambda_2, \dots, \lambda_n)$. فقط r بردار ویژه متناسب با r بزرگترین مقادیر ویژه وجود دارد که هر یک از r بردار یک eigenface نامیده می‌شود. اگر مجموعه تصاویر تست را Y بنامیم، $Z_j = V^T Y_j \ \ (j = 1,2, \dots, N)$ که در آن N تعداد تصاویر تست است. با توجه به مطالب ذکر شده، داده تصاویر با $m \times n$ بردار، به یک بردار با r جزء تبدیل می‌شود.

یکی از ساده‌ترین و موثرترین رویکردهای PCA که در سیستم های تشخیص چهره استفاده می‌شود، رویکرد به اصطلاح eigenface (چهره ویژه) است. Eigenface نامی است که به مجموعه ای از بردارهای ویژه اطلاق می شود که در مسئله

[1] Principal Component Analysis

تشخیص چهره انسان از حوزه بینایی کامپیوتر استفاده می‌شود[۸]. این رویکرد، چهره‌ها را به یک مجموعه کوچک از ویژگی‌های اساسی(چهره‌های ویژه) تبدیل می‌کند که اجزاء اصلی مجموعه اولیه تصاویر یادگیری (مجموعه آموزش) هستند.

نویسندگان [۹] PCA و نویسندگان [۱۰] از LDA برای استخراج ویژگی‌های چهره استفاده کرده‌اند. تبدیل ویژگی نامتغیر با اسکیل (SIFT[1]) یکی دیگر از روش پر کاربرد در استخراج ویژگی چهره است که عناصر کلیدی محلی برای توصیف چهره را استخراج می‌کند. پس از استخراج ویژگی‌ها، فاصله بین تصویر چهره مورد نظر و تمام تصاویر چهره در پایگاه داده محاسبه می‌شود. افرادی که تصویر چهره آنها در پایگاه داده فاصله کمتری نسبت به تصویر چهره مورد بررسی داشته باشد بعنوان هویت مورد نظر انتخاب می‌شوند. این روش‌ها در شرایطی که تعداد تصاویر چهره در پایگاه داده زیاد باشد بسیار زمانبر هستند. مهمتر از همه، این باعث می‌شود سیستم در هر صورت یک گزینه را از پایگاه داده بعنوان نزدیک ترین داده انتخاب کند که این موضوع در کنترل دسترسی خطرناک است.

در این مقاله، از الگوریتم یادگیری شبکه عصبی برای شناسایی افراد مجاز و تمایز آن با سایر افراد استفاده شده است. در این روش زمان کمتری برای پردازش صرف خواهد شد. از همه مهمتر اینکه در این روش، شبکه عصبی با کارت RFID افراد مجاز در تعامل است و تنها این افراد از مرحله تشخیص چهره سیستم کنترل دسترسی عبور خواهند کرد.

شبکه‌های عصبی RBFNN[2]

شبکه‌های عصبی RBFNN در بسیاری از زمینه‌ها از جمله پردازش تصویر بسیار پرکاربرد هستند. در مقایسه با دیگر شبکه-های عصبی، شبکه عصبی با پایه شعاعی (RBFNN) دارای مزایای ساختار شبکه ساده و سرعت یادگیری سریع و مینیمم سراسری است [۱۱]. آموزش RBFNN معمولا در دو مرحله انجام می شود [۱۲]در مرحله اول، پارامترهای پنهان مربوط به تابع پایه شعاعی را تعیین می‌کند و در مرحله بعد، وزن‌های خروجی را تعیین می‌کند. در مقایسه با شبکه‌های MLP، یک مزیت RBFNN ها این است که پارامترهای مناسب برای لایه پنهان بدون انجام بهینه سازی غیرخطی پارامترهای شبکه می توانند یافت شوند. با این حال، در انتخاب تعداد مناسب نورونهای پنهان (توابع پایه)، مسئله مهمی برای RBFNN ها باقی می‌ماند. پیچیدگی و قابلیت تعمیم پذیری RBFNN توسط تعداد نورون‌های مخفی کنترل می‌شود. تعداد بسیار کم نورون‌های پنهان موجب انعطاف پذیری کم و محدود شدن قابلیت تعمیم برای داده‌های جدید می‌شود. در مقابل، RBFNN با تعداد بسیار زیاد از نورون‌های پنهان نیز بدلیل Overfit شدن به داده‌های ورودی و نویز، موجب محدود شدن تعمیم می‌شود. واریانس کم و تخمین گر با بایاس بالا با تعداد کمی از نورونهای پنهان به دست می‌آید در حالیکه تخمین گر با واریانس بالا و بایاس کم با تعداد زیادی از نورون‌های پنهان به دست می‌آید. برای تعیین بهترین عملکرد بهینه سازی، باید درمورد الزامات متناقض کاهش واریانس و همزمان کاهش بایاس مصالحه بهینه درنظر گرفته شود. این مصالحه بر اهمیت انتخاب ساختار مدل RBFNN تاکید می‌کند. برای مقابله با این مشکل، می‌توان از روش انتخاب معماری شبکه بر اساس مدل خطای تعمیم محلی (L-GEM) استفاده کرد. [۹]L-GEM یک حد بالا (R * SM) خطای تعمیم نمونه‌های دیده نشده در همسایگی Q نمونه‌های آموزش (SQ) تعیین می‌کند. خطای تعمیم محلی در همسایگی Q نمونه‌های آموزش (SQ) بصورت زیر تعریف می‌شود:

