Evaluation of PPG Feature Values Toward Biometric Authentication Against Presentation Attacks

SHUN HINATSU\textsuperscript{1,2}, DAISUKE SUZUKI\textsuperscript{1}, HIROKI ISHIZUKA\textsuperscript{2}, SEI IKEDA\textsuperscript{2}, (Member, IEEE), AND OSAMU OSHIRO\textsuperscript{2}

\textsuperscript{1}Information Technology Research and Development Center, Mitsubishi Electric Corporation, Kamakura 247-8501, Japan
\textsuperscript{2}Graduate School of Engineering Science, Osaka University, Toyonaka 560-8531, Japan

Corresponding author: Shun Hinatsu (Hinatsu.Shun@bc.MitsubishiElectric.co.jp)

This work involved human subjects or animals in its research. Approval of all ethical and experimental procedures and protocols was granted by the Ethical Committee of Information Technology R&D Center, Mitsubishi Electric Corporation under Application No. 2020–B001.

\textbf{ABSTRACT} In this study, we examined information leakage in photoplethysmogram (PPG)-based biometric authentication and assessed an attack against authentication based on the information leakage. Several approaches have been proposed to apply PPG to biometric authentication using a wearable device; however, there may be several attacks against PPG-based authentication. One of the attacks is a “presentation attack” (PA), which utilizes the information leakage originating from the various PPG measurement sites on a body. The PA records the victim’s PPG stealthily on non-genuine measurement sites and transmits it to the PPG sensor to break the authentication. We examined the information leakage and assessed the PA by evaluating feature values extracted from the PPG signals. We recorded the PPG signals of 12 participants on their fingertips and wrists. We compared the feature values extracted from the recorded PPG signals by computing the differences, correlation coefficients, and mutual information to examine the leakage of information required for the PPG-based authentication. We then assessed the feasibility of a PA based on existing PPG-based authentication algorithms and evaluated the contribution of each value to authentication and PA by computing the permutation importance of all feature values. The experimental results indicated that there might be information leakage and selection of feature values to reduce the feasibility of the PA up to 62.8\%.

\textbf{INDEX TERMS} Biometric authentication, identity spoofing, photoplethysmogram and presentation attack.

\section{I. INTRODUCTION}

With the growth of the Internet and wearable devices, such as smartwatches, our bodies are becoming connected to networks [1]. Many devices provide users with applications via networks. The devices often retain and show confidential information in applications such as message exchange by connecting to smartphones. Some devices are even able to provide users with applications such as payment functions using stored personal wallet data without connecting to smartphones [2]. However, there may be attackers who try to access and steal confidential information to show the capability to hack or make a profit from the information. Therefore, an authentication function must be added to the device to identify the user of the device and reject attackers in case it is stolen.

There are several authentication methods for wearable devices, such as smartwatches. The pervasive methods are password- and pattern-based authentication, which require touching the touchscreen mounted on the device [3]. However, the authentication methods can be vulnerable to identity spoofing such as shoulder-surfing and brute-force attacks [4]. Several approaches have been proposed to apply biometric authentication to wearable devices. For example, ring-type devices equipped with fingerprint sensors [5] and watch-type devices equipped with electrocardiogram (ECG)-based authentication modules [6] have been developed. These methods contribute to user convenience because there is no risk of
forgetting or losing the information required for authentication [7]. However, many biometric authentication methods for wearable devices often restrict the user activity. For example, fingerprint- or ECG-based authentication requires the user to have a specific posture, such as touching the sensor or the electrode with the finger. Therefore, it is necessary to develop a biometric authentication method for wearable devices with few restrictions, such as posture limitations.

Meanwhile, there have been several approaches utilizing the distinctiveness of photoplethysmogram (PPG) for biometric authentication [8]. A PPG signal is a noninvasive circulatory signal related to changes in blood volume in the tissue [9], which can be recorded by a sensor mounted on a smartwatch to provide health information such as SpO2 (arterial oxygen saturation) [10]. As shown in Fig. 1, the sensor comprises a light source such as a typical light-emitting diode (LED) illuminating the tissue and a photodetector such as a phototransistor (PTr) sensing the arterial expansion and contraction in the intensity of the reflected or transmitted light [10]. PPG-based biometric authentication can be realized by extracting feature values from recorded PPG signals and comparing them to registered templates [11]. The advantage of a PPG is that its measurements can be performed on various sites, such as fingers and wrists using only one sensor, as shown in Fig. 1, whereas ECG measurements require at least two electrodes on separated sites on the body. PPG is often an alternative to ECG for heart rate (HR) estimation because it can be recorded with fewer restrictions than ECG [12]. PPG is expected to seamlessly connect some applications, such as health monitoring and authentication, with one sensor [13]. Therefore, wearable devices may provide PPG-based authentication with PPG sensors installed on them in the near future.

However, there may be specific vulnerabilities in PPG-based authentication. Although the variety of measurement sites on a body with few restrictions is an advantage of PPG measurement, it may lead to a leakage of information required for PPG-based authentication because several biomedical approaches have investigated the similarity in PPG waveforms recorded at different measurement sites on one person [14]. If an attacker stealthily records a victim’s PPG signal on non-genuine measurement sites and utilizes the signal as an input to the PPG sensor, the PPG-based authentication algorithm may accept the input as genuine.

In this study, we investigated the vulnerability of PPG-based authentication to develop PPG-based authentication systems with countermeasures. We focused on the variety in PPG measurement sites on the body and the waveforms at each site to examine the leakage of information required for authentication. Several studies have been conducted on PPG-based authentication and its attacks. Our previous work also investigated attacks against PPG-based authentication [15]. The attack utilized a victim’s PPG signal stealthily recorded on non-genuine measurement sites on the victim’s body and transmitted the signal to the PPG sensor to break authentication. However, there is a paucity of studies investigating the effect of waveform variety on PPG-based authentication and attacks against it. Studying the relationships between PPG waveforms recorded at different sites may lead to the development of countermeasures against attacks. Therefore, we investigated the vulnerability by recording PPG signals at multiple measurement sites on the participants’ bodies, examining the information leakage, and assessing the feasibility of the attack using the recorded PPG signals.

