International Conference on
RESEARCH IN ELECTRICAL AND COMPUTER ENGINEERING
کنفرانس بین‌المللی پژوهش در مهندسی برق و کامپیوتر
15 December 2016 Singapore www.receconf.com سنگاپور ۲۵ آذر ۱۳۹۵

ارائه‌ی روشی برای حفظ حریم خصوصی دیداری کاربران تلفن همراه از افراد همجوار

آبتین تشکر
دانشجوی کارشناسی ارشد مهندسی فناوری اطلاعات، دانشگاه تحصیلات تکمیلی صنعتی و فناوری پیشرفته
abtin.tashakor@gmail.com

حمیدرضا ناجی
دانشیار، عضو هیأت علمی دانشکده برق و کامپیوتر، دانشگاه تحصیلات تکمیلی صنعتی و فناوری پیشرفته
hamidnaji@ieee.org

محمد مهدی فقیه
استادیار، عضو هیأت علمی دانشکده برق و کامپیوتر، دانشگاه تحصیلات تکمیلی صنعتی و فناوری پیشرفته
mehdi.faghih@gmail.com

چکیده
با رشد روزافزون کاربران تلفن‌های هوشمند، نگرانی‌ها در مورد حفظ حریم خصوصی دیداری کاربران نیز در حال افزایش است. افراد دوست دارند در اماکن عمومی از تلفن هوشمندشان برای دیدن فیلم و عکس و یا انجام کارهای شخصی مثل امور بانکی استفاده کنند. ولی در این اماکن همیشه افرادی هستند که به صفحه‌نمایش دیگران نگاه می‌کنند.
در این پژوهش با مروری بر روش‌های موجود برای حفظ حریم خصوصی دیداری کاربران تلفن همراه، روشی جدید برای این کار معرفی می‌شود. در روش پیشنهادی، نرم‌افزاری بر روی گوشی نصب می‌شود و نویزی رنگی با یک طول موج مشخص را روی تصویر صفحه نمایش ایجاد می‌کند. این نویز به گونه ای است که کاربران با نگاه کردن به صفحه نمایش نمی‌نوانند تصویر را به وضوح مشاهده کنند. کاربری که می‌خواهد با گوشی کار کند، عینک مخصوصی را بر چشم می‌گذارد. این عینک از فیلتر نوری میان ناگذر ساخته شده است. عملکرد این فیلتر به گونه‌ای است که طول موج مشخصی از نور را از خود رد نمی‌کند و بقیه‌ی طول موج‌های نور به خوبی از آن می‌گذرند. بدین ترتیب نویزی که توسط نرم افزار روی تصویر ایجاد شده از عینک عبور نکرده و تصویر برای کاربری که از عینک استفاده می‌کند به وضوح قابل نمایش است در صورتی که افراد دیگر بدون عینک، تصویر را با نویز مشاهده می‌کنند.
روش پیشنهادی با استفاده از نرم‌افزار متلب شبیه سازی شده است. با مقایسه‌ی نتایج تحقیقات گذشته و روش پیشنهادی، نقاط قوت و ضعف هرکدام بیان شده است. روش پیشنهادی این پژوهش از قدرت بالاتری نسبت به سایر روش‌های موجود در حفظ حریم خصوصی دیداری برخوردار است. همچنین قابلیت کنترل پذیری بالایی دارد و مصرف انرژی آن نسبت به روش‌های دیگر کمتر است.

کلمات کلیدی: تلفن هوشمند، حریم خصوصی دیداری، صفحه‌نمایش، فیلتر میان‌ناگذر

۱- مقدمه

با هوشمند شدن تلفن‌های همراه، تعداد کاربران این دستگاه‌ها برای انجام کارهای شخصی مانند ارسال ایمیل، انجام امور بانکی، دیدن فیلم و عکس، در اماکن عمومی نظیر اتوبوس، مترو، هواپیما و ... رو به افزایش است. اگرچه استفاده از تلفن‌های هوشمند در این اماکن، کارایی کاربران را زیاد کرده و برای فرد نیز لذت‌بخش است، نگرانی‌های جدیدی برای حفظ حریم خصوصی کاربران به وجود آمده است.

برای مثال ممکن است شخصی از تلفن همراه خود هنگام مسافرت با قطار یا در زمان انتظار برای اتوبوس و یا هنگامی که در یک کافه نشسته است، استفاده کند، در این هنگام ناگهان احساس کند که شخص دیگری به صفحه نمایش دستگاهش نگاه می‌کند. او سرش را برمی‌گرداند و با شخصی مواجه می‌شود که خیلی سریع نگاهش را به سمت دیگری می‌چرخاند. این قبیل اتفاقات تا زمانی که راهی برای جلوگیری از دزدکی نگاه کردن وجود نداشته باشد، ممکن است رخ دهد. زیرا اشخاص نمی‌توانند هنگامی که بر روی کارشان تمرکز کرده‌اند، مدام حواسشان به اطراف نیز باشد.

ناتوانی افراد از جلوگیری از نظاره‌کنندگان مجاورشان که به صفحه‌نمایشگر تلفن هوشمندشان خیره شده‌اند، امکان آن را به وجود آورده که کلمه عبور، پیام‌های مهم، اطلاعات تجاری یا تصاویر شخصی کاربران در معرض دید افراد دیگر قرار گیرد که این خود نوعی تجاوز به حریم خصوصی کاربران است.

با توجه به تازگی عرضه‌ی فنّاوری تلفن‌های هوشمند، هنوز فرهنگ استفاده‌ی محترمانه آن‌چنان‌که باید در دنیا جا نیفتاده است و این نوع از تجاوز به حریم خصوصی در همه‌ی کشورها وجود دارد و نگرانی‌ها در این مورد در حال افزایش است (Iachello,2007). تحقیقات نشان می‌دهد که بیش از نیمی از مردم فرانسه در مورد دزدیده شدن اطلاعات شخصی تلفن‌های هوشمندشان در اماکن عمومی نگران هستند. همچنین ۷۲ درصد مردم کشور انگلیس که با وسایل نقلیه عمومی نظیر مترو و اتوبوس رفت‌وآمد می‌کنند، از روی شانه‌ی یکدیگر به صفحه‌نمایش گوشی دیگران نگاه می‌کنند (Honan,2012).

برای دستگاه‌های ثابت نظیر رایانه‌های شخصی با صفحات نمایش بزرگ، کاربران روش‌هایی برای حفظ حریم خصوصی دیداری‌شان به کار می‌برند. به‌طور مثال از بدن خود برای محدود کردن دید دیگران استفاده می‌کنند، یا در بانک برای جلوگیری از دید مشتری به رایانه‌ی صندوقدار، از شیشه محافظ جلوی روی مشتریان استفاده می‌شود. در ادارات صفحات نمایش را به‌گونه‌ای قرار می‌دهند که دید دیگران روی آن کم باشد. یا به‌محض اینکه شخصی وارد اتاقشان شد صفحه‌ی مربوط به برنامه‌ای که برایشان مهم هست را پنهان می‌کنند (Brudy et al,2014).

