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

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%.

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 [24, 45], which suffer from various attacks including password theft, shoulder surfing [46] and smudge attacks [7]. Biometric-based user verification opens up a new pathway to secure mobile devices, especially fingerprint-based solutions [5, 26], 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 [39]. 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 [30]. Moreover, fingerprint-based solutions are vulnerable to synthetic fingerprints created through victims' photographs [12, 35, 41]. 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 [6, 21, 36, 10] or Doppler radar [25] is 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

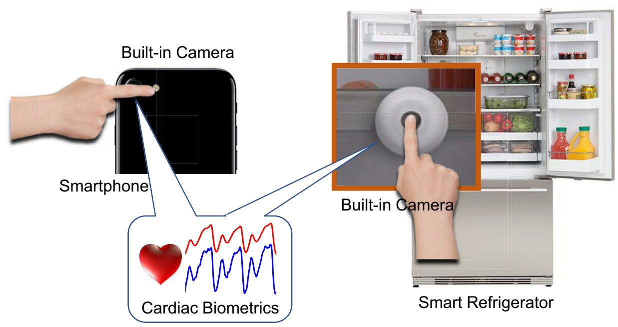


Figure 1: Enabling cardiac-pattern based user verification using device's built-in camera.

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 [27, 44], but 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 [37] 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 [34], 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 [23], facial features [13] and palm print [40]. 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 [42]. The TrueDepth camera in iPhone X can capture the geometry and depth of the user's face [16] to verify user's identity. It however requires high-end and expensive cameras and also could be easily spoofed by the fabricated $3D$ synthetic mask [14]. 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 [48, 1, 22, 28]. 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) [20] 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

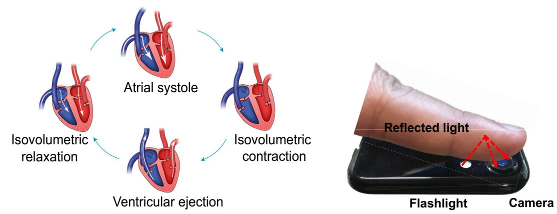
lights on the built-in camera when the user presses her/his fingertip upon.

- 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 [24] or graphic screen patterns [45], 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 [46], and smudge attack [7].

As an alternative, many researchers resort to physiological biometrics to perform user verification. In particular, fingerprint-based solutions [5, 26, 18, 19] have become an essential specification on many premium smartphones such as iPhone and Samsung Galaxy S series. However, such biometrics can be easily compromised by the synthetic artifacts [12, 41], and the fingerprint reader is still unavailable in most of the mid-range and low-end mobile devices. Besides the fingerprints, other human biometric features (e.g., iris [23], face [13], and palmprint [40]) 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 [8]. However, they are usually suffered from spoofing attacks with forged biometrics. For instance, the iris-based user verification system can be deceived by forged contact lens that have the same iris texture as the authorized user [42, 15], and $3D$ masks can also be fabricated through $3D$ printing technologies to spoof facial recognition systems [14]. Additionally, the privacy concerns of such vision-based solutions also 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.



(a) Human cardiac cycle [31] (b) Data collection

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

To overcome the aforementioned weaknesses, some studies rely on intrinsic cardiac biometrics (e.g., heartbeat patterns) derived from electrocardiogram (ECG) [9, 17, 38, 48] and photoplethysmography (PPG) [21] 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 [25] 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.

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.* [27] demonstrate that the heart rate and pulse volume can be measured when the users put their fingertips upon the built-in camera. Additionally, Seismo [44] proposes to derive pulse transit time (PTT) leveraging smartphone accelerometer and built-in camera. Some researchers [11, 43] 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.

