北京理工大学

本科生毕业设计（论文）外文翻译

外文原文题目： CardioCam: Leveraging Camera on Mobile Devices to Verify Users While Their Heart is Pumping

中文翻译题目： CardioCam：利用移动设备上的摄像头在用户心跳时对其进行验证

北京理工大学本科生毕业设计（论文）题目

The Subject of Undergraduate Graduation Project (Thesis) of Beijing Institute of Technology

学　　院：计算机学院

专　　业：计算机科学与技术

班　　级：07111906

学生姓名：钮海洋

学　　号：1120192605

指导教师：李凡

CardioCam: Leveraging Camera on Mobile Devices to Verify Users While Their Heart is Pumping

Jian Liu*
WINLAB, Rutgers University
New Brunswick, NJ, US
jianliu@winlab.rutgers.edu

Cong Shi*
WINLAB, Rutgers University
New Brunswick, NJ, US
cs1421@scarletmail.rutgers.edu

Yingying Chen
WINLAB, Rutgers University
New Brunswick, NJ, US
yingche@scarletmail.rutgers.edu

Hongbo Liu
Indiana University-Purdue University
Indianapolis
Indianapolis, IN, US
hl45@iupui.edu

Marco Gruteser
WINLAB, Rutgers University
New Brunswick, NJ, US
gruteser@winlab.rutgers.edu

ABSTRACT

With the increasing prevalence of mobile and IoT devices (e.g., smartphones, tablets, smart-home appliances), massive private and sensitive information are stored on these devices. To prevent unauthorized access on these devices, existing user verification solutions either rely on the complexity of user-defined secrets (e.g., password) or resort to specialized biometric sensors (e.g., fingerprint reader), but the users may still suffer from various attacks, such as password theft, shoulder surfing, smudge, and forged biometrics attacks. In this paper, we propose, CardioCam, a low-cost, general, hard-to-forge user verification system leveraging the unique cardiac biometrics extracted from the readily available built-in cameras in mobile and IoT devices. We demonstrate that the unique cardiac features can be extracted from the cardiac motion patterns in fingertips, by pressing on the built-in camera. To mitigate the impacts of various ambient lighting conditions and human movements under practical scenarios, CardioCam develops a gradient-based technique to optimize the camera configuration, and dynamically selects the most sensitive pixels in a camera frame to extract reliable cardiac motion patterns. Furthermore, the morphological characteristic analysis is deployed to derive user-specific cardiac features, and a feature transformation scheme grounded on Principle Component Analysis (PCA) is developed to enhance the robustness of cardiac biometrics for effective user verification. With the prototyped system, extensive experiments involving 25 subjects are conducted to demonstrate that CardioCam can achieve effective and reliable user verification with over 99% average true positive rate (TPR) while maintaining the false positive rate (FPR) as low as 4%.

CCS CONCEPTS

• **Security and privacy** → **Authentication**; **Biometrics**.

KEYWORDS

camera, authentication, mobile devices, cardiac biometric

ACM Reference Format:
Jian Liu, Cong Shi, Yingying Chen, Hongbo Liu, and Marco Gruteser. 2019. CardioCam: Leveraging Camera on Mobile Devices to Verify Users While Their Heart is Pumping. In *The 17th Annual International Conference on Mobile Systems, Applications, and Services (MobiSys '19), June 17–21, 2019, Seoul, Republic of Korea.* ACM, New York, NY, USA, 13 pages. https://doi.org/10.1145/3307334.3326093

1 INTRODUCTION

The increasingly prevalent usage of mobile and IoT devices (e.g., smartphones, tablets and smart-home appliances) inevitably contains private and sensitive information (e.g., contact list, emails, credit card numbers and merchandise ordering information). Unauthorized access to such devices could put huge amounts of sensitive information at the risks of misuse. Traditional user verification solutions mainly rely on passwords or graphical patterns [29, 52], which suffer from various attacks including password theft, shoulder surfing [53] and smudge attacks [9]. Biometric-based user verification opens up a new pathway to secure mobile devices, especially fingerprint-based solutions [7, 31], which are widely deployed in many premium smartphones (e.g., iPhones and Samsung phones) and offer a more secured way to access mobile and smart devices. However, there is still a large market for phones with 50 dollars and less (e.g., BLU A4) in many developing regions around the world where phones do not come with dedicated fingerprint sensors [46]. Furthermore, some of these low-cost markets heavily rely on mobile payments due to the large distribution of geographic areas and the lacking establishment of traditional banking and payments infrastructure [36]. Moreover, fingerprint-based solutions are vulnerable to synthetic fingerprints created through victims' photographs [14, 41, 48]. These lead to a renewed search of a low-cost, general, hard-to-forge security solution, which could also facilitate the usage of increasingly convenient mobile payment systems. Existing studies have demonstrated that using either body-attached PPG/ECG sensors [8, 12, 25, 42] or Doppler radar [30] is

[*] Both authors contributed equally to this research.

MobiSys '19, June 17–21, 2019, Seoul, Republic of Korea
© 2019 Association for Computing Machinery.
ACM ISBN 978-1-4503-6661-8/19/06...$15.00
https://doi.org/10.1145/3307334.3326093

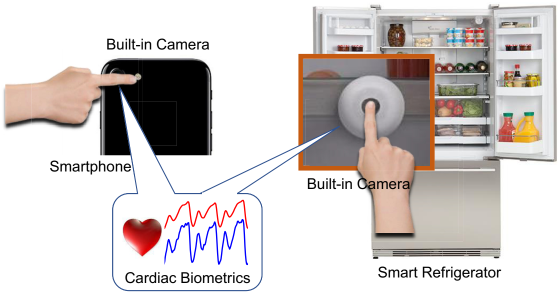


Figure 1: Enabling cardiac-pattern based user verification using device's built-in camera.

promising to perform user verification by capturing human cardiac biometrics. These existing investigations usually require specialized equipments (e.g., sensors or radar devices), which could add extra cost and bring inconvenience the mobile users. Towards this direction, we propose *CardioCam* that does not involve specialized equipments to extract unique cardiac biometrics to perform user verification. CardioCam makes use of the built-in camera which is readily available in almost all kinds of mobile devices including both premium and low-end devices (e.g., phones under 50 dollars).

Some researchers have shown that the built-in camera on smartphone could be utilized to measure heart rate and pulse volume [32, 51]. Existing work [28] also demonstrated the correctness and suitability of the cardiac signals captured by the smartphone's camera, which are very close to those measured by the specialized medical instrument (i.e., pulse oximetry) [28]. However, whether the camera is able to extract unique cardiac biometrics for user verification remains an open issue. CardioCam takes one step further to explore the limits of the built-in camera and aims to achieve user verification leveraging the unique cardiac biometrics extracted from the camera. The system simply requires the user to press his/her fingertip on the camera surface for cardiac feature extraction as shown in Figure 1. Therefore, it could be directly applied to almost all the mobile devices to perform user verification including unlocking the devices and authorizing specific permissions. Furthermore, there is a growing trend of deploying low-cost cameras on smart appliances to support a broad range of emerging IoT applications. For instance, FridgeCam [43] allows users to stick a small camera to the inside of the refrigerator for storage food monitoring. Amazon's virtual assistant Echo Look [3] is also equipped with a camera to support its growing commands sets (e.g., asking for the opinion on which outfit looks best). In addition, small IoT devices, such as video doorbell [40], equipped with low-cost cameras are serving for many home security systems these days, and Amazon Dash Button [4] can be easily integrated with a low-cost camera to enable user verification for privacy protection. Therefore, the large-scale deployment of the cameras on IoT devices provides great opportunities for CardioCam to verify users for various applications, such as entrance's access control, ordering food via the refrigerator with parental control and purchasing clothes via the virtual assistant without disclosing personal lifestyle.

Traditional Solutions. The built-in cameras on mobile devices have been used to perform user verification with biometric features including iris patterns [27], facial features [15] and palm print [47]. These solutions mainly rely on computer-vision based methods and usually suffer from spoofing attacks with forged biometrics. For instance, the iris-based user verification system can be deceived by the synthesized iris images with identical iris texture as the legitimate user [49]. Face ID on iPhone X can capture the geometry and depth of the user's face [19] to verify user's identity. Although it has been proved to be more secure than fingerprint-based authentication (e.g., Touch ID) [6], this technique requires high-end and expensive camera (i.e., TrueDepth front-facing camera). Additionally, these vision-based solutions may result in privacy concerns induced by the rich information embedded in the visual content captured by camera, and their performance could be degraded by the surrounding lighting conditions.

Cardiac-pattern based User Verification Using Built-in Camera. In this paper, we explore to extract cardiac biometrics from the built-in camera. It has been demonstrated the cardiac feature is intrinsic, unique and non-volitional among a large population [1, 26, 34, 55]. Instead of using PPG/ECG sensors, in this work we search for the unique cardiac features extracted from the cardiac motion patterns in fingertips, by pressing on the built-in camera. We hope the extracted cardiac features from fingertips are distinguishable among different individuals and could serve as a candidate for effective user verification. The cardiac features are usually affected under practical scenarios: the extracted cardiac motion patterns are impacted by the lighting conditions; Heartbeats are varied under movements and human emotion changes; the fingertip pressing position and pressure also play a critical role in cardiac biometric feature extraction. To address the above challenges, CardioCam adaptively updates camera configuration and dynamically derives cardiac motion patterns to suppress the effects caused by ambient light changes. We also develop a mechanism that could handle different fingertip pressing positions and pressure by choosing the most sensitive pixels to derive cardiac motion patterns from the video frames captured by the built-in camera.

To facilitate biometric extraction, CardioCam segments the cardiac measurements into different heartbeat cycles and normalizes the duration/amplitude of each cardiac cycle to mitigate the impact of heartbeat rate/strength variations. The normalization process will enhance the robustness of the derived cardiac biometrics while preserving morphological distinctiveness embedded in the cardiac motion pattern. We further extract user-specific heartbeat features within each cardiac cycle via morphological characteristic analysis. To effectively suppress the small-scale cardiac motion variations, a feature transformation scheme based on Principal Component Analysis (PCA) [23] is developed. These feature abstractions are used to construct legitimate user profiles during the system enrollment. During verification phase, CardioCam examines the Euclidean distance of the feature abstractions between new observations and the user profiles to authenticate the legitimate user or reject adversaries. The main contributions of our work are summarized as follows:

- To the best of our knowledge, CardioCam is the first low-cost, general user verification system that uses cardiac biometrics extracted from the built-in cameras on mobile devices or IoT appliances.

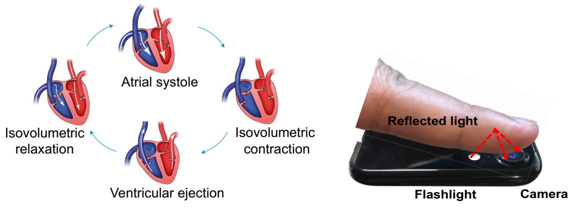
- We demonstrate that the intrinsic, unique and non-volitional cardiac properties can be preserved when extracting the cardiac features from fingertips; the cardiac biometrics are well captured by the reflected lights on the built-in camera when the user presses her/his fingertip upon.
- We develop a gradient-based optimization technique that adapts the configuration of camera to ambient light changes and human movements variations and derives high-quality cardiac measurements from a set of dynamically selected image pixels. Given the selected pixels that are sensitive to cardiac motion, the impacts of fingertip position and pressure upon the camera can be suppressed.
- With the proposed cardiac biometric feature extraction and the feature transformation scheme based on PCA, we demonstrate that CardioCam can robustly verify users and is resilient to the modeled attacks, in which an adversary presses his/her own fingertip upon the camera hoping to pass the system.
- We perform extensive experiments involving 25 subjects under various data collection strategies and system settings. The results demonstrate that CardioCam can achieve over 99% average true positive rate (TPR) to verify users while maintaining less than 4% false positive rate (FPR) to well reject adversaries.

2 RELATED WORK

Traditional user verification mechanisms rely on either password [29] or graphic screen patterns [52], which require users to memorize complicated text/graph secrets, to verify their identities. Since these solutions only verify the secret itself instead of a user, they are usually vulnerable to various attacks such as shoulder surfing [53], and smudge attack [9].

As an alternative, many researchers resort to physiological biometrics to perform user verification. In particular, fingerprint-based solutions [7, 21, 22, 31] have become an essential specification on many premium smartphones such as iPhone and Samsung Galaxy S series. However, the fingerprint reader is still unavailable in most of the mid-range and low-end mobile devices, the fingerprint based systems are also vulnerable to spoofing attacks by using synthetic artifacts [14, 48]. Besides the fingerprints, other human biometric features (e.g., iris [27], face [15], and palmprint [47]) are also exploited to achieve user verification with the assistance of cameras, especially the built-in camera on mobile devices, which has already been used for device authentication [10]. However, the privacy concerns of such vision-based solutions prevent them from extensive use due to the rich information embedded in the image/video captured by cameras. For instance, the surrounding background scene may disclose the user's location, living environment or any personal stuff. Additionally, the biometrics (e.g., iris, face, palmprint) captured in the aforementioned vision-based solutions are all *external* features of human beings, which can be forged by an adversary for launching spoofing attacks [17, 18, 49].

To overcome the aforementioned weaknesses, some studies rely on intrinsic cardiac biometrics (e.g., heartbeat patterns) derived from electrocardiogram (ECG) [11, 20, 45, 55] and photoplethysmography (PPG) [25] signals. However, these methods require the users to attach specialized sensors to their chest or fingertip, making them hard to be applied to mobile users. Cardiac Scan [30] recently proposes a non-obtrusive way to extract distinct cardiac motion pattern with Doppler radar for user authentication, but the involvement of specialized devices also adds extra cost and brings inconvenience to the mobile users.



(a) Human cardiac cycle [37]

(b) Data collection

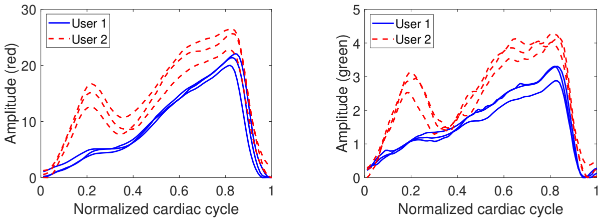
Figure 2: Four phases of cardiac cycle and data collection leveraging camera and flashlight.