خوشبختانه راهکاری به نام میکرولوور[1] (Ying,2012) توسط محققین اختراع شده که برچسبی شفاف است که بر روی صفحه نمایش تلفن‌های همراه قابل نصب است. با این کار زاویه دید صفحه نمایش محدود می‌شود و افرادی که از بغل نگاه می‌کنند، صفحه را سیاه می‌بینند. بنابرین اطلاعات نمایش داده شده در صفحه تنها برای افرادی که مستقیماً جلوی آن قرار دارند قابل دیدن است.

اگرچه این گونه برچسب ها نازک و قابل حذف هستند، ولی تنها یک زاویه دید محدودی؛ مثلا ۳۰ درجه از چپ و راست؛ را برای کاربر ایجاد می‌کنند. بنابرین اگر فردی بخواهد صفحه نمایشش را برای دوستانش به اشتراک بگذارد، احساس راحتی ندارد. همچنین این قبیل برچسب‌ها باعث کاهش شفافیت تصویر می‌شوند که مورد انتظار کاربر نیست.

تاکنون روشی بهینه برای جلوگیری از نگاه کردن دزدکی اطرافیان به صفحه نمایش معرفی نشده است. اما روش‌هایی برای تشخیص تعرض دیداری افراد وجود دارد. در این روش‌ها با کمک دوربین و الگوریتم‌های تشخیص چهره، تعداد افرادی که به صفحه نمایش نگاه می‌کنند شمارش می‌شود و در صورت تجاوز از حد مشخص، به کاربر هشدار می‌دهند (Sencar et al,2010)، اگرچه با توجه به کوچک بودن ابعاد صفحه نمایش تلفن‌های همراه و ضعیف بودن دوربین به کار رفته در آن‌ها، این روش‌ها چندان کاربردی نیستند.

در بخش دوم این پژوهش با مروری بر گذشته، خلاصه‌ای از چند روشی که توسط محققین مختلف برای حفظ حریم خصوصی دیداری کاربران تلفن همراه ارائه‌شده، بیان می‌شود. این تحقیقات به دو دسته روش‌های سخت‌افزاری و نرم‌افزاری تقسیم شده‌اند.

[1] micro louver

بخش سوم به طرح ایده‌ی پیشنهادی این پژوهش می‌پردازد. در بخش چهارم شبیه سازی و بحث پیرامون ایده پیشنهادی انجام شده و نتایج آن با روش‌های گذشته مقایسه شده است. در انتها با مقایسه روش‌های ارائه‌شده و ایده‌ی پیشنهادی و بررسی نقاط قوت و ضعف هرکدام به یک نتیجه‌گیری رسیده و پیشنهاداتی برای آینده این حوزه ارائه می‌شود.

۲- پیشینه‌ی پژوهش

روش‌هایی که به کمک سخت‌افزار و نرم‌افزار، حریم خصوصی دیداری کاربران محافظت می‌شود را در این بخش بررسی می‌کنیم. دو روش سخت‌افزاری و دو روش نرم‌افزاری در ادامه معرفی می‌شود.

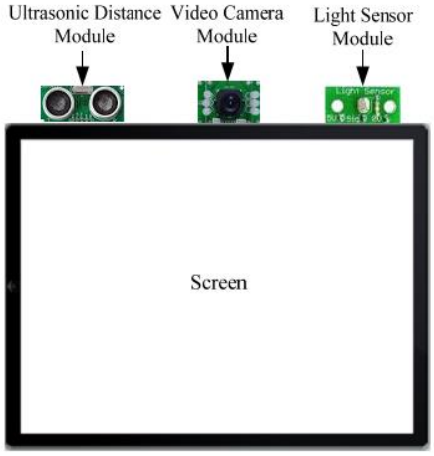
۲-۱- روش‌های سخت افزاری

در این بخش، ابتدا روش "حفظ هوشمند حریم خصوصی بر پایه حسگرهای چندگانه مرکب" که توسط شیگولیان و همکاران ارائه‌شده است را بررسی خواهیم کرد (Lian et al,2013). سپس به معرفی " فیلتر حریم خصوصی" که یک برچسبی فیزیکی است و توسط کمپانی 3M آمریکا عرضه‌شده است، خواهیم پرداخت (3M Company).

۲-۱-۱- حفظ هوشمند حریم خصوصی بر پایه حسگرهای چندگانه مرکب

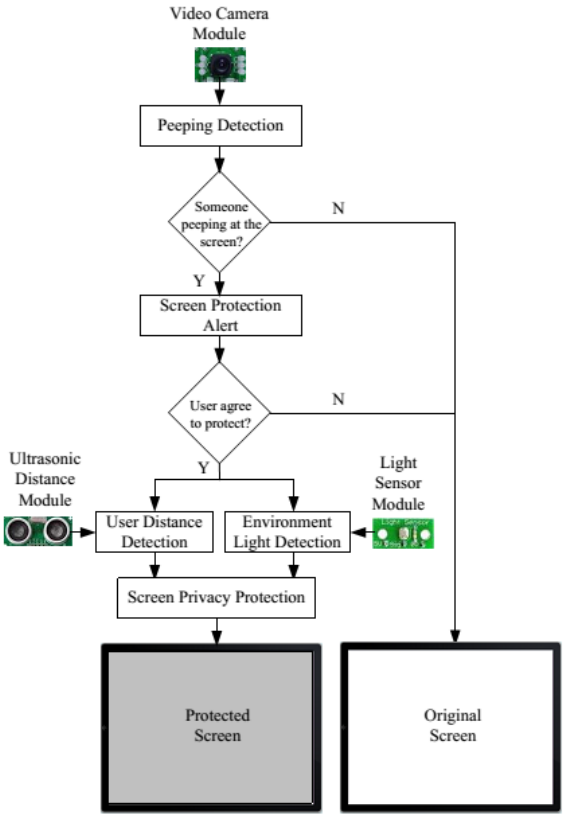
در این روش سه ماژول سخت‌افزاری به گوشی تلفن هوشمند افزوده می‌شود که شکل (۱) موقعیت آن‌ها را روی صفحه‌نمایش گوشی نشان می‌دهد.

- ماژول دوربین
- حسگر سنجش فاصله
- حسگر سنجش نور محیط



شکل (۱) ماژول‌های افزوده‌شده به صفحه گوشی هوشمند

سپس روند فلوچارت شکل (۲) طی می‌شود.



شکل (۲) فلوچارت روند کارکرد روش حسگرهای مرکب

۱- ابتدا با استفاده از ماژول دوربین و الگوریتم‌های تشخیص چهره، سیستم تشخیص می‌دهد که آیا فردی متجاوز به گوشی نگاه می‌کند یا خیر. این کار با شمردن تعداد چشم‌هایی که به صفحه نگاه می‌کنند انجام می‌شود.