3. PRELIMINARIES

3.1 Kinetics of Cardiovascular System

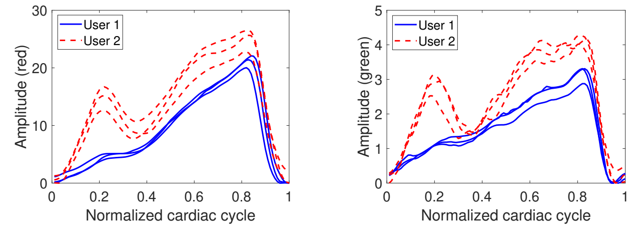
The heart pumps the blood into the vessels through alternative cardiac muscle contraction and relaxation, which forms a periodic heartbeat pattern, called cardiac cycle, while the vessels carry blood circulated throughout the whole body, including the fingertips. The human heart contains four chambers (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 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. The veins in fingertips also belong to the cardiovascular system and exhibit distinct physiological structures among different people. The blood flow passing through the veins in fingertip will result in unique cardiac motion pattern, which has been demonstrated among a large population [32, 48]. 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.



(a) Red channel (b) Green channel

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

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

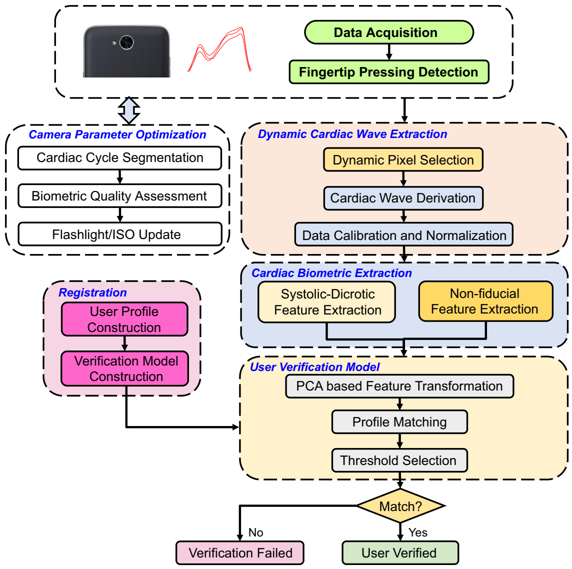


Figure 4: System Overview of CardioCam.

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 camera or adjust finger pressure, aiming to yield similar cardiac biometrics as the legitimate users.

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 devices. As illustrated in Figure 4, *Data Acquisition* is 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 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.

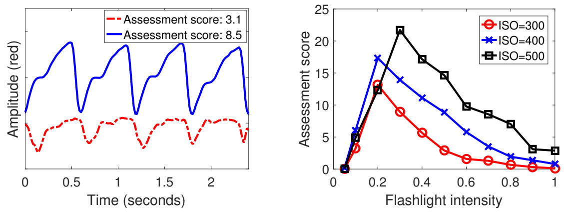
5. FINGERTIP TOUCH DETECTION & CAMERA PARAMETER OPTIMIZATION

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., color of blood) if the camera is fully covered by a fingertip.When the camera is fully covered, the red color show extreme high intensity, otherwise gives relatively low intensity. We thus examine the proportion of red channel component in the overall light intensity across all the pixels (x, y) in each frame $t \in T$ as follows:

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

where $r_{(x,y)}$, $g_{(x,y)}$, $b_{(x,y)}$ denote the light intensity in



(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.

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., τ = 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.

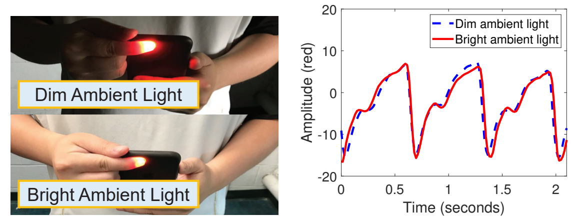
5.2 Camera Parameter Optimization

Our preliminary study finds that the reliable cardiac motion patterns can only be obtained under appropriate camera configurations 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. To capture the cardiac biometrics, it is essential to separate each cardiac cycle for both biometric sensitivity assessment and feature extraction. Since we find that the red channel could capture the most significant response to blood volume changes, we perform cardiac cycle segmentation using the average value of the red channel crossing all the pixels. Particularly, we enable reliable cardiac cycle segmentation by recursively selecting local minimums with a pre-defined threshold along the video stream. 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 max-to-min light intensity difference $Diff(r_{(x,y)})$ in red channel as:

$$Diff(r_{(x,y)}) = Max(\sum_{x,y} r_{(x,y)}(t)) - Min(\sum_{x,y} r_{(x,y)}(t)), \quad (x \in X, y \in Y), \tag{2}$$



