Liquid Crystal Mimics Your Heart: A Physical Spoofing Attack Against PPG-Based Systems

Junhao Wang, Li Lu, *Member, IEEE*, Hao Kong, *Member, IEEE*, Feng Lin, *Senior Member, IEEE*, Zhongjie Ba, *Member, IEEE*, and Kui Ren, *Fellow, IEEE*

***Abstract*—Photoplethysmography (PPG) has been extensively employed in commercial and medical products to assess human cardiac activities. However, despite PPG's active role in improving people's daily lives, research on the vulnerabilities of PPG systems is still in its infancy. This paper investigates the feasibility of deceiving PPG sensors in the physical domain. We propose *FakePPG*, which utilizes a low-cost Liquid Crystal Modulator (LCM) device to mimic the PPG signals of a legitimate user, thus deceiving both the PPG-based health assessment and potential authentication applications. To implement *FakePPG* in practical scenarios, we build the attack prototype using commercial off-the-shelf electronic components and further design an automated optimization and attack framework. By leveraging the modified multi-Gaussian model for parameterization, the evolutionary strategy for optimization, and the reference heart rate model for heartbeat variability alignment, *FakePPG* can achieve efficient, flexible, and automated PPG forgery against arbitrary users and heart states. Extensive experimental results show that *FakePPG* can achieve a success rate of 96.7% for Atrial Fibrillation (AFib) spoofing and 91.2% for identity spoofing, respectively, revealing a realistic threat to PPG systems.**

***Index Terms*—Presentation attack, PPG-based authentication, impersonation, liquid crystal.**

I. Introduction

As MOBILE and wearable health monitoring gains popularity, Photoplethysmography (PPG) has seen notable advancements in technology and application. PPG signals have become an essential tool for non-invasive monitoring of vital signs (e.g., heart rate and oxygen saturation) and detection of cardiovascular diseases in modern wearables (e.g., Apple Watch, Samsung Smart Ring) owing to their ability to provide rich and unique physiological information [1], [2]. Moreover, leading vendors are proactively exploring PPG biometric authentication to enhance the security and user experience of their smart devices, as evidenced by their filed patents [3], [4], [5].

Meanwhile, significant security concerns arise as PPG-based systems are becoming closely connected with personal health and data privacy. For instance, attackers will try to bypass the heartbeat biometric-based authentication on wearable devices for unauthorized access to assets and social privacy [6], [7]. Furthermore, leveraging people's trust in PPG health monitoring systems, attackers could initiate crimes (e.g., medical fraud and forensic forgery) and even endanger victims' health and well-being by tampering with the PPG measurement data. Despite these pressing risks, research on the security of PPG technology remains limited, with only a few studies exposing the vulnerabilities in PPG authentication [7], [8], [9].

This paper investigates an undiscovered vulnerability during the PPG measurement and proves the feasibility of manipulating critical data via PPG sensor spoofing. The motivation is twofold. First, although digital-domain attacks can also compromise the PPG systems, they typically rely on exploitable attack surfaces such as root privileges to modify sensor data, which are increasingly difficult to obtain in mainstream products with strengthened security measures. Without such access points, digital intrusions struggle to establish a complete attack route. Second, existing works often assume the malicious PPG signals can be directly fed into the target systems to launch attacks [7], [8], while none have provided a clear and feasible way. In contrast, our work aims to realize PPG sensor spoofing attacks in the physical domain, allowing realistic fake signals to mislead the PPG systems into incorrect decisions.

However, unlike traditional biometrics that can be spoofed using simple materials (e.g., facial spoofing with printed photos [10]), PPG sensor spoofing is still challenging due to the complex physiological mechanisms and dynamic patterns of PPG signals. To this end, we propose FakePPG, a novel attack vector that can impersonate an arbitrary target's PPG signals in different heart health states. FakePPG is achieved with the help of a dedicated attack device and an efficient attack framework. 1) *Attack Device*: Through preliminary studies, we identified a vulnerability in PPG measurement: the intensity of probing light can be manipulated via specialized optical means, i.e., a liquid crystal optical modulator (LCM) with dynamically adjustable transmittance. Leveraging this finding, we developed an LCM-based attack device using

Received 21 December 2024; revised 29 June 2025 and 28 July 2025; accepted 10 August 2025. Date of publication 13 August 2025; date of current version 20 August 2025. This work was supported in part by the Zhejiang Provincial Natural Science Foundation of China under Grant LY24F020007 and Grant LD24F020010; in part by the Key Research and Development Programme of Zhejiang Province under Grant 2025C02264; in part by the National Natural Science Foundation of China under Grant 62102354, Grant 62402302, Grant 62372406, Grant 62172359, and Grant 62032021; and in part by the National Key Research and Development Program of China under Grant 2023YFB3107402. The associate editor coordinating the review of this article and approving it for publication was Dr. Haoliang Li. *(Corresponding author: Li Lu.)*

This work involved human subjects or animals in its research. Approval of all ethical and experimental procedures and protocols was granted by the Institutional Review Board of Zhejiang University.

Junhao Wang, Li Lu, Feng Lin, Zhongjie Ba, and Kui Ren are with the State Key Laboratory of Blockchain and Data Security, School of Cyber Science and Technology, and College of Computer Science and Technology, Zhejiang University, Hangzhou 310027, China, and also with Hangzhou High-Tech Zone (Binjiang) Institute of Blockchain and Data Security, Hangzhou 310027, China (e-mail: wangjunhao@zju.edu.cn; li.lu@zju.edu.cn; flin@zju.edu.cn; zhongjieba@zju.edu.cn; kuiren@zju.edu.cn).

Hao Kong is with the School of Computer Engineering and Science, Shanghai University, Shanghai 200444, China (e-mail: haokong@shu.edu.cn).

Digital Object Identifier 10.1109/TIFS.2025.3598472

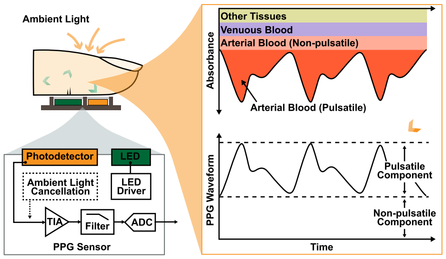


Fig. 1. Illustration of the PPG measurement principle using a reflective type PPG sensor and the corresponding PPG waveforms.

only low-cost, off-the-shelf electronic components. 2) *Attack Framework*: We developed an automated optimization and attack framework to facilitate the forgery of PPG signals. Given the victim's PPG pulse waveform, the framework utilizes a modified multi-Gaussian model for efficient and flexible parameterization of the digital voltage signals. Then, an evolutionary strategy is employed to search for the optimal control parameters automatically. Finally, the voltage signal is calibrated to align its heartbeat variability with that of either atrial fibrillation (AFib) patients or healthy individuals, thus enabling the mimicry of PPG signals in various heart conditions.

FakePPG not only reveals the vulnerability of PPG-based healthcare and authentication systems on wearables but also brings insights on enhancing the security of PPG applications in the future. In summary, our contributions are as follows:

- To the best of our knowledge, FakePPG is the first feasible and low-cost PPG sensor spoofing attack.
- We propose a spoofing method applicable to various PPG sensors using a liquid crystal modulator and validate the feasibility of optical modulator-based attacks.
- We implement FakePPG with an attack device comprising low-cost off-the-shelf components, and we further design an automated optimization and attack framework to enable flexible and efficient PPG signal forgery.
- The extensive experiments, involving a total of 36 subjects and three commercial PPG sensors, have shown the effectiveness of FakePPG under various realistic conditions, achieving an attack success rate of 96.7% for AFib spoofing and 91.2% for identity spoofing. Additionally, we demonstrate its feasibility in deceiving the PPG heart health functions of various real-world products.

II. Background and Related Works

A. Fundamentals of PPG

Photoplethysmography (PPG) is an optical method to noninvasively detect blood volume changes in the skin's microvascular bed. The measured PPG signal describes the activities of the human cardiovascular system during heartbeats, thus containing rich heart-related information.

1) Measurement Principle: The PPG sensor comprises Light-Emitting Diodes (LEDs), photodetectors (PDs), and other components for front-end processing. As shown in Fig. 1, it is placed in contact with the human skin during the measurement. A light beam from the LED shines through the skin, which is absorbed, reflected, and scattered by the skin structure (e.g., tissues, veins, and arteries). Finally, the photodetector detects the transmitted or reflected light intensity and converts it into digital signals at fixed sampling rates, i.e., $Y(t) = \mathcal{H}(I(t))$. Ideally, considering human skin is composed of different layers of light-absorbing substances with extinction coefficient ε_i, concentration c_i, and optical path length l_i, the attenuation of light passing through the skin can be expressed by Beer-Lambert Law [11],

$$I(t) = I_0 A(t) = I_0 e^{\sum -\varepsilon_\text{i} c_\text{i} l_\text{i}}, \tag{1}$$

where I_0 is the irradiated light intensity, and $A(t)$ is the overall light absorbance of human skin. As illustrated in Fig. 1, the ultimate PPG signal is determined by the combined effects of non-pulsating factors like basic blood volume and hemoglobin concentration in the tissue, and the pulsating factors such as artery blood volume changes due to heartbeat.

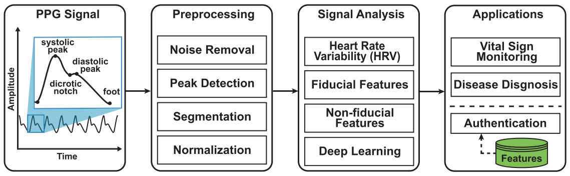


Fig. 2. Illustration of a typical workflow of PPG systems.

2) Signal Preprocessing: The PPG data acquisition is affected by various noises, such as low-frequency noises caused by body motions, respiration, and temperature changes, and high-frequency noises induced by electromagnetic interference and sensor defects [12], [13]. Hence, noise removal is indispensable to enhance the reliability of PPG applications. Typically, a bandpass filter can eliminate the noise while retaining the most essential information. Next, individual PPG pulses are obtained via segmentation and normalization. Fig. 2 illustrates a single PPG pulse that contains multiple fiducial points (e.g., systolic peak, diastolic peak, and dicrotic notch), which are highly related to cardiac activities.

3) Feature Analysis: By detecting the positions of fiducial points, various physiological parameters, such as inter-beat intervals (IBI) and heart rate variability (HRV), can be calculated to assess the health status. Besides, the waveform of the PPG pulse also reflects distinctive traits of the cardiovascular system. Thus, researchers have employed various methods to extract valuable information from the PPG pulses, including time-domain analysis (e.g., fiducial features), frequency-domain analysis (e.g., Fourier Transform and Wavelet Transform), and deep learning methods.

B. PPG Applications

1) Health Monitoring: Today's wearable devices (e.g., smartwatches, wristbands, and smart rings) are widely integrated with PPG sensors to measure critical heart-related parameters such as heart rate and oxygen saturation (SpO2). Besides, PPG is utilized in the early screening of atrial fibrillation (AFib or AF) [14], which could lead to severe complications such as stroke and heart failure if not received timely treatment [15]. However, professional AFib testing apparatus and procedures are expensive [16] and inconvenient in daily use, while AFib often presents no apparent symptoms, making it easily unnoticed or ignored by patients. Fortunately, wearable PPG technology offers a promising solution for the early and continuous AFib detection. Both Apple Heart Study [17] and Huawei Heart Study [18] have demonstrated the feasibility of detecting AFib using smartwatch PPG signals, leading to a growing favor of this functionality in wearable devices.

