# Non-Fiducial PPG-based Authentication for Healthcare Application

Nima Karimian*, Mark Tehranipoor, Domenic Forte

***Abstract*— Biometrics have a great deal of potential in healthcare applications, most notably authentication for medical record privacy and fraud prevention. In this paper, we examine, for the first time, non-fiducial feature extraction for photoplethysmography (PPG) based authentication. PPG signals have unique identity properties for human authentication, and are becoming easier to capture by emerging IoT sensors such as MaxFast. Different machine learning techniques are used to compare non-fiducial and fiducial feature extractions. Our experimental results show that 99.84% accuracy with EER of 1.31% can be achieved based on non-fiducial feature extraction.**

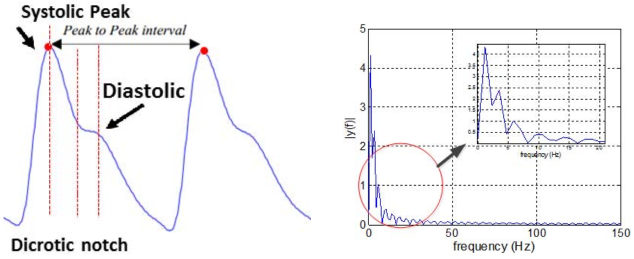
## I. INTRODUCTION

Biometrics have several benefits to the healthcare industry including prevention of fraud and abuse in entitlement programs, protection and management of confidential medical records, patient identification, and access control for medical facilities and equipment [1]. knowledge-based (e.g., PIN, password, or possession-based (e.g., smartcard) can be circumvented by guessing, hacking or theft. Including biometric technology is much better since it is much more difficult to fake, steal or imitate. Furthermore, by linking medical records to biometrics, medical care can be provided more accurately and efficiently. This capability can also be invaluable in emergency situations such as when patients are unresponsive, uncooperative, or unconscious.

An increasing number of applications requiring user authentication are making use of biometric modalities such as fingerprint, iris, and face. In the healthcare domain, systems already capture and process certain universal human biological signals for heath monitoring. With a few minor tweaks, the same systems can re-purpose these signals for continuous human authentication. Among the human biological signals, electrocardiogram (ECG) and photoplethysmograph (PPG) are two of the most popular signals for capturing the electrical activity of the heart and changes in blood flow during heart activity (Fig.1 (a)).

PPG is a particularly simple and low-cost optical technique that detects blood volume changes in the blood vessels through measurements at the skin surface. PPG sensors are included in many different wearable devices today. Unlike ECG, PPG measurements only need to be acquired from one side of the body, allowing it to be used in a larger number of human recognition scenarios.

Gu et al. [2] was the first group to investigate PPG for user authentication. They considered four feature parameters and achieved 94% accuracy. More recently, Kavsaolu et al. [3] proposed a feature ranking algorithm based on 40 time domain features, acquired from first and second derivatives of the PPG signal and achieved 94.44% accuracy. In 2016, [4] proposed 12 time domain features from PPG and its derivatives.



(a) (b)

Fig. 1: (a) A normal PPG, (b) Power spectrum of PPG.

Our goal in this work is to develop more robust approaches for processing PPGs and use them for authentication purpose. The above prior work relies on fiducial characteristics (i.e., landmarks) obtained from PPG signals in the time domain. Non-fiducial methods have had better success in biometric systems for electrocardiogram (ECG) [5] and to our knowledge have not been applied to PPGs. Non-fiducial approaches take a more holistic approach where features are extracted statistically based on the overall signal morphology. In this paper, we evaluate non-fiducial and fiducial approaches for feature extraction with both supervised and unsupervised machine learning classification techniques. Non-fiducial approach achieves 99.75% and 99.84% accuracy for supervised and unsupervised machine learning respectively.

The remainder of the paper is organized as follows. The next section will discuss building blocks of a PPG authentication system including pre-processing and feature extraction methods. In Section III, two step feature selection are discussed. Supervised and unsupervised machine learning methods are described in Section IV. Experiments and results are discussed in Section V. Finally, the paper is concluded in Section VI.

## II. PROPOSED PPG AUTHENTICATION SYSTEM

Our PPG biometric authentication system is shown in Figure 2. First, PPG signals are captured by a PPG sensor and pre-processed to remove noise. Next, peak detection of the PPG signal is used in order to divide the PPG into different segments (beats). After segmentation and normalization, feature extraction is applied. The resulting features are processed by a two-step approach to reduce dimensionality and correlation. Finally, classification is applied to distinguish genuine and imposer PPG data.

