electronics

MDPI

Article

Detecting Fake Finger-Vein Data Using Remote Photoplethysmography

Jin Yeong Bok [1], Kun Ha Suh [1] and Eui Chul Lee [2,*]

[1] Department of Computer Science, Graduate School, Sangmyung University, Hongjimun 2-Gil 20, Jongno-Gu, Seoul 03016, Korea; bjywlsdud23@gmail.com (J.Y.B.); tjrjsgk@naver.com (K.H.S.)

[2] Department of Intelligent Engineering Informatics for Human, Sangmyung University, Hongjimun 2-Gil 20, Jongno-Gu, Seoul 03016, Korea

* Correspondence: eclee@smu.ac.kr; Tel.: +82-2-781-7553

Received: 16 August 2019; Accepted: 9 September 2019; Published: 11 September 2019

Abstract: Today, biometrics is being widely used in various fields. Finger-vein is a type of biometric information and is based on finger-vein patterns unique to each individual. Various spoofing attacks have recently become a threat to biometric systems. A spoofing attack is defined as an unauthorized user attempting to deceive a system by presenting fake samples of registered biometric information. Generally, finger-vein recognition, using blood vessel characteristics inside the skin, is known to be more difficult when producing counterfeit samples than other biometrics, but several spoofing attacks have still been reported. To prevent spoofing attacks, conventional finger-vein recognition systems mainly use the difference in texture information between real and fake images, but such information may appear different depending on the camera. Therefore, we propose a method that can detect forged finger-vein independently of a camera by using remote photoplethysmography. Our main idea is to get the vital sign of arterial blood flow, a biometric measure indicating life. In this paper, we selected the frequency spectrum of time domain signal obtained from a video, as the feature, and then classified data as real or fake using the support vector machine classifier. Consequently, the accuracy of the experimental result was about 96.46%.

Keywords: biometrics; finger-vein; spoofing attacks; photoplethysmography; vital sign

1. Introduction

There has been a significant increase in interest surrounding biometric systems and their applications in human verification and identification [1]. Since each person's biological characteristics are unique and hard to counterfeit [2], biometric recognition technology has advantages over traditional methods. Therefore, biometrics, such as face, fingerprint, voice, iris, and finger-vein recognition, is being widely used in many applications. These applications include: Internet banking, personal identification for computers, and automated teller machines (ATMs) [3]. Besides fingerprint and face recognition, which are widely used in smart devices, the finger-vein recognition system has attracted attention because of its high recognition rate, small device size, low-risk forgery, noninvasiveness, and noncontact [4,5]. As a biometric characteristic, finger veins have several beneficial properties, such as universality, distinctiveness, permanence, and acceptability [6]. In addition, in terms of security and convenience, it could be today's leading biometric technology since it introduces features inside the human body [7,8]. Finger-vein recognition uses the geometric information of blood vessels inside the skin [9,10]. Thus, the possibility of spoofing attacks is relatively low compared to face and fingerprint recognition [11]. Spoofing attacks can occur when people try to masquerade as someone else by falsifying data. The purpose is to allow unauthorized users to deceive the authentication system, thereby gaining illegitimate access and advantages. However, finger-vein recognition is not completely safe from spoofing attacks. When a finger-vein image captured by a near-infrared imaging device is leaked out, it can be printed and used successfully as a spoofing attack on a vein recognition sensor. Recently, methods of fake finger-vein attacks have been introduced to prevent the possibility of spoofing attacks. For instance, various databases of fake finger-vein images were constructed and printed on a paper, and an overhead projector film, with which the researchers evaluated the performance of their system [3]. Furthermore, a finger-vein artifact database was introduced in another study, which was collected using three different kinds of artifacts: (1) Inkjet print, (2) laser printer, and (3) a smartphone display [12]. However, since previous methods do not utilize the dynamic characteristics of biological signals, other spoofing methods can be devised if the defense method is exposed. In order to solve this problem, we propose a method for recognizing finger-veins through remote photoplethysmography (PPG).

Figure 1 shows the acquisition process of real and fake finger-vein image using the remote PPG with an infrared camera. With this PPG methodology, we detected a fake finger-vein by analyzing the frequency spectrum of a time-series signal, which was obtained from the change of brightness of the finger-vein image according to the heartbeat. After obtaining the entire data, the distributions of feature vectors extracted from real and fake finger-vein samples were classified using a support vector machine (SVM).

