Poster: Image-synch: a liveness detection method based on ambient image

Yuan Sun, Huiping Sun✉, Xixin Cao✉
School of Software and Microelectronics
Peking University
yuanyouyuan@pku.edu.cn, {sunhp, cxx}@ss.pku.edu.cn

***Abstract*—Traditionally, face recognition requires additional inconvenient human device interactions to verify users' identity. In this poster, we introduce a novel authentication method, Image-synch. It provides additional information by comparing reflection image from eyes and ambient image from different camera without human device interaction. Confined to the hardware capacity, We build simple prototypes and conduct experiments in the android system, providing empirical evidence that illustrates Image-synch is a robust authentication method. Furthermore, we discovered that it is possible to authenticate without any human device interactions, which indicates the potential of being widely used in future.**

I. Introduction

Traditionally, face authentication method requires inconvenient blinking or nodding, to enhance the authentication system. Research shows that participants are willing to spend about 2.9% of their smartphone challenge and response time with unlocking alone [1].The main reason for the low rate is inconvenient interactions, which causes approximately 40% of smartphone users to abandon the authentication system on their devices [2]–[5]. In this poster, our goal is to propose a novel authentication method, through the use of ambient image to eliminate human device interactions and prevent presentation attack. Our contributions are summarized as follows:

(1) we propose a novel authentication method by synchronizing the eyes reflection image from front camera and ambient image from rear camera. If they match, the presentation attack will be largely prevented without any human device interaction and database. The entropy will be maximum for the constant changing of ambient image (2) we build simple prototypes in the Android system, as smartphones are the most widely used and hardest to be tested. (3) we discuss the main challenges and solutions.

II. Rationale and Discussion

As shown in figure 1, we design the system by using both front and rear cameras. The front camera extracts the corneal reflection. The reflection is from the same view of the rear camera. The rear camera also generates an image from the same direction. And then, we compare these two images. If both of them have the same sychronized image feature and other features match, the user can log into the system. The essence of this novel method is double camera and cross reference. It adds extra information to enhance the security without human device interactions.

Purkinje images are images reflected from different parts of human eyes, which is shown in figure 2. Our eyes reflect lights four times. The first one is from the front surface of the cornea (image a). The second one is from the back surface of the cornea (image b). The last two are from the front and back surface of the lens (image c and d). Most of them are difficult to see. Therefore, we normally use images reflect from the front surface of the cornea (image a). We generally locate the image in the region of the pupil, this region allows us to take an image with a high-resolution rate. As it is shown in Figure 3, we have a digital clock image detected from the pupil by the front camera and a digital clock in the ambient image detected by the rear camera. Only when these two images and other features match, can we prove the user's identity. Adversaries couldn't get this synchronized image in advance, when they replay videos, photos, or present hardcopy to spoof the system.

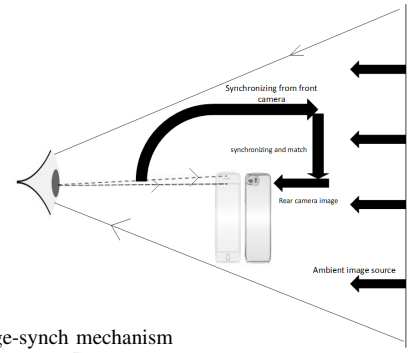


Fig. 1. Image-synch mechanism

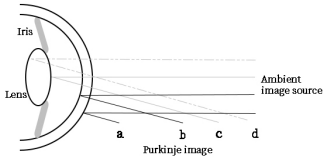
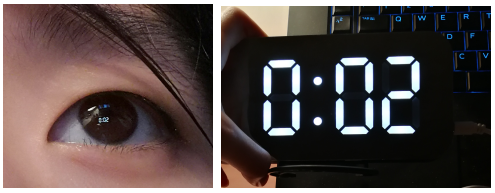


Fig. 2. Four reflections in Purkinje image

The system has endless images from the ambient environment. Thus, the entropy is the maximum and attackers can't record it before the authentication. Normally, we adopt multi-factor system to enhance the security. Knowledge factor and possession factor which in common require information only shared between the user and device. Ambient image changes, like those mechanisms, sends new information to users all the time and only shares the information between the user and the device. If we implement it in authentications like iris, face recognition (inherent factor), the system will be more secure and convenient than before. Except for 3D mask, presentation attacks, e.g. replaying videos, photos, or present hardcopy, will be detected. 3D mask will be discussed in the next part.

The main challenges are low average camera resolution rate, environmental light requirement and 3D mask attack. Actually, the level of environmental light requirement lowering while the camera resolution rate improving. The camera will



(a) Front camera image (b) Rear camera image

Fig. 3. Image-synch without a traditional database

be enhanced in the near future.

