Poster: Keep Others from Peeking at Your Mobile Device Screen!

Chun-Yu (Daniel) Chen, Bo-Yao Lin, Junding Wang, and Kang G. Shin
CSE/EECS, University of Michigan
Ann Arbor, MI, USA
{chunyuc,boyaolin,jundwang,kgshin}@umich.edu

ABSTRACT

The information displayed on mobile device screens can be seen by nearby (unauthorized) parties, called *shoulder surfers*. To protect sensitive on-screen information, we have developed `HideScreen` by utilizing the human vision and optical system properties to hide the users' on-screen information from the shoulder surfers.

Specifically, `HideScreen` discretizes the on-screen information (OSI) into grid patterns to neutralize the low-frequency components so that the OSI will "blend into" the background when viewed from the outside of the designed range. We have developed and evaluated several ways of hiding both on-screen texts and images from shoulder surfers. Our extensive experimental evaluation of `HideScreen` has demonstrated its high protection rates (>96% for texts and >99% for images) while providing good user experience.

CCS CONCEPTS

• **Security and privacy → Privacy protections**.

KEYWORDS

Shoulder surfing; mobile privacy; privacy protection; human machine interaction

ACM Reference Format:
Chun-Yu (Daniel) Chen, Bo-Yao Lin, Junding Wang, and Kang G. Shin. 2019. Poster: Keep Others from Peeking at Your Mobile Device Screen!. In *The 25th Annual International Conference on Mobile Computing and Networking (MobiCom '19), October 21–25, 2019, Los Cabos, Mexico.* ACM, New York, NY, USA, 3 pages. https://doi.org/10.1145/3300061.3343384

MobiCom '19, October 21–25, 2019, Los Cabos, Mexico

ACM ISBN 978-1-4503-6169-9/19/10.
https://doi.org/10.1145/3300061.3343384

Figure 1: A common case of shoulder surfing in a train/bus and the effect of applying our proposed solution, `HideScreen`.

1 INTRODUCTION

People use mobile devices everywhere they go and run all kinds of tasks/apps that could be personal or sensitive. Peeking at other users' device screen without their permission is an act of *shoulder surfing* (Fig. 1). Although users will take proper defensive actions when they beware of someone else's peeking at their device screens, they are reported to beware of only 7% of shoulder surfing incidents [3]. Moreover, Aviv *et al.* [1] have shown that a shoulder surfer can succeed in obtaining a 6-digit PIN with a 10.8% probability by taking just one peek. Users may try to avoid viewing sensitive/private information in public areas, but cannot always help it. For example, the Justice Secretary of Philippines, Vitaliano Aguirre II, was enraged at the leakage of his text messages by someone who had peeked at, and taken a picture of, his smartphone screen during a Senate hearing [5].

Considering the possible leakage of sensitive on-screen information (SOSI) and the lack of its effective protection, we would like to enable information senders/providers to *proactively* protect SOSI instead of *passively* relying on the awareness and presence of a privacy film at the receivers. We meet this goal by developing a novel solution, called `HideScreen`, for SOSI protection without requiring any additional hardware. It (i) can protect the SOSI without compromising users' intended tasks/apps, and (ii) is simple enough to implement and run on commodity mobile devices while consuming as little resources (*e.g.*, computing power and energy) as possible to support good user experience.

Based on optical system properties of minimum resolvable angle [6] and the average limitation of human vision [4], `HideScreen` uses grid patterns to inject high spatial frequency components into the information to be displayed,

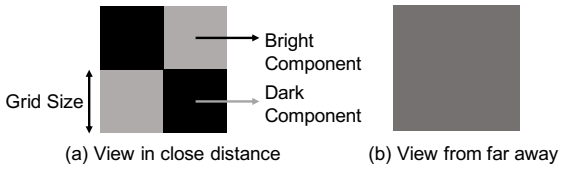
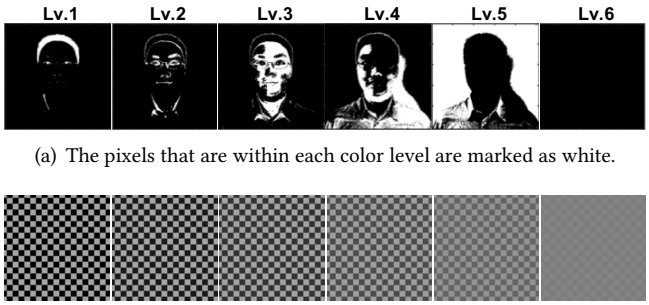


Figure 2: Basic concept of `HideScreen`

(a) Example of basic protection by grids

(b) Example of `HideText`

Figure 3: Text protection examples



(a) The pixels that are within each color level are marked as white.