* Nima Karimian is with Department of Electrical and Computer Engineering, University of Connecticut, Storrs, CT 06269 USA `e-mail: nima@engr.uconn.edu`

M. Tehranipoor, and D. Forte are with the Department of Electrical and Computer Engineering, University of Florida, Gainesville, FL 32611

978-1-5090-4179-4/17/$31.00 ©2017 IEEE

### A. Pre-processing

There are various sources of artifacts that interfere with PPG signal acquisition including baseline wander (BW), motion artifact (MA), and respiration. PPG signal spans frequencies between 0.5 Hz to 5 Hz (Fig. 1 (b)). In this paper, a third order Butterworth band pass filter with cutoff frequency 1Hz-5Hz was deployed to reduce the effect of noise. Segmentation is necessary to extract discriminative features from data as input to classification models. We have created PPG segments by identifying the systolic peak of each beat using a modified Pan Tompkins peak detection algorithm. Since there are variations between segments, we normalize each segment in terms of maximum amplitude and time.

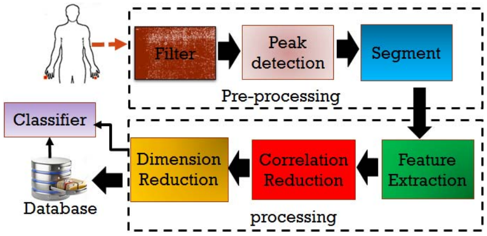


Fig. 2: Block diagram of the proposed PPG authentication system.

### B. Feature Extraction

We have divided the feature extraction methods into two major categories fiducial point methods and non-fiducial methods which will be discussed below.

**Fiducial Features**: In fiducial point methods, the most often used features are based on local landmarks of heart beats such as temporal or amplitude difference between consecutive fiducial landmarks. For PPG, the fiducial features are often determined from the original PPG signal and its second derivative. In Fig.1 (a), the main landmarks are shown as a systolic peak, dicrotic notch, and diastolic peak. The peak amplitude and their peak times are employed as fiducial feature. Even with pre-processing, peak detection can be undependable especially in the case of dicrotic notch and diastolic peak. For example, age is an important factor that affects the contour of PPG signals which accelerates the disappearance of PPG's dicrotic notch. If the peaks cannot be extracted at all, the PPG biometric system will require more segments in order to identify the individual which impacts its usability and convenience. On the other hand, noise in the peaks can also impact the accuracy of authentication, resulting in false positives and false negatives.

**Non-Fiducial Features**: The wavelet transform is a very popular technique for biomedical signal processing due to the fact that it is lightweight and capable of providing time and frequency information simultaneously. In wavelet transform, a linear operation transforms the PPG signal by decomposing it into various scales. The PPG signal is passed through a series of high and low pass filters in order to analyze both high as well as low frequency components. The discrete wavelet transform (DWT) is defined by

$$y[n] = \sum_{k=-\infty}^{\infty} x[k]\psi[n-k] \tag{1}$$

where the $x[k]$ represents the PPG signal under authentication.. The set of wavelet functions is usually derived from the mother wavelet $\psi(t)$ which is dilated by value $s = 2^j$, translated by constant $\tau = k \times 2^j$, and normalized, where the $j$, $k$ are integers. A wavelet defined by the solution of a dilation follows[6]

$$\psi_{j,k}[t] = \frac{1}{\sqrt{s}}\psi[\frac{t-\tau}{s}] = \frac{1}{\sqrt{2^j}}\phi[2^{-j}t-k] \tag{2}$$

where, $j$ is the dilation parameter, or the visibility in frequency, and $k$ is the parameter about the position.

The wavelet coefficients can be obtained by taking the inner product:

$$V_\phi[j_0,k] = \frac{1}{\sqrt{M}}\sum_n PPG[n]\phi_{j_0,k}[n] \tag{3}$$

$$W_\psi[j_0,k] = \frac{1}{\sqrt{M}}\sum_n PPG[n]\psi_{j,k}[n] \quad j_0 \leq k \tag{4}$$

where $\phi_{j_0,k}[n]$ and $\psi_{j,k}[n]$ are discrete functions. $\{\phi_{j_0,k}[n]\}_{k\in z}$ and $\{\psi_{j,k}[n]\}_{(j,k)\in z^2, j\leq j_0}$ are orthogonal to each other. Equation 3 represents approximation coefficients (CA) while Equation 4 denotes detailed coefficients (CD). In this paper, CA and CD are used as the non-fiducial feature vectors. For this purpose, we have investigated several mother wavelet transforms, and found Coiflet to be the best.

