2021 43rd Annual International Conference of the
IEEE Engineering in Medicine & Biology Society (EMBC)
Oct 31 - Nov 4, 2021. Virtual Conference

Attack on PPG Biometrics: Presentation Attack by Stealth Recording and Waveform Estimation

Shun Hinatsu[1,2], Daisuke Suzuki[1], Hiroki Ishizuka[2], Sei Ikeda[2], and Osamu Oshiro[2]

Abstract— **To develop a photoplethysmogram (PPG)-based authentication system with countermeasures, we investigate a "presentation attack" against the authentication. The attack uses the PPG for performing measurements on various sites on each subject's body. It records PPG on a nongenuine measurement site stealthily, generates a spoofing signal based on the recorded PPG, and transmits the signal to the authentication device. To investigate the feasibility of the attack, we developed a PPG-based authentication system. We recorded the PPGs of the subjects' bodies using the developed system and investigated the feasibility of attack in the experiment. The results indicated that an attack can occur with a probability of more than 80 % under ideal conditions.**

I. INTRODUCTION

A photoplethysmogram (PPG) is a noninvasive circulatory signal related to blood volume in the tissue [1]. It contains various types of information, such as arterial expansion and contraction with each heartbeat, oxygen saturation, venous flow, and respiration, which are used for various purposes such as estimation of heart rate (HR) and respiratory rate (RR) for healthcare monitoring [2], [3]. A PPG can be recorded using a sensor that comprises a typical light-emitting diode (LED) that illuminates the tissue and a phototransistor (PTr) that senses variations in the intensity of the reflected or transmitted light associated with changes in the blood volume [2]. The advantage of a PPG is that its measurements can be performed on various sites such as the fingertip, proximal part of the finger, and wrist using only one sensor. It is often an alternative to the electrocardiogram (ECG) for the estimation of HR because it can be recorded under fewer restrictions [3]. Certain recent studies have estimated human activities based on PPGs recorded through devices wearable on the proximal part of the finger or wrist to realize several applications such as user interfaces [4], [5].

In addition, the PPG has also been applied to biometric authentication owing to features such as high distinctiveness and difficulty in replication [6]. Because PPG sensors have been installed in several smartwatches for healthcare applications, smartwatches may provide a PPG-based authentication function in the near future. If PPG-based authentication is available, it will be possible to seamlessly connect authentication with applications. For example, a smartwatch can provide healthcare applications after PPG-based authentication using only one sensor.

[1]Shun Hinatsu and Daisuke Suzuki are with Mitsubishi Electric Corporation, 5-1-1 Ofuna Kamakura Kanagawa 247-8051, Japan, Hinatsu.Shun@bc.MitsubishiElectric.co.jp

[2]Shun Hinatsu, Hiroki Ishizuka, Sei Ikeda and Osamu Oshiro are with the Graduate School of Engineering Science, Osaka University, Japan.

However, several attack vectors against biometric authentication systems have also developed [7]. One of the vectors presents fake biometrics at the sensor of the system. It is referred to as "presentation attack (PA)", which has been demonstrated in pervasive biometric authentication. For example, certain PAs can be executed easily using commercially available products such as photographs for face recognition [8], and gummi candies for fingerprint recognition [9]. Further, PAs against ECG-based authentication and countermeasures have been proposed [6]. Therefore, in addition to other biometric authentication, the prediction of PAs against PPG-based authentication and the consideration of countermeasures against them are required.

In this paper, we propose a PA against PPG-based authentication to develop a PPG-based authentication system with countermeasures. By utilizing the advantage of the PPG in performing measurements on various sites with only one sensor, the PA stealthily records a PPG on a particular site on a victim's body, which is different from the genuine measurement site used by an authentication device. Thereafter, it maps the recorded PPG onto the PPG that is recorded in a genuine measurement site and transmits the signal to the device. In this paper, the scheme of the PA is described, and its feasibility is investigated using the developed PPG-based authentication system. Furthermore, countermeasures against the PA are considered based on the investigation results.

II. METHOD

To develop an authentication system with countermeasures, we propose a PA against PPG-based authentication. The PA uses the advantage of PPG sensing, in which signals can be recorded at various sites on a subject's body.

