بکارگیری بیومتریک چندگانه در راستای دستیابی به قابلیت کنترل حضور در سیستم مدیریت یادگیری

چکیده

در دهه گذشته پیشرفت‌های چشمگیری در حوزه یادگیری الکترونیکی صورت گرفته است. با این وجود، همچنان در سیستم‌های مدیریت یادگیری ضعف‌هایی مشاهد می‌شود. از مهمترین این ضعف‌ها می‌توان به عدم اطمینان از حضور دانشجوی موردنظر (ثبت نام‌کننده) و نیز عدم امکان کنترل حضور مستمر دانشجو در کلاس الکترونیکی، اشاره کرد. استفاده از تکنیک‌های تأیید هویت در ممانعت از دسترسی افراد غیر مجاز به سیستم‌های یادگیری الکترونیکی حائز اهمیت می‌باشد.

هدف از این مقاله ارائه‌ی یک مدل یادگیری الکترونیکی مبتنی بر کاربردهای وب با قابلیت کنترل حضور است. مدل ارائه شده بر اساس روش بیومتریک چندگانه می‌باشد و به منظور شناسایی، تأیید هویت و ردیابی دانشجو در سیستم مدیریت یادگیری استفاده می‌شود. در این راستا از دو بیومتریک رفتاری (الگوی حرکات ماوس و الگوی تایپ) و یک بیومتریک فیزیکی (چهره) استفاده شده است. شیوه استفاده از این سه بیومتریک با ارائه یک الگوریتم مشخص می‌گردد. با توجه به نتایج آزمایش انجام گرفته، راهکار ارائه شده کمترین نیاز به مشارکت دانشجو در فرآیند تأیید هویت و کنترل حضور را دارا می‌باشد. مدل پیشنهادی قابلیت اضافه شدن به LMSهای موجود و سازگاری با آن‌ها را دارا می‌باشد. بنابراین می‌توان از این مدل جهت محاسبه میزان شخص یادگیرنده در طی مراحل حساس فرآیند یادگیری الکترونیکی بهره برد.

واژه‌های کلیدی

یادگیری الکترونیکی، بیومتریک چندگانه، تأیید هویت، حضور، ردیابی.

۱- مقدمه

سیستم‌های یادگیری الکترونیکی[۱] شکل جدیدی از یادگیری را ارائه می‌دهند و هرروزه شیوه‌های نوینی برای این سیستم یادگیری مطرح می‌شود، از اینرو نیاز به امنیت در این سیستم‌ها بسیار محسوس است. مدیران آموزشی به منظور طراحی و اجرای واحدهای آموزشی متناسب با نیازهای خود، از سیستم‌های مدیریت یادگیری[۲](LMS) استفاده می‌کنند. . یکی از مهم‌ترین ضعف‌های LMS فقدان ابزارهای کافی برای ردیابی درستی رفتار کاربران می‌باشد[1,6]. راه حل های سنتی که تعامل بین کاربر و سیستم را ثبت می‌کنند نمی‌توانند تضمین نمایند که کاربر همان کسی است که او ادعا می‌کند، و یا حتی، آنها نمی‌توانند تضمین کنند که آیا کاربر در مقابل کامپیوتر وجود دارد یا خیر[4]. اطلاعاتی که در فایل‌های گزارش[۳] سنتی کاربران ثبت می‌گردد، فقط زمان ورود و خروج دانشجو را ثبت می‌کنند و زمان واقعی که دانشجو مقابل کامپیوتر نشسته و به درس توجه کرده را مشخص نمی‌کند[1,4]. یک کاربر می‌تواند با نام کاربری و کلمه عبور خود وارد کلاس الکترونیکی شود و چند دقیقه بعد سیستم را ترک کند و در پایان کلاس بازگشته و از سیستم خارج شود. واضح است که این عمل در فایل گزارش قابل تشخیص نیست و بازتابی ندارد.

موقعیت‌های مشابهی مانند آنچه در بالا توضیح داده شده وجود دارد که زمان واقعی که دانشجو مقابل کامپیوتر گذرانده را نشان نمی‌دهد. در اینجا نقش تکنیک‌های تأیید هویت در جلوگیری از دسترسی افراد غیر مجاز اهمیت زیادی دارد. به طور کلی روش‌های تأیید هویت را می توان در قالب سه دسته بیان نمود: ۱- روش‌های مبتنی بر حافظه انسانی مانند کلمه عبور ۲- روش‌های مبتنی بر ابزارهای سخت افزاری مانند کارت‌های مغناطیسی ۳- روش‌های مبتنی بر فناوری بیومتریک مانند اثر انگشت، عنبیه چشم و غیره. روش‌های نوع اول یا دوم مشکلاتی مانند فراموشی، مفقود شدن یا دزدیده شدن را دارند به همین جهت روش‌های نوع سوم امروزه مورد توجه قرار گرفته‌اند[1,5].

در این مقاله یک راهکار جهت تأیید هویت و محاسبه مدت‌زمان حضور بر اساس یک روش بیومتریک چندگانه ارائه می‌گردد. بیومتریک چندگانه[۴] جهت بهبود قابلیت اطمینان در تائید هویت با استفاده از بیومتریک، در مواقعی که تأیید هویت تنها براساس یک

[۱] E-learning System
[۲] Learning Management System
[۳] Log Files
[۴] Multimodal Biometric

ویژگی بیومتریک، سطح اطمینان مورد نظر را برآورده نمی‌کند، مفید می‌باشد. [3,5,9].

در ادامه مطالب، در بخش دوم تحقیقات انجام شده قبلی در این زمینه مشخص شده است. نکات و تعاریف مورد نیاز مدل در بخش سوم بیان می‌گردد. در بخش چهارم راهکار پیشنهادی و سیستم‌های بیومتریک به کار رفته در مدل ارائه می‌گردد. معماری مدل پیشنهادی در بخش پنجم نشان داده شده است. در بخش ششم پیاده‌سازی سیستم بیان گردیده است. نتایج ارزیابی راهکار پیشنهادی در بخش هفتم ارائه گردیده و در نهایت در بخش هشتم نتیجه‌گیری و کارهای آینده بیان شده است.

