Basic Study on Presentation Attacks against Biometric Authentication using Photoplethysmogram

Shun Hinatsu,*, **, # Daisuke Suzuki, * Hiroki Ishizuka, ** Sei Ikeda,** Osamu Oshiro **

Abstract Several kinds of biometric authentications have been used as countermeasures against identity spoofing. Recently, some approaches have utilized time-series biosignals for biometrics, and one of the approaches is photoplethysmogram (PPG)-based authentication. PPG sensing has the advantage of fewer restrictions of measurement sites than other time-series physiological signals. Moreover, it can connect the authentication and the healthcare applications seamlessly with one sensor. However, identity spoofing against PPG-based authentication may occur by exploiting this advantage. To develop a PPG-based authentication system with countermeasures, we propose the feasibility of a presentation attack against PPG-based authentication. The attack stealthily records PPGs on non-genuine measurement sites, and transmits the signals to the authentication device, thereby utilizing the advantage of PPG sensing in which signals can be recorded on various sites of a subject’s body. We conducted an experiment to investigate the feasibility of the attack. We developed a PPG-based authentication system comprising a PPG sensing system including PPG sensors for multiple measurement sites, and an authentication algorithm based on an existing PPG-based identification algorithm. We recorded PPGs on three measurement sites on the subjects’ bodies using the developed system. Then, we investigated the feasibility of the attack by inputting the feature values extracted from the PPGs recorded on non-genuine measurement sites to the classifier generated by the values from the PPGs recorded on genuine measurement sites. The results indicate that the attack can occur within a short time without any mapping under an ideal condition. Therefore, countermeasures such as liveness detection and utilization of unique information of measurement sites are required against the attack.

Keywords: security, biometrics, authentication, photoplethysmogram, identity spoofing, presentation attack.

Adv Biomed Eng. 10: pp. 101–112, 2021.

1. Introduction

Several authentication methods have been used as countermeasures against identity spoofing, which is a kind of cyber attack. One of the methods is inputting passwords with a keyboard or touch panel. Meanwhile, with the proliferation of electronic devices such as smartphones, biometric authentication has become widely available. A typical biometric authentication system comprises a sensor that obtains biometric information from a user, a feature value extractor that obtains identifiable information from the biometric information and stores them as templates, and a matcher that compares a new value with the stored templates [1]. However, there are several attack vectors against the system. Ratha et al. [2] classified the vectors into eight types: i) presentation of fake biometrics to the sensor, ii) resubmission of old biometrics, iii) overriding of the feature extractor, iv) alteration of the feature representation, v) overriding of the matcher, vi) alteration of the stored templates, vii) alteration of the data between the stored templates and the matcher, and viii) overriding of the output of the matcher. i) is referred to as presentation attack (PA), and it has been demonstrated on existing image-based biometric authentication systems such as face and fingerprint recognition [3, 4]. Some PAs can be easily executed by utilizing commercially available products such as photographs or liquid-crystal displays for face
recognition [3] and silicone rubbers or gummi candies for fingerprint recognition [4]. Therefore, it is essential to predict probable PAs based on various biometric authentication systems and propose countermeasures against them.

Recently, time-series biosignals have been utilized for biometric authentication owing to their distinctiveness and difficulty of replication [5]. One of the time-series biosignals is electrocardiogram (ECG) signal, which measures the electrical activity of the heart [6]. With miniaturization of the electrodes and the processor, a watch-type device called Nymi Band, which provides ECG-based authentication, is available [7]. Meanwhile, several PAs against ECG-based authentication and their countermeasures have been proposed. Eberz et al. [8] proposed a PA against Nymi Band that maps the victim’s ECG signal by a device other than the victim’s device to produce a genuine signal, which is transmitted to the Nymi Band. Karimian et al. [5] also proposed a PA that maps the attacker’s ECG signal into the victim’s genuine ECG signal and transmits it to the authentication device. Therefore, adding countermeasures such as liveness detection techniques to the authentication device are required against the PAs.

Meanwhile, photoplethysmogram (PPG) has also been utilized for biometric authentication. PPG sensing is an optical technique used to measure blood volume changes [9], and it is an alternative to ECG sensing for clinical applications [10]. Recently, PPG sensors have been installed on many smartwatches for healthcare applications. If PPG-based authentication is available in the near future, it will be possible to connect the authentication and the applications seamlessly. For example, a smartwatch can provide healthcare applications after PPG-based authentication with only one sensor. However, attackers may try to steal users’ personal information from the smartwatch if there are no countermeasures. Therefore, the prediction of probable attacks against PPG-based authentication, including PAs, and the consideration of countermeasures against them are required as in ECG-based authentication.

In this study, to develop a PPG-based authentication system with countermeasures, we propose the feasibility of PA against PPG-based authentication as an attack strategy that may emerge in the near future. By utilizing the advantage of PPG in performing measurements on various sites with only one sensor, the PA stealthily records PPG on a site on a victim’s body, which is different from the PPG of a genuine site measured by an authentication device, and transmits the signal to the device. In this paper, the scheme of the proposed PA is described and its feasibility is investigated using a developed PPG-based authentication system. The PPG-based authentication system comprises a PPG sensing system, which includes PPG sensors for multiple measurement sites and an authentication algorithm based on existing PPG-based identification algorithms. Furthermore, countermeasures against the PA are considered based on the investigation results.

2. PPG-based authentication

2.1 PPG sensing

PPG sensing is an optical biomonitoring technique used to noninvasively measure blood volume changes that contain various information such as arterial expansion and contraction with each heartbeat, venous flow, and respiration [9]. Time-series PPG can be recorded by using a sensor that comprises a typical light-emitting diode (LED) and a phototransistor (PTr). The LED illuminates the tissue and the PTr senses small variations in the intensity of reflected or transmitted light associated with changes in blood volume [11]. Additionally, the PPG of the subject’s skin can be recorded by a camera and by image processing [9].

