لب‌خوانی: روش جدید احراز هویت در برنامه‌های کاربردی گوشی‌های تلفن همراه اندروید

فاطمه سادات لسانی*، فرانک فتوحی قزوینی و روح‌الله دیانت

گروه مهندسی کامپیوتر و فناوری اطلاعات، دانشگاه قم، قم، ایران

چکیده

در این مقاله با استفاده از پردازش اطلاعات تصویری لب‌های کاربر، کلمهٔ عبور با استفاده از دوربین گوشی دریافت می‌شود تا با استفاده از الگوریتم‌های لب‌خوانی، حرکات لب دنبال شده و تشخیص داده شود. تشخیص تصویری کلمهٔ عبور، مانع از دزدیدن آن توسط نرم‌افزارهای واقعه‌نگار می‌شود. با این حال، سیاربودن گوشی همراه منجر به تغییر نور محیط می‌شود. در این پژوهش، روشی برای حل این چالش مطرح شده و درنهایت یک نمونه برنامه کاربردی برای اجرا در سیستم عامل اندروید طراحی و پیاده‌سازی شده است. این لب‌خوان به‌صورت غیربرخط و بدون نیاز به ارتباطات اینترنتی و وجود یک سرور خارجی، عمل شناسایی کلمهٔ عبور کاربر را انجام می‌دهد. موفقیت روش پیاده‌سازی‌شده در تشخیص، حدود هفتاددرصد است. این برنامه برای پردازش ویدیوی حرفی که ۱۰ قاب دارد، به ۳٫۸ ثانیه زمان و ۶۲۸ کیلوبایت حافظه نیاز دارد که به‌راحتی در گوشی‌های تلفن همراه امروزی قابل دسترس است.

واژگان کلیدی: احراز هویت در تلفن همراه، لب‌خوانی خودکار، تجارت سیار، ردیابی لب، اندروید

Lip Reading: a New Authentication Method in Android Mobile Phone's Applications

Fatemeh Sadat Lesani *, Faranak Fotouhi Ghazvini and Rouhollah Dianat

Computer and Information Technology Engineering, University of Qom, Qom, Iran

Abstract

Today, mobile phones are one of the first instruments every individual person interacts with. There are lots of mobile applications used by people to achieve their goals. One of the most-used applications is mobile banks. Security in m-bank applications is very important, therefore modern methods of authentication is required. Most of m-bank applications use text passwords which can be stolen by key-loggers. Key-loggers are hidden softwareto record the keys struck by users. To overcome the key-logging issue, One-Time Passwords are used. They are secure but require additional tools to be used, therefore they cannot be user-friend. Moreover, the voice-based passwords are not secure enough, since they can be heard by other people easily. In other hand, Image based passwords cannot satisfy users, cause of screen limitation in mobile phones.

In this article, a new authentication method is introduced. The password is based on user lip's motion which is received via a mobile cellphone camera. The visual information extracted from the user's lips movement forms the password. Then the lip motion is tracked to recognize the password by incorporating the lip reading algorithms. The algorithm is based on the Viola-Jones method. It combines the method with a pixel-based approach to segment lips and extract features. After segmenting the lips, some special points of Region of Interests are selected. The information extracted from lips are saved in order to act as algorithm's

* نویسندهٔ عهده‌دار مکاتبات

[DOI: 10.18869/acadpub.jsdp.14.1.3]

features. In addition, some normalizing methods are considered to normalize the features and prepare them to enter classification phase. In classification step, some known algorithms like Support Vector Machine and K-Nearest Neighbor are applied on features to recognize password and authenticate people. Visual passwords prevent key-loggers from stealing passwords. However, the mobility of a mobile user causes ambient lights to vary in different environments. In this research, a solution is designed to tackle this challenge. Finally a mobile banking application is designed and developed to run on android mobile phones platform. It incorporates a lip reader which recognizes the passwords in offline mode. The application is independent from the internet connection or a dedicated server. The implemented recognition method has achieved a 70% success rate. In this application a video capture of a letter with 10 frames could be processed in 3.8 seconds using 628 kilo bytes of memory. These resources are easily available in today's mobile phones.

Some mobile bank users tested the application to feedback about lip reading password. Most of them were satisfied when using it. They believed the lip reader is more trustable than text passwords and voice-based passwords. In addition, the user-friendliness of it, is a bit more than text password which means that the method can satisfies a mobile bank application user.

Keywords: Mobile Phone Authentication, Automatic Lip Reading, Mobile Commerce, Lip Tracking, Android

۱-مقدمه

در دنیای امروز استفاده از گوشی‌های تلفن همراه و نرم‌افزارهای آن، رشد قابل توجهی داشته است. یکی از نگرانی‌های مهم در استفاده از گوشی‌های همراه و نرم‌افزارهای آن، امنیت است. این نگرانی به‌ویژه خود را در نرم‌افزارهای بانکی بیش‌تر نشان می‌دهد؛ زیرا ناامنی این نرم‌افزارها، ضررهای اقتصادی جبران‌ناپذیری به افراد وارد می‌کند. تاکنون روش‌های مختلفی برای احزار هویت کاربران به کار گرفته شده است. معمول‌ترین روش احراز هویت، استفاده از نام کاربری و رمز عبور است. در ساده‌ترین حالت، رمز عبور افراد، شامل تعدادی حرف یا رقم است که به‌وسیله تایپ کاربر از روی صفحه کلید یا صفحه لمسی وارد گوشی می‌شود. با این حال استفاده از آن امن نیست و خطراتی مانند بدافزار واقعه‌نگار[1] آن را تهدید می‌کند.

واقعه‌نگارها برنامه‌های کوچک نرم‌افزاری و مخفی هستند که به‌صورت مخفیانه حرکات موش‌واره یا حروف واردشده توسط کاربر را تشخیص داده و با استفاده از ارتباطات اینترنتی، آن‌ها را برای شخصی که این نرم‌افزار را روی رایانه شخصی یا گوشی تلفن همراه قربانی نصب کرده است، می‌فرستند. با استفاده از واقعه‌نگار می‌توان کلمه عبور تایپ‌شده به وسیلهٔ فرد را بازیابی کرده و به اطلاعات حساب کاربری او دست یافت. این بدافزارها در گوشی‌های هوشمند نیز می‌توانند لمس‌های کاربر را از صفحه خوانده و تشخیص دهند که چه حروف یا ارقامی به‌عنوان کلمهٔ ورود، وارد شده‌اند. بنابراین روش‌های سنتی واردکردن کلمهٔ عبور که براساس تایپ کلمه عبور بود، در برابر واقعه‌نگارها امن نیستند. برای مقابله با این مشکل، روش‌های جدیدی جایگزین کلمه عبور متنی[2] شده‌اند. از جمله این روش‌ها می‌توان به کلمه عبور یک‌بارمصرف[3]، روش‌های احراز هویت مبتنی بر صوت[4]، روش‌های احراز هویت مبتنی بر تصویر[5] و روش‌های زیست‌سنجه[6] اشاره کرد.

لب‌خوانی عبارت از شناسایی حرکات لب گوینده به هنگام صحبت است. یکی از پرکاربردترین حوزه‌هایی که از لب‌خوانی استفاده می‌شود، در محیط‌های نوفه‌ای و برای اصلاح کلام‌های صوتی است؛ با این حال می‌توان از لب‌خوانی برای بالابردن امنیت کلمات عبور و جلوگیری از دزدیده‌شدن آن توسط واقعه‌نگار استفاده کرد. پیاده‌سازی لب‌خوان در گوشی‌های تلفن همراه به‌عنوان روشی برای واردکردن کلمهٔ عبور نیاز به ابزار جانبی خاصی ندارد؛ زیرا تنها ابزار لازم برای گرفتن اطلاعات در آن، دوربین است و امروزه بیش‌تر گوشی‌های تلفن همراه مجهز به دست‌کم یک دوربین با وضوح مناسب هستند. هم‌چنین امنیت این روش در مقایسه با روش صوتی ورود کلمه عبور بیشتر است؛ چون در روش صوتی، به‌دلیل گفتن کلمه عبور، امکان شنیدن آن توسط سایر افراد وجود دارد. از طرفی برخلاف روش‌های کلمهٔ عبور یک‌بارمصرف که نیاز به ابزار خاصی برای تولید کلمات عبور دارند، استفاده از آن نیاز به ابزار اضافی ندارد. به همین دلیل در این مقاله، لب‌خوانی به‌عنوان روشی جدید برای سامانه‌های احراز هویت برنامه‌های کاربردی تلفن همراه از جمله نرم‌افزارهای بانکی همراه مورد استفاده قرار گرفته است.