(b) The pixels marked as white in each level are replaced by the corresponding grids.

Figure 4: Example of applying color level partition

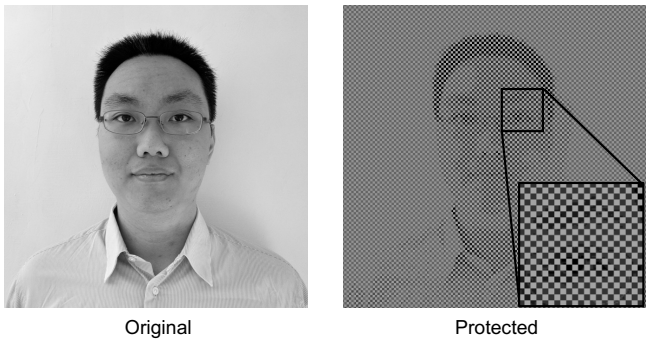


Figure 5: Example of applying `HideImage` protection

thereby neutralizing the low-frequency components that are easily viewable by shoulder surfers. This way, the information to be protected can only be viewed within the designed range (d_{max}). This mechanism is equivalent to moving the low-frequency components to the higher-frequency space that cannot be seen by shoulder surfers.

Furthermore, since `HideScreen` does not rely on the spatial frequency of the OSI itself to provide protection, the viewable range of the protected information can be adjusted dynamically and automatically based on the user's viewing distance by changing the grid parameters, thus broadening its use for various applications with different requirements.

`HideScreen` is tailored to meet the need of apps that display some short but sensitive information — such as PIN, account/password, and partially-personal messages — and protect the OSI from unauthorized parties located outside of the designed viewing range. Specifically, `HideScreen` focuses on the protection of short texts on the screen which can also protect the texts shown on soft keypad/keyboard. When key shuffling is used, `HideScreen` will prevent a shoulder surfer from acquiring sensitive information by observing the on-screen locations the user touches. Other than on-screen texts, some images, such as personal photos or the security picture used for bank account login, can also be privacy/security-sensitive, and hence `HideScreen`'s protection is extended to on-screen images.

2 SYSTEM DESIGN

`HideScreen` is built on one basic idea: if a user views a grid pattern within the designed range, s/he will see the grid (Fig. 2a), else s/he will only see an area of single color (Fig. 2b). The visible range of the grid is determined by the grid size (Fig. 2a). `HideScreen` captures the information to be shown on the screen and transforms it into an image composed of grids.

We can utilize grids for hiding OSI because if a person views the grid from the outside of the visible range, s/he cannot resolve the bright and dark components into two individual sources. Therefore, s/he will only see the "mixture" of the two light sources. By utilizing this property, we can use the grid to create a pattern P for a designated visible distance d_{max}. What remains is to find a background B that has the same color as P when viewing from the outside of the visible range. We can then create a grid image $G = P + B$, so that only the person within the visible distance can see the pattern correctly. Figs. 3(a) and 3(b) show an example of applying the grids-based protection to a text (where the word "book" is the P component that is replaced by grids and the gray background is the B component) and its enhanced version for better readability, respectively.

For image protection, `HideScreen` utilizes multiple dark-bright combinations that have the same "average color" as shown in Fig. 4(b) to present corresponding colors in an image (Fig. 4(a)), and combines them to form a protected grid image (Fig. 5).

Case (User Viewing Dist.)	URR	SSRR	SSRR w/ Binoculars
Phone (10-12")	100%	3.8%	0%
Phone (20-24")	96.4%	2.2%	0%
Tablet (≈18")	100%	0.0%	0%
Laptop (≈24")	100%	3.6%	0%

Table 1: Effectiveness of text protection

`HideText`, `HideImage`, and `SelImage` are the three protection schemes employed in `HideScreen`. `HideText` focuses on the protection of texts, and the other two protect images. All of these are designed to protect information by viewing distance and angle, meaning that a shoulder surfer will not be able to read the information correctly from the outside of the designed viewing range. The two image protection schemes differ in loss or no loss of information. `HideImage` protects the images at the cost of some content loss (*i.e.*, not showing the original image on the screen), while `SelImage` protects the images without loss of content, thus allowing a shoulder surfer (SS) to be able to identify the real information with some probability.