PPG contains personal bio-information and permits several clinical applications such as heart rate (HR) estimation, percutaneous oxygen ($\text{SpO}_2$) saturation, and respiratory rate (RR) estimation [9]. PPG sensing has often been used as an alternative to ECG sensing because it uses one sensor to perform measurements on different sites [12], whereas ECG uses multiple electrodes to perform measurements on specific sites. By utilizing this advantage, several PPG sensing devices have been proposed, such as finger ring-type and earring-type devices [9]. Recently, general consumers can use healthcare applications such as HR estimation in their daily lives via their smartwatches equipped with PPG sensors.

2.2 Utilizing PPG for authentication

By utilizing the distinctiveness and difficulty of replication of the PPG waveform [5], various PPG-based authentication methods have been proposed since Gu et al. published the first approach [13, 14]. Figure 1 describes an overview of a typical PPG-based authentication. In the process, a subject’s PPG is recorded by a PPG sensor, and the signals are filtered and amplified. Then, feature values are extracted from the signal, and the subject is either registered with a template consisting of feature values or identified by the matcher. If PPG-based authentication is available in the smartwatch, it will be possible to connect the authentication and the applications seamlessly. For example, the smartwatch can provide healthcare applications after authentication by installing only one sensor.

However, the advantage of PPG in performing measurements on different sites with one sensor may lead to
unfavorable results for the subjects. An attacker may record the subject’s PPG by exploiting this advantage to obtain his/her personal information in the PPG. If the abuse occurs on the PPG-based authentication, the attacker may obtain the information via the application after authentication. However, there are few studies on attacks such as PAs against PPG-based authentication. Seepers et al. [15] investigated the possibility of attack against a heartbeat-based authentication by utilizing heartbeats estimated by camera-based PPG as an attack vector. They used only the heartbeats as feature values and did not focus on other values such as amplitude commonly used in a typical PPG-based authentication. Therefore, the prediction of more attacks and their countermeasures is needed to develop a PPG-based authentication system with countermeasures as well as other biometric authentications such as ECG-based authentication.

3. Proposed presentation attack

To develop an authentication system with countermeasures against the PA, we propose the feasibility of a PA against PPG-based authentication. Because PPG can easily be recorded on various measurement sites of the body with a sensor comprising a typical LED and PTr, an attacker may install malicious PPG sensors in some places, stealthily record the victim’s PPG, and utilize the recorded PPG to break the authentication. Before the proposed PA is described, we assume a situation in which the PA can occur in order to investigate the feasibility of the attack. In this PA scenario, there are two people: a victim and an attacker. The victim is the person whose identity is stolen by the attacker while the attacker is the person who impersonates the victim. Figure 2 describes an example of the PA scenario.

3.1 Victim’s condition

The victim has a smartwatch that includes a genuine PPG sensor and wears it on his/her wrist every day. He/she often logs in some applications such as healthcare monitoring, and message exchange including his/her personal information after PPG-based authentication. The victim sometimes takes off the smartwatch before sleeping, bathing, charging the battery, etc., and puts it in a place where the attacker can access physically. Furthermore, the victim touches some daily necessities or office supplies such as a mouse or a desk with his/her finger without knowing that the attacker has installed malicious PPG sensors in them.

3.2 Attacker’s scheme

The attacker has an intention to steal the victim’s personal information by the PA. He/she installs a malicious PPG sensor in the victim’s mouse (Step 1) and stealthily records the victim’s PPG by a PPG sensor installed at a place which the victim’s finger may touch (Step 2). The attacker then generates an electrical signal or controls the light intensity based on the signal recorded from the installed sensor using an arbitrary waveform generator (Step 3). Thereafter, he/she obtains the victim’s smartwatch after the victim takes it off (Step 4), and tries to transmit the generated signal to the PPG sensor installed on the smartwatch to break its authentication (Step 5).
4. Experiment

We conducted an experiment to investigate the feasibility of the proposed PA. We developed a PPG-based authentication system comprising a PPG sensing system and a PPG-based authentication algorithm. We recorded PPGs from various measurement sites of the participants’ bodies using the developed sensing system. Then, we extracted feature values from the recorded PPGs, generated classifiers based on the algorithm, and evaluated the capacity of the authentication algorithm. Finally, we evaluated the PA by utilizing the feature values and classifiers.

4.1 Implemented PPG sensing system

We developed the PPG sensing system including three sensors containing a LED and a PTr. Figure 3 shows the experimental setup. The LED and PTr were mounted on the same chip (NJJ5303R-TE1, New Japan Radio Co., Ltd.). The LED color was green (the emitting peak is at a wavelength of 570 nm), which is often mounted on the PPG sensors of several smartwatches. Generally, PPGs are recorded on the subjects’ fingertip in clinical applications [16], whereas smartwatches with PPG sensors record PPGs on the subjects’ wrist. Additionally, in some approaches, the PPGs are recorded on the subjects’ proximal finger using a ring-type wearable device to realize several applications such as healthcare monitoring and user interface [17, 18]. Therefore, each participant in this experiment wore the sensors on the wrist, fingertip, and the proximal part of his/her index finger, and Velcro tape was used to stabilize the PPGs securely. There are more candidate measurement sites such as toes and ear lobes [9], which are distant from the three measurement sites described above. However, we selected the three sites to focus on the PA using impostor sites that are relatively close to genuine sites because the waveforms recorded on the sites may be more similar to each other than distant sites due to the blood vessel configuration and blood circulation. In addition, the PA focused on the situation in which the sensor was installed at a place which the victim’s finger may touch. Therefore, we selected the wrist, fingertip, and the proximal part of the index finger as measurement sites in the experiment. Each output signal of the PTr was bandpass-filtered with a low-frequency cutoff of 0.40 Hz and a high-frequency cutoff of 5.0 Hz, because the frequency of a typical PPG ranges from 0.40 to 5.0 Hz [19]. The signal was then amplified by a non-inverting amplifier with a gain of 47 dB. Each signal was recorded at a sampling rate of 1 kHz with a resolution of 16 bits using an AD converter (USB-6216, National Instruments).

4.2 Implemented authentication algorithm

The proposed PA was evaluated by utilizing a PPG-based authentication algorithm based on the identification algorithm proposed by Jindal et al. [20]. We chose this algorithm because it is the first approach that utilizes deep learning, which is currently the most popular class of machine learning. The algorithm does not use a dicrotic notch as the feature value, which is a small and brief increase in every one period of PPG that appears when the aortic valve closes [21]. Many approaches for PPG-based authentication use the dicrotic notch in a PPG as a feature value [14]. However, it is often difficult to extract a dicrotic notch from every period of a PPG [22]. Therefore, we chose the algorithm and implemented the authentication algorithm for the system based on it.