In order to remove the limitation on involving specialized equipments, some studies explore to capture the cardiac biometrics leveraging the readily available sensors on commercial off-the-shelf devices. Specifically, Matsumura *et.al.* [32] demonstrate that the heart rate and pulse volume can be measured when the users put their fingertips upon the built-in camera. Additionally, Seismo [51] proposes to derive pulse transit time (PTT) leveraging smartphone accelerometer and built-in camera. Some researchers [13, 50] further make use of both built-in camera to estimate blood oxygen level PhO_2 and Hemoglobin level. Towards this direction, this paper takes one step further to explore the feasibility of using built-in camera to extract non-volitional and hard-to-forge cardiac biometrics to perform user verification. Comparing to existing biometric authentication (e.g., fingerprint, face recognition), CardioCam has better scalability since it only requires the built-in camera and flashlight that are available in almost all kinds of mobile devices. In addition, our system is a light-weight user verification system with extremely low computational complexity and memory/energy overhead.

3 PRELIMINARIES

3.1 Kinetics of Cardiovascular System

The heart pumps the blood into the vessels through alternative cardiac muscle contraction and relaxation, which forms a periodic heartbeat pattern, called cardiac cycle, while the vessels carry blood circulated throughout the whole body, including the fingertips. The human heart contains four chambers (i.e., upper left and right atria; and lower left and right ventricles), and a typical cardiac cycle usually involves four major phases: atrial systole, isovolumetric contraction, ventricular ejection and isovolumetric relaxation, as shown in Figure 2 (a). In the phase of atrial systole, the ventricles are contracting, while the atria are relaxing and collecting blood. Then isvolumetric contraction occurs, and the ventricles contract with no corresponding blood volume change in all chambers. When the ventricles start ejecting blood (i.e., ventricular ejection), the atria contracts to pump blood to the ventricles. Finally, a short interval, called isovolumetric relaxation, begins and the atria valve starts



(a) Red channel

(b) Green channel

Figure 3: Cardiac cycles of two users extracted from the camera's red and green channels.

closing until the onset of another cardiac cycle. Due to the existence of physiological differences on cardiovascular systems (e.g., heart size, shape and tissues, etc.), different people have different amplitudes of cardiac muscle contraction and relaxation. Consequently, the blood flow in the vessels follows a unique variation trend within a cardiac cycle for different individuals. Both ECG and PPG signals have the capability to reveal unique cardiac biometrics embedded in the four phases of a cardiac cycle [5], and existing work [34] has demonstrated the uniqueness such cardiac biometrics among a large population. Similar to PPG based approaches, CardioCam measures cardiac motion patterns in terms of blood flow variations by illuminating the fingertip with an external light source (i.e., flashlight), making it possible to capture equivalent unique biometrics. In addition, the blood flow passing through the veins in fingertip will result in unique cardiac motion pattern. Such pattern could reveal the distensibility of fingertip vascular [16] and reflect distinctive vein characteristics (e.g., vein distribution), which has been demonstrated among a large population [38, 55].

Therefore, we are inspired to extract effective biometric features from the cardiac motion pattern to perform user verification.

3.2 Capturing Cardiac Motion

Given the intrinsic, unique and non-volitional properties of cardiac motion pattern, the next step is how to effectively extract the biometric features. Unlike existing works that rely on specialized instruments to capture the cardiac motion, we seek to examine the blood flow, which reflects the unique cardiac motion, through the fingertips with commercial off-the-shelf devices. As shown in Figure 2 (b), by illuminating the fingertip skin with the flashlight on smartphone, the built-in camera can continuously observe the variations on light absorption introduced by blood flow changes, where the unique cardiac features are embedded.

Specifically, each pixel of the built-in camera acts as an independent light sensor to detect the light changes on fingertip. Due to the high resolution of current smartphone cameras (e.g., 1280 × 720 pixels per frame), fine-grained cardiac cycle monitoring can be achieved. Besides, the three color channels (i.e., Red, Blue and Green) of each pixel provide multiple dimensions for effective feature extraction. By contrast, traditional cardiac monitors, such as photoplethysogram (PPG) sensors, can only support up to 3 different photodiodes (i.e., red, green, infrared photodiodes), which is equivalent to three pixels, for cardiac dynamic detection [2].

Figure 3 shows light intensity changes of two different color channels (i.e., red and green) across three cardiac cycles of two different users. We normalized the time scale of each cardiac cycle to remove the impacts of fluctuating heartbeat rate. It is obvious to find that the two users exhibit different cardiac motion patterns for both color channels, which confirm that unique cardiac features can be captured by smartphone camera. Additionally, since human skin has different absorption/reflection rate for the light of different colors, the cardiac motion patterns revealed by red and green channels have slight differences, which instead provide some redundancy for reliable cardiac feature extraction.

4 SYSTEM OVERVIEW

4.1 Challenges

In order to achieve effective user verification leveraging unique cardiac biometrics with ubiquitous built-in camera on mobile and smart devices, a number of challenges need to be addressed.

Reliable Cardiac Measurements. The success of user verification is built upon reliable measurements on cardiac motion pattern. However, various impacting factors, such as ambient lighting condition, fingertip pressing position and human motion can impact the reliability of the derived cardiac measurements under practical scenarios. Thus, it is critical to mitigate these impacts in cardiac measurements for the proposed system.

Uniqueness of Cardiac Characteristics. Since the cardiac motion pattern is indirectly obtained by capturing the blood flow variation in fingertips with built-in camera, it is a challenging task to convert the recorded video frames to reliable cardiac biometrics associated with unique cardiac motion pattern. Furthermore, to facilitate effective user verification, it is important to extract and validate representative biometric features from the raw cardiac measurements.

System Robustness. The cardiac measurements are also affected by many random factors, such as the emotion changes, heart and breath rate variations. The system should be capable to eliminate such randomness and derive robust biometric abstractions. It is necessary to develop a transformation algorithm that can suppress the small-scale cardiac motion variations.

4.2 Attack Model

We consider the attacking scenario where an adversary attempts to access the sensitive information or functionality (e.g., schedule, photos and mobile payment) on the private mobile device that is left unattended by legitimate users. The adversary does not have any prior knowledge of the cardiac biometrics of the legitimate users. To spoof the device, the adversary tries to pass the user verification process with the adversary's own cardiac biometrics by pressing his or her fingertip upon the built-in camera. Furthermore, the adversary can also shift the position of his fingertip with respect to the camera or adjust finger pressure, aiming to yield similar cardiac biometrics as the legitimate user.

4.3 System Overview

The basic idea of CardioCam is to verify the user's identity leveraging the intrinsic, unique, and non-volitional cardiac biometrics with the assistance of ubiquitous built-in camera/flashlight on mobile

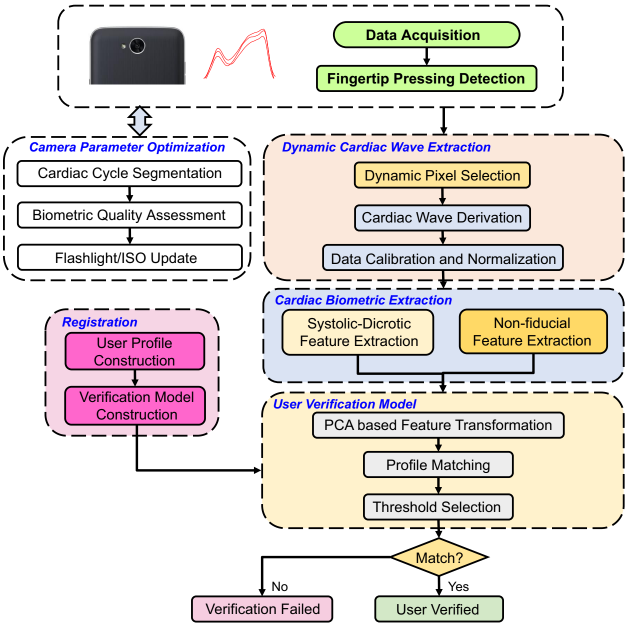

Data Acquisition
Fingertip Pressing Detection
Camera Parameter Optimization
Cardiac Cycle Segmentation
Biometric Quality Assessment
Flashlight/ISO Update
Dynamic Cardiac Wave Extraction
Dynamic Pixel Selection
Cardiac Wave Derivation
Data Calibration and Normalization
Registration
User Profile Construction
Verification Model Construction
Cardiac Biometric Extraction
Systolic-Dicrotic Feature Extraction
Non-fiducial Feature Extraction
User Verification Model
PCA based Feature Transformation
Profile Matching
Threshold Selection
Match?
No
Yes
Verification Failed
User Verified

Figure 4: System Overview of CardioCam.

devices. CardioCam can be triggered when a user is trying to access sensitive information/functionalities (e.g., mobile payment, photo) or unlock her or his mobile device by either swiping up on the device's touchscreen or pressing the on-off button. Considering time for video recording and profile matching, CardioCam takes about 2.5 seconds to complete one-time user verification. As illustrated in Figure 4, *Data Acquisition* is then initialized with both the build-in camera and flashlight turned on when detecting the camera is covered by a fingertip. Under the illumination of flashlight, the blood flow in fingertip, which is associated with cardiac motion pattern, will be captured by the built-in camera in the form of video frames. Before cardiac motion derivation, we first develop a gradient-based optimization technique to adapt the camera configurations (i.e., flashlight intensity, ISO) to complement ambient light changes. Next, the reliable cardiac motion pattern is derived via the module *Dynamic Cardiac Wave Extraction* from the captured video frames. Since the pressing position and pressure of fingertip may keep slightly changing during the verification process, we propose *Dynamic Pixel Selection* to merely include a subset of pixels that are most sensitive to cardiac motion to boost the signal-to-noise ratio of the cardiac measurements. In particular, the sensitive pixels are determined within each individual cardiac cycle, which is segmented by searching for subsequent local minima in cardiac measurements. Then the video stream of the selected pixels will be converted to three cardiac waves with respect to red, green and blue channels, following with a bandpass filter and a normalization process to mitigate the impacts caused by human respiration and heart rate changes, respectively.

In the *Cardiac Biometric Extraction* module, CardioCam extracts 30 systolic-diastolic features directly from the cardiac measurements and 36 non-fiducial features after further processing. The systolic and diastolic features are represented as normalized distances/slopes between four fiducial points (i.e., Diastolic Point (DP), Systolic Point (SP), Dicrotic Notch (DN), Dicrotic Wave (DW) [2]) within each cardiac cycle. The four fiducial points are used to characterize the four phases of cardiac contraction and relaxation. The fiducial point positions can be localized through recursively finding the local maxima and minima within a cardiac cycle. To further extend feature space, CardioCam also passes the cardiac measurements through two high-pass filters to reveal cardiac uniqueness via overall signal morphology and extract more fine-grained non-fiducial features. The non-fiducial features, which are denoted as the normalized distance between local maximums and minimums of the processed measurements, are also unique among different users.

Finally, *User Verification Model* facilitates user verification by matching new cardiac observations to the predefined a user profile. Instead of directly building user profile with the aforementioned morphological features, the system performs profile construction by converting these features into a set of robust feature abstracts through principal component analysis (PCA). PCA transformation preserves the key characteristics that are effective to discriminate different users while eliminates the impact of unpredictable interferences. The verification succeeds if the featured abstracts are within a certain Euclidean distance from the user profile. Otherwise, it fails and denies the access request.

5 FINGERTIP TOUCH DETECTION & CAMERA PARAMETER OPTIMIZATION

In this section, we first introduce how to detect fingertip touch on the built-in camera, and we then discuss the camera/flashlight configuration optimization to mitigate the impacts of ambient light for reliable cardiac motion derivation.

5.1 Fingertip Touch Detection

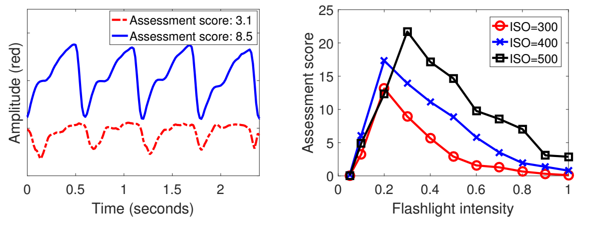
Under the illumination of the built-in flashlight, the captured video frames have the color dominated by red channel (i.e., the color of blood) if the camera is fully covered by a fingertip. When the camera is fully covered, the red pixels would show extreme high intensity, otherwise give relatively low intensity. We thus examine the proportion of red channel component in the overall light intensity across all the pixels in each frame $t \in T$ as follows:

$$Pr(x,y) = \frac{r_{(x,y)}(t)}{r_{(x,y)}(t) + g_{(x,y)}(t) + b_{(x,y)}(t)}, \qquad (x \in X, y \in Y, t \in T), \tag{1}$$

where $r_{(x,y)}$, $g_{(x,y)}$, $b_{(x,y)}$ denote the light intensity in red, green, and blue channel at pixel (x,y), respectively. X and Y represent the frame width and height, and T is the total number of frames in the captured video. By comparing Pr with a predefined threshold (i.e., $\tau = 0.85$), we can determine the pixels that are covered, and the cardiac motion derivation starts up only when over 95% of the pixels are dominated by red channel.

5.2 Camera Parameter Optimization

Our preliminary study finds that the reliable cardiac motion patterns can only be obtained under appropriate camera configurations



(a) Cardiac waves with different assessment scores

(b) Assessment scores under different light intensity/ISO

Figure 5: Illustration of the assessment score S of cardiac waves under various conditions.

with adequate amount of light entering the camera. Extremely low or high flashlight illumination would degrade the pixel sensitivity on capturing the cardiac motion patterns from the camera. Due to the various ambient lighting conditions, CardioCamera needs to adapt the camera configurations to complement the light introduced by ambient sources (e.g., sun, artificial light). We thus design a gradient-based optimization scheme on camera/flashlight configuration to mitigate the impacts of ambient light.

