سیستم‌های تشخیص چهره در گوشی‌های هوشمند

استاد راهنما: دکتر رضا صفابخش

نگارنده: سید نوید کرمی‌نژاد

دی ۱۳۹۶

چکیده

با توجه به گسترش روزافزون کاربرد گوشی‌های هوشمند در زندگی روزمره‌ی انسان‌ها، توجه به حفظ امنیت اطلاعات افراد موضوعی حائز اهمیت است.

هر روزه شاهد ربوده شدن اطلاعات شخصی افراد هستیم و پیدا کردن روشی قابل اعتماد برای حفاظت از آن‌ها احساس می‌شود.

بر همین اساس و با پیشرفت فناوری، سیستم‌های جدیدتر و پیشرفته‌تری برای حفظ امنیت گوشی‌ها و مقابله با حمله‌ی هکرها طراحی شده‌است.

در این گزارش قصد داریم با یکی از جدیدترین سیستم‌های امنیتی به نام "سیستم‌های تشخیص چهره[۱]" و کاربردهای آن در زمینه‌های مختلف و بطور ویژه در گوشی‌های هوشمند صحبت آشنا شویم و با بررسی یک نمونه‌ی واقعی استفاده از این سیستم‌ها در گوشی‌ها درک بهتری از نحوه‌ی عملکرد آن پیدا کنیم.

[۱] Face Recognition Systems

فهرست مطالب

فهرست اشکال

۱. مقدمه

امروزه با توجه به اینکه اکثر افراد اطلاعات شخصی خود را در گوشی‌های خود نگهداری می‌کنند، استفاده از سیستم‌های حفاظتی امری ضروری به شمار می‌رود. این سیستم‌ها معمولا از ویژگی‌های انسانی نظیر اثر انگشت[۲]، عنبیه چشم[۳]، صدا و ... برای شناسایی فرد مجاز استفاده می‌کنند. به چنین سیستم‌هایی که از مشخصه‌های انسانی برای تشخیص هویت افراد استفاده می‌کنند، سیستم‌های "بیومتریک[۴]" می‌گویند.

یکی از انواع سیستم‌های بیومتریک، سیستم تشخیص چهره است که در ادامه و فصل‌های بعد بطور مفصل در مورد آن صحبت می‌کنیم.

[۲] Fingerprint

[۳] Iris Recognition

[۴] Biometric Systems

۲. سیستم تشخیص چهره

۲-۱. معرفی

یک نوع از سیستم‌های بیومتریک برای شناسایی افراد به کمک مقایسه چهره‌ی زنده‌ی فرد یا داده‌های تصویر دیجیتالی با اطلاعات ثبت شده از فرد موردنظر در یک پایگاه داده‌ی محلی یا مرکزی است. در صورت مطابقت این دو نمونه، فرد به عنوان فردی با هویت مجاز شناخته شده و اجازه دسترسی پیدا می‌کند.

۲-۲. کاربرد

این سیستم بطور فزاینده‌ای در بسیاری از برنامه‌های کاربردی نمود پیدا کرده‌است. برای مثال در کنسول بازی کینکت، برای تشخیص چهره در تمایز بین بازیکنان استفاده می‌شود.
البته اغلب برای اهداف امنیتی مورد استفاده قرار می‌گیرد. از نمونه‌های آن استفاده در فرودگاه‌ها برای شناسایی مجرمان و تایید هویت، نیروهای پلیس برای ردیابی مجرمان و همچنین افراد گم‌شده است.
در دستگاه‌های خودپرداز[۵] نیز به جای ورود با رمز عبور می‌توان استفاده نمود.

توجه به این نکته ضروری است که می‌تواند اهداف سوء هم داشته باشد. دولت‌ها با نصب دوربین‌هایی در سراسر شهر امکان این را خواهند داشت که بدانند هر فرد کجاست و چه کاری انجام می‌دهد.

۲-۳. مزایا

این سیستم نسبت به دیگر سیستم‌ها ارزان‌تر است. به این علت که کاملا نرم‌افزاری پیاده‌سازی می‌شود و تنها کافی است یک سنسور برای ثبت چهره افراد داشته باشیم که هزینه‌ای بسیار پایین‌تر در مقایسه با سنسورهایی مثل سنسور اثر انگشت دارند.