(a) Experimental setup

(b) Cardiac waves

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

Then, we indicate the distribution of $Diff(r_{(x,y)})$ with a histogram H with k bins, and then derive the assessment score as below:

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

where $|H_i|$ denotes the number of the pixels falling into ith bin. Figure 5(a) shows the average light intensity in 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 larger average max-to-min difference, 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 $\bigtriangledown S(a_n)$ 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 environment is in two different ambient lighting conditions (i.e., dim and bright ambient light), respectively. As CardioCamera adaptively adjusts the camera flashlight and ISO

Algorithm 1 Video Biometric Optimization

```
function CameraAdjustment
    FL = 0.1, ISO = 550, S_prev = 0, FL_prev
    while S < Threshold do
        FL = Camera.flashlight
        S = Score(Frame_peak, Frame_valley)
        Feedback = (S − S_prev)
        if FL − FL_prev > τ then
            Offset_fl = Feedback ∗ γ_FL
            FL = FL + Offset_fl
            Camera.flashlight = FL
        else
            Offset_iso = Feedback ∗ γ_iso
            ISO = ISO + Offset_iso
            Camera.ISO = ISO
        end if
        S_prev = S
        FL_prev = FL
    end while
end function
```

configuration to complement the ambient 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 ensure the high-quality cardiac motion pattern derivation.

6. DYNAMIC CARDIAC WAVE EXTRACTION

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 ineffective camera pixels for cardiac wave extraction.

Specifically, we first calculate the light intensity average of each frame (e.g., t) in the red channel for peak/valley detection as follows:

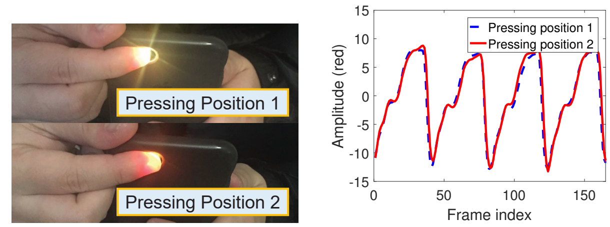
$$P(t) = \frac{\sum_{x,y} r_{(x,y)}(t)}{X \times Y}, \tag{5}$$

and identify the frames with maximum and minimum light intensity average. We then evaluate the pixel sensitivity within each cardiac cycle as Equation 2, and select the effective pixels with a mask matrix, $M^k(x,y)$, defined as follows:

$$M^k(x,y) = \begin{cases} 1, & Diff_r^k(x,y) > \gamma \\ 0, & Diff_r^k(x,y) \le \gamma, \end{cases} \tag{6}$$

where $Diff_r^k(x,y)$ is the max-to-min 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 for pixel selection.

6.2 Cardiac Wave Derivation



(a) Pressing positions (b) Cardiac waves

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

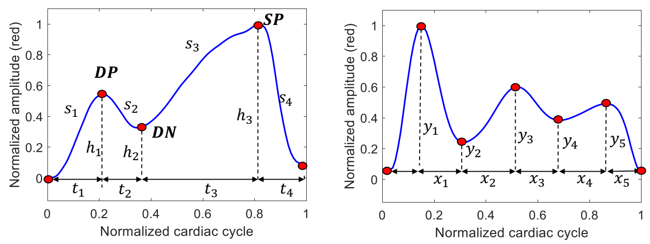
Although blood flow variation can be captured by all sensitive pixels, deriving cardiac measurements from all individual pixels will incur significant computational overhead. Additionally, cardiac motion patterns derived from different camera pixels may exhibit extremely high similarity aross different 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:

$$W_c^k(t) = \frac{\sum_{x,y} M^k(x,y) \times c_{(x,y)}^k(t)}{\sum_{x,y} M^k(x,y)}, \tag{7}$$

where $W_c^k(t)$ and $c_{(x,y)}^k(t)$ 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 7, only the sensitive pixel values are involved in cardiac wave generation through multiplying the pixel matrix by the mask. Figure 7 (a) give 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 from the position changes of fingertip touch.

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 [29] 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 band-pass Butterworth filter [33] 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



(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.

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.

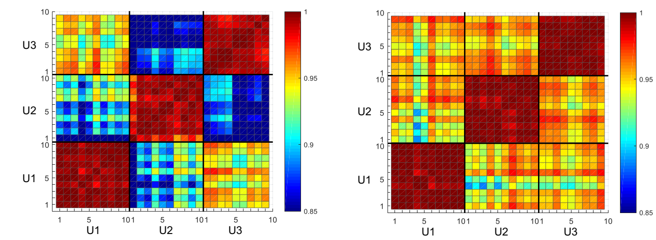
7. BIOMETRIC EXTRACTION

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 [17]. 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 each color channel 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. Specifically, the cardiac waves pass through two high-pass filters with the cut-off 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 $\{x_1, x_3, x_4, |y_1 - y_2|, |y_3 - y_4|, |y5|\}$ are extracted from each color channel of one non-fiducial cardiac wave, so there are 36 non-fiducial features in total. As shown in Figure 9 (b), the high correlation between the non-fiducial features from the same user demonstrates the effectiveness of this 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 [20]. 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

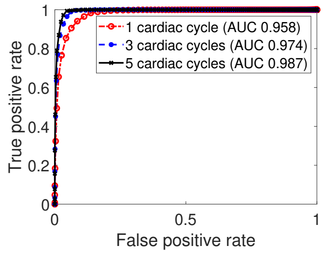


Figure 10: Performance of CardioCam leveraging cardiac cycles from 25 users.

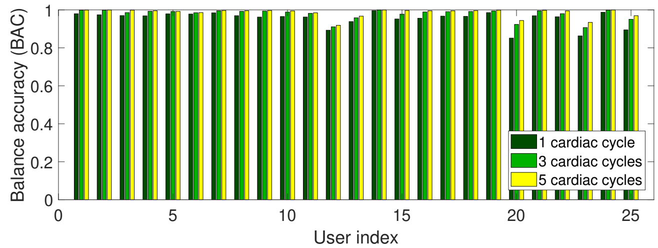


Figure 11: Performance of CardioCam on verifying individual user leveraging 1 cycle, 3 cycles, and 5 cycles, respectively.

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: $argmin\{k|\sum_{j=3}^{k}\frac{w_j}{\sum_{i=1}^{p}w_i} < \tau, k < p\}$, 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. Given the profiled cardiac abstracts as $F = \{f_1, ..., f_n\}$ (i.e., $n = 70$ in our system), 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:

$$Dist(s) = \frac{\sum_{i=1}^{n}\|f_i - s\|}{n}. \tag{8}$$

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 [47], 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: $argmaxJ(\eta_u) = \{\eta_u|\eta_u \in S \land \eta_y \in S : J(\eta_y) \leq J(\eta_u)\}$, where S denotes the set of distances for threshold selection.