[1] Key Logger
[2] Text-Based Password
[3] One Time Password (OTP)
[4] Voice-Based Authentication
[5] Image-Based Authentication
[6] Biometric

[DOI: 10.18869/acadpub.jsdp.14.1.3]

در این مقاله برای نخستین‌بار از الگوریتم‌های لب‌خوانی برای احراز هویت در گوشی‌های تلفن همراه و نرم‌افزارهای بانکی همراه استفاده شده است. پیش از این، پژوهش‌هایی برای استفاده از لب‌خوانی به‌عنوان روشی برای احراز هویت در محیط‌های غیرسیار انجام گرفته بود، ولی پژوهش‌های یادشده با چالش‌های پیاده‌سازی لب‌خوان در محیط‌های سیار مواجه نبودند. به‌عنوان مثال در سال ۲۰۱۱ سامانه‌ای طراحی شد که در محیط وب، از حرکات لب گوینده برای تشخیص کلمه عبور گفته‌شده استفاده می‌کرد[1].

پیاده‌سازی لب‌خوان در گوشی‌های تلفن همراه با چالش‌هایی مواجه است. منابع موجود در گوشی‌های همراه، همواره محدودیت‌هایی دارند. این محدودیت‌ها شامل محدودیت در باتری، قدرت پردازنده و حافظه است[2] . نخستین مشکلی که در پیاده‌سازی لب‌خوان در گوشی‌های همراه وجود دارد این است که در مقایسه با رایانه‌های رومیزی، منابع کم‌تری وجود دارد. بنابراین، بلادرنگ‌بودن آن‌ها، مستلزم استفاده از روش‌هایی است که نیازمند منابع کم‌تری در مقایسه با رایانه‌های رومیزی باشند. در سال ۲۰۰۹ یونگ و همکاران، یک سامانهٔ لب‌خوان برای محیط تلفن هوشمند، طراحی و پیاده‌سازی کردند[3]. این روش ابتدا، با استفاده از اطلاعات رنگی پوست، صورت فرد را تشخیص داده و مکان چشم‌ها را تشخیص می‌دهد؛ سپس با استفاده از فاصله بین لب‌ها و چشم‌ها، لب‌های فرد را نیز تشخیص می‌دهد.

مشکل دیگر پیاده‌سازی لب‌خوان در محیط‌های سیار، جابه‌جایی افراد هنگام استفاده است[3]. جابه‌جایی باعث تغییر محیط، تغییر پس‌زمینه، و تغییر نور محیط می‌شود. بنابراین در این محیط‌ها باید تدابیری اندیشیده شود تا تغییر نور محیط، بر تشخیص کلمات، کم‌ترین تأثیر ممکن را بگذارد. در این مقاله روشی برای مقابله با حل مشکل نور در محیط‌های سیار پیشنهاد شده است؛ هم‌چنین الگوریتم‌های پیاده‌سازی‌شده به‌نحوی انتخاب شده‌اند که منابع زیادی از گوشی تلفن همراه را اشغال نکنند.

در بخش ۲ مروری بر کارهای مرتبط در زمینه ورود کلمه عبور و احراز هویت در گوشی‌های تلفن همراه انجام شده است. در بخش ۳ سامانهٔ پیشنهادی و الگوریتم‌های مورد استفاده در آن تشریح شده است. درنهایت پس از ارزیابی سامانه در بخش ۴، در بخش ۵ بحث و نتیجه‌گیری نهایی سامانهٔ لب‌خوان پیاده‌سازی‌شده آورده شده است.

[1] Fresh Password

۲-کارهای مرتبط

تاکنون روش‌های زیادی برای احراز هویت در نرم‌افزارهای گوشی تلفن همراه مورد استفاده قرار گرفته است. در ادامه به‌اختصار به این روش‌ها اشاره خواهد شد.

۲-۱-سامانه‌های احراز هویت مبتنی بر کلمه عبور یک‌بارمصرف

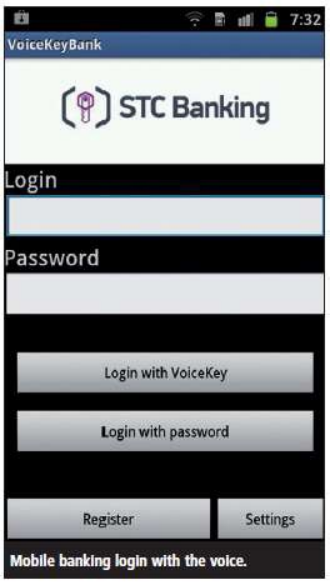
در روش کلمه عبور یک‌بارمصرف، با انجام یک سری محاسبات، هر بار یک کلمه عبور جدید[1] برای کاربر تولید می‌شود. ایده اصلی این کار نخستین‌بار توسط آقای لمپارت مطرح شد[4] . به این ترتیب حتی اگر واقعه‌نگار بتواند کلمه عبور تایپ‌شدهٔ کاربر را تشخیص دهد، نمی‌تواند از آن برای ورود به سامانه استفاده کند. با این حال یکی از مشکلاتی که در استفاده از کلمات عبور یک‌بارمصرف وجود دارد، وجود یک ابزار اضافی برای تولید کلمات عبور است. به‌عنوان مثال در سال ۲۰۱۳ روشی جدید برای تولید کلمات عبور یک‌بارمصرف با استفاده از سازوکار چالش و پاسخ[2] معرفی شد[5] . با این حال برای محاسبات مورد نیاز و ذخیره کلمات عبور جدید باید از یک میکروکنترلر جداگانه استفاده می‌شد. هم‌چنین در همان سال روش دیگری برای محاسبه کلمات عبور یک‌بارمصرف ارائه شد [6] . روش آن‌ها از برچسب‌های زمانی و اعداد ترتیبی برای محاسبات خود بهره می‌برد. درنهایت نمونه اولیه روش آن‌ها برای گوشی‌های تلفن همراه، پیاده‌سازی و آزمایش شد.

۲-۲-سامانه‌های احراز هویت مبتنی بر صوت

روش دیگر احراز هویت در سامانه‌های همراه‌بانک، استفاده از کلمات عبور مبتنی بر صوت است. مطابق شکل (۱)، در ساده‌ترین حالت، کلمه عبور فرد را به‌صورت صوتی از او می‌توان دریافت کرده و با اعمال الگوریتم‌های مختلف پردازش صوت، کلمه عبور او را شناسایی کرده و عمل احراز هویتش را انجام داد. این روش در برابر واقعه‌نگار امن است؛ ولی مشکل اصلی آن این است که کلمه عبور فرد با صدای بلند، گفته می‌شود و سایر افراد می‌توانندکلمه عبور او را شناسایی کنند. با پیشرفت فناوری و استفاده از روش‌های شناسایی زیست‌سنجه، می‌توان سامانه‌های مبتنی بر صوت را ارتقا داده و با استخراج الگوی صوتی گوینده، کلمه عبور او را شناسایی کرد[7] . نمونه‌ای از واسط کاربری این سامانه در شکل (۱) آمده است.