II. RELATED WORKS

There can be several attacks on biometric authentication systems. A typical biometric authentication system comprises three components: a sensor that obtains biometric information from a user, a feature value extractor that obtains identical information from the biometric information and stores it as templates, and a matcher that compares a new value with the stored templates [16]. Several attack vectors exist for the components of the system. One of the most well-known vectors is the presentation of fake biometrics to a sensor, which is referred to as a presentation attack (PA). PAs have been demonstrated for pervasive image-based biometric authentication systems utilizing commercially available products. For example, face recognition can be achieved by presenting photographs or liquid-crystal displays to cameras [17]. Fingerprint recognition can also be achieved by presenting silicone rubbers or gummi candies to a fingerprint sensor [18].

In general, most pervasive biometric authentication systems utilize physical images such as faces and fingerprints. Recently, an increasing number of approaches have utilized time-series physiological signals for biometric authentication because of their distinctiveness and difficulty in replication [8]. For example, a watch-type device called Nymi Band, which provides authentication using an ECG signal derived from the electrical activity of the heart, is
available [6]. An electroencephalogram (EEG) signal, which can be recorded by electrodes mounted on headband- and headset-type devices, is also utilized for biometric authentication [19]. In addition, many approaches utilize PPG signals that can be recorded by sensors mounted on smartwatches for biometric authentication [11]. However, several PAs against biometric authentication using time-series physiological signals and physical image-based authentication have been proposed. For example, several approaches proposed PAs against ECG-based authentication and demonstrated them against the Nymi Band. Eberz et al. proposed a PA against the Nymi Band, which focused on a variety of ECG measurement sites on the body [20]. The PA maps the victim’s ECG signal using a device other than the victim’s device to produce a genuine signal, which is transmitted to the Nymi Band. Shukla et al. proposed a PA for EEG-based authentication [21]. The PA utilizes the correlation between the recorded EEG and the user’s movement during EEG recording. In addition, several PAs against PPG-based authentication have been proposed, focusing on the various PPG measurement sites on the body. Seepers et al. investigated the possibility of passing a heartbeat-based authentication by utilizing heartbeats estimated based on blood circulation in the face using camera-based PPG as an attack vector [22].

Our previous work also proposed a PA against PPG-based authentication that utilizes multiple feature values [15]. We assumed that the victim wore a smartwatch that included a genuine PPG sensor, and often logged into some applications using confidential information after PPG-based authentication. We also assumed that the attacker intended to steal the information through the PA, which was executed as follows:

Step 1: Install a malicious PPG sensor in the daily necessities or office supplies such as mouse or a desk that the victim may touch with the finger.
Step 2: Record the victim’s PPG signal at the finger using the malicious PPG sensor.
Step 3: Generate an electrical signal or control the light intensity based on the recorded signal.
Step 4: Obtain the victim’s smartwatch after he/she removes it for charging the battery.
Step 5: Transmit the signal to the PPG sensor installed on the smartwatch to break its authentication.

In the experiment, we investigated the feasibility of proposed PA using the PPG signals recorded at multiple measurement sites on participants and an existing PPG-based authentication algorithm. The experimental results suggested that the PA could occur [15].

The PAs against biometric authentication using time-series physiological signals in the previous paragraphs are based on a hypothesis about possibility of information leakage; the biometric information required for authentication may be available on other measurement sites or sensing devices. For example, a feature value extracted from a signal recorded at a measurement site may be equal to a value from a signal at another site. However, there are few studies examining the information leakage required for biometric authentication. To the best of our knowledge, no studies have examined the leakage of information, such as feature values required for PPG-based biometric authentication, to investigate attacks. Our previous work [15] also did not examine the leakage using the feature values in the PPG-based authentication algorithm. If we examine this and evaluate the contribution of information to authentication and PAs, we may derive an optimized authentication algorithm with countermeasures against PAs. For example, if the same feature values extracted from PPG signals recorded at different sites are equal based on the hypothesis, we should eliminate the value from the algorithm against the PA. Therefore, to develop PPG-based authentication with countermeasures, we investigated information leakage as a vulnerability in PPG-based authentication. We evaluated the feature values extracted from the PPG signals recorded on multiple measurement sites to examine information leakage. Then, we evaluated the contribution of each feature value to the authentication and PA to derive an optimized authentication algorithm with countermeasures against the PA.

III. EXPERIMENT
A. OVERVIEW

We conducted an experiment to examine information leakage in PPG-based biometric authentication and assessed the feasibility of PA. Figure 2 presents an overview of the experimental protocol. We recorded PPG signals at two measurement sites on the participants using the developed sensing system. Then, we extracted feature values from the recorded PPG signals and compared them to examine information leakage for authentication. Subsequently, we assessed the capabilities of the authentication and feasibility of the PA against it using feature values and classifiers based on existing algorithms.

At the same time, we evaluated the contribution of each value to the authentication and PA and compared the results in combination with the values.

B. SETUP AND RECORDING

We developed a PPG sensing system to record PPG signals at two measurement sites on the body. The system included two sensors consisting of an LED and a PTr (LED emitting peak wavelength: 570 nm, New Japan Radio Co., Ltd., NJL5303R-TE1). Each output of the PTr was filtered with a low-frequency cutoff of 0.40 Hz and a high-frequency cutoff of 5.0 Hz, amplified with a gain of 47 dB and a sampling rate of 1 kHz with a resolution of 16 bits, and recorded using an AD converter (National Instruments, USB-6216).