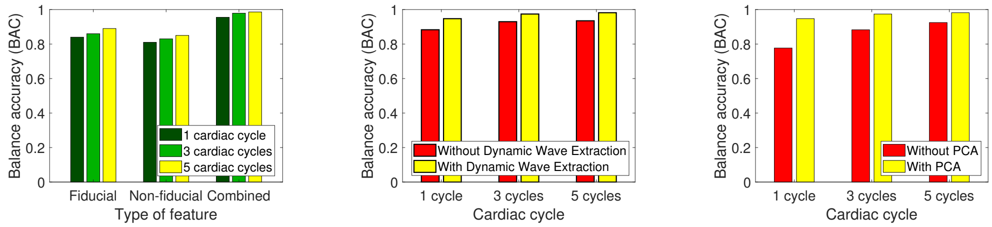
9. PERFORMANCE EVALUATION

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



(a) Three different feature sets

(b) Dynamic cardiac wave extraction

(c) Feature transformation grounded on PCA

Figure 12: Performance of Individual system components.

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 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

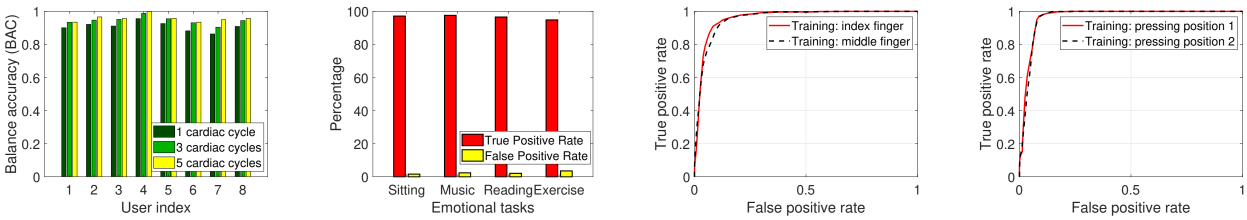
Systolic-Diastolic/non-fiducial Features. To analyze the effectiveness of the extracted systolic-diastolic/non-fiducial features, we evaluate CardioCam under three different feature sets: systolic-diastolic feature only, non-fiducial feature only, and the combined feature set. Figure 12(a) shows BAC 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 helps to achieve better verification performance than that of the non-fiducial feature set. This is because the fiducial features, which describe the four stages of a cardiac cycle, are more unique for each individual than the overall morphology of cardiac wave. Additionally, 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 pat-



(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.

terns 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 70 cardiac cycles from the samples collected on the first day to construct the profile for each of the 8 participants, and then the data collected in the following three months are used for testing. 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.

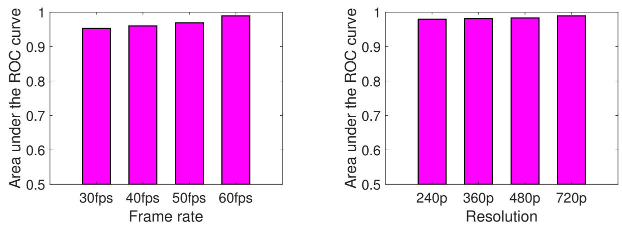
Impacts of Emotion State. We also study the robustness of CardioCam under various human emotional states. We design a set of emotional tasks involving different levels of stress, and each participant is asked to perform two low-stress tasks (i.e., sitting, listening to music) and two high-stress tasks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

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) Impacts of frame rate

(b) Impacts of resolution

Figure 14: Performance evaluation under different video qualities.

(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 configure the camera with different resolutions as 320×240, 640×360, 854×480, 1280×720 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. CardioCam achieves reliable verification accuracy with 99% true positive rate while maintaining the false positive rate as low as 4%. However, 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.

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.

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. While it is not yet clear whether cardiac features are sufficiently distinctive in a large user population, these results show promise, at least as an additional signal used in conjunction with other existing techniques.

12. REFERENCES

[1] F. Agrafioti, J. Gao, and D. Hatzinakos. Heart biometrics: Theory, methods and applications. In *Biometrics*. InTech, 2011.

[2] J. Allen. Photoplethysmography and its application in clinical physiological measurement. *Physiological measurement*, 28(3):R1, 2007.