[2] Challenge/ Response Mechanisms

[DOI: 10.18869/acadpub.jsdp.14.1.3]



(شکل-۱): کلمه عبور مبتنی بر صوت در یک برنامه کاربردی همراه‌بانک[7]

(Figure-1): A voice-based password in a m-bank application [7]

۲-۳-سامانه‌های احراز هویت مبتنی بر تصویر

سومین دسته از روش‌های احراز هویت، مبتنی بر تصویر است. یکی از روش‌های احراز هویت مبتنی بر تصویر به این صورت است که کاربر دنباله‌ای متوالی از چند تصویر را انتخاب می‌کند و آن‌ها را به‌عنوان کلمه عبور خود به‌خاطر می‌سپارد. در مقاله‌های [8] و [9] از این روش برای احزار هویت کاربران استفاده شده است.

در سامانهٔ PassPoint، کاربر با فشردن روی یک تصویر، کلمه عبور خود را انتخاب می‌کند و سامانهٔ ناحیه‌ای کوچک در اطراف هر پیکسل انتخاب‌شده در نظر می‌گیرد [10]. به این ترتیب که کاربر چند ناحیه تصویر را انتخاب کرده و ترتیب آن‌ها را به‌خاطر می‌سپارد. با این عمل، هر زمان که کاربر بخواهد وارد سامانه شود، کلمه عبور خود را با فشردن متوالی و ترتیبی نواحی انتخابی وارد می‌کند. با این وجود، روش آن‌ها برای پیاده‌سازی در گوشی‌های تلفن همراه مناسب نیست؛ زیرا گوشی‌های تلفن همراه دارای صفحه‌هایی با اندازه کوچک هستند.

در سال ۲۰۰۳، روشی جدید برای احراز هویت برای گوشی‌های تلفن همراه پیاده‌سازی شد[11] . در روش مبتنی بر شکل آن‌ها، کاربر کلمه عبور خود را با انتخاب تعدادی متوالی از تصاویر کوچک از میان سی تصویر وارد می‌کرد. هم‌چنین در سال ۲۰۰۴، محققان این روش، کار خود را بهبود داده و به کاربر اجازه دادند که بتواند هر تصویر را بیش از یک بار انتخاب کند[12] .

(شکل-۲): سامانه شناسایی کلمه عبور Pass Point [10]

(Figure-2): The Pass Point password identification [10]

(شکل-۳): واسط کاربری ورود کلمه عبور در [11] و [12]

(Figure-3): The interface of entering password in [11] and [12]

در سال ۲۰۱۲، یک روش احراز هویت مبتنی بر تصویر برای تلفن‌های همراه مجهز به صفحه لمسی پیاده‌سازی شد [13]. سامانه آن‌ها از فشاری که کاربر به صفحه لمسی وارد می‌کند، به‌عنوان یک ویژگی زیست‌سنجه جدید استفاده کردند. در ابتدا کاربر تصویر دلخواه خود را در سامانه بارگزاری می‌کند؛ سپس سامانه تصویر بالا را به سی قسمت تقسیم کرده و کاربر یک دنباله سه الی شش‌تایی را از تصاویر بریده‌شده به‌عنوان کلمهٔ عبور خود انتخاب می‌کند. عمل انتخاب کلمه عبور با لمس صفحه گوشی انجام می‌شود. واسط کاربری این روش، در شکل (۴) آورده شده است.

همان‌طورکه در شکل (۴) مشخص است، سامانهٔ تعداد دفعات مورد نیاز برای واردکردن کلمهٔ عبور را به شخص نشان می‌دهد.

[DOI: 10.18869/acadpub.jsdp.14.1.3]

(شکل-۴): واسط کاربری ورود کلمه عبور در [13]
(Figure-4): The interface of entering password in [13]

۲-۴-سامانه‌های احراز هویت مبتنی بر زیست‌سنجه

فناوری زیست‌سنجه، مبتنی بر کلمه عبور یا شماره اختصاصی که در حافظه فرد قرار دارند نیست. این سامانه‌ها بر اساس ویژگی‌های فیزیکی و زیستی فرد و این‌که شخص، به‌درستی چه کسی است عمل احراز هویت را انجام می‌دهند. تاکنون روش‌های زیست‌سنجه مختلفی برای احراز هویت در گوشی‌های تلفن همراه به کار برده شده‌اند. برخی از ویژگی‌های استفاده‌شده شامل اثر انگشت، ویژگی‌های مرتبط به چهره، دست فرد، قرنیه، صدا و امضا است.

یکی از روش‌های معروف زیست‌سنجه، شناسایی چهره است. در سال ۲۰۱۰ پژوهشی انجام شد تا الگوریتم‌های مختلف شناسایی چهره که برای اجرا در گوشی‌های مجهز به سیستم عامل اندروید پیاده‌سازی شده‌اند، بررسی شوند[14]. نتایج نشان داد که میزان موفقیت آن‌ها در شناسایی ۹۴ درصد است و اجرای آن‌ها در بدترین حالت، ۱/۶ ثانیه طول می‌کشد.

در سال ۲۰۱۱ هندسه دست برای تشخیص هویت افراد به کار برده شد [15].روش‌های مبتنی بر هندسه دست، از ویژگی‌های هندسی و شکل ظاهری دست افراد برای شناسایی آن‌ها استفاده می‌کنند. با این حال باید توجه داشت که ویژگی هندسی دست افراد یک ویژگی منحصربه‌فرد نیست و ممکن است بیش از یک نفر دارای دست‌هایی با ویژگی‌های یکسان باشند. بنابراین استفاده از این روش در سامانه‌هایی مانند بانک که باید امنیت بالایی داشته باشند، مناسب نیست.

در سال ۲۰۱۲، از ویژگی‌های قرنیه افراد برای احراز هویت در گوشی‌های هوشمند مجهز به سامانهٔ عامل اندروید استفاده شد [16]. ۸۰ الی ۹۰ ثانیه نیاز بود تا احراز هویت یک فرد از یک پایگاه داده که شامل اطلاعات ۷۵ نفر است انجام شود. در این پایگاه داده پنج تصویر قرنیه برای هر فرد نگهداری شده بود. سامانه آن‌ها روی یک گوشی مجهز به سیستم عامل اندروید با پردازنده یک گیگاهرتزی و حافظه داخلی چهار گیگابایت آزمایش شد.

رفتارهای فرد نیز به‌عنوان پارامترهای زیست‌سنجشی مورد استفاده قرار می‌گیرند. در سال ۲۰۱۴ ترکیبی از الگوهای رفتاری فرد، هنگام کار با سامانهٔ خود به کار برده شد تا سامانه‌ای برای احراز هویت پیاده‌سازی شود [17]. در این سامانه داده‌های جمع‌آوری‌شده از صفحه‌کلید، موش‌واره و واسط گرافیکی ترکیب شده و برای ارزیابی رفتارهای فرد به کار گرفته شد. ترکیب داده‌های رفتاری فرد از منابع مختلف، به افزایش دقت سامانه کمک شایانی کرد.

در همین اواخر ویژگی‌های جدید دیگری نیز به‌عنوان معیار زیست‌سنجشی برای احراز هویت مورد استفاده قرار گرفته‌اند. به‌عنوان مثال در سال ۲۰۱۵، سامانه‌های تشخیص هویت مبتنی بر الگو از ویژگی مدت‌زمان لمس صفحه به‌عنوان یک ویژگی زیست‌سنجشی استفاده کرده‌اند تا از دزدیده‌شدن کلمه عبور فرد جلوگیری کنند. در این سامانه از الگوریتم‌های هوش مصنوعی و شبکهٔ عصبی برای تقویت سامانه بهره برده‌اند[18] .

در سال ۲۰۱۵، گروهی دیگر از پژوهش‌گران از ویژگی‌ها و رفتارهای حرکتی افراد برای به‌دست‌آوردن یک ویژگی سنجشی مناسب برای احراز هویت استفاده کردند [19]. بدن‌های مختلف و شخصیت‌های متفاوت، منجر به حرکات بدنی متفاوتی می‌شوند که استخراج این ویژگی به‌عنوان یک پارامتر برای تشخیص افراد به کار برده می‌شود.

