electronics

Article

Fake Biometric Detection Based on Photoplethysmography Extracted from Short Hand Videos

Byeongseon An [1,†], Hyeji Lim [1,†] and Eui Chul Lee [2,*]

[1] Department of AI & Informatics, Graduate School, Sangmyung University, Hongjimun 2-Gil 20, Jongno-Gu, Seoul 03016, Republic of Korea; 202232033@sangmyung.kr (B.A.); 202232034@sangmyung.kr (H.L.)
[2] Department of Human-Centered Artificial Intelligence, Sangmyung University, Hongjimun 2-Gil 20, Jongno-Gu, Seoul 03016, Republic of Korea
[*] Correspondence: eclee@smu.ac.kr
[†] These authors contributed equally to this work.

Abstract: An array of authentication methods has emerged, underscoring the importance of addressing spoofing challenges arising from forgery and alteration. Previous studies utilizing palm biometrics have attempted to circumvent spoofing through geometric methods or the analysis of vein images. However, these approaches are inadequate when faced with hand-printed photographs or in the absence of near-infrared sensors. In this study, we propose using remote photoplethysmography (rPPG) signals to tackle spoofing concerns in palm images captured in RGB environments. rPPG signals were extracted using video durations of 3, 5, and 7 s, and 30 features within the heart rate band were identified through frequency conversion. A support vector machine (SVM) model was trained with the processed features, yielding accuracies of 97.16%, 98.4%, and 97.28% for video durations of 3, 5, and 7 s, respectively. These features underwent dimensionality reduction through a principal component analysis (PCA), and the results were compared with the initial 30 features. Additionally, we evaluated the confusion matrix with zero false-positives for each video duration, finding that the overall accuracy experienced a decline of 1 to 3%. The 5 s video retained the highest accuracy with the smallest decrement, registering a value of 97.2%.

Keywords: anti-spoofing; hand biometrics; remote photoplethysmogram; printed hand; support vector machine

Citation: An, B.; Lim, H.; Lee, E.C. Fake Biometric Detection Based on Photoplethysmography Extracted from Short Hand Videos. *Electronics* **2023**, *12*, 3605. https://doi.org/10.3390/electronics12173605

Academic Editor: Gongping Yang

Received: 8 August 2023
Revised: 24 August 2023
Accepted: 24 August 2023
Published: 26 August 2023

1. Introduction

Biometric authentication, a longstanding method for verifying user identity, employs various anatomical features such as palms, irises, fingerprints, veins, and facial structures [1]. The human hand, in particular, possesses multiple attributes suitable for biometric authentication. Among these, palm prints and geometrics serve as the primary visible characteristics, while palm vein patterns function as an invisible feature. Similar to fingerprints, palm prints are distinct for each individual and derived from unique skin patterns. As an additional advantage, both low-resolution imaging and cost-effective capture devices can be utilized for palm print analysis [2]. The geometric features of the hand encompass all visible characteristics, including finger shape and joints as well as palm shape and size. These attributes are typically combined with other biometric measures to enhance authentication accuracy [3]. Palm vein patterns, known for their high precision in authentication, act as a distinct unit and are resistant to spoofing. These patterns are identified through the analysis of specific regions in palm infrared images [4]. However, authentication methods employing geometrics and palm prints may be vulnerable to compromise, while those utilizing palm vein patterns necessitate supplementary infrared equipment. Despite the absence of tampering and equipment concerns, conventional biometric authentication methods involving palm features remain susceptible to spoofing attacks [5,6]. Thus, robust anti-spoofing techniques are essential in combination with forgery and alteration resilience, as well as equipment accessibility. Recently, facial recognition, an alternative biometric authentication approach, has employed remote photoplethysmography (rPPG) technology to bolster anti-spoofing measures, demonstrating high accuracy [7]. rPPG extracts heart rate information from skin color differences observed through camera imaging, eliminating the need for additional wearable equipment by utilizing an RGB camera alone [8]. Moreover, as rPPG relies on heartbeat signals, the risk of damage is minimal. This presents the possibility of applying heart rate information derived from rPPG to palm print authentication methods. Consequently, this study examines the use of palm rPPG signals in an RGB environment, demonstrating that palm rPPG signals offer a spoof-resistant authentication solution and proposing a novel approach for palm biometric authentication. Figure 1 illustrates the method proposed in this study.

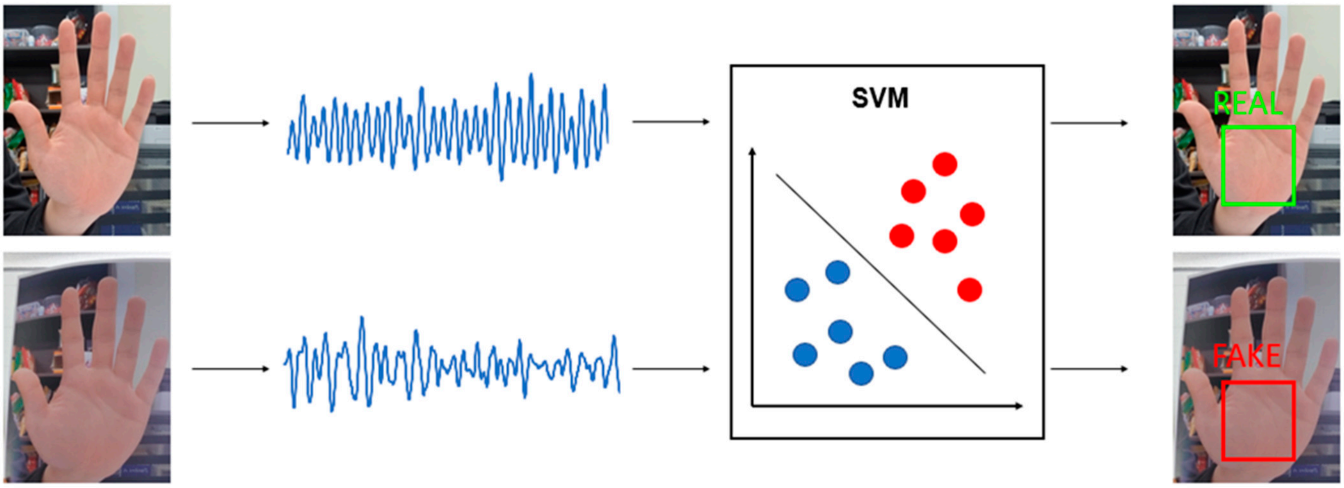


Figure 1. Diagram of the method proposed in this study. Using the rPPG signal extracted from the hand, real and fake palms are classified through the use of a support vector machine (SVM).

2. Related Works

Previous research on spoofing detection for hand biometrics related to the proposed method can be categorized into two categories. As shown in Table 1, these include methods that use human physical characteristics and methods based on image quality.

Hong Chen et al., 2005 utilized plaster and paper cards to fabricate artificial hand silhouettes, which were employed in experiments conducted with the HandKey II system. Specifically, five artificial hands with geometric features were utilized for testing [5]. However, it is important to note that the reliability of their findings was limited due to the utilization of a small dataset. In contrast, our research aims to enhance the reliability of the model's performance by employing a larger dataset consisting of 138 samples of real palm data and 124 samples of artificial palm data. Furthermore, our study overcomes potential limitations associated with the geometric approach, where performance may be compromised when encountering swollen hands or obscured hand regions. By focusing on bio-signals extracted from the hand rather than relying solely on hand geometry, our approach enables the detection of spoofing attempts independent of hand shape.

Haixia Wang et al., 2023 proposed a novel dual-wavelength synchronization acquisition system tailored for palm biometrics. The study demonstrated the system's capability to accurately extract SpO2 and pulse rate from palm fingerprint and palm vein images. Moreover, it was established that the integration of SpO2 and pulse rate significantly enhances the anti-counterfeiting effectiveness of palm biometrics. To investigate the system's performance, artificial palm prints and artificial palm veins were fabricated by utilizing diverse materials. Objects were classified as genuine when the SpO2 readings fell within the range of 70% to 100%, and similarly, objects were categorized as genuine when the pulse rate ranged between 40 and 200. The PPG signal was processed using a residual network, and a classification approach was employed, with the train and test data split in a ratio of 4:1 to enable cross-validation. Leveraging the dynamic function, a three-layer anti-spoofing strategy was devised, ensuring the preservation of palm biometric recognition capabilities while achieving robust anti-spoofing functionality without necessitating additional hardware [9]. In contrast with this study's approach, where SpO2 and pulse rate were employed, our research focuses solely on the rPPG signal for spoofing detection. This simplification of the algorithm yielded comparable accuracy results. Furthermore, palm vein image acquisition devices, which operate in the NIR spectrum, can be costly. In contrast, our study presents the advantage of conveniently detecting spoofing without the need for a separate NIR device, as it effectively utilizes an RGB camera.