[3] Amazon. Echo look | hands-free camera and style assistant with alexa, 2018. https://www.amazon.com/Amazon-Echo-Look-Camera-Style-Assistant/dp/B0186JAEWK.

[4] Amazon.com. Amazon dash button, official site, 2018. https://www.amazon.com/Amazon-JK29LP-Tide-Dash-Button/dp/B0187TMRYM.

[5] A. Arakala, J. Jeffers, and K. J. Horadam. Fuzzy extractors for minutiae-based fingerprint authentication. In *International Conference on Biometrics (Springer)*, pages 760–769, 2007.

[6] J. S. Arteaga-Falconi, H. Al Osman, and A. El Saddik. Ecg authentication for mobile devices. *IEEE Transactions on Instrumentation and Measurement*, 65(3):591–600, 2016.

[7] A. J. Aviv, K. L. Gibson, E. Mossop, M. Blaze, and J. M. Smith. Smudge attacks on smartphone touch screens. *Woot*, 10:1–7, 2010.

[8] Z. Ba, S. Piao, X. Fu, D. Koutsonikolas, A. Mohaisen, and K. Ren. Abc: Enabling smartphone authentication with built-in camera.

[9] L. Biel, O. Pettersson, L. Philipson, and P. Wide. Ecg analysis: a new approach in human identification. *IEEE Transactions on Instrumentation and Measurement*, 50(3):808–812, 2001.

[10] A. Bonissi, R. D. Labati, L. Perico, R. Sassi, F. Scotti, and L. Sparagino. A preliminary study on continuous authentication methods for photoplethysmographic biometrics. In *Workshop on Biometric Measurements and Systems for Security and Medical Applications (IEEE BIOMS)*, pages 28–33, 2013.

[11] N. Bui, A. Nguyen, P. Nguyen, H. Truong, A. Ashok, T. Dinh, R. Deterding, and T. Vu. 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)*, pages 29–31, 2017.

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

[13] S. Chen, A. Pande, and P. Mohapatra. 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)*, pages 109–122, 2014.

[14] N. Erdogmus and S. Marcel. Spoofing face recognition with 3d masks. *IEEE transactions on information forensics and security*, 9(7):1084–1097, 2014.

[15] P. Gupta, S. Behera, M. Vatsa, and R. Singh. On iris spoofing using print attack. In *2014 22nd international conference on Pattern recognition (ICPR)*, pages 1681–1686. IEEE, 2014.

[16] A. Inc. About face id advanced technology, 2017. https://support.apple.com/en-us/HT208108.

[17] S. A. Israel, J. M. Irvine, A. Cheng, M. D. Wiederhold, and B. K. Wiederhold. Ecg to identify individuals. *Pattern recognition*, 38(1):133–142, 2005.

[18] A. K. Jain, L. Hong, S. Pankanti, and R. Bolle. An identity-authentication system using fingerprints. *Proceedings of the IEEE*, 85(9):1365–1388, 1997.

[19] T.-Y. Jea and V. Govindaraju. A minutia-based partial fingerprint recognition system. *Pattern Recognition*, 38(10):1672–1684, 2005.

[20] I. T. Jolliffe. Principal component analysis and factor analysis. In *Principal component analysis*, pages 115–128. Springer, 1986.

[21] A. R. Kavsaoğlu, K. Polat, and M. R. Bozkurt. A novel feature ranking algorithm for biometric recognition with ppg signals. *Computers in biology and medicine (Elsevier)*, 49:1–14, 2014.

[22] M. Kono, H. Ueki, and S.-i. Umemura. Near-infrared finger vein patterns for personal identification. *Applied Optics*, 41(35):7429–7436, 2002.

[23] A. Kumar and A. Passi. Comparison and combination of iris matchers for reliable personal authentication. *Pattern recognition (Elsevier)*, 43(3):1016–1026, 2010.

[24] L. Lamport. Password authentication with insecure communication. *Communications of the ACM*, 24(11):770–772, 1981.