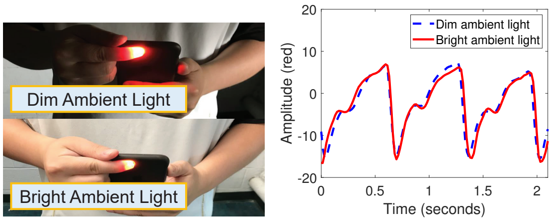
Cardiac Cycle Segmentation. Periodic cardiac motion results in regular changes of blood flow in the fingertip, which are represented as pixel value variations on camera videos. To capture the cardiac cycles embedded in such pixel value variations, CardioCam first calculates the time-series cardiac measurements by averaging pixel values of red channel for each frame in a video stream. We choose the red channel because the captured video frames have the color dominated by the color of blood, and the red pixels have the best sensitivity on the blood flow variations. Then, CardioCam exploits peak-valley detection algorithm [44] to identify the valleys with a minimum prominence of 40, and the segment between two detected consecutive valleys is considered as a cardiac cycle. The threshold is determined through our empirical study based on the cardiac signal samples collected from 25 subjects. Due to heart rate differences between individuals, the number of frames in each cardiac cycle ranges from 36 to 65. Note that the above segmentation algorithm will also be used for both *Dynamic Cardiac Wave Extraction* (Section 6) and *Biometric Extraction* (Section 7).

Biometric Sensitivity Assessment. We study the pixel sensitivity by evaluating the light intensity changes (i.e., absolute pixel value changes in frames) during each cardiac cycle. Specifically, we calculate the element-wise (pixel-by-pixel) difference, $Diff(r_{(x,y)})$, between the two frames with maximum and minimum pixel averages in red channel as:

$$Diff(r_{(x,y)}) = r_{(x,y)}(t_{max}) - r_{(x,y)}(t_{min}), \quad (x \in X, y \in Y), \tag{2}$$

where t_{max} and t_{min} denote the indexes of frames that have maximum and minimum averages of pixel values, respectively. Then, we indicate the distribution of $Diff(r)$ with a histogram H with k bins and derive the assessment score as below:

$$S = \sum_{i=1}^{k} i^2 \times \frac{|H_i|}{X \times Y}, \tag{3}$$



(a) Experimental setup

(b) Cardiac waves

Figure 6: Comparison of the cardiac waves derived under dim and bright ambient light conditions, respectively.

where $|H_i|$ denotes the number of the pixels falling into ith bin. Figure 5(a) shows the average light intensity in the red channel of two video streams including the four cardiac cycles. It is obvious to observe that higher assessment score (i.e., S=8.5) indicates a better biometric sensitivity, and thus confirms the effectiveness of the proposed assessment scheme on assessing pixel sensitivity.

Gradient-based Configuration Update. As illustrated in Figure 5 (b), either high or low camera ISO/flashlight illumination cannot achieve satisfied frame quality on detecting cardiac motion pattern. Particularly, the maximum assessment score can be found at flashlight intensity of 0.2, 0.2, 0.3 when ISO is 300, 400, and 500, respectively. This observation motivates us to search for an optimal camera and flashlight configuration (i.e., ISO and flashlight intensity) that maximizes the pixel sensitivity (i.e., assessment score S). Specifically, we develop an iterative searching method, where the next configuration adjustment is based on the feedback from current one. The flashlight/ISO offset of each iteration is calculated as follows:

$$a_{n+1} = a_n + \gamma \bigtriangledown S(a_n), \tag{4}$$

where a_n denotes either flashlight intensity or camera ISO configuration at n-th cardiac cycle and the corresponding assessment score is represented as $S(a_n)$. At each cardiac cycle, a_n is updated following the gradient ascent direction $\nabla S(a_n)$ with fixed step values (i.e., $\gamma_{FL} = 0.05$ and $\gamma_{ISO} = 5$) until the satisfactory pixel sensitivity is reached (i.e., beyond an empirical threshold). The optimization procedures are summarized in Algorithm 1.

Figure 6 shows an example of the derived cardiac waves from a user when the surrounding environments are in two different ambient lighting conditions (i.e., dim and bright ambient light), respectively. As CardioCamera adaptively adjusts the camera flashlight and ISO configuration to complement the light variations, we observe that the cardiac waves collected under the two different lighting environments exhibit similar morphological characteristics. The results indicate that the proposed camera parameter optimization is a promising and reliable approach to ensuring the high-quality cardiac motion pattern derivation.

6 DYNAMIC CARDIAC WAVE EXTRACTION

To extract unique and reliable cardiac biometrics, it is essential to derive cardiac waves that are robust to ambient noises and the ever-changing position/pressure of fingertip during the verification process. In this section, we introduce how to derive reliable cardiac

Algorithm 1 Video Biometric Optimization

```
function CameraAdjustment
    $ISO = 550, S_{prev} = 0, FL_{prev} = 0$
    while $S < Threshold$ do
        $S_{prev} = S$
        $FL = Camera.flashlight$
        $S = Score(Frame_{peak}, Frame_{valley})$
        $Feedback = (S - S_{prev})$
        if $FL - FL_{prev} > \tau$ then
            $FL_{prev} = FL$
            $Offset_{fl} = Feedback * \gamma_{FL}$
            $FL = FL + Offset_{fl}$
            $Camera.flashlight = FL$
        else
            $Offset_{iso} = Feedback * \gamma_{iso}$
            $ISO = ISO + Offset_{iso}$
            $Camera.ISO = ISO$
        end if
    end while
end function
```

via selecting the most sensitive pixels to cardiac motion in the video frames captured by built-in camera.

6.1 Dynamic Pixel Selection

Our preliminary studies find that the light intensity sensed by different pixels on camera are subject to the differences of fingertip thickness, pressing position and pressure. Therefore, a pixel selection strategy is required to dynamically exclude the ineffective camera pixels for cardiac wave extraction.

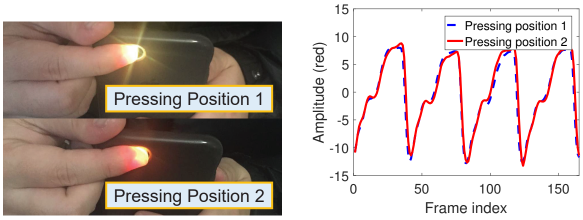
Specifically, we first calculate the average of the frames in a cardiac cycle and then identify two frames that have the maximum and minimum average pixel values, respectively. Element-wise difference between these two frames is then calculated by using Equation 2. We select the effective pixels that have sufficient max-to-min difference and obtain a mask matrix, $M^k(x, y)$, by using the following equation:

$$M^k(x, y) = \begin{cases} 1, & Diff^k(r_{(x,y)}) > \gamma \\ 0, & Diff^k(r_{(x,y)} \leq \gamma, \end{cases} \tag{5}$$

where $Diff^k(r_{(x,y)})$ is the element-wise difference of pixel (x, y) in the k^{th} cardiac cycle. Based on our experiments with different subjects, we empirically determine $\gamma = 15$ to ensure fiducial features (i.e., systolic and dicrotic points) can be correctly derived. The mask matrix has the same size as the video frames and is applied to all the frames in one cardiac cycle.

6.2 Cardiac Wave Derivation

Although blood flow variation can be captured by all sensitive pixels, deriving cardiac measurements from all individual pixels will incur significant computational overhead. Additionally, cardiac motion patterns derived from different camera pixels may exhibit extremely high similarity across different color channels (i.e., red, green, blue). Thus we use the pixel average over the three color channels (i.e., red, green, blue) to derive three cardiac waves. In particular, the cardiac waves are derived based on the selected pixels, which are adaptively updated for each cardiac cycle. To simplify the cardiac wave derivation, the derived cardiac wave segment of the k^{th} cardiac cycle can be obtained as:



(a) Pressing positions

(b) Cardiac waves

Figure 7: Two different fingertip pressing positions and the corresponding cardiac motion patterns.

$$W_c^k(t) = \frac{\sum_{x,y} M^k(x, y) \times c^k_{(x,y)}(t)}{\sum_{x,y} M^k(x, y)}, \tag{6}$$

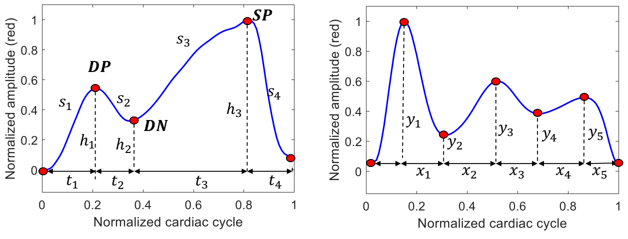
where $W_c^k(t)$ and $c^k_{(x,y)}(t)$ denote the derived cardiac wave and light intensity respectively at tth frame in the channel c (i.e., r, g, b). As shown in Equation 6, only the sensitive pixel values are involved in cardiac wave generation through multiplying the pixel matrix by the mask. Figure 7 (a) gives an example that two different fingertip-touch positions from the same person, respectively. And Figure 7 (b) shows the corresponding cardiac waves derived from the selected pixels. We can observe that the two cardiac waves are surprisingly similar to each other even the fingertip touch positions are different. The results validate that our dynamic cardiac wave derivation algorithm is robust to the impact of the fingertip position changes.

6.3 Data Calibration and Normalization

According to our empirical study, the cardiac wave derivation is also affected by the user's respiration and inherent defects of camera. Previous study [35] found that the impacts of respiration on cardiac measurement normally appear at the frequency band less than $0.3Hz$. To further mitigate the above interferences, a bandpass Butterworth filter [39] with the passing frequency band $0.3Hz \sim 10Hz$ is adopted to further calibrate the cardiac wave. Additionally, there are several intrinsic factors related to human emotion (e.g., exercising or resting) that may also affect human heartbeat rate and strength, so the cardiac wave duration and amplitude will be either stretched or shrunk. To ensure the robustness of the cardiac biometrics, we normalize both the duration and amplitude of one cardiac cycle into a common scale [0, 1] to mitigate the impact of heartbeat rate/strength fluctuation.

7 BIOMETRIC EXTRACTION

We propose to exploit both systolic-diastolic and non-fiducial features to capture the unique physiological characteristics inherited from the user's cardiovascular system. Specifically, systolic-diastolic features are the amplitude of the inflection points in the cardiac cycles. Such amplitudes represent round-trip delay time of blood flow and are proportional to unique physiological characteristics (e.g., height, arterial stiffness [33]). While non-fiducial features characterize the overall signal morphology of the cardiac cycle.



(a) Systolic-diastolic features

(b) Non-fiducial features

Figure 8: Systolic-diastolic features extracted from a cardiac wave and non-fiducial features derived from the decomposed wave passing a $2Hz$ high-pass filter.

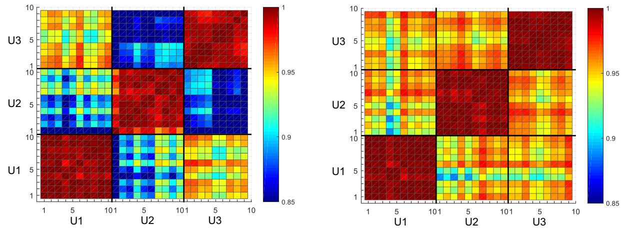
Such morphology characteristics represent cardiac motion patterns which are unique among individuals.

7.1 Systolic-Diastolic Features

In our proposed system, we first extract 30 systolic-diastolic features (i.e., fiducial features) directly from the cardiac wave to characterize cardiac motion. The fiducial features contain the biometric characteristics that are unique and non-volatile with respect to different individuals, and these features are invariant to the emotional state, such as anxiety, nervousness or excitement [20]. As shown in Figure 8 (a), the four cardiac phases in a cardiac cycle are separated by three fiducial points: diastolic peak (DP), dicrotic notch (DN) and systolic peak (SP). We locate these fiducial points by searching for the local maximums and minimums within each cardiac cycle. Specifically, the normalized time intervals t_1, t_2, t_3 and t_4 characterize the duration of ventricular ejection, isovolumetric relaxation, atrial systole and isovolumetric contraction, respectively, while the normalized amplitude values h_1 and h_2 represents the blood flow volumes in corresponding cardiac phases. Note that h_3 is excluded as a feature since it keeps constant (i.e., 1) after normalization. Additionally, we also explore the normalized slopes s_1, s_2, s_3 and s_4 to depict the gradient of blood flow changes in each phase as: $s_j = |\frac{h_j}{t_j}|, j = 1, 2, 3, 4$. We extract a set of 10 systolic-diastolic features from every color channel (i.e., red, green, blue) and obtain 30 features in total. As depicted in Figure 9 (a), the pairwise Pearson correlation of the systolic-diastolic features from the same user present higher correlation than those of different users, which validates the effectiveness of this feature-set.

7.2 Non-fiducial Feature Derivation

The data calibration process (i.e. bandpass filter with cutoff frequency $0.3 - 10Hz$) removes the impacts of human respiration, but the subtle movement of fingertip still introduces the interferences beyond $0.3Hz$ and thereby distorts the biometrics embedded in the cardiac wave. We are thus motivated to utilize high-pass filter to mitigate the interferences caused by the fingertip movement and then extract distinct non-fiducial features. Comparing to fiducial characteristics, non-fiducial features could better characterize overall signal morphology (e.g., shape) of each cardiac cycle. Recent study [24] has shown the success in deriving non-fiducial features from the PPG signal for differentiating users. Specifically, the cardiac waves pass through two high-pass filters with the cutoff frequencies of $1Hz$ and $2Hz$ to obtain two non-fiducial cardiac waves W_{d1} and W_{d2}, respectively. The normalized distances between the local maximums and minimums of W_{d1} and W_{d2} are unique to each individual and together serve as non-fiducial features for characterizing cardiac motion. As shown in Figure 8 (b), 6 features $\{x_1, x_3, x_5, |y_1 - y_2|, |y_3 - y_4|, |y5|\}$ are extracted from every color channel of the two non-fiducial cardiac waves, so there are 36 non-fiducial features in total. The 6 features are selected by finding the horizontal and vertical peak-to-valley distances that are the most distinctiveness among different users. As shown in Figure 9 (b), the much lower correlation between the non-fiducial features of different user than that of the same user demonstrates the effectiveness of this selected feature-set.