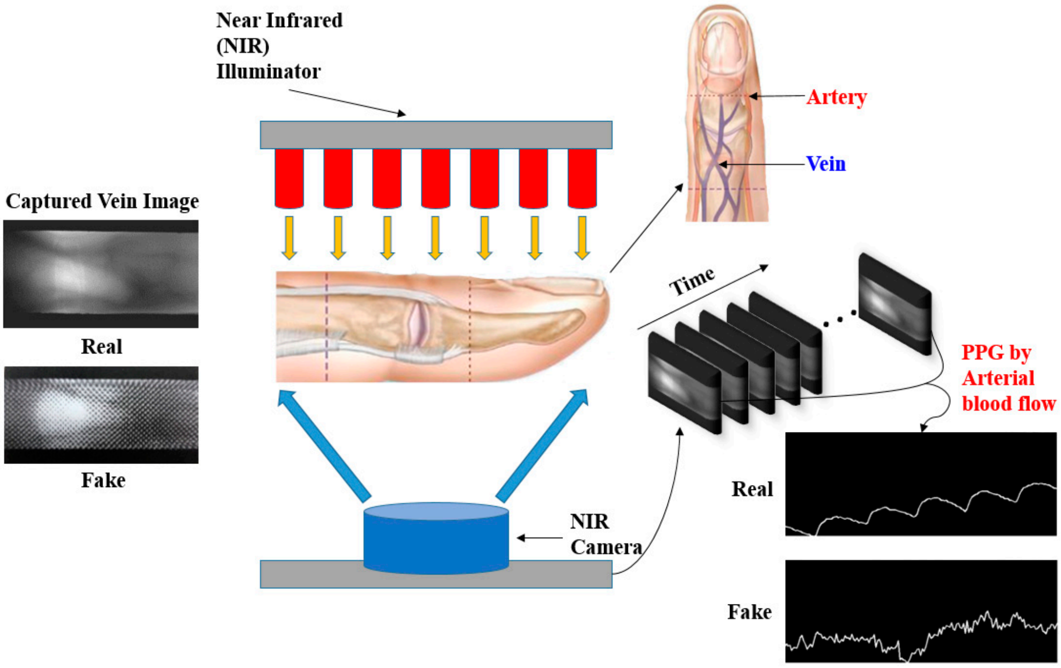


Figure 1. Overall process of finger-vein image acquisition using remote PPG (photoplethysmography) with the near infrared camera.

The rest of this paper is organized as follows. Section 2 describes our own finger-vein database and proposed method. In the finger-vein database, the camera system and the capture environment were described with the design of our database. Section 3 shows the result of our experiment numerically. The detailed analysis about the result is shown in Section 4. Finally, we explain the conclusion of our research in Section 5.

2. Materials and Method

In this section, a detailed explanation of our finger-vein database built for the experiment is given. The camera settings used in order to obtain the real and fake finger-vein data and the environment applied to capture the images accurately under stable conditions are shown in the subsection. In addition, the design of our own database is described with some image samples obtained by using remote PPG. Next, the proposed method for determining whether the finger-vein data was forged is explained in detail, including the description of the algorithms and SVM classifier.

2.1. Finger-Vein Database

In order to obtain stable finger-vein images with a fixed finger pose, we used a device that we manufactured. In addition, since unnecessary external light may affect the real and fake finger-vein classification while acquiring the image, capturing was performed using a light blocking object in our laboratory room for minimizing misclassification. The camera system and capture environment of the design of our own database are specifically described as follows.

2.1.1. Camera Environment

A device that consists of 850 nm infrared illuminators and a Logitech C600 webcam was used to obtain real and fake finger-vein image data. The webcam was converted into an infrared camera by removing the infrared rejection filter and attaching an infrared bandpass filter. The spatial resolution of the images and the frame rate of capturing were set to 640 × 480 pixels and 30 frames per second, respectively. During capturing, the camera was aimed at the palm of the hand and infrared light was transmitted through the back of the finger. In order to consider the fingertip pattern and focus on the finger appropriately, the finger and the camera were placed in a noncontact state at a distance of about 25 mm. Figure 2a,b show, respectively, a finger-vein capture device with a real finger and the fake image sample through the device.

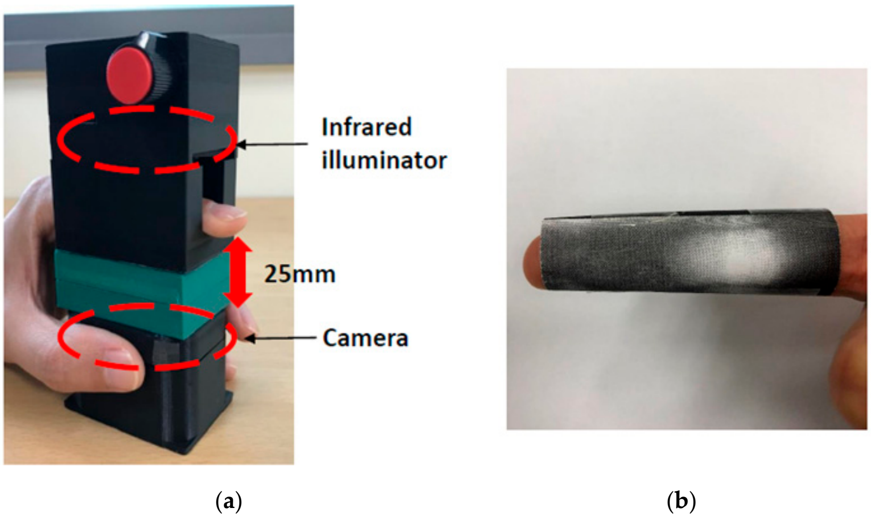


Figure 2. Procedure of real and fake video clip acquisition through our device: (**a**) Suggested capture device with a real finger; (**b**) fake image example for spoofing attacks.