۲- کارهای مرتبط انجام شده

تاکنون تحقیقات زیادی روی ترکیب فناوری‌های بیومتریک در زمینه‌های مختلف و از جمله یادگیری الکترونیکی، صورت انجام گرفته است. برای نمونه در [8] جزئیات فایل گزارش ثبت شده مربوط به هرکاربر با اطلاعات بیومتریک بدست آمده از کاربر ترکیب می‌شود. جزئیات فایل گزارش شامل اطلاعاتی در مورد زمانی که کاربر شروع به کار کرده، رخدادهای مرورگر و وضعیت فعال بودن مرورگر می‌باشد. با این حال مشکلاتی از قبیل شرایط بد نور اتاق در بیومتریک‌های چهره و عنبیه، می‌تواند کارآیی مکانیزم تأیید هویت را کاهش دهد. علاوه بر این، عوامل انسانی به طور جدی می‌تواند کارایی سیستم را کاهش دهند از جمله: برخی از کاربران بیشتر زمان کلاس حالت نامناسبی برای تشخیص چهره دارند. یک راه حل در [6] ارایه گردیده است به طوری که سیستم علاوه بر تأیید از طریق چهره از ویژگی اثر انگشت نیز استفاده می‌کند. این سیستم برای تأیید هویت نیاز به مشارکت کاربر دارد. ضمن آنکه ردیابی مستمر با این روش سبب تداخل در کار کاربر می‌گردد. همچنین اثر انگشت می تواند براحتی از سطوح لمس شده جعل شود و با استفاده از یک لایه نازک ژلاتینی یا سیلیکنی کپی شود.

در [3] ردیابی دانشجو فقط بر اساس تشخیص چهره صورت گرفته است. هر چند این راه حل به دو شیوه مشارکتی[۱] و غیر مشارکتی[۲] با کاربر انجام می‌پذیرد که احتمال سوءاستفاده را کمتر می‌کند ولی هنوز امکان سوءاستفاده وجود دارد. برای مثال دانشجو می‌تواند یک تصویر یا ویدئو از خود را در مقابل دوربین وب[۳] قرار داده و خودش سیستم را ترک کند. همچنین در تأیید هویت مشارکتی نیاز به تعامل با کاربر زیاد است. در [5] یک راه حل برای اندازگیری مدت زمان حضور دانشجو ارائه گردیده که از دو بیومتریک چهره و اثر انگشت یا صدا استفاده می‌کند. این راه حل تقریبا بهترین راهکاری است که تاکنون ارائه شده و امکان سوءاستفاده را به حداقل ممکن رسانده است. اما استفاده از بیومتریک اثر انگشت علاوه بر مشکلات مذکور برای سیستم‌های تشخیص اثر انگشت، نیاز به ابزار جدیدی دارد[9].

به طور کلی در سیستم‌هایی که تنها از یکی از روش‌های چهره، اثر انگشت یا شبکیه جهت تأیید هویت و ردیابی استفاده می‌کنند مشکلاتی وجود دارد که به راحتی قابل حل نمی‌باشد. از جمله این مشکلات عدم حصول اطمینان کافی از حضور کاربر واقعی با استفاده از تنها یک ویژگی بیومتریک می‌باشد. در این مقاله سعی بر آن شده که با بکارگیری بیومتریک چندگانه، ضعف‌های موجود در راه حل‌های مذکور مرتفع گردد. بیومتریک‌های مورد استفاده در این مقاله چهره، الگوی حرکات موس و الگوی تایپ کاربر می باشد. لازم به ذکر است که هیچ یک از تحقیقاتی که تاکنون بر روی ترکیب فناوری‌های بیومتریک انجام گرفته، بر روی ترکیب این سه ویژگی تمرکز نداشته‌اند.

۳- مفاهیم فنی مدل

در این قسمت به اختصار بعضی از مفاهیمی که در ادامه از آنها استفاده خواهیم کرد، بیان می‌گردد. این مفاهیم در زیربخش‌های ۳-۱ تا ۳-۳ ارائه می‌گردند.

۳-۱. پردازش داده‌های بیومتریک در سرویس‌دهنده

در این روش قسمت مفید داده‌های بیومتریک کاربر توسط برنامه‌ای که بر روی سرویس‌گیرنده قرار دارد، استخراج شده و جهت تحلیل و بررسی به سمت سرویس‌دهنده ارسال می‌گردد. این روش دارای مزیت به حداقل رساندن بار محاسباتی در سمت سرویس‌گیرنده است چرا که این عملیات می‌تواند روی کامپیوترهای قوی در سمت سرویس‌دهنده اجرا شود. همچنین از نظر امنیت و تطبیق پذیری[۴] تأیید در سمت سرویس‌دهنده شکل بهتری دارد[1,8].

۳-۲. پردازش داده‌های بیومتریک در سرویس‌گیرنده

در این روش داده‌های بیومتریک کاربران به طور کامل در سمت سرویس‌گیرنده پردازش شده و اطلاعات مفید آن به صورت نمودار یا جدول استخراج می‌گردد و سپس برای مقایسه با الگوهای ثبت شده کاربر به سمت سرویس‌دهنده ارسال می‌گردد. مزیت این روش استفاده از قدرت پردازش سرویس‌گیرنده می‌باشد[1].

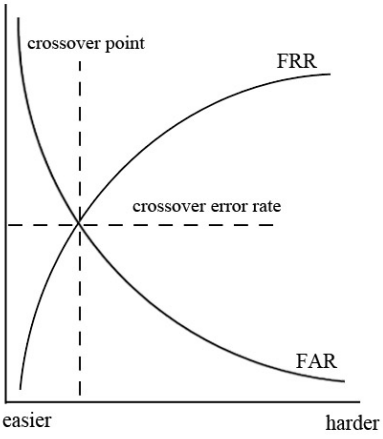
۳-۳. بیومتریک چندگانه

در این تحقیق سعی شده با ترکیب چند ویژگی بیومتریک کاربر، احتمال رخداد خطا در تأیید هویت و ردیابی به حداقل برسد.