درصد اطمینان بالاتری نسبت به سایر سیستم‌ها داشته و خطای کمتری دارند.
عملکرد سریعی دارند که سبب می‌شود گروه‌های مختلفی جذب این سیستم‌ها شوند.
انتشار آلودگی و بیماری‌های واگیر دار را به میزان خوبی کاهش می‌دهند.
دیگر نیازی به به‌یادسپاری چندین رمز عبور برای انواع دستگاه‌ها و حساب‌های کاربری نیست.

[۵] ATM

۲-۴. معایب و چالش‌ها

مشخص است که هر فناوری علاوه‌بر اینکه ویژگی‌های خوبی دارد و امکاناتی که در اختیار ما قرار می‌دهد، مشکلاتی هم دارد. سیستم‌های تشخیص چهره نیز از این قاعده مستثنا نیستند.

برای مثال تشخیص یک فرد غیرمجاز یا یک عکس به عنوان فردی با هویت درست و با تشخیص نادرست بک فرد مجاز زمانی که عینک زده، آرایش کرده، ریش گذاشته و هر تغییری که چهره‌ی فرد را متفاوت کرده باشد و هچنین زمانی که سن فرد بالا رفته باشد.

۳. ساختار کلی سیستم‌های تشخیص چهره

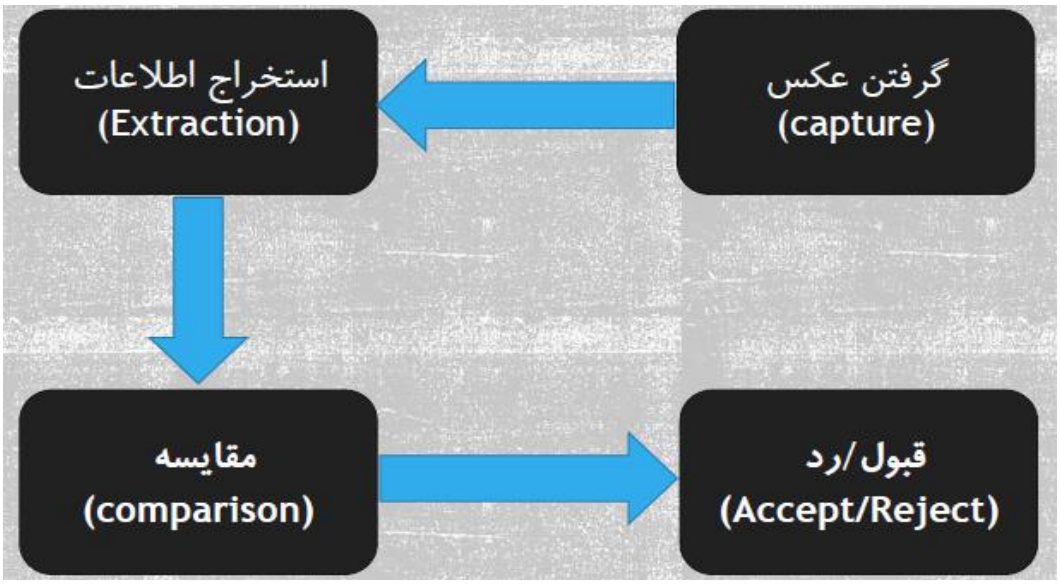
تمامی این سیستم‌ها شامل چهار گام اساسی به شرح زیر هستند:

۱) گرفتن عکس[۶]: زمانی که فرد در مقابل سنسور قرار می‌گیرد وظیفه سنسور این است که اطلاعات چهره فرد را به عنوان یک نمونه ثبت کند.

۲) استخراج اطلاعات[۷]: داده‌های منحصر به فرد و واحدی از نمونه استخراج می‌شود و یک قالب مشخص از نمونه موردنظر ساخته می‌شود.

۳) مقایسه[۸]: در این مرحله قالب ساخته شده با اطلاعات از پیش ذخیره شده در پایگاه داده مقایسه می‌شود.

۴) قبول/رد[۹]: در صورت مطابقت داشتن الگوهای مقایسه شده در مرحله قبل، هویت فرد به عنوان فردی مجاز شناخته می‌شود.