A. Overview

Figure 1 presents an overview of the PA. The victim has a smartwatch that includes a genuine PPG sensor, wears it on the wrist every day, and often logs into applications such as healthcare monitoring and message exchange using personal information after PPG-based authentication. The attacker intends to steal the victim's personal information through the PA, which is executed as follows:

- Install a malicious PPG sensor on certain daily necessities or office supplies, which the victim may touch with the finger without noticing the sensor (**Step 1**).
- Record the victim's PPG stealthily using a malicious PPG sensor (**Step 2**).
- Generate the electrical signal or control the light intensity based on the recorded signal (**Step 3**).

978-1-7281-1178-0/21/$31.00 ©2021 IEEE

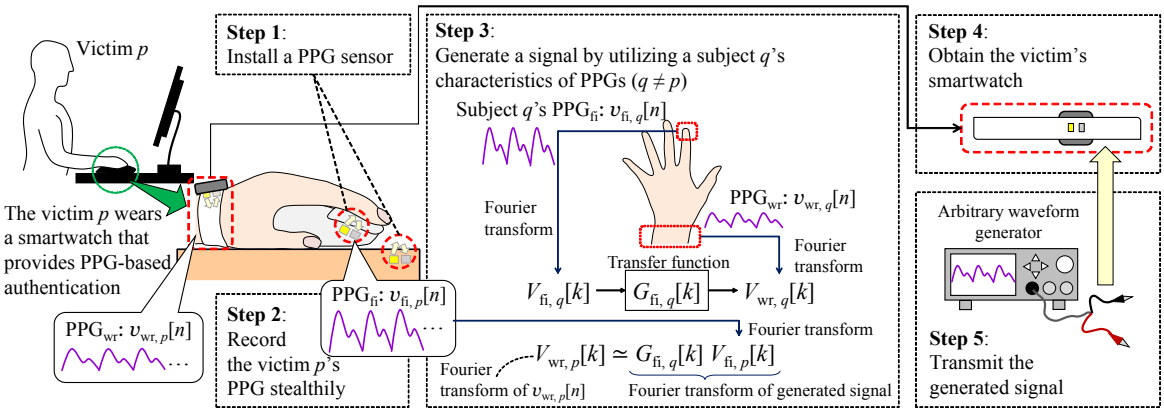

Fig. 1. Overview of the proposed PA. Boxes with dashed line describe the attacker's scheme.

- Obtain the victim's smartwatch after he/she removes it for charging the battery and so on and keeps it in a place where the attacker can access it (**Step 4**).
- Transmit the signal to the PPG sensor installed on the smartwatch to break its authentication (**Step 5**).

B. Waveform Estimation

When the attacker generates a signal in **Step 3**, he/she can use the recorded PPG to transmit to the smartwatch in **Step 5**. However, the attacker may map the PPG onto the other waveform to estimate the PPG recorded by the smartwatch because there are differences in PPG waveforms recorded at different measurement sites. Certain previous studies indicated that an arterial blood pressure (ABP) waveform is similar to a PPG waveform. They proposed a method to estimate the ABP waveform from the PPG using a transfer function (TF) between them [10]. However, there are also similarities between PPGs recorded at different measurement sites [11]. Therefore, to estimate the PPG waveform recorded by the smartwatch, we assume that there is a TF between two PPGs recorded at different measurement sites. The TF of each subject may be different from that of another; however, the TFs may also have the same characteristics based on the tendencies in the PPG waveforms recorded at different measurement sites. For example, the amplitude of the PPG recorded on the wrist tends to be less than that of the PPG recorded on the finger [11]. Therefore, using the TF of another subject, the attacker may estimate the victim's PPG waveform recorded on the wrist through the smartwatch and use it for the PA.

In this paper, to estimate the PPG$_{\mathrm{wr}}$ for the victim p, we assume that there is a TF between the PPGs recorded on the fingertip (PPG$_{\mathrm{fi}}$) and wrist (PPG$_{\mathrm{wr}}$), as illustrated in Fig. 1. The PPG$_{\mathrm{fi}}$ for victim p is recorded stealthily by the attacker. In addition, we assume a time-invariant system for each subject, whose input and output are PPG$_{\mathrm{fi}}$ and PPG$_{\mathrm{wr}}$, respectively. The TF of the subject q is defined as follows ($p \neq q$) [12]:

$$G_{\mathrm{fi},q}[k] = \frac{V_{\mathrm{wr},q}[k]}{V_{\mathrm{fi},q}[k]}, \tag{1}$$