The only problem here is the 3D mask attack. Lee et al [6], use four Purkinje images mentioned above (Figure 2) to detect if it is a real iris or a fake one. Four images have a theoretical distance, while fake iris images doesn't. However, except for the first image reflect from the front cornea, other images are almost impossible to get, in the normal environment. The special equipment designed to capture four Purkinje images, is impossible to bring around in our daily life. However, it has been proved in Lee's research that compares to the real eye, fake eyes or contact lens has an obvious big spot around the pupils. The eye reflection image is distorted into a big spot, which is an intrinsic vulnerability of fake iris contact lens. The reflection property changed obviously. It's hard to gauge the distance of Purkinje image in our daily lives. For the 3D mask attack, which has a real eye behind the mask, we can detect the reflection like the big spot or abnormal reflection in their eyes, which has been mentioned in the above research to detect the fake iris. If both are combined, all of the presentation attacks can be prevented without any human device interactions.

In a wider range, eyes reflections should also help us to log into the browsers, PC, access control system, or other system, with additional information from extra cameras which might be located in the front, back or other angle of the users. We can even use it as a special timestamp. The wider range will be part of our future work.

From the discussion above, we have shown that it is possible to find an authentication method which can be used in our daily life and prevent presentation attacks without any human device interactions.

III. Prototype in android system

We adopt an android system to build simple prototypes, as it works best thus so far. The critical environment is still required, so we select a digital clock as the ambient image to be synchronized. Therefore, we check the time in the subject's eyes and from the clock at the same angle. If the synchronized image matches, our system identifies the user. If not, we put it into a fake template.

We build 2 types of prototype:

The first prototype is that we open both of the front and rear camera to detect the image. Having tested a large number of mobile devices, the only one that fits the requirement has a mere 8MP front camera. Therefore, it is still unstable as there are limited angles for the camera to authenticate. We test this version and its performance is not as good as the second prototype. This version is not stable not only because of its resolution rate. Sharpness is another point to influence the result. The requirement of the lens is also high in this situation. There are lots of higher resolution rate mobile devices currently, but the lens is not satisfied with our requirement. The camera in our experiment is from a leading brand, but it only has an 8MP front camera. In this circumstance, the camera's ability to locate eye reflection image is still weak. We may find a camera with a better resolution rate and sharpness later.

In the second prototype, we take the front camera image and the rear camera image and synchronize after saving them in the cellphone. This is more stable than the former method. After this, the mobile device can check the synchronized image successfully and in a stable way.

We tested many methods and finally decide to use OpenCV's Imgproc.matchTemplate function for a limited computational resource of the smartphone. This function detects the highest matching area by sliding one image on the other image. Even with different angles and special reflection property of eyes causing slight view differences, we still could find the highest matching image. Many metrics were tested to select the highest correlated area and TM_CCOEFF_NORMED (formula(1)) showed the best performance. The formula can be seen from formula (1). I represents the source image in which we expect to find a match to the template image. T represents a template image which will be compared to the target image. The range of R value is from -1 to 1. The value of 1 is an ideal matching value which means a perfect match. We use function Core.minMaxLoc() to evaluate output the final result. We set 0.8 as our threshold and can successfully identify the synchronized image and deny the mismatched image. We will conduct experiments in different systems and develop more detection algorithms in our future work.

$$R(x,y) = \frac{\sum_{x',y'}(T'(x',y') * I'(x+x',y+y'))}{\sqrt{\sum_{x',y'} T'(x',y')^2 * \sum_{x',y'} I'(x+x',y+y')}} \quad (1)$$

IV. Conclusion

In this poster, we propose Image-synch, a novel liveness detection method and prove its feasibility through experimenting on a smartphone, as it is the most widely used and hardest to be tested. The challenges and other issues discussed will be our future work.

References

[1] M. Harbach, E. Von Zezschwitz, A. Fichtner, A. De Luca, and M. Smith, "It'sa hard lock life: A field study of smartphone (un) locking behavior and risk perception," in *10th Symposium On Usable Privacy and Security ({SOUPS} 2014)*, 2014, pp. 213–230.

[2] E. Hayashi, O. Riva, K. Strauss, A. Brush, and S. Schechter, "Goldilocks and the two mobile devices: going beyond all-or-nothing access to a device's applications," in *Proceedings of the Eighth Symposium on Usable Privacy and Security*. ACM, 2012, p. 2.

[3] A. Mahfouz, I. Muslukhov, and K. Beznosov, "Android users in the wild: Their authentication and usage behavior," *Pervasive and Mobile Computing*, vol. 32, pp. 50–61, 2016.

[4] S. Egelman, S. Jain, R. S. Portnoff, K. Liao, S. Consolvo, and D. Wagner, "Are you ready to lock?" in *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 2014, pp. 750–761.

[5] O. Riva, C. Qin, K. Strauss, and D. Lymberopoulos, "Progressive authentication: deciding when to authenticate on mobile phones," in *Presented as part of the 21st {USENIX} Security Symposium ({USENIX} Security 12)*, 2012, pp. 301–316.

[6] E. C. Lee, K. R. Park, and J. Kim, "Fake iris detection by using purkinje image," in *International Conference on Biometrics*. Springer, 2006, pp. 397–403.