(a) Systolic-diastolic features

(b) Non-fiducial features

Figure 9: Pairwise Pearson Correlation of systolic-diastolic and non-fiducial features extracted from 30 cardiac cycles for three different users (i.e., U1, U2, and U3): the features of same user are highly correlated while the features of different users present lower correlation.

8 USER VERIFICATION MODEL

8.1 Feature Transformation grounded on PCA

Cardiac waves may have small-scale variations from day to day, thus we propose a feature transformation scheme to construct reliable user profile and perform user verification ground on PCA [23]. Specifically, PCA transforms cardiac features into a set of orthogonal principal components in a low dimensional space, where the first few ones are the most representative and robust to signal disturbances. The principle components can be derived through applying singular value decomposition (SVD) to the biometric matrix, which consists cardiac features of n cardiac cycle observations, and derive the principle components as $W = \{w_1, w_2, ..., w_p\}$, where $w_j, j = 1, \cdots, p$, represents a n-by-1 principle component vector. Next, we select the top k principal components, called cardiac abstracts, with the largest normalized variances. Particularly, we find that all the cardiac cycles share similar first several principal components, which describe the morphological outline of the derived cardiac wave, and the remaining components could better discriminate different individuals. Therefore, we discard the first two principal components and start the principal component selection process from the third component. The principal component selection process satisfies the following objective function:

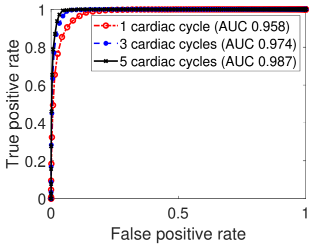


Figure 10: Performance of CardioCam leveraging cardiac cycles from 25 users.

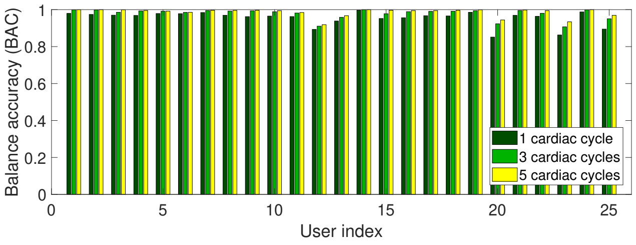


Figure 11: Performance of CardioCam on verifying individual user leveraging 1 cycle, 3 cycles, and 5 cycles, respectively.

$argmin\{k | \sum_{j=3}^{k} \frac{w_j}{\sum_{i=1}^{p} w_i} < \tau, k < p\}$, where k is the number of selected principal components and $\tau = 0.9$ is a pre-defined threshold, which is empirically determined to balance the tradeoff between verification performance and computational complexity.

8.2 Profile Matching

Given that the cardiac abstracts derived from feature transformation, we conduct the user verification through measuring the similarity between the newly captured cardiac abstracts and the profiled cardiac abstracts. Intuitively, the cardiac signs from the legitimate user should have small distance from his/her profile, whereas an unauthorized user should have a relatively large distance. CardioCam uses a set of cardiac abstract vectors $F = \{f_1, ..., f_{70}\}$ derived from 70 cardiac cycles in the profile of a legitimate user. For each cardiac cycle, the cardiac abstract vector is obtained via multiplying a cardiac feature vector with principal component matrix W described in Section 8.1. Given the profiled cardiac abstracts, each newly captured cardiac wave that requests verification will undergo feature transformation grounded on PCA to obtain a cardiac abstract vector s. Then, we compute the average Euclidean distance between each s and F as below:

$$Dist(s) = \frac{\sum_{i=1}^{n} \|f_i - s\|}{n}. \qquad (7)$$

Subsequently, a threshold η is then applied to perform profile matching through a hypothesis test as: the user verification successes if $Dist(s) \leq \eta$; otherwise the verification fails, indicating an adversary or unauthorized user is detected. In order to obtain an optimized threshold, our system needs both legitimate samples and also some adversarial samples from simulated spoofing attacks to examine and score a set of pre-defined thresholds. Particularly, we recursively score the thresholds leveraging Youden's J statistic [54], which is a single statistic that characterizes performance on identifying both the attacker and the legitimate user, and choose the threshold with the maximum Youden's J statistic. Specifically, the optimized threshold η_u for the user u is derived via the following optimization function: $argmax J(\eta_u) = \{\eta_u | \eta_u \in S \land \eta_y \in S : J(\eta_y) \leq J(\eta_u)\}$, where S denotes the set of distances for threshold selection.

9 PERFORMANCE EVALUATION

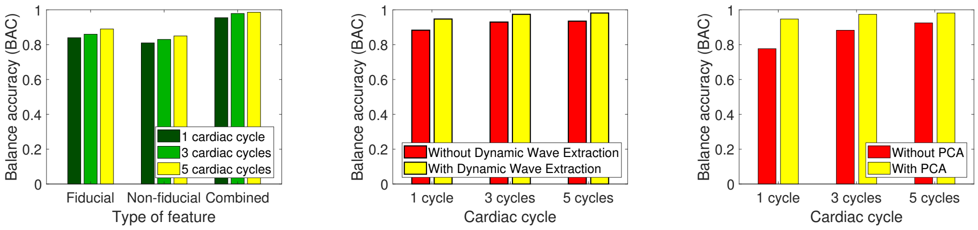
9.1 Experimental Methodology

Devices. We implement *CardioCam* on iPhone 7 with *AVFoundation* framework which provides various image processing and camera configuration functions. iPhone 7 is equipped with a built-in high-definition rear camera with 12 megapixel, which enables video frame rate of $60fps$ with a resolution of $720p/1080p$. Although iPhone 7 supports slow-motion video recording with $120fps/240fps$, we choose the frame rate of $60fps$ that is available on most of the mobile devices, especially the mid-range/low-end smartphones. In addition, we further adjust the frame rate (i.e., $30/40/50/60fps$) and video resolution (i.e., $240/360/480/720p$) programmatically by calling the built-in AVCaptureDevice.Format class to test the generality of our system, which is presented in Section 9.5. Note that CardioCam only adjusts flashlight intensity and camera ISO for better capturing cardiac motion pattern, and the other camera parameters, such as focus distance, shutter speed, and white balance, are locked in the proposed system.

Cardiac Data Collection. The cardiac dataset is collected from 25 participants (19 males and 6 females) aging from 25 to 33. Particularly, we construct a main dataset, which contains three trails for each participant, and each trail lasts 60 seconds including around 60-75 cardiac cycles. In total, we collect 5, 583 cardiac cycle samples from the 25 participants. During the data collection, there is no restriction on the postures of participant (e.g., standing or sitting) and surrounding environments (e.g., indoor or outdoor). In addition, we further construct four separated datasets involving 8 participants to investigate the impacts of biometric variations, different fingers, various fingertip pressing positions, and emotion state changes. We will elaborate the data collection details in section 9.4.

Verification Strategies. To test the performance of our system, we alternatively set each participant as the legitimate user and the remaining 24 participants act as attackers. During the process of user enrollment, the first 70 pre-collected cardiac cycles of each legitimate user is used for PCA coefficient derivation and profile construction, and the rest of the cardiac cycles are for system validation.

Evaluation Metrics. To evaluate our system performance, we define five different metrics: *true positive rate (TPR)* and *false positive rate (FPR)*; *balanced accuracy (BAC)*; *receiver operating characteristic (ROC)* curve; *area under the ROC curve (AUC)*. Particularly, TPR is the percentage of users that are correctly verified as legitimate users, and FPR is the percentage of attackers that are mistakenly identified as legitimate users. BAC is the equal-weight combination of TPR and true negative rate (TNR), i.e., $TNR = 1 - FPR$. The ROC curve is created by plotting the TPR against the FPR under various threshold settings (i.e., η from 0 to 400). AUC is a measurement



(a) Three different feature sets

(b) Dynamic cardiac wave extraction

(c) Feature transformation grounded on PCA

Figure 12: Performance of Individual system components.

of how well the verification model can distinguish between the legitimate and spoofing samples. Note that AUC is usually between 0.5 (random guess) and 1 (perfect verification).

9.2 Performance of User Verification

Figure 10 depicts the average ROC curves of verifying 25 participants leveraging different numbers of cardiac cycles (i.e., 1, 3 and 5) in each verification. Specifically, the AUC for each ROC curve is calculated as 0.958, 0.974, 0.987 for verification with 1 cycle, 3 cycles and 5 cycles, respectively. It is easy to find that 5 cardiac cycles give the best performance. The results demonstrate the effectiveness of CardiaoCam on user verification even with only 3 cardiac cycles per user. Furthermore, in Figure 11, we also present BAC of verifying all 25 participants. We can find that CardioCam achieves 95.5%, 97.9% and 98.6% average BAC with the corresponding standard deviation (STD) of 3.8%, 2.7%, 2.2% for 1 cycle, 3 cycles and 5 cycles, respectively. The above results confirm that CardioCam is highly reliable on verifying all the legitimate users while rejecting the adversaries.

9.3 Effectiveness of Each System Component

Systolic-Diastolic/non-fiducial Features. To analyze the effectiveness of the extracted systolic-diastolic/non-fiducial features, we evaluate CardioCam under three different feature sets: systolic-diastolic feature only, non-fiducial feature only, and the combined feature set. Figure 12(a) shows BAC of verifying 25 users leveraging the three feature sets under 1 cycle, 3 cycles, and 5 cycles. Given 5 cardiac cycles, our system can achieve average BAC of 89.8%, 85.3%, 98.6%, with only systolic-diastolic, only non-fiducial, and the combined feature set, respectively. We observe that systolic-diastolic feature set could achieve better verification performance than that of the non-fiducial feature set. This is because the fiducial features, which describe the amplitude of the inflection points in the four stages of the cardiac cycle, are more robust to heartbeat rate variations. In fact, both fiducial and non-fiducial features contribute to the authentication power of CardioCam, and they are complementary. We observe that the combined feature set achieves the best BAC, indicating that the combination of systolic-diastolic and non-fiducial feature sets can further enhance the user verification accuracy.

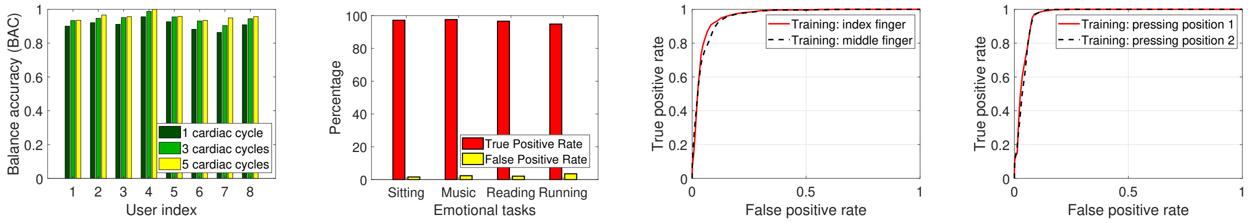
Dynamic Cardiac Wave Extraction. Figure 12(b) the impact of dynamic cardiac wave extraction on the user verification performance. We find that CardioCam is more effective in verifying user with dynamic wave extraction. In particular, when using only 1 cardiac cycle for user verification, CardioCam is improved by 7% BAC using dynamic cardiac wave extraction. This is because the proposed dynamic cardiac wave extraction mechanism can effectively select sensitive pixels and suppress the impacts of ambient noises introduced by small scale variations of fingertip pressing position and pressure.

Feature Transformation grounded on PCA. Next we study the effectiveness of the proposed feature transformation scheme grounded on PCA method. Figure 12(c) depicts the BAC of user verification with and without feature transformation leveraging 1, 3, and 5 cycles. We find that the feature transformation scheme can greatly improve the user verification accuracy, especially when only 1 cardiac cycle is used for user verification. This is because the proposed feature transformation method suppresses the biometric variations in the cardiac biometrics, making the system more robust.

9.4 Evaluation of System Robustness

Biometric Permanence. The cardiac motion patterns always experience small-scale disturbance from day to day, so we further study the robustness of CardioCam by examining the biometric permanence of cardiac motion. Specifically, we take the first 70 cardiac cycles from all the samples to construct the profile for each of the 8 participants, including 5 males and 3 females with ages ranging from 21 to 35.. The data collected in the following three months are used for testing. In addition, during the data collection, there is no restriction on the time of day and surrounding environments (e.g., indoor or outdoor), thus the cardiac cycles of each participant are collected under various ambient light conditions. Figure 13(a) shows the BAC of user verification with 1, 3, and 5 cycles. We find that CardioCam shows very robust performance on user verification even though the cardiac cycles are collected on different days. Specifically, we can observe that CardioCam achieves 90.8%, 94.4%, 95.7% average BAC with standard deviation of 3.1%, 2.6%, 2.2% for 1 cycle, 3 cycles and 5 cycles, respectively. Therefore, we can conclude that there is no significant performance decreasing with the cardiac samples collected from different days, which demonstrates the robustness of CardioCam in a long term.

Impacts of Emotion State. We also study the robustness of CardioCam under various human emotional states. We design a set of emotional tasks involving different levels of stress, and each participant is asked to perform two low-stress tasks (i.e., sitting, listening to music) and two high-stress tasks (i.e., reading, running).



(a) Different days (b) Emotion States (c) Different fingers (d) Two pressing positions

Figure 13: Performance evaluation of collecting cardiac cycles from different days, different emotion states, different fingers, and different fingertip placements.

The designed tasks involve both mental activities and physical exercise (i.e., running) that would greatly change the human's heartbeat rate. Particularly, we construct user profile with 70 cardiac cycles when the participant is sitting. Then, we evaluate CardioCam when the 8 participants are performing one of the four emotional tasks. Figure 13(b) shows the user verification accuracy with respect to four different emotional tasks in terms of TPR and FPR. We find that CardioCam achieves high TPR while maintaining low FPR for all the four tasks. Even for the high-stress task of exercise, which can significantly raise heartbeat rate, CardioCam can still achieve over 94% TPR and less than 4% FPR. This is because the cardiac normalization process and the proposed feature transformation mechanism greatly suppress the interferences caused by human emotion changes. Additionally, since running activity is the aerobic exercise that incurs more significant heartbeat variations than many other common physical activities (e.g., walking), CardioCam has the potential to suppress cardiac motion variations introduced by both physical exercises and daily activities.