We recorded PPG signals from 12 participants (S1, S2, ..., S12, one female and 11 males, aged 25-30 years) who did not have any cardiovascular diseases. As illustrated in Fig. 3, the sensors were fastened using Velcro tape to record PPG signals on the fingertip and wrist. Although there are more candidates for PPG measurement sites, as shown in Fig. 1, we selected the two sites as our scope to examine the information leakage and assess the PA using PPG signals recorded.
on relatively close sites, which might resemble each other in waveform based on the blood vessel configuration and blood circulation. In addition, PPG signals are generally recorded on the fingertips in many clinical applications [23], whereas smartwatches record PPG signals on the wrist. The participants wore the PPG sensors on the two measurement sites and maintained a resting state for 30 s while the PPG signals were recorded. Five recordings (trial T1, T2,..., T5) were obtained for each participant. The experiment was approved by the Ethical Committee of Information Technology R&D Center (2020-B001), Mitsubishi Electric Corporation, Japan. Informed consent was obtained from the participants before recording was started.

C. EXAMINATION OF INFORMATION LEAKAGE

1) FEATURE EXTRACTION

We extracted 43 feature values $C_{i,1}$, $C_{i,2}$, . . . , $C_{i,43}$ from PPG segments to examine the leakage of the information required for authentication, where $i$ denotes the number of segments. Each PPG segment contained a negative peak at the starting point, followed by at least one positive peak, followed by a negative peak at the end of the segment as illustrated in Fig. 4. The values were originally from previous works on PPG measurement, including not only biometric authentication, but also physiological studies [24]–[27] as follows:

- $C_{i,1}$, . . . , $C_{i,4}$ were the peak-related values such as number of peaks, which might reflect the arterial stiffness. Gu et al. proposed the first approach to apply PPG to biometric authentication using those four values [24].
- $C_{i,5}$, . . . , $C_{i,15}$ were mainly statistics-related metrics such as mean and maximum value in a segment. The values also included mean of dynamic time warping (DTW) distance, which was similarity between one time-series segment and another segment. DTW distance might reflect changes in arterial distensibility in one recording. Jindal et al. proposed the first approach to apply a deep-learning technique to PPG-based authentication using those 11 values [25].
- $C_{i,16}$, . . . , $C_{i,39}$ were 24 Mel-frequency cepstral coefficients (MFCC1, . . . , MFCC24), which were often used in audio signal processing systems. They were computed by applying discrete Fourier transform, logarithmic transform of mel-scale warped spectrum, and discrete cosine transform to an input PPG signal. Those MFCCs might reflect frequency characteristics of PPG signals. Siam et al. proposed the application of a deep-learning technique to PPG-based authentication using those MFCCs [26].
- $C_{i,40}$, . . . , $C_{i,43}$ were amplitude-related values such as the peak-to-peak values in each segment. The values included those related to the dicrotic notch, which is a small and brief increase in a segment [28]. The dicrotic notch might reflect the arterial stiffness. Hartmann et al. proposed them for the evaluation of differences in PPG waveforms recorded at multiple measurement sites on the body, but not for PPG-based authentication [27].

Table 1 shows the abstract of each feature value.

2) EVALUATION OF FEATURE VALUES

We used three evaluation metrics between the feature values: the mean absolute percentage error (MAPE), correlation coefficient (CC), and mutual information (MI) to investigate the relationship between a feature value $C_{i,m}^{\text{wr}}$ from the PPG signal recorded on the wrist (PPG$_{\text{wr}}$) and a value $C_{i,m}^{\text{fi}}$ from
the PPG signal recorded on the fingertip (PPGfi), where \( m \) denotes the identifier of the extracted feature values \((m = 1, 2, \ldots, 43)\). We computed the difference between \( C_{i,m}^{\text{wt}} \) and \( C_{i,m}^{\text{fi}} \) as MAPE assuming the former as a true value as follows [29]:

\[
\text{MAPE}_m = \frac{1}{N} \sum_{i=1}^{N} \left| \frac{C_{i,m}^{\text{wt}} - C_{i,m}^{\text{fi}}}{C_{i,m}^{\text{wt}}} \right|,
\]

where \( N \) denotes the total number of segments. We used CC to describe the linear relationship between \( C_{i,m}^{\text{wt}} \) and \( C_{i,m}^{\text{fi}} \) as follows [23]:

\[
\text{CC}_m = \frac{\sum_{i=1}^{N} (C_{i,m}^{\text{wt}} - \bar{C}_{i,m}^{\text{wt}})(C_{i,m}^{\text{fi}} - \bar{C}_{i,m}^{\text{fi}})}{\sqrt{\left(\sum_{i=1}^{N} (C_{i,m}^{\text{wt}} - \bar{C}_{i,m}^{\text{wt}})^2\right) \left(\sum_{i=1}^{N} (C_{i,m}^{\text{fi}} - \bar{C}_{i,m}^{\text{fi}})^2\right)}}.
\]

where \( \bar{C}_{i,m}^{\text{wt}} \) and \( \bar{C}_{i,m}^{\text{fi}} \) denote the mean of \( C_{i,m}^{\text{wt}} \) and the mean of \( C_{i,m}^{\text{fi}} \), respectively. We computed MI between \( C_{i,m}^{\text{wt}} \) and \( C_{i,m}^{\text{fi}} \) to describe a nonmonotonic relationship as follows [31]:

\[
\text{MI}_m = \sum_{i=1}^{N} \sum_{j=1}^{N} p(C_{i,m}^{\text{wt}}, C_{j,m}^{\text{fi}}) \log \frac{p(C_{i,m}^{\text{wt}}, C_{j,m}^{\text{fi}})}{p(C_{i,m}^{\text{wt}})p(C_{j,m}^{\text{fi}})},
\]

where \( p(C_{i,m}^{\text{wt}}), p(C_{j,m}^{\text{fi}}) \), and \( p(C_{i,m}^{\text{wt}}, C_{j,m}^{\text{fi}}) \) denote marginal probability mass function of \( C_{i,m}^{\text{wt}} \), the marginal probability mass function of \( C_{j,m}^{\text{fi}} \), and joint probability mass function of \( C_{i,m}^{\text{wt}} \) and \( C_{j,m}^{\text{fi}} \), respectively.

