Poster: Toward a Secure QR Code System by Fingerprinting Screens

Yijie Li*
yijieli@sjtu.edu.cn
Shanghai Jiao Tong University
Shanghai, China

Yi-Chao Chen*
yichao@utexas.edu
Shanghai Jiao Tong University
Shanghai, China

Xiaoyu Ji
xji@zju.edu.cn
Zhejiang University
Hangzhou, China

Hao Pan
Lanqing Yang
panh09@sjtu.edu.cn
yanglanqing@sjtu.edu.cn
Shanghai Jiao Tong University
Shanghai, China

Guangtao Xue
gt_xue@sjtu.edu.cn
Shanghai Jiao Tong University
Shanghai, China

Jiadi Yu
jiadiyu@sjtu.edu.cn
Shanghai Jiao Tong University
Shanghai, China

ABSTRACT

Quick response (QR) codes have been widely used in mobile applications, due to its convenience and the pervasive built-in cameras on smartphones. Recently, however, QR codes have been reported suffering attacks for being sniffed just before the QR code is scanned, which lead to financial loss. In this study, we propose ScreenID, for enhancing the QR code security by identifying its authenticity, which embeds a QR code with information of unique screen fingerprint - PWM frequency. PWM frequencies are adjusted to different values by screen manufacturers, therefore can successfully differentiate screens. To improve the estimation accuracy of PWM frequency, ScreenID incorporates a model for the interaction between the camera and screen in the temporal and spatial domains. Extensive experiments demonstrate that ScreenID can differentiate screens of different models, types and manufacturers and thus improve the security of QR codes.

CCS CONCEPTS

• **Security and privacy → Software and application security**; • **Human-centered computing → Ubiquitous and mobile computing**.

KEYWORDS

Screen-camera communication; Secure QR code; PWM frequency

ACM Reference Format:
Yijie Li, Yi-Chao Chen, Xiaoyu Ji, Hao Pan, Lanqing Yang, Guangtao Xue, and Jiadi Yu. 2020. Poster: Toward a Secure QR Code System by Fingerprinting Screens. In *MobiCom 2020 (MobiCom '20), September 21–25, 2020, London, United Kingdom.* ACM, New York, NY, USA, 3 pages. https://doi.org/10.1145/3372224.3418165

MobiCom '20, September 21–25, 2020, London, United Kingdom

ACM ISBN 978-1-4503-7085-1/20/09…$15.00
https://doi.org/10.1145/3372224.3418165

1 INTRODUCTION

Quick response (QR) codes are barcodes comprising white and black blocks, which have been widely adopted in mobile applications such as communication, payment, etc, with the pervasive built-in cameras on smartphones. Especially, for mobile payment scenarios, QR code system is almost a standard module for service providers. Users just need to show their QR codes on smartphones for a quick transaction conveniently.

However, the transaction process using QR codes is far from secure. Recently, researchers have reported that a QRCode system is susceptible to the Synchronized Token Lifting and Spending (STLS) attack [1]. In this attack, the adversary first acquires an image of the QR code displayed on victim's device when the victim is showing the QR code to the cashier. Then the adversary can replay the stolen QR code for another transaction. Cryptographic techniques or inserting codewords cannot mitigate the concern because attackers do not need to decrypt the message embedded in the QR code.

Therefore, we propose ScreenID, which embeds a QR code with information bound to the screen that is displaying it, thereby the generated QR code can reveal whether its source, i.e., reproduced by an adversary or not. In ScreenID, we utilize the pulse width modulation (PWM) frequency of screens as the unique screen fingerprint. PWM frequency makes a good candidate for screen fingerprint as PWM frequencies are adjusted to different values by screen manufacturers and even for the same manufacture, they show variance due to variations in manufacturing process. On the receiver side, e.g., the camera in a cashier, the PWM frequency is measured by the stripes produced by rolling shutter effect on the cashier's camera. The QR code is legal and the transaction proceeds only if the PWM frequency embedded in the QR code and the one measured from the screen match.