where k, $V_{\mathrm{wr},q}[k]$, and $V_{\mathrm{fi},q}[k]$ denote the discrete frequency and the Fourier transforms of PPG$_{\mathrm{wr}}$ $v_{\mathrm{wr},q}[n]$ and PPG$_{\mathrm{fi}}$ $v_{\mathrm{fi},q}[n]$ for subject q, respectively (n denotes the discrete time). If we consider the same characteristics of the TF, we can assume that $G_{\mathrm{fi},p}[k] \simeq G_{\mathrm{fi},q}[k]$, where $G_{\mathrm{fi},p}[k]$ denotes the TF for the victim p. Therefore, the Fourier transform of PPG$_{\mathrm{wr}}$ $v_{\mathrm{wr},p}[n]$ for victim p can be calculated as follows:

$$\begin{aligned} V_{\mathrm{wr},p}[k] &= G_{\mathrm{fi},p}[k] V_{\mathrm{fi},p}[k] \\ &\simeq G_{\mathrm{fi},q}[k] V_{\mathrm{fi},p}[k], \end{aligned} \tag{2}$$

where $V_{\mathrm{fi},p}[k]$ denotes the Fourier transform of PPG$_{\mathrm{fi}}$ $v_{\mathrm{fi},p}[n]$ for victim p. Following a similar procedure, $V_{\mathrm{wr},p}[k]$ can also be calculated using a PPG recorded on the proximal part of the finger (PPG$_{\mathrm{pr}}$) as follows:

$$V_{\mathrm{wr},p}[k] \simeq G_{\mathrm{pr},q}[k] V_{\mathrm{pr},p}[k], \tag{3}$$

where $G_{\mathrm{pr},q}[k]$ and $V_{\mathrm{pr},p}[k]$ denote the TF between PPG$_{\mathrm{pr}}$ and PPG$_{\mathrm{wr}}$ for subject q and the Fourier transform of PPG$_{\mathrm{pr}}$ for victim p. The attacker can estimate PPG$_{\mathrm{wr}}$ $v_{\mathrm{wr},p}[n]$ for victim p by calculating the inverse Fourier transform of $V_{\mathrm{wr},p}[k]$ and transmit it to the authentication device.

III. EXPERIMENT

To investigate the feasibility of the proposed PA, we developed a PPG-based authentication system comprising a PPG sensing device and an authentication algorithm. We conducted an experiment using this system.

A. Experimental Setup

The PPG sensing device in the developed PPG-based authentication system includes three sensors consisting of an LED and a PTr (New Japan Radio Co., Ltd., NJL5303R-TE1). The emitting peak of the LED is at a wavelength of 570 nm. The sensors are fastened on the wrist, fingertip and proximal part of the index finger using the Velcro tape to record the PPG as stably as possible, as illustrated in Fig. 2. 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 [13]. Then, the signal was amplified using a non-inverting amplifier with a gain of 47 dB, and a sampling rate of 1 kHz with a resolution of 16 bits was recorded using an AD converter (National Instruments, USB-6216).

The recorded signals were processed using an authentication algorithm based on the PPG-based identification algorithm proposed by Jindal et al. [14]. The signal was standardized to have a mean of zero and a standard deviation of 1, and segmented to extract feature values from every period of the PPG. Then, 11 feature values, such as the maximum value, were extracted from each segment. Subsequently, the algorithm identifies subjects by inputting the feature values to a multilayer perceptron (MLP) as a classifier. The MLP includes three hidden layers consisting of 40, 40, and 10 nodes. To authenticate a subject as genuine or as an impostor, we set a threshold (TH) for the predicted probability that decides the subject identified by the MLP. TH was set to equalize the false rejection rate (FRR) and false acceptance rate (FAR) to obtain an equal error rate (ERR) [15].

B. Experimental Procedure

We recorded PPGs from five healthy male participants aged between 26 and 29 years (subject S1, S2, ..., S5) in the experiment. They wore the PPG sensors on three measurement sites and maintained a resting state for 30 s while their PPGs were being recorded. Five recordings (trial T1, T2, ..., T5) were obtained from three measurement sites for each participant. The experiment was approved by the Ethical Committee of Information Technology R&D Center (2020-B001), Mitsubishi Electric Corporation, Japan.