۲- اگر متجاوزگر به گوشی نگاه می‌کند، سیستم به کاربر هشدار می‌دهد. درصورتی‌که کاربر با حفاظت گوشی موافقت کند روند ادامه می‌یابد.

۳- در مرحله بعد با استفاده از حسگر فاصله‌سنج، فاصله صفحه‌نمایش گوشی تا چشم کاربر مجاز محاسبه می‌شود. همچنین میزان نور محیط با استفاده از حسگر سنجش نور، اندازه گرفته می‌شود.

۴- با استفاده از مقادیر به‌دست‌آمده از مرحله قبل، میزان نور صفحه نمایش به گونه‌ای تنظیم می‌شود که فقط توسط کاربر مجاز قابل‌رؤیت باشد.

۲-۱-۲- فیلتر حریم خصوصی صفحه‌نمایش

این فیلتر یک برچسب فیزیکی است که بر روی صفحه‌نمایش نصب می‌شود و زاویه دید صفحه‌نمایش را به کاربری که از روبه‌رو به صفحه می‌نگرد محدود می‌کند. (شکل ۳ تا ۵)

شکل (۳) صفحه‌ی نمایش یک رایانه‌ی همراه که برچسب حریم خصوصی روی آن نصب شده است را از زاویه‌ی روبه‌رو نشان می‌دهد.

شکل (۳) صفحه‌نمایش با برچسب حریم خصوصی از روبه‌رو

در شکل (۴) عملکرد برچسب حریم خصوصی در زاویه مشخص شده است. می‌بینیم که با تغییر زاویه‌ی نگاه کردن به صفحه، بخشی از صفحه تاریک شده است.

شکل (۴) صفحه‌نمایش با برچسب حریم خصوصی از زاویه

شکل (۵) بیانگر آن است که صفحه نمایش با برچسب حریم خصوصی در زاویه های زیاد، کاملا تاریک شده و قابل مشاهده نخواهد بود.

شکل (۵) صفحه‌نمایش با برچسب حریم خصوصی از زاویه بیشتر

این فیلتر با استفاده از قطبیده کردن نور خروجی از صفحه‌نمایش، زاویه دید را محدود می‌کند. نور خروجی از صفحه‌نمایش به‌صورت امواجی است که در همه جهت منتشر می‌شود. هنگامی‌که نور از یک فیلتر قطبنده عبور می‌کند، تنها در یک راستا قابلیت خروج از فیلتر را دارد. برچسب حریم خصوصی صفحه‌نمایش که توسط کمپانی 3M آمریکا به بازار عرضه گشته است، یک برچسبی است که

از مواد قطبنده پوشانده شده است. نور خروجی از صفحه‌نمایش با عبور از این فیلتر در راستای عمودی قطبیده می‌شود. درنتیجه نور صفحه‌نمایش به زاویه‌های دیگر منتشر نمی‌شود. بنابراین کاربرانی که از زاویه به صفحه‌نمایش نگاه می‌کنند، آن را سیاه می‌بینند.

۲-۲- روش‌های نرم‌افزاری

در این بخش روش‌هایی که به کمک نرم‌افزار، حریم خصوصی دیداری کاربران محافظت می‌شود را بررسی می‌کنیم. مروری بر دو روش "حفظ کاربران موبایل از حملات دیداری حریم خصوصی" (Eunus et al,2014) و اختراع "حفظ حریم خصوصی صفحه‌نمایش با استفاده از نرم‌افزار" (Yang, 2015) ارائه می‌شود.

۲-۲-۱- حفظ کاربران موبایل از حملات دیداری حریم خصوصی

محققین این روش با گسترش دادن یک نرم‌افزار که بر روی گوشی هوشمند نصب می‌شود روند زیر را برای حفظ حریم خصوصی دیداری کاربران پیاده‌سازی کرده‌اند.

۱- محیط اطراف گوشی توسط دوربین جلوی گوشی فیلم‌برداری می‌شود.

۲- الگوریتم تشخیص چهره اجرا می‌شود.

۳- فاصله افرادی که به صفحه گوشی نگاه می‌کنند، بر مبنای فاصله بین جفت چشم‌ها تخمین زده می‌شود.

۴- با توجه به فاصله تخمین زده‌شده تشخیص می‌دهد که آیا متن تصویر برای افراد پشت سر قابل‌خواندن هست یا خیر.

۵- درصورتی‌که تصویر برای افراد پشت سر کاربر قابل‌خواندن باشد، با یک علامت رنگی به کاربر هشدار می‌دهد.

این نرم‌افزار همیشه بر روی گوشی در حالت اجرا و رصد اطراف خواهد بود. همچنین این قابلیت را دارد که تعداد افراد مجازی که می‌توانند به صفحه گوشی نگاه کنند را برای نرم‌افزار تعریف کرد. پس از این که نرم‌افزار تشخیص داد که تعداد افراد مناظره کننده از تعداد مجاز بیشتر است با علامت‌های سبز، زرد و قرمز به کاربر هشدار می‌دهد. رنگ سبز به آن معناست که صفحه گوشی برای فرد متجاوز غیرقابل‌خواندن است. رنگ زرد نشان از آن دارد که نرم‌افزار از اینکه کاربر عقبی می‌تواند صفحه را بخواند یا خیر مطمئن نیست و رنگ قرمز هشدار خطری است که کاربر متجاوز به صفحه گوشی اشراف کامل دارد.

۲-۲-۲- اختراع حفظ حریم خصوصی صفحه‌نمایش با استفاده از نرم‌افزار

این روش به‌عنوان یک اختراع در آمریکا به ثبت رسیده است. در این روش، نرم‌افزار با انداختن یک الگو بر روی تصویر اصلی صفحه، باعث ایجاد خطای دید برای کاربران مجاور می‌شود و درنتیجه زاویه دید صفحه‌نمایش محدود می‌شود.

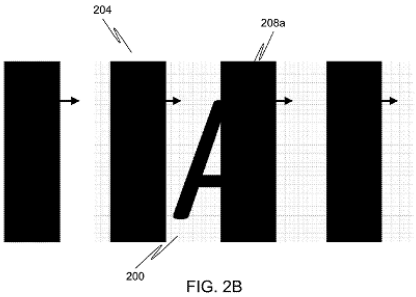
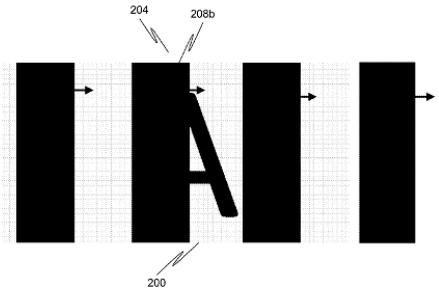


FIG. 2B



شکل (۶) نحوه عملکرد اختراع فیلتر حریم خصوصی با استفاده از نرم‌افزار

همان‌طور که در شکل (۶) نشان داده‌شده است، این اختراع مدعی است هنگامی‌که یک الگویی مثل خطوط موازی عمودی که با سرعت بر روی تصویر به‌صورت افقی حرکت بکند، باعث ایجاد خطای دید برای افرادی که از زاویه به صفحه‌نمایش نگاه می‌کنند، می‌شود.