Impact of Different Fingers. We next examine the performance of CardioCam with different fingers of the same user applied for user verification. Since the blood circulating in the five fingers are supplied by the same artery, the blood flow pattern should be consistent across different fingertips. For each person among the 8 participants, we collect around 180 cardiac cycles from both index and middle fingers. The user profile is constructed with 70 cardiac cycles collected from either index finger or middle finger, and the remaining cardiac cycles are used for system validation. In order to test the worst case performance of CardioCam, only 1 cardiac cycle is used to verify each individual user. As shown in Figure 13(c), CardioCam achieves similar ROC curves no matter the training set is collected based on index or middle finger. Specifically, both two ROC curves achieve high AUC around 0.953, which validate the effectiveness of our system regardless of which fingertip pressing upon the camera surface.

Impact of Different Fingertip Pressing Positions. To validate the effectiveness of CardioCam on mitigating the impact of varying fingertip pressing positions, we conduct a set of experiments involving 8 participants with their fingertips pressing at different positions upon the camera. Specifically, each subject is required to collect two sets of cardiac motion patterns, and each set includes around 180 cardiac cycles with two different fingertip pressing positions the participant is accustomed to. Specifically, the user profile is constructed with the first 70 cardiac cycles collected from one of the two pressing positions, and the proposed system is then evaluated with the rest of the cardiac samples. Figure 13(d) depicts the average ROC curves of verifying the 8 users leveraging only 1 cardiac cycle in each verification. CardioCam has similar verification performance for both pressing positions, which imply the effectiveness of the proposed method on suppressing the impacts of different fingertip pressing positions.

9.5 Impact of Video Quality

Impact of Camera Sampling Frame Rates. CardioCam infers cardiac motion pattern from the light intensity changes of recorded video stream, so the quality of caridac features is easily affected by the video frame rate. To evaluate the impact of frame rate, the cardiac samples from 25 participants are collected under the frame rates of 30, 40, 50, 60 frames per second(fps) to verify the user identity with 5 cardiac cycles. As the average AUC for user verification shown in Figure 14 (a), we can observe that the higher the frame rate is, the more the verification accuracy improves. This is because the high frame rate mitigates the motion blur in the cardiac wave derivation and ensures a high resolution on the cardiac motion pattern estimation. The above results show that our system has consistently good performance regardless of different frame rates.

Impact of Camera Resolution. At last, to further study the impact of the video quality on capturing unique cardiac biometrics, we use systolic-diastolic/non-fiducial features from video frames with scaled-down resolutions (i.e., 320 × 240, 640 × 360, 854 × 480) to verify 25 users' identity with 5 cardiac cycles. The AUC for the four different camera resolutions are shown in Figure 14 (b). We can find that CardioCam achieves over 0.98 AUC for all of the four resolutions. And the verification performance is highly consistent across different camera resolutions. This is primarily because CardioCam leverages the average light intensity changes of the whole frame, instead of individual or portions of pixels, to capture cardiac biometrics. It is easy to conclude that video resolution has little impact on the user verification performance.

10 DISCUSSION

Deployment Feasibility. CardioCam has a minimum hardware requirement (i.e., camera and flashlight) to facilitate user verification leveraging cardiac biometrics. Specifically, the camera and flashlight are readily available in most mobile devices and IoT appliances, so it will not bring extra cost and inconvenience to the mobile users. Furthermore, as illustrated in section 9, the proposed

CardioCam system can still achieves high verification accuracy of 0.953 and 0.98 even under low frame rate (i.e., 30fps) and a low camera resolution (i.e., 240p). Therefore, we believe CardioCam can be applied to a broad range of mobile and IoT devices with the need of reliable user verification.

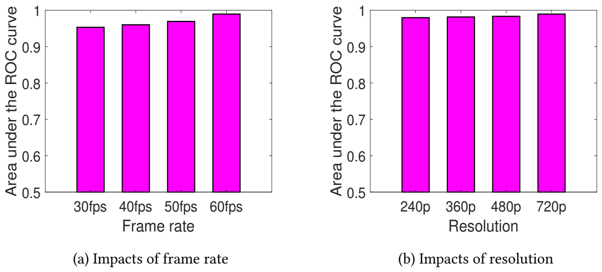
Memory and Energy Consumption. Our system is a lightweight user verification system with low computational complexity and memory/energy overhead. The most memory and power-intensive task in CardioCam is data acquisition, which captures user cardiac pattern with the built-in camera. The recorded video lasts for 2 seconds and takes up only 0.2MB of the memory, and the corresponding power consumption is as low as 4.6J. Given the captured cardiac pattern, CardioCam only takes around 0.5 seconds to complete one-time user verification due to its low complexity design, affordable for most mobile and IoT devices without imposing much overhead.

Authentication Delay. In contrast to other user verification scheme, such as fingerprint and face ID, CardioCam normally takes longer time to complete the verification process (i.e., at least 2.5 seconds depending on individual heart rate). We further find that a large proportion of the time cost is spent on optimizing the camera configuration instead of cardiac sign collection. To reduce the time cost, we will conduct in-depth study on the relationship between pixel sensitivity and ambient light intensity, so that the optimization process can be completed in prior to the cardiac sign collection.

Accuracy Improvement and Further Evaluation. While it is not yet clear whether the cardiac features in our system are sufficiently distinctive in a large user population, our results show promise, at least as an additional signal used in conjunction with other existing techniques (e.g., fingerprint and face recognition). In our future work, we target to evaluate the system's scalability using various devices with different camera-flashlight settings, more serious attacks (e.g., the attacker can reproduce the systolic-diastolic features). We will try to improve the verification accuracy by exploring the advances in mobile/IoT hardware, such as emerging multiple cameras and improvements in video frame rate (e.g., 120-240fps), and the fiducial/non-fiducial features that are more discriminative among different people. In addition, we used the video frames with various scaled-down resolutions for evaluating the impact of camera resolution. The results show that CardioCam is capable of suppressing the impacts of frame resolution due to the use of pixel average instead of the image features (e.g., edges, interest points). To further study the impact of low-resolution cameras on our system, we will evaluate the scalability of CardioCam with low-end smartphones that have lower camera resolution (e.g., 320 × 240).

Copping with Spoofing Attack. The most extreme case is when an adversary acquires cardiac waves of the legitimate user (e.g., via pulse oximetry) and tries to spoof CardioCam by regenerating the cardiac motion pattern with a semiconductor light source (e.g., a red light-emitting diode). To deal with such attacks, we could further explore cardiac motion patterns of different color channels (e.g., green and blue), which are hard to forge with the light source of single color. We would leave the detailed study of such adversarial cases as an avenue for our future work.

Robustness under Cardiac Illnesses. Currently, our work mainly focuses on verifying the identifies of health people, who do not have heart diseases such as arrhythmia and congenital heart failure. But the cardiac abnormalities could have considerable impacts on the cardiac motion pattern and thus affect the stability of cardiac biometrics. In the future, we plan to apply CardioCam to the people with cardiovascular diseases and develop more general user verification mechanisms.



(a) Impacts of frame rate

(b) Impacts of resolution

Figure 14: Performance evaluation under different video qualities.

11 CONCLUSION

In this paper, we propose CardioCam, the first low-cost, general and hard-to-forge cardiac biometric based user verification system. Unlike existing user verification systems, CardioCam extracts unique cardiac biometrics for verifying the user's identity leveraging the readily available built-in camera in mobile devices and IoT appliances. To enable highly reliable cardiac motion derivation, we devise a gradient-based camera configuration optimization technique together with dynamic pixel selection to mitigate the impact from ever-changing ambient light and fingertip touch pressure/positions. To facilitate accurate user verification, CardioCam takes two types of biometrics, morphological and non-fiducial features, into consideration. A prototype system is implemented to evaluate the performance of CardioCam through extensive experiments involving 25 subjects. The results demonstrate that CardioCam can achieve remarkable accuracy and robustness on verifying legitimate user while denying unauthorized users under various camera settings and data collection modes.

12 ACKNOWLEDGMENT

We thank our shepherd, Dr. Landon Cox, and the anonymous reviewers for their insightful feedbacks. This work was partially supported by the National Science Foundation Grants CNS-1820624, CNS-1801630, CNS-1814590, CNS-1717356, CNS-1815908, CNS-1618019 and ARO W911NF-18-1-0221.

REFERENCES

[1] Foteini Agrafioti, Jiexin Gao, and Dimitrios Hatzinakos. 2011. Heart biometrics: Theory, methods and applications. In *Biometrics*. InTech.
[2] John Allen. 2007. Photoplethysmography and its application in clinical physiological measurement. *Physiological measurement* 28, 3 (2007), R1.
[3] Amazon. 2018. Echo Look, Hands-Free Camera and Style Assistant with Alexa. https://www.amazon.com/Amazon-Echo-Look-Camera-Style-Assistant/dp/B0186JAEWK.
[4] Amazon.com. 2018. Amazon Dash Button, Official Site. https://www.amazon.com/Amazon-JK29LP-Tide-Dash-Button/dp/B0187TMRYM.
[5] Anatomy and Physiology. 2019. Cardiac Cycle. http://library.open.oregonstate.edu/aandp/chapter/19-3-cardiac-cycle/.

[6] Apple. 2017. Face ID Security. https://www.apple.com/ca/business-docs/FaceID_Security_Guide.pdf.

[7] Arathi Arakala, Jason Jeffers, and Kathy J Horadam. 2007. Fuzzy extractors for minutiae-based fingerprint authentication. In *International Conference on Biometrics (Springer)*. 760–769.

[8] Juan Sebastian Arteaga-Falconi, Hussein Al Osman, and Abdulmotaleb El Saddik. 2016. ECG authentication for mobile devices. *IEEE Transactions on Instrumentation and Measurement* 65, 3 (2016), 591–600.

[9] Adam J Aviv, Katherine L Gibson, Evan Mossop, Matt Blaze, and Jonathan M Smith. 2010. Smudge Attacks on Smartphone Touch Screens. *Woot* (2010).

[10] Zhongjie Ba, Sixu Piao, Xinwen Fu, Dimitrios Koutsonikolas, Aziz Mohaisen, and Kui Ren. [n. d.]. ABC: Enabling Smartphone Authentication with Built-in Camera. ([n. d.]).

[11] Lena Biel, Ola Pettersson, Lennart Philipson, and Peter Wide. 2001. ECG analysis: a new approach in human identification. *IEEE Transactions on Instrumentation and Measurement* 50, 3 (2001), 808–812.

[12] Angelo Bonissi, Ruggero Donida Labati, Luca Perico, Roberto Sassi, Fabio Scotti, and Luca Sparagino. 2013. A preliminary study on continuous authentication methods for photoplethysmographic biometrics. In *Workshop on Biometric Measurements and Systems for Security and Medical Applications (IEEE BIOMS)*.

[13] Nam Bui, Anh Nguyen, Phuc Nguyen, Hoang Truong, Ashwin Ashok, Thang Dinh, Robin Deterding, and Tam Vu. 2017. Photometry based Blood Oxygen Estimation through Smartphone Cameras. In *Proceedings of the 9th ACM Workshop on Wireless of the Students, by the Students, and for the Students (ACM S3)*. 29–31.

[14] tokyo Cara McGoogan Danielle Demetriou. 2017. Peace sign selfies could let hackers copy your fingerprints. http://www.telegraph.co.uk/technology/2017/01/12/peace-sign-selfies-could-let-hackers-copy-fingerprints/.

[15] Shaxun Chen, Amit Pande, and Prasant Mohapatra. 2014. Sensor-assisted facial recognition: an enhanced biometric authentication system for smartphones. In *Proceedings of the 12th annual international conference on Mobile systems, applications, and services (ACM MobiSys)*. 109–122.

[16] Mohamed Elgendi. 2012. On the analysis of fingertip photoplethysmogram signals. *Current cardiology reviews* 8, 1 (2012), 14–25.

[17] Nesli Erdogmus and Sebastien Marcel. 2014. Spoofing face recognition with 3D masks. *IEEE transactions on information forensics and security* (2014).

[18] Priyanshu Gupta, Shipra Behera, Mayank Vatsa, and Richa Singh. 2014. On iris spoofing using print attack. In *2014 22nd international conference on Pattern recognition (ICPR)*. IEEE, 1681–1686.

[19] Apple Inc. 2017. About Face ID advanced technology. https://support.apple.com/en-us/HT208108.

[20] Steven A Israel, John M Irvine, Andrew Cheng, Mark D Wiederhold, and Brenda K Wiederhold. 2005. ECG to identify individuals. *Pattern recognition* 38, 1 (2005), 133–142.

[21] Anil K Jain, Lin Hong, Sharath Pankanti, and Ruud Bolle. 1997. An identity-authentication system using fingerprints. *Proc. IEEE* 85, 9 (1997), 1365–1388.

[22] Tsai-Yang Jea and Venu Govindaraju. 2005. A minutia-based partial fingerprint recognition system. *Pattern Recognition* 38, 10 (2005), 1672–1684.

[23] Ian T Jolliffe. 1986. Principal component analysis and factor analysis. In *Principal component analysis*. Springer, 115–128.

[24] Nima Karimian, Mark Tehranipoor, and Domenic Forte. 2017. Non-fiducial ppg-based authentication for healthcare application. In *Biomedical & Health Informatics (BHI), 2017 IEEE EMBS International Conference on*. IEEE, 429–432.

[25] A Reşit Kavsaoğlu, Kemal Polat, and M Recep Bozkurt. 2014. A novel feature ranking algorithm for biometric recognition with PPG signals. *Computers in biology and medicine (Elsevier)* 49 (2014), 1–14.

[26] Miyuki Kono, Hironori Ueki, and Shin-ichiro Umemura. 2002. Near-infrared finger vein patterns for personal identification. *Applied Optics* (2002).

[27] Ajay Kumar and Arun Passi. 2010. Comparison and combination of iris matchers for reliable personal authentication. *Pattern recognition (Elsevier)* (2010).

[28] Yuriy Kurylyak, Francesco Lamonaca, Domenico Grimaldi, and FJ Duro. 2012. Smartphone based photoplethysmogram measurement. *Digital image and signal processing for measurement systems* (2012), 135–164.

[29] Leslie Lamport. 1981. Password authentication with insecure communication. *Commun. ACM* 24, 11 (1981), 770–772.