4.2.1 Preprocessing

Before the extraction of feature values from the recorded PPGs and generation of a classifier based on the values in the implemented algorithm, the recorded PPG \( v_{\text{raw}}[n] \) of each trial of each subject was standardized to have a mean of zero and a standard deviation of 1 as follows:

\[
\begin{align*}
&v_{\text{std}}[n] = \frac{v_{\text{raw}}[n] - \mu_{\text{raw}}[n]}{\sigma_{\text{raw}}[n]},
\end{align*}
\]

where \( n \), \( \mu_{\text{raw}} \), and \( \sigma_{\text{raw}} \) denote the discrete time, mean of \( v_{\text{raw}}[n] \), and standard deviation of \( v_{\text{raw}}[n] \), respectively.

Then, the standardized signal was divided into PPG segments, each containing a negative peak at the starting point followed by a positive peak and then a negative peak at the end of the segment, as illustrated in Figure 4 [20]. Feature values were extracted from each segment after this preprocessing.

![Fig. 3 Experimental setup. The participant wears three PPG sensors on three parts of the body: fingertip, proximal finger, and wrist.](image-url)
4.2.2 Feature extraction

The algorithm extracted 11 feature values \((C_{i,1}, C_{i,2}, \ldots, C_{i,11})\) [20] from each PPG segment after the preprocessing, where \(i\) denotes the ordinal number of the segment. Each value has a relationship with physiological characteristics based on hemodynamics [16], which may have individual differences and contribute to biometric authentication. Table 1 is a list of the feature values for the implemented algorithm. \(N_i\) denotes the number of points in the segment \(v_{\text{std},i}[n]\). \(\text{DTW}(v_{\text{std},i}[n], v_{\text{std},c}[n])\) indicates the dynamic time warping distance, which provides the minimum distance between \(v_{\text{std},i}[n]\) and \(v_{\text{std},c}[n]\) \((i \neq c)\) [23], where \(v_{\text{std},i}[n]\) denotes the chosen segment from \(M_t\) total segments except \(v_{\text{std},i}[n]\) in each trial. \(W_{\text{std},i}[b, a]\), \(b\) and \(a\) denote the wavelet transform of \(v_{\text{std},i}[n]\), translation and scale parameters, respectively.

### Table 1

| Feature | Abstract of extraction | Physiological meanings |
|---------|------------------------|------------------------|
| Mean value | \(C_{i,1} = \frac{1}{N_i} \sum_{n=0}^{N_i-1} v_{\text{std},i}[n]\) | Average of arterial diameter in one period |
| Standard deviation | \(C_{i,2} = \sqrt{\frac{1}{N_i} \sum_{n=0}^{N_i-1} (v_{\text{std},i} - C_{i,1})^2}\) | Change in arterial diameter in one period |
| Average of DTW distance | \(C_{i,3} = \frac{1}{M_t} \sum_{i=1}^{M_t} \text{DTW}(v_{\text{std},i}[n], v_{\text{std},c}[n])\) | Change in arterial diameter in one trial |
| Maximum value | \(C_{i,4} = \max_{n \in [0, N_i-1]} v_{\text{std},i}[n]\) | Arterial diameter |
| Minimum value | \(C_{i,5} = \min_{n \in [0, N_i-1]} v_{\text{std},i}[n]\) | Arterial diameter |
| Time which has \(C_{i,4}\) | \(C_{i,6} = \arg \max_{n \in [0, N_i-1]} v_{\text{std},i}[n]\) | Arterial expansion velocity |
| Time which has \(C_{i,5}\) | \(C_{i,7} = \arg \min_{n \in [0, N_i-1]} v_{\text{std},i}[n]\) | Arterial contraction velocity |
| Maximum of wavelet coefficients | \(C_{i,8} = \max_{n \in [0, N_i-1]} W_{\text{std},i}[b, a]\) | Frequency characteristics of arterial expansion and contraction |
| Minimum of wavelet coefficients | \(C_{i,9} = \min_{n \in [0, N_i-1]} W_{\text{std},i}[b, a]\) | Frequency characteristics of arterial expansion and contraction |
| Skewness | \(C_{i,10} = \frac{1}{N_i C_{i,2}^3} \sum_{n=0}^{N_i-1} (v_{\text{std},i}[n] - C_{i,1})^3\) | Arterial expansion and contraction velocity |
| Kurtosis | \(C_{i,11} = \frac{N_i \sum_{n=0}^{N_i-1} (v_{\text{std},i}[n] - C_{i,1})^4}{(\sum_{n=0}^{N_i-1} (v_{\text{std},i}[n] - C_{i,1})^2)^2}\) | Arterial diameter, expansion velocity, and contraction velocity |

Fig. 4 Abstract of segmentation of PPG.
TH for the predicted probability that decides the identified subject by the MLP. If the probability is higher than the TH, the subject will be authenticated as genuine by the implemented algorithm. The TH was set to equalize the false rejection rate (FRR) and false acceptance rate (FAR) to obtain the equal error rate (EER) [25].

### 4.3 Experimental procedure

Twelve participants (one female and eleven males) aged between 25 and 30 years (S1, S2, ..., S12) participated in the experiment. They wore the PPG sensors on the three measurement sites and maintained a resting state for 30 s while their PPG was recorded. The total number of recordings was 180, and five recordings were taken from three measurement sites (trial T1, T2, ..., T5) of the participants. The experiment was approved by the Ethical Committee of Information Technology R&D Center (2020-B001), Mitsubishi Electric Corporation, Japan.