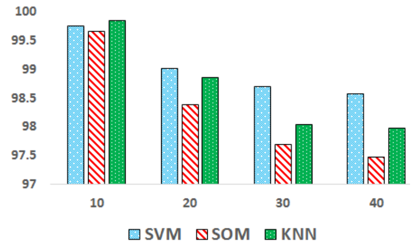


Fig. 3: Coiflet results based on different PCA dimensions.

## III. Two-Step Feature Selection

The resulting feature vector may have correlation and high dimensionality, which makes it unsuitable for resource-constrained systems (e.g., wearables) and produces high false rejection rate. Thus, we have employed a two-step feature selection in order to reduce the dimension of the features. In our method, Kolmogorov-Smirnov (KS-test) correlation based filter is applied to remove correlated features. A feature is considered to be good if it is highly correlated to the class but not to any other features. Second, Kernel PCA (KPCA) [7], a nonlinear technique is used for dimensionality reduction. We have investigated $10, 20, 30$, and 40 dimensions to find the best dimension for our work. We find that the authentication accuracy improves as dimensionality decreases. Based on experimental results (Fig. 3), we use a 10 dimensional feature vector for later results.

## IV. Machine Learning for Classification

Here we have categorized classification techniques into supervised (SVM) and unsupervised learning (SOM, KNN) methods.

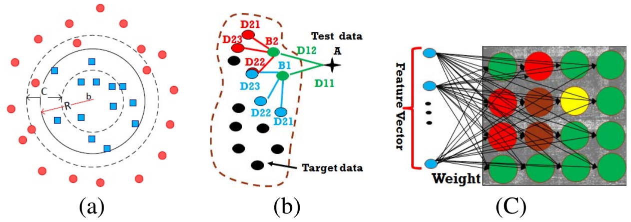
### A. Supervised Learning

**Support vector machines (SVMs)**: SVM has become one of the most popular supervised learning techniques. In biometric authentication systems, one-class classification [8] approach is trained by only one class of data, and therefore classifiers are designed to distinguish between the one known class and any other which are unseen during training. One-class SVM classifiers minimize the volume of the hypersphere which contains the training data ( Fig. IV (a)). The hypersphere is defined by center $b$ and a radius $R > 0$. Minimizing the size of the hypersphere is equivalent to minimizing $R^2$ as shown in the following quadratic programming problem:

$$\min_{R,b,\xi} \qquad R^2 + \frac{1}{N\nu}\sum_{i=1}^{N}\xi_i \qquad (5)$$

$$Subject\ to, \qquad ||\phi(\bar{x}_i) - b|| \leq R^2 + \xi_i \qquad (6)$$

Here $R$ and $b$ are parameters determined by solving the above problem and represent the hypersphere where $i = 1,\ldots,N$. and $\xi_i \geq 0$,. $\xi_i$ are "slack" variables that allows for some points to be within the margin in the scenario of a nonexistent separating hypersphere. $\nu$ can be interpreted as the margin of the hypersphere used to separate the data. The goal of the classification problem is learning an optimal separable hypersphere known as a decision function. For our purposes, the RBF kernel is used because the Coiflet wavelet transform feature vectors follow a Gaussian distribution.



(a) (b) (C)

Fig. 4: (a) The SVM hypersphere where circles and squares are unknown (outlier) and known(target) data respectively and the sphere with solid line represents dividing boundary, (b) topological structure of k-NN scheme, (c) and structural graph of SOM neural network where the circles are neurons.

### B. Unsupervised Learning

**(1) k-nearest-neighbors (k-NN)** is based on the minimum distance of the sample features to the training features. Consider a set of labeled feature vectors set to train this classifier, and another set of unlabeled feature vectors used for test purposes (see Fig. IV (b)). The test set is accepted when its local density is larger or equal to the local density of its nearest neighbor in the training set. As can be seen in Fig. IV (b), the distance from a test data A to its nearest neighbour $B_j$ is computed and called $D_{1j}$. Then average distances of the k nearest neighbors for $B_j$ to its nearest neighbor in the target sample is computed and called $D_2$. If $D_{1j}/D_2 \geq$ threshold value, test sample is rejected as an outlier or else accepted as member of target sample. This simple method is very efficient, especially in high dimensional feature spaces.