Before the evaluation of the PA, the MLP was generated by the feature values extracted from each subject's $\mathrm{PPG_{wr}}$ of one recording (T1). Then, the accuracy was computed for the identification performance as follows:

$$\text{Accuracy} = \frac{\mathrm{TP} + \mathrm{TN}}{\mathrm{TP} + \mathrm{TN} + \mathrm{FP} + \mathrm{FN}}, \tag{4}$$

where TP, TN, FP, and FN are defined as true positive, true negative, false positive, and false negative, respectively. This calculation is performed through leave-one-out cross validation, which uses all segments except one for training, uses the remaining one for testing, and repeats this process based on the number of segments. The PA was then investigated by inputting the feature values extracted from $\mathrm{PPG_{fi}}$ and $\mathrm{PPG_{pr}}$ to the MLP rather than transmitting the signal to the sensor. In addition, we mapped $\mathrm{PPG_{fi}}$ and $\mathrm{PPG_{pr}}$ onto the estimated $\mathrm{PPG_{wr}}$ ($\mathrm{PPG^{fi}_{wr}}$ and $\mathrm{PPG^{pr}_{wr}}$, respectively) using the other subject's TF, and input the feature values extracted from the signals to the MLP. We defined "success segment" as the segment authenticated as the subject correctly and "success trial" as the trial that included at least one success segment to evaluate the PA, assuming that the attacker continued to transmit the signal until they were successful. We also calculated success rate (SR), which is defined as follows:

$$\mathrm{SR} = T_{\mathrm{suc}} \,/\, T, \tag{5}$$

where T_{suc} and T denote the number of success trials and total number of trials, respectively.

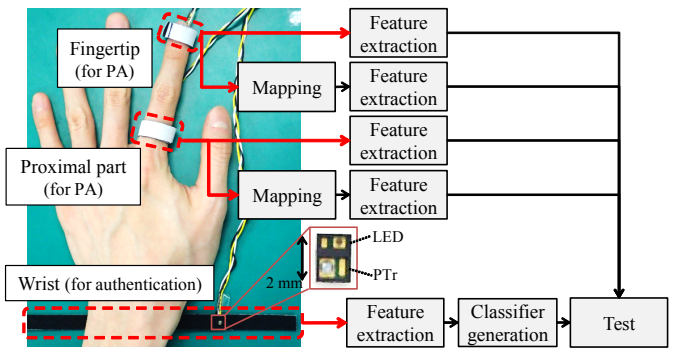

Fig. 2. Experimental setup and procedure.

C. Results and Discussion

Figure 3 presents a portion of the PPGs recorded simultaneously at three measurement sites on a subject's body (S2, T3) at the same time. We computed the accuracy (0.910) using $\mathrm{PPG_{wr}}$, and TH = 0.469 when FRR = FAR (EER = 0.146). Table I presents the results of the PA. The check marks before the slashes indicate the success trials using $\mathrm{PPG_{fi}}$ and $\mathrm{PPG_{pr}}$, and the check marks after the slashes indicate the success trial by utilizing $\mathrm{PPG^{fi}_{wr}}$ and $\mathrm{PPG^{pr}_{wr}}$ computed using the TF generated from the PPGs for S5 in T4. The shaded cells indicate the trials in which the PA failed by using $\mathrm{PPG_{fi}}$ and $\mathrm{PPG_{pr}}$. By utilizing $\mathrm{PPG_{fi}}$ and $\mathrm{PPG_{pr}}$, we calculated SR = 0.920 and 0.840, respectively. If we calculate these except for S5's trials used for TF generation, we would obtain $\mathrm{SR_{tr}}$ = 0.900, 0.800, respectively. Using $\mathrm{PPG^{fi}_{wr}}$ and $\mathrm{PPG^{pr}_{wr}}$, we calculated SR = 1.000, 0.950, respectively. Figure 4 presents examples of waveform estimation.

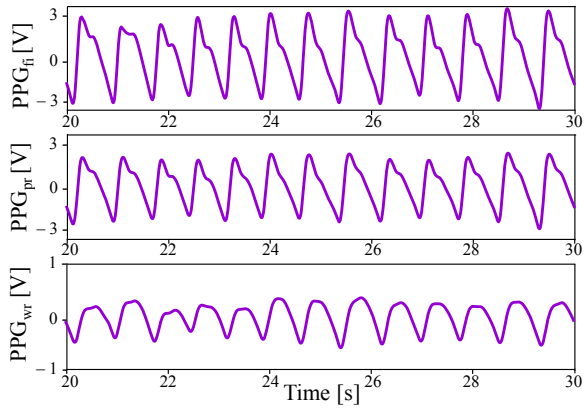

Fig. 3. Example of PPGs recorded on three sites at same time.