---

[۱] Collaborative
[۲] Non-Collaborative
[۳] WebCam
[۴] Versatility

ترکیب روش‌های بیومتریک با روش‌های آماری یا منطقی قابل انجام است. روش‌های منطقی هر تأیید هویت را به صورت جداگانه انجام داده و برای بدست آوردن نتیجه نهایی، بر روی نتایج آنها AND یا OR را اعمال می‌نمایند. روش‌های آماری ابتدا با استفاده از هر یک از ویژگی‌های بیومتریک تأیید هویت چندگانه‌ای انجام داده و سپس با تکیه بر توابع آماری نتیجه تأیید هویت چندگانه را مشخص می‌کنند[1,5,9,13]. قابلیت اطمینان روش بیومتریک چندگانه بوسیله تابع چگالی کاربر واقعی و کاربر غیر واقعی(متقلب)، با استفاده از ایجاد دو نرخ خطای FAR[۱] و FRR[۲] بررسی می‌گردد[5,9]. منحنی‌های نشان داده شده در شکل ۱ رابطه بین این خطاها را نشان می‌دهد.



شکل۱- ارتباط بین خطاهای FAR و FRR

محل تقاطع دو منحنی نقطه‌ای است که FRR و FAR برابر هستند. در زمینه شناسایی شخصی، جهت داشتن قابلیت اطمینان بالا، مقادیر FAR و FRR مورد نیاز باید از محل تقاطع دو منحنی کمتر باشد.

۴- راهکار پیشنهادی

در مدل پیشنهاد شده جهت تأیید هویت، ردیابی و کنترل حضور دانشجو از بیومتریک فیزیکی تصویر چهره، و دو ویژگی بیومتریک رفتاری الگوی حرکات ماوس و الگوی تایپ استفاده شده است. سیستم کنترل حضور به عنوان یک سیستم نظارت مستمر طراحی گردیده است که رفتار دانشجو را در طول جلسه یادگیری ذخیره می‌کند. این سیستم از سه زیرسیستم تشکیل شده است: الف) زیرسیستم تشخیص چهره ب) زیرسیستم تشخیص الگوی حرکات ماوس ج) زیرسیستم تشخیص الگوی تایپ. این زیرسیستم‌ها در بخش‌های ۴-۳ تا ۴-۵ شرح داده می‌شوند.

۴-۱. الگوریتم کنترل حضور

در این مقاله الگوریتمی به منظور کنترل حضور دانشجو در کلاس الکترونیکی ارائه می‌گردد. این الگوریتم ACT[۳] نامیده می‌شود. در الگوریتم ACT از سه ویژگی بیومتریک ذکر شده استفاده می‌گردد. شبه کد الگوریتم پیشنهادی در شکل۲ ارائه گردیده است.

Presence control Tracker(PCT)

```
1   Initialize:
2     Attendance =0, Absence=0
3     face-result=false
4     km-result=false
5     Collaborative-result =false
6     Timecalss=S  // time of calss is S seconds
7   While (Timecalss>0)
8     Compare face image with templates, get result in face-
      result
9     if  face-result =false then
10  Compare keystroke & mouse movement rhythm with
      template, get result in km-result
11    end if
12    if  km-result =false  then
13          Collaborative verification by face, get result in
      Collaborative-result
14    end if
15    if  face-result =true or km-result =true or Collaborative-
      result =true  then
16  Attendance  = Attendance  +1  // Register a Attendance
      for student
17    else
18          Absence = Absence +1  // Register a Absence for
      student
19    end if
20    wait n seconds   // n is expiry time for new verification
21    timeclass=timeclass - n
22    end while
23    all-Attendance = Attendance  × n
24    all-Absence = Absence × n
25    end   // end of virtual class
```

شکل۲- الگوریتم پیشنهادی جهت کنترل حضور در کلاس الکترونیکی

[۱] False Accept Rate
[۲] False Reject Rate
[۳] Attendance Control Tracker

این الگوریتم جهت بیان فرآیند کنترل حضور و نحوه کاربرد ویژگی‌های بیومتریک ارائه شده است. الگوریتم ACT به شکلی طراحی گردیده که هر ویژگی بیومتریک مورد نیاز می تواند جایگزین بیومتریک های به کار رفته در این مقاله گردد. عملکرد الگوریتم ارائه شده به این صورت است که در مرحله اول داده‌های بیومتریک کاربر جهت تأیید هویت دریافت شده و به سمت زیربرنامه تأیید هویت در سرویس‌دهنده ارسال می‌گردد. در مرحله بعد زیربرنامه تأیید هویت این اطلاعات را با الگوی متعلق به کاربر روی بانک اطلاعات، مقایسه کرده و میزان مطابقت آن را به صورت یک مقدار عددی بدست می‌آورد. این عدد با یک حد آستانه مقایسه شده تا نتیجه تأیید هویت مشخص شود و در صورت مثبت بودن نتیجه، دانشجو وارد کلاس الکترونیکی می‌شود. پس از ورود دانشجو اطلاعات بیومتریک او به صورت پیوسته و متناوب در فاصله‌های زمانی مشخص در طول برگزاری کلاس از کاربر دریافت شده و به زیربرنامه کنترل حضور ارسال می‌گردد. این زیربرنامه مدت زمان حضور دانشجو در کلاس را محاسبه کرده و در فایل گزارش مربوط به هر دانشجو در بانک اطلاعات ذخیره می‌کند. ضمن اینکه این زیربرنامه می‌تواند به صورت همزمان اطلاعات حضور دانشجو را در اختیار مدرس کلاس نیز قرار دهد. مراحل الگوریتم ACT به شرح زیر می باشد:

مرحله ۱: ثبت نام- هنگام اولین ورود دانشجو، الگوهایی از چهره، حرکات ماوس و تایپ کاربر، دریافت شده و در بانک اطلاعاتی سیستم ذخیره می‌گردد.

مرحله ۲: تأیید هویت بیومتریک- فرآیند تأیید هویت به شیوه بیومتریک یا ترکیبی با آن، هنگام ورود دانشجو به کلاس الکترونیکی انجام می‌گیرد.