شکل ۱. ساختار کلی و مراحل کاری سیستم‌های تشخیص چهره

[۶] Capture

[۷] Extraction

[۸] Comparison

[۹] Accept/Reject

۳-۱. الگوریتم‌های استخراج اطلاعات

مهم‌ترین و اساسی‌ترین گام در بین قدم‌های بالا، مرحله دوم یعنی استخراج اطلاعات است. هرچه الگوریتم بهینه‌تری، دقیق‌تر و سریع‌تری انتخاب شود نتیجه‌ی به‌دست آمده به نتیجه مورد انتظار نزدیک‌تر می‌شود.

اصطلاحا به این الگوریتم‌ها، "توصیف‌گر بافت[۱۰]" گفته می‌شود.

در ادامه قصد داریم به معرفی دو الگوریتم و آشنایی با نحوه‌ی عملکرد آن‌ها بپردازیم.

۳-۱-۱. الگوریتم FBG[۱۱]

چهره‌ی هر فرد چندین نشانه‌ی منحصر به فرد دارد. مانند فاصله‌ی بین چشم‌ها، طول و عرض بینی، گونه‌ها، فک، چانه و ... .

این الگوریتم حدود ۸۰ نشانه‌ی چهره‌ی افراد را شناسایی و آن‌ها را به عنوان گره‌های یک گراف انتخاب می‌کند. این گراف یک نمایش عمومی از چهره‌ی فرد را به دست می‌دهد. بر طبق این الگوریتم، گراف ساخته شده به یک کد عددی به نام "فِیس پرینت[۱۲]" تبدیل می‌شود و در پایگاه داده نگهداری می‌شود.

هر بار که فرد در مقابل سنسور قرار می‌گیرد، کد حاصل از ساخته شدن گراف چهره با کد ذخیره شده در پایگاه داده مقایسه می‌شود و براساس میزان شباهت، هویت فرد تایید و یا رد می‌شود.

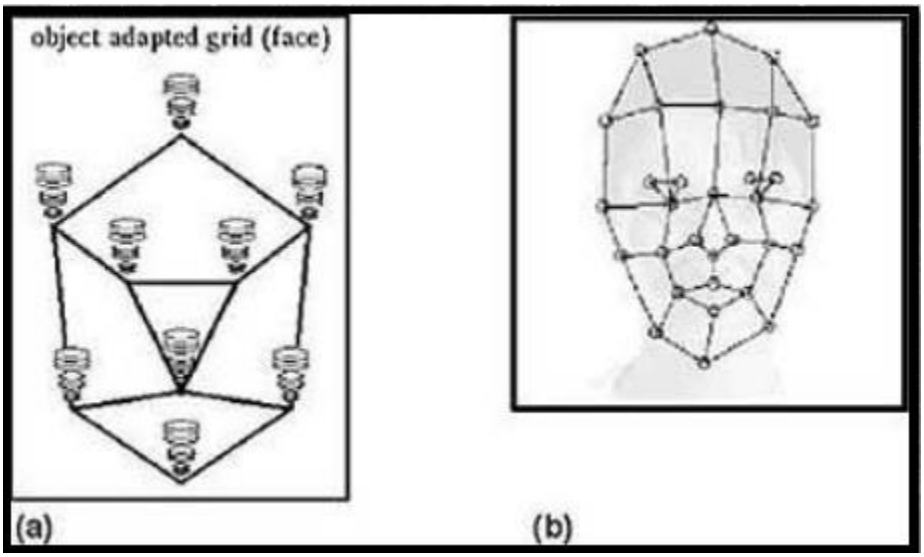
میزان شدت نور در این الگوریتم، در تشخیص چهره بسیار موثر است.

---

[۱۰] Textural descriptor

[۱۱] Face Bunch Graph

[۱۲] Faceprint



شکل ۲. گراف ساخته شده توسط الگوریتم FBG

۳-۱-۲. الگوریتم LBP[۱۳]

این الگوریتم در دنیای واقعی عملیاتی نشده‌است اما از نظر تئوری یکی از بهترین الگوریتم‌های موجود است. با آزمایش‌های انجام شده در محیط شبیه‌سازی شده روی گوشی‌های اندرویدی نتایج قابل قبولی از خروجی الگوریتم به‌دست آمده است.

این الگوریتم پیچیدگی پایینی دارد و به همین خاطر در گوشی‌ها عملکرد خوبی خواهد داشت زیرا گوشی‌ها توان پردازشی و محاسباتی کمتری در مقایسه با کامپیوترها دارند.