[30] Feng Lin, Chen Song, Yan Zhuang, Wenyao Xu, Changzhi Li, and Kui Ren. 2017. Cardiac Scan: A Non-contact and Continuous Heart-based User Authentication System. In *Proceedings of the 23rd Annual International Conference on Mobile Computing and Networking (ACM MobiCom)*. 315–328.

[31] Davide Maltoni, Dario Maio, Anil K Jain, and Salil Prabhakar. 2009. *Handbook of fingerprint recognition*. Springer Science & Business Media.

[32] Kenta Matsumura and Takehiro Yamakoshi. 2013. iPhysioMeter: a new approach for measuring heart rate and normalized pulse volume using only a smartphone. *Behavior research methods (Springer)* 45, 4 (2013), 1272–1278.

[33] SC Millasseau, RP Kelly, JM Ritter, and PJ Chowienczyk. 2002. Determination of age-related increases in large artery stiffness by digital pulse contour analysis. *Clinical science* 103, 4 (2002), 371–377.

[34] Naoto Miura, Akio Nagasaka, and Takafumi Miyatake. 2004. Feature extraction of finger-vein patterns based on repeated line tracking and its application to personal identification. *Machine vision and applications* 15, 4 (2004), 194–203.

[35] Yunyoung Nam, Jinseok Lee, and Ki H Chon. 2014. Respiratory rate estimation from the built-in cameras of smartphones and tablets. *Annals of biomedical engineering (Springer)* 42, 4 (2014), 885–898.

[36] PaymentsSource. 2018. Slideshow Data: IndiaâĂŹs mobile payments market is ready to boom. https://www.paymentssource.com/slideshow/data-indias-mobile-payments-market-is-ready-to-boom.

[37] The Student Physiologist. 2016. The Cardiac Cycle And Cardiac Output. https://thephysiologist.org/study-materials/the-cardiac-cycle-and-cardiac-output/.

[38] Carmen CY Poon, Yuan-Ting Zhang, and Shu-Di Bao. 2006. A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health. *IEEE Communications Magazine* 44, 4 (2006), 73–81.

[39] Lawrence R Rabiner, Bernard Gold, and CK Yuen. 1978. Theory and application of digital signal processing. *IEEE Transactions on Systems, Man, and Cybernetics* 8, 2 (1978), 146–146.

[40] Ring. 2018. Video Doorbells. https://shop.ring.com/collections/video-doorbells.

[41] Aditi Roy, Nasir Memon, and Arun Ross. 2017. MasterPrint: exploring the vulnerability of partial fingerprint-based authentication systems. *IEEE Transactions on Information Forensics and Security* 12, 9 (2017), 2013–2025.

[42] Sairul I Safie, John J Soraghan, and Lykourgos Petropoulakis. 2011. Electrocardiogram (ECG) biometric authentication using pulse active ratio (PAR). *IEEE Transactions on Information Forensics and Security* 6, 4 (2011), 1315–1322.

[43] SAMSUNG. 2018. Family Hub Refrigerator. https://www.samsung.com/us/explore/family-hub-refrigerator/overview/.

[44] Roger Schneider. 2011. Survey of peaks/valleys identification in time series. *Department of Informatics, University of Zurich, Switzerland* (2011).

[45] Tsu-Wang Shen, WJ Tompkins, and YH Hu. 2002. One-lead ECG for identity verification. In *24th annual conference and the annual fall meeting of the biomedical engineering society (IEEE EMBS)*, Vol. 1. 62–63.

[46] Women Love Tech. 2017. Bridging the Gap Smartphones in Third World Countries. https://womenlovetech.com/bridging-the-gap-smartphones-in-third-world-countries/.

[47] Kamlesh Tiwari, C Jinshong Hwang, and Phalguni Gupta. 2016. A palmprint based recognition system for smartphone. In *Future Technologies Conference (IEEE FTC)*. 577–586.

[48] Ton Van der Putte and Jeroen Keuning. 2000. Biometrical fingerprint recognition: donâĂŹt get your fingers burned. In *Smart Card Research and Advanced Applications (Springer)*. 289–303.

[49] Shreyas Venugopalan and Marios Savvides. 2011. How to generate spoofed irises from an iris code template. *IEEE Transactions on Information Forensics and Security* 6, 2 (2011), 385–395.

[50] Edward J Wang, William Li, Junyi Zhu, Rajneil Rana, and Shwetak N Patel. 2017. Noninvasive hemoglobin measurement using unmodified smartphone camera and white flash. In *Engineering in Medicine and Biology Society (EMBC), 2017 39th Annual International Conference of the IEEE*. IEEE, 2333–2336.

[51] Edward Jay Wang, Junyi Zhu, Mohit Jain, Tien-Jui Lee, Elliot Saba, Lama Nachman, and Shwetak N Patel. 2018. Seismo: Blood Pressure Monitoring using Built-in Smartphone Accelerometer and Camera. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. ACM, 425.

[52] Susan Wiedenbeck, Jim Waters, Jean-Camille Birget, Alex Brodskiy, and Nasir Memon. 2005. Authentication using graphical passwords: Effects of tolerance and image choice. In *Proceedings of the 2005 symposium on Usable privacy and security (ACM SOUPS)*. 1–12.

[53] Tzong-Sun Wu, Ming-Lun Lee, Han-Yu Lin, and Chao-Yuan Wang. 2014. Shoulder-surfing-proof graphical password authentication scheme. *International journal of information security* 13, 3 (2014), 245–254.

[54] William J Youden. 1950. Index for rating diagnostic tests. *Cancer* (1950).

[55] Zhaomin Zhang and Daming Wei. 2006. A new ECG identification method using bayes' teorem. In *2006 ieee region 10 conference Tencon*. IEEE, 1–4.

CardioCam：利用移动设备上的摄像头在用户心跳时对其进行验证

摘 要

随着移动和物联网设备（如智能手机、平板电脑、智能家电）的日益普及，这些设备上存储了大量私人和敏感信息。为了防止对这些设备的未经授权访问，现有的用户验证解决方案要么依赖于用户定义的秘密（例如密码）的复杂性，要么求助于专门的生物特征传感器（例如指纹读取器），但用户仍可能遭受各种攻击，如密码盗窃、肩部冲浪、污迹和伪造的生物特征攻击。在本文中，我们提出了 CardioCam，这是一种低成本、通用、难以伪造的用户验证系统，利用了从移动和物联网设备中现成的内置摄像头中提取的独特心脏生物特征。我们证明，通过按下内置摄像头，可以从指尖的心脏运动模式中提取出独特的心脏特征。减轻各种环境照明条件和人类活动的影响。

关键词：摄像头、身份验证、移动设备、心脏生物特征。

目　录

第 1 章 介绍

移动和物联网设备（如智能手机、平板电脑和智能家电）的使用越来越普遍，不可避免地包含私人和敏感信息（如联系人列表、电子邮件、信用卡号和商品订购信息）。未经授权访问此类设备可能会使大量敏感信息面临被滥用的风险。传统的用户验证解决方案主要依赖于密码或图形模式[1]，它们会遭受各种攻击，包括密码盗窃、肩部冲浪[2]和污迹攻击[3]。基于生物识别的用户验证为安全移动设备开辟了一条新途径，尤其是基于指纹的解决方案[4-5]，这些解决方案被广泛部署在许多高级智能手机（如 iPhone 和三星手机）中，并为访问移动和智能设备提供了一种更安全的方式。然而，在世界上许多没有专用指纹传感器的发展中地区，50 美元及以下的手机（如 BLU A4）仍有很大的市场[6]。此外，由于地理区域分布广泛，缺乏传统的银行和支付基础设施，其中一些低成本市场严重依赖移动支付[7]。此外，基于指纹的解决方案容易受到通过受害者照片创建的合成指纹的影响[8]。这导致人们重新寻找低成本、通用、难以伪造的安全解决方案，这也有助于使用越来越方便的移动支付系统。现有研究表明，使用附体 PPG/ECG 传感器[9-12]或多普勒雷达[13]正在寻求通过捕捉人类心脏生物特征来执行用户验证。这些现有的调查通常需要专门的设备（例如传感器或雷达设备），这可能会增加额外的成本并给移动用户带来不便。朝着这个方向，我们提出了 CardioCam，它不需要专门的设备来提取独特的心脏生物特征来进行用户验证。CardioCam 使用内置摄像头，几乎所有类型的移动设备都可以使用，包括一些研究人员已经表明，智能手机上的内置摄像头可以用来测量心率和脉搏容积[14]。现有工作[15]还证明了智能手机摄像头捕捉的心脏信号的正确性和适用性，这些信号与专业医疗仪器（即脉搏血氧计）测量的信号非常接近[15]。然而，摄像头是否能够提取独特的心脏生物特征用于用户验证仍然是一个悬而未决的问题。CardioCam 进一步探索了内置摄像头的局限性，旨在利用摄像头提取的独特心脏生物特征实现用户验证。该系统只需用户将指尖按在相机表面即可提取心脏特征，如图 1-1 所示。因此，它可以直接应用于几乎所有的移动设备，以执行用户验证，包括解锁设备和授权特定权限。例如，FridgeCam 允许用户将一个小摄像头贴在冰箱内部，用于储存食物监控。亚马逊的虚拟助理 Echo Look 也配备了摄像头，以支持其不断增长的命令集（例如，询问对哪套衣服最好看的意见）。此外，如今，配备低成本摄像头的小型物联网

设备，如视频门铃，正在为许多家庭安全系统提供服务，亚马逊 Dash Button 可以轻松地与低成本摄像头集成，以实现用户验证，从而保护隐私。因此，在物联网设备上大规模部署摄像头为 CardioCam 验证用户的各种应用提供了巨大的机会，例如入口的访问控制、通过带家长控制的冰箱点餐以及通过虚拟助理购买衣服，而不透露个人生活方式。

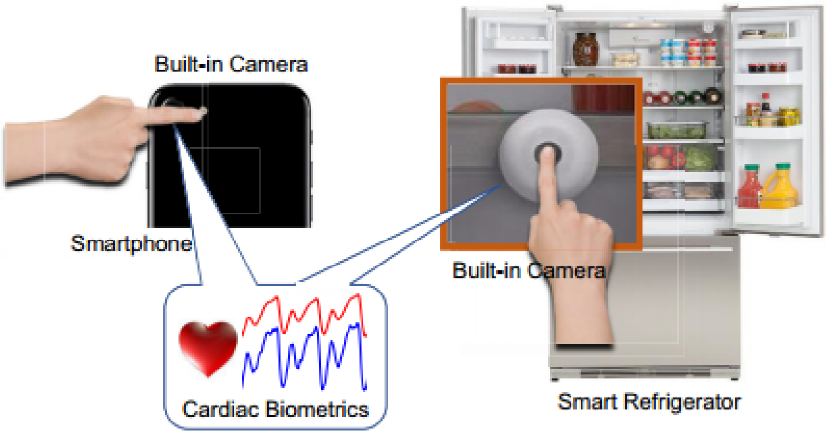


图 1-1 使用设备内置摄像头实现基于心脏模式的用户验证

传统解决方案。移动设备上的内置摄像头已被用于使用生物特征进行用户验证，包括虹膜图案、面部特征和掌纹。这些解决方案主要依赖于基于计算机视觉的方法，通常会受到伪造生物特征的欺骗攻击。例如，基于虹膜的用户验证系统可能会被与合法用户具有相同虹膜纹理的合成虹膜图像欺骗。iPhone X 上的 Face ID 可以捕捉用户面部的几何形状和深度，以验证用户的身份。尽管已被证明比基于指纹的身份验证（如 Touch ID）更安全，但该技术需要高端且昂贵的摄像头（如 TrueDepth 前置摄像头）。此外，这些基于视觉的解决方案可能会导致相机拍摄的视觉内容中嵌入的丰富信息引起的隐私问题，并且它们的性能可能会因周围的照明条件而降低。

使用内置摄像头进行基于心脏模式的用户验证。在本文中，我们探索从内置摄像头中提取心脏生物特征。已经证明，在大量人群中，心脏特征是内在的、独特的和非意志的[16-17]。在这项工作中，我们没有使用 PPG/ECG 传感器，而是通过按下内置相机，搜索从指尖的心脏运动模式中提取的独特心脏特征。我们希望从指尖提取的心脏特征在不同的个体之间是可区分的，并可以作为有效用户验证的候选者。心脏

特征通常在实际场景下受到影响：提取的心脏运动模式受到照明条件的影响；心跳随着动作和人类情绪的变化而变化；指尖按压位置和压力在心脏生物特征提取中也起着关键作用。为了解决上述挑战，CardioCam 自适应地更新相机配置，并动态导出心脏。

为了便于生物特征提取，CardioCam 将心脏测量分为不同的心动周期，并对每个心动周期的持续时间/振幅进行归一化，以减轻心率/强度变化的影响。归一化过程将增强导出的心脏生物特征的鲁棒性，同时保留心脏运动模式中嵌入的形态学特征。我们通过形态学特征分析进一步提取每个心动周期内用户特定的心跳特征。为了有效抑制小规模的心脏运动变化，开发了一种基于主成分分析（PCA）的特征变换方案。这些特性抽象用于在系统注册期间构建合法的用户配置文件。在验证阶段，CardioCam 检查新观察结果和用户配置文件之间的特征抽象的欧几里得距离，以验证合法用户或拒绝对手。我们工作的主要贡献总结如下：

- 据我们所知，CardioCam 是第一个低成本的通用用户验证系统，它使用从移动设备或物联网设备上的内置摄像头中提取的心脏生物特征。

- 我们证明，当从指尖提取心脏特征时，可以保留固有的、独特的和非意志的心脏特性；当用户按下指尖时，内置摄像头上的反射光可以很好地捕捉到心脏生物特征。

- 我们开发了一种基于梯度的优化技术，该技术使相机的配置适应环境光的变化和人类运动的变化，并从一组动态选择的图像像素中获得高质量的心脏测量值。给定对心脏运动敏感的选定像素，可以抑制指尖位置和压力对相机的影响。