مرحله ۳: کنترل حضور با چهره- پس از ورود دانشجو به کلاس الکترونیکی، به صورت پیوسته در طول کلاس ردیابی می‌گردد و به طور مستمر مشخصات تصویر دریافتی از چهره با اطلاعات موجود در بانک اطلاعاتی مطابقت داده می‌شود. هر ردیابی چهره زمان انقضای مشخصی، به طور مثال n ثانیه، دارد و بعد از n ثانیه به یک تأیید چهره مجدد نیاز است.

مرحله ۴: کنترل حضور با ماوس و صفحه کلید- اطلاعات رفتاری مربوط به ماوس و صفحه کلید در زمان استفاده کاربر، بصورت پیوسته، در فایل گزارش بیومتریک کاربر ذخیره می شود. در صورتی که تصویر دریافتی از چهره به هر علتی جهت تشخیص مناسب نباشد، از این دو ویژگی رفتاری دانشجو جهت ردیابی استفاده می‌گردد.

مرحله ۵: کنترل حضور مشارکتی- در صورتی که سیستم با دریافت تصویر چهره، اطلاعات ماوس و صفحه کلید، قادر به تأیید هویت کاربر نباشد اقدام به تأیید هویت مشارکتی می‌کند. بدین صورت که درخواستی مبنی بر قرار گرفتن مناسب در مقابل دوربین و دریافت تصویر جدید از چهره، به کاربر داده می‌شود. در این مرحله نیز یک زمان انقضا برای قرار دادن چهره به شکل مناسب در مقابل دوربین تعیین می‌گردد.

مرحله ۶: محاسبه میزان حضور- در صورتی که دانشجو تأیید هویت گردد برای این بازه‌ی زمانی برای وی حضور و در غیر این صورت غیبت ثبت می‌گردد. در پایان کلاس با توجه به این حضور و غیابها، مدت زمان حضور کلی دانشجو در کلاس محاسبه می‌گردد.

لازم به ذکر است در مراحل ۳ و ۵ زمان انقضا به عوامل متعددی از جمله: پهنای باند شبکه، قدرت پردازش سرویس‌دهنده یا سرویس‌گیرنده و میزان دقت مورد انتظار از سیستم، بستگی دارد. در حالت ایده‌آل زمان انقضا توسط مدرس تنظیم می‌گردد تا بتواند میزان دقت و نظم کلاس خود را مشخص نماید.

۴-۲. شیوه‌ی ترکیب و نحوه‌ی تصمیم‌گیری

در راهکار ارائه شده، استفاده از هر سه ویژگی بیومتریک ضروری نمی‌باشد و تا حد امکان تنها از چهره استفاده می‌شود. ردیابی از طریق چهره با ورود دانشجو به سیستم و بدون تعامل و مشارکت دانشجو شروع می‌گردد. تا زمانی که کاربر از طریق چهره قابل ردیابی است داده‌های خام دریافت شده از ماوس و صفحه کلید، بدون استخراج ویژگی‌ها، در فایل گزارش بیومتریک کاربر ذخیره می‌گردد. میزان استفاده از دو روش الگوی حرکات ماوس و الگوی تایپ ممکن است در LMSهای مختلف و محتوای یک صفحه خاص، متفاوت باشد. در صورت عدم امکان ردیابی دانشجو از طریق چهره، تأیید و ردیابی با استفاده از اطلاعات ماوس و صفحه کلید انجام می‌گیرد. برای این منظور اطلاعات رفتاری ماوس و صفحه کلید اخیر دانشجو که در بانک اطلاعاتی ذخیره گردیده، جهت استخراج ویژگی‌ها و مقایسه با الگوی ثبت شده در بانک اطلاعاتی، پردازش شده و نتیجه تأیید هویت مشخص می‌گردد. از مزایای این روش می‌توان به کاهش بار محاسباتی جهت تأیید کاربر و نیز تأمین قابلیت اطمینان مطلوب سیستم، اشاره نمود.

در مدل ارائه شده، در صورت نیاز به تأیید هویت از طریق ماوس و صفحه کلید، یک تأیید هویت مستقل توسط ویژگی‌های ماوس و صفحه کلید انجام شده و با اعمال AND منطقی بر روی نتایج این دو ویژگی، نتیجه تأیید هویت مشخص می‌شود. تصمیم-گیری در مورد پذیرش یا عدم پذیرش در هر روش با توجه به سیاست سیستم انجام می‌پذیرد. چنانچه یک سیاست می‌تواند تعیین کند که در یک روش بیومتریک اگر میزان تطبیق کمی کمتر از حد آستانه ثابت بود، کاربر پذیرفته شود، و یا سیاستی دیگر مشخص می‌کند که یک میزان کمتر تطبیق از حد آستانه، کاربر پذیرفته نشود.

۴-۳ . زیرسیستم تشخیص چهره

فناوری تشخیص چهره نیاز به ابزار خاصی نداشته و تنها از طریق یک دوربین وب می‌توان چهره کاربر را تشخیص داد. این فناوری در مقایسه با فناوری‌های تشخیص عنبیه یا شبکیه چشم، که نیاز به دوربین‌های پرهزینه دارند، هزینه‌های کمتری در بر دارد[12].

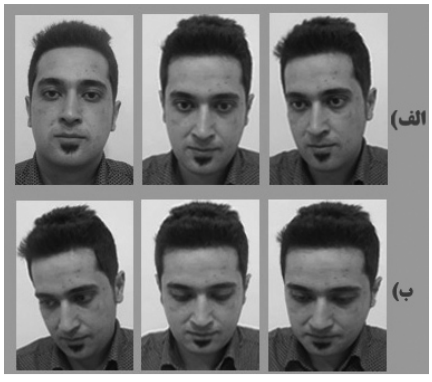
کشف چهره به معنای یافتن الگوهای بنیادی در تصویر گرفته شده از کاربر و مقایسه با پایگاه داده موجود می باشد. سیستم کشف چهره، مبتنی بر الگوریتم Viola-Jones می باشد[11,14]. این سیستم با استفاده از برنامه نویسی Matlab توسعه داده شده است. این زیربرنامه جهت جستجو و ردیابی چهره کاربر جدید، از یک تشخیص‌دهنده و ردیاب چهره استفاده می‌کند. با قرار گرفتن کاربر در زاویه دید دوربین، سیستم چهره کاربر را تشخیص داده و مناسب بودن چهره از نظر حالت قرارگیری را بررسی می‌نماید. تا زمانی که چهره از زاویه دید دوربین خارج نشود و یا تصویر چهره‌ی کاربر به شکلی مسدود نگردد، این ردیابی از چهره ادامه می یابد.