طبق متن اختراع، با حرکت این خطوط عمودی، در لحظه اول یک قسمت از تصویر برای کاربری که مستقیم به صفحه نگاه می‌کند قابل‌رؤیت است و در لحظه دوم، بخش دیگر آن تصویر مشاهده می‌شود و چون این الگو به‌سرعت در حال حرکت است و این سرعت از تأخیر چشم برای تشخیص تصویر متحرک بیشتر است، درنتیجه الگو محافظ رؤیت نمی‌شود و کاربر به‌صورت عادی تصویر را می‌بیند. ولی کاربری که از زاویه به صفحه‌نمایش نگاه می‌کند دچار خطای دید می‌شود و نمی‌تواند تصویر را به‌وضوح ببیند.

در ابتدا تصویر اصلی بر روی صفحه به نمایش درمی‌آید. سپس یک لایه نیمه شفاف بر روی تصویر اصلی قرار می‌گیرد و در آن الگوی مربوطه نمایش داده می‌شود. این الگو بسته به تصویر اصلی می‌تواند متفاوت باشد. یعنی شکل، نحوه حرکت، سرعت، رنگ و... مختلفی می‌تواند داشته باشد.

این اختراع مدعی است که زاویه دید تصویر را از چهار طرف صفحه، یعنی چپ و راست و بالا و پایین محدود می‌کند. همچنین فردی که از فاصله بیش‌ازحد مجاز به صفحه نگاه کند نیز دچار خطای دید می‌شود درنتیجه این روش برای افرادی که از پشت سر به صفحه نگاه می‌کند نیز مفید است.

۳- روش پیشنهادی

روش پیشنهادی برای حفظ حریم خصوصی دیداری کاربران تلفن همراه، از اجزای نرم‌افزاری و سخت‌افزاری تشکیل شده است. شکل (۷) عینک مخصوص و صفحه نمایش تلفن در حین اجرای نرم افزار به کار رفته را نشان می‌دهد.

شکل (۷) شمایی از عملکرد ایده‌ی پیشنهادی

در این روش با استفاده از یک عینک که از فیلتر نوری مخصوصی ساخته شده و بر روی چشم کاربر قرار می‌گیرد و نرم‌افزاری که بر روی تلفن همراه اجرا می‌شود، شرایطی ایجاد می‌شود که فقط کاربر صاحب و استفاده کننده از گوشی بتواند صفحه نمایش را ببیند. نرم‌افزار نصب شده بر روی گوشی هوشمند نویزی رنگی با یک طول موج مشخص را روی تصویر صفحه نمایش ایجاد می‌کند. این نویز به گونه ای است که کاربران با نگاه کردن به صفحه نمایش نمی‌توانند تصویر را به وضوح مشاهده کنند. کاربری که می‌خواهد با گوشی کار کند عینک مخصوصی را بر چشم می‌گذارد. این عینک از فیلتر نوری میان ناگذر[۲] ساخته شده است. عملکرد این فیلتر به گونه‌ای است که طول موج مشخصی از نور را از خود رد نمی‌کند و بقیه طول موج‌های نور به خوبی از آن می‌گذرند. بدین ترتیب نویزی که توسط نرم افزار روی تصویر ایجاد شده از عینک عبور نکرده و تصویر برای کاربری که از عینک استفاده می‌کند به وضوح قابل نمایش است در صورتی که افراد دیگر بدون عینک، تصویر را با نویز مشاهده می‌کنند.

۱-۳- نرم‌افزار

برای درک بهتر عملکرد نرم‌افزار یاد شده، مباحثی که در ادامه آورده می‌شود پیرامون فیزیک نور رنگی، عملکرد نمایشگرهای رنگی و ساختار نویز استفاده شده، قابل توجه است.

نور در حقیقت گونه ای از انرژی است. نور قسمتی از طیف الکترومغناطیسی است که با چشم انسان قابل دیدن است. چشم انسان می‌تواند نور طول موجهای بین ۴۰۰ و ۷۰۰ نانومتر را درک کند. امواج نورانی به طور فیزیکی رنگی نیستند بلکه رنگها در سیستم دیداری انسان شکل می‌گیرند. رنگ دریافت شده با طول موج یا فرکانس موج تعیین می شود.

هنگامی که انرژی یک موج الکترومغناطیسی در تمام باند مرئی، برابر باشد، ما سفید تشخیص می دهیم، هنگامی که هیچ انرژی در طول باند مرئی موجود نباشد، ما سیاه می بینیم.

در سال ۱۶۷۶، نیوتن نشان داد که اشعه نور سفید می تواند توسط یک منشور اپتیکی شکسته شود تا یک باند چند لایه رنگی به عنوان طیف نور سفید نشان دهد.

خواص رنگ به طور ریاضی می تواند توسط مدل ها یا بازنمایی های متعددی تعریف شود. یکی از معمول‌ترین مدل‌ها برای بازنمایی رنگ، مدل قرمز، سبز، آبی (RGB) است (Smith,1931). مدل RGB برای توصیف رنگ‌هایی استفاده می شودکه به منابع نور روشن کننده مربوط است. این رنگها از قانون رنگهای افزایشی پیروی می کند. ترکیب تمام رنگ‌ها با هم رنگ سفید را ایجاد می کنند.

[۲] Optical Notch Filter

ترکیب قرمز و سبز، زرد را نتیجه می‌دهد. رنگ‌های افزایشی برای نور افکنی، نمایش ویدئو، ضبط فیلم و صفحه های نمایش استفاده می‌شوند. انواع صفحات نمایش کامپیوترها و گوشی‌های همراه از این مدل برای تولید رنگ استفاده می‌کنند.

۱-۱-۳- تبدیل طول موج به RGB

فضای رنگ "CIE 1931" اولین تعریف کمّی پیوند میان رنگ‌های فیزیکی خالص (طول موج) در طیف مرئی الکترومغناطیسی، با دریافت روان‌شناختی رنگ در دید انسان است. روابط ریاضی که این فضای رنگی را تعریف می‌کنند، ابزاری ضروری برای مدیریت رنگ هستند به ویژه هنگامی که با چاپگرهای رنگی، نمایشگرها و دوربین‌های دیجیتال سروکار داریم (CIE,1931).