Table 1. Previous studies on anti-spoofing categorized by human physical characteristics and image-quality-based features.

Method	Author	Summary	Limitation
Using human physical characteristics	Hong Chen et al. [5]	Using gypsum and silhouette images to create a fake hand, revealing that the hand geometry system is insensitive to changes in hand thickness	Low reliability of results due to the small amount of data used
	Haixia Wang et al. [9]	Proposed three-layer anti-spoofing strategy for spoofing detection using PPG, SpO2, and pulse rate	As it uses dual-wavelength signals, an infrared camera as well as an RGB camera are required
	Our proposed method	After rPPG signal extraction, a PCA application and an SVM classifier are used	Image acquisition time and noise to features caused by hand movement
Using image-quality-based features	Vivek Kanhangad et al. [10]	Using a SVM after extracting features using local texture pattern analysis	In the case of LBP, it has not been used recently because it is vulnerable to noise or lighting changes.
	Vivek Kanhangad et al. [11]	Presents an approach to detecting display- and print-based spoofing attacks	It is sensitive to the external environment because surface reflectance is used to extract features.
	Asish Bera et al. [12]	Presenting the PAD (presentation attack detection) method using visual quality evaluation	Using artificially generated noise for fake hands
	Xiaoming Li et al. [13]	Based on binarized statistical image function (BSIF) and image quality assessment	Not available at high resolution as the feature is used in which the fake hand data have less detail than the real hand data
	P. Pravallika et al. [14]	Using SVM classifiers based on quality differences, such as pixel differences and edge-based measurements, via IQM	Proceed with the assumption that the quality of the fake image will be different from the quality of the real image
	Mina Farmanbar et al. [15]	Based on a fusion of different texture-based and IQA-based methods to counter both printed photo attacks and reproduced video attacks	If there is physical damage to the palm print, it is fatal to the performance

The method presented in this study exhibits robustness against various sources of noise, including artifacts worn on the hand, due to its independence from the hand's geometric characteristics. Moreover, by solely utilizing the features extracted from the rPPG signal within the palm's region of interest (ROI), our technique offers simplicity compared to complex bio-signal-based anti-spoofing methods while demonstrating comparable or superior performance.

Vivek Kanhangad et al., 2013 introduced a methodology aimed at safeguarding a palmprint-based biometric system against spoofing attacks by utilizing human hand photos. The proposed approach employed a local texture pattern analysis to extract palm print features. Specifically, a local binary pattern (LBP) was utilized to train a classifier responsible for determining the authenticity of an input hand image, distinguishing between real and fake palms. Support vector machines (SVMs) served as the classification model. The study employed a dataset consisting of 611 samples from 100 subjects, achieving an impressive accuracy rate of 97.35% [10]. While LBP has exhibited limitations in scenarios involving uniform brightness or susceptibility to noise and lighting variations, its usage has declined in recent times. However, our proposed methodology overcomes these challenges by leveraging bio-signals instead of relying solely on hand feature extraction, thereby offering a viable solution to address these issues.

Vivek Kanhangad et al., 2015 introduced a novel approach for the detection of display- and print-based spoofing attacks targeting palm print authentication systems. The study specifically focused on two distinct categories of sensor-level attacks, namely print-based and display-based attacks. The analysis of acquired hand images was conducted to estimate surface reflectance, and the feature set was constructed using first- and higher-order statistical features derived from the distribution of pixel intensities and sub-band wavelet coefficients. A trained binary classifier leveraged the identification information to discern between genuine and fake hand images. The study utilized a dataset consisting of 1300 samples obtained from 230 subjects. The results demonstrated a spoof acceptance rate of 79.8% when presented with a counterfeit digital or printed copy, and the proposed approach consistently achieved an average 10-fold cross-validation classification accuracy of above 99% [11]. It is noteworthy that while the extraction of surface reflectance served as the basis for feature extraction in the referenced paper, our research diverges in the utilization of rPPG bio-signals extracted from the hand. If a bio-signal is used, spoofing can be detected by being less sensitive to external factors.

Asish Bera et al., 2021 introduced a presentation attack detection (PAD) method that employs visual quality evaluation to mitigate illicit attempts on hand biometric systems. In their study, the hand images of 255 subjects were genuine samples, and counterfeit images were obtained by capturing images using a Canon EOS 700D camera for each authentic sample. Additionally, artificial, fake images were created by introducing Gaussian blur and noise to the original images. A threshold-based gradient size similarity quality metric was proposed, taking into account the intensity variation between adjacent pixels, to differentiate real hands from fake hands. Classification experiments were conducted, utilizing k-nearest neighbors, random forests, support vector machine classifiers, and deep convolutional neural networks. Notably, an average classification error of 1.5% was achieved using the k-nearest neighbors and random forest classifiers [12]. Since this paper uses artificially created noise from real hand data for fake hands, if spoofing is attempted in a method other than noise, such as using a printed hand photo, fake data may not be identified. In our case, this problem does not occur because the extracted bio-signal is used.

Xiaoming Li et al., 2015 proposed a novel approach leveraging binarized statistical image features (BSIFs) and image quality evaluation. The evaluation of image quality revealed that the re-captured images exhibited blurry and low-detail characteristics, thus making palm print a suitable feature due to its ability to provide more textural information compared to the original image features. Data collection was carried out using iPhone 5 and iPhone 5s devices. The BSIFs calculated binary codes for each pixel using a filter, and the filter's base vector was learned from natural images through an independent component analysis. An SVM was employed for the learning process [13]. It should be noted that, in this case, the utilization of features indicating that fake hand data possess lower levels of detail than real hand data makes it challenging to determine high-resolution fake hand data. However, our study addresses this limitation by capturing both fake hand images and real hand images using the same device. Consequently, it becomes feasible to detect spoofing in images of comparable quality.

P. Pravallika et al., 2016 investigated the applicability of their approach to iris, face, and palm print modalities. Their study focused on liveness detection and demonstrated that biometric security can be enhanced through image quality evaluation and the fusion of diverse biometric characteristics. To discriminate between real and fake samples, LDA, QDA, and SVM classifiers were employed. Image quality evaluation was performed using FR-IAQ (21IQMs) and NIR-IQA (41QMs). The highest accuracy was achieved using an SVM with an FGR at 9.2%, an FFR at 10.1%, and an HTER at 9.65% [14]. Since the quality of the fake image is assumed to be different from the quality of the real image, spoofing detection may not work well if the quality is similar.

Mina Farmanbar et al., 2017 introduced a novel approach that combines texture-based methods with image quality evaluation metrics to mitigate spoofing attacks on face and palm prints. The texture-based methods employed in the study included LBP and HOG descriptors. For the generation of fake data, printed paper was utilized, and a dataset was collected from 50 individuals. Seven image quality features were employed, namely one-peak signal-to-noise ratio, structural similarity, mean squared error, normalized cross-correlation, maximum difference, normalized absolute error, and mean difference [15]. It is worth noting that this method operates under the assumption that spoofed images exhibit distinct quality differences compared to genuine images, which can affect the performance depending on the quantity and quality of the image data used for spoofing. In contrast, our proposed approach leverages the rPPG signal extracted from the hand, which is a biological signal that is inherently difficult to manipulate, thus offering a higher level of security.

In our study, we focused on performing spoofing detection solely based on the rPPG signal, which results in reduced computational complexity compared to methods utilizing multiple image quality characteristics. By relying on the rPPG signal, our approach demonstrates consistent performance irrespective of variations in skin condition or skin type, making it suitable for daily usage scenarios.

