Continuous User Verification via Respiratory Biometrics

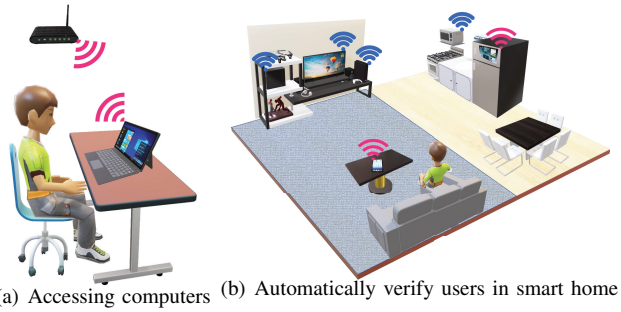
Jian Liu*, Yingying Chen*, Yudi Dong‡, Yan Wang§, Tiannming Zhao§ and Yu-Dong Yao‡
*Rutgers University, New Brunswick, NJ, USA 08901
‡Stevens Institute of Technology, Hoboken, NJ, USA 07307
§Temple University, Philadelphia, PA, USA 19122
Email: jianliu@winlab.rutgers.edu, yingche@scarletmail.rutgers.edu, ydong6@stevens.edu,
{y.wang, tum94362}@temple.edu, yyao@stevens.edu

***Abstract*—The ever-growing security issues in various mobile applications and smart devices create an urgent demand for a reliable and convenient user verification method. Traditional verification methods request users to provide their secrets (e.g., entering passwords and collecting fingerprints). We envision that the essential trend of user verification is to free users from active participation in the verification process. Toward this end, we propose a continuous user verification system, which re-uses the widely deployed WiFi infrastructure to capture the unique physiological characteristics rooted in user's respiratory motions. Different from the existing continuous verification approaches, posing dependency on restricted scenarios/user behaviors (e.g., keystrokes and gaits), our system can be easily integrated into any WiFi infrastructure to provide non-intrusive continuous verification. Specifically, we extract the respiration-related signals from the channel state information (CSI) of WiFi. We then derive the user-specific respiratory features based on the waveform morphology analysis and fuzzy wavelet transformation of the respiration signals. Additionally, a deep learning based user verification scheme is developed to identify legitimate users accurately and detect the existence of spoofing attacks. Extensive experiments involving 20 participants demonstrate that the proposed system can robustly verify/identify users and detect spoofers under various types of attacks.**

I. Introduction

Respiration monitoring has drawn considerable attention as it provides the essential information about the physical health of a person, which could enable a variety of emerging applications. For instance, respiratory patterns could be used for early detection of diseases in many areas including sleep, pulmonology, and cardiology. In addition, existing studies [4], [27] have shown that people's respiratory motions generate unique biometric information in terms of breathing rhythms, breathing sound, and corresponding thoracoabdominal motions. Thus, it is possible to exploit respiratory motions to distinguish individuals without requiring any extra human effort since people breathe all the time without conscious volition [7]. In this work, we target on building a non-intrusive continuous user verification system using respiratory biometrics, which is the most challenging application based on respiration monitoring. The resulting technique could be easily extended to support many emerging applications, such as customized services in smart homes and access management in mobile healthcare systems.

We envision that the ultimate goal of user verification is to free users from manually entering secret information for identity verification and enable computing devices to automatically identify the users around-the-clock. To enable automatic user verification, existing approaches usually utilize users' unique behavioral patterns (e.g., gait pattern [28], keystroke/mouse dynamics [31]) to continuously perform identity verification. However, these systems can only identify users when they are involved in particular activities. In addition, biometrics resulted from spontaneous physiological processes (i.e., heart beating and breathing) have been successfully used to continuously identify individuals. For instance, recent advancement [19], [25] uses cardiac patterns to enable unobtrusive continuous user verification. Chauhan et al. [4] leverage the audio generated by three distinct respiratory gestures (i.e., sniff, normal breath, and deep breath) to perform user verification. However, this work requires the user to perform the specific respiratory gestures close to a microphone, which is inconvenient and impractical in many real-world scenarios.