2) Information Security: PPG biometrics has been extensively studied recently due to the uniqueness of PPG signals [19], [20], [21], [22]. Unlike those static biometric modalities (e.g., faces and fingerprints) that can be easily compromised with simple materials (e.g., printed photos, gummy fingers), the PPG signal is invisible and dynamically generated via complex cardiovascular activities. Hence, PPG biometric is considered *secure* to enable various security applications. For example, PPG-based authentication can ensure data privacy on wearable devices [20], [23]. Moreover, PPG signals also provide crucial information to enhance other biometric modalities, such as in detecting face spoofing and forgery attacks [22], [24], [25].

C. Security Threats to PPG Systems

Biometric systems are vulnerable to various spoofing attacks [26]. Static human biometrics, like facial recognition, can be fooled by printed photos [27], adversarial images [28], or 3D facial masks [22], while fingerprint and vein recognition can be deceived by fake fingers or materials bearing the same patterns [29], [30]. Moreover, intangible voiceprints are also threatened by voice replay and voice cloning attacks [31], [32], [33], and even dynamic behavioral traits captured by novel sensing modalities face risks of eavesdropping and imitation [34], [35]. However, research on the security of PPG biometric systems remains extremely limited, and no relevant study has been devoted to exploring the security of PPG health systems.

1) Targeting PPG Biometrics: Existing works primarily focus on stealing or restoring the user's PPG signals. For instance, Hinatsu et al. [8] utilized a hidden sensor to achieve stealthy PPG signal recording. In other studies, Li et al. [9] proposed to recover PPG signals from video clips, and Krish et al. [7] employed the generative adversarial network (GAN) to generate PPG signals from other biosignals. However, these studies often make an unrealistic assumption that attackers can access the target PPG system from the digital domain without considering how to make the system accept a malicious PPG signal from the physical world.

2) Targeting Health Monitoring: Unlike those attacks targeting medical devices such as pacemakers [36] or insulin pumps [37] to cause direct interference with medication or normal physiological functions, attacks on PPG health systems mainly produce erroneous measurements of heart-related information. However, such risks should not be overlooked. In the case of AFib detection, wrong health records could lead to the failure of early detection and treatment of serious diseases, and subject healthy individuals to unnecessary examinations. Additionally, tampered health evidence may be exploited in specific scenarios, such as medical fraud and forensic forgery. These scenarios will be discussed in Section III.

TABLE I
SUMMARY OF DIFFERENT ATTACKERS AND MALICIOUS GOALS FOR PPG SENSOR SPOOFING

Attacker Role	Target		Attack Goals				
	AU	HM	👁	👛	🩺	♥	🔨
Strangers	✓	-	●	●	○	○	○
Healthcare Providers	-	✓	○	●	●	○	○
Intimates & Caregivers	✓	✓	●	●	●	●	●
Malicious Users	-	✓	○	○	●	○	●

* HM: **H**ealth **M**onitoring system; AU: **AU**thentication system.
* 👁: Data Privacy 👛: Assets Stealing 🩺: Insurance Fraud ♥: Health Injury 🔨: Forensic Forgery

III. THREAT MODEL

With the popularity of consumer wearables, PPG systems are becoming increasingly connected with personal health and user privacy. An adversary attempts to mislead these systems through sensor spoofing in the physical world, thus bypassing PPG-based authentication or falsifying critical health evidence. Table I summarizes the potential malicious goals, depending on the adversary's role in specific scenarios. Notably, this paper primarily targets PPG systems that utilize green reflective-type PPG sensors to extract heartbeat-related information. The wearable devices, according to a recent market report [38], hold the largest market share of PPG sensors (e.g., 40% held by smartwatches and 30% by smart wristbands). Among them, the green reflective-type sensors dominate this market segment due to their excellent noise resistance in heart rate (variability) measurement [39].

A. Attack Scenarios

1) Attack From Strangers: Wearable devices adopting PPG authentication can be unlocked with the unique pulse signals. However, when the wearable is not worn by users (e.g., charging in a public space), a malicious stranger can approach and inject realistic PPG signals to bypass authentication, enabling unauthorized actions such as stealing personal information and initiating illicit payments.

2) Attack From Malicious Users: Health data from wearables is emerging as court-admissible evidence [40], [41]. This raises the possibility that dishonest users can exploit falsified PPG data to gain unfair advantages in court. For example, a suspect will fabricate heart rate records as alibis, or someone colludes with medical assessors to falsify cardiac health data, thereby securing unjust compensation in personal injury claims.

3) Attack From Healthcare Providers: When PPG devices are employed for initial cardiac disease screening, malicious staff may exploit falsified health readings to deceive victims into undergoing expensive, unnecessary medical examinations. By manipulating the PPG sensor to produce data that supports false diagnoses, such fraud becomes more covert and difficult to detect, especially for victims lacking relevant knowledge.

4) Attack From Intimates: Wearable AFib detection greatly benefits the elderly and patients who need continuous at-home heart health monitoring. However, this could be exploited by malicious intimates or caregivers to carry out covert physical harm to inherit assets or commit insurance fraud [42], [43].

For example, an adversary can falsify PPG readings through sensor spoofing while the victim is asleep, leading to erroneous alarms or concealing detectable AFib symptoms. Such interference may disrupt proper diagnosis and treatment, ultimately causing indirect harm to the victim's health.

B. Assumptions and Attacker Capabilities

1) Victim Devices and Systems: Adversary primarily targets two types of PPG systems on wearable devices: 1) PPG-based authentication, taking several seconds of PPG signal to verify the user's identity, and 2) PPG-based cardiac health monitoring (i.e., AFib detection), which requires a short time measurement (usually within one minute) to assess the heart status. Although PPG authentication has not yet been widely deployed, we still include it in our scope because of its promising future.

2) Physical Accessibility: Attackers attempting to forge PPG records on their own devices face no restrictions on accessing and manipulating the victim devices, with unlimited time to carry out attacks. In other cases, attackers can target moments when devices are not being worn by users (e.g., when left unattended or charging in public places). Such limited opportunities are enough to complete the attack inconspicuously, since the PPG measurement takes no more than a minute. Moreover, if the attacker is an intimate partner of the victim, like a family member or healthcare provider, they will have more chances and legitimate reasons to interact with the victim's device.

3) Integrity of Victim Devices: We assume that victim devices will not be altered at the hardware or software level. Attackers cannot directly inject malicious signals by hijacking circuits or modifying sensor firmware, which could alert users or demand higher expertise; nor can they facilitate the attacks by modifying specific sensor parameters (e.g., LED brightness), which are typically inaccessible on commercial devices. Additionally, attackers are not allowed to supply users with custom-made malicious devices, because wearable devices with health functions are usually regulated (e.g., FDA approval), and devices from unknown sources tend to raise suspicion.

4) Adversary's Knowledge: We assume the adversary is an outsider in cybersecurity but is familiar with wearable devices and PPG applications, and can utilize an out-of-the-box attack device to launch PPG sensor spoofing attacks.

5) Accessibility to Victim's Legitimate PPG Signal: We also assume that the adversary can obtain several seconds of the victim's PPG data in advance as a reference to fabricate fake signals. This is reasonable because healthcare data breaches are very common today [44]. The market for personal health devices is growing rapidly, including some products that are flawed in security and data protection. Moreover, the development of remote PPG (rPPG) technology [9] also enables attackers to extract victims' legitimate PPG signals from video clips, which is stealthy and hard to prevent.

IV. PPG Sensor Spoofing

A. Vulnerability in PPG Measurement

Since PPG sensors detect the variance of light intensity, they are susceptible to ambient light interference. A straightforward way to fabricate PPG signals is *attacking via external light* [45]. However, this approach does not always work in today's commercial PPG sensors. According to our statistics, around 82% of the sensors are equipped with the feature of Ambient Light Cancellation (ALC) [46], allowing them to eliminate the ambient light part from the electrical signal. Hence, the feasibility of external light-based attacks is greatly weakened.

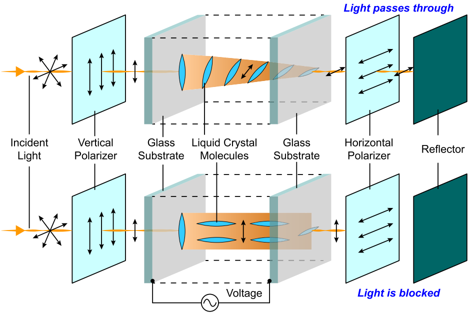


Fig. 3. Schematics of a twisted nematic (TN) liquid crystal cell. It consists of two glass substrates deposited with transparent conducting electrodes, filled with a layer of liquid crystal material. The liquid crystal molecules are generally slender rods, forming a 90-degree twisting helix structure. Besides, polarizers are employed to filter incoming and outgoing light with specific polarization orientations.

Observing this limitation, we turn to a more general method of PPG sensor spoofing, i.e., *attacking via optical modulator*. The optical modulator can modify the properties of light beams (e.g., amplitude, phase, polarization, and propagation paths) [47], which is widely used in photonic applications. In essence, human skin functions like a biological optical modulator in PPG measurement, altering the direction and intensity of light emitted by the LED. However, physically simulating the complexity of human skin and the cardiovascular system inevitably entails high cost and significant technical challenges. Instead, we utilize a relatively simple device, i.e., an electro-optical modulator, to mimic the periodic light absorption exhibited by human skin, thereby inducing fake signals on the PPG sensor.

B. Feasibility Study

The basic idea of falsifying PPG signals is to manipulate the light intensity detected by the photodetector. To implement *optical modulator-based attack*, we employ a Liquid Crystal Modulator (LCM) component, which leverages the properties of liquid crystals in an electric field to regulate light polarization, and finally changes the light intensity passing through it. We further develop a simple LCM-based attack device and verify its feasibility in PPG sensor spoofing.

1) Basis of Liquid Crystal Modulator: The LCM is a thin panel filled with liquid crystal material designed to manipulate the light passing through it. According to the structure and configuration, there are several common types of LCM in the Liquid Crystal Display (LCD) industry, such as Twisted Nematic (TN), In-Plane Switching (IPS), and Vertical Alignment (VA) [48]. In this work, we utilize a TN-type liquid crystal modulator because of its affordability, energy efficiency, and fast response times. Fig. 3 shows its basic structure.

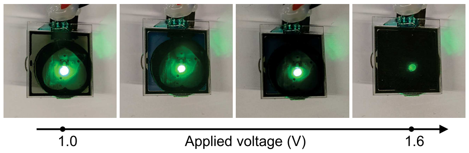
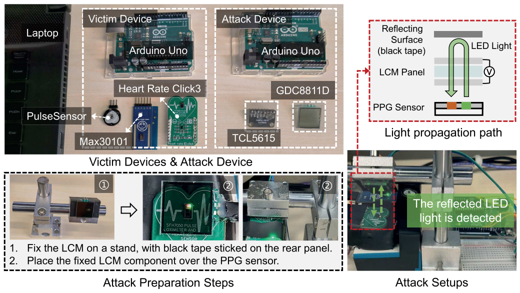


Fig. 4. Demonstration of LCM's light transmission under varying voltages. More light is blocked as the voltage increases.



1. Fix the LCM on a stand, with black tape sticked on the rear panel.
2. Place the fixed LCM component over the PPG sensor.

Fig. 5. Experimental setup for optical modulator-based attack where a small TN-type liquid crystal light valve is utilized to manipulate the PPG signals.

The optical modulation is achieved by changing the alignment of liquid crystal molecules in the electric field. In the absence of an electric field, the polarized light will be rotated by 90° under the guidance of the helical structure, causing its polarization direction to be parallel to the rear polarizer. As depicted in Fig. 3 (top), the incoming light completely passes through the TN cell. Under a sufficient electric field, the liquid crystal molecules realign themselves along the field direction and lose the ability to rotate polarized light. As illustrated in Fig. 3 (bottom), the polarized light is perpendicular to the rear polarizer, thus being entirely blocked.