Before the PA was evaluated, the MLP was generated in all subjects by the feature values extracted from the recordings at each measurement site of each subject to evaluate the performance of the developed PPG-based authentication system. The identification accuracy was computed based on five-fold cross-validation. The validation uses all trials except one for training and the remaining trials for testing, considering the separation of the data for registration and authentication in the actual use condition of the PPG-based authentication system. The accuracy is calculated as follows:

\[
\text{Accuracy} = \frac{TP + TN}{TP + FP + TN + FN},
\]

where TP, TN, FP, and FN are defined as true positive, true negative, false positive, and false negative, respectively. This process was repeated according to the number of trials (five times) to calculate the average accuracy as the score of the identification performance by each-measurement-site-based authentication. Next, TH was determined for each measurement site (as genuine measurement site) to authenticate each subject by the implemented algorithm.

The PA was then investigated by inputting the feature values extracted from the PPGs recorded on the other measurement site (impostor measurement site) to the classifier rather than transmitting the signal to the sensor (Step 5). Table 2 shows six combinations of the measurement sites for the evaluation. We evaluated the performance of the PA based on five-fold cross validation as well as the evaluation of the performance of the developed PPG-based authentication system. In addition, the different measurement sites were used for training and testing in this evaluation. For example, a classifier was generated using the feature values extracted from the PPGs recorded on the wrists in T1-4, and the values from the PPGs recorded on the proximal fingers and fingertips in T5 were input to the classifier. We evaluated the performance of the PA in terms of the classifier. We computed a success rate (SR), which is a ratio of the trials that include at least one authenticated segment (“success trial”) to all trials as follows:

\[
\text{SR} = \frac{T_{\text{success}}}{T},
\]

where \(T_{\text{success}}\) and \(T\) denote the number of success trials, and the total number of trials, respectively. SR was used to investigate the probability of the PA considering the attacker’s scheme: continuously transmitting the recorded signal which may include segments authenticated as the victim by the authentication system. In addition, we computed a segment acceptance rate (SAR), which is the ratio of the segments correctly accepted as the true subject (“accepted segment”) to all segments as follows:

\[
\text{SAR} = \frac{\sum_{t=1}^{T} M_{\text{accept},t}}{\sum_{t=1}^{T} M_t},
\]

where \(M_{\text{accept},t}\) and \(M_t\) denote the number of authenticated segments in one trial, and the total number of segments in one trial, respectively. SAR was used to evaluate the PA compared with EER (= FAR = FRR) in terms of segments.

### 4.4 Results

Figure 5 shows an example of the PPG recorded simultaneously on three measurement sites of a subject’s body (S2, T4). Table 3 shows the number of PPG segments detected at each measurement site. We computed the accuracy (0.867) and EER = 0.087 by utilizing the PPG on the subjects’ wrist using five-fold cross-validation. Figure 6 presents an example of the relationship between FRR and FAR for the implemented authentication by tuning TH (EER = 0.051). Moreover, the accuracy (0.951, 0.876), and EER values (0.022, 0.057) were computed by utilizing the PPGs recorded on the proximal finger and fingertip, respectively, of the 12 subjects.

We investigated the feasibility of the proposed PA for the combinations shown in Table 2. To investigate

| Number | Genuine site | Impostor site |
|--------|--------------|---------------|
| I      | Wrist        | Fingertip     |
| II     | Wrist        | Proximal finger |
| III    | Proximal finger | Fingertip  |
| IV     | Proximal finger | Wrist     |
| V      | Fingertip    | Proximal finger |
| VI     | Fingertip    | Wrist        |

Advanced Biomedical Engineering. Vol. 10, 2021.
the PA against PPG-on-wrist-based authentication, we input the values extracted from the PPGs on the subjects’ fingertip (I) and proximal finger (II) to the MLP generated by the values of the PPG on the wrist.

Table 4 shows the result of the PA against PPG-on-wrist-based authentication (I and II). The check marks indicate successful trials, and the numbers in parentheses show the numbers of successful segments / the total number of segments in the trial. By utilizing the PPGs on the fingertip (I) and proximal finger (II), we calculated SR = 0.833 and 0.817, respectively. Similarly, we investigated the PA against PPG-on-proximal-finger-based authentication and PPG-on-fingertip-based authentication. Table 5 shows the result of the PA against PPG-on-proximal-finger-based authentication (III and IV). By utilizing the PPGs on the fingertip (III) and wrist (IV), we calculated the SR values as 1.000 and 0.833, respectively. Table 6 shows the result of the PA against PPG-on-fingertip-based authentication (V and VI). By utilizing the PPGs on the proximal finger (V) and wrist (VI), we calculated the SR values as 1.000 and 0.833, respectively. Tables 7–9 show the SAR of the proposed PA against PPG-on-wrist-based authentication (I and II), PPG-on-proximal-finger-based authentication (III and IV), and PPG-on-fingertip-based authentication (V and VI), respectively.

5. Discussion

5.1 Evaluation of performances

We implemented the PPG-based authentication algorithm on the authentication system we developed based on an existing identification algorithm. Before investigation of the proposed PA against the authentication, we evaluated the identification performance of the PPGs recorded from the 12 subjects. The results show accuracy of more than 0.800 for all the measurement sites, which is similar to the result obtained by applying the algorithm to multiple datasets of three or four subjects in the original article [20]. Then, we investigated the feasibility of the PA. Tables 4–6 and SR suggest that the PA may occur with a probability of more than 0.800. The experimental procedure and results also suggest that the PA could be successfully executed within a short duration of 30 s of stealth recording and 30 s of signal transmission. Therefore, the PA may be executed when the victim takes off the smartwatch and charges the battery to 100% for more than one hour [26]. In addition, the PA succeeded without mapping the recorded PPG to the other signals, whereas existing PAs against ECG-based authentication mapped the signals which could be accessed by the attacker to the genuine signals [5, 8].