**D. ASSESSMENT OF PA**

1) CLASSIFIER GENERATION

To compute the capability of PPG-based authentication and the feasibility of the PA, we used four classifiers: k-nearest neighbor classifier (kNN), multilayer perceptron (MLP), support vector machine (SVM), and random forest (RF), which were used in existing PPG-based authentication algorithms [24–26], [32], [33]. kNN is a classifier based on the minimum distance from the sample feature vectors to the training feature vectors [32]. We selected the Mahalanobis distance (MD) as the distance function, which has been successfully applied in various biometric systems [35]. We used an MLP with three hidden layers consisting of 40, 40, and 10 nodes, which were estimated as the optimal combination of layers and nodes using a grid search approach as well as the original article [25]. SVM is a classifier that creates boundaries that divide data into two or more classes to maximize the margin between the boundaries and data, and has been successfully applied in various biometric systems [36]. RF is a classifier that generates many classifiers and aggregate their results to satisfy the requirement, and has the capability to use many feature values and classes that biometric authentication processes require [36]. We compared the performance of the four classifiers in the verification.

2) VERIFICATION

We computed performance metrics of authentication and PA based on fivefold cross-validation using the feature values in five trials. In the authentication, the validation used the feature values extracted from PPGwt in all trials except one for training and the remaining trials for testing using each classifier to compute the equal error rate (EER) as the performance metric. The EER was computed by tuning parameters such as the threshold for the predicted probability of each classifier to equalize the false rejection rate (FRR) and false acceptance rate (FAR). In the PA, the validation used the feature values extracted from PPGwt in all trials except one for training and the values from PPGfi in the remaining trials for testing using each classifier to compute the segment acceptance rate (SAR) as the performance metric. For example, a classifier was generated using the feature values extracted from PPGwt in T1-4, and the values from PPGfi in T5 were input to the classifier.

SAR is defined as follows:

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

where \( T \), \( M_{\text{acpt},t} \), and \( M_{t} \) denote the total number of trials, number of authenticated segments in one trial, and total number of segments in one trial, respectively. We used SAR to assess the feasibility of PA by comparing it with EER (= FAR), which describes the feasibility of simple identity spoofing using the authentication device of the other person. Each validation was repeated five times and the average EERs and SARs were computed for each classifier.

3) FEATURE VALUE SELECTION

We evaluated the contribution of each feature value to authentication and PA by computing the permutation importance (PI). The PI is computed by shuffling one column of a dataset of feature values to generate a corrupted dataset and calculating the classification performance using the corrupted dataset. The PI of feature value \( C_{i,m} \) is defined as follows [37]:

\[
\text{PI}_m = s - \frac{1}{K} \sum_{k=1}^{K} s_{k,m},
\]

where \( s, K, \) and \( s_{k,m} \) represent the accuracy score of the trained classifier, total number of repetitions, and accuracy score using the corrupted feature values, respectively. We computed the PIs of all 43 values for both authentication and PA, using these values. If we exclude values with high PIs in PA, we may reduce the SAR. Therefore, we selected...
values based on PIs to reduce the feasibility of the PA. Several approaches have investigated the optimal number of feature values for PPG-based authentication, and their results showed that 15-24 values were effective in achieving a high accuracy of identification [26], [28], [38]. For this investigation, we used 20 feature values selected from all 43 values extracted from the recorded We compared four combinations of values selected from all values based on the PIs as follows:

i) All 43 feature values,

ii) Top 20 feature values which have highest PIs in authentication,

iii) Top 20 feature values which have highest PIs in PA, and

iv) Top 20 feature values that have the highest PIs in authentication, except for the values used in iii).

We compared the EER and SAR using the combinations i) - iv) for each classifier.

E. RESULTS

1) EXAMINATION OF INFORMATION LEAKAGE

Figure 5 shows an example of PPG signals recorded simultaneously at the two measurement sites on a participant’s body (S6, T3). Table 1 presents the evaluation metrics (MAPE, CC, and MI) computed for each feature value. However, we exclude the case in which the denominators become zero in in Eq. (1), (2) when we computed the MAPE and CC. MAPES smaller than 0.100, CCs larger than 0.300, and MIs larger than 0.300 are shown in bold in Table 1. Figures 6, 7, 8, and 9 show the examples of the relationships between the feature values extracted from the two measurement sites, which were proposed by Gu et al. [24], Jindal et al. [25], Siam et al. [26], and Hartmann et al. [27], respectively.

Some of the relationships and evaluation metrics between $C_{i,m}^{wr}$ and $C_{i,m}^{fi}$ showed the possibility of information leakage. For example, Fig. 6(b) $C_{i,2}^{wr}$: positive slant, Fig. 7(a) $C_{i,7}^{wr}$: mean of DTW, Fig. 7(b) $C_{i,11}^{wr}$: minimum value time, and Fig. 9(b) $C_{i,42}^{wr}$: dicrotic notch time show a weak correlation between the values extracted from PPGs recorded on wrist and fingertip. Generally, if the CC between two values is greater than 0.300, we can assume they have a correlation [30]. Therefore, $CC_2 = 0.422$, $CC_7 = 0.389$, $CC_{11} = 0.398$, and $CC_{42} = 0.389$ indicate that there is a correlation between the values PPGs recorded at the other sites. Therefore, the results suggest that there was leakage of information required for PPG-based authentication.

However, as far as we can see in some relationships and evaluation metrics, there were also feature values that did not indicate the possibility of information leakage. For example, Fig. 8(a) $C_{i,16}^{wr}$: MFCC1 and (b) $C_{i,17}^{wr}$: MFCC2 did not show a definite correlation between the MFCCs extracted from PPGs recorded on wrist and fingertip. In addition, many MFCCs had MI $MI_m = 0.000$, as shown in Table 1. These relationships and metrics suggest that there is less information leakage than the other values, and the difficulty of estimating the values of an MFCC extracted from a PPG signal recorded at a measurement site using MFCCs extracted from PPG signals recorded at the other sites. Therefore, the results suggest that the appropriate selection of feature values for the PPG-based authentication algorithm may contribute to a reduction in feasibility of the PA.