2.1.2. Design of Our Own Database

To construct our finger-vein database, we used a remote PPG approach. This method is a noninvasive, optical approach that extracts the heartbeat signals of live person by measuring blood flow changes in the tissue layer of capillaries inside one's skin. As the finger-vein recognition system uses the overall geometric information of the blood vessels, the application of the remote PPG technology is suitable. In addition, the information can distinguish between real and fake finger-vein images.

All experiments were performed with our subjects in a stable posture, and the infrared illumination inside our device was adjusted appropriately to obtain clear finger-vein images. The captured video clips were stored in our program. Figure 3 shows samples of images from real and fake videos used in our research.

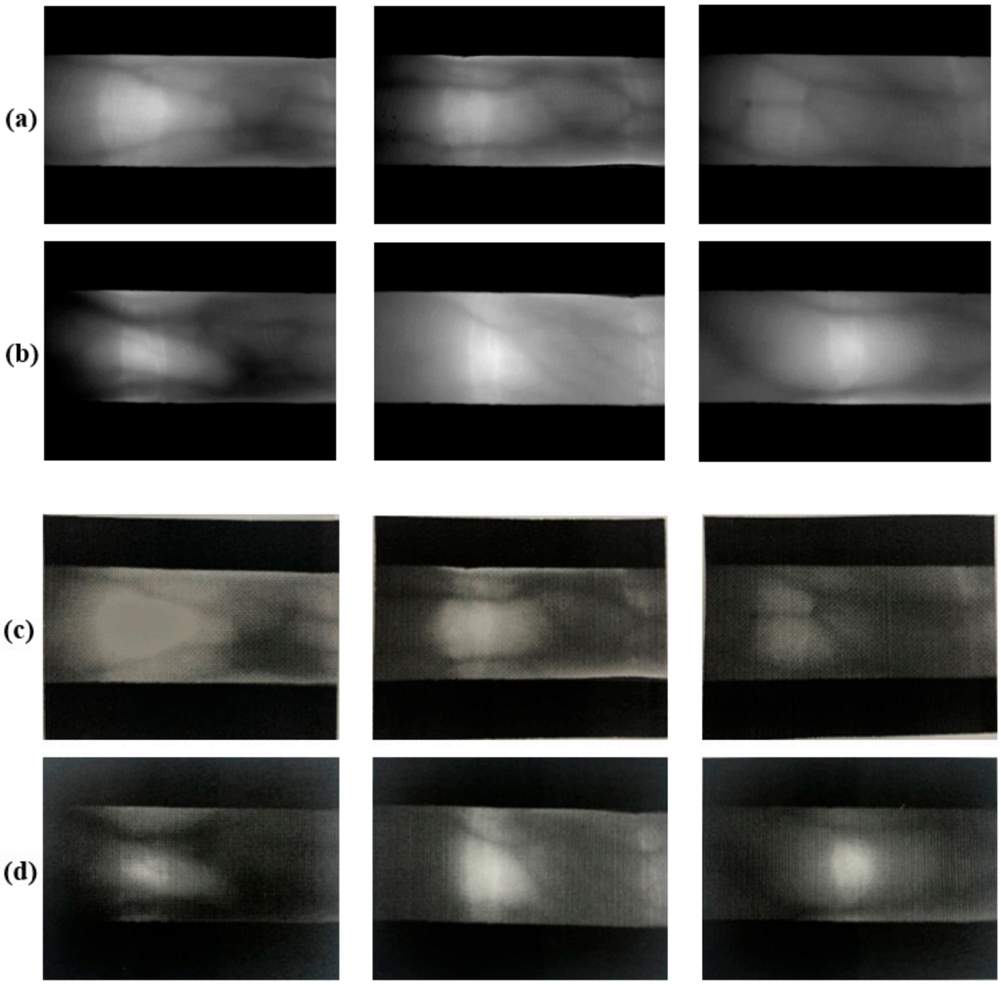


Figure 3. Examples of finger-vein images obtained from a constructed database: (**a**,**b**) Real finger-vein image samples; (**c**,**d**) fake finger-vein image samples.

We captured each person's finger-vein image for about a minute and saved that as a video file. At that time, only the index and the middle fingers of both hands were captured for about 15 s. There are several considerations for using only two fingers instead of all other fingers. First, the thumb is thick, its veins are difficult to observe from the captured image, and the quality of real thumb-vein images is therefore not suitable [3]. In addition, a fake thumb is not elaborate enough to fool the finger-vein recognition system. Second, in general, the ring and little fingers are not commonly used in biometric recognition systems. This is due to the fact that the convenience of the recognition posture has to be considered. As a result, four video files were acquired from each person.

To construct a counterfeit finger-vein database, fake images were obtained using a high-resolution printer. While making counterfeit data, a single frame of a captured real finger-vein image was printed.