Tables 7–9 indicate that the average SAR values are higher than all EER (= FAR = FRR) values by utilizing the 12 subjects’ PPGs. This result suggests that the PPG-based authentication system used in this study may accept a segment recorded by the PA as genuine at a higher
Table 4  Results of PA against PPG-on-wrist-based authentication. The PPGs on the fingertip and proximal finger of each trial are used for PA.

| Subject | Fingertip (I) | Proximal finger (II) |
|---------|---------------|----------------------|
|         | T1 | T2 | T3 | T4 | T5 | T1 | T2 | T3 | T4 | T5 |
| S1      | (0/37) ✓ | (3/37) ✓ | (3/38) ✓ | (1/37) ✓ | (0/37) | (0/40)   | (0/39) | (0/40) | (0/39) | (0/39) |
| S2      | (0/39) ✓ | (0/40) | (0/40) | (2/40) | (0/40) | ✓ (1/38) | (0/39) | (0/39) | (0/39) | (0/39) |
| S3      | ✓ (4/30) | (7/30) ✓ | (6/30) ✓ | (7/30) | (8/30) | ✓ (5/30) | (5/30) | ✓ (8/30) | ✓ (4/30) | ✓ (6/30) |
| S4      | ✓ (11/33) | ✓ (11/33) | ✓ (15/33) | ✓ (12/33) | ✓ (13/33) | ✓ (15/31) | ✓ (11/31) | ✓ (22/30) | ✓ (12/29) | ✓ (14/29) |
| S5      | ✓ (1/26) | (3/28) ✓ | ✓ (1/29) | (2/30) | ✓ (3/30) | ✓ (2/34) | ✓ (2/34) | ✓ (3/34) | ✓ (3/34) | ✓ (7/34) |
| S6      | ✓ (10/33) | ✓ (4/34) | (0/34) | ✓ (7/34) | (0/34) | ✓ (19/34) | ✓ (0/34) | ✓ (1/34) | ✓ (4/34) | ✓ (1/34) |
| S7      | ✓ (16/31) | ✓ (16/32) | ✓ (15/32) | ✓ (9/32) | ✓ (13/32) | ✓ (14/32) | ✓ (21/31) | ✓ (20/32) | ✓ (22/32) | ✓ (25/32) |
| S8      | ✓ (17/37) | ✓ (17/36) | ✓ (19/37) | ✓ (20/37) | ✓ (20/36) | ✓ (11/37) | ✓ (16/37) | ✓ (23/38) | ✓ (16/38) | ✓ (23/37) |
| S9      | ✓ (6/34) | ✓ (8/34) | ✓ (20/34) | ✓ (11/34) | ✓ (21/33) | ✓ (5/33) | ✓ (10/35) | ✓ (9/35) | ✓ (8/35) | ✓ (1/35) |
| S10     | ✓ (1/30) | ✓ (4/30) | ✓ (1/29) | ✓ (1/30) | (0/29) | ✓ (1/35) | ✓ (3/36) | ✓ (4/35) | ✓ (1/36) | (0/36) |
| S11     | ✓ (23/36) | ✓ (24/36) | ✓ (16/36) | ✓ (19/36) | ✓ (13/36) | ✓ (15/36) | ✓ (14/36) | ✓ (19/36) | ✓ (20/36) | ✓ (16/36) |
| S12     | ✓ (2/37) | ✓ (1/37) | (0/35) | ✓ (4/34) | ✓ (4/34) | ✓ (4/34) | ✓ (13/33) | ✓ (3/32) | ✓ (6/31) | ✓ (1/32) |

Table 5  Result of PA against PPG-on-proximal-finger-based authentication. The PPGs on the fingertip and wrist of each trial are used for PA.

| Subject | Fingertip (III) | Wrist (IV) |
|---------|----------------|------------|
|         | T1 | T2 | T3 | T4 | T5 | T1 | T2 | T3 | T4 | T5 |
| S1      | ✓ (2/37) | ✓ (3/37) | ✓ (7/38) | ✓ (2/37) | ✓ (4/37) | ✓ (2/25) | ✓ (2/25) | ✓ (2/26) | ✓ (1/25) | ✓ (1/25) |
| S2      | ✓ (4/39) | ✓ (2/40) | ✓ (4/40) | ✓ (2/40) | ✓ (3/40) | (0/35) | (0/36) | (0/36) | (0/36) | (0/36) |
| S3      | ✓ (25/30) | ✓ (17/30) | ✓ (17/30) | ✓ (24/30) | ✓ (18/30) | ✓ (4/30) | ✓ (17/30) | ✓ (10/30) | ✓ (8/30) | ✓ (16/30) |
| S4      | ✓ (8/33) | ✓ (6/33) | ✓ (8/33) | ✓ (8/33) | ✓ (7/33) | ✓ (9/29) | ✓ (2/30) | ✓ (6/30) | ✓ (3/30) | ✓ (7/30) |
| S5      | ✓ (3/26) | ✓ (14/28) | ✓ (6/29) | ✓ (12/30) | ✓ (7/30) | ✓ (10/29) | ✓ (12/29) | ✓ (16/30) | ✓ (17/30) | ✓ (7/30) |
| S6      | ✓ (29/33) | ✓ (30/34) | ✓ (30/34) | ✓ (28/34) | ✓ (23/34) | (0/33) | ✓ (16/34) | (0/34) | ✓ (17/34) | (0/34) |
| S7      | ✓ (9/31) | ✓ (7/32) | ✓ (7/32) | ✓ (4/32) | ✓ (4/32) | ✓ (16/29) | ✓ (3/30) | ✓ (10/31) | ✓ (9/31) | ✓ (5/31) |
| S8      | ✓ (6/37) | ✓ (12/36) | ✓ (10/37) | ✓ (12/37) | ✓ (10/36) | ✓ (15/36) | ✓ (17/36) | ✓ (13/36) | ✓ (12/37) | ✓ (22/36) |
| S9      | ✓ (21/34) | ✓ (28/34) | ✓ (14/34) | ✓ (16/34) | ✓ (10/33) | ✓ (1/32) | ✓ (6/32) | ✓ (1/32) | ✓ (2/33) | ✓ (1/32) |
| S10     | ✓ (9/30) | ✓ (5/30) | ✓ (6/29) | ✓ (7/30) | ✓ (9/29) | ✓ (14/33) | ✓ (6/33) | ✓ (13/32) | ✓ (13/33) | ✓ (19/33) |
| S11     | ✓ (27/36) | ✓ (26/36) | ✓ (26/36) | ✓ (25/36) | ✓ (26/36) | ✓ (9/32) | ✓ (9/33) | ✓ (8/34) | ✓ (8/34) | ✓ (7/34) |
| S12     | ✓ (16/37) | ✓ (7/37) | ✓ (16/35) | ✓ (11/34) | ✓ (21/34) | ✓ (9/34) | (0/34) | (0/32) | ✓ (2/32) | ✓ (5/32) |