در این مقاله تشخیص چهره به روش "ویدئو به تصویر" انجام می‌گیرد. در این شیوه هنگام ثبت نام دو نمونه ویدئویی از کاربر دریافت شده و تأیید هویت در مراجعات بعد با مقایسه یک تصویر با این دو ویدئو انجام می‌پذیرد. این روش جهت کاهش نیاز به پهنای باند شبکه انجام می‌گیرد. جهت پیاده سازی این روش در زمان ثبت نام دو ویدئو براساس الگوهای زیر از کاربر دریافت می‌گردد :

الف) در هنگام خواندن یک متن ۲۰۰ کلمه ای از نمایشگر

ب) در هنگام تایپ یک متن توسط کاربر

این دو حالت در شکل ۳ نشان داده شده است. در هر یک از حالت‌های مذکور ۳ ثانیه تصویر گرفته می‌شود که با توجه به سرعت دوربین وب دارای تعداد فریم‌های مختلفی می‌باشد.



شکل۳- الف) دانشجو در حال خواندن ب) دانشجو در حال تایپ

فریم‌های ویدئوی حالت اول در بردار T1 و فریم‌های ویدئوی حالت دوم در بردار T2 قرار داده می‌شوند. جهت تأیید هویت یا ردیابی کاربر در مراجعات بعد، یک ویدئو به مدت ۳ ثانیه از کاربر دریافت شده و توسط قطعه برنامه‌ای که بر روی سرویس‌گیرنده نصب گردیده بهترین فریم آن از نظر حالت چهره، روشنایی و کیفیت تصویر انتخاب وV نامیده می‌شود. فریم V به سرویس‌دهنده ارسال شده و با دو بردار T1 و T2 مقایسه می‌گردد. استراتژی مقایسه فریم V با فریم های الگوی T1 و T2 از طریق مقایسه فریم V با تمام فریم‌های T1و T2 می باشد. حاصل این مقایسه دو بردار ارزش SA و SB می باشد:

$S_A=\{S_{A1},S_{A2},\ldots,S_{AN}\}$
$S_B=\{S_{B1},S_{B2},\ldots,S_{BN}\}$

در دو معادله بالا SAi نشان دهنده‌ی میزان تشابه iامین فریم از SA و فریم V می‌باشد. نتیجه نهایی مقایسه فریم های T1 و T2 با فریم V به صورت زیر بدست می‌آید:

$$S_m = \max\{\max(S_A) , \max(S_B)\} \quad \text{معادله(1)}$$
$$=\max\{\max\{S_{A1},S_{A2},\ldots,S_{AN}\},\max\{S_{B1},S_{B2},\ldots,S_{BN}\}\}$$

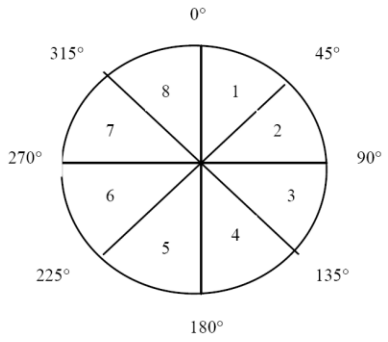
در صورتی که در معادله(۱) Sm از یک حد آستانه مشخص بالاتر باشد نتیجه مقایسه مثبت و در غیر این صورت نتیجه منفی می‌باشد. حد آستانه ذکر شده با توجه به دقت مورد انتظار از سیستم تعیین می‌شود و می‌تواند متغیر باشد.

۴-۴ . زیر سیستم تشخیص الگوی حرکات ماوس

الگوی حرکات ماوس امضایی است که بر اساس ویژگی‌های حرکت ماوس بدست می‌آید. دریافت الگوی حرکات ماوس به ابزار جدیدی نیاز ندارد، در طول کل جلسه انجام می‌پذیرد و به صورت غیرتعاملی با کاربر بدست می‌آیند[7]. حرکت ماوس ویژگی‌های زیادی دارد که برای تجزیه و تحلیل‌های بعدی استخراج می‌شوند، ازجمله: سرعت و شتاب حرکت نشانگر ماوس، جهت حرکت ماوس، دامنه ارتعاشات دست، میزان استفاده از دکمه چرخان ماوس، فرکانس راست کلیک و چپ کلیک و زمان بیکاری ماوس[7,15]. سرعت نشانگر ماوس، فاصله‌ای است که بوسیله نشانگر در طول یک دوره زمانی ثابت طی می شود. شتاب بصورت تفاضل بین سرعت لحظه‌ای و سرعت اندازه گیری شده در طی دوره زمانی قبلی محاسبه می‌شود. پارامتر لرزش دست، میزان نوسان نشانگر ماوس را نشان می‌دهد.

جمع‌آوری داده‌ها بوسیله یک زیربرنامه پس‌زمینه و مخفی از کاربر انجام می‌گیرد. هنگامی که کاربر با ماوس کار می‌کند، نوع حرکت و زمان انجام آن بر حسب میلی ثانیه محاسبه شده و در بانک اطلاعات مربوط به کاربر ذخیره می‌گردد. همچنین مختصات طول و عرض نشانگر ماوس روی صفحه ثبت می‌شود. سپس در صورت نیاز به تأیید هویت از طریق ماوس، بر روی داده-ها پردازش‌هایی صورت گرفته و در گراف‌های مختلف نمایش داده می‌شوند. هر نمودار بوسیله اندازه، طول، شتاب، انحنا و غیره توضیح داده می‌شود.