۳-سامانهٔ پیشنهادی

به‌منظور افزایش سرعت و کاهش بار سرور، تشخیص کلمه عبور گفته‌شده توسط کاربر به‌صورت غیربرخط[1] و روی گوشی انجام می‌شود؛ سپس به‌منظور احزار هویت فرد، نام کاربری و کلمه عبور، به سرور بانک فرستاده می‌شود تا بررسی شود که آیا کلمه عبور واردشده با نام کاربری فرد هم‌خوانی دارد یا نه.

[1]Offline

[DOI: 10.18869/acadpub.jsdp.14.1.3]

لازم به ذکر است که در این سامانه نیاز نیست که تمام صورت فرد در جلوی دوربین گوشی قرار گیرد و وجود لب‌ها برای تشخیص لب‌ها و تشخیص کلمه عبور کافی است. پایگاه داده مدل‌های لب برای نویسه‌های مختلف، آموزش دیده است و به‌صورت محلی روی گوشی افراد قرار گرفته است. این پایگاه به وسیلهٔ گویندگان مختلف آموزش دیده شده است تا دقت آن بالا رود.

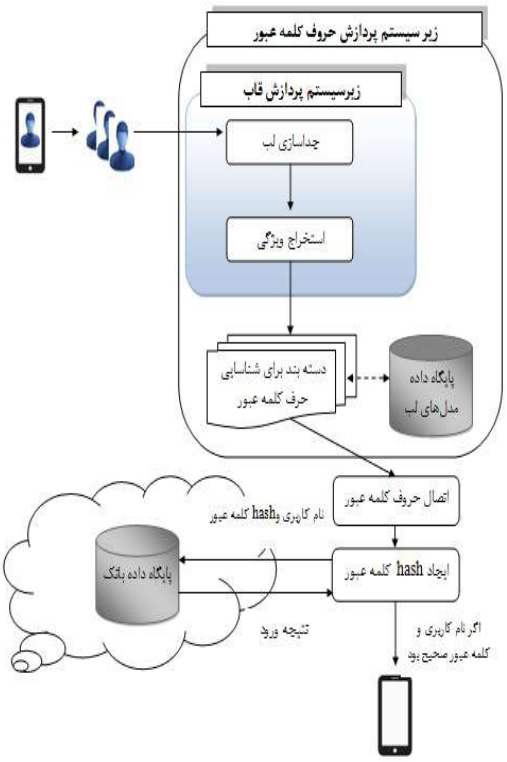
۳-۱-معماری سامانه

برای تشخیص کلمه عبور، مطابق شکل (۵) بدین‌صورت عمل می‌شود: ابتدا حروف مختلف یک کلمه عبور، به‌صورت جداگانه و توسط زیرسامانه پردازش حروف کلمه عبور تشخیص داده می‌شود. این زیرسامانه متشکل از دو زیرسامانهٔ پردازش قاب[1] و دسته‌بندی است. ابتدا ویدیوی هر حرف کلمه عبور به قاب‌های سازنده خود تجزیه شده و هر قاب وارد زیرسامانهٔ پردازش قاب می‌شود تا بخش لب در آن تشخیص داده شده و جدا شود؛ سپس لب جداشده وارد مرحلهٔ استخراج ویژگی می‌شود تا مختصات اطراف لب فرد در هر قاب مشخص شود. پس از استخراج ویژگی مربوط به هر قاب، ویژگی‌های قاب‌های یک حرف در کنار هم قرار گرفته و وارد بخش دسته‌بندی می‌شوند تا مشخص شود که ویدیوی تجزیه‌شده مربوط به چه حرفی است. به این ترتیب که فاصلهٔ ویژگی‌ها از همه طبقه‌های ذخیره‌شده در مدل‌های لب محاسبه شده و نزدیک‌ترین حرف به‌عنوان نتیجه برگردانده می‌شود.

مراحل قبل برای هر حرف کلمه عبور به‌صورت مجزا انجام شده و تک‌تک حروفی که کاربر به‌عنوان کلمه عبور، وارد کرده است، شناسایی می‌شود؛ سپس، حروف به‌ترتیب واردشده، در کنار هم قرار گرفته و کلمه عبور ورودی را می‌سازند؛ سپس چکیده مربوط به کلمه عبور، محاسبه شده و به همراه نام کاربری واردشده به سرور بانک فرستاده می‌شود تا بررسی شود که آیا نام کاربری و کلمه عبور، هم‌خوانی دارند یا نه. درصورت مثبت‌بودن پاسخ سرور بانک به برنامه کاربردی، احراز هویت شخص با موفقیت انجام شده، کاربر به صفحه اصلی برنامه هدایت می‌شود تا به انجام اعمال بانکی خود بپردازد.

۳-۲-روش کار

برای پیاده‌سازی این سامانه از الگوریتم‌های مختلفی استفاده شده است. یکی از محدودیت‌های پیاده‌سازی الگوریتم‌ها در گوشی‌های تلفن همراه، محدودیت منابع از قبیل پردازنده و حافظه است. بنابراین الگوریتم‌های پیاده‌سازی‌شده باید به حافظه معقولی برای اجرا نیاز داشته باشند. از طرفی باید زمان اجرای الگوریتم برای تشخیص کلمه عبور قابل قبول باشد. در این بخش الگوریتم‌های پیاده‌سازی‌شده معرفی خواهند شد و در بخش ۵-۱، میزان حافظه مصرفی و زمان اجرای هر الگوریتم توضیح داده می‌شود.



(شکل-۵): معماری سامانهٔ پیشنهادی
(Figure-5): The proposed system architecture

۳-۲-۱-حل مشکل تغییر نور هنگام جابه‌جایی

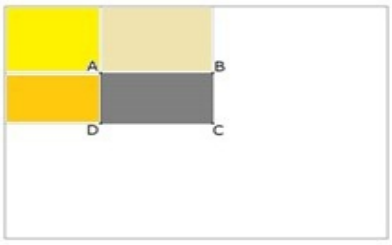
همان‌طورکه گفته شد، افراد هنگام استفاده از گوشی تلفن همراه، همواره در حال حرکت و جابه‌جایی هستند. از طرفی حتی کم‌ترین میزان لرزش دست، می‌تواند زاویه تابش نور به صفحه گوشی را تغییر داده و منجر به تغییر رنگ‌ها و میزان شدت آن‌ها در تصویر شود. در این مقاله روشی برای این مشکل در نظر گرفته شده است. برای کاهش اثر نور بر تصویر، ماتریس شدت نور تصویر برای هر قاب محاسبه شده و عملیات تشخیص لب و استخراج ویژگی روی ماتریس شدت نور قاب انجام می‌شود. مطابق فرمول (۱) ماتریس تبدیل A به روی هر پیکسل از تصویر قاب که دارای مقادیر RGB متفاوتی است، اعمال شده و مقدار شدت نور آن نقطه را محاسبه

[1] Frame

[DOI: 10.18869/acadpub.jsdp.14.1.3]

می‌کند. در این فرمول، R به‌میزان رنگ قرمز، G به‌میزان رنگ سبز و B به‌میزان رنگ آبی پیکسل اشاره دارد. هم‌چنین A، شدت نور نقطه را نشان می‌دهد.

$$A = [\,0.299 \quad 0.587 \quad 0.114\,]\begin{bmatrix}R\\G\\B\end{bmatrix} \qquad (۱)$$



(شکل-۶): محاسبه مجموع مقادیر پیکسلی یک ناحیه در روش تصاویر انتگرالی

(Figure-6): The calculation of summation of pixel values in a region in integral images method

۳-۲-۲-جداسازی لب

برای جداسازی ناحیه لب‌ها از سایر بخش‌های هر قاب، از الگوریتم ویولا و جونز[1] به نام هار[2] که در شناسایی چهره معروف است، استفاده شده است[20]. الگورتیم هار یک تصویر را به چند ناحیه تقسیم کرده و تفاوت نواحی را برای شناسایی یک شیء هدف محاسبه می‌کند. برای کاهش مقدار محاسبات مورد نیاز، از تصاویر انتگرالی[3] برای محاسبات استفاده می‌شود. تصاویر انتگرالی مجموع پیکسل‌های یک ناحیه را با استفاده از فرمول سادهٔ زیر محاسبه می‌کند:

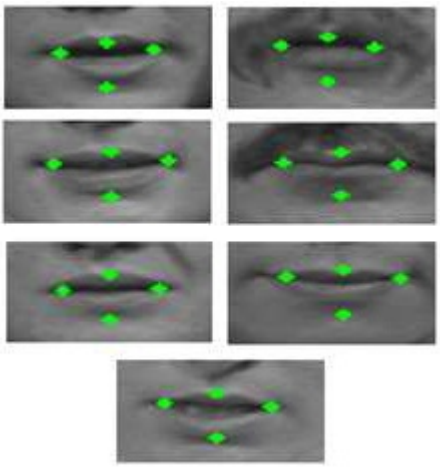
$$Sum = I(C) + I(A) - I(B) - I(D) \qquad (۲)$$

۳-۲-۳-استخراج ویژگی

پس از جداسازی ناحیه لب‌ها توسط الگوریتم هار، الگوریتم استخراج ویژگی روی هر قاب اعمال می‌شود تا مختصات نقاط اصلی اطراف لب افراد، استخراج شود. در مرحله اعمال الگوریتم هار، بزرگ‌ترین ناحیه‌ای که با الگوی تعریف‌شده هم‌خوانی دارد، به‌عنوان ناحیه دهان انتخاب می‌شود. از آن‌جا که این سامانه در گوشی تلفن همراه پیاده‌سازی می‌شود، کاهش زمان و حافظه مورد نیاز برای پردازش نقاط ضروری است. به همین دلیل در این پژوهش، مختصات چهار نقطه اصلی و اساسی لب خارجی یعنی بالا، پایین و دو طرف لب خارجی به‌عنوان منبعی برای استخراج اطلاعات مورد پردازش قرار گرفته‌اند. چند نمونه از اجرای این الگوریتم روی لب هفت گوینده در شکل (۷) نشان داده شده است.

به‌منظور استخراج ویژگی‌های اطراف لب‌ها، ابتدا مختصات دو طرف دهان محاسبه می‌شود. برای پیداکردن مختصات نقطه راست دهان، از آخرین ستون تصویر ROI شروع کرده و کم‌ترین مقدار شدت نور هر ستون با متوسط کم‌ترین شدت نورها مقایسه می‌شود. ستونی که کم‌ترین مقدار شدت خودش و ستون‌های قبلی‌اش کم‌تر از مقدار متوسط باشند، به‌عنوان نقطه راست لب انتخاب می‌شود. مشابه همین عملیات برای یافتن مختصات نقطه چپ دهان انجام می‌شود. با این تفاوت که از ستون نخست تصویر ROI شروع کرده و آن ستونی که کم‌ترین مقدار شدت نور خود و ستون‌های بعدی‌اش دارای مقداری کم‌تر از مقدار شدت نور متوسط باشند، به‌عنوان نقطه چپ دهان انتخاب می‌شود.

به‌منظور کاهش حجم محاسبات، میانگین مختصات x نقاط راست و چپ لب، به‌عنوان x نقاط بالایی و پایینی لب در نظر گرفته می‌شود. برای تعیین y این نقاط، تک‌ستونی که مختصات x آن برابر با x محاسبه شده است، مورد بررسی قرار می‌گیرد. نقطه‌ای که مقدار شدت نور آن از تمامی نقاط پایینی‌اش کم‌تر است، به‌عنوان نقطه بالای لب، و نقطه‌ای که از تمام نقاط بالایی خود دارای مقدار شدت نور کم‌تری است، به‌عنوان نقطه پایینی لب برگردانده می‌شود. در شکل (۸) مراحل استخراج نقاط از ROI رنگی نشان داده شده است.

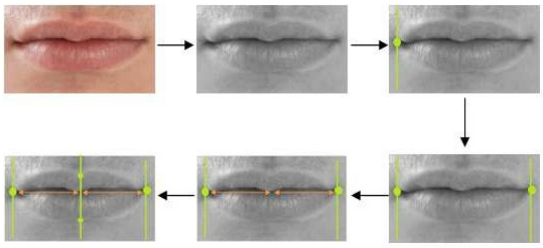


(شکل-۷): اجرای الگوریتم استخراج ویژگی روی لب ۷ گوینده

(Figure-7): Applying feature extraction algorithm on lips of 7 speakers

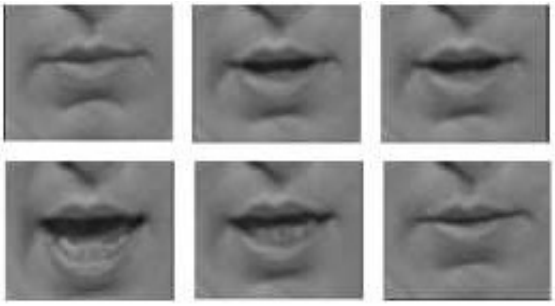
[1] Viola and Jones
[2] Haar
[3] Integral Images

[DOI: 10.18869/acadpub.jsdp.14.1.3]



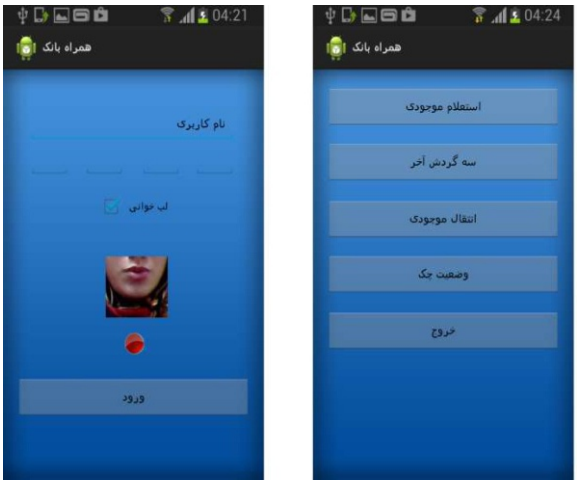
(شکل-۸): مراحل استخراج ویژگی‌ها از روی ROI رنگی لب

(Figure-8): The steps of extracting features on ROI



(شکل-۹): توالی حرکات لب یک گوینده در مجموعه داده AVLetter هنگام ادای حرف‘A’

(Figure -9): The sequence of pronouncing ‘A’ in AVLetter dataset



(شکل-۱۰): نمونه‌ای از پیاده‌سازی نمونه اولیه نرم افزار بانکی همراه‌بانک

(Figure-10): The m-bank application prototype

۳-۲-۴-دسته‌بندی و شناسایی کلمه عبور

پس از استخراج ویژگی برای هر قاب، باید ویژگی‌های استخراجی قاب‌های مختلف هر حرف، در کنار هم قرار گیرند و وارد مرحلهٔ دسته‌بندی شوند. دسته‌بند، ویژگی‌های استخراجی را بررسی کرده و حرف مرتبط با آن را شناسایی می‌کند. از آن‌جا که الگوریتم ماشین بردار پشتیبان[1] دقت بالایی دارد، برای مرحلهٔ دسته‌بندی، از الگوریتم ماشین بردار پشتیبان با هسته چندجمله‌ای برای تشخیص کلمه عبور استفاده شده است. پس از تشخیص کلمه عبور، چکیده این کلمه با استفاده از الگوریتم SHA-256 محاسبه شده و به همراه کلمه عبور به سرور بانک فرستاده می‌شود. هم‌چنین سامانه با الگوریتم k تا از نزدیک‌ترین همسایه‌ها[2] نیز مورد آزمون قرار گرفت تا میزان دقت سامانه در هر دو حالت مشاهده شود. نمونه‌ای از توالی حرکات لب یک گوینده برای ادای حرف ’A‘ در شکل (۹) آمده است.