2) ASSESSMENT OF PA

Table 2 shows the EERs as the capability of authentication and SARs as the capability of PA. The combinations of
TABLE 1. Abstract of feature values, evaluation metrics (MAPE, CC, and MI) and PI ranks for the values in the experiment.

| Variable | Abstract of feature values | Evaluation metrics | kNN | MLP | SVM | RF |
|----------|---------------------------|--------------------|-----|-----|-----|----|
| C13      | Number of peaks           | 0.044              | 2   | 8   | 32  | 13 |
| C12      | Positive slant            | 1.602              | 9   | 10  | 4   | 2  |
| C13      | Negative slant            | 0.334              | 20  | 13  | 20  | 2  |
| C14      | 1st peak time             | 0.594              | 24  | 11  | 13  | 4  |
| C15      | Mean                      | 2.487              | 14  | 40  | 27  | 6  |
| C16      | Standard deviation        | 0.624              | 21  | 11  | 8   | 2  |
| C17      | Mean of dynamic time warping distance | 0.573 | 1   | 17  | 2   | 2  |
| C18      | Maximum value             | 4.052              | 13  | 15  | 30  | 5  |
| C19      | Minimum value             | 0.631              | 33  | 30  | 18  | 10 |
| C20      | Maximum value time        | 0.349              | 4   | 6   | 5   | 8  |
| C21      | Minimum value time        | 0.057              | 34  | 26  | 36  | 3  |
| C22      | Maximum value of wavelet coefficients | 0.809 | 5   | 33  | 17  | 24 |
| C23      | Minimum value of wavelet coefficients | 0.431 | 6   | 20  | 4   | 10 |
| C24      | Skewness                  | 0.978              | 5   | 33  | 7   | 13 |
| C25      | Kurtosis                  | 0.431              | 6   | 20  | 4   | 10 |
| C26      | MFCC1                     | 0.916              | 29  | 7   | 3   | 7  |
| C27      | MFCC2                     | 2.628              | 36  | 2   | 42  | 39 |
| C28      | MFCC3                     | 1.471              | 25  | 10  | 39  | 11 |
| C29      | MFCC4                     | 0.356              | 30  | 13  | 33  | 17 |
| C30      | MFCC5                     | 0.926              | 37  | 12  | 43  | 23 |
| C31      | MFCC6                     | 0.720              | 27  | 16  | 28  | 27 |
| C32      | MFCC7                     | 0.419              | 18  | 31  | 32  | 31 |
| C33      | MFCC8                     | 0.365              | 38  | 38  | 17  | 38 |
| C34      | MFCC9                     | 0.343              | 31  | 42  | 37  | 29 |
| C35      | MFCC10                    | 0.320              | 39  | 15  | 19  | 28 |
| C36      | MFCC11                    | 0.501              | 41  | 9   | 14  | 32 |
| C37      | MFCC12                    | 0.470              | 10  | 19  | 25  | 18 |
| C38      | MFCC13                    | 0.408              | 40  | 4   | 20  | 37 |
| C39      | MFCC14                    | 0.375              | 11  | 41  | 16  | 42 |
| C40      | MFCC15                    | 0.348              | 43  | 25  | 41  | 16 |
| C41      | MFCC16                    | 0.322              | 8   | 27  | 29  | 11 |
| C42      | MFCC17                    | 0.387              | 24  | 14  | 15  | 34 |
| C43      | MFCC18                    | 0.430              | 35  | 23  | 40  | 36 |
| C44      | MFCC19                    | 0.443              | 32  | 39  | 24  | 23 |
| C45      | MFCC20                    | 0.400              | 22  | 32  | 29  | 24 |
| C46      | MFCC21                    | 0.363              | 26  | 3   | 34  | 25 |
| C47      | MFCC22                    | 0.343              | 19  | 24  | 21  | 43 |
| C48      | MFCC23                    | 0.452              | 17  | 43  | 22  | 27 |
| C49      | MFCC24                    | 0.438              | 42  | 18  | 35  | 10 |
| C50      | Peak-to-peak              | 9.869              | 28  | 34  | 30  | 12 |
| C51      | Dicrotic notch time       | 0.340              | 12  | 5   | 6   | 1 |
| C52      | Reflection index          | 0.178              | 5   | 21  | 23  | 6  |

TABLE 2. Performance metrics of authentication and PA using combinations of feature values and classifiers.

| Classifier | Metrics | Combination of feature values | i) | ii) | iii) | iv) |
|------------|---------|-------------------------------|----|-----|------|-----|
| kNN        | EER     | 0.001                         | 0.002 | 0.002 |      |     |
|            | SAR     | 0.197                         | 0.233 | 0.244 | 0.149 |     |
| MLP        | EER     | 0.015                         | 0.010 | 0.006 | 0.029 |     |
|            | SAR     | 0.279                         | 0.272 | 0.274 | 0.130 |     |
| SVM        | EER     | 0.010                         | 0.007 | 0.011 | 0.031 |     |
|            | SAR     | 0.242                         | 0.234 | 0.252 | 0.144 |     |
| RF         | EER     | 0.005                         | 0.004 | 0.005 | 0.027 |     |
|            | SAR     | 0.222                         | 0.226 | 0.249 | 0.087 |     |