چشم انسان با دید معمولی، سه نوع یاخته‌ی مخروطی دارد که در انتهای چشم و در شبکیه قرار دارند. این یاخته‌ها انرژی نورانی را به پیام عصبی تبدیل کرده و به مغز توانایی دیدن رنگ‌ها و جزئیات ظریف اشیا را می‌دهند. هر کدام از یاخته‌ها به انرژی طول موج خاصی از نور حساسیت نشان می‌دهند.

توابع تطبیق رنگ CIE که با نمادهای $\bar{x}(\lambda)$، $\bar{y}(\lambda)$ و $\bar{z}(\lambda)$ نشان داده می‌شوند، توصیفی عددی از واکنش رنگی دید انسان به طول موج‌های طیف مرئی هستند که مقادیر سه گانه X، Y و Z را حاصل می‌کنند.

این سه مقدار با استفاده از معادلات (۱) تا (۵) و رادیانس طیف $L_{e,\Omega,\lambda}$ به دست می‌آیند.

$$X = \int_{380}^{780} L_{e.\Omega.\lambda}(\lambda)\bar{x}(\lambda)d\lambda \quad (۱)$$

$$Y = \int_{380}^{780} L_{e.\Omega.\lambda}(\lambda)\bar{y}(\lambda)d\lambda \quad (۲)$$

$$Z = \int_{380}^{780} L_{e.\Omega.\lambda}(\lambda)\bar{z}(\lambda)d\lambda \quad (۳)$$

$$L_{e.\Omega} = \frac{\partial^2 \Phi_e}{\partial\Omega\partial A\cos\theta} \quad (۴)$$

$$L_{e.\Omega.\lambda} = \frac{\partial L_{e.\Omega}}{\partial\lambda} \quad (۵)$$

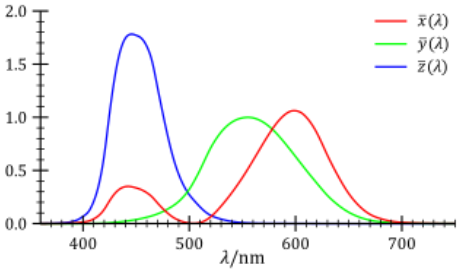
∂ : نماد مشتق جزئی

Φ_e : شار تابشی

Ω : زاویه فضایی

$A\cos\theta$: مساحت محدوده

λ : طول موج نور مورد نظر



شکل (۸) نمودار تابع تطبیق رنگ CIE

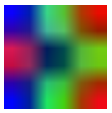
مقادیر سه گانه X، Y و Z با استفاده از معادله‌ی (۶) به مدل RGB قابل تبدیل است. اعداد موجود در ماتریس توسط استاندارد CIE اعلام شده است.

$$\begin{bmatrix} R \\ G \\ B \end{bmatrix} = \begin{bmatrix} 0.418.47 & 0.158.66 & -0.082.835 \\ -0.091.169 & 0.252.43 & 0.015.708 \\ 0.000.920.90 & -0.002.549.8 & 0.178.60 \end{bmatrix} \cdot \begin{bmatrix} X \\ Y \\ Z \end{bmatrix} \qquad (۶)$$

۲-۱-۳- مدل RGB در تصاویر کامپیوتری

تصاویر صفحات نمایش کامپیوترها و تلفن‌های همراه از مدل RGB برای تولید رنگ استفاده می‌کنند. بدین صورت که هر تصویری که نشان داده می‌شود از سه کانال رنگی قرمز، سبز و آبی ساخته شده است. یعنی هر پیکسل از ترکیب این سه رنگ به وجود می‌آید. می‌توان هر کانال تصویر را به ماتریسی دو بعدی تشبیه کرد که درایه‌های آن مختصات پیکسل‌های تصویر را تشکیل می‌دهند. پس هر تصویر رنگی یک ماتریس سه بعدی T=[A,B,C] است که A و B، مختصات هر پیکسل و C شماره کانال رنگی آن پیکسل است (Jayaraman,2009,272).

برای درک بهتر ماتریس کانال‌ها، شکل (۹) را در نظر بگیرید. ابعاد عکس ۶ در ۶ پیکسل می‌باشد. پس تصویر از سه ماتریس ۶ در ۶ تشکیل شده است. هر درایه از ماتریس می‌تواند مقادیر ۰ تا ۲۵۵ را بگیرد.



شکل (۹) سه رنگ اصلی در ابعاد ۶ در ۶ پیکسل

$$R = \begin{bmatrix} 0 & 0 & 0 & 0 & 255 & 255 \\ 0 & 0 & 0 & 0 & 255 & 255 \\ 255 & 255 & 0 & 0 & 0 & 0 \\ 255 & 255 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 255 & 255 \\ 0 & 0 & 0 & 0 & 255 & 255 \end{bmatrix} \quad G = \begin{bmatrix} 0 & 0 & 255 & 255 & 0 & 0 \\ 0 & 0 & 255 & 255 & 0 & 0 \\ 0 & 0 & 0 & 0 & 255 & 255 \\ 0 & 0 & 0 & 0 & 255 & 255 \\ 0 & 0 & 255 & 255 & 0 & 0 \\ 0 & 0 & 255 & 255 & 0 & 0 \end{bmatrix} \quad B = \begin{bmatrix} 255 & 255 & 0 & 0 & 0 & 0 \\ 255 & 255 & 0 & 0 & 0 & 0 \\ 0 & 0 & 255 & 255 & 0 & 0 \\ 0 & 0 & 255 & 255 & 0 & 0 \\ 255 & 255 & 0 & 0 & 0 & 0 \\ 255 & 255 & 0 & 0 & 0 & 0 \end{bmatrix}$$

۳-۱-۳- نویز

یکی از مدل‌های نویزی که می‌توانیم برای این کار از آن استفاده کنیم، نویز نمک و فلفل[۳] است (Marqeus,2011,275). این نویز به صورت تصادفی پیکسل‌های تصویر را تغییر می‌دهد. برای پیاده کردن ایده‌ی پیشنهادی، می‌بایست نویز مورد نظر را فقط در یکی از کانال‌های رنگی تصویر ایجاد کرد. اگر نویز بر روی همه‌ی کانال ها اعمال شود، پیکسل‌های تصویر خراب شده و فیلتر نوری برای حذف نویز کار نمی‌کند.

فیلترهای نوری میان‌ناگذر، یک محدوده کوچک از طول موج را از خود عبور نمی‌دهند. پس برای ایجاد نویز، طول موجی که فیلتر کمترین گذردهی را دارد را انتخاب کرده و با محاسبه RGB آن، نویز را در آن کانال ایجاد می‌کنیم.