We verified the uniqueness and stability of PWM frequency to ensure the feasibility of utilizing it as a feature to identify screens. We also verified the efficacy of a ScreenID prototype using screens (including both LCD and OLED) under a variety of camera settings and capturing position. The results show ScreenID can achieve high estimation accuracy of PWM frequency and it can successfully enhance security by preventing QR code from STLS attack.

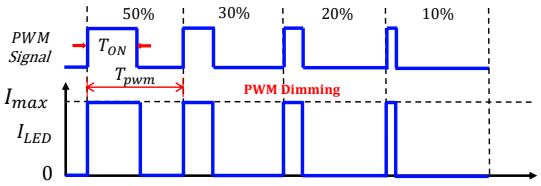


Figure 1: An illustration of PWM dimming.

2 BACKGROUND

2.1 Pulse Width Modulation (PWM) Dimming Control

Pulse Width modulation (PWM) dimming [2] is a common technique which adjusts screen brightness by digital encoding an analog signal to appear for a given period of time, wherein the power is either fully on or fully off. Essentially, the screen brightness is adjusted by regulating the on-time (T_{ON}) in each cycle (T_{pwm}) as shown in Fig. 1. Since human eyes are insensitive to changes of high frequency, we do not notice the flickering, but rather perceive a difference in brightness. Essentially, the screen appears brighter when the on:off ratio is larger.

2.2 Rolling Shutter Camera

Complementary metal-oxide semiconductor (CMOS) technology is widely used to fabricate the cameras used in smartphones. The sequential sampling by different rows is referred to as a rolling shutter. [3] The latency between the start of each exposure in each row is denoted by Δ_C. The time during which one frame is captured is denoted by T_f.

When using a rolling shutter sensor to capture an image from a screen with PWM-induced flicker, the light intensity indicates the total number of photons received throughout the duration of the exposure. Fig. 2 shows the black (darker) and white (lighter) stripes created by the sensor rows, while PWM signals periodically turn the screen on and off. ScreenID extracts PWM frequency by modeling the stripes produced by the flickering in terms of communication between screen and camera.

3 SYSTEM OVERVIEW

ScreenID is designed to enhance the security of QR code system by embedding PWM frequency in QR code as a screen fingerprint. Note that each pixel in an OLED screen is controlled by an LED light source and the PWM cycle of each row is asynchronous. The flickering of rows is delayed by latency Δ_S, which is kept constant among rows in order to prevent fluctuations in current. Specifically, $\Delta_S = 0$ for LCD screens because they only have a single light source.

The system architecture of ScreenID comprises two parts: encoding by the sender (smartphone screen) and decoding by the receiver (camera). In the encoding step, authenticity information should be embedded in advance in the QR code, namely (i) PWM frequency f_{pwm} and (ii) PWM latency between two rows Δ_S. In the decoding step, ScreenID determine the position of QR code and extract the PWM frequency for verification.

Encoding. Using ScreenID requires that f_{pwm} and Δ_S are both known in advance.f_{pwm} can be obtained when the user first uses the system and presents his/her phone to the cashier. The cashier then uses the Frequency Extraction scheme to compute f_{pwm}. PWM

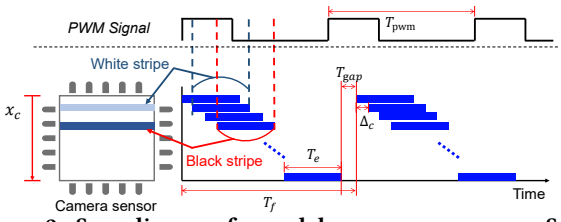


Figure 2: Sampling performed by camera sensors. Some of the rows sample during the PWM on-time, and others sample during the off-time, respectively producing black (darker) and white (lighter) stripes in the captured image.

latency Δ_S is determined from an image captured at an angle of 90° using a camera with a known configuration. $\Delta_S = \Delta_C M \tan\phi$ where ϕ is the angle of stripe to horizontal and M is the projection ratio. It means that M rows on the camera sensor capture one row from the screen.

Determining QR Code Position. On the receiver side, ScreenID first estimate the distance and angle by detecting the QR code based on three position symbols. The right-angle triangle formed by three position symbols can be used to estimate rotation angle α. The displayed QR code on screen is fixed so that it is possible to compute projection ratio M as a fraction of the length of a pixel along the both sides of the original QR code.