3. Method

In this research, rPPG signals are derived from palm images collected in an RGB setting. A total of 30 features associated with heart rate are extracted from the frequency domain of the obtained signal. A principal component analysis (PCA) [16] is employed to reduce feature dimensionality, followed by a binary classification of the reduced vector values to calculate accuracy. This overall process is depicted in Figure 2. Detailed methodologies for each step are elaborated on in the subsequent sections.

3.1. Dataset

For real palm data, palm videos were collected from a total of 35 participants, consisting of 19 males and 16 females, all in their 20s and 30s. Each participant was instructed to record a one-minute video of their right and left palms using various smartphone models, utilizing the front camera. Restrictions were imposed to avoid direct sunlight or fluorescent light irradiating the camera. Aside from this constraint, no limitations were placed on the environment or palm movement during filming, offering a realistic palm recognition setting without distinguishing between moving and static scenarios. For the counterfeit palm data, authentic palm prints were captured and printed, and a one-minute video of the printed palm was recorded under similar conditions to the authentic palm videos. The video was compressed using the MPEG technique. Figure 3 illustrates the process of obtaining both real and fake videos.

Figure 4 presents examples of both genuine and fake palms, obtained as illustrated in Figure 3. Two videos were collected from each participant, one representing the left palm and the other representing the right palm. The collected dataset excluded rPPG signals when the palm was outside the frame or exposed to direct sunlight. Each 1 min video was divided according to the rPPG extraction time. Consequently, the datasets with durations of 3, 5, and 7 s comprised a total of 5289, 3122, and 2202 data points for real and fake palms, respectively.

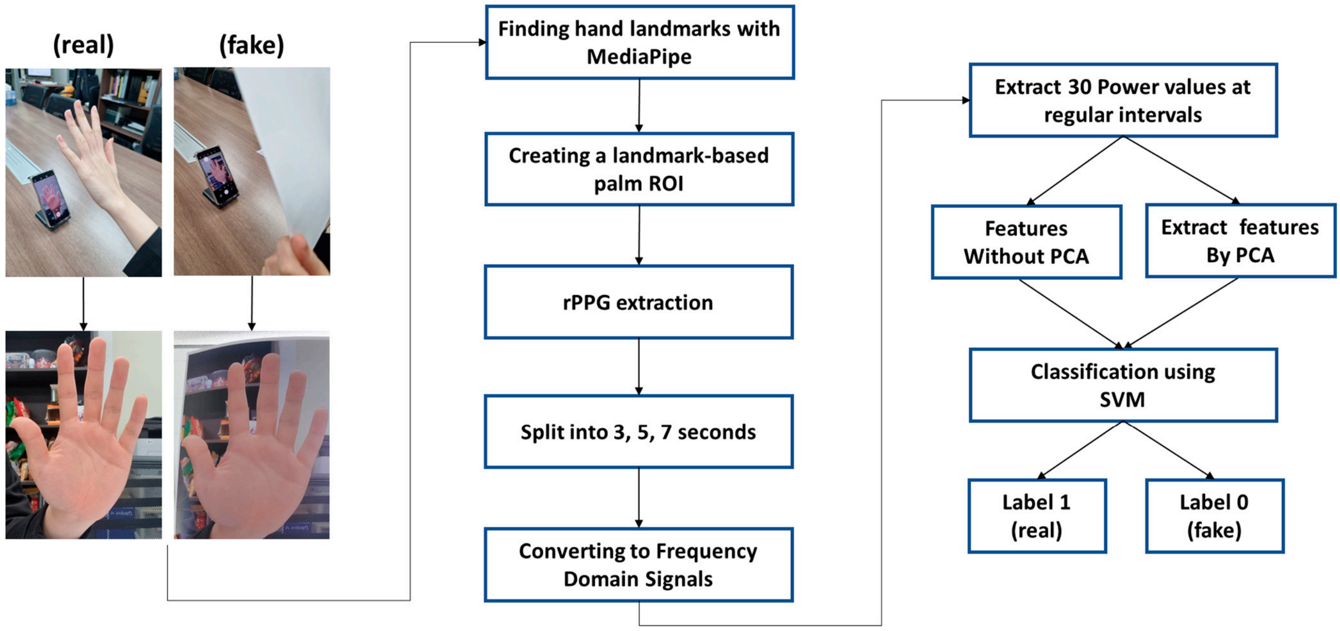

(real)
(fake)
Finding hand landmarks with MediaPipe
Creating a landmark-based palm ROI
rPPG extraction
Split into 3, 5, 7 seconds
Converting to Frequency Domain Signals
Extract 30 Power values at regular intervals
Features Without PCA
Extract features By PCA
Classification using SVM
Label 1 (real)
Label 0 (fake)

Figure 2. Anti-spoofing process through the acquisition of real and fake palm images and the classification of 30 features defined in palm rPPG signals.

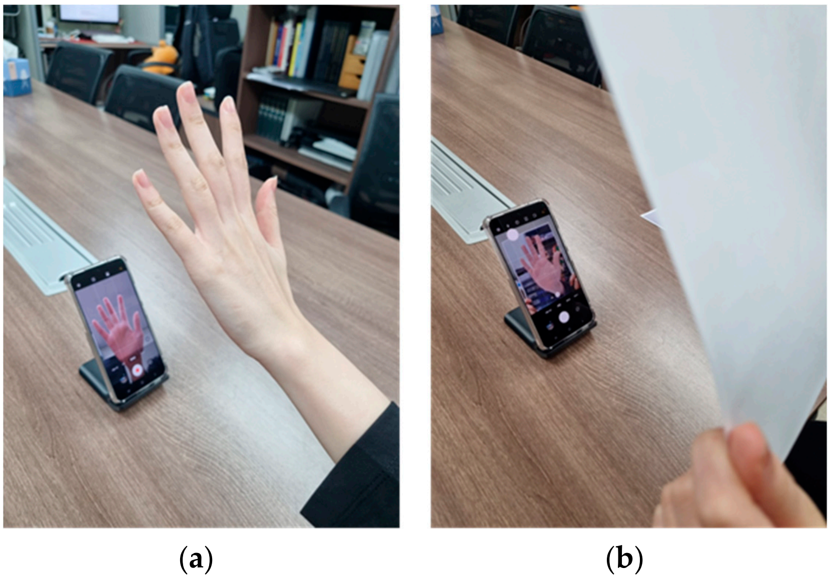


Figure 3. Example of the palm data acquisition process: (**a**) real palm data acquisition process and (**b**) fake palm data acquisition process.

3.2. rPPG Signal Acquire

In this study, we employed a technique to extract the rPPG signal from the palmar ROI region. Blood absorbs light more efficiently than surrounding tissues, resulting in fluctuating light absorption rates as blood flows through the vessels. Consequently, periodic minor skin color changes occur. The rPPG signal is obtained due to these skin color alterations. The rPPG acquisition process is conducted as follows: First, the hand is detected in an unknown frame using the MediaPipe algorithm, and the palm's region of interest (ROI) is extracted through the palm's landmark. Subsequently, skin pixel filtering is performed using the skin color range within the YCbCr color space. Pixels within the range from 133 to 177 for Cb and within the range from 77 to 127 for Cr were judged to be skin. The rPPG signal is then acquired through a color-difference-based approach.

