# Protecting Mobile Users from Visual Privacy Attacks

**Mohammed Eunus Ali**
CSE Department
Bangladesh University of Engineering and Technology
Dhaka 1000 Bangladesh
eunus@cse.buet.ac.bd

**Tanzima Hashem**
CSE Department
Bangladesh University of Engineering and Technology
Dhaka 1000 Bangladesh
tanzimahashem@cse.buet.ac.bd

**Anika Anwar**
CSE Department
Bangladesh University of Engineering and Technology
Dhaka 1000 Bangladesh
anika.anwar@yahoo.com

**Lars Kulik**
CIS Department
University of Melbourne
VIC 3010 Australia
lkulik@unimelb.edu.au

**Ishrat Ahmed**
CSE Department
Bangladesh University of Engineering and Technology
Dhaka 1000 Bangladesh
ishratahmedmren@yahoo.com

**Egemen Tanin**
CIS Department
University of Melbourne
VIC 3010 Australia
etanin@unimelb.edu.au


*UbiComp'14* Adjunct, September 13-17, 2014, Seattle, WA, USA
ACM 978-1-4503-3047-3/14/09.
http://dx.doi.org/10.1145/2638728.2638788

## Abstract
An increasing number of people are using mobile devices in public places such as buses, trains, airports, coffee shops, and restaurants. Though the flexibility to work remotely using mobile devices make people more productive, this new working practice incurs un-authorized visual access of the mobile display by the bystanders, which we call *visual privacy attack*. Failing to prevent un-authorized people viewing sensitive information such as passwords, emails, and business information could lead to financial loss, public exposure, and embarrassment. In this paper, we propose a solution that captures the surrounding environment through user's mobile phone camera and determines whether any un-authorized person is obtaining visual access to the user's mobile screen. We develop an Android application, *iAlert*, that runs as a background process on a user's mobile device and alerts the user based on whether or not the displayed text on the screen is readable by bystanders.

## Author Keywords
Visual Privacy; Shoulder Surfing

## ACM Classification Keywords
H.5.m [Information interfaces and presentation]: Miscellaneous.

## Introduction

The advancement of mobile and internet technologies enables people to work virtually from any place using their mobile devices. Though the flexibility of working remotely, in particular in public places (e.g., buses, trains, and coffee shops) make people more productive, this new working practice comes along with a number of risks. One of the major risks involves un-authorized visual access to the user mobile screen by bystanders, which we call *visual privacy attack*. A recent survey by UK Polling organization ComRes shows that 71% of the surveyed people have been able to see or read what other people are doing in their computing devices - either in workplaces or in public places [4]. In particular, with the arrival of modern and bigger screen technologies that provide higher and sharper resolutions with quality displays, un-authorized people can now easily read or see what is going on the mobile screen of a user from a distant position. The un-authorized viewing of a user's sensitive information such as passwords, emails, and business information could potentially lead to financial loss, public exposure, and embarrassment.

To protect the mobile screen from un-authorized visual access by bystanders from various angles (e.g., 60 degree in either side of the device), different hardware companies make privacy screen protectors for mobile users [3]. These protectors cannot prevent bystanders from viewing the device for many viewpoints, and also most users do not like the reduced quality and sensitivity of the screen with a protector. To protect passwords or PINs from shoulder surfing by an un-authorized user, a large body of graphical or gaze based techniques have been proposed (e.g., [5, 6]). These techniques cannot prevent bystanders to read or see what is going on the screen of in general. In this paper, we propose the first *reactive* solution, iAlert (read Eye Alert), to combat visual privacy attacks on mobile user screen in public places.

The key idea of the iAlert is to capture the surrounding environment through user's mobile phone camera to identify whether any un-authorized person is getting visual access to the user's mobile screen. To determine whether a bystander can read the displayed text, we exploit the *eyedistance*, measured as the distance between a pair of eyes, of the bystander. A bystander with a smaller eyedistance is further away from the screen than a bystander with a larger eyedistance. Based on the eyedistance and the reference point, i.e., the midpoint of two eyes, of the detected face, we have derived a linear regression model from test data to infer the distance (i.e., depth) and angle (i.e., orientation) of the bystander with respect to the mobile screen. Finally, by using the concept of visual acuity test [1], iAlert gives an alert to the user whether the displayed text on screen is readable by bystanders positioned at different locations.

We have built a prototype application of iAlert in the Android platform that runs as a background process in a user's device. iAlert gives a red alert (like a traffic light signal) to a user if it finds that the displayed text is readable by any bystander. On the other hand, iAlert shows a green signal on the screen if the displayed text is not readable by any bystander. If iAlert cannot determine or not a bystander can read the displayed text, it shows a yellow alert to the user. Our experimental results show that iAlert can identify quite accurately whether a text/screen is readable or not by bystanders.

## iAlert: Combating Visual Privacy Attacks

In this paper, we propose a software solution, iAlert, for mobile users to combat visual privacy attacks in public

places. The operation of iAlert is summarized in the following steps:

1. The mobile device captures the surrounding environment through image capturing via the front camera.
2. iAlert applies a face detection algorithm to identify human faces from its surroundings.
3. The system then identifies faces of different sizes based on their eyedistance measured as the distance between the detected pair of eyes, computes the midpoint of two eyes as the reference point.
4. Our algorithm then applies a linear regression model to determine the distance (depth) and the angle (orientation) between the reference point of the face and midpoint of the mobile screen.
5. Based on calculated distance and angle, our system can determine whether the text displayed on the mobile screen is readable or not. We use the Snellen chart [1] to determine the visual acuity of a person.
6. Finally, our system alerts a user with red, yellow, and green signals (analogous to traffic lights), where the red alert is use when the displayed text can be read by any bystander, the green signal represents the state that no bystander can read the text, and the yellow signal indicated the system is unsure whether the text is readable or not by a bystander.