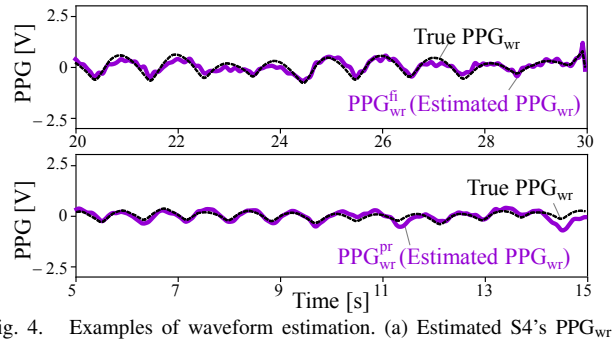

Fig. 4. Examples of waveform estimation. (a) Estimated S4's $\mathrm{PPG_{wr}}$ in T5 by TF between S5's $\mathrm{PPG_{fi}}$ and $\mathrm{PPG_{wr}}$ in T2. (b) Estimated S1's $\mathrm{PPG_{wr}}$ in T4 by TF between S5's $\mathrm{PPG_{pr}}$ and $\mathrm{PPG_{wr}}$ in T4.

TABLE I

RESULT OF THE PA BASED ON THE PPGS DERIVED FROM THE FINGERTIP AND PROXIMAL PART.

Subject	Fingertip (PPG_{fi} / PPG^{fi}_{wr})					Proximal part (PPG_{pr} / PPG^{pr}_{wr})				
	T1	T2	T3	T4	T5	T1	T2	T3	T4	T5
S1	✓ / ✓	✓ / ✓	✓ / ✓	✓ / ✓	✓ / ✓	✓ / ✓	✓ / ✓	✓ / ✓	✓ / ✓	✓ / ✓
S2	✗ / ✓	✓ / ✓	✓ / ✓	✓ / ✓	✗ / ✓	✓ / ✓	✗ / ✗	✗ / ✓	✗ / ✓	✗ / ✓
S3	✓ / ✓	✓ / ✓	✓ / ✓	✓ / ✓	✓ / ✓	✓ / ✓	✓ / ✓	✓ / ✓	✓ / ✓	✓ / ✓
S4	✓ / ✓	✓ / ✓	✓ / ✓	✓ / ✓	✓ / ✓	✓ / ✓	✓ / ✓	✓ / ✓	✓ / ✓	✓ / ✓
S5	✓ / -	✓ / -	✓ / -	✓ / -	✓ / -	✓ / -	✓ / -	✓ / -	✓ / -	✓ / -

We confirmed that certain components such as the amplitudes of each waveform were different from the other; however, all the signals repeated their waveforms at nearly constant term, as illustrated in Fig. 3. We also confirmed that PPG_{wr}s tend to have smaller amplitudes, as depicted. When we mapped the signal, we found that SR was higher than 0.800, and FRR = FAR = 0.146. Although the mapped signals PPG^{fi}_{wr} and PPG^{pr}_{wr} have high-frequency noises, as depicted in Fig. 4, we confirmed that the number of success trials and SR were improved by these in comparison with the results obtained using PPG_{fi} and PPG_{pr}.

We recruited only a small number of male subjects who do not have any cardiovascular diseases, and they wore the sensors on the body to record PPGs stably in the experiment. Other factors such as a temperature that may affect PPG waveforms [16] were not taken into consideration. In addition, we did not generate signals for the PA as explained in **Step 3** and **5**. Therefore, it is required to recruit a larger number of diverse subjects, and conduct experiments under more various conditions to ensure the results. However, countermeasures against the PA should be considered because the results suggested that the PA can occur. One of the countermeasures is typical replay attack prevention, such as using one-time information in the authentication protocol [17]. Because the PA sends artificial signals to the sensor, it is also effective to add liveness detection techniques, such as a humidity sensor, to recognize the object of measurement as a human body. In addition, it may be effective to use unique information about the measurement site from the PPG. For example, using the dicrotic notch in each PPG segment as a feature value may contribute to the countermeasure, which is difficult to stably extract from several PPG segments [11].

IV. CONCLUSIONS

To develop a PPG-based authentication system with countermeasures, we propose a PA against PPG-based authentication. The PA uses the advantage of PPG sensing, in which signals can be recorded at different measurement sites on the subjects' body. To investigate the feasibility of the PA and consider countermeasures against it, we conducted an experiment. We recorded the PPGs on multiple measurement sites of the subjects and investigated the feasibility of the PA using the developed PPG-based authentication system. We found that the PA succeeded with an SR of more than 80 % under the condition that the sensors were stabilized on all measurement sites. We conclude that PA can occur under ideal attacking conditions and countermeasures such as replay attack prevention are required.