[1] Support Vector Machine (SVM)

۳-۳-پیاده‌سازی نمونه اولیه یک نرم‌افزار بانکی مجهز به لب‌خوان در گوشی‌های هوشمند اندروید

نمونه‌ای اولیه از یک برنامه کاربردی بانکی برای اجرا در گوشی‌های مجهز به سیستم عامل اندروید ساخته شد. نمونه‌ای از این پیاده‌سازی در شکل (۱۰) آمده است. در این برنامه، کاربر نام کاربری خود را تایپ کرده، ولی برای وارد کردن رمز خود دو انتخاب دارد. درصورتی‌که گزینه "لب‌خوانی" را انتخاب کند، می‌تواند با حرکات لب خود، تک تک حروف رمز را بدون هیچ صدایی و تنها با حرکات لب خود بگوید. دوربین گوشی، ویدیوی حروف بیان‌شده را ضبط کرده و مورد پردازش قرار می‌دهد؛ سپس کلمه عبور بیان‌شدهٔ کاربر را تشخیص داده و چکیده آن را به همراه نام کاربری، به سرور بانک می‌فرستد. درصورت موفقیت در ورود، شخص وارد صفحه دوم(تصویر سمت راست) شده و می‌تواند عملیات مختلف را انجام دهد. لازم به ذکر است که در این سیستم، فرض شده است که کلمات عبور چهار نویسه‌ای هستند. در صورت عدم انتخاب گزینه "لب‌خوانی" کاربر می‌تواند به روش سنتی و با تایپ کلمه عبور، وارد برنامه کاربردی بانکی خود شود. این گزینه در مواقعی که نور محیط برای استفاده از لب‌خوان مناسب نباشد، به کار می‌رود.

۴-نتایج ارزیابی

نمونه اولیه این برنامه با مجموعه دادهٔ انگلیسی AVLetter آزمایش شد که در آن ده گوینده هر یک از حروف الفبای انگلیسی را سه بار تکرار کرده‌اند[21] . برای آزمون این برنامه، هفت گوینده از ده گوینده که دارای ویژگی‌های چهره متفاوتی بودند انتخاب شدند. تفاوت‌ها در اندازه و شکل لب‌ها، رنگ

[2] K- Nearest Neighbor (KNN)

[DOI: 10.18869/acadpub.jsdp.14.1.3]

پوست، سرعت گوینده و دارا بودن ریش و سبیل بودند. هم‌چنین مجموعه حروف B، F، H و Z از الفبای انگلیسی برای آموزش و آزمون انتخاب شدند. درنهایت نمونه اولیه برنامه روی گوشی سامسونگ گلکسی اس-۳ مینی با پردازنده دوهسته‌ای ۱ گیگاهرتز و حافظه ۱ گیگابایت مورد آزمون قرار گرفت.

برای آزمون و ارزیابی لب‌خوان، دو سامانهٔ لب‌خوان پیاده‌سازی شد. در سامانهٔ نخست از ماشین بردار پشتیبان به‌عنوان دسته‌بند استفاده شد و در سامانهٔ دوم، الگوریتم k تا از نزدیک‌ترین همسایه‌ها با مقدار یک به کار گرفته شد. دقت این دو سامانه در جدول (۱) آمده است. میزان موفقیت الگوریتم لب‌خوانی پیاده‌سازی‌شده روی این مجموعه داده در سامانهٔ یک حدود ۶۹ و در سامانهٔ دو حدود ۶۳ درصد است.

حروف	سامانه اول	سامانه
حرف B	75	50
حرف F	50	50
حرف H	50	50
حرف Z	100	100
متوسط	**68.75**	**62.5**

(جدول-۱): نتایج ارزیابی لب خوان. سامانه اول با ماشین بردار پشتیبان و سامانه دوم با k تا نزدیک‌ترین همسایه

(Table-1): The lip readers evaluation

۴-۱-زمان و حافظه مصرفی سامانه

دو عامل مهم روی حافظه مصرفی و زمان اجرای نرم‌افزارهای کاربردی سیستم عامل اندروید تأثیر دارد: الگوریتم‌های به‌کارگرفته‌شده و مشخصات سخت‌افزاری سیستم. به‌دلیل محدودیت قدرت پردازنده و میزان حافظه، توجه به این دو منبع از اهمیت ویژه‌ای برخوردار است، در غیر این صورت اجرای برنامه با شکست مواجه می‌شود.

زمان اجرا و حافظهٔ مصرفی مراحل مختلف اجرای برنامه در دو سامانه در جدول (۲) آمده است. در هر مرحله، متوسط حافظه مورد نیاز پس از انجام آزمایش‌های مختلف آورده شده است. هم‌زمان با ضبط هر ویدیو، قاب‌های مخلتف جداسازی شده و ناحیه لب در هر یک تشخیص داده می‌شود تا ویژگی‌های اطراف لب شناسایی شود. اجرای این مرحله به ۰/۲۵ کیلوبایت حافظه و ۱۱۱ میلی‌ثانیه زمان نیاز دارد. بنابراین به‌طور متوسط برای پردازش یک حرف که حاوی ده قاب است، به ۱/۱ ثانیه زمان نیاز داریم؛ ولی میزان حافظه مورد نیاز همان ۰/۲۵ کیلوبایت است؛ زیرا حافظه مصرفی برای پردازش هر قاب پس از استفاده آزاد می‌شود. هم‌زمان با پردازش هر قاب، نقاط استخراجی روی صفحه گوشی فرد نشان داده می‌شود. حافظهٔ مورد نیاز برای اجرای الگوریتم ماشین بردار پشتیبان(سامانه نخست) ۶۲۸ کیلوبایت و زمان مورد نیاز برای اجرای آن ۲,۷ ثانیه می‌باشد. درحالی‌که حافظه مورد نیاز برای اجرای الگوریتم k تا نزدیک‌ترین همسایگی(سامانه دوم) ۱۳۶۱ کیلوبایت و زمان مورد نیاز برای اجرای آن دو ثانیه است. درنهایت محاسبه چکیده کلمه عبور، به یک کیلوبایت حافظه و دوازده میلی‌ثانیه زمان برای اجرا نیاز دارد.

(جدول-۲): زمان اجرا و حافظه مصرفی فازهای مختلف اجرای برنامه در دو سامانه

(Table-2): The running time and consumed memory of different steps in two lip readers

	سامانه اول		سامانه دوم	
مرحله	**زمان**	**حافظه**	**زمان**	**حافظه**
جداسازی لب و استخراج ویژگی هر قاب	111	0.25	111	0.25
دسته‌بندی	2727	628.41	2021	1361
محاسبه چکیده کلمه عبور	12	1.13	12	1.13
ارسال اطلاعات به بانک و دریافت پاسخ	بستگی به شبکه دارد	بستگی به شبکه دارد	بستگی به شبکه دارد	بستگی به شبکه دارد
مجموع	**3849**	**628.41**	**3143**	**1361**

درنهایت در صورتی که به‌طور متوسط هر حرف کلمه عبور دارای ده قاب باشد، زمان لازم برای پردازش هرحرف در سامانهٔ نخست حدود ۳,۸ ثانیه و در سامانهٔ دوم حدود ۳,۱ ثانیه می‌شود که از زمان مورد نیاز برای سامانهٔ نخست کم‌تر است. هم‌چنین از آن‌جا که حافظه مصرفی هر فاز در پایان آن مرحله آزاد می‌شود، درنهایت حافظه مورد نیاز برنامه برای پردازش یک حرف برابر با بیشترین مقدار حافظه مصرفی مراحل است که در سامانه نخست برابر ۶۲۸ کیلوبایت و در سامانه دوم حدود ۱/۳ مگابایت است که بیشتر از سامانه نخست است. درنتیجه سامانه دوم به زمان کم‌تری برای اجرا نیاز دارد؛ ولی چون در مقابل، دقت کم‌تری نیز دارد و حافظه مورد نیاز آن بیشتر است برای استفاده در نرم‌افزار کاربردی برتری کم‌تری دارد.

[DOI: 10.18869/acadpub.jsdp.14.1.3]

۴-۲-نظرسنجی درباره پذیرش سامانه

در این مقاله، یک نظرسنجی از افراد مختلف انجام گرفت تا مشخص شود نظر افراد درباره سه روش مختلف واردکردن کلمه عبور در برنامه‌های کاربردی تلفن همراه چیست.