پس از اینکه عکس ورودی به تصویری سیاه-سفید تبدیل شد، ماتریس حاصل به زیربلوک‌های ۳*۳ پیکسل تبدیل می‌شود و اکنون برای هر پیسکل میانی از این زیربلوک‌ها ضریبی محاسبه می‌شود که نحوه‌ی محاسبه‌ی آن به صورت زیر است:

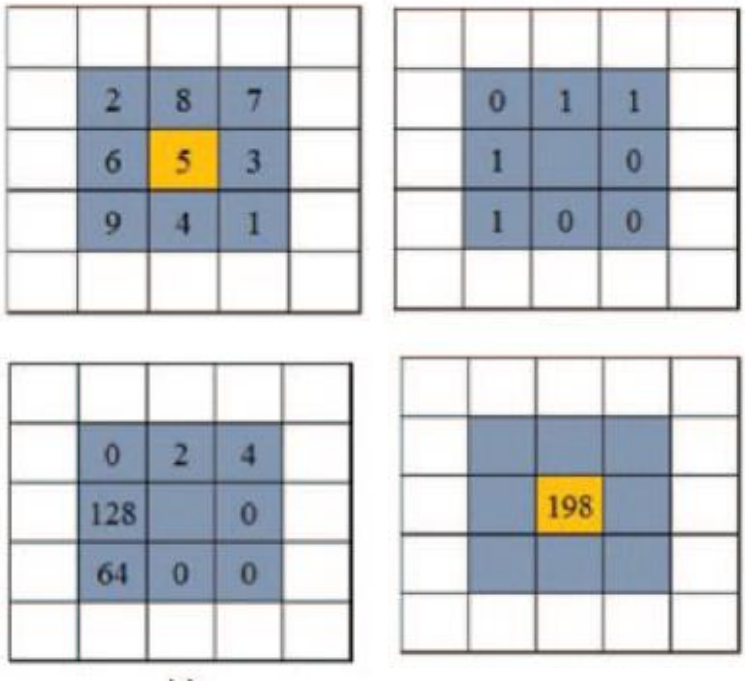
۱) پیکسل میانی شناسایی می‌شود و براساس اینکه شدت روشنایی آن نسبت به پیکسل‌های مجاور بیشتر یا کمتر است عدد صفر یا یک به هر یک از پیکسل‌های مجاور نسبت داده می‌شود.

۲) از پیکسل بالا- چپ (خانه‌ی شماره‌ی صفر) شروع کرده با حرکت ساعتگرد هر پیکسلی که عدد یک به آن نسبت داده‌شده بود این عدد را به "دو به توان شماره خانه" تبدیل می‌کنیم.

[۱۳] Local Binary Pattern

۳) در نهایت مجموع این اعداد را برای پیکسل میانی یادداشت می‌کنیم.

شکل۳ مراحل انجام این عملیات را نشان می‌دهد.



شکل ۳. نحوه‌ی محاسبه‌ی ضریب پیسکل میانی هر زیربلوک

پس از محاسبه این ضرایب، ماتریسی برای هر عکس به دست می‌آید. این ماتریس در پایگاه داده ذخیره می‌شود. برای تشخیص هویت افراد، به کمک فرمول۱ که به فرمول "فاصله اقلیدسی" معروف است، میزان اختلاف میان ماتریس ورودی و ماتریس ذخیره شده به‌دست می‌آید که براساس این عدد تایید یا رد هویت صورت می‌گیرد.

فرمول ۱. فاصله اقلیدسی

$$\text{میزان اختلاف دو ماتریس} = \sqrt{(x_s - y_t) * (x_s - y_t)^T}$$

در این فرمول x_s ماتریس ورودی و y_t ماتریس ذخیره شده در پایگاه داده است.
عددی که از این فرمول به دست می‌آید معیاری است که میزان شباهت دو تصویر را مشخص می‌کند و

به کمک آن می‌توان برای تایید و یا رد فرد مجاز استفاده کرد.

۴. کاربرد پردازنده‌ی گرافیکی[۱۴] در سیستم‌های تشخیص چهره

یکی از کاربردهای بسیار خوب پردازنده‌های گرافیکی استفاده از آن در تشخیص چهره است. چون یکی از وظایف این واحد، پردازش تصویر است که در این فناوری نقش اصلی را ایفا می‌کند.