As YCbCr is more robust to changes in skin color and environmental factors compared to obtaining signals by projecting RGB image frames onto a color map (a conventional color-difference-based method), this study involves converting RGB frames to YCbCr. The YCbCr conversion of the RGB color space is calculated as in Equation (1). R′, G′, and B′ mean normalized R, G, and B values [17].

$$\begin{gathered} \mathrm{Y} = 16 + \left(65.481 \cdot \mathrm{R}' + 128.553 \cdot \mathrm{G}' + 24.966 \cdot \mathrm{B}'\right) \\ \mathrm{Cb} = 128 + \left(-37.797 \cdot \mathrm{R}' + 74.203 \cdot \mathrm{G}' + 112.0 \cdot \mathrm{B}'\right) \\ \mathrm{Cr} = 128 + (112.0 \cdot \mathrm{R}' + 93.786 \cdot \mathrm{G}' + 18.214 \cdot \mathrm{B}') \end{gathered} \quad (1)$$

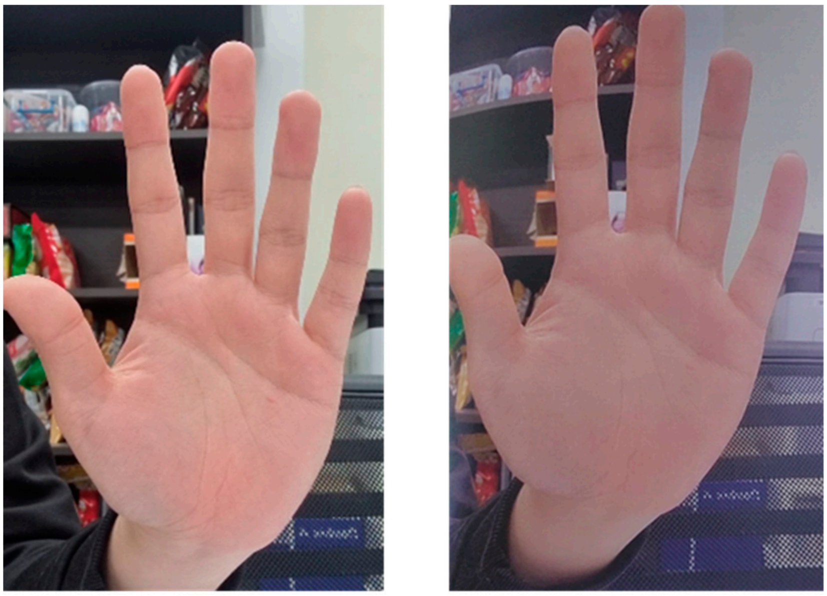

(**a**) (**b**)

Figure 4. Example of acquired palm data images: (**a**) real palm image and (**b**) fake palm image.

Skin pixels are calculated on the Cb-Cr plane. More specifically, P is defined as a pixel in the plane of Cb-Cr. The values of Cb and Cr of P extend radially n times from the central value of the cluster. At this time, n is a scale factor that determines the magnification scale. P′, which is the result of expanding P to the center of the cluster, is calculated by Equation (2) as follows:

$$\begin{aligned} Cb' &= Cbcenter \ + \ (Cb - Cbcenter) \times n \\ Cr' &= Crcenter \ + \ (Cr - Crcenter) \times n \end{aligned} \quad (2)$$

As the scale factor increases, the Cb and Cr values of some pixels may exceed the valid range of the color domain. Appropriate handling is required for a valid conversion between the two-color spaces. For this purpose, excess pixels were clipped to the nearest boundary value of the Cb-Cr plane, considering the radial direction. However, since the signal is still noisy, except for brightness values, detrending and bandpass filtering remove motion noise, such as breathing, to improve signal quality [18]. Based on this procedure, the rPPG signal for each image is obtained at the respective image's sampling rate. The rPPG extraction process is depicted in Figure 5, while the palm ROI area setup using MediaPipe is detailed in the next paragraph.

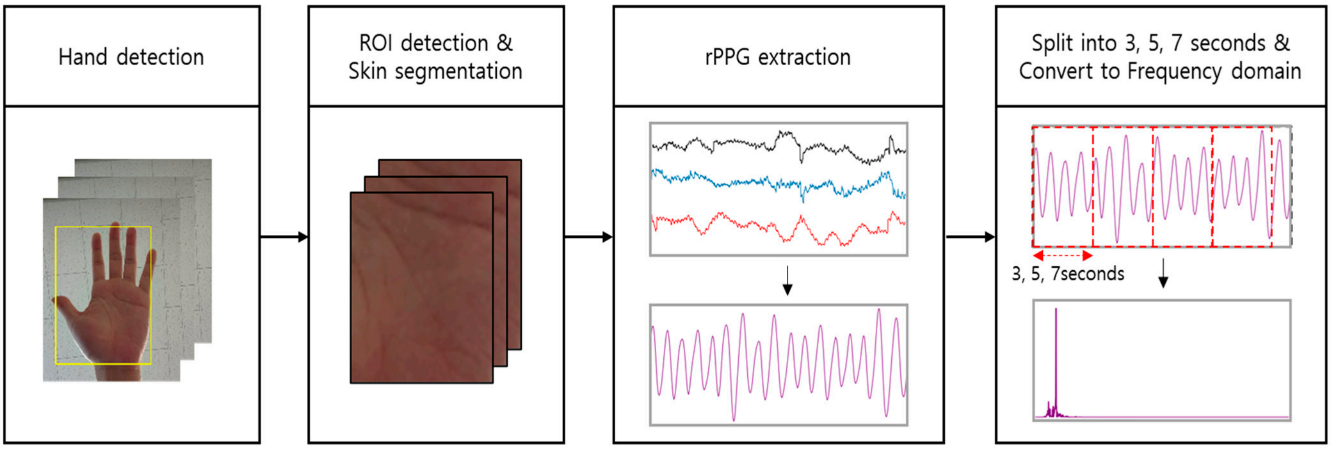

Hand detection
ROI detection & Skin segmentation
rPPG extraction
Split into 3, 5, 7 seconds & Convert to Frequency domain
3, 5, 7seconds

Figure 5. PPG signal acquisition process. After hand detection using MediaPipe, skin pixel filtering is performed based on the landmark of the palm obtained. Then, the rPPG signal is extracted, divided based on 3, 5, and 7 s, and converted into frequency bands.

Skin segmentation was employed to eliminate background noise during the processing of input hand images, enabling the extraction of the rPPG signal. However, due to the inherent nature of hands, artifacts such as items worn on fingers can be extracted from the area near the wrist and hand. Consequently, the palm was designated as the region of interest (ROI). The palm ROI assignment was based on MediaPipe [19]. As illustrated in Figure 6, the palm's ROI was determined using hand landmark numbers 17, 5, and 1, which were extracted from MediaPipe. The horizontal length of the palm's ROI was set as the distance between the x-coordinates of landmarks 17 and 5, while the vertical length was defined as the distance between the y-coordinates of landmarks 1 and 17. Figure 7 exhibits the resultant ROI obtained after extracting landmarks using MediaPipe.

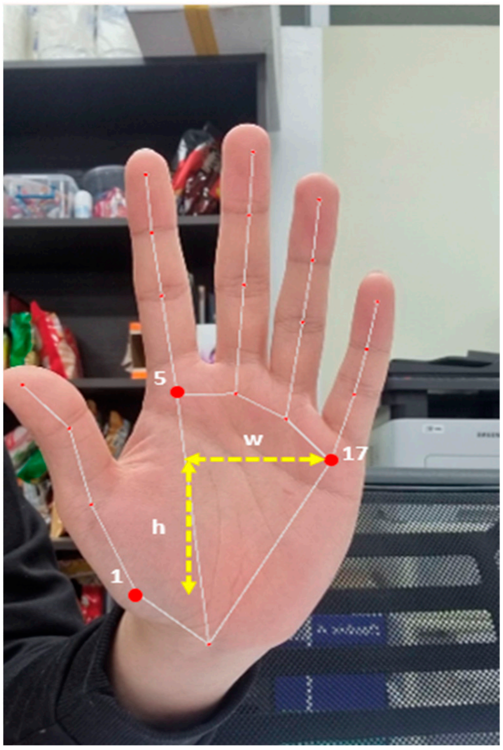


Figure 6. ROI detection method using the horizontal length (w) and vertical length (h) of the palm ROI defined using MediaPipe landmarks.