feature values i)-iv) were selected based on the PI ranks included in Table 1. Smaller numbers of PI ranks indicate greater importance in either authentication or PA when using combinations of all feature values and each classifier. Table 2 i) indicates that the implemented authentication algorithm achieved an EER (= FAR) between 0.001 and 0.019 when using each classifier. Meanwhile, it also indicates that the algorithm SARs were between 0.197 and 0.279 when using each classifier, which were greater than the EERs. These results suggest that PPG-based authentication algorithms might accept the available signals in the PA with a higher probability than the impostor’s signal (false acceptance).
As shown in Table 1, PI ranks for the feature values often depended on classifiers. However, several values such as \( C_{i,7} \), \( C_{i,41} \) and \( C_{i,42} \), as shown in Fig. 7(a), Fig. 9(a), and Fig. 9(b), respectively, contributed to both authentication and PA in many combinations of feature values and classifiers. Using these values for the authentication algorithm is discouraged in terms of countermeasures against the PA, although they contribute to authentication performance. Table 2 indicates that the selection of feature values led to changing EERs and SARs, where i), ii), iii) and iv) denote the combination of all feature values, values that improved the authentication performance, values that improved the PA performance and values that did not improve the PA performance, respectively. Although the same number of values were used in ii) and iv), the SAR in iv) was smaller than the SARs in ii) for each classifier. The EER in iv) was larger than the SAR in ii); however, the EER difference between ii) and iv) was smaller than the SAR difference between ii) and iv) for each classifier. The results suggest that the selection of feature values based on the PIs would be effective for the PPG-based authentication algorithm against the PA. We succeeded in the reduction of SAR by 35.8 %, 52.4 %, 38.6 %, and 62.8 % by comparing the combinations iv) to ii) when we used kNN, MLP, SVM, and RF as the classifier, respectively.

### IV. DISCUSSION

#### A. RELATIONSHIP BETWEEN INFORMATION LEAKAGE AND PA

Greater evaluation metrics did not necessarily lead to a higher PI rank of PA for the feature values, depending on the classifier as shown in Table 1, although several metrics suggested that there might be information leakage based on their relationships such as the linear correlation between the values from PPG\(_{wr}\) and PPG\(_{fi}\). We expected that the PA might be more likely to succeed when many feature values \( C_{i,m}^{wr} \) and \( C_{i,m}^{fi} \) satisfying \( C_{i,m}^{wr} \simeq f(C_{i,m}^{fi}) \) were in input to the classifiers in the experiment. Conversely, if there is a relationship where \( C_{i,m} = aC_{i,m}^{fi} \), and the constant \( a \neq 1 \), although \( C_{i,m} \) can be easily estimated using \( C_{i,m}^{fi} \), it may not contribute to the SAR. Meanwhile, there are several techniques for mapping a time-series signal to another signal [20]. If an attacker can estimate \( C_{i,m}^{wr} \) based on the information leakage and the relationships such as linear correlation between the feature values, and generate PPG\(_{wr}\) from PPG\(_{fi}\) satisfying \( C_{i,m}^{wr} \simeq f(C_{i,m}^{fi}) \) based on the relationship, where \( f \) denotes the mapping function, the PA may be more serious against the PPG-based authentication.

We used the 43 values proposed for the authentication and evaluation of differences in PPG waveforms in the four articles [24]-[27] and compared the same feature values such as \( C_{i,5}^{wr} \) from PPG\(_{wr}\) and \( C_{i,1}^{fi} \) from PPG\(_{fi}\). Although they were different from each other in the computation methods, there might be correlations between the values extracted from the same PPG signal, which might contribute to information leakage and redundancy in the algorithm. The redundancy cannot be solved by computing and comparing PIs of the feature values. For example, \( C_{i,8} \): maximum value and \( C_{i,40} \): peak-to-peak (difference between maximum value and minimum value), which were originally from the different articles [25], [27], may have a correlation that leads to information leakage because both of the values are related to the maximum value of the PPG signal. An attacker may estimate \( C_{i,m_1}^{wr} \) using \( C_{i,m_2}^{fi} \), where \( m_1 \neq m_2 \), and generate PPG\(_{wr}\) to break the authentication. If we reduce the number of values for authentication based on metrics such as CC and MI between the values extracted from the PPG signal, we can prevent information leakage and realize efficient PPG-based authentication algorithms.

#### B. LIMITATIONS

Under limited experimental conditions, we examined the information leakage and assessed the PA. We have addressed the following three limitations:

1) **RECORDING CONDITION**

We have to record PPG signals of a larger number of diverse participants at their more various measurement sites. Although a larger number of participants are required statistically to ensure the reliability of biometric authentication systems [24], [25], we focused on the examination of the information leakage and assessment of the PA rather than the performance of the PPG-based authentication systems. If we record PPG signals at the other measurement sites, there may be more differences in the waveforms than the two sites, which may not lead to information leakage and PA. Meanwhile, the characteristics of blood vessels such as compliances depending on ages and measurement sites contribute to the PPG waveforms [39]. If blood vessels in different measurement sites of one participant have same characteristics, the feature values may be close to each other and contribute to information leakage and PA. In addition, considering the time between registration and authentication, we have to record PPG signals for a longer duration because the PPG waveforms gradually change, which may also contribute to the experimental results.

2) **AUTHENTICATION ALGORITHM**

We must examine the information leakage and assess the PA using other PPG-based authentication algorithms. We used...
only the algorithms using hand-crafted feature values such as a maximum value, although there have been many PPG-based authentication algorithms [11]. Some of them use hand-crafted feature values such as a maximum value, which includes the values used in the experiment, while others use all PPG signals based on deep-learning techniques such as a combination of convolution neural network (CNN) and long short-term memory (LSTM) [11].

3) SIGNAL GENERATION
PA was assessed by inputting the feature values extracted from the recorded PPG signals to the classifier, rather than transmitting artificial signals such as modulated current or light intensity to the input of the authentication system as proposed in our previous work [15]. Our future works include the assessment of PA by generating and transmitting the signals to the PPG sensor. Fuji et al. investigated a technique to modulate the light intensity to a PPG sensor to get the target HR from smartwatches [40]. We expect that the similar technique may contribute to the PA against the PPG-based authentication, which spoofs the sensor to impersonate a victim.