- 通过所提出的心脏生物特征提取和基于 PCA 的特征转换方案，我们证明了 CardioCam 可以稳健地验证用户，并对建模的攻击具有弹性，在这种攻击中，对手将自己的指尖压在相机上，希望通过系统。

- 我们在各种数据收集策略和系统设置下对 25 名受试者进行了广泛的实验。结果表明，CardioCam 可以实现 99% 以上的平均真阳性率（TPR）来验证用户，同时保持低于 4% 的假阳性率（FPR）来很好地拒绝对手。

第 2 章 相关工作

传统的用户验证机制依赖于密码或图形屏幕模式[1]，这需要用户记住复杂的文本/图形秘密，以验证他们的身份。由于这些解决方案只验证秘密本身，而不是用户，因此它们通常容易受到各种攻击，如肩部冲浪[2]和污迹攻击[3]。

作为一种替代方案，许多研究人员采用生理生物特征来进行用户验证。特别是，基于指纹的解决方案已成为 iPhone 和三星 Galaxy S 系列等许多高端智能手机的基本规范。然而，指纹读取器在大多数中低端移动设备中仍然不可用，基于指纹的系统也容易受到使用合成伪像的欺骗攻击。除了指纹之外，其他人类生物特征（例如虹膜、人脸和掌纹）也被用来在摄像头的帮助下实现用户验证，尤其是移动设备上的内置摄像头，它已经被用于设备认证。然而，由于相机捕获的图像/视频中嵌入了丰富的信息，这种基于视觉的解决方案的隐私问题阻碍了它们的广泛使用。例如，周围的背景场景可以公开用户的位置、生活环境或任何个人物品。此外，上述基于视觉的解决方案中捕获的生物特征（如虹膜、人脸、掌纹）都是人类的外部特征，可以被对手伪造以发动欺骗攻击。

为了克服上述弱点，一些研究依赖于从心电图（ECG）和光体积描记术（PPG）信号中得出的内在心脏生物特征（例如，心跳模式）。然而，这些方法需要用户将专用传感器连接到他们的胸部或指尖，这使得它们很难应用于移动用户。心脏扫描[13]最近提出了一种利用多普勒雷达提取不同心脏运动模式的非侵入性方法，用于用户身份验证，但专用设备的参与也增加了额外的成本，给移动用户带来了不便。

对移动用户的不便。

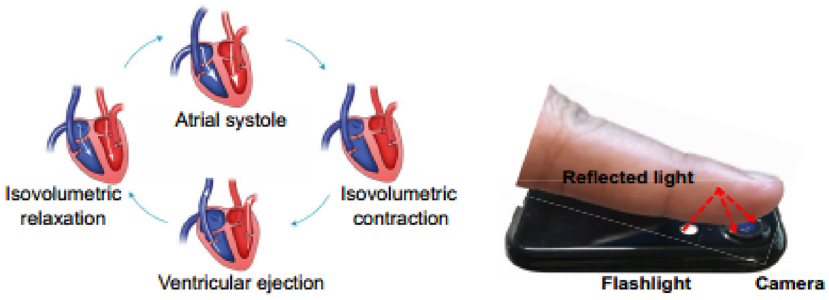
为了消除涉及专业设备的限制，一些研究探索利用商业现成设备上现成的传感器来捕捉心脏生物特征。具体而言，Matsumura 等人[14]证明，当用户将指尖放在内置相机上时，可以测量心率和脉搏容积。此外，Seism 提出利用智能手机加速度计和内置摄像头推导脉冲传输时间（PTT）。一些研究人员进一步利用内置摄像头来估计血氧水平 PhO2 和血红蛋白水平。朝着这个方向，本文进一步探索了使用内置摄像头提取非自愿且难以伪造的心脏生物特征来进行用户验证的可行性。与现有的生物识别认证（如指纹、人脸识别）相比，CardioCam 具有更好的可扩展性，因为它只需要内置摄像头和手电筒，几乎所有类型的移动设备都可以使用。此外，我们的系统是一

个轻量级的用户验证系统，具有极低的计算复杂度和内存/能量开销。

第 3 章 预备知识

3.1 心血管系统动力学

心脏通过交替的心肌收缩和舒张将血液泵入血管，形成一种周期性的心跳模式，称为心动周期，而血管携带血液在包括指尖在内的全身循环。如图 3-1（a）所示，人类心脏包含四个腔室（即左上心房和右心房；以及左下心室和右下心室），典型的心动周期通常包括四个主要阶段：心房收缩、等容收缩、心室射血和等容舒张。在心房收缩阶段，心室收缩，而心房放松并采集血液。然后是体积收缩，心室收缩，所有心室的血容量都没有相应的变化。当心室开始喷出血液（即心室喷出）时，心房收缩，将血液泵送到心室。最后，一个称为等容舒张的短时间间隔开始，心房瓣膜开始闭合直到另一个心动周期开始。由于心血管系统存在生理差异（如心脏大小、形状和组织等），不同的人心肌收缩和舒张的幅度不同。因此，血管中的血流在不同个体的心动周期内遵循独特的变化趋势。ECG 和 PPG 信号都有能力揭示嵌入心动周期四个阶段的独特心脏生物特征，现有工作[17]已经证明了这种心脏生物特征在大量人群中的独特性。与基于 PPG 的方法类似，CardioCam 通过用外部光源（即手电筒）照射指尖来测量血流变化方面的心脏运动模式，从而可以捕获等效的独特生物特征。此外，通过指尖静脉的血流会产生独特的心脏运动模式。这种模式可以揭示指尖血管的扩张性，并反映独特的静脉特征（如静脉分布），这已在大量人群中得到证明。



(a) Human cardiac cycle [37]

(b) Data collection

图 3-1 心动周期的四个阶段以及利用相机和手电筒进行的数据收集。

因此，我们受到启发，从心脏运动模式中提取有效的生物特征，以进行用户验

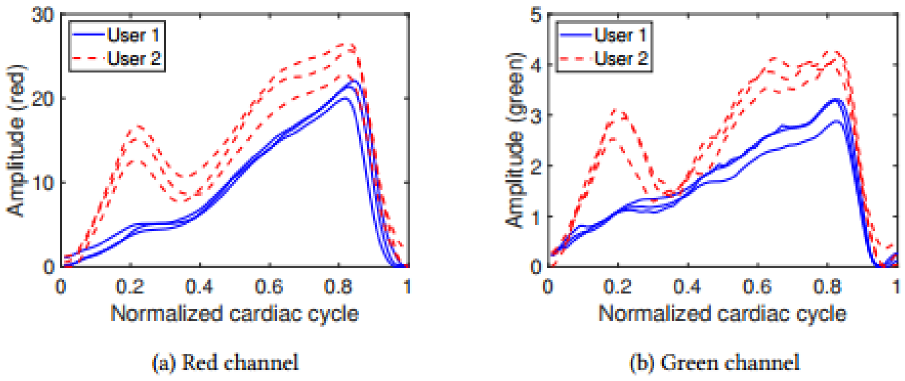
证。

3.1.1 捕捉心脏运动

考虑到心脏运动模式的内在、独特和非意志特性，下一步是如何有效地提取生物特征。与现有的依靠专门仪器捕捉心脏运动的工作不同，我们试图通过商用现成设备通过指尖检查反映独特心脏运动的血流。如图 3-1（b）所示，通过用智能手机上的手电筒照射指尖皮肤，内置摄像头可以连续观察血流变化引起的光吸收变化，其中嵌入了独特的心脏特征。

具体来说，内置相机的每个像素都充当一个独立的光传感器，以检测指尖上的光变化。由于当前智能手机摄像头的高分辨率（例如，每帧 1280×720 像素），可以实现细粒度的心动周期监测。此外，每个像素的三个颜色通道（即红色、蓝色和绿色）为有效的特征提取提供了多个维度。相比之下，传统的心脏监测仪，如光电心电图（PPG）传感器，只能支持多达 3 种不同的光电二极管（即红色、绿色、红外光电二极管），相当于三个像素，用于心脏动态检测。

图 3-2 显示了两个不同用户在三个心动周期内两个不同颜色通道（即红色和绿色）的光强变化。我们对每个心动周期的时间尺度进行了归一化，以消除心率波动的影响。很明显，两位用户在两种颜色通道中都表现出不同的心脏运动模式，这证实了智能手机摄像头可以捕捉到独特的心脏特征。此外，由于人类皮肤对不同颜色的光具有不同的吸收/反射率，由红色和绿色通道揭示的心脏运动模式具有轻微的差异，这反而为可靠的心脏特征提取提供了一些冗余。



(a) Red channel (b) Green channel

图 3-2 从相机的红色和绿色通道中提取的两个用户的心动周期

第 4 章 系统概述

4.1 挑战

为了利用移动和智能设备上无处不在的内置摄像头，利用独特的心脏生物识别技术实现有效的用户验证，需要解决许多挑战。

可靠的心脏测量。用户验证的成功建立在对心脏运动模式的可靠测量之上。然而，在实际情况下，各种影响因素，如环境照明条件、指尖按压位置和人体运动，都会影响导出的心脏测量的可靠性。因此，在所提出的系统的心脏测量中减轻这些影响是至关重要的。

心脏特征的独特性。由于心脏运动模式是通过用内置相机捕捉指尖的血流变化间接获得的，因此将记录的视频帧转换为与独特心脏运动模式相关联的可靠心脏生物特征是一项具有挑战性的任务。此外，为了促进有效的用户验证，从原始心脏测量中提取和验证代表性的生物特征是很重要的。

系统鲁棒性。心脏测量也受到许多随机因素的影响，如情绪变化、心率和呼吸频率的变化。该系统应该能够消除这种随机性，并得出稳健的生物特征抽象。有必要开发一种能够抑制小规模心脏运动变化的变换算法。

4.2 攻击模型

我们考虑的攻击场景是，对手试图访问合法用户无人看管的私人移动设备上的敏感信息或功能（如时间表、照片和移动支付）。对手对合法用户的心脏生物特征没有任何先验知识。为了欺骗设备，对手试图通过将指尖按在内置摄像头上，利用对手自己的心脏生物特征通过用户验证过程。此外，对手还可以移动其指尖相对于相机的位置或调整手指压力，旨在产生与合法用户相似的心脏生物特征。

4.3 系统概述

CardioCam 的基本理念是借助手机上无处不在的内置摄像头/手电筒，利用内在、独特和非自愿的心脏生物特征来验证用户的身份设备。当用户试图访问敏感信息/功能（例如，移动支付、照片）或通过向上滑动设备的触摸屏或按下开关按钮解锁其移动设备时，可以触发 CardioCam。考虑到视频录制和配置文件匹配的时间，CardioCam

完成一次性用户验证大约需要 2.5 秒。当检测到相机被指尖覆盖时，数据采集将在内置相机和手电筒打开的情况下初始化。在手电筒的照射下，与心脏运动模式相关的指尖血流将被内置相机以视频帧的形式捕捉到。在推导心脏运动之前，我们首先开发了一种基于梯度的优化技术，以调整相机配置（即闪光灯强度，ISO），以补充环境光的变化。接下来，通过模块“动态心波提取”从捕获的视频帧中导出可靠的心脏运动模式。由于指尖的按压位置和压力在验证过程中可能会保持轻微变化，我们建议动态像素选择仅包括对心脏运动最敏感的像素子集，以提高心脏测量的信噪比。特别地，在每个单独的心动周期内确定敏感像素，该心动周期通过搜索心脏测量中的后续局部最小值来分割。然后，所选像素的视频流将被转换为关于红色、绿色和蓝色通道的三个心波，随后分别进行带通滤波器和归一化处理，以减轻由人类呼吸和心率变化引起的影响。

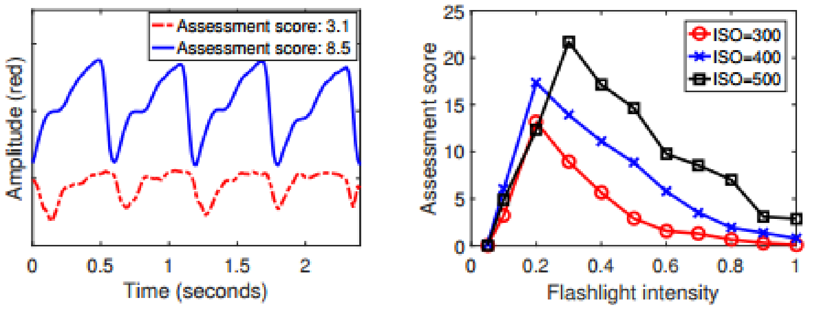
第 5 章 摄像机参数优化

我们的初步研究发现，只有在适当的摄像机配置下才能获得可靠的心脏运动模式有足够数量的光进入相机。极低或极高的闪光灯照明会降低从相机捕捉心脏运动模式时的像素灵敏度。由于各种环境照明条件，CardioCamera 需要调整相机配置，以补充环境光源（如太阳、人造光）引入的光线。因此，我们在相机/手电筒配置上设计了一个基于梯度的优化方案，以减轻环境光的影响。

如图 5-1（b）所示，无论是高或低相机 ISO/闪光灯照明，在检测心脏运动模式时都无法达到令人满意的帧质量。特别地，当 ISO 分别为 300、400 和 500 时，在 0.2、0.2 和 0.3 的闪光灯强度下可以发现最大评估分数。这一观察结果促使我们寻找最佳的相机和闪光灯配置（即 ISO 和闪光灯强度），以最大限度地提高像素灵敏度（即评估分数 S）。具体来说，我们开发了一种迭代搜索方法，其中下一次配置调整是基于当前配置的反馈。每次迭代的闪光灯/ISO 偏移量计算如下：

$$a_{n+1} = a_n + \gamma \nabla S(a_n) \tag{5-1}$$

其中 an 表示第 n 个心动周期的闪光灯强度或相机 ISO 配置，并且相应的评估分数表示为 S（an）。在每个心动周期，都会按照梯度上升方向更新 $\nabla S(an)$，具有固定的步长值（即，γFL=0.05 和 γi SO=5），直到达到令人满意的像素灵敏度（即，超过经