Since we obtained 80 video files from real and fake finger-vein data, respectively, the data were divided to augment learning data for better SVM classifier learning. Thus, we divided one video into 150 frames overlapping 100 frames. If the length of the frame is too short, it will be difficult to detect the shape of a heartbeat-like signal through a finger-vein image. This also reduces the distinction between real and fake videos. Conversely, if the length is too long, then the features will be excessively derived, which may cause classification to take a longer time. Because of these problems, the frame length is determined as 150 frames.

Consequently, the whole number of real and fake finger-vein video clips was 1139 (real: 579, fake: 560). The real and fake finger-vein video database is described in Table 1 in more detail.

Table 1. Explanation of the real and fake video database.

Database	Explanation
Real video	20 people × 4 fingers = 579 real video clips From the index and middle fingers (divided into 150 frames overlapping 100 frames)
Fake video	Using a high-resolution printer Printed on an A4 paper 20 people × 4 fingers = 560 fake video clips From the index and middle fingers (divided into 150 frames overlapping 100 frames)
Total	Real video clips: 579 Fake video clips: 560 Total video clips: 1139

2.2. Proposed Method

In previous studies of fake biometric detection, machine learning based pattern classification methods were generally used by analyzing predefined features [4]. In this method, we used 800 out of the total 1139 real and fake finger-vein videos for SVM training.

Since our fake finger vein detection method is based on the photoplethysmography principle, it is essential to check the periodicity of the blood flow signals synchronized with the heart rate. As shown in Figure 4, although the time-series signal clearly has a visual difference between real and fake cases, the dimension is too high and there is a lot of redundancy to use all samples of the signal as a feature vector. In order to use the low dimensional feature vector which reduces the redundancy of the periodic signal, while checking the periodicity of the signal, the feature is defined in the frequency domain as the right graph of Figure 4. The DFT algorithm is a tool in which a periodic signal is represented through a combination of continuous sinusoidal signals by converting the signal from the time domain to the frequency domain.