برای مثال، یک فیلتر میان ناگذر با طول موج قطع ۵۱۰ نانومتر را در نظر می‌گیریم. طول موج ۵۱۰ نانومتر برابر با RGB(0,255,0) (رنگ سبز) می‌باشد. پس در کانال G تصویر نویز را اعمال می‌کنیم. بدین صورت که به صورت تصادفی درایه‌های ماترین کانال G را به ۲۵۵ تغییر می‌دهیم. با این کار تصویر از حالت اصلی خود خارج می‌شود ولی شخصی که از فیلتر استفاده می‌کند، چون

[۳] Salt & Pepper Noise

RGB(0,255,0) برابر با طول موج ۵۱۰ نانومتر است، این رنگ از فیلتر عبور نمی‌کند و کاربر می‌تواند تصویر را به صورت خوبی ببیند.

نرم‌افزار نصب شده بر روی تلفن همراه، با استفاده از تنظیمات اولیه طول موج مورد نظر، نویز را روی تصویر صفحه نمایش ایجاد می‌کند. کاربران مجاز می‌توانند با استفاده از عینک مخصوص ساخته شده از فیلتر میان‌ناگذر با طول موج قطع مربوطه، تصویر را مشاهده کنند، ولی کاربرانی که از فیلتر استفاده نمی‌کنند تصویر را به وضوح نمی‌بینند.

۴- شبیه سازی

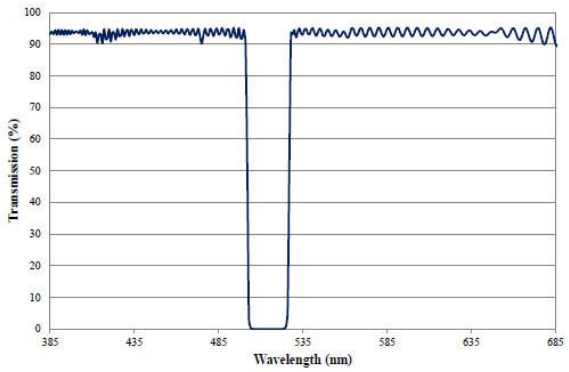
برای شبیه‌سازی قسمت نرم‌افزاری ایده‌ی پیشنهادی، از کد نویسی در نرم‌افزار متلب[۴] استفاده شده است. کتابخانه‌ی نویز نمک و فلفل در متلب وجود دارد. با استفاده از آن، یک ماتریس صفر با اندازه‌ی تصویر اصلی ایجاد می‌کنیم و سپس نویز در آن اعمال می‌شود. یعنی به صورت تصادفی درایه‌های آن مقادیر ۰ یا ۲۵۵ می‌گیرند.

سپس، ماتریس نویز تولید شده را درکانال سبز تصویر اصلی‌مان می‌ریزیم. یعنی درایه‌های ماتریس کانال G تصویر، مقادیر نویز (۰ یا ۲۵۵) را به خود می‌گیرد. شکل‌های (۱۰) و (۱۱) تصویر اصلی و تصویر با نویز را نشان می‌دهد.

شکل (۱۰) تصویر اصلی

شکل (۱۱) تصویر با نویز

فیلتر نوری میان‌ناگذری که برای این کار استفاده شده است، OD 4 notch filter با طول موج قطع در محدوده‌ی ۵۰۰ تا ۵۵۰ نانومتر، محصول شرکت Edmond Optic است. در شکل (۱۲) نمودار گذردهی این فیلتر نشان داده شده است.



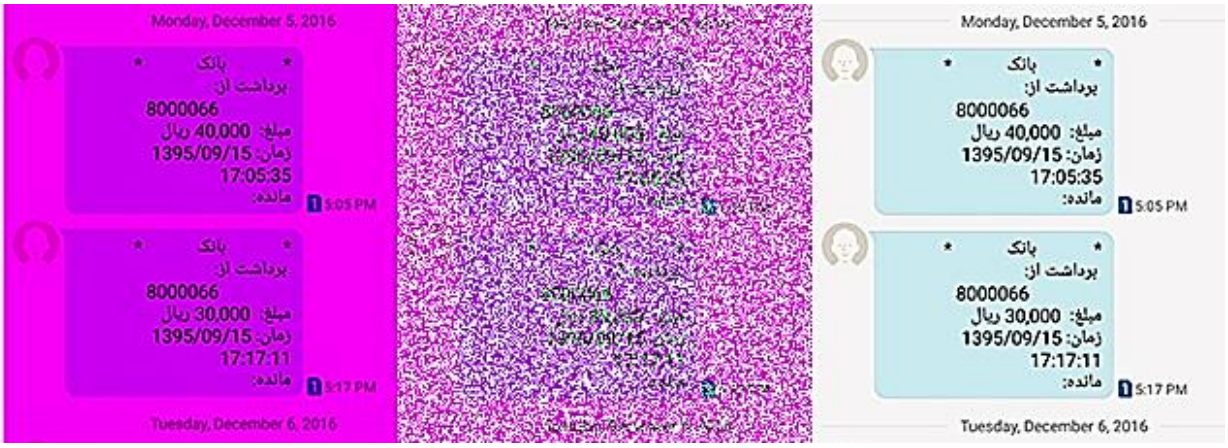
[۴] MATLAB

شکل (۱۲) نمودار گذردهی فیلتر

این فیلتر، طول موج ۵۱۰ نانومتر را از خود عبور نمی‌دهد. این طول موج در مدل سه رنگ با RGB(0,255,0) مشخص می‌شود. پس ماتریس کانال سبز تصویر عبوری از فیلتر، یک ماتریس صفر خواهد بود. از طرف دیگر، ما نویز را بر روی کانال سبز اعمال نمودیم. پس شخصی که از فیلتر استفاده می‌کند، کانال سبز تصویر (نویز) را نخواهد دید. شکل (۱۲)، تصویر دیده شده توسط کاربر استفاده کننده از فیلتر را نشان می‌دهد.

شکل (۱۲) تصویر دیده شده توسط کاربر پس از استفاده از فیلتر

مثالی دیگر از عملکرد روش پیشنهادی در شکل (۱۳) دیده می‌شود. در این مثال تصویر شامل متن است. در سمت راست تصویری از صفحه‌ی پیامک‌های تراکنش بانک است. شکل وسط، همان صفحه با افزوده شدن نویز مشاهده می‌شود. سمت چپ تصویر مشاهده شده توسط کاربر پس از استفاده از فیلتر را نشان می‌دهد.



شکل (۱۳) عملکرد روش پیشنهادی

۵- مقایسه‌ی روش‌ها و بحث

در بخش دوم این پژوهش، چهار روش که به کمک سخت‌افزار و نرم‌افزار، حریم خصوصی دیداری کاربران را محافظت می‌کنند، معرفی شدند. در دو جدول (۱) و (۲) به صورت خلاصه نقاط قوت و ضعف این روش‌ها در کنار هم آورده شده است.