۸ جهت برای حرکت ماوس مطرح می‌شود که درشکل ۴ نشان داده شده است جهت‌ها از ۱ تا ۸ نامگذاری شده‌اند.



شکل۴- جهات مختلف حرکات ماوس

هر یک از این ۸ جهت مجموعه‌ای از حرکات ماوس که در یک ناحیه ۴۵ درجه است را پوشش می‌دهد. فرض کنید کاربر ماوس را در ناحیه صفر تا ۴۵ درجه حرکت می‌دهد، برای مسافت طی شده سرعت متوسط محاسبه خواهد شد. به همین ترتیب میانگین سرعت و متوسط مسافت طی شده در یک زمان خاص، در هر ۸ ناحیه محاسبه می‌گردد. این اطلاعات در مجموع اجزای الگوی حرکات ماوس کاربر را تشکیل می‌دهند.

یکی از پارامترهایی که بر دقت و صحت ردیابی ماوس موثر است، وضوح تصویر[۱] صفحه نمایش است. اگر الگو در وضوح تصویر خاصی پردازش شده باشد و فرآیند ردیاب بر روی وضوح تصویر دیگری محاسبه شده باشد، این کار طیف وسیعی از اطلاعات جمع آوری شده را تحت تاثیر قرار خواهد و روی نتایج منعکس می‌شود. یکی دیگر از پارامتر ها سرعت اشاره گر ماوس سیستم عامل و تنظیمات شتاب آن می‌باشد؛ هر گونه تغییر در این تنظیمات بر روی شکل‌های محاسبه شده، و در نتیجه، روی رفتار کاربر تاثیر خواهد گذاشت.

۴-۵ . زیر سیستم تشخیص الگوی تایپ

الگوی تایپ یک روش بیومتریک رفتاری است که مشابه الگوی حرکات ماوس به ابزار جدیدی برای بدست آوردن داده‌ها نیاز ندارد. جهت بدست آوردن الگوی تایپ، فواصل زمانی ضربات وارد شده به صفحه کلید[۲] در هنگام تایپ کاربر ارزیابی شده و به شکل امضایی برای شخص مورد نظر بدست می‌آیند. این روش مبتنی بر این حقیقت می‌باشد که هر کاربر الگوی تایپ خاص خود را دارد و معمولاً در تلفیق با روش‌های دیگری به عنوان روش تقویت کننده استفاده می‌شود. برخی ویژگی‌هایی که جهت ارزیابی الگوی تایپ مورد استفاده قرار می‌گیرند عبارتند از: مدت زمان پایین نگه داشتن کلید، وقفه بین ضربه‌های وارد شده به صفحه کلید، سرعت کلی تایپ و غیره. فشار دادن و بالا و پایین نگه داشتن کلید در زبانهای برنامه نویسی مدرن به آسانی قابل تشخیص است. بنابراین به سادگی می توان با توجه به زمان فشار دادن و رها کردن کلید، فاصله زمانی فشار دادن یک کلید را محاسبه نمود. گاهی لازم است برای هر کاربر بیش از یک الگو ثبت گردد چرا که الگو بستگی به چیدمان صفحه کلید، روحیه یا محیط کار دارد.

جهت تحلیل الگوی تایپ روش‌های متعددی وجود دارد مانند: تکنیک‌های منطق فازی، روش‌های آماری و شبکه‌های عصبی. همانطور که در [16] نشان داده شده است روش‌های آماری بیشترین دقت را دارند. دو ویژگی اصلی که از اعمال کاربر دریافت می‌گردد عبارتند از: الف) کد کلید: کد اسکی کلید فشرده شده. ب) فاصله‌ی زمانی بین اعمال: این پارامتر فاصله‌ی زمانی بین تایپ دو کلید متوالی را نشان می‌دهد. به این فاصله زمانی digraph گفته می‌شود. فاصله‌ی زمانی مذکور وابسته به طرحبندی صفحه کلید و سخت افزاری است که جهت جمع‌آوری داده از آن استفاده می شود[10,16]. به همین علت هدف این راهکار این است که معماری‌های برگزیده برای تحلیل الگوی تایپ، مشتق از مشخصه-های ماشین و عوامل تاثیرگذار بر نحوه‌ی عملکرد کاربر باشد. لذا نسبت بازه‌ی زمانی را به کل زمان سپری شده برای تایپ کامل کلمه را به عنوان digraph در نظر می‌گیریم. بنابراین خواهیم داشت:

بردار مرجع $R=(r_1 ,r_2 ,r_3 , \dots , r_N)$

برداری با طول N شامل diagraphهای تولید شده از یک کلمه به طول N+1 که هنگام الگوبرداری از کاربر ایجاد می‌گردد.

بردار تست $U=(u_1 , u_2 , \dots , u_N)$

برداری با طول N از کلمه به طول N+1 که هنگام تأیید هویت و ردیابی کاربر و در حین تایپ ایجاد می‌گردد. سپس این دو بردار با معیارهای مشخصی با یکدیگر مقایسه می‌شوند که از ذکر این معیارها بدلیل کمبود فضا خودداری می‌شود. معیارهای انتخابی بر این اساس برگزیده شده‌اند که میزان FAR وFRR را به حداقل برسانند یعنی دقت بیشتر و خطای کمتر. حاصل این مقایسه نتیجه تأیید هویت کاربر را مشخص می‌نماید.