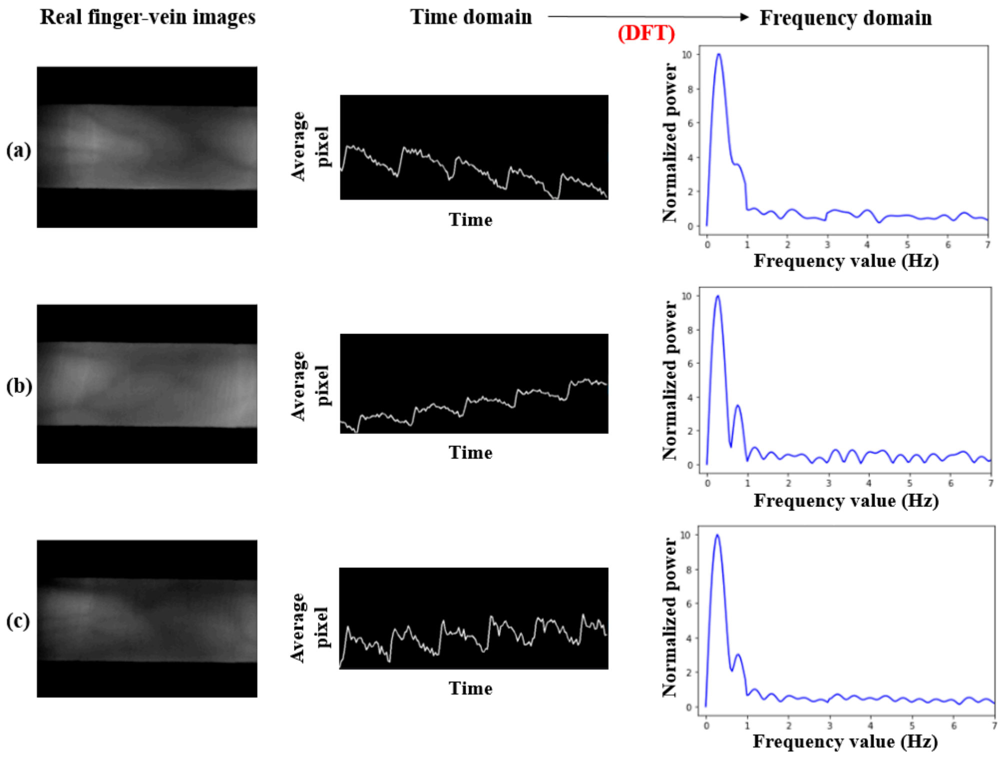


Figure 4. *Cont.*

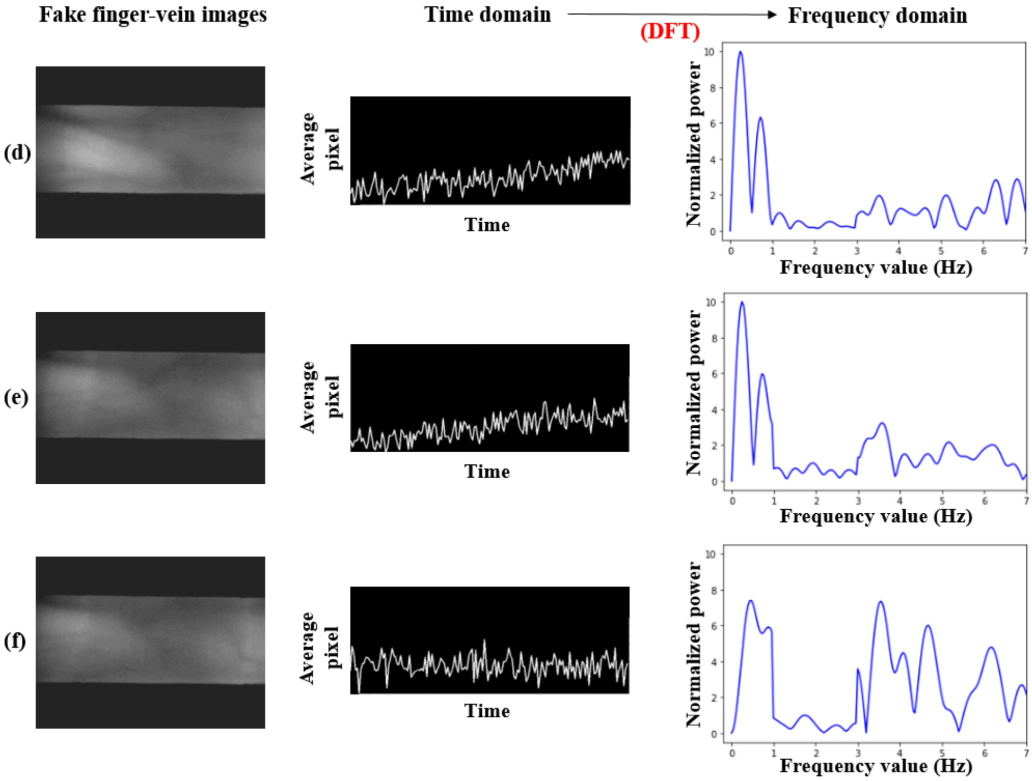


Figure 4. Temporal and frequency visualizations of photoplethysmography extracted from captured finger vein videos: (**a**–**c**) Cases of real finger vein; (**d**–**f**) Cases of fake finger vein.

Next, we removed the low-frequency and high-frequency components that occurred because of the movement of the fingers, changes in the illumination, and intrinsic noise of the sensor. In general, since the heart rate of people appears to be between 60 and 180 beats per minute, the frequency components of finger-vein image less than 1.0 Hz and more than 3.0 Hz were eliminated. For this processing, zero padding of 10 times the signal length was used to extract feature vectors at a high-frequency resolution. As a result, the magnitude values are used as feature vectors of 50 dimensions. No normalization procedure was applied.

Then, we used an SVM model to classify real and fake finger-vein data. As one of the techniques for pattern classification, this has been widely used in many application areas, including pattern recognition, bioinformatics, and text categorization [13,14]. The classifier takes the feature vector and determines to which class it belongs. However, this technique has difficulties, the most difficult being to choose a kernel function and its parameter values. If these are not set properly, then the classification outcomes will be much less than optimal. Therefore, proper kernel and parameter settings are very important for the improvement of the SVM classification accuracy. There are some strategies for searching kernel and input parameters, the simplest one being the grid-search algorithm [15]. Thus, we used this algorithm to determine the optimal kernel and parameters. Once the parameters are determined, using feature vectors applied to training, the SVM model is performed by classifying data with different labels (real: 1, fake: −1). In this paper, linear, radial basis function (RBF), polynomial, and sigmoid kernels were considered [16–19]. The expression of kernel functions is shown in Table 2. Additionally, the grid-search algorithm, the gamma value, c-value set in the kernel, respectively, and the F1-score obtained are shown is Table 3. The F1-score, which is one of the indicators for evaluating accuracy, is usually used in an unbalanced class and calculated by statistically integrating the two called precision and recall [20]. The reason for combining the two is that in most cases the precision and recall are inversely proportional. These are the formulas for precision, recall, and F1-score:

$$\text{precision} = \text{TP} / (\text{TP} + \text{FP}) \quad (1)$$

$$\text{recall} = \text{TP} / (\text{TP} + \text{FN}) \tag{2}$$

$$\text{F1-score} = 2 \times (\text{precision} \times \text{recall})/(\text{precision} + \text{recall}) \tag{3}$$

Table 2. The expression of various support vector machine kernel functions.

Kernel	Expression
Linear	$K(x_i, x_j) = x_i^{\mathcal{T}} \cdot x_j$
RBF	$K(x_i, x_j) = e^{(-\gamma \lVert x_i - x_j \rVert^2)}, \gamma > 0$
Polynomial	$K(x_i, x_j) = (r x_i^{\mathcal{T}} \cdot x_j + r)^d, \gamma > 0$
Sigmoid	$K(x_i, x_j) = \tanh(\gamma x_i^{\mathcal{T}} \cdot x_j + r)$

(kernel parameter: γ, r, d).

Table 3. The results of the gamma value, c-value, and F1-score for each kernel.