REFERENCES

[1] A. Reisner, P. A. Shaltis, D. McCombie, H. H. Asada, D. S. Warner, and M. A. Warner. Utility of the photoplethysmogram in circulatory monitoring. *The Journal of the American Society of Anesthesiologists*, Vol. 108, No. 5, pp. 950–958, 2008.

[2] Y. Sun and N. Thakor. Photoplethysmography revisited: from contact to noncontact, from point to imaging. *IEEE Transactions on Biomedical Engineering*, Vol. 63, No. 3, pp. 463–477, 2015.

[3] M. A. F. 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 Transactions on Biomedical Engineering*, Vol. 64, No. 8, pp. 1914–1923, 2016.

[4] S. Yoshimoto, S. Hinatsu, Y. Kuroda, and O. Oshiro. Hemodynamic sensing of 3-d fingertip force by using nonpulsatile and pulsatile signals in the proximal part. *IEEE transactions on biomedical circuits and systems*, Vol. 12, No. 5, pp. 1155–1164, 2018.

[5] T. Buddhika, H. Zhang, S. W. T. Chan, V. Dissanayake, S. Nanayakkara, and R. Zimmermann. fsense: Unlocking the dimension of force for gestural interactions using smartwatch ppg sensor. In *Proceedings of the 10th Augmented Human International Conference 2019*, pp. 1–5, 2019.

[6] N. Karimian, D. Woodard, and D. Forte. Ecg biometric: Spoofing and countermeasures. *IEEE Transactions on Biometrics, Behavior, and Identity Science*, Vol. 2, No. 3, pp. 257–270, 2020.

[7] N. K. Ratha, J. H. Connell, and R. M. Bolle. An analysis of minutiae matching strength. In *International Conference on Audio-and Video-Based Biometric Person Authentication*, pp. 223–228. Springer, 2001.

[8] R. Ramachandra and C. Busch. Presentation attack detection methods for face recognition systems: A comprehensive survey. *ACM Computing Surveys (CSUR)*, Vol. 50, No. 1, pp. 1–37, 2017.

[9] C. Sousedik and C. Busch. Presentation attack detection methods for fingerprint recognition systems: a survey. *Iet Biometrics*, Vol. 3, No. 4, pp. 219–233, 2014.

[10] A. Dash, N. Ghosh, A. Patra, and A. D. Choudhury. Estimation of arterial blood pressure waveform from photoplethysmogram signal using linear transfer function approach. In *2020 42nd Annual International Conference of the IEEE Engineering in Medicine & Biology Society (EMBC)*, pp. 2691–2694. IEEE, 2020.

[11] V. Hartmann, H. Liu, F. Chen, Q. Qiu, S. Hughes, and D. Zheng. Quantitative comparison of photoplethysmographic waveform characteristics: effect of measurement site. *Frontiers in physiology*, Vol. 10, pp. 1–8, 2019.

[12] S. Mahto, T. Arakawa, and T. Koshinak. Ear acoustic biometrics using inaudible signals and its application to continuous user authentication. In *2018 26th European Signal Processing Conference (EUSIPCO)*, pp. 1407–1411. IEEE, 2018.

[13] M. R. Ram, K. V. Madhav, E. H. Krishna, N. R. Komalla, and K. A. Reddy. A novel approach for motion artifact reduction in ppg signals based on as-lms adaptive filter. *IEEE Transactions on Instrumentation and Measurement*, Vol. 61, No. 5, pp. 1445–1457, 2011.

[14] V. Jindal, J. Birjandtalab, M. B. Pouyan, and M. Nourani. An adaptive deep learning approach for ppg-based identification. In *2016 38th Annual international conference of the IEEE engineering in medicine and biology society (EMBC)*, pp. 6401–6404. IEEE, 2016.

[15] J. Malik, D. Girdhar, R. Dahiya, and G. Sainarayanan. Reference threshold calculation for biometric authentication. *IJ Image, Graphics and Signal Processing*, Vol. 2, pp. 46–53, 2014.

[16] M. Khan, C. G. Pretty, A. C. Amies, R. Elliott, G. M. Shaw, and J. G. Chase. Investigating the effects of temperature on photoplethysmography. *IFAC-PapersOnLine*, Vol. 48, No. 20, pp. 360–365, 2015.

[17] Y. Ueshige and K. Sakurai. A proposal of one-time biometric authentication. In *Security and Management*, pp. 78–83. Citeseer, 2006.