(a) Accessing computers using breath (b) Automatically verify users in smart home

Fig. 1. Example applications of continuous user verification that leverages respiratory motions captured by off-the-shelf WiFi.

In our work, we reuse the WiFi infrastructures that are prevalent in our daily lives and devise an innovative user verification system that can automatically verify users' identities based on their respiratory biometrics independent of any specific activities. Different from the aforementioned existing solutions, our solution can be easily integrated into any WiFi-enabled mobile devices to provide contactless continuous verification independent of user behaviors in various applications as depicted in Figure 1. For example, our system could let a user log in his laptop as an assistance to their passwords to enhance security (or even without entering passwords in the future) and further access user-specific applications continuously without additional identity verification as shown in Figure 1(a). In another set of applications, the system could

be applied to WiFi-enabled devices (e.g., Amazon Echo, smart TV at home), which allow users to perform operations (e.g., online purchase and parent control) without manually input user-privilege information.

The goal of our system is to reconstruct reliable respiratory patterns by directly examining CSI from WiFi signals despite of interferences and noises coming from environments and human bodies. Toward this end, we extract respiratory-related patterns in CSI readings from WiFi-enabled devices and apply an Empirical Mode Decomposition (EMD) based filter [12] to mitigate the effects caused by the immanent radio interference or other irrelevant body movements. Unlike conventional filters (e.g., low-pass filter) that may mistakenly remove useful signal components due to fixed cutoff frequencies, the EMD-based filter can adaptively filter the noisy components to better preserve the respiration-related signals. To determine the sensitive subcarriers in CSI samples that are significantly impacted by respiratory motions, a subcarrier selection mechanism is developed based on the signal's periodicity and sensitivity. The system further reconstructs the respiratory motion signals leveraging the selected subcarriers to reconstruct the reliable respiratory patterns.

To extract effective features, we examine the reconstructed CSI signals and identifies the segments containing complete respiratory cycles. It then extracts unique respiratory biometrics in each respiratory segment by employing waveform morphology analysis and fuzzy wavelet packet transform (FWPT) [16]. The extracted morphological features (e.g., inhaling/exhaling rhythm, breathing depth, and duration) and the FWPT based features constitute a unique complementary set to discriminate each individual. These derived respiratory features are used to construct each legitimate user's profile during the system enrollment. During the verification process, the respiratory features derived at run-time are continuously examined and compared to the user's profile by the system to either authenticate the legitimate user or reject a spoofing adversary, who tries to fool the system by mimicking the legitimate user's breathing patterns. To further identify the user's identity under the scenarios when multiple users are legitimate to access a service (e.g., the hot stove in a smart home could be used by both parents but not for grandparents and young kids), we build a two-layer deep neural network (DNN) model to learn high-level abstractions of intrinsic human respiration characteristics. The main contributions of our work are summarized as follows:

- We develop the first user verification system that is based on human natural breathing motions without requiring user's active participation of providing specific respiratory gestures.
- Our system can be easily integrated into any WiFi-enabled devices (e.g., laptops, smartphones, and smart appliances) to perform contactless and continuous user verification by integrating the morphologic-based features and fuzzy-wavelet-packet-based features together to model the unique respiratory biometrics.
- Our system detects the existence of a spoofing attack by developing a spoofing detection mechanism and further perform user identification by using the distinct biometric information rooted in respiratory motions based on deep-learning techniques.
- Our system is evaluated through extensive experiments involving 20 subjects with different setups of WiFi devices and attack models. The results demonstrate that our system can achieve over 95% verification/authentication success rate and robustly detect spoofing attacks with over 92% accuracy and less than 5% false positive rate.

II. Related Work

Biometric-based User Verification. A couple of approaches have been developed to identify the user's identity based on their highly discriminative physiological-based biometrics (e.g. fingerprint [2] and iris [17]), behavioral-based biometrics (e.g., gait pattern [28], keystroke/mouse dynamics [31] or vibration-based finger-input [20]). However, these verification schemes not only require dedicated sensors but also are vulnerable to replay/spoofing attacks (e.g., gummy finger [9]).