Kernel	Gamma Value	c-Value	F1-Score
Linear	-	0.001	0.88
RBF	0.001	10	0.96
Polynomial	0.001	1000	0.87
Sigmoid	0.00001	1000	0.91

As a result, the optimal kernel and parameters determined by the grid-search algorithm are the RBF kernel with a gamma value of 0.001 and a c-value of 10. Figure 5 shows the proposed procedure.

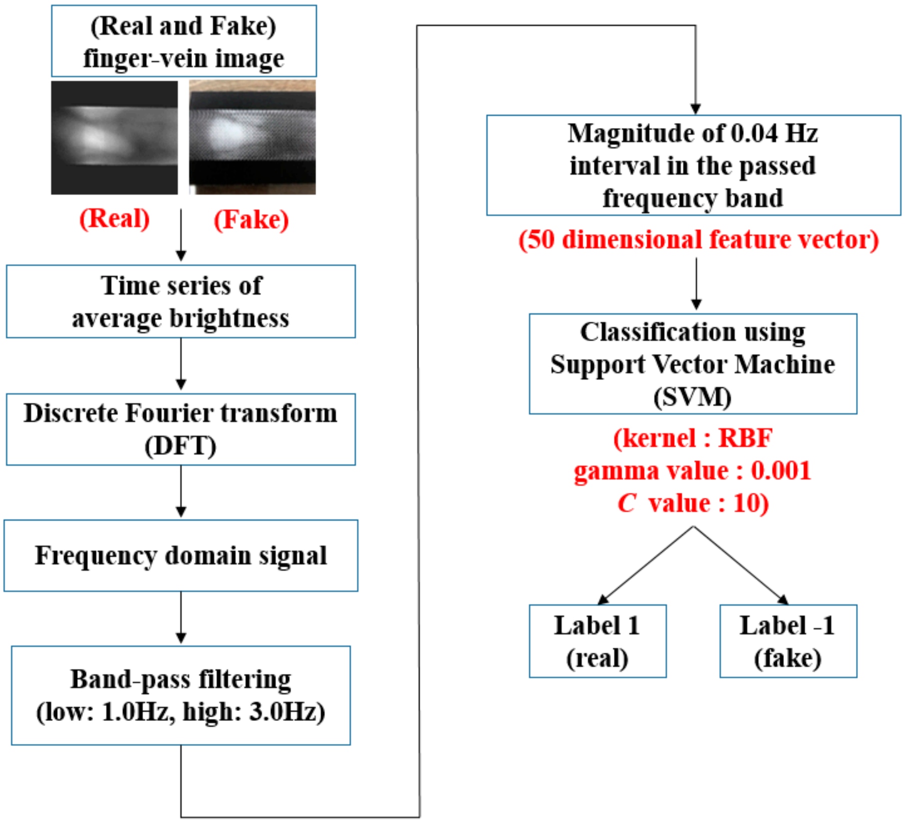
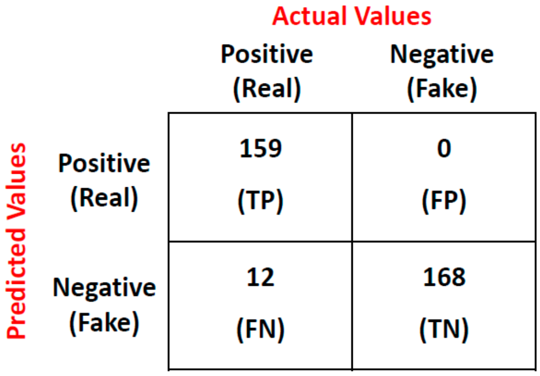

(Real and Fake) finger-vein image
(Real)
(Fake)
Time series of average brightness
Discrete Fourier transform (DFT)
Frequency domain signal
Band-pass filtering (low: 1.0Hz, high: 3.0Hz)
Magnitude of 0.04 Hz interval in the passed frequency band
(50 dimensional feature vector)
Classification using Support Vector Machine (SVM)
(kernel : RBF
gamma value : 0.001
C value : 10)
Label 1 (real)
Label -1 (fake)

Figure 5. Flowchart of the proposed method for classification.

After completing the SVM training, 339 videos that were not used in training were used in the test to measure the classification accuracy.

3. Results

In this paper, the counterfeit finger-vein data detection accuracy was obtained by using the consequence of confusion matrix analysis. Confusion matrix is one of the simplest and most intuitive methods used to measure the accuracy of the model. The analysis was based on the concept of true positive (TP), true negative (TN), false positive (FP), and false negative (FN), assuming real and fake finger veins as positive and negative, respectively. The result of the four values obtained from the above method is shown in Figure 6. The classification accuracy calculated by the classification accuracy formula of the confusion matrix with the four values is about 96.5%.



		Actual Values	
		Positive (Real)	Negative (Fake)
Predicted Values	Positive (Real)	159 (TP)	0 (FP)
	Negative (Fake)	12 (FN)	168 (TN)

Figure 6. Result in terms of the confusion matrix.