Beyond switching between transparent and opaque states, the TN-type modulator can also perform more fine-grained light intensity control, as depicted in Fig. 4. When the applied voltage reaches a threshold and continuously increases, there is a continuous and smooth decline of light transmission instead of an abrupt switch. Therefore, the amount of light passing through the TN-type modulator can be precisely controlled by dynamically adjusting the voltage within a specific range.

2) Experimental Setup: We conduct a preliminary experiment to verify the feasibility of LCM-based sensor spoofing.

a) Victim Devices: We choose three commercial PPG sensors as the targets (PulseSensor [49], Max30101 [50], and Heart Rate Click3 [51]). They are wired with Arduino Uno R3 boards [52] for voltage supply and sensor data reading. Max30101 and Click3 have ALC features, albeit with variations in specific implementations.

b) Adversary: The attack device consists of an LCM module (i.e., a small TN-type liquid crystal light valve GDC8811D [53]), an Arduino board, and a TCL5615 [54] chip for converting digital signals from the microcontroller into analog voltage outputs. In addition, we employ a laptop to transmit control signals to the attack device while saving the produced PPG signals in real-time.

c) Attack Settings: As shown in Fig. 5, the LCM component is mounted on a sensor bracket facing the PPG sensor during attacks, enabling the LED light of the PPG sensor to pass through the panel, reflecting on the black electrical tape covering the panel's back and ultimately being received by the photodetector.

3) Results and Analysis: We manually generated a pulsating voltage signal, as illustrated in Fig. 6(a), to drive the LCM. By measuring the LCM's light transmittance-voltage curve, as shown in Fig. 7, we can determine that the valid range of the control voltage signal is around 1.0 to 1.6V. Note that both green light (495 ~ 570nm) and red light (610 ~ 700nm) can be modulated with similar voltage ranges. Under the modulation of LCM, we successfully falsified the PPG signals on three distinct sensors. Fig. 6 illustrates that the waveforms of fake PPG signals are very close to those of genuine human targets, with Pearson distances [55] of merely 0.078 (PulseSensor), 0.116 (Max30101), and 0.022 (Click3), respectively. Similar results were further obtained on a 10-volunteer dataset, with an average distance of 0.039. And we also observe that simple classifiers (e.g., support vector machines) fail to distinguish between fake and genuine PPG segments effectively.

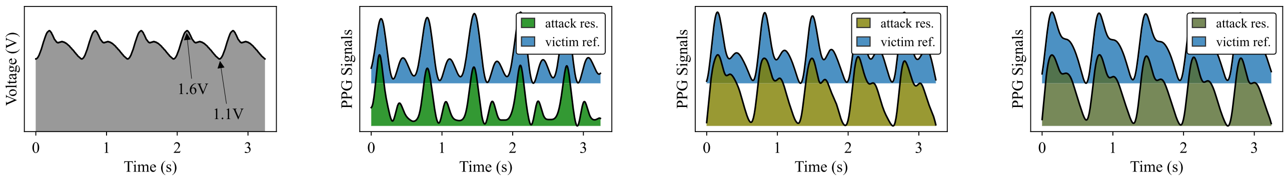
4) Discussion: The experimental results demonstrate the potential of using simple LCMs to deceive PPG sensors (even with ALC functionality). However, LCMs inherently cannot simulate any optical properties of human skin. Human skin modulates light intensity through absorption, scattering, and reflection by tissues and blood, while LCMs regulate transmitted light by filtering polarized light with altered polarization directions, creating a signal-level phenomenon similar to "light absorption." These mechanisms are fundamentally different, yet sufficiently effective for PPG sensors that simply respond to light intensity variations.

However, attacking practical PPG-based authentication and health monitoring systems remains challenging, as it requires the attack device to convincingly mimic both the waveform uniqueness and temporal variability of the natural PPG signals of a specific target. Moreover, the attack must adapt to different scenarios by flexibly generating appropriate control voltages to deceive the downstream algorithms. To this end, we propose an efficient LCM-based attack scheme capable of forging PPG signals for arbitrary users and health conditions.

V. Attack Design

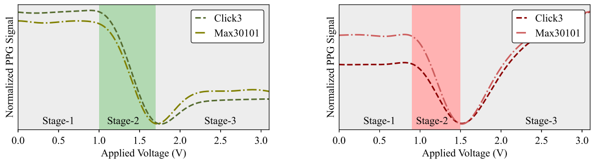
To reveal the potential vulnerabilities of PPG technology, we propose FakePPG, a practical sensor spoofing attack targeting various PPG-based systems. This attack aims to manipulate the light captured by PPG sensors and produce fake signals, ultimately bypassing the PPG authentication or injecting false atrial fibrillation (AFib) detection results of arbitrary targets to achieve various malicious intents. The system overview is illustrated in Fig. 8. To ensure the effectiveness of FakePPG in real-world scenarios, we face the following challenges:

- C1: *How can PPG signals be falsified non-invasively with off-the-shelf electrical components?*
- C2: *How to fabricate realistic PPG signals that mislead heart health algorithms while possessing unique characteristics specific to the target's identity.*
- C3: *How to achieve the attack flexibly and efficiently to adapt to diverse users and scenarios?*



(a) Driving voltage signal (b) PulseSensor Readings (c) Max30101 Readings (d) Click3 Readings

Fig. 6. Illustration of PPG readings on different victim sensors under the modulation of LCM. (a) shows the driving voltage applied to LCM. (b), (c) and (d) show the falsified PPG recordings compared with the target's genuine signals on three sensors, respectively.



(a) Measured on green LED (b) Measured on red LED

Fig. 7. Light transmission in the liquid crystal light valve at different voltages. A smaller PPG signal value means lower transmission.

To address challenge **C1**, we utilize an electronically modulated optical device, i.e., the Liquid Crystal Modulator (LCM), as the core component to construct the attack device. Through dynamically modulating LCM's input voltage, we can simulate the pulsating light absorption of human skin and manipulate the PPG sensor readings. For challenge **C2**, we optimize the voltage cycle based on the target PPG pulse pattern and refine it with the referenced heart rate model. Driven by periodic voltage signals, the attack device can fabricate realistic PPG signals with specific individual patterns and heart health states. For challenge **C3**, we developed an automated optimization and attack framework to search for the optimal attack parameters and control the heart health condition of produced fake PPG signals. Overall, FakePPG can be integrated into a portable attack device, enabling it to *transform* into anyone and mimic their heartbeat, thereby deceiving PPG systems for authentication or health monitoring.

A. PPG Signal Fabrication

The PPG sensor converts the physiological characteristics of the human body into a digital signal representing light intensity, which is mathematically formulated in Equation (1). The adversary aims to simulate the human skin light absorbance with an LCM-based attack device, whose light transmission is related to the applied voltage, i.e., $\tilde{A}(t) = \mathcal{M}(V(t))$, where V is the voltage input, and $\mathcal{M}(\cdot)$ defines the relationship between voltage and light transmission of LCM. Formally, the objective is to find an optimal voltage function to minimize the discrepancy between fake and genuine PPG signals, namely,

$$V^* = \arg\min_{V} \quad \|Y_{\text{ref}}(t) - \mathcal{H}(I_0\mathcal{M}(V(t)))\| \qquad \text{s.t.} \quad V(t) \in [V_1, V_2] \tag{2}$$

where $[V_1, V_2]$ is the valid voltage interval for the LCM component, $Y_{\text{ref}}(t)$ is the genuine PPG signals of a target person. Then, the fake PPG signals can be produced by driving the attack device with the optimal control voltages $V^*(t)$.

1) Task Formulation: Defining the target PPG systems $P_{\text{id}} : \mathcal{Y} \mapsto \mathcal{C}_{\text{id}}$ for authentication and $P_{\text{af}} : \mathcal{Y} \mapsto \{0, 1\}$ for AFib detection, respectively. In the identity spoofing task, the fake PPG signals can deceive the system to output the target's identity, i.e., $P_{\text{id}}(Y^*) = c_{\text{ref}}$. In the AFib spoofing task, the system is misled to output a false health label, i.e., $P_{\text{af}}(Y^*) = c_{\text{af}}$, indicating whether symptoms of atrial fibrillation are detected. Notably, in the AFib spoofing task, the reference PPG data Y_{ref} obtained from the target individual might be associated with a different AFib state from the one an adversary aims to forge. For instance, the PPG data from a healthy person would lack characteristics of AFib symptoms. To address this issue, further refinement on V^* is required to fabricate PPG signals with specific AFib labels, which will be discussed in the subsequent section.

2) Attack Device Construction: The attack device comprises a controller, a Digital-to-Analog Converter (DAC), and the LCM component. The controller automatically optimizes a digital voltage signal $x(t)$, which can be sequentially fed into the DAC and transformed into an analog voltage $V(t)$ that drives the LCM to exhibit pulsating light absorption characteristics. To emphasize portability and affordability, the attack device will be built upon off-the-shelf electronic components. For instance, we can employ a highly integrated System-on-Chip (SoC) as the attack controller and choose the TN-type liquid crystal cells (also called liquid crystal light valves or LCD controllable blackout panels) as the low-cost LCM component. During the attack procedure, the LCM covers the PPG sensor, as shown in Fig. 4, allowing the light passing through it to be received by the photodetector after reflection.

3) Optimization Proxy: In practice, solving Equation (2) may encounter obstacles, as commercial wearables typically do not provide access to raw PPG recordings. This prevents us from determining whether the fabricated PPG signals are sufficiently close to the target. Although query-based black-box optimization can operate with only the binary prediction results [56], [57], applying this method to real-world physical devices is highly constrained and time-consuming. Hence, the optimization is carried out on a proxy PPG system, which may share the same PPG sensor configurations as the target device but provides real-time PPG data output.

B. PPG Pulse Generation

Since PPG signals contain consecutive pulses, the control voltage signal $x(t)$ can also be composed of repeating voltage cycles, with N sample points in each cycle. However,

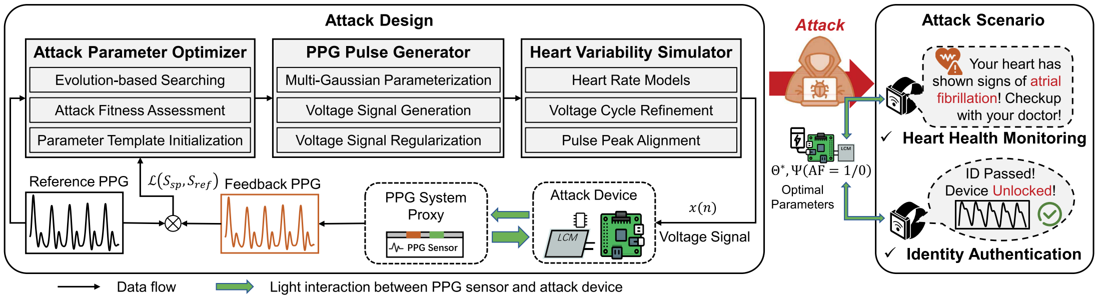
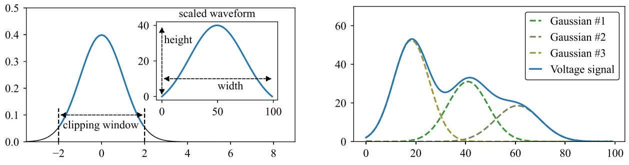

Attack Design
Attack Parameter Optimizer
Evolution-based Searching
Attack Fitness Assessment
Parameter Template Initialization
PPG Pulse Generator
Multi-Gaussian Parameterization
Voltage Signal Generation
Voltage Signal Regularization
Heart Variability Simulator
Heart Rate Models
Voltage Cycle Refinement
Pulse Peak Alignment
Reference PPG
$\mathcal{L}(S_{sp}, S_{ref})$
Feedback PPG
PPG System Proxy
PPG Sensor
Attack Device
LCM
$x(n)$
Voltage Signal
Attack
$\Theta^*, \Psi(\mathrm{AF} = 1/0)$
Optimal Parameters
Attack Scenario
Your heart has shown signs of atrial fibrillation! Checkup with your doctor!
✓ Heart Health Monitoring
ID Passed! Device Unlocked!
✓ Identity Authentication
Data flow
Light interaction between PPG sensor and attack device

Fig. 8. System overview of FakePPG. Three key modules work together with a proxy PPG system to optimize the attack device iteratively. Spoofing attacks are then launched to mislead the PPG-based algorithms on the target devices.