Multi-frame Concatenation. Each frame is first transformed into a gray-scale image to enhance contrast, then undergoes denoising and binarization, to obtain the boundaries of screen district. ScreenID selects the longest column as a data sample of the screen captured in the photo, and then concatenate columns from multiple frames to improve frequency resolution for differentiating screens.

Decoding (Frequency Extraction). In order to reduce the time required to capture frames, while estimating the PWM frequency with a high degree of precision, we down sample a sequence of samples of length N (e.g., $[x_1, x_2, x_3, \cdots, x_N]$) by a factor of K by taking a sample at K intervals, which results in K segments. (e.g., $[x_1, x_{K+1}, x_{2K+1}, \cdots]$, $[x_2, x_{K+2}, x_{2K+2}, \cdots]$, $\cdots$) from the original sequence. The sampling rate of each segment is becomes f_{sample}/K. We then concatenate all of the segments into a single sequence of length N. We apply the Hanning window to make the concatenation smoother before applying the Chirp-Z transform (CZT) to improve spectral resolution in the frequency range of interest (i.e., f_{pwm}). ScreenID finally extract the characteristic frequency through the above process.

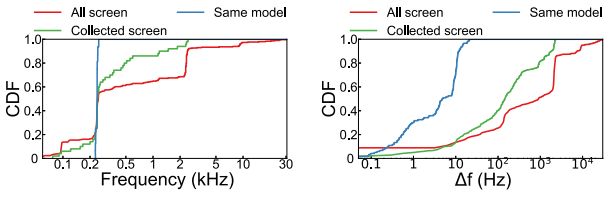
Verification. ScreenID compares the estimated PWM frequency with the one embedded in the QR code. When the difference between the two is less than a given threshold ($0.05Hz$ in the current study), the QR code is accepted. Otherwise, it is rejected.

4 PRELIMINARY EVALUATION

4.1 Experiment Setup

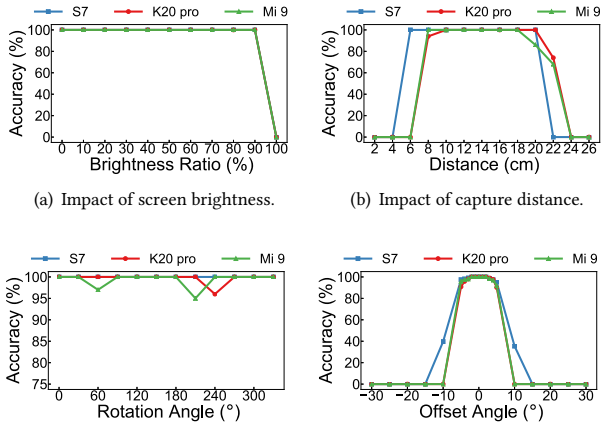
We used a light sensor ADPD2212 sampling at $80kHz$ to measure the PWM frequencies of 50 phone screens. Among the 50 phones, 16 are of the same model. If PWM dimming frequency is to be used as a feature by which to identity screens, then we must first verify its uniqueness and stability.

We also evaluate the robustness of ScreenID. We displayed 20 QR codes where 10 embedded the correct PWM frequency of the screen while the other 10 embedded that of another screen. We



(a) PWM frequencies. (b) Pairwise PWM frequency differences.

Figure 3: CDF of PWM frequencies and pairwise differences of 300 screens reported in NotebookCheck [4] and 50 screens (16 are of the same model) we collected.



(a) Impact of screen brightness. (b) Impact of capture distance.

(c) Impact of rotation angle. (d) Impact of offset angle.

Figure 4: Verification accuracy under various impact factors.

defined the verification accuracy as the ratio of the number of QR codes are correctly accepted/rejected to the total number. The higher accuracy is, the better ScreenID performs.