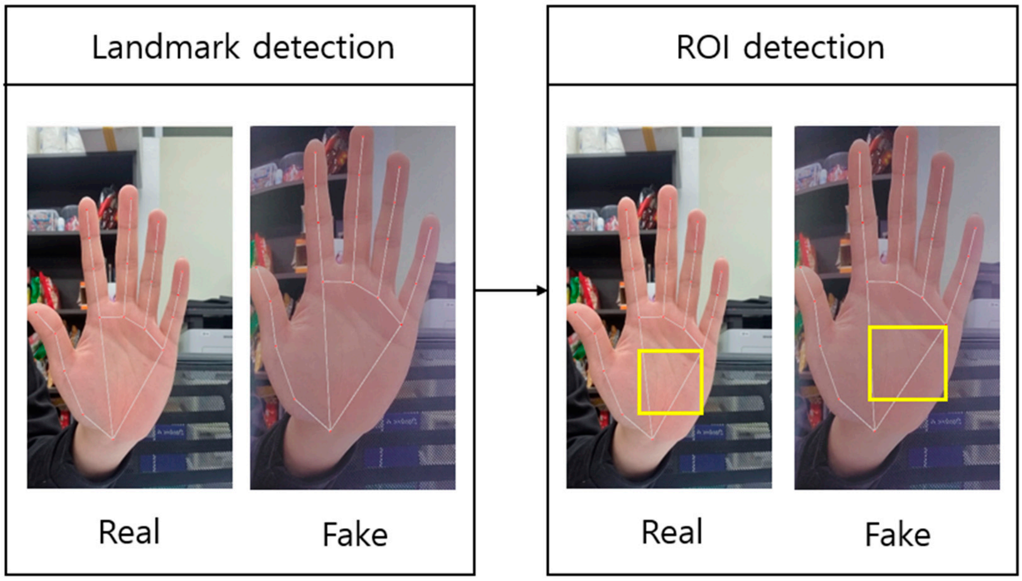


Figure 7. Setting the ROI based on MediaPipe landmarks from acquired palm images.

The above procedure was applied to both authentic and counterfeit images as a means to minimize finger artifacts and background noise. Subsequently, palmar rPPG signals were extracted from the ROI images. Bandpass filtering was conducted to identify only the wavelength range between 42 bpm and 180 bpm, which was established as the human heart rate. While extracting the rPPG signal, there may be additional physiological implications, such as motion and respiration. Therefore, noise was removed through bandpass filtering and detrending, but this part is not completely excluded. Figure 8 shows the rPPG signals of the extracted genuine and spoof images. The acquired image is 30 frames, and the length of the x-axis is 90, 150, and 210 in the cases of 3, 5, and 7 s, respectively.

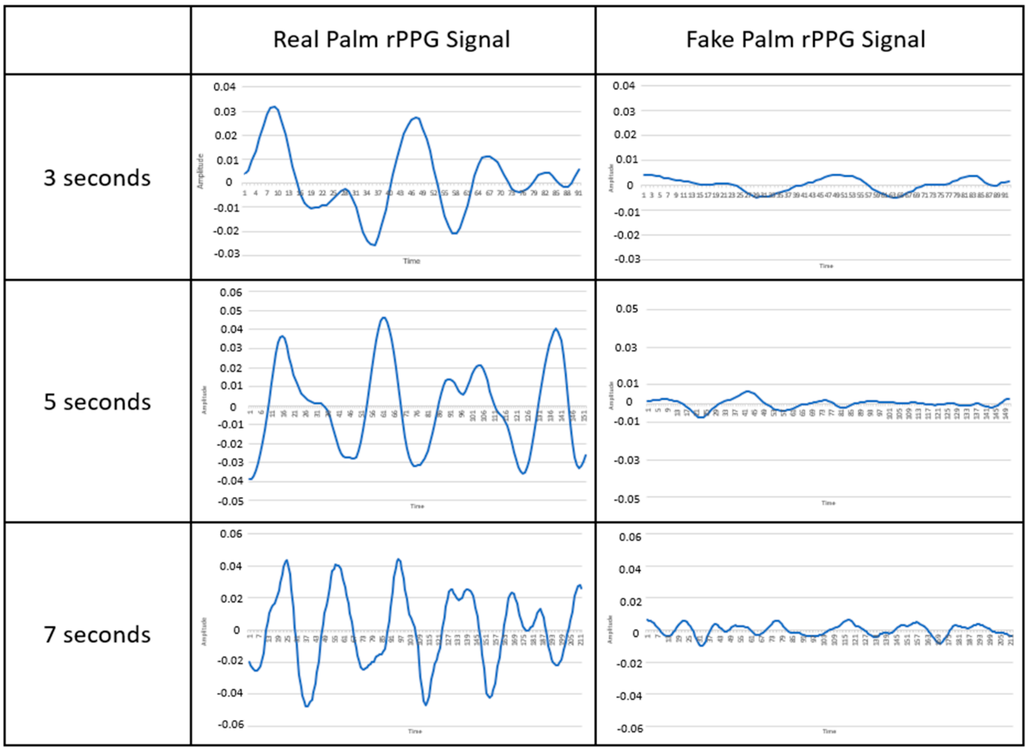


Figure 8. Examples of rPPG signals of real and fake palms. The x-axis refers to time, and the y-axis refers to amplitude.

3.3. Feature Extraction from Acquired Signals

The rPPG signal obtained from the palm is transformed into a periodogram power spectral density estimate. By converting the bio-signal into a frequency signal, a standard less dependent on the signal length can be established. The frequency of the heart rate band corresponding to each second in both authentic and counterfeit images, along with the associated power values, are presented in Figure 9.

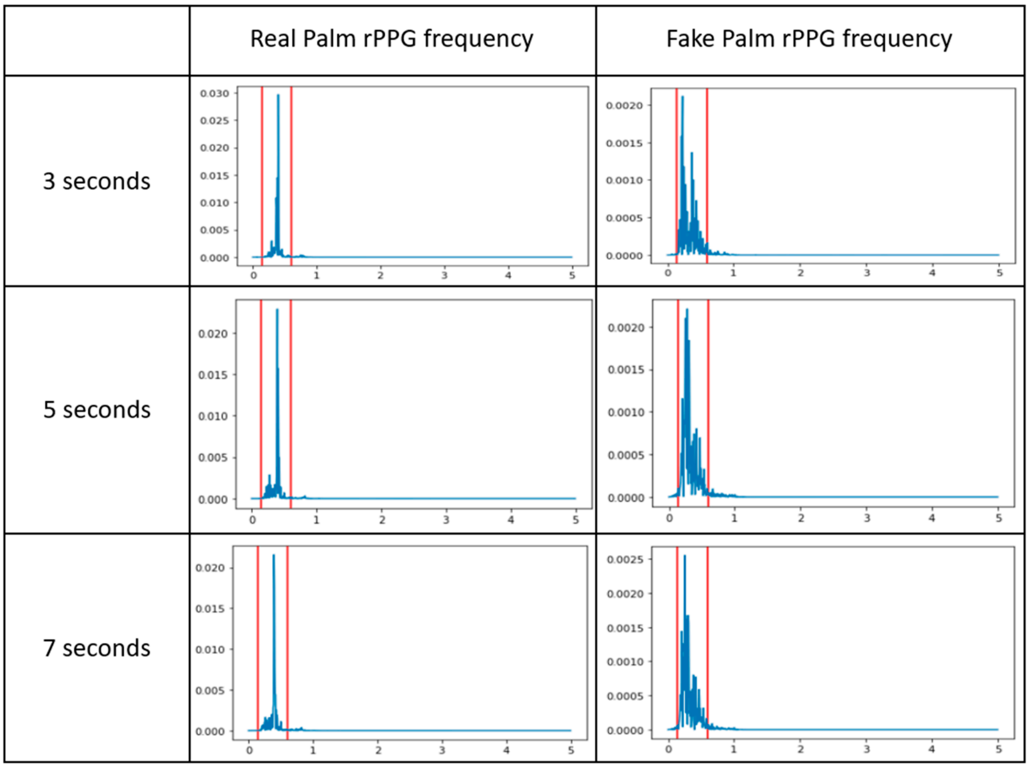


Figure 9. Principal component number decision. The x-axis refers to frequency, and the y-axis refers to amplitude.