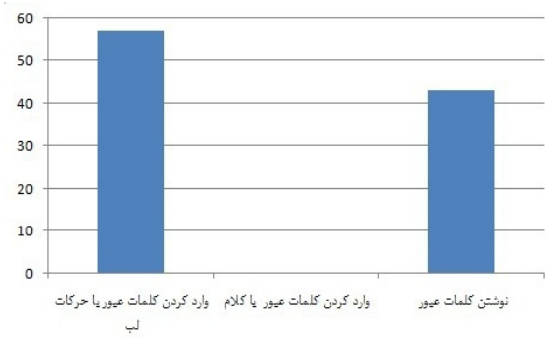
الف. کاربر کلمه عبور را با حرکات لب گفته و سامانه به‌صورت خودکار و با استفاده از الگوریتم‌های لب‌خوانی، کلمه عوبر را شناسایی می‌کند.

ب. کاربر کلمه عبور را به‌صورت صوتی گفته و سامانه کلمه عبور را با استفاده از الگوریتم‌های پردازش صوت تشخیص می‌دهد.

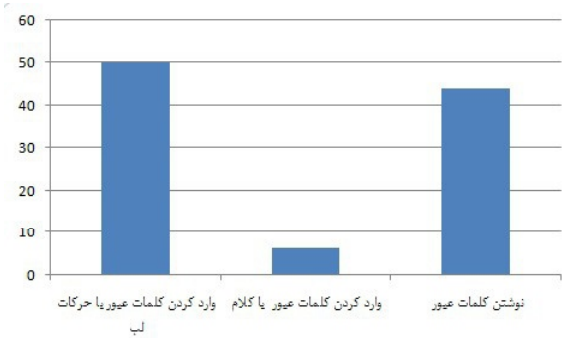
ج. کاربر کلمه عبور را تایپ کرده و به‌صورت مستقیم وارد سیستم می‌کند.

۵۸ نفر در نظرسنجی شرکت کردند. حدود ۵۷ درصد آن‌ها معتقد بودند که وارد کردن کلمات عبور با استفاده از حرکات لب، در مقایسه با دو روش دیگر، از اعتماد بیشتری برخوردار و امن‌تر است. با این وجود، ۴۳ درصد باقی‌مانده وارد کردن کلمات از طریق صفحه‌کلید را امن‌تر دانسته و هیچ کدام به روش‌های مبتنی بر صوت اعتماد نداشتند. شکل (۱۱) نتایج نهایی اعتماد افراد به سه روش واردکردن کلمه عبور را نشان می دهد.

در سؤالی دیگر از افراد پرسیده شد که کدام‌یک از سه روش را کاربر پسندتر می دانند و استفاد از آن را ترجیح می‌دهند؟ نیمی از آن‌ها ورود کلمه عبور با استفاده از حرکات لب را کاربر پسندتر می‌دانستند، ۴۴ درصد از آن‌ها روش نوشتن و تایپ کلمه عبور و تنها ۶ درصد از آن‌ها روش صوتی ورود کلمه عبور را ترجیح می‌دادند. شکل (۱۲) نتایج نهایی این نظرسنجی را نشان می‌دهد.



(شکل- ۱۱): میزان اعتماد کاربران به سه روش ورود کلمه عبور
(Figure-11): User trustiness on three password types



(شکل-۱۲): نتایج کاربر پسند بودن سه روش ورود کلمه عبور
(Figure-12): The user-friendliness of three password types

۵-بحث و نتیجه‌گیری

در این مقاله، روشی جدید برای احراز هویت کاربران در نرم‌افزارهای گوشی‌های مجهز به سیستم عامل اندروید معرفی شد. یکی از نگرانی‌های اصلی در پیاده‌سازی نرم‌افزارهای بانکی، امنیت آن‌ها در برابر نرم‌افزارهای مخرب مانند واقعه‌نگارها است تا از دزدیده‌شدن کلمه عبور کاربران جلوگیری شود.

روش لب‌خوانی در مقایسه با سایر روش‌های احراز هویت در گوشی‌های تلفن همراه، مزایایی دارد. روش کلمه عبور یک‌بارمصرف نیاز به ابزار اضافی برای تولید کلمات عبور جدید دارد. روش‌های مبتنی بر صوت به‌دلیل امکان شنود امنیت پایینی دارد. پیاده‌سازی روش‌های احراز هویت مبتنی بر تصویر در گوشی‌های تلفن همراه به‌دلیل محدودیت اندازه صفحه، مناسب نیست. استفاده از روش‌های احراز هویت مبتنی بر ویژگی‌های زیستی مانند قرینه، به زمان زیادی برای اجرا نیاز دارد. هم‌چنین برخی از روش‌های احراز هویت زیست‌سنجه مانند تشخیص چهره، با استفاده از برخی روش‌ها فریب می‌خورد. روش لب‌خوانی هیچ‌کدام از مشکلات روش‌های بالا را نداشته و برای جلوگیری از دزدیدن کلمه عبور توسط واقعه‌نگارها، بسیار مناسب است.

در سامانه‌های احراز هویت مبتنی بر لب‌خوانی، می‌توان با استفاده از دنبال‌کردن حرکات لب و پردازش ویدیو، کلمه عبور کاربر را شناسایی کرد. در این مقاله روشی جدید و ساده با ترکیب الگوریتم معروف ویولا جونز و یک روش مبتنی بر پیکسل برای جداسازی لب و استخراج ویژگی به کار گرفته شد. هم‌چنین ترکیبی جدید از روش‌ها برای پیاده‌سازی یک نمونه اولیه از نرم‌افزار در گوشی‌های هوشمند ارائه شد. موفقیت نرم‌افزار در تشخیص کلمات عبور حدود ۷۰ درصد

بود. با بهبود الگوریتم‌های هر مرحله می‌توان دقت نرم‌افزار را بالا برد.

مشکلات مختلفی در زمینه پیاده‌سازی لب‌خوان وجود دارد. به‌عنوان مثال، رنگ پوست صورت افراد که برای تشخیص ناحیه صورت به کار می رود، متفاوت است؛ یا رنگ لب افراد با هم تفاوت داشته و تشخیص لب را با مشکل مواجه می‌سازد. از طرفی وجود موی سر یا ریش در برخی از الگوریتم‌های تشخیص لب، ایجاد مشکل می‌کند. هم‌چنین یکی از محدویت‌های تشخیص ناحیه لب، وجود شکاف در کام است. برای غلبه بر این مشکل، در سال ۲۰۱۱ روشی توسط لی ارائه شده است [22] .

از طرفی همان‌طور که درقبل گفته شد، محدودیت منابع و تغییرات نور محیط در اثر جابه‌جایی نیز از دیگر مشکلات پیاده‌سازی لب‌خوان در محیط‌های سیار است. به همین دلیل رسیدن به درصد بالای تشخیص در این محیط‌ها، نیازمند بهینه‌سازی الگوریتم‌ها و به‌کارگیری روش‌هایی است که مشکل تغییرات نور را در این محیط‌ها برطرف کند. در این مقاله روشی برای غلبه بر تغییرات نور در گوشی‌های همراه معرفی شد. با این وجود می‌توان روش‌های دیگری را نیز در ترکیب با این روش به کار برد تا تأثیر نور محیط بر تصویر به کم‌ترین میزان ممکن برسد.

دو نمونه از سامانه لب‌خوان پیاده‌سازی شده و زمان و حافظه مصرفی آن‌ها اندازه‌گیری شد. سامانه‌ای که از ترکیبی از الگوریتم ویولا جونز برای جداسازی لب، روشی برای استخراج ویژگی و دسته‌بند ماشین بردار پشتیبان ساخته شده بود، نتایج دقیق‌تری نسبت به سامانه مشابهی که از دسته‌بند دیگری استفاده می‌کرد، داشت(K تا نزدیک‌ترین همسایگی). هم‌چنین حافظه مصرفی سامانه نخست نسبت به سامانه دوم کم‌تر بوده و برای پیاده‌سازی در گوشی‌های هوشمند که نسبت به رایانه رومیزی حافظه کم‌تری دارند، مناسب‌تر است. سامانه دوم به زمان کم‌تری برای اجرا نیاز داشت؛ ولی به‌دلیل دقت کم‌تر در تشخیص، برای به‌کارگیری در این محیط مناسب نیست.