**(2) Self-organizing map (SOM)**: is a single layer feed-forward artificial neural network and is trained by an unsupervised clustering method. Input vectors features in SOM are given to the first layer of the network. The second layer of the network is the output layer depending on the similarities among them. The construction of the SOM is such that all objects in the feature space retain their distance as much as possible and neighborhood relations in a mapped space (Fig. IV (c)). Using this feature, SOM can be used for clustering and classification of the large amount of input vectors [9]. To evaluate the fitness of test data in this model, a reconstruction error is considered that defines the difference between an object and its closest cluster center (neuron) in the SOM.

## V. Experimental Results

### A. Database

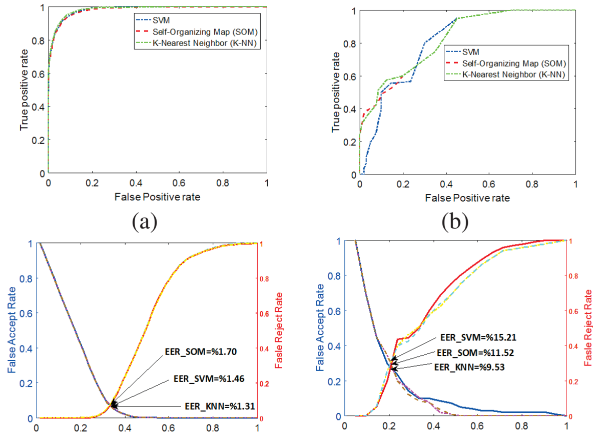
In order to evaluate the efficiency of the PPG authentication and the proposed non-fiducial feature extraction, a publically available Capnobase IEEE TBME benchmark dataset [10] was used. The raw PPG signals are 8 minutes long with 300 Hz sample rate for 42 healthy subjects.

### B. Metrics for Evaluation

In order to evaluate the performance of PPG authentication, several experiments were carried out. We divided the data-set (subject features) into a training and a test set. The training set is used to train the classifiers and to tune their parameters. We then test the classifiers on the data that has not been seen by the classifiers during training time. In training set, we only consider genuine data (authentic users) while in the test sets impostors are also included. Here, we have employed 95% of subjects as an impostor (outlier) and 5% of subjects as genuine (target). Our evaluation metric involves the false positive/acceptance rate (FPR/FAR) and the true positive/acceptance rate (TPR/TAR). FAR refers to the rate at which a classifier incorrectly matches impostor data (outlier) to the target class. TAR refers to the rate that a classifier correctly matches the genuine data (target) to the target class. The two error rates FAR and false negative/reject rate (FNR/FRR) can be traded-off with each other. At the cost of missing out some imposers, one can reduce FAR by making the classifiers less sensitive; at the cost of more false negatives, one can increase the probability of detecting intruders. In order to account the usability-security trade off, we report the equal error rate (EER) in all experiments. This is the error rate the classifier where FAR equals FRR.

In addition for evaluating the performance of biometric PPG authentication, receiver operating characteristic (ROC) and EER curves are considered in this paper (see Fig 5). The

ROC curve represents the trade-off between FAR and FRR, while EER is generally adopted as a unique measure for characterizing the performance level of a biometric system. The EER can be seen in the figure where the FAR and FRR cross each other.



(a)

(b)

(c)

(d)

Fig. 5: Receiver operating characteristic (ROC) (a) and (c) Coiflet wavelet, (b) and (d) fiducial feature extraction.

### C. Discussion

In our evaluation, the target data is randomly chosen. For different classification sets with the same percentage of all the data, we get different results in each iteration. For characterizing a classification set of a given size, the experiments were conducted for 50 random trials. Then, the average, standard deviation (STD) of accuracy, and EER are calculated. The classification accuracy and EER for the above approaches are summarized in Table I. Coiflet wavelet transform (non-fiducial) and fiducial feature extractions with different classification are considered in our experiments. Comparing the results of the non-fiducial and fiducial, it can clearly be seen that non-fiducial has better performance in terms of accuracy and EER. For example, in Table I, the standard deviation value of fiducial result is 15.59 which is much more than non-fiducial one (2.6) since the features are not recognized well in noisy signals for some of the subjects. Our observation indicates that unsupervised learning methods have better performance compared to supervised ones especially in fiducial feature extraction. It can be observed that non-fiducial method results in 99.75% of accuracy based on SVM classifier while fiducial features only succeed in accuracy of 91.46%. Therefore, as shown in Table I, fiducial features classification accuracy has a lack of approximately 9% meaning they are more sensitive to noise. This leads to impact the result although non-fiducial features are far less dependent on peak detection correctness.