The power value was characterized by the frequency corresponding to the heartbeat. A total of 30 features were established, and the method for obtaining them is depicted in the subsequent equation. X(f) is a Fourier transform formula.

$$\begin{gathered} X(f) = \int_{-\infty}^{\infty} x(t) \cdot e^{-j2\pi ft} dt \\ Power\ of\ I_n = |X(f_n))| \\ I = [(Freq_{\,end} - Freq_{start})/30] \\ Feature_{vector} = [Power\ of\ I_0,\ Power\ of\ I_1 \cdots,\ Power\ of\ I_{30}] \end{gathered} \tag{3}$$

The rationale for defining the feature vector in the frequency domain as having 30 dimensions is as follows: The average absolute error of the rPPG extraction method developed in our lab is approximately 2.2 bpm (beats per minute). Therefore, based on the ground truth, the error range is about 4.4 bpm. The decision to divide the available rPPG frequency band into 30 dimensions was made considering the above error range. When dividing the 42~180 bpm band into 30 equal intervals, one sample covers a range of 4.6 bpm. This range approximates the mentioned rPPG measurement's average absolute error of 2.2 bpm, considering both positive and negative directions, resulting in an error range of 4.4 bpm.

Upon dividing the length corresponding to the heartbeat frequency by 30, a cycle value was established. The power value corresponding to the starting point of frequency was designated as the first value. While the cycle value was added, the corresponding power values were retained as feature values. The 30 features extracted through this process underwent a dimensionality reduction to reset the principal components. During this step, the number of principal components was set to the region where the explainable variance ratio was 0.7 or less and the cumulative contribution ratio was 0.8 or more. The results of this process can be observed in Figure 10.

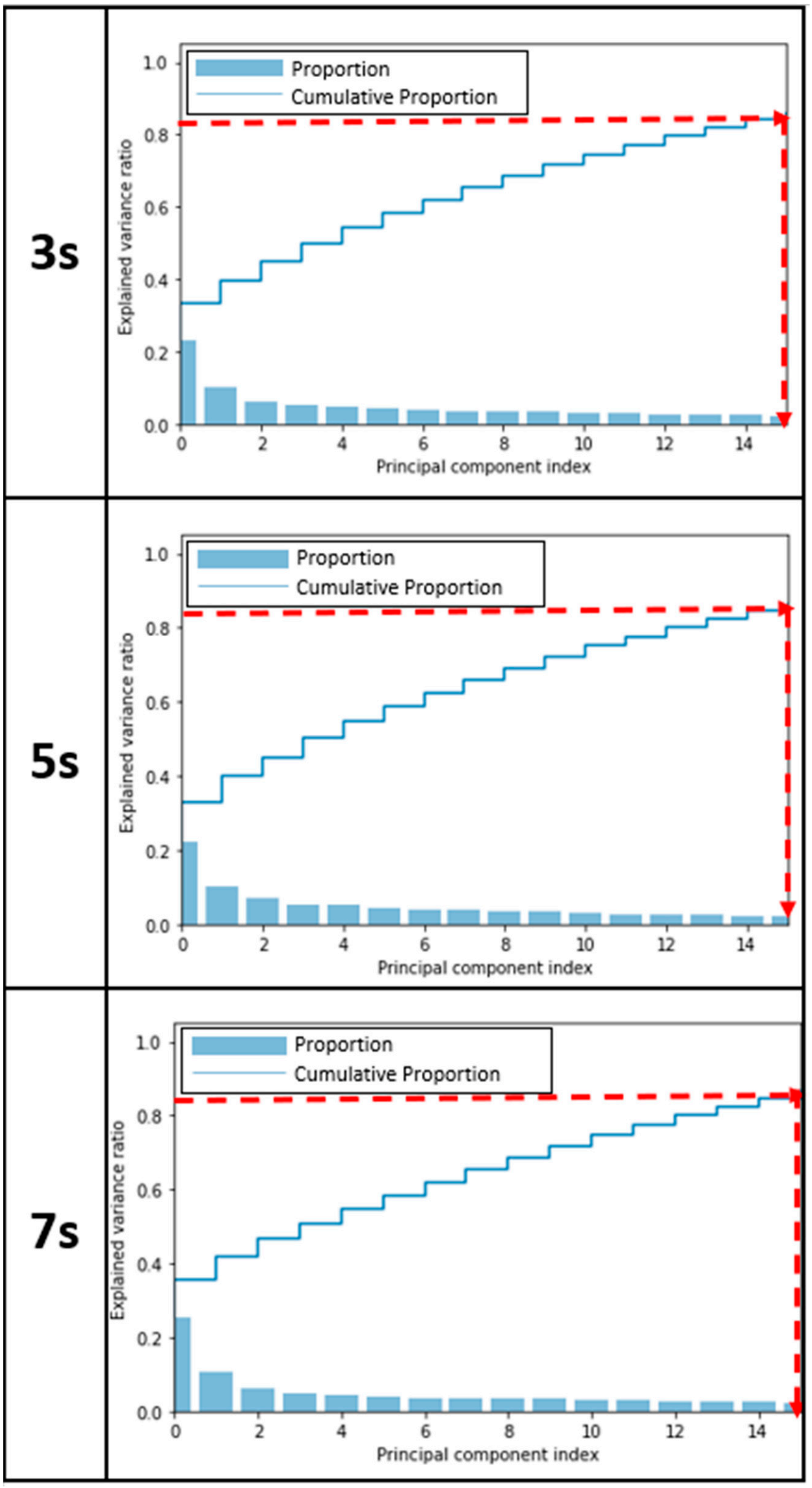


Figure 10. The number of principal components in a region with an explainable variance ratio less than or equal to 0.7 and a cumulative contribution ratio greater than or equal to 0.8.

The explained variance ratio, proportion, and cumulative proportion for each second were extracted. The bar sections of the graph represent the explained variance ratio, while the step graph denotes the cumulative proportion value. After establishing the number of principal components at 15 for durations of 3 s, 5 s, and 7 s, a dimensionality reduction was executed and subsequently utilized as a training model dataset.

3.4. Model Training

A support vector machine is a classifier that identifies a decision boundary at the greatest distance from two distinct classes. Upon the emergence of a novel unclassified data point, the SVM undertakes classification by assessing its positioning relative to the boundary [20]. In this study, we employed Python version 3.8.0 along with the scikit-learn library. A training dataset and a testing dataset were constructed by combining the features of previously acquired PCA-processed real and fake palm data and subsequently shuffling the datasets. The training and testing datasets were divided at an 8:2 ratio, and cross-validation was implemented to address the issue of insufficient test datasets.

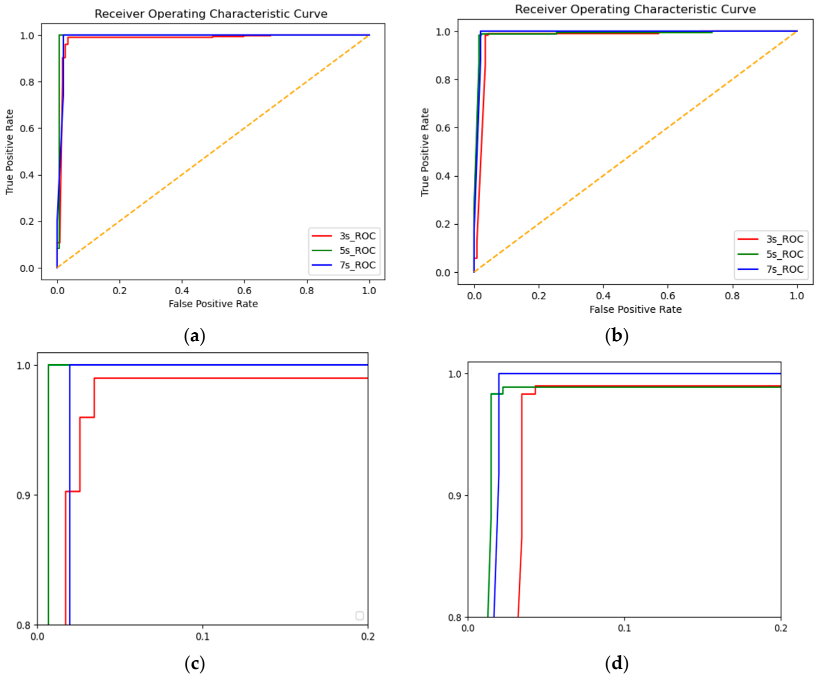
4. Results

The rPPG signal, frequency-converted and extracted with video lengths of 3, 5, and 7 s, was classified using an SVM model. The results using features without PCA and the precision, recall, and F1-score values extracted with PCA of 15 or fewer components are summarized in Table 2. Without PCA, the accuracies were 97.16% for a 3 s video, 98.4% for a 5 s video, and 97.28% for a 7 s video. The lowest accuracy was observed for the 3 s video, while the highest was achieved with the 5 s video.