[1] Scale Invariant Feature Transform (SIFT)
[2] Radial Basis Function Neural Networks

$$R_{SM}(Q) = \int_{S_Q} (f(x) - F(x))^2 p(x) dx$$

که در آن Q، $f(x)$، $F(x)$ و $p(x)$ بترتیب بیان کننده همسایگی Q ، خروجی واقعی x، خروجی مطلوب x و تابع احتمال x در Q هستند. با احتمال $(1-\eta)$ داریم:

$$R_{SM} \leq (\sqrt{R_{emp}} + \sqrt{E_{S_Q}((\Delta y)^2)} + A)^2 + \varepsilon = R_{SM}^*$$

که در آن

$$R_{emp} = (\frac{1}{N}) \sum_{b=1}^{N} (f(x^{(b)}) - F(x^{(b)}))^2$$

$$\Delta y_b = f(x^{(b)}) - F(x^{(b)})$$

$$\varepsilon = B\sqrt{ln^{\eta}/(-2N)}$$

$x^{(b)}$ ، $E_{S_Q}((\Delta y)^2)$ ، η ، A و B ، بترتیب b امین تصویر آموزش، حساسیت تصادفی شبکه عصبی، سطح اطمینان از محدوده، اختلاف بین حداکثر و حداقل مقدار خروجی‌های هدف و مقدار ماکسیمم خروجی واقعی و خروجی هدف هستند.

در این مقاله، یک سیستم کنترل دسترسی که ترکیبی از فناوری RFID و شناسایی چهره بر اساس شبکه عصبی است ارائه شده است. این سیستم چهره فردی که کارت RFID در اختیار دارد را شناسایی می‌کند و در صورت تناقض اطلاعات این دو، دسترسی را غیرممکن می کند. در این سیستم، یک شبکه عصبی پایه شعاعی (RBFNN) برای یادگیری چهره صاحبان مجاز کارت بهمراه مدل خطای تعمیم محلی (L-GEM) برای آموزش RBFNN به کار می‌رود و بمنظور صرفه جویی در حافظه سیستم زمانی که تعداد دارندگان کارت‌ها زیاد می‌شود، فقط پارامترهای RBFNN ذخیره می‌شوند.

ساختار و عملکرد سیستم پیشنهادی

سیستم کنترل دسترسی پیشنهادی از یک RFID reader وایرلس، یک wireless router ، یک کامپیوتر و یک دوربین تشکیل شده است. Wireless router، RFID reader و کامپیوتر را به شبکه وایرلس متصل می‌کند.

سیستم کنترل دسترسی پیشنهادی از دو فاز ثبت[1] و فاز شناسایی[2] تشکیل شده است:

[1] Registration
[2] Recognition

- فاز ثبت

۱. برای هریک از پرسنل یک کارت RFID با ID منحصر به فرد تخصیص می‌یابد.

۲. از هر شخص ۱۰ عکس در حالتهای مختلف مثل تفاوت در شدت روشنایی، تفاوت در زاویه و حالات چهره تهیه می‌شود.

۳. الگوریتم PCA به ۱۰ عکس تهیه شده از هر شخص اعمال می‌شود و eigenface های بدست آمده ذخیره می‌شوند.

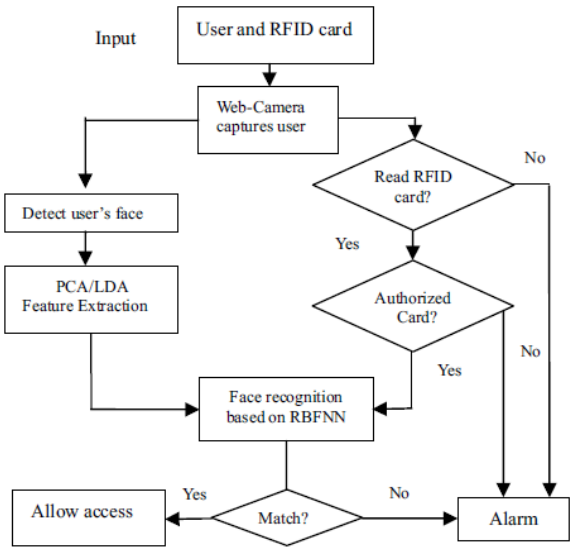
۴. برای هر ID یک شبکه عصبی RBFNN با الگوریتم L-GEM آموزش داده می‌شود که داده های آموزش این شبکه‌ها eigenface های بدست آمده مرحله قبل است.