This is the accuracy formula we used:

$$\text{Classification accuracy} = (\text{TP} + \text{TN}) / (\text{TP} + \text{FP} + \text{TN} + \text{FN}) \tag{4}$$

From the results obtained, we observed that no counterfeit data was identified as actual data; only real data was misclassified as counterfeit data. In order to discover the characteristics of normally classified data and the causes of misclassified data, we analyzed the state of the frequency distribution. The result of the analysis is described in the discussion.

4. Discussion

In this section, we analyzed the result obtained from our finger-vein database in two cases. The detailed explanation is as follows.

First, in normally classified real finger-vein data, we found that the frequency distribution was biased to 1.0–1.5 Hz. Next, in regard to the frequency value, most of the images showed that the difference between the maximum value in the above range and the maximum value in 2.5–3.0 Hz, which is a relatively high frequency, is more than double. On the other hand, most of the fake data showed a uniform distribution throughout, not biased to any side. However, approximately 10% of the frequency distribution from counterfeit finger-vein data was exceptionally biased to 1.0–1.5 Hz, as compared to the remainder. This was similar to the distribution of real finger-vein data. In such cases, fake data indicated that the difference under the same conditions as above is less than double.

Second, in abnormally classified cases, the FP that classified fake data as real data was 0, but the FN that classified real data as fake data was 12. As a result of analyzing the causes of misclassification, the frequency distribution of real finger-vein data was mostly the same as that of correctly classified data. However, the difference of the frequency value was similar to that of the fake data, and it was observed to be a result of FN. The reasons for this problem were motion noise and illumination changes that occurred in the capture apparatus.

To visualize the result obtained, we used a receiver operating characteristic (ROC) curve, which is useful for organizing classifiers and visualizing performances [21]. The curve of our experiment result is shown in Figure 7.

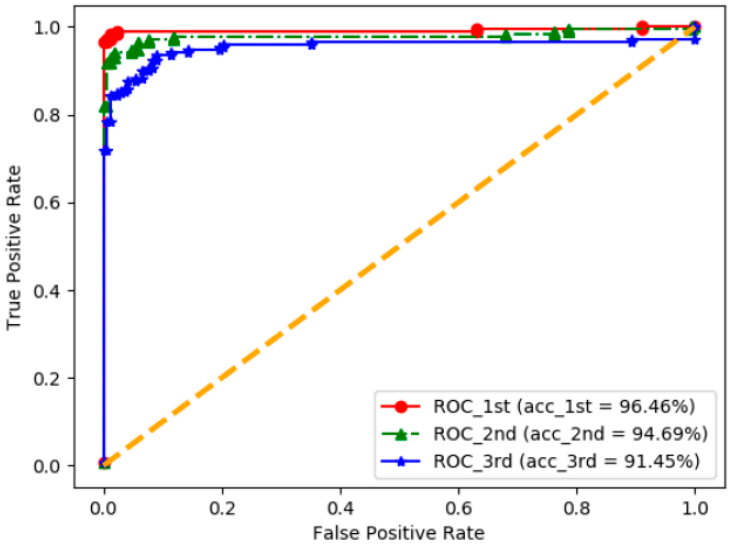


Figure 7. Result in terms of ROC (receiver operating characteristic) curve.

The rate of specificity, called FP value, and rate of sensitivity or recall, called TP value, are plotted each on the x-axis and y-axis. The highest accuracy was obtained using the heart rate band, and the second highest was obtained using only the respiration band, which was about 0.8–1.3 Hz. When only high-frequency band filtering is used, the lowest result is obtained. Therefore, we found that the range that we set showed the best performance.

5. Conclusions

In this paper, we proposed a fake finger-vein detection methodology using PPG, which utilized the characteristics of heartbeat-like signals observed in finger-vein images. Time-series signals were transformed into a frequency domain using DFT algorithm and frequency features of real and fake finger-veins. These were then applied to SVM model for classification. The classification accuracy was 96.46%.

The proposed method uses only printed images as fake finger-vein images. As our method uses time series changes as a feature, it can be susceptible to replay attacks through actual finger vein video and display devices. However, as shown in Figure 2, the finger vein imaging device is usually sized so that one finger can barely be inserted, so it is impossible to attempt a spoofing attack by properly positioning a smartphone or tablet display device.

If the proposed method is known to the attacker, he can simulate the photoplethysmography signal by moving the finger similar to the heartbeat cycle. However, by detecting the presence of motion through the analysis of the movement of the finger boundary in the captured images, such malicious attack can also be easily defended. In previous fake finger-vein detection methods, it can be seen that only the attack through the printed image is considered [3,22].

In future works, we will implement the method for determining the optimal video capture time and fuse it with other features, considering the other fake finger vein spoofing scenarios.

Author Contributions: Conceptualization, E.C.L.; methodology, E.C.L.; software, J.Y.B; validation, J.Y.B. and K.H.S.; formal analysis, E.C.L., J.Y.B; investigation, K.H.S.; resources, E.C.L.; data curation, J.Y.B; writing—original draft preparation, J.Y.B.; writing—review and editing, E.C.L. and K.H.S.; visualization, J.Y.B; supervision, K.H.S.; project administration, E.C.L.; funding acquisition, E.C.L.