6-Refrences ۶-مراجع

[1]K. Alghatbar, "Real-time algorithmic design for silent pass lip reading authentication system," *International Journal of the Physical Sciences,* vol. 6, no. 7, pp. 1665-1672, 2011.

[2]S. Chai, "Mobile Challenges for Embedded Computer Vision," in *Embedded Computer Vision*, B. Kisačanin, S. Bhattacharyya, and S. Chai, Eds. (Advances in Pattern Recognition: Springer London, 2009, pp. 219-235.

[3]K. Young-Un, K. Sun-Kyung, and J. Sung-Tae, "Design and implementation of a lip reading system in smart phone environment," *in Information Reuse & Integration,IEEE International Conference on,* 2009.

[4]L. Lamport, "Password Authentication with Insecure Communication," *Comm. ACM,* vol. 24, no. 11, pp. 770-772, 1981.

[5]L. Gong, J. Pan, B. Liu, and S. Zhao, "A novel one-time password mutual authentication scheme on sharing renewed finite random sub-passwords," *Journal of Computer and System Sciences,* vol. 79, no. 1, pp. 122-130, 2013.

[6]Y. Huang, Z. Huang, H. Zhao, and X. Lai, "A new One-time Password Method," *IERI Procedia,* vol. 4, pp. 32-37, 2013.

[7]M. Khitrov, "Talking passwords: voice biometrics for data access and security," *Biometric Technology Today,* vol. 2013, no. 2, pp. 9-11, 2013.

[8]R. Dhamija and A. Perrig, "Déjà vu: A user study using images for authentication," *In: 9th USENIX Security Symposium,* 2000.

[9]S. Brostoff and M. A. Sasse, "Are passfaces more usable than passwords? a field trial investigation," *In: People and Computers XIV—Usability or Else: Proceedings of HCI,* pp. 405–424, 2000.

[10]S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N. Memon, "Authentication using graphical passwords: basic results," *In: 11th Human–Computer Interaction International (HCII),* 2005.

[11]W. A. Jansen, "Authenticating users on handheld devices," *In: Canadian Information Technology Security Symposium,* 2003.

[12]W. A. Jansen, "Authenticating mobile device users through image selection," *In: Data Security,* 2004.

[13]T.-Y. Chang, C.-J. Tsai, and J.-H. Lin, "A graphical-based password keystroke dynamic authentication system for touch screen handheld mobile devices," *Journal of Systems and Software,* vol. 85, no. 5, pp. 1157-1165, 5// 2012.

[14]D. G, X. Chao, and K. Sriadibhatla, "Face Recognition in Mobile Phones," *epartment of*

[DOI: 10.18869/acadpub.jsdp.14.1.3]

Electrical Engineering Stanford University, USA, 2010.

[15]D. S. S. A, C. S. Avila, A. MendazaOrmaza, and J. G. Casanova, "Towards Hand Biometrics in Mobile devices," *In Proceeding of BIOSIG, Darmstadt,* 2011.

[16]G. M, J. J. S. Rani, M. Ramiah, N. T. N. Babu, A. A. Fathima, and V. Vaidehi, "Mobile Authentication Using Iris Biometrics," *Published by Springer Berlin Heidelberg, Networked Digital Technologies,* vol. 294, pp. 332-341, 2012.

[17]K. O. Bailey, J. S. Okolica, and G. L. Peterson, "User identification and authentication using multi-modal behavioral biometrics," *Computers & Security,* vol. 43, pp. 77-89, 6// 2014.

[18]O. Alpar, "Intelligent biometric pattern password authentication systems for touchscreens," *Expert Systems with Applications,* vol. 42, no. 17–18, pp. 6286-6294, 10// 2015.

[19]A. Drosou, D. Ioannidis, D. Tzovaras, K. Moustakas, and M. Petrou, "Activity related authentication using prehension biometrics," *Pattern Recognition,* vol. 48, no. 5, pp. 1743-1759, 5// 2015.

[20]P. Viola and M. Jones, "Rapid object detection using a boosted cascade of simple features," *Computer Vision and Pattern Recognition, 2001. CVPR 2001. Proceedings of the 2001 IEEE Computer Society Conference on,* vol. 1, 2001.

[21]I. Matthews, T.Cootes, J. Bangham, S. Cox, and R. Harvey, "Extraction of visual features for lipreading," *IEEE Trans. on Pattern Analysis and Machine Vision,* vol. 24, no. 2, pp. 198-213, 2002.

[22]N. Lee and e. al, "Facial Landmark Extraction for Lip Tracking of Patients with Cleft Lip Using Active Appearance Model," *in HCI International 2011 – Posters' Extended Abstracts, C. Stephanidis, Editor. 2011, Springer Berlin Heidelberg,* pp. 350-354, 2011.

فاطمه سادات لسانی، در سال ۱۳۹۱ مدرک کارشناسی خود را در رشته مهندسی کامپیوتر با گرایش نرم‌افزار از دانشگاه قم دریافت و مدرک کارشناسی ارشد خود را نیز از همان دانشگاه در رشته مهندسی فناوری اطلاعات با گرایش تجارت الکترونیک در سال ۱۳۹۳ اخذ کرد. موضوع پایان‌نامه کارشناسی ارشد ایشان استفاده از فناوری لب‌خوانی برای ارتباط با واسط کاربری تلفن همراه هوشمند اندروید بوده است. وی هم‌اکنون دانشجوی مقطع دکترا در همان رشته و همان دانشگاه می‌باشد. زمینه‌های پژوهشی مورد علاقه وی پردازش سیگنال‌های تصویری، روش‌های احراز هویت هوشمند و سیستم‌های زمینه‌آگاه می‌باشد.

نشانی رایانامه ایشان عبارت است از:

aslesani@gmail.com

فرانک فتوحی قزوینی، مدرک کارشناسی خود را در رشته مهندسی برق گرایش مخابرات در سال ۱۳۷۹ از دانشگاه لندن انگلستان و مدرک کارشناسی ارشد خود را نیز در سال ۱۳۸۰ از همان دانشگاه و در همان رشته دریافت کرده است. ایشان در سال ۱۳۹۰ دکترای خود را در رشته سیستم‌های اطلاعاتی چندرسانه‌ای موبایل و فراگیر از دانشگاه برادفورد انگلستان اخذ کرد. وی هم‌اکنون استادیار گروه مهندسی کامپیوتر و فناوری اطلاعات دانشگاه قم می‌باشد. زمینه‌های پژوهشی مورد علاقه ایشان سیستم‌های سیار، سیستم‌های چندرسانه‌ای، محاسبات فراگیر و سیستم‌های پزشکی از راه دور است.

نشانی رایانامه ایشان عبارت است از:

f-fotouhi@qom.ac.ir

روح‌الله دیانت، مدرک کارشناسی خود را در رشته مهندسی کامپیوتر گرایش سخت‌افزار در سال ۱۳۸۰ از دانشگاه شهید بهشتی دریافت کرده است. ایشان در سال ۱۳۸۲ مدرک کارشناسی ارشد خود را در رشته مهندسی کامپیوتر گرایش سخت‌افزار از دانشگاه صنعتی شریف و در سال ۱۳۸۹ نیز مدرک دکترای خود را از همان دانشگاه و در همان رشته کسب کرده است. وی هم‌اکنون استادیار گروه مهندسی کامپیوتر و فناوری اطلاعات دانشگاه قم است. زمینه‌های پژوهشی مورد علاقه ایشان سیستم‌های چندرسانه‌ای و پردازش سیگنال‌های صوتی و تصویری است.

نشانی رایانامه ایشان عبارت است از:

rouhollah.dianat@gmail.com

[DOI: 10.18869/acadpub.jsdp.14.1.3]