The probability than an impostor’s segment. To compare the SAR values among conditions, we conducted an analysis of variance (ANOVA) after establishing the homogeneity of variance among the SAR values (Tables 7–9). The ANOVA results indicate no significant differences in the SAR values among the conditions. However, Tables 7–9 show that a combination of the PPGs on the proximal finger and fingertip (III and V) achieves higher SAR values than other combinations including the PPG on the wrist (I, II, IV, and VI). This is because the sensors on the proximal finger and fingertip may record the PPG derived from the same blood vessel, such as a proper digital artery in the finger [27]. The information derived from the same artery, such as expansion and contraction, may contribute to the waveforms and the feature values extracted from them. Table 3 indicates that the number of segments differs among various measurement sites, with fewer segments detected in the PPG recorded on the wrist than on other sites. This is partly because we could not unify the conditions such as the shading state due to physical differences such as the diameter of finger and wrist. Moreover, segmentation of the PPG on the wrist
Table 6  Result of PA against PPG-on-fingertip-based authentication. The PPGs on the proximal finger and wrist of each trial are used for PA.

| Subject | Proximal finger (V) | Wrist (VI) |
|---------|---------------------|------------|
|         | T1      | T2      | T3      | T4      | T5      | T1      | T2      | T3      | T4      | T5      |
| S1      | ✓(1/40) | ✓(1/39) | ✓(4/40) | ✓(3/39) | ✓(4/39) | ✓(8/25) | ✓(1/26) | ✓(4/25) | ✓(1/25) |         |
| S2      | ✓(25/38) | ✓(16/39) | ✓(22/39) | ✓(17/39) | ✓(28/39) | ✓(6/35) | (0/36) | (0/36) | ✓(1/36) | ✓(3/36) |         |
| S3      | ✓(16/30) | ✓(11/30) | ✓(10/30) | ✓(9/30) | ✓(7/30) | ✓(2/30) | ✓(1/30) | ✓(3/30) | ✓(2/30) | (0/30) |         |
| S4      | ✓(8/31) | ✓(11/31) | ✓(10/30) | ✓(12/29) | ✓(12/29) | ✓(7/29) | ✓(21/30) | ✓(3/30) | ✓(7/30) | ✓(5/30) |         |
| S5      | ✓(10/34) | ✓(11/34) | ✓(11/34) | ✓(18/34) | ✓(10/34) | ✓(6/29) | ✓(15/29) | ✓(3/30) | ✓(8/30) | ✓(13/30) |         |
| S6      | ✓(26/34) | ✓(29/34) | ✓(24/34) | ✓(25/34) | ✓(19/34) | ✓(1/33) | (0/34) | ✓(4/34) | ✓(0/34) | ✓(0/34) |         |
| S7      | ✓(15/32) | ✓(17/31) | ✓(18/32) | ✓(18/32) | ✓(13/32) | ✓(13/29) | ✓(15/30) | ✓(14/31) | ✓(18/31) | ✓(15/31) |         |
| S8      | ✓(10/37) | ✓(7/37) | ✓(3/38) | ✓(2/38) | ✓(8/37) | ✓(9/36) | ✓(10/36) | ✓(7/36) | ✓(13/37) | ✓(17/36) |         |
| S9      | ✓(8/33) | ✓(17/35) | ✓(14/35) | ✓(9/35) | ✓(12/35) | ✓(2/32) | ✓(5/32) | ✓(6/32) | ✓(4/33) | ✓(3/32) |         |
| S10     | ✓(15/35) | ✓(16/36) | ✓(16/35) | ✓(19/36) | ✓(15/36) | ✓(9/33) | ✓(12/33) | ✓(16/32) | ✓(8/33) | ✓(15/33) |         |
| S11     | ✓(18/36) | ✓(20/36) | ✓(21/36) | ✓(20/36) | ✓(18/36) | ✓(12/32) | ✓(9/33) | ✓(12/34) | ✓(8/34) | ✓(6/34) |         |
| S12     | ✓(6/34) | ✓(7/33) | ✓(8/32) | ✓(7/31) | ✓(7/32) | (0/34) | ✓(4/34) | ✓(1/32) | ✓(0/32) | ✓(1/32) |         |

Table 7  SAR of PA against PPG-on-wrist-based authentication. The PPGs on the fingertip and proximal finger are used for PA.

| Subject | Measurement site for attack |
|---------|----------------------------|
|         | Fingertip (I) | Proximal finger (II) |
| S1      | 0.038          | 0.000                |
| S2      | 0.010          | 0.005                |
| S3      | 0.213          | 0.187                |
| S4      | 0.376          | 0.493                |
| S5      | 0.070          | 0.104                |
| S6      | 0.124          | 0.147                |
| S7      | 0.434          | 0.642                |
| S8      | 0.508          | 0.476                |
| S9      | 0.391          | 0.191                |
| S10     | 0.047          | 0.051                |
| S11     | 0.528          | 0.467                |
| S12     | 0.062          | 0.168                |

Average 0.233 ± 0.191  0.248 ± 0.208

Table 8  SAR of PA against PPG-on-proximal-finger-based authentication. The PPGs on the fingertip and wrist are used for PA.

| Subject | Measurement site for attack |
|---------|----------------------------|
|         | Fingertip (III) | Wrist (IV) |
| S1      | 0.097          | 0.063                |
| S2      | 0.075          | 0.000                |
| S3      | 0.673          | 0.367                |
| S4      | 0.224          | 0.181                |
| S5      | 0.294          | 0.419                |
| S6      | 0.828          | 0.195                |
| S7      | 0.195          | 0.283                |
| S8      | 0.273          | 0.436                |
| S9      | 0.527          | 0.068                |
| S10     | 0.243          | 0.396                |
| S11     | 0.722          | 0.246                |
| S12     | 0.401          | 0.098                |

Average 0.379 ± 0.240  0.230 ± 0.146

sometimes fails because the amplitudes tend to be smaller compared with other measurement sites [22], as depicted in Fig. 5. If some external factors such as motion artifacts occur, the PPG on the wrist may be more buried in them than PPGs on the other sites. Therefore, although each PPG was standardized, the PPG recorded on the wrist may have fewer information for PPG-based authentication or PA compared with other sites.