۵. بمنظور صرفه جویی در حافظه و بهبود غملکرد سیستم، تنها پارمترهای شبکه RBFNN ذخیره خواهند شد.

- فاز شناسایی:

هنگامیکه یک کاربر با کارت RFID خود وارد ناحیه حفاظت شده از سیستم کنترل دسترسی می‌شود، RFID reader با سیگنال ارسالی از طرف کارت RFID فعال می‌شود. درصورتیکه دارنده ID متناظر با آن کارت RFID اجازه دسترسی به آن ناحیه را نداشته باشد، سیستم هشدار می‌دهد. درصورتیکه یک کارت RFID با اجازه دسترسی وارد منطقه مورد نظر شود، فاز تشخیص چهره سیستم فعال می‌شود و شبکه عصبی مختص این کارت RFID جهت تشخیص چهره فعال می‌شود. درصورتیکه چهره شناسایی شده توسط سیستم با دارنده کارت RFID تطابق نداشته باشد، سیستم هشدار می‌دهد، در غیر اینصورت، شخص مورد نظر اجازه دسترسی به محل حفاظت شده مورد نظر را خواهد داشت.

الگوریتم سیستم کنترل دسترسی پیشنهادی در شکل زیر نشان داده شده است



شکل ۵: الگوریتم سیستم کنترل دسترسی پیشنهادی

نتیجه گیری:

RFID یکی از رایج‌ترین سیستم‌های کنترل دسترسی است. با این حال، فناوری RFID فعلی، هویت دارنده کارت RFID (یا برچسب) را شناسایی نمی‌کند در نتیجه، هر فرد غیر مجازی که یک کارت RFID مجاز بهمراه داشته باشد می‌تواند به منطقه امن دسترسی پیدا کند. برای مقابله با این مشکل، یک روش شناسایی بیومتریک تشخیص چهره ادغام شده با RFID برای کنترل دسترسی پیشنهاد شده است. در این مقاله، یک سیستم کنترل دسترسی که ترکیبی از فناوری RFID و شناسایی چهره بر اساس شبکه عصبی است ارائه شده است. این سیستم چهره فردی که کارت RFID در اختیار دارد را شناسایی می-کند و در صورت تناقض اطلاعات این دو، دسترسی را محدود می کند. در این سیستم، یک شبکه عصبی پایه شعاعی (RBFNN) برای یادگیری چهره صاحبان بکمک eigenface های چهره افراد مجاز بهمراه مدل خطای تعمیم محلی (L-GEM) برای آموزش RBFNN به کار رفته است و بمنظور صرفه جویی در حافظه سیستم زمانی که تعداد دارندگان کارت‌ها زیاد می‌شود، فقط پارامترهای RBFNN ذخیره می‌شوند.

منابع

1. *THE IMPORTANCE OF ACCESS CONTROL SYSTEMS IN HOSPITALS.* Customer 1st communication, 2016.
2. *A guide to access control for the healthcare sector.* british security industry association, 2017. **293**.
3. Bigira, E.S., *Management of Hospital Security in General Hospitals of Southwestern Uganda.* International Journal of Public Health Research, 2015. **3**: p. 173-179.
4. *Meeting the access control challenge in hospitals.* 2018.
5. *RFID Based Security and Access Control System.* IACSIT International Journal of Engineering and Technology, 2014. **6**(4).
6. *Localized Generalization Error and Its Application to Architecture Selection for Radial Basis Function Neural Network.* IEEE Transaction on Neural Networks, 2007. **18**: p. 1294-1305.
7. Turk, M. and A. Pentland, *Eigenfaces for Recognition.* Journal of Cognitive Neuroscience, 1991. **3**(1): p. 71-86.
8. Thuseethan, S., Kuhanesan, S., *Eigenface Based Recognition of Emotion Variant Faces.* 2016.
9. Satyanarayana, C., D.M. Potukuchi, and L. Pratap Reddy, *Performance evaluation of incremental training method for face recognition using PCA.* Journal of Real-Time Image Processing, 2007. **1**(4): p. 311-327.
10. Zuo, W., et al., *Combination of two novel LDA-based methods for face recognition.* Neurocomputing, 2007. **70**(4): p. 735-742.
11. Toit, T.d., *Automated Architecture Selection for Radial Basis Function Neural Networks.* Research Journal of Applied Sciences, Engineering and Technology 2016. **12**(11): p. 1146-1151.
12. Moody, J. and C.J. Darken, *Fast Learning in Networks of Locally-Tuned Processing Units.* Neural Computation, 1989. **1**(2): p. 281-294.