In more details, Fig. 5 (a) & (c) present the ROC curve results of the authentication for the non-fiducial PPG performance with EER values 1.46%, 1.31%, and 1.70% for SVM, k-NN, and SOM respectively. Fig. 5 (b) & (d) indicate the ROC curve results of fiducial PPG authentication with EER of 15.21%, 9.53%, and 11.52% for SVM, k-NN, and SOM respectively. The results that are shown in Fig. 5 can demonstrate that unsupervised learning technique perform better especially in the case of fiducial feature compared to supervised learning technique.

TABLE I: Results of authentication

| | | SVM | SOM | KNN |
|---|---|---|---|---|
| Non-Fiducial | Acc | $99.75 \pm 0.7$ | $99.65 \pm 0.9$ | $99.84 \pm 0.4$ |
| | EER | $1.46 \pm 2.7$ | $1.70 \pm 3.4$ | $1.31 \pm 2.6$ |
| Fiducial | Acc | $91.46 \pm 15.24$ | $92.96 \pm 15.44$ | $93.76 \pm 15.59$ |
| | EER | $15.35 \pm 20.22$ | $11.52 \pm 15.84$ | $9.53 \pm 15.92$ |

Overall, the results of the experiments show that it is possible to perform PPG biometric authentication without the use of PPG fiducial detection. The non-fiducial method provides an efficient, robust, and computationally efficient authentication technique in healthcare application.

## VI. Conclusion

Biometrics can protect the confidentiality of medical records through healthcare provider authentication. In this paper, we present non-fiducial and fiducial feature extraction for photoplethysmography (PPG) based authentication. Our results indicate that two-step feature selection technique can give a degree of freedom to remove the correlated feature that may have impact on authentication performance. Supervised and unsupervised machine learning techniques are considered for authentication evaluation. The experimental results show that 99.84% accuracy with EER of 1.31% can be achieved based on non-fiducial feature extraction. This outperforms the fiducial based approaches is prior work by a significant margin.

## References

[1] Marohn, Dana. ”Biometrics in healthcare.” Biometric Technology Today 14.9 (2006): 9-11.

[2] Gu, Y. Y., Y. Zhang, and Y. T. Zhang., “A novel biometric approach in human verification by photoplethysmographic signals.” Information Technology Applications in Biomedicine,”*4th International IEEE Conference nn EMBS Special Topic*, pp. 13–14, 2003.

[3] Kavsaolu, A. Reit, Kemal Polat, and M. Recep Bozkurt., “A novel feature ranking algorithm for biometric recognition with ppg signals,” *Computers in biology and medicine*, vol. 49, PP. 1–14, 2014.

[4] Chakraborty, Samik, and Saurabh Pal., “Photoplethysmogram signal based biometric recognition using linear discriminant classifier,” *2nd International Conference on Control, Instrumentation, Energy & Communication (CIEC)*, pp. 183–187, 2016.

[5] Karimian, N., Guo, Z., Tehranipoor, M., and Forte, D., “Highly reliable key generation from electrocardiogram (ECG),” *IEEE Transactions on Biomedical Engineering* , 2016.

[6] D.E. Newland, “An introduction to random vibrations, spectral & wavelet analysis,” *Courier Corporation*, 2012.

[7] Schlkopf, Bernhard, Alexander Smola, and Klaus-Robert Mller., “Kernel principal component analysis,” *International Conference on Artificial Neural Networks.*, Springer Berlin Heidelberg, pp. 583–588, 1997.

[8] D.M.J. Tax, et al., “Feature extraction for one-class classifications,” *Artificial Neural Networks and Neural Information Processing-ICANN/ICONIP* pp. 342–349, 2003.

[9] Vesanto, Juha, and Esa Alhoniemi. ”Clustering of the self-organizing map.” IEEE transactions on neural networks 11.3 (2000): 586-600.

[10] Karlen, W., Raman, S., Ansermino, J. M., and Dumont, G. A., “Multiparameter respiratory rate estimation from the photoplethysmogram,” in *IEEE Transactions on Biomedical Engineering*, vol. 60, pp. 1946–1953, 2015.