دانشگاه علم و صنعت ایران
دانشکده مهندسی کامپیوتر

تصدیق هویت براساس نحوه کلیدزنی به روش آماری-کوواریانسی

پایان نامه برای دریافت درجه کارشناسی ارشد

مهندسی کامپیوتر - هوش ماشین و رباتیک

علی‌اصغر کاجی

استاد راهنما : دکترمرتضی آنالوئی

بهار ۱۳۸۰

تقدیم به

پدر و مادر عزیزم

که کلیهٔ موفقیت‌هایم را مدیون ایشان هستم

چکیده

استفاده از خصوصیات بیولوژیکی و رفتاری افراد جهت کنترل دسترسی‌به منابع و حفظ امنیت سیستمها به شیوه‌های مختلف، همواره مورد توجه بوده است. روشهای مبتنی بر تشخیص‌گفتار، تشخیص‌چهره، تشخیص اثرانگشت و شناسائی از روی شبکیهٔ چشم از جملهٔ معروفترین این روشها هستند. روشی که در این تحقیق موردتوجه قرارگرفته است، استفاده از ویژگیهای کلیدزنی افراد است.

در این تحقیق ویژگیهای اولیه زمان‌فشارکلیدها و مدت‌زمان بین کلیدها می‌باشد. با اخذ این ویژگیها از رشته‌های ثابت بعنوان داده‌های اولیه پس از انجام یک مرحله پیش‌پردازش اولیه با استفاده از یک کلاس‌بند ترکیبی کوواریانسی که در اینجا پیشنهاد می‌شود در کلاس‌بندی کاربران بکارگرفته‌می‌شود. این روش با حفظ سادگی روشهای آماری و سهولت پیاده‌سازی نسبت به روشهای شبکه‌عصبی، خطای کمتری نسبت به سایر روشهای آماری نشان می‌دهد. همچنین در این روش می‌توان تغییراتی را که بطور مداوم و به کندی درجهت تثبیت الگوی کلیدزنی کاربران بوجود می‌آید، دنبال کرد.

همچنین با توجه به مسئله تغییر صفحه‌کلید و نقش آن در تغییر الگوی کاربران روشی برای اعمال اثر آن در الگوی کلیدزنی کاربران پیشنهاد شده‌است.

کلمات کلیدی: کلیدزنی، تصدیق‌هویت، کلاس‌بند آماری، الگوی کلیدزنی.

سپاس خدایی را که سخنوران در ستودن او بمانند و شمارگران شمردن نعمت های او ندانند و کوشندگان حق او را گزاردن نتوانند. خدایی که پای اندیشه تیزگام در راه شناسایی او لنگ است، و سر فکرت ژرف رو به دریای معرفتش بر سنگ. صفت‌های او تعریف ناشدنی است و به وصف درنیامدنی، و در وقت ناگنجیدنی، و به زمانی مخصوص نابودنی...

(خطبه اول نهج البلاغه)

از جناب آقای دکتر مرتضی آنالوئی استاد ارجمند که همواره از راهنمائی‌های ایشان در انجام این پروژه بهره‌مند بوده‌ام سپاسگزارم،

همچنین لازم است از دوستان عزیز آقایان مهندس افشین ریاضی و مهندس بابک ناصرشریف که از نظراتشان بهره‌مند شدم و دانشجویان دوره کارشناسی ارشد کامپیوتر در سایت کارشناسی‌ارشد و آزمایشگاه شبکه‌های کامپیوتری که با کمال صبر اینجانب را در تهیه داده‌های موردنیاز یاری نمودند، کمال تشکر و تقدیر را بنمایم.

فهرست مطالب

صفحه

فهرست شکلها صفحه

فصل‌اول

فصل‌سوم

فصل‌چهارم

فصل پنجم

ضمیمه الف

فهرست جداول

صفحه

فصل دوم

فصل پنجم

مقدمه

استفاده از خصوصیات بیولوژیکی افراد جهت شناسایی و تأیید آنها در ورود و استفاده از کلیهٔ سیستمها، همواره بمنظور کنترل دسترسی و حفظ امنیت مورد توجه بوده است. روشهای تشخیص گفتار *[1]*، تشخیص چهره *[2]*، تشخیص اثرانگشت *[3]* و تشخیص از روی شبکیهٔ چشم *[4]* از جملهٔ معروفترین روشهایی هستند که از این خصوصیات در شناسائی افراد استفاده‌می‌کنند. روشی که ما موردتوجه قرار داده‌ایم، استفاده از ویژگیهای کلیدزنی افراد است.

عمومی ترین وسیلهٔ ارتباطی یک کاربر با کامپیوتر صفحه‌کلید است. در هنگام کلیدزنی می‌توان داده‌هائی نظیر زمانهای کلیدزنی، میزان فشار واردشده بر کلیدها، دمای سر انگشت کاربر و جهت ضربه‌زدن به کلیدها را علاوه بر کاراکترهای واردشده از کاربر اخذ نمود. با توجه به سخت افزار صفحه‌کلیدهای موجود عادی‌ترین داده‌های قابل اخذ از کاربر زمانهای کلیدزنی شامل زمان فشار یک کلید و زمان رهاسازی کلید می‌باشد. استفاده از این داده‌ها علاوه بر سهل‌الوصول‌بودن و عدم نیاز به تغییر سخت افزار، نسبت به سایر روشهائی که از ویژگیهای بیولوژیکی افراد استفاده می‌کنند بدلیل شفاف‌بودن و در نتیجه مخفی‌ماندن از دید کاربر دارای مزیت می‌باشد.