(a) Single Gaussian component (b) Multiple Gaussian model

Fig. 9. Illustration of voltage cycle parameterization.

directly parameterizing the N-sample voltage cycle will cause a combinatorial explosion. Hence, we need a method that can efficiently represent $x(t)$ with a limited number of parameters Θ to reduce the problem's complexity.

1) Voltage Cycle Parameterization: Researchers in the field of PPG signal analysis have introduced a dynamical model [58] where the PPG pulse is basically a sum of different Gaussian functions. Inspired by this, we employ a modified multi-Gaussian model to parameterize the voltage cycle flexibly and efficiently. As shown in Fig. 9, each Gaussian component is constructed through a clipping-scaling method. Given the standard Gaussian function $g(t) = \frac{1}{\sqrt{2\pi}} \exp\left(-t^2/2\right)$, we first clip the segment between $[-c_i, +c_i]$ and then apply min-max normalization as well as shift transformation to obtain the component basis, i.e.,

$$g_i'(t) = \begin{cases} \dfrac{g(t - c_i) - g(c_i)}{g(0) - g(c_i)}, & \text{for } t \in [0, 2c_i] \\ 0, & \text{for } \textit{otherwise} \end{cases} \tag{3}$$

Then, we apply temporal and amplitude scaling so that the scaled component has a width of w_i and a height of h_i. At the same time, for the convenience of subsequent implementation, we discretize the i^{th} component in advance:

$$\phi_i(n; \theta_i) = h_i g_i' \left(t = \frac{2c_i}{w_i} n \right), \tag{4}$$

where $\theta_i = \{h_i, w_i, c_i\}$ is used to define the component shape, and $w_i, h_i \in N^+$. The width w_i also represents the number of sample points. Finally, the voltage cycle is the summation of multiple components:

$$\phi(n) = \phi(n; \Theta) = \sum_{i \in \mathcal{I}} \phi_i(n - p_i; \theta_i), \tag{5}$$

where $p_i \in N^+$ is the offset of component ϕ_i. The overall control parameters Θ are therefore defined as $\{(\theta_i, p_i)\}_{i \in \mathcal{I}}$.

2) Voltage Signal Generation: Assuming that the discrete voltage signal $x(n)$ contains K identical and equally spaced cycles, it can be expressed as:

$$x(n) = \sum_{k=1}^{K} \phi_k(n) = \sum_{k=1}^{K} \phi(n - kN_t), \tag{6}$$

where N_t is the voltage cycle interval in terms of sampling points. To match the target's heartbeat interval, the duration of the voltage cycle is the same as one PPG cycle. Specifically, assuming the voltage signal transmitted at a rate of f_t samples per second and the PPG cycle duration T, we have $N_t = f_t T$, where T can be estimated by applying peak detection and calculating the average peak-to-peak interval.

3) Regularization and Transmission: Since the effective voltage of LCM lies in $[V_1, V_2]$, the voltage signal $x(n)$ should be regulated to the corresponding range by adding a base offset ΔV and truncating out-of-range values. The regulated voltage signal will be transmitted to the DAC module to dynamically adjust the light transmission of the LCM module, ultimately causing synchronous changes in the PPG sensor readings. Meanwhile, the spoofing PPG signals Y_{sp} produced on the proxy PPG system are further received and stored as feedback for attack optimization.

C. Attack Parameter Optimization

Based on our voltage signal model, optimizing the voltage function V^* is transformed into searching for the optimal control parameters Θ^*. To facilitate this process, we implement an evolutionary strategy-based optimization framework [59] to iteratively update and evaluate parameters until the produced fake PPG signal is sufficiently close to the reference signal. Specifically, it includes the following steps:

1) Initialize a population of candidate solutions, each representing a possible combination of control parameters. Perform an initial attack assessment with the fitness function for each candidate solution.
2) Select the candidates with better attack effectiveness as parents. To avoid a local optimum, there is a chance τ of random selection.
3) Apply mutation to the selected candidates to generate offspring, i.e., generate a neighboring candidate with only one of the parameters Θ being changed.
4) Perform attack assessment for the offspring and replace the least effective candidate in the population.

5) Repeat the steps from 2) to 4) until reaching a maximum number of iterations.

1) Fitness Assessment: To assess the performance of candidate attack parameters, we utilize a distance-based fitness function to measure the deviation between the spoofing PPG signals and the reference signals. We segment the spoofing and reference PPG signals into individual PPG cycles and calculating their average cycle vectors, S_{sp} and S_{ref} respectively, the fitness score is calculated as the mean square error (MSE) of them: $\mathcal{L}(S_{sp}, S_{ref}) = \frac{1}{N_r}\|S_{sp} - S_{ref}\|^2$. The cycle vectors are all min-max normalized, each with $N_r = T \cdot f_r$ sample points.

2) Parameter Template: In our approach, initializing the population is crucial for finding the optimal parameters. Therefore, we build parameter templates containing three Gaussian components and generate the initial population through mutation operations. To determine the initial offsets of individual components, we detect the fiducial points (i.e., systolic peak, dicrotic notch, and diastolic peak) of the reference PPG signal and then calculate their centers through K-means clustering. Other parameters are empirically initialized.

D. Heart Variability Simulation

Heart rate variability (HRV), referring to the variation in time intervals between consecutive heartbeats, is the most critical feature in determining whether the target's heart is healthy, particularly for atrial fibrillation (AFib) detection. For example, the HRV features of healthy persons usually exhibit stable peak intervals, while patients show abnormal fluctuation in the intervals and amplitudes of PPG pulses.

To deceive the AFib detection systems, the HRV patterns in PPG signals should be carefully fabricated into a target heart state (i.e., AF, non-AF). We achieve this by aligning the intervals and amplitudes of voltage cycles with genuine PPG signals from patients or healthy persons. For this purpose, we first construct the reference heart rate models based on public PPG datasets for AFib detection. A reference model describes the relative changes of consecutive peak-to-peak intervals and PPG pulse amplitudes, which can be calculated after peak detection. Then, we adjust the connections of voltage cycles according to the reference heart rate model. The modified k^{th} voltage cycle can be expressed as:

$$\phi'_k(n) = \begin{cases} \alpha_k \phi\left(\frac{1}{\beta_{k-1}}\left(n - n_p\right); \Theta^*\right), & n \le n_p \\ \alpha_k \phi\left(\frac{1}{\beta_k}\left(n - n_p\right); \Theta^*\right), & n > n_p \end{cases} \tag{7}$$

where n_p is the position of the voltage cycle peak, α_i is the relative amplitude of the i^{th} PPG pulse compared to the average peak amplitude, and β_i is the relative peak-to-peak interval between the i^{th} and $(i+1)^{\text{th}}$ PPG pulses. The reference heart rate model $\Psi(\text{AF})_{\text{AF}=0,1}$ is defined as $\{\alpha_i\} \cup \{\beta_i\}$. The ultimate voltage signal is defined as:

$$x'(n) = \sum_{k=1}^{K} \phi'_k(n - \delta_k), \tag{8}$$

where $\delta_k = N_t \cdot \sum_{i=0}^{k-1} \beta_i$ is the corrected position (or offset) of each voltage cycle. Since the voltage cycle peaks usually correspond to the PPG pulse peaks, we can precisely adjust the systolic peak positions of the spoofing PPG signals to exhibit specific HRV characteristics.

VI. Evaluation

Consumer-grade wearables typically do not disclose technical details or permit access to raw PPG data and sensor configuration. Hence, we construct the victim systems using standard commercial PPG sensors and common implementations in the literature. We evaluate the performance of FakePPG in falsifying PPG signals of different individuals and heart health conditions under a controlled laboratory environment, as well as under various crucial impact factors in practical usage. Furthermore, FakePPG is transferred to compromise commercial devices, demonstrating its real-world threats.

A. Experimental Setup

1) Attack Device Construction: The attack device consists of commercial off-the-shelf electronic components, including a Raspberry Pi board [60], a DAC chip TCL5615 (10 bits) [54], and a TN-type liquid crystal light valve GDC8811D [53] in 36 × 36 × 0.5 mm. Such a device is compact (< 10 cm) and portable, making it easy to conceal during attacks.

2) Implementation Details: The raw PPG signal is preprocessed using a 3rd-order Butterworth bandpass filter (0.5 Hz to 8 Hz), with its systolic peaks detected by the Elgendi algorithm [61] via the NeuroKit2 toolbox[1]. Individual PPG cycles are segmented by detecting troughs around each systolic peak and extracting the segments between adjacent troughs, followed by Z-score normalization. During attack optimization, the voltage signal transmission rate f_t and feedback PPG sampling rate f_r are set to 100 Hz. The parameter model consists of 3 Gaussian components with the optimizable parameters constrained as: $c_i \in [1, 5]$, $h_i \in [0, 70]$, and $w_i, p_i \in (0, N_t)$. The evolutionary strategy, based on the Openbox library[2], has a population size of 30, a slight chance of random offspring selection ($\tau = 0.2$), and a maximum of 300 iterations for optimization.

3) Evaluation Tasks: We have set two attack tasks for evaluation: a) *AFib spoofing*. In this task, the attack device generates two types of PPG samples (AF and non-AF) and attempts to make the AFib detection algorithm classify these fake samples as their claimed categories. b) *Identity spoofing*. This task requires the attack device to accurately forge the target's PPG waveform to deceive the identity recognition algorithm, which is more difficult than AFib spoofing.

4) Victim Systems: The AFib detection system extracts 68 HRV features (RMSSD, SDNN, pNN50, etc) from the time and frequency domains of PPG signals with NeuroKit2[1] and adopts a random forest classifier to determine the health status. For identity spoofing, five distinct PPG identification systems are implemented. One is based on the raw waveform of PPG pulses and support vector machines (SVM). Others follow the same structures of previous studies, with one utilizing Discrete

[1]https://github.com/neuropsychology/NeuroKit

[1]https://github.com/PKU-DAIR/open-box

Wavelet Transform (DWT) features and SVM [19], and the remaining adopting different deep learning models: CNN [62], CNN-LSTM [21], and PPG-MobileNet [63], respectively. All of them accept the normalized PPG pulse cycles as input.