بهره‌مندی از پرازنده‌ی گرافیکی در کنار پردازنده‌ی مرکزی[۱۵]، سبب می‌شود که سرعت اجرای الگوریتم‌ها افزایش یابد و پردازنده‌ی مرکزی درگیر محاسبات زیادی نشود.

همانطور که در جدول۱ مشاهده می‌کنید بهره‌مندی از پردازنده‌ی گرافیکی هم از لحاظ زمان مصرفی و هم انرژی مصرف شده عملکرد سیستم را بهبود بخشیده است.

فرایند	استخراج ویژگی‌ها		تشخیص چهره	
شیوه	CPU	CPU + GPU	CPU	CPU + GPU
زمان مصرفی (ثانیه)	۵,۱	۱,۲	۸,۵	۴,۶
انرژی مصرفی (ژول)	۱۸,۷	۴,۹	۲۹,۸	۱۶,۳

جدول ۱. مقایسه عملکرد سیستم بدون پردازنده‌ی گرافیکی و با پردازنده‌ی گرافیکی

[۱۴] GPU

[۱۵] CPU

۵. سیستم تشخیص چهره در گوشی آیفون

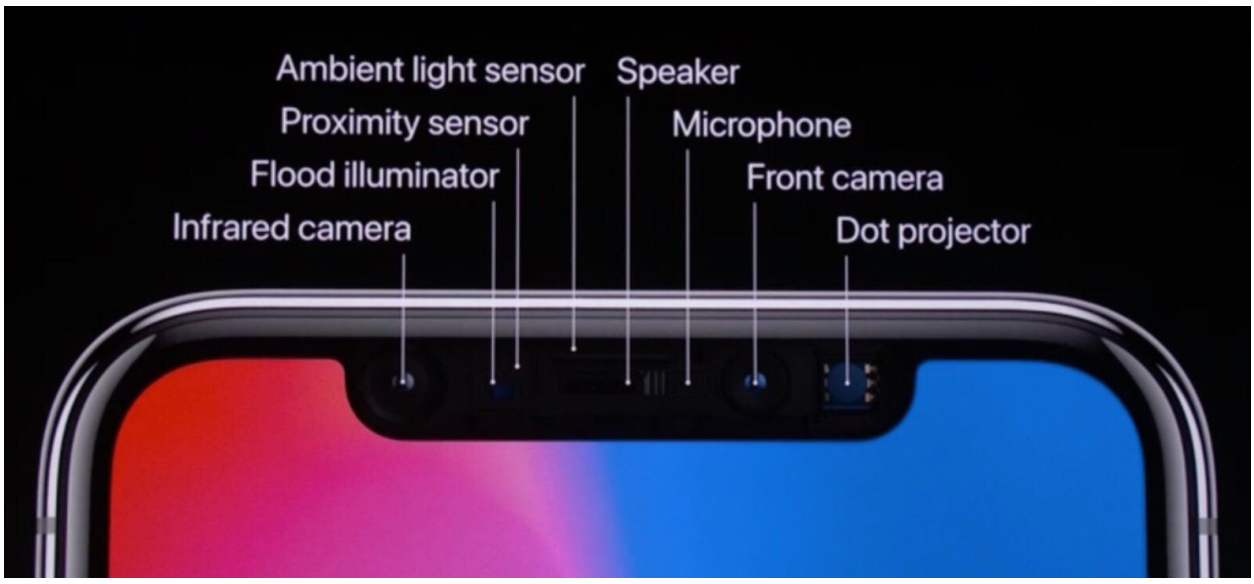
اخیرا شرکت اپل گوشی هوشمندی[۱۶] تولید کرده‌است که از سیستم تشخیص چهره در استفاده کرده و اسم این فناوری را "فِیس آی‌دی[۱۷]" گذاشته است.

فیس آی‌دی با کشف جهت خیره شدن فرد میزان توجه فرد را تایید و سپس از شبکه‌های عصبی برای مطابقت دادن چهره و جلوگیری از حقه‌ی افراد برای فریب دادن سیستم –چه به صورت دیجیتالی و چه فیزیکی– استفاده می‌کند. در نتیجه فرد می‌تواند تنها با یک نگاه گوشی خود را باز کند.