استفاده از این زمانها می‌تواند همراه با دو رشته کاراکتری وارد شده در هنگام ورود به سیستمها شامل شناسهٔ‌کاربر[1] و کلمه‌عبور[2] در تأیید هویت کاربران استفاده‌شده و امنیت بالاتری را تأمین می‌کند. همچنین با دریافت این داده‌ها از کاربر پس از ورود به سیستم و در هنگام کار دائمی با شناسایی کاربر

---

[1] UserID

[2] PassWord

می‌توان یک نظارت دائمی را بر سیستم اعمال نمود. در سیستم‌هائی که حفظ امنیت آنها قابل توجه می‌باشد این مراقبت می‌تواند مانع از سوءاستفادهٔ افراد غیرمجاز، پس از ترک سیستم و باز ماندن آن توسط افراد مجاز شود. در هر دو وضعیت، زمانهای کلیدزنی در دو دستهٔ قابل‌تمایز قرار می‌گیرند. زمان‌فشارکلید مدت زمان بین فشار یک کلید تا رهاکردن آن کلید می‌باشد و زمان بین دو کلید مدت‌زمان بین رهاکردن یک کلید تا فشار کلید بعدی می‌باشد. در کلیه روشهایی که برای دو موضوع شناسایی کاربران و تاییدهویت آنها مطرح می‌باشد از یک یا هر دوی این ورودی‌ها*[5][6][8]* و در بعضی از روشها نیز ورودی دیگر نظیر سختی کلیدزنی*[7]* استفاده می‌شود.

در مبحث تصدیق‌هویت بر اساس نحوه کلیدزنی، از سال ۱۹۹۰ تاکنون کارهایی انجام شده‌است که گزارش تعدادی از آنها را در دست داریم و بطورمختصر روشها و نتایج آنها را مرورمی‌کنیم.

اولین کار منتشرشده، درسال ۱۹۹۰ توسط آقایان Joyce و Gupta بوده‌است *[5]*که بعنوان یک کار پایه در تحقیقات دیگران به آن اشاره شده است. در این تحقیق با استفاده از معیار فاصله اقلیدسی یک دسته ویژگی زمانهای بین کلیدهای متوالی (Latency) با یکدیگر مقایسه‌شده‌اند. این کلاس‌بند با جمع‌آوری داده‌هایی از ۳۳ کاربر بر روی ایستگاههای کاری SUN و با دقت ۱۰میلی‌ثانیه آزمایش‌شده و دقتی در حدود ۹۵٪ را نشان داده‌است.

کار دیگری که در همان سال توسط Bleha ، Slivinsky و Hussien انجام شده‌است *[6]* بر اساس رساله دکترای آقای Bleha در سال ۱۹۸۸ بوده است. این تحقیق با استفاده از روشهای آماری و براساس یک رشته ثابت با طول زیاد و با پیش فرض اولیه توزیع نرمال برای داده‌ها انجام می‌شود و در آن یک احتمال‌گاوسی چندمتغیره بر روی ویژگی‌های زمانهای بین‌کلیدی محاسبه می‌شود. بهترین نتایج این کار دقتی در حدود ۹۶٪ و ۹۷٪ را نشان می‌دهد.

در سال ۱۹۹۷ آقایان De Ru و Ellof کلاس‌بندی را پیشنهاد کرده‌اند که در آن بطور کامل از روش فازی استفاده شده‌است. *[7]* در این کلاس‌بند از ویژگی‌های زمانهای بین‌کلیدی بهمراه ویژگی جدیدی به نام سختی‌کلیدزنی استفاده شده است. برای ویژگی‌های زمانهای بین‌کلیدی چهار مجموعه فازی و برای ویژگی سختی‌کلیدزنی یک مجموعه فازی درنظرگرفته شده است. در این روش خروجی، دسته‌بندی زوج کلید متوالی است و برای آن چهار مجموعه فازی درنظرگرفته‌شده‌است. پس از دسته‌بندی اولیه، کلیه خروجی‌ها با یک قانون فازی با یکدیگر ترکیب‌شده و یک خروجی تک مقداری بدست می‌آید. در آزمایش این کلاس‌بند داده‌ها شامل تعدادی نام کاربری متفاوت بوده و دقت ۹۲/۵٪ و ۹۷٪ بدست‌آمده‌است.

در همین سال Obaidat و Sadoun تعدادی از شبکه‌های‌عصبی را برای ایجاد کلاس‌بند مناسب بکارگرفته‌اند*[8]* . این تحقیق در ادامه کار قبلی آقای Obaidat در سال ۱۹۹۴ است که با استفاده از شبکه‌عصبی MLP صورت گرفته‌است[28]. در این تحقیق بجز ویژگی‌های زمانهای بین‌کلیدی از زمانهای فشار کلیدها (Durations) نیز استفاده‌شده‌است. براساس این دودسته ویژگی تعدادی از شبکه‌های‌عصبی آزمایش شده‌اند. برای آزمایش‌های عملی نیز تعداد زیادی نمونه در مدت‌زمان حدود دوماه بطور مداوم جمع‌آوری شده است. پس از انجام آزمایش‌هایی بهترین نتایج با شبکه‌های , Fuzzy ARTMAP RBFN, LVQ و با دقت بالای ۹۹٪ گزارش شده است.

آخرین تحقیق گزارش شده توسط Robinson و Liang در سال۱۹۹۸بوده‌است*[9]*. که با استفاده از روشهای آماری و بکاربردن یک کلاس‌بند یادگیرنده استنتاجی[3] بر روی حجم نسبتا کم داده‌ها صورت‌گرفته‌است. در اینکار نیز از دو دسته ویژگی‌های زمانهای بین‌کلیدی و زمانهای فشارکلیدها

[3] Inductive Learning Classifier