3 EVALUATION RESULTS

We use *shoulder surfer recognition rate* (SSRR) and *user recognition rate* (URR) as the metrics for the evaluation of `HideScreen`'s effectiveness. SSRR is defined as the probability that the shoulder surfer successfully reads the information on the screen. SSRR indicates the likelihood to fail to protect the on-screen information. Similarly, URR is defined as the probability that the user successfully reads the information on the screen. URR indicates whether or not the protection scheme maintains the comprehensibility of information. Ideally, SSRR (URR) should be close to 0 (1).

We recruited 20 volunteers of ages 18–40 on our campus for the evaluation of `HideScreen`. The participants will first act as a user to read the information shown on a device screen and then be asked to act as a shoulder surfer that stands behind a user (with 12" distance) to retrieve the information that the user is reading.

The results of text protection effectiveness are summarized in Table 1, showing that `HideText` is able to achieve high URR ($\geq$ 96.4%) and low SSRR ($\leq$ 3.8%).

Tables 2 summarizes the results of the effectiveness of `HideImage` and `SelImage`. `HideImage` is able to achieve 92.5% URR and 0.9% SSRR. For `SelImage`, URR is 100% and SSRR is 2%, indicating `HideScreen`'s protection of information from a SS who tries to read on-screen information. We also asked participants to use binoculars to read the OSI. Participants are then asked whether they have any clue in telling the real object. As expected, none of the participants was able to read the information.

	URR (%)	SSRR (%)	SSRR w/ Bin. (%)
`HideImage` (w/o ref.)	92.5	0.9	0
`SelImage`	100.0	2.0	0

Table 2: Effectiveness of image protection

We conducted user studies by implementing 3 example applications, including PIN code entering, account login, and a messenger. The results show that all the applications can achieve good user experience (71+ SUS score [2]) while providing SOSI protection, and 72+% of the participants indicate that they will use `HideScreen`-supported apps frequently.

4 CONCLUSION

We have proposed `HideScreen` to protect the information displayed on device screens from shoulder surfers. The protection scheme is grounded on optical system properties and human vision characteristics, which provide fundamental protection guarantees. Grids are used to replace low-frequency components so that the information may not be distinguished from the background when viewed from the outside of the designed viewing range. Shoulder surfers or malicious parties will not be able to read the information on the screen while the user can read it without difficulty. Our extensive evaluation has shown `HideScreen` to be able to provide a high rate of on-screen information protection ($>$ 96% for texts and $>$ 99% for images) while incurring low overhead. Furthermore, our use-case study shows that `HideScreen` achieves good user experience while providing privacy protection.

ACKNOWLEDGEMENT

The work reported in this paper was supported in part by the NSF under grants CNS-1505785 and CNS-1646130.

REFERENCES

[1] A. J. Aviv, J. T. Davin, F. Wolf, and R. Kuber. Towards Baselines for Shoulder Surfing on Mobile Authentication. In *Proceedings of the 33rd Annual Computer Security Applications Conference on - ACSAC 2017*, pages 486–498, New York, New York, USA, 2017. ACM Press.

[2] A. Bangor, P. Kortum, and J. Miller. Determining What Individual SUS Scores Mean: Adding an Adjective Rating Scale. *Journal of Usability Studies*, 4(3):114–123, 2009.

[3] M. Eiband, M. Khamis, E. von Zezschwitz, H. Hussmann, and F. Alt. Understanding Shoulder Surfing in the Wild. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems - CHI '17*, pages 4254–4265, New York, New York, USA, 2017. ACM Press.

[4] J. Mannos and D. Sakrison. The effects of a visual fidelity criterion of the encoding of images. *IEEE Transactions on Information Theory*, 20(4):525–536, Jul 1974.

[5] Polotiko. Aguirre furious at photo leak of private text message. http://politics.com.ph/aguirre-furious-photo-leak-private-text-message/, 2017. Accessed: 2018-01-31.

[6] D. Singh. *Fundamentals of optics.* Prentice-Hall Of India, 2015.