این سیستم بطور خودکار خود را تغییر ظاهر فرد منطبق می‌کند و با ضریب دقت بالا از حریم خصوصی و امنیت اطلاعات بیومتریک افراد حفاظت می‌کند.

تکنیکی که اپل در این گوشی بکار گرفته‌است، "ترو دِپت[۱۸]" نام دارد.

این سیستم از تکنولوژی‌های پیشرفته‌ای استفاده می‌کند تا به درستی شکل هندسی صورت افراد را نگاشت کند. همانطور که در شکل۴ ملاحظه می‌کنید این سیستم روی نواری در جلوی گوشی تعبیه شده‌است.



شکل ۴. اجزای سیستم True Depth

[۱۶] iPhone X

[۱۷] Face ID

[۱۸] True Depth

زمانی که فرد در مقابل دوربین جلوی گوشی قرار می‌گیرد این سیستم ابتدا تشخیص می‌دهد که چشم فرد باز است و مستقیما در مقابل دستگاه قرار گرفته باشد. سپس حدود ۳۰,۰۰۰ نقطه مادون قرمز از چهره را شناسایی کرده و از آن برای شکل‌دهی یک نقشه‌ی عمقی[۱۹] از صورت، همراه با یک تصویر دوبعدی مادون قرمز استفاده می‌کند. به کمک این اطلاعات و شبکه‌های عصبی برای ساختن یک دنباله‌ی دوبعدی از تصاویر و نقشه‌های عمق ــ که به صورت دیجیتالی نشانه‌گذاری شده‌اند ــ و ارسال آن به بخش "سکیور اینکلیو[۲۰]" استفاده می‌شود. در واقع این سیستم یک مدل ریاضی از چهره فرد ایجاد می‌کند.

برای شناسایی حقه‌ی فیزیکی و یا دیجیتالی نیز دوربین ترو دپت، دنباله‌ی دوبعدی تصاویر و نقشه‌ها عمق را بطور تصادفی تشکیل می‌دهد و یک الگوی کاملا تصادفی ایجاد می‌کند تا امکان فریب دادن سیستم به کمترین میزان ممکن برسد.

اطلاعات فیس آی‌دی که شامل یک نمایش ریاضی از چهره است، کدگذاری شده و تنها در بخش سکیور اینکلیو ذخیره می‌شود. این داده‌ها هیچگاه از دستگاه خارج نشده و حتی از آن پشتیبان نیز گرفته نمی‌شود و چون بخش سکیور اینکلیو در سخت‌افزار دستگاه نهفته است، امکان ربوده شدن این کد به هیچ عنوان وجود نخواهد داشت و تنها به هنگام احراز هویت افراد از آن استفاده می‌شود.

از ویژگی‌های منحصر به فرد این سیستم به‌روز شدن شبکه‌های عصبی پس از هر بار تقاضای ورود افراد است و به کمک تکنیک یادگیری خودکار می‌تواند چهره‌ی فرد مجاز را باد بگیرد و بتواند عکس و همچنین ماسک را از چهره‌ی واقعی تمییز دهد. همچنین این بادگیری کمک می‌کند زمانی که فرد عینک زده باشد، کلاه گذاشته باشد، آرایش کرده‌باشد، موهای خود را کوتاه کرده‌باشد و مواردی شبیه این چهره‌ی صاحب دستگاه را به درستی و با دقت بالا تشخیص دهد.

از دیگر مزایای این سیستم این است که زمانی که فرد در فضای بسته، باز و یا حتی در محیط‌های تاریک باشد می‌تواند عمل کند و هیچ تاثیری در نتیجه نداشته باشد.

شرکت اپل اعلام کرده است که درصد خطای این سیستم، بک در میلیون است درحالی که استفاده از تکنولوژی "تاچ آی‌دی[۲۱]" یک در ۵۰,۰۰۰ است که این مطلب نشان می‌دهد که فیس آی‌دی از نظر امنیتی بسیار پیشرفته‌تر از نسل‌های قبلی سیستم‌های امنیتی بکار گرفته‌شده در گوشی‌های آیفون است.