5) Datasets: Three datasets are involved in our evaluation:

a) Multi-Sensor PPG Dataset: We collected the fingertip PPG signals from 30 volunteers (including 13 females and 17 males), all of whom are Asian, healthy, and aged between 2030 years. Three commercial sensors with distinct hardware and signal processing characteristics are utilized: PulseSensor (S1), Max30101 (S2), and Heart Rate Click3 (S3). Among them, sensor S3 simultaneously captures PPG signals from both red and green LED channels. The data collection was conducted in a bright and open office environment, where participants were instructed to sit calmly and place their index finger on the sensor positioned on the desktop, while permitted to talk or browse their smartphones. We collected recordings from all three sensors for each participant, with each recording lasting approximately 2 minutes and sampled at 100 Hz. This custom dataset is used to train identity recognition models. Also, segments of around 10 s are randomly extracted as the reference PPG data for attack optimization.

b) PPG-Dalia Dataset: [64]. This public dataset is utilized to enrich the race and skin color diversity among victims. It is initially used for PPG-based heart rate estimation, providing the wrist PPG signals collected from healthy subjects (primarily European) under real-life activities. We select 6 subjects (3 male, 3 female) who have stable PPG signals and extracted their resting-state PPG segments for the identity spoofing task. Each recording lasts 2 minutes and is resampled to 100 Hz, followed by the same signal processing procedures. Similarly, a 10-second segment in each recording was used as the attack reference. Note that the subsequent attack optimization and sensor spoofing experiments are carried out on sensor S3.

c) Mimic PERform Af Dataset: [65]. This public dataset contains PPG signals from healthy individuals and patients during atrial fibrillation. It is utilized to train the AFib detection models and construct reference heart rate models.

6) Attack Procedure: We first utilize the reference PPG signal and the heart rate models to generate the voltage signal. Since the attack occurs when the wearable devices are not being worn by victims (i.e., no human activities or vigorous motions are involved), we position the victim devices (sensors) on the desktop while making the LCM component either fixed on a fixed bracket or handheld by the attacker, maintaining a stable spatial relationship between them, as shown in Fig. 5. The falsified PPG samples are then produced under the modulation of the attack device. Multiple trials are conducted with different attack parameters for identity spoofing, each lasting 5 s to 8 s. For AFib spoofing, attacks are sustained for 30 s to 45 s.

7) Metrics: We use the attack success rate (ASR) to evaluate the performance of FakePPG, which is the ratio of successful attacks to the total number of trials. A successful trial indicates that the fake PPG sample is classified as the claimed category or identity. For identity spoofing, we further define two ASR variants: a) ASR-T = $\frac{1}{M}\sum_{i\in\mathcal{D}}\left(N^{i}_{\text{succ}}/N^{i}_{\text{total}}\right)$, which is the average ratio of successful trials over all the attempts targeting subject-*i*, and b) ASR-S = M_{succ}/M, where M is the number of subjects, M_{succ} is the number of subjects whose identities can be impersonated within 10 trials.

TABLE II

OVERALL ATTACK SUCCESS RATES OF FAKEPPG FOR AFIB SPOOFING (ASR%) AND IDENTITY SPOOFING (ASR-T/ASR-S%)

Task	**Models**	**Multi-Sensor Dataset**			**PPG-DaLia**
		S1	S2	S3	(S3)
AFib Spf.	AF [*]	100.0	94.7	100.0	/
	non-AF [*]	94.0	96.4	94.8	/
	Average	**97.0**	**95.6**	**97.4**	/
ID Spf.	Raw	61.1 / 96.4	59.1 / 78.3	57.9 / 91.7	58.9 / 100.0
	Dwt+SVM	58.9 / 96.4	58.3 / 73.9	57.1 / 91.7	58.9 / 100.0
	CNN	59.6 / 96.4	67.3 / 90.9	58.3 / 88.9	60.7 / 83.3
	CNN-LSTM	58.9 / 100.0	70.9 / 95.7	62.1 / 95.8	50.0 / 100.0
	MobileNet	53.7 / 92.6	54.6 / 90.9	65.6 / 88.9	51.8 / 66.7
	Average	58.5 / **96.4**	62.0 / **85.9**	60.2 / **91.4**	56.1 / **90.0**

[*] Atrial fibrillation detected (AF); Normal Heartbeat (non-AF).

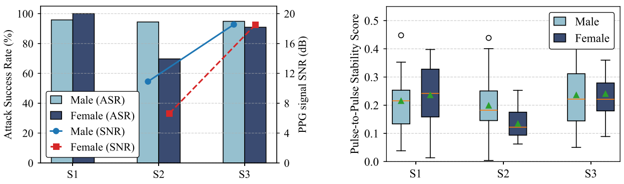
B. Overall Performance

In general, FakePPG has demonstrated impressive capabilities in falsifying PPG signals with diverse waveforms and heart rate variability, posing a significant threat to the decisions of PPG-based systems. As shown in Table II, FakePPG achieves an attack success rate of up to 96.7% in the AFib spoofing task and even 100% when forging PPG signals in the state of atrial fibrillation on S1 and S3. In identity spoofing, approximately 91.2% (ASR-S) of individuals are successfully impersonated, and the deep learning models are more susceptible to attacks (with an average success rate of 93.3%) compared with the machine learning methods utilizing Raw waveforms (88.8%) and DWT features (87.3%). Additionally, the effectiveness of FakePPG is virtually unaffected by the race and skin color of target subjects, achieving a comparable ASR-S on S3 when victim data is from the PPG-DaLiA subset (90.0% vs. 91.4%).

Despite the good performance, the success rate of identity spoofing for single attack attempts is inconsistent, with an overall ASR-T of about 60%. This indicates that our parameter optimization exhibits certain randomness and bias due to various factors, leading to some failed trials. Another interesting finding is that the Max30101 (S2) has the highest ASR-T (62.0%) but the lowest ASR-S (85.9%) in identity spoofing. One contributing factor lies in the lower signal-to-noise ratio (SNR) of S2, which introduces more noise into the measured signals. Another factor is individual variability, particularly the gender difference, which will be studied and discussed in Section VI-C.

C. Impact of Genders

The ASR against females, as shown in Fig. 10(a), is notably lower than that of males (69.70% vs. 94.45%) on sensor S2, while comparable on the other two sensors. This is largely because of the high instability of the female's referenced PPG signal when attacking sensor S2. Since females generally have less blood perfusion in the fingertips, the AC components of their PPG signals (i.e., the pulsatile part reflecting blood volume changes) are much weaker than those of males, and more



(a) Comparison of ASR and SNR (b) Pulse Cycle Stability Analysis

Fig. 10. Impact of the victim genders in identity spoofing.

susceptible to noise interference. This is well demonstrated by the SNR of PPG data collected on S2 (6.65 dB for females vs. 10.91 dB for males). Even with noise reduction, the waveform of the pulse cycles remains unstable for low SNR signals. To verify this, we introduce a new metric to measure the pulse-to-pulse stability: score = $\exp\left(-\frac{1}{\sqrt{n}}\|\mathbf{S}-\overline{\mathbf{S}}\|_2\right)$, where $\|\cdot\|_2$ is the Euclidean norm and $\overline{\mathbf{S}}$ is the average PPG cycle. The results in Fig. 10(b) indicate that the PPG signal stability score of female volunteers (0.135) is much worse than that of males (0.200) on sensor S2. Given that we randomly clip a portion of the victim's PPG signal as the reference in attack optimization, the referenced pulse waveform with greater deviation can result in suboptimal attack parameters and lower attack success rates.

However, exceptions exist for sensors with effective noise suppression. For example, all subjects exhibit high signal SNRs (18.51 dB for females, slightly lower than 18.55 dB for males) and close stability scores (0.241 for females, 0.237 for males) on sensor S3, resulting in comparable ASR between the two groups. This is attributed to the fact that, on high-SNR PPG sensors, noise remains insignificant relative to the signal amplitude for both male and female victims, rendering such gender difference negligible. In practice, sensors with low SNR are uncommon since they will impair the normal functioning of PPG-based systems. Hence, FakePPG can still effectively attack individuals of different genders.

D. Impact of Relative Positions and Motions

During the attack, the attack device's LCM panel is presented in close proximity to the PPG sensors of the victim device to forge PPG signals. Thus, the relative position, especially the angles, may affect the attack performance.

1) Angle: We evaluate the impact of angles on a subset of optimized attack parameters (3 males and 3 females). In evaluation, the LCM component is rotated around two axes (X-axis and Y-axis) in its plane while keeping a distance of 0.5 cm. The attack results on sensor S3 are depicted in Fig. 11(a) and 11(b). We find that as the rotation angle (X-axis in particular) increases, the ASR-S is almost not influenced, while the ASR-T experiences a slight drop but remains above 50%. The impact of angle deviation on FakePPG is relatively minimal with an acceptable angle range within (-60°, 60°). This finding suggests that adversaries do not need to precisely control the angle of the LCM panel relative to the sensor during attacks, significantly reducing the operational difficulty.

2) Distance: The surface housing PPG sensors in wearables may not be flat. Thus, we evaluate the impact of the distance between the LCM panel and the PPG sensor. The results show that ASR-T on all three PPG sensors decreases noticeably as distance increases due to lower signal SNR. Moreover, the effective attack distance varies across sensors, which is 5 cm (S1), 2 cm (S3), and 1 cm (S2), respectively, when keeping the ASR-T above 50%. The sensor characteristics can explain this difference, with S1's attack distance attributed to its highest LED brightness (715 lx). Although FakePPG has a limited attack range, this does not compromise its stealthiness. In addition to the fact that the attacking device is small and easy to conceal, the attack execution is fast (a few seconds). These characteristics ensure that the attack can be conducted discreetly without drawing attention.

3) Motions: To simulate realistic usage scenarios, we evaluated attack scenarios where the attacker holds the LCM component by hand, which could introduce subtle hand movements. The experimental results in Fig. 11(c) show that the hand motion can result in more failed attack attempts, due to the difficulty in eliminating motion artifacts. Compared with the setups where LCM is fixed on a stand, the average ASR-T decreases from 92.78% to 60.41%; however, under multiple attempts, the overall performance (ASR-S) shows only a marginal decline (from 100% to 94.44%). This suggests that FakePPG has robustness against mild motion interference in practical settings.

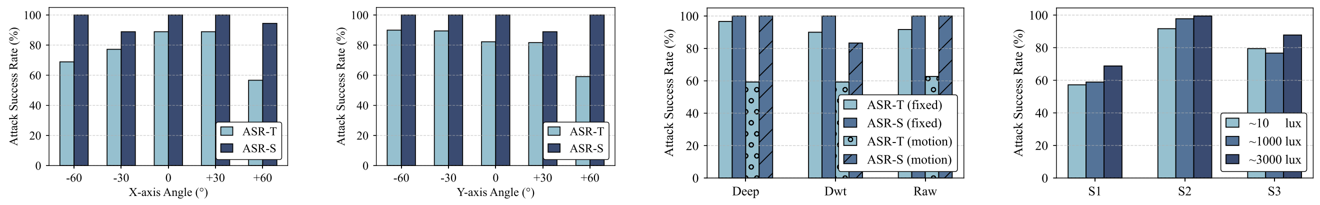
E. Impact of Light Conditions

In this section, we evaluate the impact of ambient light conditions that may interfere with the attack. We conducted the experiments in an office and manipulated the natural light illumination by adjusting the curtains. Since the illumination is not uniform in the room, we mainly ensure the conditions at the desktop where our attack device and PPG sensors are positioned. The ambient illumination intensity is set at three different levels: complete darkness (~10 lx), medium brightness (~1000 lx), and strong brightness (~3000 lx). From the results illustrated in Fig. 11(d), we find that the attack success rate shows an increasing trend as the ambient light intensity increases; conversely, there is a slight drop as ambient light decreases. This is because the PPG sensors suffer from more noise under low light conditions and vice versa in high illumination levels. Overall, even in the worst light condition (< 10 lx), FakePPG can achieve an ASR-T of 57.22% and an ASR-S of 77.78%, indicating that our attack can adapt to most light conditions.