Poster: Image-synch: a liveness detection method based on ambient image

Yuan Sun, *Huiping Sun, *Xixin Cao
School of Software and Microelectronics
Peking University

Abstract

Traditionally, face recognition requires additional inconvenient human device interactions to verify users' identity. In this poster, we introduce a novel authentication method, Imagesynch. It provides additional information by comparing reflection image from eyes and ambient image from different camera without human device interaction. Confined to the hardware capacity, We build simple prototypes and conduct experiments in the android system, providing empirical evidence that illustrates Image-synch is a robust authentication method. Furthermore, we discovered that it is possible to authenticate without any human device interactions, which indicates the potential of being widely used in future.

Overview

Key Contributions: (1) we propose a novel authentication method by synchronizing the eyes reflection image from front camera and ambient image from rear camera.(2) we build simple prototypes in the Android system, as smartphones are the most widely used and hardest to test. (3) we discuss main challenges and solutions.

Mechanism

Purkinje images:

- Purkinje images (showed in figure 1) are images reflected from different parts of human eyes. Our eyes reflect lights four times. Most of them are difficult to see. Therefore, in the authentication mechanism, we normally use images reflect from the front surface of the cornea (image a).
- We generally locate the image in the region of the pupil, this region allows us to take an image with a high-resolution rate. In Figure 3&4, we have a digital clock reflection detected from the pupil.

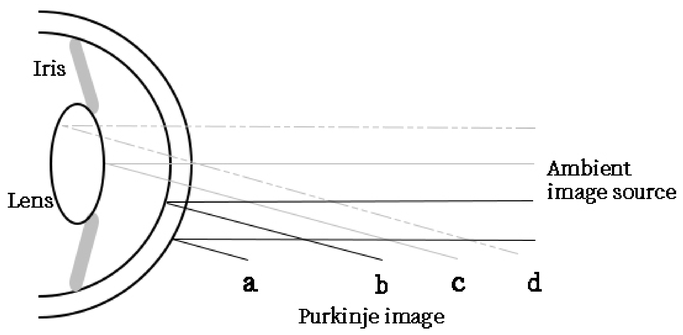


Fig. 1. Four reflections in Purkinje image

The synchronized image system:

- Image-synch has endless images from the ambient environment. The entropy is the maximum and the attacker can't forge it.
- Only the user share the ambient image with the device.
- As it is shown in figure 2, we design the system by synchronizing the ambient image from both front and rear camera.

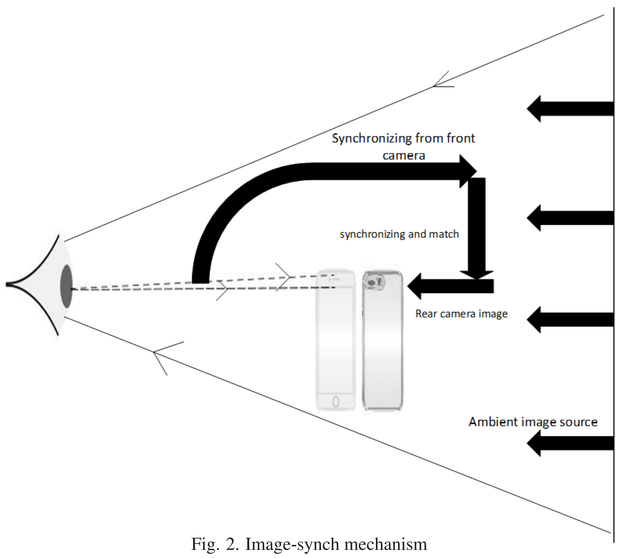


Fig. 2. Image-synch mechanism

Main challenges and discussion

Key Contributions:

- Low average camera resolution rate—hard ware upgrade
- Environmental light requirement—hard ware upgrade
- 3D mask attack — combined with research[1]

Reflection image and Illumination source

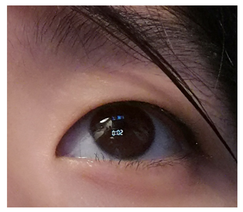


Fig.3-1. Reflection image from front camera

Fig.3-2. Ambient image from rear camera

Reflection image and Illumination source

We can see the system is designed by deploying both front and rear cameras. If both of them have the same image and other features match, the user can log into the system. Even different angles and reflection property of eyes cause slight view differences, we still can find the highest matching image by the function in our experiment.

Fig.4-1. Reflection image from front camera

Fig.4-2. Ambient image from rear camera

Experiment & Prototype in Android System

- We select a digital clock with time in number as the ambient image to be synchronized. Therefore, we check the time in the subject's eyes and from the clock at the same angle and time. If the sychronized image matches, our system accepts the user. If not, we put it into a fake template.
- We implement our experiment in android system, more experiments will be conducted in the future

Conclusion

In this poster, we propose Image-synch, a novel liveness detection method and prove its feasibility through experimenting on a smartphone, as it is the most widely used and hardest to be tested. The challenges and other issues discussed will be our future work.

Reference

[1] E. C. Lee, K. R. Park, and J. Kim, "Fake iris detection by using purkinje image," in International Conference on Biometrics. Springer, 2006, pp. 397–403.