Funding: This study was funded by the NRF of Korea funded by the MSIT (grant number: NRF-2019R1A2C4070681).

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

References

1. Waluś, M.; Kosmala, J.; Saeed, K. Finger vein pattern extraction algorithm. *Int. Conf. Hybrid Artif. Intell. Syst.* **2011**, 404–411. [CrossRef]
2. Liu, Y.; Ling, J.; Liu, Z.; Shen, J.; Gao, C. Finger vein secure biometric template generation based on deep learning. *Soft Comput.* **2018**, *22*, 2257–2265. [CrossRef]
3. Nguyen, D.T.; Park, Y.H.; Shin, K.Y.; Kwon, S.Y.; Lee, H.C.; Park, K.R. Fake finger-vein image detection based on Fourier and wavelet transforms. *Digit. Signal Process.* **2013**, *23*, 1401–1413. [CrossRef]
4. Yang, J.; Shi, Y.; Yang, J. Personal identification based on finger-vein features. *Comput. Hum. Behav.* **2011**, *27*, 1565–1570. [CrossRef]
5. Wang, K.; Ma, H.; Popoola, O.P.; Liu, J. *Biometrics*; Yang, G., Ed.; Intech: Rijeka, Croatia, 2010; pp. 31–53.
6. Yang, L.; Yang, G.; Yin, Y.; Zhou, L. A survey of finger vein recognition. *Lect. Notes Comput. Sci.* **2014**, *8833*, 234–243. [CrossRef]
7. Mulyono, D.; Jinn, H.S. A study of finger vein biometric for personal identification. In Proceedings of the 2008 International Symposium on Biometrics and Security Technologies, Islamabad, Pakistan, 23–24 April 2008; pp. 1–8. [CrossRef]
8. Rosdi, B.A.; Shing, C.W.; Suandi, S.A. Finger vein recognition using local line binary pattern. *Sensors* **2011**, *11*, 11357–11371. [CrossRef] [PubMed]
9. Lee, E.C.; Park, K.R. Restoration method of skin scattering blurred vein image for finger vein recognition. *Electron. Lett.* **2009**, *45*, 1074–1076. [CrossRef]
10. Lu, Y.; Yoon, S.; Park, D.S. Finger vein identification system using two cameras. *Electron. Lett.* **2014**, *50*, 1591–1593. [CrossRef]
11. Hadid, A. Face biometrics under spoofing attacks: Vulnerabilities, countermeasures, open issues, and research directions. *Comput. Vis. Pattern Recognit. Workshops* **2014**, 113–118. [CrossRef]
12. Raghavendra, R.; Busch, C. Presentation attack detection algorithms for finger vein biometrics: A comprehensive study. In Proceedings of the Signal-Image Technology & Internet-Based Systems (SITIS), Bangkok, Thailand, 23–27 November 2015; pp. 628–632. [CrossRef]
13. Huang, C.L.; Wang, C.J. A GA-based feature selection and parameters optimization for support vector machines. *Expert Syst. Appl.* **2006**, *31*, 231–240. [CrossRef]
14. Lin, S.W.; Lee, Z.J.; Chen, S.C.; Tseng, T.Y. Parameter determination of support vector machine and feature selection using simulated annealing approach. *Appl. Soft Comput.* **2008**, *8*, 1505–1512. [CrossRef]
15. Wang, J.; Wu, X.; Zhang, C. Support vector machines based on K-means clustering for real-time business intelligence systems. *Int. J. Bus. Intell. Data Min.* **2005**, *1*, 54–64. [CrossRef]
16. Yang, C.; Odvody, G.; Fernandez, C.; Landivar, J.; Minzenmayer, R.; Nichols, R. Evaluating unsupervised and supervised image classification methods for mapping cotton root rot. *Precis. Agriculture.* **2015**, *16*, 201–215. [CrossRef]
17. Keerthi, S.S.; Lin, C.J. Asymptotic behaviors of support vector machines with Gaussian kernel. *Neural Comput.* **2003**, *15*, 1667–1689. [CrossRef] [PubMed]
18. Zhou, D.X.; Jetter, K. Approximation with polynomial kernels and SVM classifiers. *Adv. Comput. Math.* **2006**, *25*, 323–344. [CrossRef]
19. Lin, H.T.; Lin, C.J. A study on sigmoid kernels for SVM and the training of non-PSD kernels by SMO-type methods. *Submitt. Neural Comput.* **2003**, *3*, 1–32.
20. Powers, D.M. Evaluation: From precision, recall and F-measure to ROC, informedness, markedness and correlation. *Mach. Learn. Technol.* **2011**, *2*, 37–63.
21. Fawcett, T. An introduction to ROC analysis. *Pattern Recognit. Lett.* **2006**, *27*, 861–874. [CrossRef]
22. Nguyen, D.T.; Yoon, H.S.; Pham, T.D.; Park, K.R. Spoof Detection for Finger-Vein Recognition System Using NIR Camera. *Sensors* **2017**, *17*, 2261. [CrossRef] [PubMed]