کاربرد این تکنولوژی به باز کردن گوشی و حفاظت اطلاعات محدود نمی‌شود. از آن برای ورود به

[۱۹] Depth Map

[۲۰] Secure Enclave

[۲۱] Touch ID

حساب‌های کاربری اپل نظیر اپ استور[۲۲]، آی‌تیونز[۲۳]، آی‌کلود[۲۴]، آی‌بوک[۲۵] استفاده می‌شود و دیگر نیازی به به‌یادسپاری رمز عبور نیست.

این تکنولوژی امکان خرید نرم‌افزارها و دیگر محصولات اینترتی را با ضریب امنیتی بالا فراهم می‌کند.

۵-۱. انیموجی

از کاربردهای جالب این تکنولوژی ساخت انیموجی است. انیموجی در واقع همان ایموجی است که بصورت متحرک درآمده‌است. همانطور که قبلا نیز اشاره شد، به کمک پرتوهای مادون قرمزی که به سمت چهره تابیده می‌شود، تصویری دوبعدی از چهره ثبت می‌شود. سیستم می‌تواند به کمک پرتوهای منعکس شده، میزان فاصله و زاویه هر نقطه از چهره‌ی فرد با دوربین را تعیین و در نتیجه تمامی حرکات چهره را شناسایی کند و با در اختیار داشتن این اطلاعات می‌تواند انیموجی‌هایی که دقیقا رفتاری مشابه رفتار فرد دارند را بسازد.

[۲۲] App Store

[۲۳] iTunes

[۲۴] iCloud

[۲۵] iBook

۶. جمع‌بندی

کارا نبودن سیستم‌های امنیتی پیشین سبب شد که مهندسان و طراحان به دنبال یافتن روشی مطمئن‌تر برای حفاظت (مالی، جانی و یا اطلاعاتی) باشند که این روند به ساخت و توسعه‌ی سیستم‌های مبتنی بر تشخیص چهره شد.

در این گزارش سعی شد با معرفی این سیستم‌ها و نحوه‌ی عملکرد آن‌ها، درک بهتری از این دسته سیستم‌های امنیتی ایجاد شود.

همچنین کاربردهای گسترده‌ی آن مطرح و یک کاربرد اساسی (در گوشی‌های هوشمند) مورد بررسی دقیق قرار گرفت.

پس از آشنایی با ساختار کلی این سیستم‌ها، دو دسته الگوریتم استخراج اطلاعات شرح داده‌شد.

و در انتها در مورد استفاده از سیستم تشخیص چهره در گوشی‌های هوشمند، در دنیای واقعی صحبت به میان آمد و به اختصار نحوه‌ی پیاده‌سازی، عملکرد و ویژگی‌های آن بیان شد.

به عنوان کارهای آینده نیز می‌توان با طراحی الگوریتم‌های بهینه‌تر و با عملکرد سریع‌تر و کم خطاتر کاربرد چنین سیستم‌هایی را در همه‌ی ابعاد امنیتی زندگی انسان‌ها توسعه و گسترش داد.

۷. منابع

[1] J. Olivares, K. Toscano, G. Sanchez, H. Perez, M. Nakano,
“Face recognition System for Smartphone based on LBP,” in Biometrics and Forensics (IWBF), Coventry, UK, 2017

[2] T. Cheng, Y. C. Wang. “Using Mobile GPU for General-Purpose Computing – A Case Study of Face Recognition on Smartphones,” in VLSI Design, Automation and Test (VLSI-DAT), Hsinchu, Taiwan, 2011

[3] Ex-sight (2009). How Facial Recognition works. [On-line]. Available: http://www.ex-sight.com/technology.htm

[4] TechTarget (2017). What is ficial recognition?[On-line}. Available: http://whatis.techtarget.com/definition/facial-recognition

[5] SlideShare (October 2013). Face Recognition Technology[On-line]. Available: https://www.slideshare.net/SiddharthModi1/face-recognition-technology-27574561?from_action=save

[6] SlideShare (March 2013). Face Recognition Technology[On-line]. Available: https://www.slideshare.net/gsantosh031/face-recognitio-ppt?from_action=save

[7] Macword (December 2017). Face ID on the iPhone X. Available: https://www.macworld.com/article/3225406/iphone-ipad/face-id-iphone-x-faq.html

[8] Apple(November 2017). Face ID Security Guide[On-line]. Available: https://images.apple.com/business/docs/FaceID_Security_Guide.pdf