جدول (۱) مقایسه نقاط قوت و ضعف روش‌های سخت‌افزاری

روش	قوت	ضعف

حفظ هوشمند حریم خصوصی بر پایه حسگرهای چندگانه مرکب	- تعریف چندین کاربر مجاز - دقت در تشخیص متجاوز و فاصله به دلیل استفاده از دوربین قدرتمند و حسگر فاصله‌سنج	- هزینه بالا - نیاز به قدرت پردازشی بالا و مصرف انرژی - عدم تشخیص متجاوزین مجاور که در دید دوربین نیستند
Screen Privacy Protector 3M Company , US	- عملکرد عالی در محدود ساختن دید و حفظ حریم خصوصی دیداری از افراد همجوار - عدم نیاز به قدرت پردازشی و مصرف باتری	- قیمت بالا و در دسترس نبودن - عدم کنترل‌پذیری، برای برداشتن این قابلیت باید برچسب را جدا کرد

جدول (۲) مقایسه نقاط قوت و ضعف روش‌های نرم‌افزاری

روش	قوت	ضعف
حفظ کاربران موبایل از حملات دیداری حریم خصوصی (iAlert)	- عدم نیاز به افزودن ماژول اضافی - تعریف چندین کاربر مجاز - هشدار به کاربر - هزینه کم	- نیاز به قدرت پردازشی بالا و مصرف انرژی - عدم‌تشخیص متجاوزین مجاور که در دید دوربین نیستند - دقت پایین به دلیل ضعف دوربین جلوی تلفن
Screen Privacy Filter Using Software USPatent , 2015	- عدم نیاز به حسگر و دوربین - حفظ حریم خصوصی دیداری از افراد همجوار در جهت‌های مختلف - هزینه کم	- نیاز به قدرت پردازشی بالا و مصرف انرژی

۵-۱- نقاط قوت و ضعف روش حفظ هوشمند حریم خصوصی بر پایه حسگرهای چندگانه مرکب

در روش " حفظ هوشمند حریم خصوصی بر پایه حسگرهای چندگانه مرکب " قابلیت تعریف چند کاربر مجاز برای دیدن صفحه‌نمایش وجود دارد. از طرفی به خاطر افزوده شدن دوربین قدرتمند به گوشی، دقت در تشخیص متجاوزگر بالا است.

از طرفی به خاطر افزوده شدن سه ماژول اضافی به گوشی، هزینه بالایی برای کاربر تحمیل می‌شود. همچنین هرکدام از سه ماژول نام‌برده برای عملکرد خود نیاز به مصرف انرژی دارد که باید از باتری گوشی تأمین شود. نکته دیگر اینکه دوربین به‌کاربرده شده در این روش، توانایی رصد محدوده از اطراف کاربر را دارد و متجاوزینی که در دید دوربین نباشند تشخیص داده نمی‌شوند.

۵-۲- نقاط قوت و ضعف روش فیلتر حفظ حریم خصوصی

در این روش دیگر نیازی به افزودن حسگر یا سخت‌افزاری اضافه به تلفن هوشمند نیست درنتیجه برای عملکرد آن نیاز به استفاده از باتری وجود ندارد. همچنین قابلیت محدود کردن زاویه دید و عملکرد آن در حد عالی است به‌گونه‌ای که با استفاده از این برچسب دیگر نگرانی از تجاوز به حریم خصوصی دیداری کاربر از بین می‌رود.

برای تهیه یک برچسب محافظ حریم خصوصی محصول شرکت 3M ، بسته به اندازه برچسب در حدود ۱۰۰ دلار آمریکا هزینه لازم است. مهم‌ترین ضعف این روش در این است که کاربر با نصب آن روی صفحه‌نمایش گوشی خود، دیگر زاویه دید وسیع گوشی خود را از دست می‌دهد. یعنی اگر کاربر بخواهد تصویری را به همراه اطرافیان خود تماشا کند باید این برچسب را از گوشی جدا کند و در این صورت برچسب دیگر غیرقابل استفاده خواهد شد. پس در این روش کاربر کنترلی بر روی کیفیت حفظ حریم خصوصی دیداری تلفن هوشمند خود نخواهد داشت.

۵-۳- قاط قوت و ضعف روش حفظ کاربران موبایل از حملات دیداری حریم خصوصی

روش‌های نرم‌افزاری مزیت عدم نیاز به افزودن ماژول اضافی به گوشی را دارند درنتیجه هزینه آن‌ها کمتر است. در این نرم‌افزار نیز قابلیت تعریف چندین کاربر مجاز وجود دارد. عملکرد نرم‌افزار به‌گونه‌ای است که در صورت شکسته شدن حریم خصوصی دیداری به کاربر هشدار می‌دهد که این خود یک مزیت است که کاربر بداند چه اتفاقی در اطرافش در حال رخ دادن است.

نرم‌افزار از الگوریتم‌های تشخیص چهره برای عملکرد خود استفاده می‌کند. این الگوریتم‌ها نیاز به قدرت پردازشی بالایی دارند درنتیجه نرم‌افزار قابلیت اجرا بر روی گوشی‌های رده پایین را ندارد. از طرفی هرچه نیاز به قدرت پردازشی بالاتری باشد مصرف باتری نیز بیشتر می‌شود.

این نرم‌افزار از دوربین جلوی گوشی برای عملکرد خود استفاده می‌کند. دوربین‌های جلو معمولاً کیفیت پایینی دارند درنتیجه دقت نرم‌افزار در تشخیص متجاوزین پایین است. همچنین به دلیل محدود بودن زاویه دید دوربین جلوی گوشی، متجاوزینی در کنار دست کاربر به صفحه‌نمایش او نگاه می‌کنند تشخیص داده نمی‌شود و فقط برای محافظت از پشت سر کاربرد دارد.

۵-۴- نقاط قوت و ضعف اختراع فیلتر حفظ حریم خصوصی با استفاده از نرم‌افزار

باآنکه جزئیات دقیقی از این اختراع موجود نیست ولی خود اختراع مدعی است که زاویه دید صفحه‌نمایش را تا حد بسیار خوبی از همه جهات محدود می‌کند. این روش نیز چون بر پایه نرم‌افزار است درنتیجه نیاز به افزودن ماژولی اضافه به گوشی ندارد و هزینه آن پایین‌تر است.

تنها نقطه‌ضعف این نرم‌افزار نیاز آن به قدرت پردازشی است که البته به خاطر ساده بودن عملکرد، به نظر می‌رسد بتوان نرم‌افزار را روی گوشی‌های میان رده و پایین رده نیز به کار برد.

البته برای اثبات ادعای این اختراع، تلاش شد تا آن را شبیه‌سازی کنیم که متاسفانه نتیجه‌ای حاصل نشد.

۵-۵- نقاط قوت و ضعف روش پیشنهادی

روش پیشنهادی با بهره‌گیری از سخت افزار و نرم‌افزار ارائه شده است. پس می‌توان گفت ترکیبی از نقاط ضعف و قوت روش‌های فوق در آن حاصل شده است.