[25] F. Lin, C. Song, Y. Zhuang, W. Xu, C. Li, and K. Ren. 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)*, pages 315–328, 2017.

[26] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar. *Handbook of fingerprint recognition.* Springer Science & Business Media, 2009.

[27] K. Matsumura and T. Yamakoshi. iphysiometer: a new approach for measuring heart rate and normalized pulse volume using only a smartphone. *Behavior research methods*

(Springer), 45(4):1272–1278, 2013.

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

[29] Y. Nam, J. Lee, and K. H. Chon. Respiratory rate estimation from the built-in cameras of smartphones and tablets. *Annals of biomedical engineering (Springer)*, 42(4):885–898, 2014.

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

[31] T. S. Physiologist. The cardiac cycle and cardiac output, 2016. https://thephysiologist.org/study-materials/the-cardiac-cycle-and-cardiac-output/.

[32] C. C. Poon, Y.-T. Zhang, and S.-D. Bao. A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health. *IEEE Communications Magazine*, 44(4):73–81, 2006.

[33] L. R. Rabiner, B. Gold, and C. Yuen. Theory and application of digital signal processing. *IEEE Transactions on Systems, Man, and Cybernetics*, 8(2):146–146, 1978.

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

[35] A. Roy, N. Memon, and A. Ross. Masterprint: exploring the vulnerability of partial fingerprint-based authentication systems. *IEEE Transactions on Information Forensics and Security*, 12(9):2013–2025, 2017.

[36] S. I. Safie, J. J. Soraghan, and L. Petropoulakis. Electrocardiogram (ecg) biometric authentication using pulse active ratio (par). *IEEE Transactions on Information Forensics and Security*, 6(4):1315–1322, 2011.

[37] SAMSUNG. Family hub refrigerator, 2018. https://www.samsung.com/us/explore/family-hub-refrigerator/overview/.

[38] T.-W. Shen, W. Tompkins, and Y. Hu. One-lead ecg for identity verification. In *24th annual conference and the annual fall meeting of the biomedical engineering society (IEEE EMBS)*, volume 1, pages 62–63, 2002.

[39] W. L. Tech. Bridging the gap smartphones in third world countries, 2017. https://womenlovetech.com/bridging-the-gap-smartphones-in-third-world-countries/.

[40] K. Tiwari, C. J. Hwang, and P. Gupta. A palmprint based recognition system for smartphone. In *Future Technologies Conference (IEEE FTC)*, pages 577–586, 2016.

[41] T. Van der Putte and J. Keuning. Biometrical fingerprint recognition: donâĂŹt get your fingers burned. In *Smart Card Research and Advanced Applications (Springer)*, pages 289–303. 2000.

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

[43] E. J. Wang, W. Li, J. Zhu, R. Rana, and S. N. Patel. 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*, pages 2333–2336. IEEE, 2017.

[44] E. J. Wang, J. Zhu, M. Jain, T.-J. Lee, E. Saba, L. Nachman, and S. N. Patel. Seismo: Blood pressure monitoring using built-in smartphone accelerometer and camera. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, page 425. ACM, 2018.

[45] S. Wiedenbeck, J. Waters, J.-C. Birget, A. Brodskiy, and N. Memon. Authentication using graphical passwords: Effects of tolerance and image choice. In *Proceedings of the 2005 symposium on Usable privacy and security (ACM SOUPS)*, pages 1–12, 2005.

[46] T.-S. Wu, M.-L. Lee, H.-Y. Lin, and C.-Y. Wang. Shoulder-surfing-proof graphical password authentication scheme. *International journal of information security*, 13(3):245–254, 2014.

[47] W. J. Youden. Index for rating diagnostic tests. *Cancer*, 3(1):32–35, 1950.

[48] Z. Zhang and D. Wei. A new ecg identification method using bayes' teorem. In *2006 ieee region 10 conference Tencon*, pages 1–4. IEEE, 2006.