Table 2. Precision, recall, and F1-score results according to second and PCA.

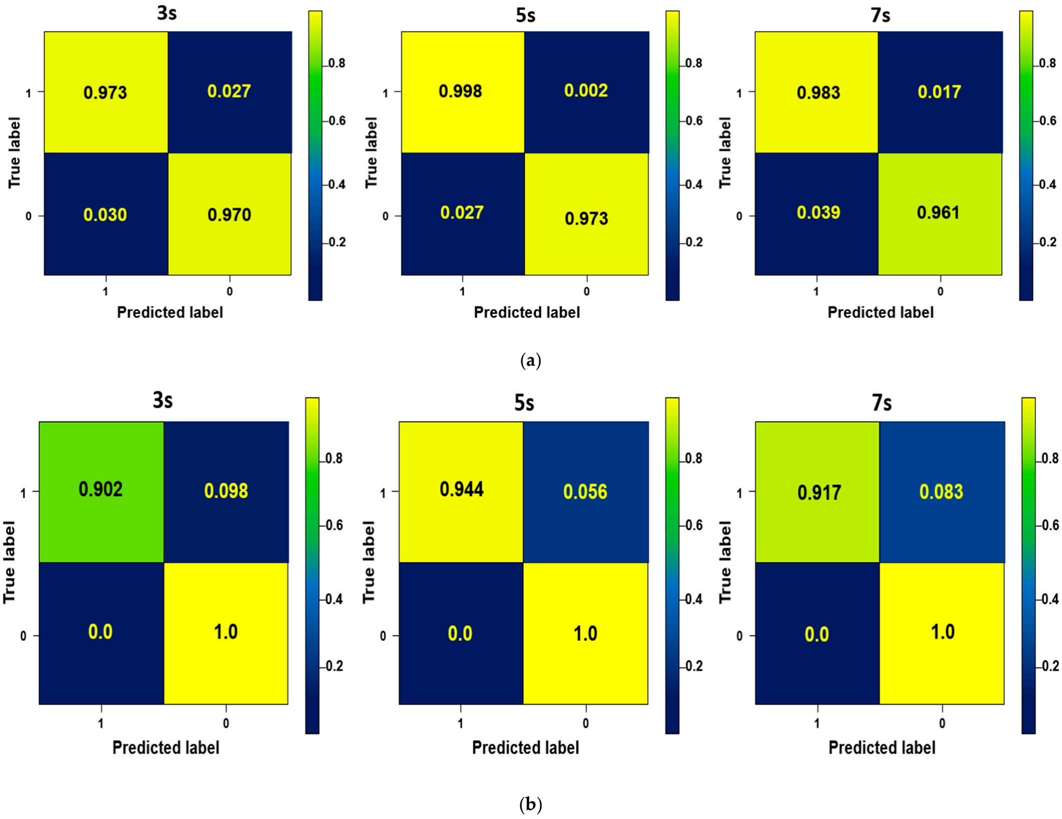
PCA	Second	Precision	Recall	F1-Score
3	**3 s**	0.96	0.85	0.90
	5 s	0.95	0.88	0.91
	7 s	0.90	0.91	0.91
5	**3 s**	0.98	0.94	0.96
	5 s	0.98	0.89	0.93
	7 s	0.96	0.94	0.95
10	**3 s**	0.96	0.97	0.96
	5 s	0.97	0.99	0.98
	7 s	0.98	0.99	0.99
15	**3 s**	0.97	0.99	0.98
	5 s	0.98	0.99	0.99
	7 s	0.98	1.0	0.9918
None	**3 s**	0.97	0.98	0.97
	5 s	0.99	1.0	0.99
	7 s	0.98	0.97	0.98

SVM kernels employ the radial basis function (rbf) kernel. Concerning the parameter configuration, when utilizing GridSearchCV, the regularization parameter (C) was set to 10.0, and the kernel coefficient (gamma) was established as 1000.0. Even in cases where PCA was not applied, the values of C and gamma remained consistent at 10.0 and 1000.0, respectively. A receiver operating characteristic (ROC) curve was employed to visualize the obtained results [21]. The ROC curve illustrates the diagnostic ability for specific decision criteria in binary classification situations, with larger area under curve (AUC) values indicating enhanced classification accuracy. Figure 11 displays the curves for each experimental result. However, to prevent spoofing, it is essential to avoid confusing fake palm signals with real ones. A comparison between the confusion matrix results when the false positive (FP) value is 0 and the confusion matrix results from the previous experiment is illustrated in the subsequent figure. In Figure 12, the number 1 denotes a real palm signal, and 0 represents a fake palm signal. The 5 s video, which had the highest accuracy at 97.2%, experienced a 1.2% reduction in accuracy. The 3 s video recorded 95.6% accuracy, and the 7 s video achieved 95.9% accuracy, indicating an accuracy drop of 1 to 3%.



(**a**) (**b**) (**c**) (**d**)

Figure 11. ROC curve of the results: (**a**) 30 feature data; (**b**) PCA 15 data; (**c**) an enlarged figure of (**a**); and (**d**) an enlarged figure of (**b**).



(**a**)

(**b**)

Figure 12. Confusion matrix results at 3, 5, and 7 s: (**a**) 30 features without PCA, and (**b**) the FP set to 0 per second.

5. Discussion

Recently, anti-spoofing techniques utilizing rPPG signals have been extensively researched. The rPPG signal can be measured from the skin surface of images, and in vision-based biometric methods that involve skin areas like the face or hands, synchronized rPPG features with heartbeats are not observed in cases of non-live biometric information.

In prior face anti-spoofing research, a method for face anti-spoofing based on a 9 s video was proposed [22]. In previous studies, using rPPG signals extracted from the face and employing deep learning models achieved 99% accuracy. This outperforms the method proposed for the hand area in this study. However, for anti-spoofing research using rPPG, it is important to shorten the measurement time for ease of use and to minimize motion noise during measurements while ensuring accuracy in various environments. In this study, a video length of 5 s was proposed as the length that could generate optimal accuracy. Additionally, by confirming the feasibility of using a 3 s video, we significantly reduced the measurement time compared to previous research. Furthermore, while previous research found that face anti-spoofing may cause overfitting issues due to learned features from limited datasets, we defined handcrafted features in the frequency domain of rPPG signals and utilized an SVM model to make decisions in the multidimensional space for classifiers. This ensured the interpretability and scalability of the results. The dataset used in this study was obtained in an uncontrolled environment using various smartphone camera devices without specifying a particular camera model. This effort represents an attempt to capture videos in wild environments, and it is expected that there will be minimal performance degradation when used in real-world scenarios.

However, this dataset does not consider various skin tones. Although there is an argument that palm skin color shows little variation across races, the impact of our study focusing on hands rather than faces could be less significant, yet empirical validation through diverse racial datasets is necessary. Furthermore, the results were derived by only using an SVM model in the result generation method. The possibility of higher accuracy was hindered by not using additional classification models. In future research, we plan to explore anti-spoofing approaches using rPPG in infrared images and hand recognition in RGB environments using infrared images.

6. Conclusions

In this study, we propose a palm spoofing detection method utilizing the remote photoplethysmography (rPPG) signal of the palm as a potential means of biometric authentication. During palm rPPG extraction, valid authentication time is analyzed through video length adjustment and frequency conversion. We define video lengths of 3 s, 5 s, and 7 s, and at each length, the frequency data of real and fake palm rPPG signals are classified using an SVM model. In the SVM model, the power value obtained by dividing the heartbeat frequency into 30 equal intervals and the subsequent value are input as PCA components and compared. This results in accuracies of 97.73% for 3 s, 97.76% for 5 s, and 99.09% for 7 s using PCA. Without using PCA, accuracies of 97.16% for 3 s, 98.4% for 5 s, and 97.28% for 7 s are achieved. Our findings indicate that the 3 s video length may not allow for the extraction of valid features, owing to its short duration. Consequently, we suggest a 5 s video, which yields the highest accuracy of 98.4%, as the optimal length. In spoofing detection, false positives (FPs) that identify fake video signals as genuine are critical. For a 5 s video with an FP value of 0, the accuracy is calculated at 97.2%. Accuracies for other durations also exhibit decreases of about 2%. Additionally, we compared the results with and without PCA. For the 3 s and 5 s results, it was observed that the performance determined as the principal component value was reduced in proceeding with PCA. This suggests that most of the features in the extracted heart rate band have significant meaning. On the other hand, as the signal extraction video length increases, performance improves when extracting results using PCA. This means that the longer the length of the image, the more meaningless information is included in the 30 features. The findings demonstrate that the palm rPPG signal serves as a spoofing-resistant authentication method in an RGB environment, offering a novel palm authentication technique. This study presents a method for preventing hand image spoofing in an RGB setting.