F. Impact of Sensor Configuration

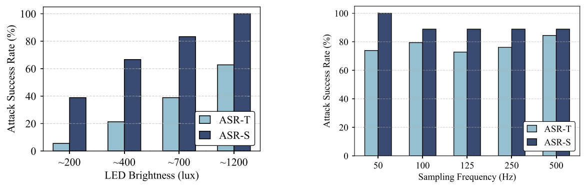
Real-world PPG sensors vary significantly in key parameters (e.g., LED color, brightness, sampling rate). While attackers cannot modify these parameters, manufacturers select different sensor configurations based on business requirements. Therefore, we conducted an in-depth evaluation on whether and how these parameters affect attack effectiveness.

1) LED Brightness: During attack, we set the current of sensor S2 to 6.25, 13, 26 and 50 mA, corresponding to the brightness of about 200, 400, 700 and 1200 lx, respectively. Note that the ambient illumination is around 400 lx–700 lx in our evaluation. To better illustrate the impact of LED brightness, we set the attack distance to 2.0 cm, where the



(a) Impact of X-axis angle (b) Impact of Y-axis angles (c) Impact of hand-held motions (d) Impact of ambient illumination

Fig. 11. Illustration of the impact factors that FakePPG may encounter in real-world scenarios.



(a) LED brightness (b) Sampling frequency

Fig. 12. Impact of PPG sensor configurations.

attack success rate against S2 is low in the default brightness setting. The results in Fig. 12(a) demonstrate that both ASR-T and ASR-S experience a substantial increase as the brightness rises. Particularly, the ASR-S reaches 100% when brightness is at 1200 lx.

This phenomenon can be explained by the underlying principle of photodiodes. According to the theoretical analysis in Appendix A, the SNR of PPG signals is nearly proportional to the square root of perceived light intensity of photodiodes, i.e., SNR $\propto \sqrt{I_p}$. In our attack scenario, with the ambient light and temperature being constant, the light intensity of the internal LED is the dominant factor. As the LED brightness increases, the amount of modulated light returned from LCM also increases, resulting in an improved SNR of the spoofing PPG signal and less deviation from the target signal. This result highlights a dilemma between security and usability for device manufacturers: the efforts to improve PPG signal quality via intensified brightness can facilitate sensor spoofing attacks, while lowering the LED brightness to enhance security will impair the PPG sensor's functionality.

2) LED Color: We evaluated FakePPG on the red channel of sensor S3, using the same settings as green-light experiments. Experimental results show that FakePPG is also effective in falsifying red-light PPG signals. The deep learning baselines are the most vulnerable, with an ASR-S of 87.8%, while the average ASR-S is relatively lower than attacks on green-light sensors (81.8% vs. 91.2%). This difference mainly stems from the red LED light's inherent susceptibility to external interference (e.g., motion artifacts). Even slight hand movements can cause more fluctuations in the red-channel PPG data compared to the green one, thereby affecting the reference waveform for attack optimization. The sensitivity of red light to motion artifacts is also why most wearable devices prefer green-light sensors.

3) Sampling Frequency: Since there is a response time for the LCM panel to adjust the orientation of the liquid crystal molecules under changing voltages, the attack modulation rate is approximately 100 Hz. Besides, due to the limitation of DAC bit-width (10 bits), the modulation of voltage magnitude is also not continuous. Hence, FakePPG might be affected by higher sampling frequencies in PPG measurement. To evaluate this, we utilize sensor S3 to collect falsified PPG signals at 50;100;125;250;500 Hz, respectively. As illustrated in Fig. 12(b), the attack performance is almost not influenced by the sampling frequency. This is because PPG systems typically perform a denoising procedure on the raw PPG signals, thereby eliminating the discrete artifacts caused by the digital control over the attack device.

TABLE III
COMMERCIAL DEVICE ATTACK RESULTS OF FAKEPPG

Devices & Apps	HR	HRV	AFib	Waveform Display
Huawei Watch GT4	✓(5/5)	-	✓(4/5)	-
Apple Watch Series 8	✓(4/5)	✓(3/5)	-	-
Samsung Galaxy 9#	✓(5/5)	-	-	✓
Pulse Oximeter KS-CM01⋆	✓(4/5)	-	-	✓
Heart Health Research†	✓(5/5)	-	✓(5/5)	✓
Cardiio‡	✓(4/5)	-	-	✓

* Attack successfully (✓); Feature not available (-). Tested devices include: two smartwatches from Apple and Huawei, a Samsung smartphone with integrated PPG sensors (#), and a medical-level fingertip pulse oximeter from Heal Force Ltd. (⋆). Two third-party apps: an AFib detection app available on Huawei Watch (†) and a camera-based remote PPG (rPPG) heart monitor on iOS (‡).

G. Attacks on Commercial Devices

We further verify the feasibility of FakePPG on commercial products. Since PPG authentication is not widely deployed, we mainly target their PPG-based heart health features.

1) Victim Devices and Systems: Various PPG-enabled devices are involved, including two popular smartwatches from Apple and Huawei utilizing multiple green LEDs, a Samsung smartphone with a green PPG sensor integrated on the back panel, and a medical-grade pulse oximeter KS-CM01 that employs red/infrared transmissive-type PPG sensors (with LEDs and PD on the opposite sides). We also tested two third-party heart health apps leveraging wearable PPG sensors or smartphone cameras. Table III lists the details of these devices (apps). We aim to compromise their cardiac health functions, including heart rate (HR) estimation, heart rate variability (HRV) assessment, and atrial fibrillation (AFib) detection.

2) Attack Process: The experiments are conducted in a well-illuminated open office environment, and the attack parameters optimized in Section VI-B are randomly selected to control the attack device. For smartwatches, we further

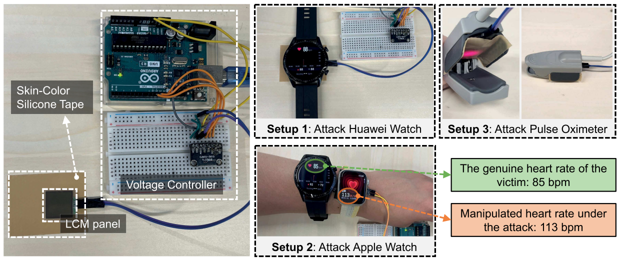

Skin-Color Silicone Tape
Voltage Controller
LCM panel
Setup 1: Attack Huawei Watch
Setup 3: Attack Pulse Oximeter
The genuine heart rate of the victim: 85 bpm
Manipulated heart rate under the attack: 113 bpm
Setup 2: Attack Apple Watch

Fig. 13. Attack setup to spoof commercial devices. To bypass the wrist detection, we could 1) attach skin-colored silicone tape beneath the LCM panel to simulate the light reflection of human skin, or 2) insert the thin and compact LCM panel between the wrist and PPG sensor while wearing it.

employ two empirical techniques, as illustrated in Fig. 13, to bypass the wrist detection, a feature that suspends all system functions when no wrist is detected. When targeting smartphone PPG sensors and cameras, we directly cover them with the LCM panel during spoofing attacks. When attacking the pulse oximeter, we insert the LCM into the cavity structure (between the PD and LED), replacing the position of a finger.

3) Attack Metrics: We use different criteria to evaluate attacks against these health-related systems. When attacking the HR systems, our objective is to cause the device to display specific erroneous heart rate readings. A successful attack requires that the error between the falsified reading and the expected value be below 5%. For HRV and AFib attacks, we try to trigger the device into producing health records or alerts for our desired heart states (e.g., false AFib symptom alerts). For each device (system), if at least one attempt succeeds within five trials, the device (system) is considered successfully compromised.

4) Results and Analysis: As shown in Table III, FakePPG successfully deceived all these commercial devices and systems, achieving overall attack success rates of 90.0% (for HR) and 80.0% (HRV, AFib). And most of the failed trials in attacking HRV or AFib systems were due to stricter wrist-off detection on smartwatches, where PPG signals deviating from normal ranges easily triggered the interruption of ongoing measurements. In those successful attacks, the falsified PPG signals closely resemble authentic PPG waveforms, producing fake heart rate readings with only 2% error from the target values. In addition, we successfully injected both AFib risk and normal heart condition records into the Huawei smartwatch. We also spoofed the transmissive-type pulse oximeter, causing its accompanying software to read fake PPG waveforms and heart rate. Notably, the camera-based PPG systems (i.e., the Cardiio app) also produced similar fake readings even though they extract PPG signals from video streams, indicating FakePPG's threats to the emerging rPPG systems [24], [66]. These experimental results indicate that existing commercial wearables and PPG-based systems lack the mechanisms to ensure the authenticity and integrity of PPG signals, which significantly undermines their reliability and security.

VII. Discussion

FakePPG is a "*presentation attack*" targeting PPG authentication and healthcare systems from the physical domain, which is conceptually similar to presentation attacks against fingerprint and facial recognition [10], [67], while it replicates the dynamic PPG signals with the help of a special optical device (i.e., LCM) and an efficient attack framework. Through extensive experiments, we have demonstrated that FakePPG is universal in falsifying cardiac information on various types of PPG sensors, regardless of their operation mode (reflective or transmissive) and their LED light color (green or red). Note that infrared light (coupled with red light) is not considered since it is used for blood oxygen (SpO2) measurement rather than the heartbeat information we aim to falsify.

Notably, although digital-domain attacks (e.g., malware) can achieve the same goals, they rely primarily on exploitable attack surfaces, such as the root permissions to write or modify PPG sensor data. Due to enhanced security measures and OS-level data protection on mainstream products (e.g., Apple Watch), it is impractical to obtain these exploitable vulnerabilities to form a complete attack path. In contrast, our attack provides a pathway to mislead the physical PPG sensors and then deceive the backend PPG algorithms. Since commercial devices lack mechanisms to verify the authenticity of sensor readings, our attack can easily bypass existing security measures.

A. Limitations

Our attack still has the following limitations: (1) FakePPG is currently incapable of manipulating the measurement of those physiological parameters that require the coordination of multiple LED lights with different wavelengths. For example, it cannot fabricate changes in blood oxygen saturation (SpO2), as doing so would require separately adjusting the absorption profiles of both red and infrared light based on two completely different parameter sets. (2) We didn't consider the PPG signal variations across different measurement sites. If the reference PPG data is collected from a different site (e.g., earlobe) rather than where the target device aims to measure (e.g., wrist and fingertip), the attack optimization would be biased, leading to more failures targeting PPG authentication. Nevertheless, we can achieve mutual conversion of PPG signals from various sites to eliminate this impact. (3) Our attack device, built with simple and low-cost LCM components, exhibits shortcomings in the forgery capability, such as low response frequency to changing voltage and a limited dynamic range of fake PPG signals. We will explore more powerful counterfeiting with specialized equipment in future studies. (4) There is still room for improvement in optimization efficiency and attack success rates. In the future, we shall employ more advanced algorithms to achieve faster and better PPG forgery.

B. Countermeasures

Although FakePPG can realistically simulate the dynamic changes of light intensity like human skin, such attacks could be effectively countered by redesigning the signal processing pipeline of current PPG systems or by integrating additional sensors from other modalities.

1) Artifacts Detection: Due to the adoption of low-cost LCM components with limited optical modulation capabilities, certain artifacts can be identified in the original signals as a

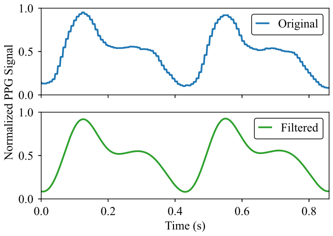


Fig. 14. Illustration of a spoofing PPG signal before and after preprocessing. The attack device adjusts its voltage at 100 Hz, while the PPG sensor S3 measures at 500 Hz. The artifacts are eliminated after denoising (bottom).

spoofing countermeasure. Specifically, since the light transmittance of the LCM changes discretely under the control of the attack device, whereas the modulation of human skin is continuous, it is possible to detect the step-like artifacts using PPG sensors with a sampling rate higher than the voltage regulation speed, as illustrated in Fig. 14. Unfortunately, however, existing PPG systems typically eliminate these artifacts through front-end signal preprocessing. Hence, the detection of spoofing artifacts must be conducted before preprocessing.