(a) Cardiac waves with different assessment scores

(b) Assessment scores under different light intensity/ISO

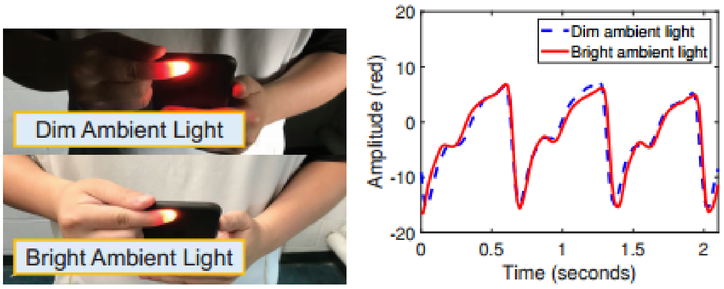
图 5-1 各种条件下心电波的评估分数 S 的图解

验阈值）。算法 1 对优化过程进行了总结。

图 5-2 显示了当周围环境分别处于两种不同的环境光照条件下（即，昏暗和明亮的环境光）时，用户导出的心搏波的示例。随着 CardioCamera 自适应地调整相机闪光灯和 ISO 配置，以补充环境光的变化，我们观察到在两种不同的照明环境下收集的心搏波表现出相似的形态特征。结果表明，所提出的摄像机参数优化是一种很有前途和可靠的方法，可以确保高质量的心脏运动模式推导。

Algorithm 1 视频生物识别优化

```
function CameraAdjustment
    $ISO = 550, S_{prev} = 0, FL_{prev} = 0$
    while $S < Threshold$ do
        $S_{prev} = S$
        $S = Score(Frame_{peak}, Frame_{valley})$
        $Feedback = (S - S_{prev})$
        if $FL - FL_{prev} > \tau$ then
            $FL_{prev} = FL$
            $Offset_{fl} = Feedback * \gamma_{FL}$
            $FL = FL + Offset_{fl}$
            $Camera.ISO = ISO$
        else
            $Offset_{iso} = Feedback * \gamma_{iso}$
            $ISO = ISO + Offset_{iso}$
            $Camera.ISO = ISO$
        end if
    end while
end function
```



(a) Experimental setup (b) Cardiac waves

图 5-2 分别在昏暗和明亮的环境光条件下得出的心搏波的比较

第 6 章 绩效评价

6.1 实验方法论

设备。我们在 iPhone 7 上使用 AVFoundation 框架实现了 CardioCam，该框架提供了各种图像处理和相机配置功能。iPhone 7 配备了 1200 万像素的内置高清后置摄像头，可实现 60f ps 的视频帧速率和 720p/1080p 的分辨率。尽管 iPhone 7 支持 120f ps/240f ps 的慢动作视频录制，但我们选择了 60f ps 的帧速率，这在大多数移动设备上都可以使用，尤其是中低端智能手机。此外，我们还通过调用内置的 AVCaptureDevice.Format 类来以编程方式进一步调整帧速率（即 30/40/50/60f ps）和视频分辨率（即 240/360/480/720p），以测试我们系统的通用性，如第 9.5 节所述。请注意，CardioCam 只调整闪光灯强度和相机 ISO，以更好地捕捉心脏运动模式，而其他相机参数，如焦距、快门速度和白平衡，都被锁定在所提出的系统中。

心脏数据采集。心脏数据集收集自 25 至 33 岁的 25 名参与者（19 名男性和 6 名女性）。特别是，我们构建了一个主数据集，其中包含每个参与者的三条轨迹，每条轨迹持续 60 秒，包括大约 60-75 个心动周期。我们总共从 25 名参与者中收集了 5583 个心动周期样本。在数据收集过程中，参与者的姿势（如站着或坐着）和周围环境（如室内或室外）没有限制。此外，我们进一步构建了四个独立的数据集，涉及 8 名参与者，以研究生物特征变化、不同手指、不同指尖按压位置和情绪状态变化的影响。我们将在第 9.4 节中详细说明数据收集的细节。

验证策略。为了测试我们系统的性能，我们交替地将每个参与者设置为合法用户，其余 24 个参与者充当攻击者。在用户注册过程中，每个合法用户的前 70 个预先收集的心动周期用于 PCA 系数推导和轮廓构建，其余心动周期用于系统验证。**评估指标**。为了评估我们的系统性能，我们定义了五个不同的指标：真阳性率（TPR）和假阳性率（FPR）；平衡精度（BAC）；受试者工作特性曲线；ROC 曲线下面积（AUC）。特别是，TPR 是被正确验证为合法用户的用户的百分比，FPR 是被错误识别为合法用户攻击者的百分比。BAC 是 TPR 和真阴性率（TNR）的等权重组合，即 TNR=1−FPR。ROC 曲线是通过在各种阈值设置（即 η 从 0 到 400）下绘制 TPR 与 FPR 来创建的。AUC 是一种度量验证模型能够在多大程度上区分合法样本和欺骗样本。注意，AUC 通常在 0.5（随机猜测）和 1（完美验证）之间。

6.2 用户验证性能

图 6-1 描述了在每次验证中利用不同数量的心动周期（即 1、3 和 5）验证 25 名参与者的平均 ROC 曲线。具体而言，对于 1 个周期、3 个周期和 5 个周期的验证，每个 ROC 曲线的 AUC 分别计算为 0.958、0.974 和 0.987。很容易发现，5 个心动周期的表现最好。结果证明了 CardiaoCam 在用户验证方面的有效性，即使每个用户只有 3 个心动周期。此外，在图 6-2 中，我们还展示了验证所有 25 名参与者的 BAC。我们可以发现，CardioCam 在 1 个周期、3 个周期和 5 个周期的平均 BAC 分别达到 95.5%、97.9% 和 98.6%，相应的标准偏差（STD）分别为 3.8%、2.7% 和 2.2%。上述结果证实，CardioCam 在验证所有合法用户的同时拒绝对手是高度可靠的。

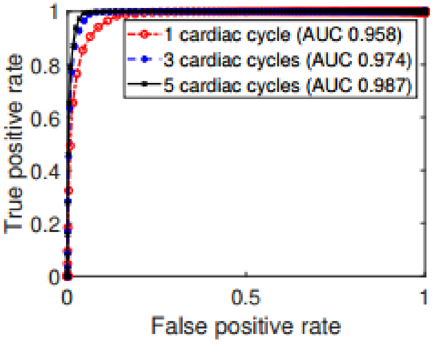


图 6-1 CardioCam 利用来自 25 个用户的心动周期的性能

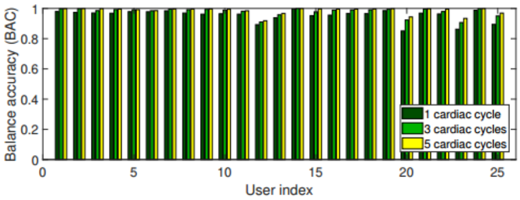


图 6-2 CardioCam 在验证单个用户分别利用 1 个周期、3 个周期和 5 个周期时的性能

第 7 章 讨论

部署可行性。CardioCam 具有最低的硬件要求（即摄像头和手电筒），以便于利用心脏生物特征进行用户验证。具体来说，相机和手电筒在大多数移动设备和物联网设备中都很容易获得，因此不会给移动用户带来额外的成本和不便。此外，如第 9 节所示即使在低帧速率（即 30fps）和低相机分辨率（即 240p）下，CardioCam 系统仍然可以实现 0.953 和 0.98 的高验证精度。因此，我们相信 CardioCam 可以应用于各种需要可靠用户验证的移动和物联网设备。**内存和能量消耗**。我们的系统是一个轻量级的用户验证系统，具有较低的计算复杂度和内存/能量开销。CardioCam 中内存和功耗最高的任务是数据采集，它通过内置摄像头捕捉用户的心脏模式。录制的视频持续 2 秒，仅占用 0.2MB 的内存，相应的功耗低至 4.6J。考虑到捕获的心脏模式，CardioCam 只需约 0.5 秒即可完成一次性用户验证，因为它的设计复杂度低，大多数移动和物联网设备都能负担得起，不会带来太多开销。**身份验证延迟**。与指纹和人脸识别等其他用户验证方案相比，CardioCam 通常需要更长的时间来完成验证过程（即，根据个人心率，至少需要 2.5 秒）。我们进一步发现，很大一部分时间成本用于优化摄像头配置，而不是心脏体征采集。为了降低时间成本，我们将深入研究像素灵敏度与环境光强度之间的关系，以便在心脏体征采集之前完成优化过程。**准确性改进和进一步评估**。虽然目前尚不清楚我们系统中的心脏特征在大量用户中是否足够独特，但我们的结果显示出了希望，至少作为与其他现有技术（如指纹和人脸识别）结合使用的额外信号。

在我们未来的工作中，我们的目标是使用具有不同相机闪光灯设置的各种设备来评估系统的可扩展性，以及更严重的攻击（例如，攻击者可以再现心脏收缩功能）。我们将尝试通过探索移动/物联网硬件的进步来提高验证准确性，例如新兴的多摄像头和视频帧速率（例如 120-240fps）的改进，以及在不同人群中更具歧视性的基准/非基准特征。此外，我们使用具有各种缩小分辨率的视频帧来评估相机分辨率的影响。结果表明，CardioCam 能够抑制帧分辨率的影响，因为 **用欺骗攻击进行 Copping**。最极端的情况是，对手获取合法用户的心搏波（例如，通过脉搏血氧计），并试图通过用半导体光源（例如，红色发光二极管）再生心脏运动模式来欺骗 CardioCam。为了应对这种攻击，我们可以进一步探索不同颜色通道（如绿色和蓝色）的心脏运动模

式，这些通道很难用单色光源伪造。我们将把对此类对抗性案件的详细研究作为我们未来工作的一个途径 **心脏病下的稳健性**。目前，我们的工作主要集中在验证健康人的身份，没有心律失常和先天性心力衰竭等心脏病的患者。但心脏异常可能会对心脏运动模式产生相当大的影响，从而影响心脏生物特征的稳定性。未来，我们计划将 CardioCam 应用于心血管疾病患者，并开发更通用的用户验证机制。

结 论

在本文中，我们提出了 CardioCam，这是第一个低成本、通用且难以伪造的基于心脏生物特征的用户验证系统。与现有的用户验证系统不同，CardioCam 利用移动设备和物联网设备中现成的内置摄像头，提取独特的心脏生物特征来验证用户的身份。为了实现高度可靠的心脏运动推导，我们设计了一种基于梯度的相机配置优化技术，以及动态像素选择，以减轻不断变化的环境光和指尖触摸压力/位置的影响。为了实现高度可靠的心脏运动推导，我们设计了一种基于梯度的相机配置优化技术，以及动态像素选择，以减轻不断变化的环境光和指尖触摸压力/位置的影响。为了便于准确的用户验证，CardioCam 考虑了两种类型的生物特征，形态特征和非基准特征。通过涉及 25 名受试者的大量实验，实现了一个原型系统来评估 CardioCam 的性能。结果表明，在各种摄像头设置和数据采集模式下，CardioCam 可以在验证合法用户的同时拒绝未经授权的用户，从而实现显著的准确性和稳健性。

参考文献

[1] Wiedenbeck S, Waters J, Birget J C, et al. Authentication using graphical passwords: Effects of tolerance and image choice[C]//Proceedings of the 1st Symposium on Usable Privacy and Security, SOUPS 2005, Pittsburgh, Pennsylvania, USA, July 6-8, 2005. 2005.

[2] Wu T S, Lee M L, Lin H Y, et al. Shoulder-surfing-proof graphical password authentication scheme [J]. International Journal of Information Security, 2014, 13(3): 245-254.

[3] M. E. Smudge attacks on smartphone touch screens[C]//Usenix Conference on Offensive Technologies. 2010.

[4] Arakala A, Jeffers J, Horadam K J. Fuzzy Extractors for Minutiae-Based Fingerprint Authentication [C]//Advances in Biometrics, International Conference, ICB 2007, Seoul, Korea, August 27-29, 2007, Proceedings. 2007.

[5] Maltoni D, Maio D, Jain A K, et al. Fingerprint Sensing[J]., 2022.

[6] Santosham S, Lindsey D. Connected women 2015 - bridging the gender gap: mobile access and usage in low and middle income countries[J].,

[7] Kumar A. CREATING RICH EXPERIENCES IN MAIL THROUGH ATTACHMENTS[Z]. 2012.

[8] Aditi, Roy, Nasir, et al. MasterPrint: Exploring the Vulnerability of Partial Fingerprint-Based Authentication Systems[J]. IEEE Transactions on Information Forensics and Security, 2017.

[9] Arteaga-Falconi J S, Osman H A, Saddik A E. ECG Authentication for Mobile Devices[J]. IEEE Transactions on Instrumentation & Measurement, 2016, 65(3): 591-600.

[10] Bonissi A, Labati R D, Perico L, et al. A preliminary study on continuous authentication methods for photoplethysmographic biometrics[C]//2013 IEEE Workshop on Biometric Measurements and Systems for Security and Medical Applications. 2013.

[11] Re?It Kavsao?Lu A, Polat K, Recep Bozkurt M. A novel feature ranking algorithm for biometric recognition with PPG signals[J]. Computers in Biology and Medicine, 2014, 49: 1-14.

[12] Safie S I, Soraghan J J, Petropoulakis L. Electrocardiogram (ECG) Biometric Authentication Using Pulse Active Ratio (PAR)[J]. IEEE Transactions on Information Forensics & Security, 2011, 6(4): 1315-1322.

[13] Feng L, Chen S, Yan Z, et al. Cardiac Scan: A Non-contact and Continuous Heart-based User Authentication System[C]//the 23rd Annual International Conference. 2017.

[14] Matsumura K, Yamakoshi T. iPhysioMeter: A new approach for measuring heart rate and normalized pulse volume using only a smartphone[J]. Behavior Research Methods, 2013, 45(4): 1272-1278.

[15] Kurylyak Y, Lamonaca F, Grimaldi D. Smartphone-Based Photoplethysmogram Measurement[M]. Digital Image, Signal, 2012.

[16] Miyuki, Kono, Hironori, et al. Near-infrared finger vein patterns for personal identification.[J]. Applied optics, 2002.

[17] Miura N, Nagasaka A, Miyatake T. Feature extraction of finger-vein patterns based on repeated line tracking and its application to personal identification[J]. Systems & Computers in Japan, 2004, 35(7): 61-71.