۴-۶ . محاسبه پهنای باند مورد نیاز

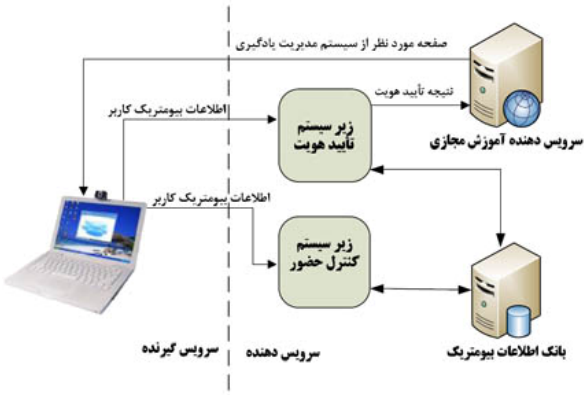
در این مقاله پیشنهاد شده که اطلاعات بیومتریک کاربر در سمت سرویس‌دهنده پردازش شود. به همین جهت کلیه اطلاعات بیومتریک کاربر به سمت سرویس‌دهنده ارسال می‌شود. جهت ردیابی دقیق کاربر، داده‌های بیومتریک در بازه‌های زمانی ۲۰ ثانیه به سرویس‌دهنده ارسال می‌گردد. در این صورت اگر هر تصویر استخراج شده به طور متوسط ۱۰۰ کیلو بایت حافظه نیاز داشته باشد، در هر دقیقه ۳۰۰ کیلو بایت اطلاعات مربوط به تصویر چهره

---
۱ Resolution
۲ KeyStroke Dynamics

به سمت سرویس‌دهنده ارسال می‌گردد. با توجه به اینکه اطلاعات دریافت شده از ماوس و صفحه کلید صرفاً اطلاعات متنی است، در دقیقه کمتر از ۱۰۰ کیلو بایت می‌باشد و در مجموع پهنای باند مورد نیاز به طور متوسط ۴۰۰ کیلو بایت در دقیقه است.

۵- معماری سیستم

در مدل ارائه شده پردازش داده‌های بیومتریک کاربر و ثبت الگو در سمت سرویس‌دهنده انجام می‌گیرد. همانطور که قبلاً ذکر گردید این روش از نظر امنیت، تطبیق‌پذیری و پردازشی شکل بهتری خواهد داشت. زیربرنامه‌های تأیید هویت و کنترل حضور دو سیستم مجزا بوده و هر دو بر روی سرویس‌دهنده یادگیری الکترونیکی قرار دارند. ابزارهای مورد نیاز جهت استفاده از سیستم، رایانه شخصی و دوربین وب می‌باشد. در این صورت می‌توان هر سه بیومتریک ذکر شده را از کاربر دریافت نمود. مدل ارائه شده به شکلی طراحی گردیده که قابلیت اضافه شدن به سیستم‌های مدیریت یادگیری متن باز و سازگار شدن با آنها را داشته باشد. در شکل ۵ معماری مدل پیشنهادی نشان داده شده است.



شکل۵- معماری مدل پیشنهادی

۶- پیاده سازی

در این مقاله مسئله کنترل دسترسی و حضور با استفاده از چارچوب BioWebAuth[1] انجام می‌گیرد. BioWebAuth یک چارچوب نرم‌افزاری متن باز جاوا[2] است که به منظور فراهم کردن تأیید هویت مبتنی بر وب هنگام ورود بوسیله نرم افزار یا دستگاه بیومتریک، استفاده می‌گردد. BioWebAuth توسعه یافته یک سیستم تأیید هویت مبتنی بر وب است که سرویس تأیید هویت مرکزی[3] (CAS) نامیده می‌شود[2,15]. سیستم CAS در ابتدا در دانشگاه ییل (Yale) توسعه یافته و بعد از آن تحت حمایت انجمن علاقمندان به معماری جاوا[4] (JA-SIG) قرار گرفت[15].

هدف اصلی استفاده از CAS این بوده که قابلیت تأیید هویت بیومتریک به سرویس تأیید هویت مرکزی اضافه گردد تا امکان استفاده از زیر ساخت‌های ارائه شده توسط CAS وجود داشته باشد. BioWebAuth یک مکانیزم دسترسی مبتنی بر بیومتریک را ارائه می‌دهد؛ LMS با استفاده از این مکانیزم ورود دانشجو به سیستم را کنترل کرده و هویت واقعی او را تشخیص می‌دهد. BioWebAuth به ما اجازه می‌دهد برای کنترل دسترسی انواع بیومتریک‌ها را با هم ترکیب نماییم. انتخاب نهایی ما برای فرآیند تأیید هویت و کنترل حضور بر اساس بیومتریک فیزیکی چهره و دو بیومتریک رفتاری الگوی حرکات ماوس و الگوی تایپ است[2,4].

سیستم‌های مدیریت یادگیری الکترونیکی متن باز مانند Moodle، ILIAS و Claroline نمونه‌های شناخته شده‌ای از برنامه‌های کاربردی وب هستند که قادر به تأیید هویت بر اساس CAS هستند. ما از سیستم Claroline برای نشان دادن قابلیت استفاده[5] سیستم توسعه داده شده، استفاده می‌کنیم.

۷- ارزیابی نتایج

هدف این مقاله ارائه یک راهکار بیومتریک چندگانه جهت محاسبه میزان حضور در کلاس الکترونیکی می‌باشد. این راهکار در یک محیط آزمایشی توسعه داده شده و از یک LMS به نام Claroline جهت آزمایش الگوریتم پیشنهادی استفاده گردید. هشت دانشجو رشته کامپیوتر با استفاده از Claroline در یک کلاس الکترونیکی به مدت ۶۰ دقیقه شرکت کردند. آزمایش در یک کلاس درس معمولی انجام شد به طوری که یک کامپیوتر مجهز به دوربین وب برای هر دانشجو وجود داشت. برای ارزیابی روش پیشنهادی از هر کاربر دو ویدئو به مدت ۳ ثانیه به عنوان الگوی چهره و از نحوه کارکردن با ماوس و صفحه کلید یک الگو ثبت گردید. در مدت ۶۰ دقیقه کلاس با توجه به الگوریتم پیشنهادی نتایج ذکر شده در جدول ۱ حاصل گردید.