To distinguish genuine human signals from attack-generated fake signals, we extract the spectral features (FFT) from PPG signals, as abrupt temporal changes in the time domain induce abnormal high-frequency noises. We further train a dedicated SVM classifier for spoofing detection. Under a high sampling rate (500 Hz), the FFT features from original signals without denoising can achieve a detection accuracy up to 99.3%, while it drops to only 81.9% on filtered signals. The experimental results clearly demonstrate the effectiveness of the artifact-based countermeasure leveraging unprocessed PPG signals.

However, it should be noted that introducing additional detection steps and using higher sampling rates also increases the data processing burden, which is another trade-off that must be considered in the design of wearable devices. Moreover, if attackers adopt more expensive devices with enhanced optical modulation capabilities, the detectable artifacts may diminish, posing greater challenges for reliable spoofing detection.

2) Liveness Detection: Another feasible way is to incorporate supplementary sensing modalities. Spoofing a single sensor is relatively easy for adversaries, while simultaneously deceiving multiple and interrelated sensors in the physical domain is almost impossible. For instance, we can utilize the Inertial Measurement Units (IMU) or temperature sensors, which are common on wearable devices, to capture the subtle movements or temperature changes of the human body during the PPG measurement, thus enabling liveliness detection. In healthcare devices, measuring multiple physiological indicators and analyzing their correlations can also help prevent non-human activities. Although these methods increase system complexity, they significantly raise the cost and difficulty of PPG sensor spoofing attacks.

VIII. Conclusion

In this paper, we investigate the vulnerabilities in PPG measurement and propose FakePPG, a successful sensor spoofing attack against PPG-based authentication and health monitoring systems. FakePPG exploits electro-optical modulation of Liquid Crystal Modulator (LCM) to mimic the light absorption effect of human skin in the physical domain, thus inducing PPG sensors to produce fake signals. To implement it, we develop an attack device based on commercial off-the-shelf electronic components and further design an automated optimization and attack framework to enable flexible and efficient forgery of PPG signals. We have evaluated FakePPG in controlled laboratory settings and commercial wearable devices. The results under various attack settings and conditions have demonstrated the effectiveness of FakePPG in falsifying PPG signals of arbitrary individuals and different heart states, which poses a realistic threat to the data integrity and authenticity of PPG-based systems.

Appendix A
Photodiode Signal-to-Noise Analysis

Suppose the photodiode current consists of the photocurrent I_p induced by light and the dark current I_d. Due to the discrete nature of electrons and photoelectrons [68], the quantum noise (or shot noise) is given by $\sigma_p = \sqrt{2qI_pB}$ and $\sigma_d = \sqrt{2qI_dB}$, where q is the electron charge and B is the noise bandwidth. We further consider the Johnson-Nyquist (or thermal) noise $\sigma_t = \sqrt{4kTB/R_L}$, where k is the Boltzmann constant, T is the absolute temperature, and R_L is the shunt resistance. Since these noises are linearly independent, the total noise can be written as $\sigma = (\sigma_p^2 + \sigma_d^2 + \sigma_t^2)^{\frac{1}{2}}$. Then, the signal-to-noise ratio (SNR) of the electrical signal is defined as:

$$\mathrm{SNR} = 20 \log \left\{ \frac{I_p}{\left[2q(I_p + I_d)B + (4kTB/R_L)\right]^{\frac{1}{2}}} \right\}. \quad (9)$$

According to Equation (9), as the light intensity gets larger (i.e., the current I_p increases), the SNR of the photodiode gradually increases. When the current I_p is much greater than the other noise terms, the SNR becomes approximately proportional to $\sqrt{I_p}$. For PPG sensors, the SNR of the measured signal is primarily affected by ambient light, environmental temperature, and the emitted LED light of the sensor itself.

References

[1] J. Allen, "Photoplethysmography and its application in clinical physiological measurement," *Physiological Meas.*, vol. 28, no. 3, pp. R1–R39, Mar. 2007.

[2] H. W. Loh et al., "Application of photoplethysmography signals for healthcare systems: An in-depth review," *Comput. Methods Programs Biomed.*, vol. 216, Apr. 2022, Art. no. 106677.

[3] H. S. Mousavi and B. Shahsavari, "*User authentication using biometric and motion-related data of a user using a set of sensors*," U.S. Patent 20 230 095 810, Mar. 30, 2023.

[4] J. Jain, V. A. Attarian, S. Sadi, and P. Mistry, "*Real time authentication based on blood flow parameters*," U.S. Patent 11 064 893, Jul. 20, 2021.

[5] S. G. J. Yuen, J. Park, A. Ghoreyshi, and A. Wu, "*User identification via motion and heartbeat waveform data*," U.S. Patent 10 942 579, Mar. 9, 2021.

[6] S. Eberz, N. Paoletti, M. Roeschlin, A. Patani, M. Kwiatkowska, and I. Martinovic, "Broken hearted: How to attack ECG biometrics," in *Proc. Netw. Distrib. Syst. Secur. Symp.*, 2017, pp. 1–15.

[7] V. Krish, N. Paoletti, M. Kazemi, S. Smolka, and A. Rahmati, "Biosignal authentication considered harmful today," in *Proc. 33rd USENIX Secur. Symp. (USENIX Secur.)*, May 2024, pp. 5521–5536.

[8] S. Hinatsu, D. Suzuki, H. Ishizuka, S. Ikeda, and O. Oshiro, "Attack on PPG biometrics: Presentation attack by stealth recording and waveform estimation," in *Proc. 43rd Annu. Int. Conf. IEEE Eng. Med. Biol. Soc. (EMBC)*, Nov. 2021, pp. 64–67.

[9] L. Li, C. Chen, L. Pan, J. Zhang, and Y. Xiang, "Video is all you need: Attacking PPG-based biometric authentication," in *Proc. 15th ACM Workshop Artif. Intell. Secur.*, Nov. 2022, pp. 57–66.

[10] R. Ramachandra and C. Busch, "Presentation attack detection methods for face recognition systems: A comprehensive survey," *ACM Comput. Surveys*, vol. 50, no. 1, pp. 1–37, Jan. 2018.

[11] D. F. Swinehart, "The beer-lambert law," *J. Chem. Educ.*, vol. 39, no. 7, p. 333, 1962.

[12] J. Park, H. S. Seok, S.-S. Kim, and H. Shin, "Photoplethysmogram analysis and applications: An integrative review," *Frontiers Physiol.*, vol. 12, Mar. 2022, Art. no. 808451.

[13] E. Mejía-Mejía, J. Allen, K. Budidha, C. El-Hajj, P. A. Kyriacou, and P. H. Charlton, "Photoplethysmography signal processing and synthesis," in *Photoplethysmography*. Amsterdam, The Netherlands: Elsevier, 2022, pp. 69–146.

[14] K. Bayoumy et al., "Smart wearable devices in cardiovascular care: Where we are and how to move forward," *Nature Rev. Cardiology*, vol. 18, no. 8, pp. 581–599, Aug. 2021.

[15] A. Odutayo, C. X. Wong, A. J. Hsiao, S. Hopewell, D. G. Altman, and C. A. Emdin, "Atrial fibrillation and risks of cardiovascular disease, renal disease, and death: Systematic review and meta-analysis," *BMJ*, vol. 354, p. 4482, Sep. 2016.

[16] N. C. Health, *Electrocardiogram Cost and Procedure Comparison*, 2024. [Online]. Available: https://www.newchoicehealth.com/procedures/electrocardiogram

[17] M. P. Turakhia et al., "Rationale and design of a large-scale, app-based study to identify cardiac arrhythmias using a smartwatch: The apple heart study," *Amer. Heart J.*, vol. 207, pp. 66–75, Jan. 2019.

[18] Y. Guo et al., "Mobile photoplethysmographic technology to detect atrial fibrillation," *J. Amer. College Cardiology*, vol. 74, no. 19, pp. 2365–2375, 2019.

[19] N. Karimian, Z. Guo, M. Tehranipoor, and D. Forte, "Human recognition from photoplethysmography (PPG) based on non-fiducial features," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP)*, Mar. 2017, pp. 4636–4640.

[20] T. Zhao, Y. Wang, J. Liu, Y. Chen, J. Cheng, and J. Yu, "TrueHeart: Continuous authentication on wrist-worn wearables using PPG-based biometrics," in *Proc. IEEE Conf. Comput. Commun. (IEEE INFOCOM)*, Jul. 2020, pp. 30–39.

[21] D. Y. Hwang, B. Taha, D. S. Lee, and D. Hatzinakos, "Evaluation of the time stability and uniqueness in PPG-based biometric system," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 116–130, 2021.

[22] S.-Q. Liu, X. Lan, and P. C. Yuen, "Learning temporal similarity of remote photoplethysmography for fast 3D mask face presentation attack detection," *IEEE Trans. Inf. Forensics Security*, vol. 17, pp. 3195–3210, 2022.

[23] S. Vhaduri and C. Poellabauer, "Multi-modal biometric-based implicit authentication of wearable device users," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 12, pp. 3116–3125, Dec. 2019.

[24] C. Yao, J. Ren, R. Bai, H. Du, J. Liu, and X. Jiang, "Mask attack detection using vascular-weighted motion-robust rPPG signals," *IEEE Trans. Inf. Forensics Security*, vol. 18, pp. 4313–4328, 2023.

[25] Z. Yu, R. Cai, Z. Li, W. Yang, J. Shi, and A. C. Kot, "Benchmarking joint face spoofing and forgery detection with visual and physiological cues," *IEEE Trans. Dependable Secure Comput.*, vol. 21, no. 5, pp. 4327–4342, Sep. 2024.

[26] I. Chingovska, A. R. Dos Anjos, and S. Marcel, "Biometrics evaluation under spoofing attacks," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 12, pp. 2264–2276, Dec. 2014.

[27] D. F. Smith, A. Wiliem, and B. C. Lovell, "Face recognition on consumer devices: Reflections on replay attacks," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 4, pp. 736–745, Apr. 2015.

[28] M. Shen, H. Yu, L. Zhu, K. Xu, Q. Li, and J. Hu, "Effective and robust physical-world attacks on deep learning face recognition systems," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 4063–4077, 2021.

[29] R. Tolosana, M. Gomez-Barrero, C. Busch, and J. Ortega-Garcia, "Biometric presentation attack detection: Beyond the visible spectrum," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 1261–1275, 2020.

[30] A. Krishnan, T. Thomas, and D. Mishra, "Finger vein pulsation-based biometric recognition," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 5034–5044, 2021.

[31] L. Lu et al., "Lip reading-based user authentication through acoustic sensing on smartphones," *IEEE/ACM Trans. Netw.*, vol. 27, no. 1, pp. 447–460, Feb. 2019.

[32] L. Wu, J. Yang, M. Zhou, Y. Chen, and Q. Wang, "LVID: A multimodal biometrics authentication system on smartphones," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 1572–1585, 2020.

[33] K. Wang et al., "From one stolen utterance: Assessing the risks of voice cloning in the AIGC era," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2025, pp. 4663–4681.