5.2 Experimental limitation
The experiment was conducted only under an ideal condition in this study. Sensors with the same specification were stabilized on the wrist and finger using a Velcro tape for both the genuine and impostor measurement sites. Additionally, the evaluation was conducted by inputting the feature values extracted from the PPGs recorded on impostor measurement sites to the classifier rather than transmitting the signals to the sensor of the
authentication system. Under non-ideal conditions, the contact state of the sensors and sites may change during recording, and the PPGs may include more motion artifacts than under ideal condition. Additionally, the hardware specification of the genuine and non-genuine PPG sensing system, such as the LED color of the PPG sensor, may be different under non-ideal conditions. Then, different light wavelengths cause differences in transmissive depth against the tissue, which may change the PPG waveform. As a result, there may be differences in the feature values extracted from the PPGs, and the authentication algorithm may output results different from those under ideal condition. Therefore, more practical experiments under other conditions are required to study more advanced attacks and countermeasures against them.

In the experiment, because we focused on the blood vessel configuration and blood circulation, and investigated the PA using the PPGs recorded on the measurement sites that are close to each other, we selected three sites: the wrist, fingertip, and the proximal part of the index finger. However, there are more candidate PPG measurement sites such as the toes and ear lobes [9], which are distant from the three selected sites. Although there may be more differences in waveform than the three selected sites, PA using PPGs recorded on sites distant from the genuine sites may also occur similar to the three measurement sites selected in the experiment. Therefore, it is necessary to record PPGs on more various sites to investigate the feasibility of PA using those sites.

We recorded PPGs from only 12 healthy young subjects in the experiment. However, more diverse individuals may be actually using general authentication systems. Although more subjects are required statistically to ensure the reliability of biometric authentication [28], we focused on the investigation of the feasibility of the PA rather than the performance of the PPG-based authentication system. In addition, if we record PPGs from elderly subjects, we may have difficulty extracting some feature values from the PPGs. The difficulty may affect the performance of the PPG-based authentication system, making it difficult to evaluate the PA against the system. Therefore, we recorded PPGs from a limited number of young subjects and investigated the feasibility of the PA. Our future works include recruiting a larger number of diverse subjects and recording PPGs from them to investigate the feasibility of the PA.

### 5.3 Countermeasures

Although the experiment was only conducted in an ideal condition, the results suggest that the proposed PA can occur. Therefore, it is important to consider countermeasures against PA in the development of a PPG-based authentication system with countermeasures.

One of the countermeasures is adding other liveness detection techniques to the authentication device with PPG sensor, in order to distinguish whether the measured object is a human body or artificial material as the proposed PA transmits artificial signals to the sensor. For example, a temperature or humidity sensor can provide a factor that indicates that the object sensed by the device is a human body and not an artificial material.

Moreover, it may be effective to obtain unique information of the measurement site from the PPG signals and utilize them for authentication. For example, utilizing the dicrotic notch in each PPG segment as a feature value may contribute to the countermeasure, although it is difficult to extract dicrotic notches stably from several PPG segments [22]. To investigate feature values that may be countermeasures, the PA needs to be applied to other PPG-based authentication algorithms that utilize various feature values.

### 6. Conclusion

To develop a PPG-based authentication system with countermeasures, we proposed the feasibility of a PA
against PPG-based authentication. The PA utilizes the advantage of PPG sensing in which signals can be recorded on different measurement sites on a person’s body with one sensor. The attacker stealthily records the victim’s PPGs by malicious sensors, and transmits the signals to the authentication device. To investigate the feasibility of the PA, we implemented a PPG-based authentication system comprising a PPG sensing system that included multiple PPG sensors, and a PPG-based authentication algorithm based on an existing identification algorithm. We recorded the PPGs on different measurement sites of the subjects in the experiment. We also investigated the feasibility of the PA by inputting the feature values extracted from the PPGs recorded on non-genuine measurement sites to the classifier generated based on the values of the PPGs recorded on genuine measurement sites. The results indicate that the PA can occur within a short duration without any mapping under an ideal condition in which sensors are stabilized on both genuine and malicious measurement sites on the subjects. Therefore, countermeasures such as liveness detection and utilization of the unique information of the measurement sites are required against the PA.

Conflicts of interest

The authors declare no conflict of interest with any company or commercial organization based on the definition of the Japanese Society of Medical and Biological Engineering.