اولین و مهمترین نقطه ضعف روش پیشنهادی در استفاده از فیلتر نوری میان‌ناگذر به عنوان عینک کاربردی برای کاربر است. هزینه‌ی ساخت این فیلتر به نسبت بالاست و کاربر ممکن است در استفاده از آن احساس راحتی نکند.

نقطه ضعف دیگر روش پیشنهادی در کیفیت تصویری که کاربر پس از استفاده از فیلتر می‌بیند است. برای اینکه ایده به درستی عمل کند مجبوریم نویز را فقط در یک کانال اعمال کنیم که این باعث می‌شود تصویری که کاربر بعد از استفاده از عینک مشاهده می‌کند، یکی از کانال‌های رنگی را شامل نشود و تصویر به صورت دو رنگ دیده شود. البته این افت کیفیت در تصاویر مختلف متفاوت است.

اما مهمترین نقطه قوتی که روش پیشنهادی دارد، قدرت آن در حفظ حریم خصوصی دیداری کاربران، در همه‌ی زوایا می‌باشد. در عین حال این قابلیت وجود دارد که کاربر هر زمان که اراده کرد از این سیستم استفاده کند و در زمان‌های دیگر به طور عادی از گوشی همراه خود استفاده کند که این کنترل پذیری روش را می‌رساند.

در یک جمع‌بندی از نقاط قوت و ضعف روش‌ها، می‌توان نتیجه گرفت که در صورت کم شدن هزینه‌ی ساخت فیلتر نوری، روش پیشنهادی از سایر روش‌های موجود بهتر است.

در جدول (۳) نقاط قوت و ضعف روش پیشنهادی به طور خلاصه بیان شده است.

جدول (۳) خلاصه ای از نقاط قوت و ضعف روش پیشنهادی

قوت	ضعف
- قدرت بالا در حفظ حریم خصوصی در همه‌ی زوایا - قابلیت کنترل پذیری بالا - نیاز به توان پردازشی و مصرف انرژی پایین نرم‌افزار به نسبت روش‌های دیگر	- هزینه‌ی نسبتاً زیاد ساخت فیلتر - عدم راحتی استفاده از عینک - افت کیفیت تصویر

با وجود نقاط ضعف روش پیشنهادی، به دلیل بهره‌مندی از نقاط قوت آن به نسبت سایر روش‌های موجود، می‌توان استفاده از این سیستم را برای شرایط خاص که نیاز به حفظ حریم خصوصی دیداری بسیار مهم است، ایده‌آل دانست.

۶- نتیجه‌گیری و پیشنهادات

مدت زیادی از عرضه تلفن‌های هوشمند با صفحه‌نمایش باکیفیت به بازار نمی‌گذرد و نگرانی‌ها درزمینه‌ی حریم خصوصی دیداری در حال افزایش است. با توجه به اینکه تمامی تحقیقات مربوط به ۳ سال اخیر است، نیاز به یک روشی که بتواند با فراهم نمودن راحتی و هزینه کم، حریم خصوصی دیداری کاربران را تا حد خوبی حفاظت کند، احساس می‌شود.

در بین روش‌های معرفی شده در بخش دوم پژوهش، اختراع "فیلتر حفظ حریم خصوصی صفحه‌نمایش با استفاده از نرم‌افزار" بیشترین میزان کارایی و کمترین هزینه را برای کاربر دارد. اما نیاز است تا ادعاهای این روش به‌صورت علمی و عملی ثابت شود، یا اگر بتوان روشی شبیه به این اختراع (فقط با اتکا به نرم افزار) برای حفظ حریم خصوصی دیداری به وجود آورد، کار بسیار مهمی انجام شده است.

در بخش مقایسه نقاط قوت و ضعف روش‌ها به این نتیجه رسیدیم که روش‌هایی که از سخت‌افزار برای امر حفاظت از حریم خصوصی دیداری استفاده می‌کنند هزینه‌بر هستند و برای کاربران راحتی لازم را ندارد. در مقابل روش‌های نرم‌افزاری هزینه کمتری دارند اما مشکل نیاز به قدرت پردازشی و مصرف باتری در آن‌ها وجود دارد. پس در کارهای آینده بهتر است تا آنجایی که امکان دارد از سخت‌افزاری علاوه بر خود تلفن هوشمند استفاده نشود تا هزینه و راحتی بیشتری برای کاربر فراهم شود. همچنین می‌توان به بررسی میزان مصرف باتری و قدرت پردازشی روش‌ها پرداخت و برای بهبود آن‌ها تحقیق کرد.

پیرامون روش پیشنهادی این پژوهش، موارد زیر به عنوان کارهای آینده معرفی می‌شود:

۱- کم کردن هزینه ساخت فیلتر میان ناگذر نوری و بهبود عملکرد آن.

۲- راحت کردن کار با عینک مخصوص، به طور مثال تلفیق آن با عینک‌های دودی برای کم کردن نیاز به حمل چند عینک.

۳- معرفی یک نوع نویز متحرک برای ایجاد خطای دید بیشتر.

مراجع

- 3M US Company, www.3m.com
- Brudy, F., Greenberg, S., Butz, A., (2014), Is Anyone Looking? Mitigating Shoulder Surfing on Public Displays through Awareness and Protection, *Proceedings of International Symposium on Pervasive Displays*, 1-6
- CIE (1931), Commission international de l'Eclairage proceedings, Cambridge
- Edmund Optics Inc, www.edmundoptics.com/optics/optical-filters/notch-filters
- Eunus, M., Ahmed, I., Hashem, T., Kulik, L., Tanin, E., (2014), Protecting Mobile Users from Visual Privacy Attacks, *UBICOMP ACM*, 7-13
- Honan, B., (2012), Visual data security white paper, http://www.visualdatasecurity.eu/wp-content/uploads/2012/07/Visual-Data-Security-White-Paper.pdf
- Iachello, G., Hong, J., (2007), End-user privacy in human-computer interaction, *Foundations and Trends in Human-Computer Interaction*, 1(1), 1-137

- Jayaraman, R., (2009), Digital Image Processing, Tata McGraw Hill Education
- Lian, S., Hue, W., Song, X., Liu, Z., (2013), Smart Privacy-Preserving Screen Based on Multiple Sensor Fusion, *IEEE Transactions on Consumer Electronics*, 136-49
- Marqeus, O., (2011), Practical Image and Video Processing Using MATLAB, Wiley
- Sencar, H., Velastin, S., Nikolaidis, N., Lian, S., (2010), Intelligent Multimedia Analysis for Security Applications, Springer
- Smith, T., (1931), The C.I.E. colorimetric standards and their use, *Transactions of the Optical Society*, 33(3), 73-134
- Yang, Q., Li, Z., (2015), Screen Privacy Filter Using Software, US Patent 9058509
- Ying, J., (2012), Low Glare Lighting for A Transit Vehicle, US Patent US8210724