Author Contributions: Conceptualization, E.C.L.; methodology, B.A. and H.L.; software, B.A. and H.L.; validation, B.A. and H.L.; formal analysis, E.C.L., B.A. and H.L.; investigation, B.A. and H.L.; resources, B.A. and H.L.; data curation, B.A. and H.L.; writing—original draft preparation, B.A. and H.L.; writing—review and editing, E.C.L.; visualization, E.C.L., B.A. and H.L.; supervision, E.C.L.; project administration, E.C.L. All authors have read and agreed to the published version of the manuscript.

Funding: This paper was supported by the Field-Oriented Technology Development Project for Customs Administration through the National Research Foundation of Korea (NRF), funded by the Ministry of Science and ICT and Korea Customs Service (2022M3I1A1095155).

Institutional Review Board Statement: Based on the 13-1-3 of the Enforcement Regulations of the Act on Bioethics and Safety of the Republic of Korea, ethical review and approval were waived (IRB-SMU-C-2023-1-008) for this study by Sangmyung University's Institutional Review Board because this study uses only simple contact measuring equipment or observation equipment that does not follow physical changes.

Data Availability Statement: The obtained data cannot be shared because it was agreed that they could be used only for this study.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Bhattacharyya, D.; Ranjan, R.; Alisherov, F.; Choi, M. Biometric Authentication: A Review. *Int. J. u- e- Serv. Sci. Technol.* **2009**, *2*, 13–28.
2. Ong Michael, G.K.; Connie, T.; Jin Teoh, A.B. Touch-Less Palm Print Biometrics: Novel Design and Implementation. *Image Vis. Comput.* **2008**, *26*, 1551–1560. [CrossRef]
3. Delac, K.; Grgic, M. A Survey of Biometric Recognition Methods. In Proceedings of the Elmar-2004: 46th International Symposium on Electronics in Marine, Zadar, Croatia, 18 June 2004; pp. 184–193.
4. Zhang, Y.-B.; Li, Q.; You, J.; Bhattacharya, P. Palm Vein Extraction and Matching for Personal Authentication. In *Advances in Visual Information Systems: 9th International Conference, VISUAL 2007, Shanghai, China, 28–29 June 2007*; Springer: Berlin/Heidelberg, Germany, 2007; pp. 154–164. [CrossRef]
5. Chen, H.; Valizadegan, H.; Jacson, C.; Soltysiak, S. Fake Hands: Spoofing Hand Geometry Systems. In Proceedings of the Biometric Consortium, Arlington, TX, USA, 19–21 September 2005.
6. Tome, P.; Marcel, S. On the Vulnerability of Palm Vein Recognition to Spoofing Attacks. In Proceedings of the 2014 International Conference of the Biometrics Special Interest Group (BIOSIG), Darmstadt, Germany, 10–12 September 2014; pp. 319–325. [CrossRef]
7. Lin, B.; Li, X.; Yu, Z.; Zhao, G. Face Liveness Detection by RPPG Features and Contextual Patch-Based CNN. In Proceedings of the 2019 3rd International Conference on Biometric Engineering and Applications, Stockholm, Sweden, 29–31 May 2019; Association for Computing Machinery: New York, NY, USA, 2019; pp. 61–68.
8. Shi, P.; Hu, S.; Echiadis, A.; Peris, V.A.; Zheng, J.; Zhu, Y. Development of a Remote Photoplethysmographic Technique for Human Biometrics. In *Design and Quality for Biomedical Technologies II*; SPIE: Bellingham, WA, USA, 2009; Volume 7170, pp. 23–30.
9. Wang, H.; Su, L.; Zeng, H.; Chen, P.; Liang, R.; Zhang, Y. Anti-Spoofing Study on Palm Biometric Features. *Expert Syst. Appl.* **2023**, *218*, 119546. [CrossRef]
10. Kanhangad, V.; Kumar, A. Securing Palmprint Authentication Systems Using Spoof Detection Approach. In Proceedings of the Sixth International Conference on Machine Vision (ICMV 2013), London, UK, 16–17 November 2013; Volume 9067, p. 90671M. [CrossRef]
11. Kanhangad, V.; Bhilare, S.; Garg, P.; Singh, P.; Chaudhari, N. Anti-Spoofing for Display and Print Attacks on Palmprint Verification Systems. In *Biometric and Surveillance Technology for Human and Activity Identification XII*; SPIE: Bellingham, WA, USA, 2015; Volume 9457, p. 94570E. [CrossRef]
12. Bera, A.; Dey, R.; Bhattacharjee, D.; Nasipuri, M.; Shum, H.P.H. Spoofing Detection on Hand Images Using Quality Assessment. *Multimed. Tools Appl.* **2021**, *80*, 28603–28626. [CrossRef]
13. Li, X.; Bu, W.; Wu, X. Palmprint Liveness Detection by Combining Binarized Statistical Image Features and Image Quality Assessment. In *Biometric Recognition: 10th Chinese Conference, CCBR 2015, Tianjin, China, 13–15 November 2015*; Yang, J., Yang, J., Sun, Z., Shan, S., Zheng, W., Feng, J., Eds.; Springer International Publishing: Cham, Switzerland, 2015; pp. 275–283.
14. Pravallika, P.; Prasad, K.S. SVM Classification for Fake Biometric Detection Using Image Quality Assessment: Application to Iris, Face and Palm Print. In Proceedings of the 2016 International Conference on Inventive Computation Technologies (ICICT), Coimbatore, India, 26–27 August 2016; Volume 1, pp. 1–6.

15. Farmanbar, M.; Toygar, Ö. Spoof Detection on Face and Palmprint Biometrics. *Signal Image Video Process.* **2017**, *11*, 1253–1260. [CrossRef]
16. Maćkiewicz, A.; Ratajczak, W. Principal Components Analysis (PCA). *Comput. Geosci.* **1993**, *19*, 303–342. [CrossRef]
17. Chai, D.; Bouzerdoum, A. A Bayesian Approach to Skin Color Classification in YCbCr Color Space. In Proceedings of the 2000 TENCON: Intelligent Systems and Technologies for the New Millennium (Cat. No.00CH37119), Kuala Lumpur, Malaysia, 24–27 September 2000; Volume 2, pp. 421–424. [CrossRef]
18. Suh, K.H.; Lee, E.C. Contactless Physiological Signals Extraction Based on Skin Color Magnification. *J. Electron. Imaging* **2017**, *26*, 063003. [CrossRef]
19. Zhang, F.; Bazarevsky, V.; Vakunov, A.; Tkachenka, A.; Sung, G.; Chang, C.-L.; Grundmann, M. MediaPipe Hands: On-Device Real-Time Hand Tracking. *arXiv* **2020**, arXiv:2006.10214. [CrossRef]
20. Noble, W.S. What Is a Support Vector Machine? *Nat. Biotechnol.* **2006**, *24*, 1565–1567. [CrossRef] [PubMed]
21. Hoo, Z.H.; Candlish, J.; Teare, D. What Is an ROC Curve? *Emerg. Med. J. EMJ* **2017**, *34*, 357–359. [CrossRef] [PubMed]
22. Kim, S.-H.; Jeon, S.-M.; Lee, E.C. Face Biometric Spoof Detection Method Using a Remote Photoplethysmography Signal. *Sensors* **2022**, *22*, 3070. [CrossRef] [PubMed]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.