References

1. Jain A, Hong L, Pankanti S: Biometric identification. Commun ACM. 43(2), 90–98, 2000.
2. Ratha NK, Connell JH, Bolle RM: An analysis of minutiae matching strength. Proc of AVBPA ’01, Halmstad, pp. 223–228, 2001.
3. Ramachandra R, Busch C: Presentation attack detection methods for face recognition systems: A comprehensive survey. ACM Comput Surv. 50(1), 1–37, 2017.
4. Sousedík C, Busch C: Presentation attack detection methods for fingerprint recognition systems: a survey. IET Biometrics. 3(4), 219–233, 2014.
5. Karimian N, Woodard D, Forte D: ECG biometric: spoofing and countermeasures. IEEE Trans Biometrics Behav Identity Sci. 1(3), 257–270, 2020.
6. Pinto JR, Cardoso JS, Loureno A: Evolution, current challenges, and future possibilities in ECG biometrics. IEEE Access. 6, 34746–34776, 2018.
7. Nymi | Workplace Wearables. <https://www.nymi.com/> [accessed on May 27, 2021].
8. Eberz S, Paolletti N, Roeschlin M, Kwiatkowska M, Martinovic I, Patane’ A: Broken hearted: How to attack ECG biometrics. Proc of NDSS ’17, San Diego, pp. 1–15, 2017.
9. Sun Y, Thakor N: Photoplethysmography revisited: from contact to noncontact, from point to imaging. IEEE Trans Biomed Eng. 63(3), 463–477, 2015.
10. Castaneda D, Esparza A, Ghamari M, Soltanpur C, Nazeran H: A review on wearable photoplethysmography sensors and their potential future applications in health care. Int J Biosens Bioelectron. 4(4), 195–202, 2018.
11. Tamura T, Maeda Y, Sekine M, Yoshida M: Wearable photoplethysmographic sensors—past and present. Electronics. 3(2), 282–302, 2014.
12. Maeda Y, Sekine M, Tamura T: Relationship between measurement site and motion artifacts in wearable reflected photoplethysmography. J Medical Syst. 35(5), 969–976, 2011.
13. Gu YY, Zhang Y, Zhang YT: A novel biometric approach in human verification by photoplethysmographic signals. Proc of IEEE ITAB ’03, Birmingham, pp. 13–14, 2003.
14. Khan S, Parkinson S, Grant L, Liu N, Mcguire S: Biometric systems utilising health data from wearable devices: applications and future challenges in computer security. ACM Comput Surv. 53(4), 1–29, 2020.
15. Seeppers RM, Wang, W, De HG, Sourdis I, Strydis C: Attacks on heartbeat-based security using remote photoplethysmography. IEEE J Biomed Health Inform. 22(3), 714–721, 2017.
16. Elgendi M: On the analysis of fingertip photoplethysmogram signals. Curr Cardiol Rev. 9(1), 14–25, 2012.
17. Kinnunen H, Rantanen A, Kettä T, Koskimäki H: Feasible assessment of recovery and cardiovascular health: accuracy of nocturnal HR and HRV assessed via ring PPG in comparison to medical grade ECG. Physiol Meas. 41(4), 1–9, 2020.
18. Yoshimoto S, Hinatsu S, Kuroda Y, Oshiro O: Hemodynamic sensing of 3-D fingertip force by using nonpulsatile and pulsatile signals in the proximal part. IEEE Trans Biomed Circuits Syst. 12(5), 1155–1164, 2018.
19. Ram M, Madhav K, Krishna E, Komalla N, Reddy K: A novel approach for motion artifact reduction in PPG signals based on AS-LMS adaptive filter. IEEE Trans Instrum Meas. 61(5), 1445–1457, 2012.
20. Jindal V, Birjandtalab J, Pouyan MB, Nourani M: An adaptive deep learning approach for PPG-based identification. Proc of IEEE EMBC ’16, Berlin, pp. 6401–6404, 2016.
21. Politi MT, Ghigo A, Fernández JM, Khelifa I, Gaudric J, Fullana JM, Lagrée PY: The dicrotic notch analyzed by a numerical model. Comput Biol Med. 72, 54–64, 2016.
22. Hartmann V, Liu H, Chen F, Qiu Q, Hughes S, Zheng D: Quantitative comparison of photoplethysmographic waveform characteristics: effect of measurement site. Front Physiol. 10(198), 1–18, 2019.
23. Berndt DJ, Clifford J: Using dynamic time warping to find patterns in time series. Proc of KDD ’94 workshop, Seattle, pp. 359–370, 1994.
24. Chio C, Freeman D: Machine Learning & Security. O’REILLY, Sebastopol, 2018.
25. Malik J, Girdhar D, Dahia R, Sainarayanan G: Reference threshold calculation for biometric authentication. IJIGSP. 2, 46–53, 2014.
26. Apple Watch—Battery—Apple. <https://www.apple.com/watch/battery/> [accessed on May 27, 2021].
27. Braga-Silva J, Kuyven CR, Fallopia F, Albertoni W: An anatomical study of the dorsal cutaneous branches of the digital arteries. J Hand Surg Eur. 27(6), 577–579, 2002.
Shun Hinatsu
Shun Hinatsu received the M.S. degree from Osaka University, Japan, in 2017. In 2017, he joined Mitsubishi Electric Corporation, Japan. He is also currently a doctoral student at the Graduate School of Engineering Science, Osaka University. His research interests include biomedical instrumentation and biometric authentication.

Daisuke Suzuki
Daisuke Suzuki received the Ph.D. degree from Yokohama National University, Japan, in 2011. In 2001, he joined Mitsubishi Electric Corporation, Japan. His research interests include implementation of cryptosystems. He is a member of the Institute of Electronics, Information and Communication Engineers.

Hiroki Ishizuka
Hiroki Ishizuka received the Ph.D. degree from Keio University in 2016. He was an Assistant Professor with a Department of Engineering, Kagawa University from 2016 to 2019. He is currently an Assistant Professor with the Graduate School of Engineering Science, Osaka University. His research interests include haptics and soft robotics. He is a member of the Society of Instrument and Control Engineers, the Japan Society of Mechanical Engineers, and the Virtual Reality Society of Japan.

Sei Ikeda
Sei Ikeda received the Ph.D. degree from the Nara Institute of Science and Technology, Ikoma, Japan, in 2006. He has worked as an Assistant Professor with the Graduate School of Information Science, Nara Institute of Science and Technology, until 2011, and the Graduate School of Engineering Science, Osaka University, until 2015. He was also a Visiting Researcher with the University of Oulu, Finland, in 2010 and 2011. He was a Lecturer with the College of Information Science and Engineering, Ritsumeikan University, from 2015 to 2019. Since 2019, he has been an Associate Professor with the Graduate School of Engineering Science, Osaka University. His research interests include human-computer interaction, mixed reality, and computer vision. He is a member of the Institute of Electronics, Information and Communication Engineers, the Virtual Reality Society of Japan, IEEE, and ACM.

Osamu Oshiro
Osamu Oshiro received the Ph.D. degree from Osaka University, Toyonaka, Japan, in 1990. He was a Research Engineer with Sumitomo Metal Industries, from 1990 to 1993, and an Assistant/Associate Professor with the Nara Institute of Science and Technology, from 1993 to 2003. Since 2003, he has been a Professor with the Graduate School of Engineering Science, Osaka University. His research interests include biomedical engineering, medical imaging, biomedical signal processing and so on. He is a member of Japanese Society for Medical and Biological Engineering, the Institute of Electronics, Information and Communication Engineers, the Institute of Systems, Control and Information Engineers, the Japanese Society of Medical Imaging Technology, the Virtual Reality Society of Japan, and Japan Society of Computer Aided Surgery.