در آزمایش ما از ۸ کاربر تنها ۱ کاربر نیاز به تأیید هویت مشارکتی دارند. این میزان ۱۲،۵٪ از کاربران می‌باشد. در حالی که در راهکار ارائه شده در [5] به ۱۸،۷۵٪ از کاربران درخواست تأیید هویت مشارکتی داده می‌شود. اضافه کردن بیومتریک های رفتاری الگوی حرکات ماوس و صفحه‌کلید در این راهکار باعث

[1] Biometrics For Web Authentication
[2] Open Source Java Framework
[3] Central Authentication Service
[4] Java Architectures Special Interest Group
[5] Usability

کاهش نیاز به تأیید هویت مشارکتی با استفاده از چهره می‌باشد. بنابراین در مدل درجه راحتی کاربران افزایش یافته است. مزیت دیگر این راهکار نسبت به راهکارهای دیگر نیاز به کمترین پهنای باند شبکه می‌باشد.

جدول۱- درصد حضور دانشجویان در کلاس الکترونیکی با استفاده از راهکار پیشنهادی

	میزان حضور با حد آستانه 2%	میزان حضور با حد آستانه 5%	میزان حضور واقعی
دانشجو ۱	95%	98%	100%
دانشجو ۲	99%	100%	100%
دانشجو ۳	97%	98%	100%
دانشجو ۴	96%	97%	100%
دانشجو ۵	68%	69%	70%
دانشجو ۶	79%	81%	82%
دانشجو ۷	54%	57%	60%
دانشجو ۸	8%	9%	10%

۸- نتیجه‌گیری و کارهای بعدی

خدمات توزیع شده مانند یادگیری الکترونیکی در صورتی موفق خواهد بود که قابلیت اطمینان، حریم خصوصی و امنیت، حفظ و تقویت شود. با استفاده از مدل ارائه شده عملیات مهمی مانند کنترل حضور دانشجو، ارزیابی و ردیابی، دقیقتر و کامل‌تر انجام می‌گیرد. راهکار ارائه شده حضور دانشجو مقابل کامپیوتر و شرکت او در کلاس الکترونیکی را تضمین می‌نماید. در حالی هنوز که امکان سوءاستفاده با در نظر گرفتن عامل دخالت انسانی وجود دارد. در حال حاضر تنها امنیت ۱۰۰٪ در روش‌های نظارت انسانی است. از جمله فعالیت‌های آتی در جهت بهبود عملکرد، ارائه یک مدل جهت کنترل دقیق دانشجو در آزمون الکترونیکی و به حداقل رساندن سوءاستفاده در آزمون می‌باشد. در مسیر دستیابی به این مهم، کنترل و پردازش اطلاعات جسمی، رفتاری و وضعیت روانی دانشجو می‌تواند بسیار مثمر ثمر واقع شود.

مراجع

[1] Kornelije Rabuzin, Miroslav, Mario Sajko, “E-learning: Biometrics as a Security Factor”, proceedings of the International Multi-Conference on Computing in the Global Information Technology (ICCGI'06), IEEE, 2008.
[2]http://sourceforge.net/projects/biowebauth, Biometrics for Web Authentication (BioWebAuth) project.
[3] E. González, L.E. Anido, J.L. Alba, C. García. “Is My Student at the Other Side? Applying Biometric Web Authentication to E-Learning Environments” Proceedings of Eighth IEEE International Conference on Advanced Learning Technologies (ICALT '08), pp. 551-553, July 2008.
[4] E. González-Agulla, E. Argones-Rúa, C. García-Mateo, and Ó W. M.Flórez, “Development and Implementation of a Biometric Verification System for E-learning Platforms”, EDUTECH, Computer-Aided Design Meets Computer-Aided Learning, IFIP 18th World Computer Congress, 2006, pp. 155-164.
[5] E. Gonz´alez Agulla ,E. Argones R´ua, J. Luis Alba Castro. “ Multimodal Biometrics-based Student Attendance Measurement in Learning Management Systems”. 11th IEEE International Symposium on Multimedia 2009.
[6] T. M. J. Auernheimer, B. “Biometric Authentication forWebBased Course Examinations”. In HICSS, 2007.
E. R. Weippl: “Security in E-Learning”, 2005. http://issep.uni- lu.ac.at/material/weippl.pdf .
[7] Ahmed Awad E. Ahmed and Issa Traore, “A New Biometric Technology Based on Mouse Dynamics” IEEE Transactions on Dependable and Secure Computing, Vol. 4, No. 3, pp 165-170, July-September 2007.
[8] J. L. Alba Castro, E. Gonz´alez Agulla, E. Argones R´ua,and L. Anido Rif´on. “ Realistic measurement of student attendance in LMS using biometrics”. In To appear on the Proceedings of the International Symposium on Engineering Education and Educational Technologies: EEET 2009,2009.
[9] L. Hong, A. K. Jain, and S. Pankanti, “Can Multibiometrics Improve Performance?”, Proc. AutoID '99, pp.59-64, October 2005.
[10] I.Sogukpinar, L. Yalçin, “User identification via keystroke dynamics”,Ist. Üniv. Journal of Electrical and Electronic Engineering, vol. 4, no. 1,2004, pp. 995-1005,2007.
[11] D. Gonz´alez-Jim´enez and J. Alba-Castro. “Shape-Driven Gabor Jets for Face Description and Authentication”. IEEE Transactions on Information Forensics and Security,2(4):769–780, 2007.
[12] S. Sanderson and J. Erbetta, “Authentication for secure environments based on iris scanning technology”, in IEEE Colloquium on Visual Biometrics, vol. 8, pp.1-7, 2005.
[13] Bharati, S.; Haseem, R.; Khan, R.; Ritzmann, M.;Wong, A. “Biometric Authentication System using the Dichotomy Model”, Proc. CSIS Research Day, Pace Univ., May 2008.
[14] Chinese Academy of Sciences – Institute of Automation. Database of 756 Grayscale Face Images. Available: http://www.sinobiometrics.com, Version 1.0,2003.
[15] Seno, S. Sadakane, T. Baba, Y. Shikama, T. Koui, Y. Nakaya, N. - “A Network Authentication System with Multi-Biometrics”, IEEE, vol. 3, pp 914 – 918, September 2003.
[16] Haider, S.; Abbas, A.; Zaidi, A. “A Multi-Technique Approach for User Identification through Keystroke Dynamic”s, IEEE International Conference of Systems, Man and Cybernetics, Vol 2, 2004, pp. 1336-1341.