4.2 Uniqueness of PWM frequency.

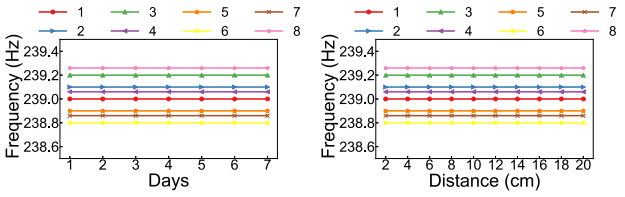
We conducted experiment to assess the uniqueness of PWM frequencies across screens Fig. 3(a) illustrates the distribution of PWM frequencies among smartphone screens. We can see that 97% of the PWM frequencies were below $10kHz$ and 68.3% were below $2kHz$. Fig. 3(b) shows the CDF of the pairwise differences in PWM frequency among screens. The frequency resolution is $0.01Hz$. We can see that among all screens and screens of the same model, 95% pairwise differences are larger than $1.1Hz$ and $0.18Hz$ The results revealed that a frequency resolution of $0.1Hz$ should be sufficient to differentiate among 99.3% screens.

4.3 Stability of PWM frequency.

We also assessed the uniformity of PWM frequencies under various conditions. Fig. 5(a) shows the PWM frequencies of 8 screens (Samsung S7) of the same model measured in various days and from various distances. The variation in PWM frequency was at most $0.04Hz$ which implies the PWM frequency is stable.

4.4 Robustness of ScreenID

ScreenID is robustly achieved above 90% verification accuracy across brightness ratio, rotation angle as shown in Fig. 4(a), Fig. 4(c). Note that when the brightness is 100%, the screen is always on so it does not flicker. ScreenID works well at the distance from $10-18cm$ (Fig. 4(b)), which is enough for the mobile payment. In order to enhance security against being sniffed, ScreenID only allows offset angle within 5° as shown in Fig. 4(d).



(a) Time. (b) Distance.

Figure 5: We measure the PWM frequencies of 8 screens of the same model across days and at various distances to show its stability.

5 APPLICATIONS AND DISCUSSION

5.1 Applications

In this poster, we present ScreenID to enhance the security of QR codes by fingerprinting the screens displaying the QR codes using PWM frequency. Apart from the employment on QR code system, ScreenID can be utilized as a compensation for watermarking schemes on account of its uniqueness bound to screen. Moreover, in our proposed system, the stripes caught on camera varies in terms of capturing distance and angle.Therefore, PWM frequency can serve as a complementary feature in various verification system to mitigate screen-photo-based leakage attacks.

5.2 Discussion

ScreenID takes around 4.8s in average to decode the QR code in proposed system for sufficient frequency resolution and additional process time. In future work, we will focus on reducing capturing time while increasing the frequency resolution. ScreenID will further consider universal feature (i.e. refresh rates) as supplementary to improve system versatility. Moreover,ScreenID cannot guarantee security due to possible frequency collisions of the same screen model (the accuracy of the same model can drop to 90%). For such security concern, we will consider crypto hash for the feature and combine multiple features. Furthermore, ScreenID does not need customized techniques so that it can meanwhile incorporate with existing authentication schemes.

ACKNOWLEDGMENTS

This work is supported in part by the NSFC under Grants 61936015 and Startup Fund for Youngman Research at SJTU and in part by National Key R&D Program of China (2018YFB2101102), the Joint Key Project of the NSFC (U1736207) and Program of Shanghai Academic Research Leader.

REFERENCES

[1] Xiaolong Bai, Zhe Zhou, XiaoFeng Wang, Zhou Li, Xianghang Mi, Nan Zhang, Tongxin Li, Shi-Min Hu, and Kehuan Zhang. 2017. Picking up my tab: Understanding and mitigating synchronized token lifting and spending in mobile payment. In *26th {USENIX} Security Symposium ({USENIX} Security 17)*. 593–608.

[2] Michael Barr. 2001. Pulse width modulation. *Embedded Systems Programming* 14, 10 (2001), 103–104.

[3] Chia-Kai Liang, Li-Wen Chang, and Homer H Chen. 2008. Analysis and compensation of rolling shutter effect. *IEEE Transactions on Image Processing* 17, 8 (2008), 1323–1330.

[4] NotebookCheck. 2019. PWM Ranking - The Best Displays for the Eyes. https://www.notebookcheck.net/PWM-Ranking-Notebooks-Smartphones-and-Tablets-with-PWM.163979.0.html