C. COUNTERMEASURES
More countermeasures against the PA should be considered because Table 2 suggests that it could occur with more SAR than EER (= FAR) in any combination of feature values and classifiers, although the selection of values contributed to reducing SAR. For example, typical replay attack prevention, such as using one-time information, is effective because the PA repeats the recorded signal. It is also effective to add liveliness detection techniques, such as a humidity sensor, to the authentication device along with the PPG sensor to recognize the object of measurement as a human body, because we assume that the attacker sends artificial signals to the sensor.

V. CONCLUSION
We assumed that PPG-based authentication would be available in the near future, and that there might be leakage of information required for authentication. The leakage is derived from the characteristics of PPG: a variety of measurement sites on a body. We examined the information leakage as the vulnerability in PPG-based authentication and assessed a PA against PPG-based authentication based on information leakage. In the experiment, we recorded PPG signals of 12 participants on their wrist and fingertip and examined the information leakage by computing evaluation metrics of the feature values extracted from the recorded PPG\textsubscript{w} and PPG\textsubscript{f}. The results indicated that there were relationships such as linear correlation between some feature values, which might lead to information leakage and PA against PPG-based authentication. Then, we assessed the feasibility of the PA using the recorded PPG\textsubscript{w} and PPG\textsubscript{f} and evaluated the contributions of the feature values extracted from the signals to the PPG-based authentication and the PA by computing the PI of each value. The experimental results suggest the PA might occur based on the contribution of the feature values and the selection of feature values could reduce the probability of PA up to 62.8%.

REFERENCES
[1] M. Bijone, “A survey on secure network: Intrusion detection & prevention approaches,” Amer. J. Inf. Syst., vol. 4, no. 3, pp. 69–88, Dec. 2016.
[2] M. Al-Sharrar, A. Salman, and L. Ahmad, “Watch your smartwatch,” in Proc. Int. Conf. Comput. Sci. Eng. (ICCSEE), Kuwait, Kuwait, Mar. 2018, pp. 1–5.
[3] M. Guerar, L. Verderame, A. Merlo, F. Palmieri, M. Migliardi, and L. Vallerini, “CirclePIN: A novel authentication mechanism for smartwatches to prevent unauthorized access to IoT devices.” ACM Trans. Cyber-Phys. Syst., vol. 4, no. 3, pp. 1–19, May 2020.
[4] Y. Zhao, Z. Qu, Y. Yang, W. Li, and M. Fan, “An empirical study of touch-based authentication methods on smartwatches,” in Proc. ACM Int. Symp. Wearable Comput. (ISWC), Maui, HI, USA, Sep. 2017, pp. 122–125.
[5] A. Magdlum, E. Sivaraman, and P. B. Honnavalli, “Contactless transaction using wearable ring with biometric fingerprint security feature,” in Proc. Int. Conf. Comput. Netw. Inventive Commun. Technol. (ICCCNT), Jun. 2021, pp. 653–666.
[6] F. Agrafioti, K. Martin, and S. Onsg, “Preauthorized wearable biometric device, system and method for use thereof,” U.S. Patent 9 472 033 B2, Oct. 18, 2016.
[7] S. Lee, W. Choi, and D. H. Lee, “Usable user authentication on a smartwatch using vibration,” in Proc. ACM SIGSAC Conf. Comput. Commun. Secur. (CCS), Virtual Event, Republic Korea, Nov. 2021, pp. 304–319.
[8] N. Karimian, D. Woodard, and D. Forte, “ECG biometric: Spoofing and countermeasures,” IEEE Trans. Biometrics, Behav., Identity Sci., vol. 2, no. 3, pp. 257–270, Jul. 2020.
[9] A. Reisner, P. A. Shaltis, D. McCombie, and H. H. Asada, “Utility of the photoplethysmograph in circulatory monitoring,” Anesthesiology, vol. 108, no. 5, pp. 950–958, May 2008.
[10] T. Tamura, “Current progress of photoplethysmography and SPO2 for health monitoring.” Biomed. Eng. Lett., vol. 9, no. 1, pp. 21–36, Feb. 2019.
[11] S. Khan, S. Parkinson, L. Grant, N. Liu, and S. Mcguire, “Biometric systems utilising health data from wearable devices: Applications and future challenges in computer security,” ACM Comput. Surv., vol. 53, no. 4, pp. 1–29, Jul. 2021.
[12] M. A. Pimentel, A. E. W. Johnson, P. H. Charlton, D. Birrenkott, P. J. Watkinson, L. Tarassenko, and D. A. Clifton, “Toward a robust estimation of respiratory rate from pulse oximeters,” IEEE Trans. Biomed. Eng., vol. 64, no. 8, pp. 1914–1923, Nov. 2016.
[13] T. Zhao, Y. Wang, J. Liu, L. Cheng, Y. Che, and J. Yu, “Robust continuous authentication using cardiac biometrics from wrist-worn wearables,” IEEE Internet Things J., early access, Nov. 6, 2021, doi: 10.1109/JIOT.2021.3128290.
[14] J. Allen, J. O’Sullivan, G. Stansby, and A. Murray, “Age-related changes in pulse risetime measured by multi-site photoplethysmography,” Physiol. Meas., vol. 41, no. 7, pp. 369–377, Aug. 2020.
[15] S. Hinatsu, D. Suzuki, H. Ishizaka, S. Ikeda, and O. Oshiro, “Basic study on presentation attacks against biometric authentication using photoplethysmography.” Adv. Biomed. Eng., vol. 10, pp. 101–112, Jul. 2021.
[16] N. K. Ratha, J. H. Connell, and R. M. Bolle, “An analysis of minutiae matching strength,” in Proc. Int. Conf. Audio Video-Based Biometric Person Authentication (AVBPA), Halmstad, Sweden, Jun. 2001, pp. 223–228.
[17] R. Raghavendra and C. Busch, “Presentation attack detection methods for face recognition systems: A comprehensive survey.” Comput. Surv., vol. 50, no. 1, pp. 1–37, Mar. 2017.
[18] C. Sousedik and C. Busch, “Presentation attack detection methods for fingerprint recognition systems: A survey.” IET Biometrics, vol. 3, no. 4, pp. 219–233, Dec. 2014.
[19] F. Lin, K. W. Cho, C. Song, W. Xue, and Z. Jin, “Brain password: A secure and truly cancelable brain biometrics for smart headwear,” in Proc. Mobisys, Munich, Germany, Jun. 2018, pp. 296–309.
[20] 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. (NDSS), San Diego, CA, USA, Feb. 2017, pp. 1–15.
[21] D. Shukla, P. P. Kundu, R. Malapati, S. Poudel, Z. Jin, and V. V. Phoha, “Thinking unveiled: An inference and correlation model to attack EEG biometrics,” Digit. Threats, Res. Pract., vol. 1, no. 2, pp. 1–29, Jun. 2020.
S.-W. Lee, D.-K. Woo, Y.-K. Son, and P.-S. Mah, “Attacks on heartbeat-based security using remote photoplethysmography,” IEEE J. Biomed. Health Inform., vol. 22, no. 3, pp. 714–721, May 2018.