[34] T. Zhu, L. Fu, Q. Liu, Z. Lin, Y. Chen, and T. Chen, "One cycle attack: Fool sensor-based personal gait authentication with clustering," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 553–568, 2021.

[35] L. Lu et al., "An imperceptible eavesdropping attack on WiFi sensing systems," *IEEE/ACM Trans. Netw.*, vol. 32, no. 5, pp. 4009–4024, Oct. 2024.

[36] D. Halperin et al., "Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2008, pp. 129–142.

[37] C. Li, A. Raghunathan, and N. K. Jha, "Hijacking an insulin pump: Security attacks and defenses for a diabetes therapy system," in *Proc. IEEE 13th Int. Conf. E-Health Netw., Appl. Services*, Jun. 2011, pp. 150–156.

[38] V. M. Reports, *Photoplethysmography Biosensors Market*, document 366298, 2025. [Online]. Available: https://www.verifiedmarketreports.com/product/photoplethysmography-biosensors-market/

[39] P. H. Charlton and V. Marozas, "Wearable photoplethysmography devices," in *Photoplethysmography*. Amsterdam, The Netherlands: Elsevier, 2022, pp. 401–439.

[40] K. Crawford. (2014). *When Fitbit is the Expert Witness*. [Online]. Available: https://www.theatlantic.com/technology/archive/2014/11/when-fitbit-is-the-expert-witness/382936

[41] G. Goth, *Can Wearables 'Testify' Against Their Owners?—IEEE Spectrum*. [Online]. Available: https://spectrum.ieee.org/wearable-data-court

[42] BBC.(2021). *Anthony Sootheran: 'Brazen' Plot to Steal Millionaire's Fortune*. [Online]. Available: https://www.bbc.com/news/uk-england-oxfordshire-51297285

[43] A. Cavallier. (2024). *Texas Caregiver Faces Murder Charge After a Patient Died-and She Could be Tied to 19 More Deaths*. [Online]. Available: https://uk.news.yahoo.com/texas-caregiver-faces-murder-charge-152945693.html

[44] J. McKeon, "61M Fitbit, Apple users had data exposed in wearable device data breach," Health IT Security, Sep. 2021. Accessed: Aug. 13, 2025. [Online]. Available: https://healthitsecurity.com/news/61m-fitbit-apple-users-had-data-exposed-in-wearable-device-data-breach

[45] J. Speth, N. Vance, P. Flynn, K. W. Bowyer, and A. Czajka, "Digital and physical-world attacks on remote pulse detection," in *Proc. IEEE/CVF Winter Conf. Appl. Comput. Vis. (WACV)*, Jan. 2022, pp. 2795–2804.

[46] J. Kim, T. Lee, J. Kim, and H. Ko, "Ambient light cancellation in photoplethysmogram application using alternating sampling and charge redistribution technique," in *Proc. 37th Annu. Int. Conf. IEEE Eng. Med. Biol. Soc. (EMBC)*, Aug. 2015, pp. 6441–6444.

[47] G. Reed et al., "Optical modulators," in *Integrated Photonics for Data Communication Applications*. Amsterdam, The Netherlands: Elsevier, 2023, pp. 69–121.

[48] P. Yeh and C. Gu, *Optics of Liquid Crystal Displays*, vol. 67. Hoboken, NJ, USA: Wiley, 2009.

[49] World Famous Electron. LLC. (2024). *The Original Pulsesensor Kit*. [Online]. Available: https://pulsesensor.com/products/pulse-sensor-amped

[50] INTEGRATED, MAXIM. (2020). *Max30101 High-sensitivity Pulse Oximeter and Heart-rate Sensor for Wearable Health*. [Online]. Available: https://www.analog.com/media/en/technical-documentation/data-sheets/max30101.pdf

[51] MikroElektronik. (2024). *Heart Rate Click Board*. [Online]. Available: https://www.mikroe.com/heart-rate-click

[52] Arduino. (2024). *Arduino UNO Rev3*. [Online]. Available: https://store.arduino.cc/products/arduino-uno-rev3

[53] Good Display. (2024). *Small Size Light Valve LCD Screen Welding Mask Display GDC8811D*. [Online]. Available: https://www.good-display.com/product/320.html

[54] Texas Instrum. (2024). *10-Bit Digital-to-Analog Converters Datasheet (Rev. E)*. [Online]. Available: https://www.ti.com/lit/ds/symlink/tlc5615.pdf

[55] J. Benesty, J. Chen, Y. Huang, and I. Cohen, "Pearson correlation coefficient," in *Noise Reduction in Speech Processing*. Berlin, Germany: Springer, 2009, pp. 1–4.

[56] A. Ilyas, L. Engstrom, A. Athalye, and J. Lin, "Black-box adversarial attacks with limited queries and information," in *Proc. 35th Int. Conf. Mach. Learn.*, 2018, pp. 2137–2146.

[57] C. Guo, J. Gardner, Y. You, A. G. Wilson, and K. Weinberger, "Simple black-box adversarial attacks," in *Proc. Int. Conf. Mach. Learn.*, 2019, pp. 2484–2493.

[58] A. Sarkar, A. L. Abbott, and Z. Doerzaph, "Biometric authentication using photoplethysmography signals," in *Proc. IEEE 8th Int. Conf. Biometrics Theory, Appl. Syst. (BTAS)*, Sep. 2016, pp. 1–7.

[59] T. Bäck and H.-P. Schwefel, "An overview of evolutionary algorithms for parameter optimization," *Evol. Comput.*, vol. 1, no. 1, pp. 1–23, Mar. 1993.

[60] Raspberry. (2024). *Raspberry PI 4 Model B*. [Online]. Available: https://www.raspberrypi.com/products/raspberry-pi-4-model-b/

[61] M. Elgendi, I. Norton, M. Brearley, D. Abbott, and D. Schuurmans, "Systolic peak detection in acceleration photoplethysmograms measured from emergency responders in tropical conditions," *PLoS ONE*, vol. 8, no. 10, Oct. 2013, Art. no. e76585.

[62] D. Y. Hwang, B. Taha, and D. Hatzinakos, "Variation-stable fusion for PPG-based biometric system," in *Proc. ICASSP - IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP)*, Jun. 2021, pp. 8042–8046.

[63] E. Lee, A. Ho, Y.-T. Wang, C.-H. Huang, and C.-Y. Lee, "Cross-domain adaptation for biometric identification using photoplethysmogram," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP)*, May 2020, pp. 1289–1293.

[64] A. Reiss, I. Indlekofer, P. Schmidt, and K. Van Laerhoven, "Deep PPG: Large-scale heart rate estimation with convolutional neural networks," *Sensors*, vol. 19, no. 14, p. 3079, Jul. 2019.

[65] P. H. Charlton et al., "Detecting beats in the photoplethysmogram: Benchmarking open-source algorithms," *Physiological Meas.*, vol. 43, no. 8, Aug. 2022, Art. no. 085007.

[66] G. Lovisotto, H. Turner, S. Eberz, and I. Martinovic, "Seeing red: PPG biometrics using smartphone cameras," in *Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit. Workshops (CVPRW)*, Jun. 2020, pp. 818–819.

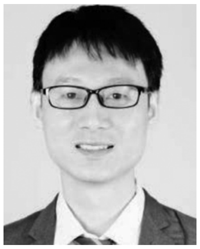
[67] M. Joshi, B. Mazumdar, and S. Dey, "Security vulnerabilities against fingerprint biometric system," 2018, *arXiv:1805.07116*.

[68] A. Rogalski, Z. Bielecki, and J. Mikolajczyk, "Detection of optical radiation," in *Handbook of Optoelectronics*. Boca Raton, FL, USA: CRC Press, 2017, pp. 65–124.

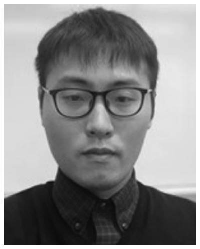
Junhao Wang received the B.E. degree in software engineering from Zhejiang University, where he is currently pursuing the Ph.D. degree with the School of Cyber Science and Technology. His research interests include the IoT security and voice security.

Li Lu (Member, IEEE) received the B.E. degree in computer science and technology from Xi'an Jiaotong University and the Ph.D. degree in computer science and technology from Shanghai Jiao Tong University. He was a Visiting Research Student with the Wireless Information Network Laboratory (WINLAB), Rutgers University. He is currently a tenure-track Research Professor with the School of Cyber Science and Technology, College of Computer Science and Technology, Zhejiang University. His research interests include intelligent voice security, autonomous driving security, the IoT security, and ubiquitous computing. He was a recipient of the ACM China SIGAPP Chapter Rising Star Award, the ACM China SIGAPP Chapter Doctoral Dissertation Award, the Best Paper Award of IEEE ICC 2025, the Best Poster Runner-Up Award from ACM MobiCom 2022, and the First Runner-Up Poster Award from ACM MobiCom 2019. He has been serving on the Editorial Board for IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY.

Hao Kong (Member, IEEE) received the B.E. degree in computer science and technology from the Ocean University of China and the Ph.D. degree in computer science and technology from Shanghai Jiao Tong University. He was a Visiting Research Student at the Broadband Communications Research Laboratory (BBCR) and Department of Electrical and Computer Engineering, University of Waterloo, Canada. He is currently an Assistant Professor with the School of Computer Engineering and Science, Shanghai University. He has published more than ten articles in prestigious journals and conferences, including IEEE TRANSACTIONS ON MOBILE COMPUTING, IEEE/ACM TRANSACTIONS ON NETWORKING, IEEE COMMUNICATIONS SURVEYS AND TUTORIALS, IEEE INFOCOM, ACM MobiSys, ACM MobiHoc, and IEEE ICDCS. His research interests include mobile sensing, wireless sensing, and ubiquitous computing. He was a recipient of the ACM China SIGAPP Chapter Doctoral Dissertation Award.



Feng Lin (Senior Member, IEEE) received the Ph.D. degree from the Department of Electrical and Computer Engineering, Tennessee Technological University, Cookeville, TN, in 2015. He was an Assistant Professor with the University of Colorado Denver, Denver, Colorado; a Research Scientist with the State University of New York (SUNY) at Buffalo, Buffalo, NY, USA, and an Engineer with Alcatel-Lucent (currently, Nokia). He is currently a Professor at the School of Cyber Science and Technology, College of Computer Science and Technology, Zhejiang University, China. His current research interests include mobile sensing, the Internet of Things security, biometrics, AI security, and the IoT applications. He was a recipient of the Best Paper Award from ACM MobiSys'20, IEEE Globecom'19, IEEE BHI'17, the Best Demo Award from ACM HotMobile'18, and the First Prize Design Award from the 2016 International 3-D printing competition.



Zhongjie Ba (Member, IEEE) received the Ph.D. degree in computer science and engineering from the State University of New York at Buffalo in 2019. He was a Post-Doctoral Researcher with the School of Computer Science, McGill University. He is currently a ZJU100 Young Professor with the College of Computer Science and Technology and the Institute of Cyberspace Research (ICSR), Zhejiang University, Hangzhou, China. His current research interests include the security and privacy aspects of the Internet of Things, artificial intelligence powered mobile sensing, and forensic analysis of multimedia contents.

Kui Ren (Fellow, IEEE) received the B.Eng. degree in chemical engineering and the M.Eng. degree in materials engineering from Zhejiang University, China, in 1998 and 2001, respectively, and the Ph.D. degree in electrical and computer engineering from Worcester Polytechnic Institute, USA, in 2007. He is currently the Dean of the College of Computer Science and Technology, Zhejiang University. He is mainly engaged in research in data security and privacy protection, AI security, and security in intelligent devices and vehicular networks. He is a fellow of AAAS, ACM, and CCF.