Steps 1 and 2 are straightforward. In Step 3, our face detection algorithm returns two parameters: eye-distance ($E_d$) and reference point ($R.x, R.y$). To derive a linear regression model in Step 4, we have collected eye distance and the reference point for 100 test cases in different settings and measured the distance ($D_r$) and angle ($\alpha$) of between each reference point and the corresponding mobile screen position. From these test data sets we derived the following linear-regression models for calculating $D_r$ and $\alpha$ for any detected face as follows: $\alpha = 2.300950943 \times 10^{-1} * R.x - 7.098698681 \times 10^{-2} * R.y + 64.1716$ and $D_r = -1.541290634 \times 10^{-2} * R.x + 5.2198 \times 10^{-2} * R.y - 5.166925 \times 10^{-1} * E_d + 0.0979 * \alpha$. Finally, we use Snellen chart [1] to determine the minimum font size that can be read from a certain distance when the observer is at $90^{\circ}$ position to the screen, and then apply the oblique projection technique to determine the perceived font size from a certain angle.

## Demo and Evaluation

We have developed an Android prototype of iAlert as a proof of concept of our approach being applied in real world scenarios to combat visual privacy attacks. We have tested the accuracy of our approach in 15 different settings with three users, and found that in 80% of the cases, iAlert accurately gives red and green alerts to the user. On other hand, 13% of the cases are identified where iAlert gives the green signal, but a bystander can actually read it, and in 7% of the cases iAlert gives a red signal but a bystander cannot read the text.

Figures 1-4 show few screenshots from our iAlert application. Figure 1 shows two bystanders who are shoulder surfing to a user's (in the middle) mobile screen. Since these two bystanders are far away and not in a position to read the displayed text on the mobile screen, iAlert gives a green signal to the user at the time of login as shown in Figure 2. Similarly, Figure 3 and Figure 4 show the nearby bystanders positions and the red alert in the user's mobile screen, respectively.

**Figure 1:** A user and two bystanders far away from the screen.

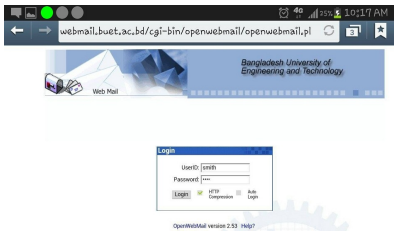

**Figure 2:** A login screen with no privacy risk (green light on the top-left corner).

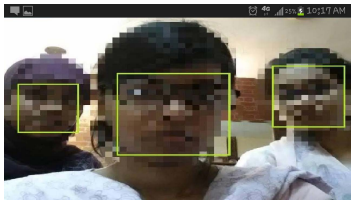

**Figure 3:** A user and two bystanders very close to the screen.

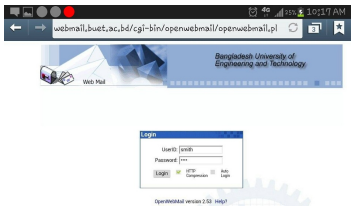

**Figure 4:** A login screen with high privacy risk (red light on the top-left corner).

## Discussion

Since the current state of the front-camera of a mobile device does not have a wide view angle, a user needs to tilt the device in different directions to check any privacy threats. We envision that future mobile cameras will incorporate wide-angle lenses.

For the face detection part, we have used the face detector available in the Android API [2]. It gives real-time face detection facilities for a given image. However, keeping the camera on and having a continuous processing will discharge the battery very fast. Since only a fraction of applications is privacy sensitive to a user, in future, we will add a control panel for the user to bind iAlert with applications having privacy sensitive components.

## Conclusion and Future Works

We propose a reactive solution, iAlert, to combat a widespread problem of visual privacy attacks on mobile users. iAlert enables a mobile user to be aware of the surrounding environment about possibly visual privacy risks and allows working privately on mobile devices in public places. Our work opens a new avenue for a number of potential future works that include developing methods for automatically adjusting screen/font size based on the positions of bystanders to make the text difficult to read for the bystanders, identifying highly sensitive areas (e.g., Textbox) of different applications and finding appropriate methods to ensure strong privacy for these areas.

## Acknowledgements

This work was done at Samsung Innovation Lab, Department of CSE, BUET, and partially supported by the NICTA Victoria Research Laboratory.

## References

[1] Eye chart. http://www.teachengineering.org/collection/cub_/activities/cub_human/cub_human_lesson06_activity1_eyechart.pdf.

[2] Face detector. http://developer.android.com/reference/android/media/FaceDetector.Face.html.

[3] How screen privacy works. http://solutions.3m.com/wps/portal/3M/en_US/3MScreens_NA/Protectors.

[4] Visual data security white paper. http://www.visualdatasecurity.eu/wp-content/uploads/2012/07/Visual-Data-Security-White-Paper.pdf.

[5] Kim, S.-H., Kim, J.-W., Kim, S.-Y., and Cho, H.-G. A new shoulder-surfing resistant password for mobile environments. In *ICUIMC* (2011), 27:1–27:8.

[6] Kumar, M., Garfinkel, T., Boneh, D., and Winograd, T. Reducing shoulder-surfing by using gaze-based password entry. In *SOUPS* (2007), 13–19.