M. Hosanee, G. Chan, K. Welykholowa, R. Cooper, P. A. Kyriacou, D. Zheng, J. Allen, D. Abbott, C. Menon, N. H. Lovell, N. Howard, W.-S. Chan, K. Lim, R. Fletcher, R. Ward, and M. Elgendi, “Cuffless single-site photoplethysmography for blood pressure monitoring,” J. Clin. Med., vol. 9, no. 3, p. 723, Mar. 2020.

Y. Y. Gu, Y. Zhang, and Y. T. Zhang, “A novel biometric approach in human verification by photoplethysmographic signals,” in Proc. IEEE EMBS Special Topic Conf. Inform. Technol. Appl. Biomed. (ITAB), Birmingham, UK., Apr. 2003, pp. 13–14.

V. Jindal, J. Birjandtalab, M. B. Pouyan, and M. Nourani, “An adaptive deep learning approach for PPG-based identification,” in Proc. 38th Annu. Int. Conf. IEEE Eng. Med. Biol. Soc. (EMBC), Orlando, FL, USA, Aug. 2016, pp. 6401–6404.

A. I. Siam, A. A. Elazm, N. A. El-Bahnasawy, G. M. El Banby, and F. E. A. El-Samie, “PPG-based human identification using mel-frequency cepstral coefficients and neural networks,” Multimedia Tools Appl., vol. 80, pp. 26001–26019, Apr. 2021.

V. Hartmann, H. Liu, F. Chen, Q. Qiu, S. Hughes, and D. Zheng, “Quantitative comparison of photoplethysmographic waveform characteristics: Effect of measurement site,” Frontiers Physiol., vol. 10, Mar. 2019, Art. no. 198.

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), Seattle, WA, USA, Jun. 2020, pp. 3565–3574.

A. R. Kavsaoğlu, K. Polat, and M. Hariharan, “Non-invasive prediction of hemoglobin level using machine learning techniques with the PPG signal’s characteristics features,” Appl. Soft Comput., vol. 37, pp. 983–991, Dec. 2015.

M. M. Mukaka, “A guide to appropriate use of correlation coefficient in medical research,” Malawi Med. J., vol. 24, no. 3, pp. 69–71, Sep. 2012.

M. H. M. Rasid, N. L. Simon, and A. Adam, “Using neural network with random weights and mutual information for systolic peaks classification of PPG signals,” in Proc. 10th Int. Conf. Biomed. Eng. Technol. (ICBET), Tokyo, Japan, Sep. 2020, pp. 276–283.

N. Karimian, M. Tehrani Poor, and D. Forte, “Non-fiducial PPG-based authentication for healthcare application,” in Proc. IEEE IEMBS Health Inform. (BHI), Orlando, FL, USA, Feb. 2017, pp. 429–432.

S.-W. Lee, D.-K. Woo, Y.-K. Son, and P.-S. Mah, “Wearable bio-signal based personal authentication method using random forest and period setting considering the feature of PPG signals,” in Proc. 38th Annu. Int. Conf. IEEE Eng. Med. Biol. Soc. (EMBC), Orlando, FL, USA, Aug. 2016, pp. 6401–6404.

A. Fujii, K. Murao, and N. Matsuhisa, “disp2ppg: Pulse wave generation algorithm for biometric recognition with PPG signals,” Comput. Biol. Med., vol. 49, pp. 1–14, Jun. 2014.

Q. Yousef, M. B. I. Reaz, and M. A. M. Ali, “The analysis of PPG morphology: Investigating the effects of aging on arterial compliance,” Metax. Sci. Rev., vol. 12, no. 6, pp. 266–271, Dec. 2012.

A. Fuji, K. Murao, and N. Matsuhisa, “disp2ppg: Pulse wave generation to PPG sensor using display,” in Proc. ACM Int. Symp. Wearable Comput. (ISWC) Sep. 2021, pp. 119–123.

SHUN HINATSU received the M.S. degree from Osaka University, Japan, in 2017, where he is currently pursuing the Ph.D. degree with the Graduate School of Engineering Science. In 2017, he joined Mitsubishi Electric Corporation, Japan. His research interests include biomedical instrumentation and biometric authentication.

DAISUKE SUZUKI received the Ph.D. degree from Keio University, in 2016. He was an Assistant Professor with the 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 implementation of cryptosystems. He is a member of the Institute of Electronics, Information and Communication Engineers.

HIROKI ISHIZUKA received the Ph.D. degree from Keio University, in 2016. He was an Assistant Professor with the Department 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, and ACM.

SEI IKEDA (Member, IEEE) 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, 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, and ACM.

OSAMU OSIRO 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, and biomedical signal processing. He is a member of the Japanese Society for Medical and Biological Engineering, the Institute of Electronics, Information and Communication Engineers, the Institute of Systems, Control and Information Engineers, and the Virtual Reality Society of Japan.

* * *