Continuous User Verification. To avoid critical security flaws in one-time verification methods, continuous user verification is emerging in the security communities. For instance, some approaches leverage physiological biometrics, such as facial recognition [29] and heartbeat vital signals [10], as well as behavioral biometrics (e.g., touch dynamics [8] and gait patterns [28]). Although these studies provide solutions for continuous user verification, they either require dedicated devices or rely on users' active participation, which are unscalable and obtrusive in reality.

Vital Signs based Verification. Existing studies have shown that the uniqueness of heartbeat/respiration dynamics among different people can be used for identifying users. For instance, heartbeat-based verification has been mainly studied by utilizing electrocardiogram (ECG) [13], [26] and photoplethysmography (PPG) [14], [15]. Cardiac Scan [19] performs cardiac dynamic-based verification using the dedicated Doppler radar. These systems, however, either require users to attach the dedicated devices on their body or require the user to sit in front of the radar device, which is not convenient in many application scenarios. Moreover, BreathPrint [4] uses breathing sound for user verification. However, it requires the user to hold the mobile devices very close to the user's nose, which is not applicable in many practical scenarios.

Radio-based Sensing/Verification. Wireless radio signals have been utilized to monitor and detect human activities in a contactless and privacy-preserving way, such as daily activities recognition [34], [35] and human dynamics [11], etc. Some recent studies identify users according to the distinct CSI changes associated with human's daily activities [30] and gait pattern [33]. However, these systems require the users to be involved in particular activities. Recently, an increasing

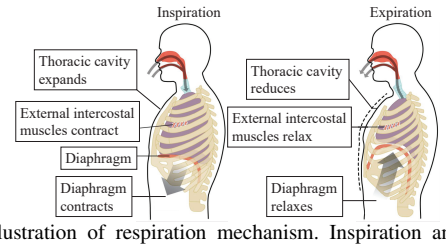
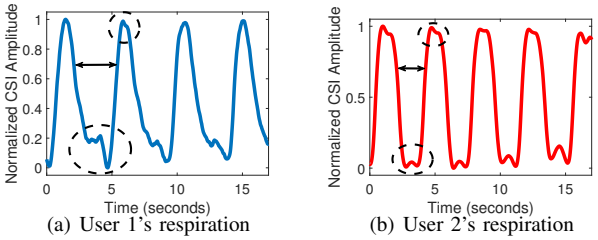


Fig. 2. Illustration of respiration mechanism. Inspiration and expiration occur due to the expansion and contraction of the thoracic cavity, respectively [5].



(a) User 1's respiration (b) User 2's respiration

Fig. 3. Distinct respiration patterns captured by CSI measurements.

trend is shown in investigating the non-contact ways of analyzing vital signs such as heartbeat and respiration for well-being. The researchers have shown the success of using either Received Signal Strength (RSS) [1] or CSI [21], [23] from existing WiFi to track human's vital signs (i.e., breathing and heart rates).

Differently, we take one step further to use the prevalent off-the-shelf WiFi devices to extract the unique biometrics rooted in respiratory motions for verification, which does not require user's active participation and enables continuous user verification in a non-contact, unobtrusive manner.

III. Feasibility Study

A. Unique Biometric Information in Respiration

In general, the process of human respiration comprises two stages, inspiration and expiration [5], which are illustrated in Figure 2. During inspiration, the size of the thoracic cavity increases due to the contractions of the diaphragm and intercostal muscles. While during expiration, the diaphragm and intercostal muscles relax and the size of the thoracic cavity decreases. Due to the human complex and diverse physiological structure (e.g., the strength of the diaphragm and intercostal muscles and volume of the thoracic cavity), the respiratory motions associated with chest movements and abdominal movements would present distinct magnitudes and patterns from person to person. Existing studies have confirmed that people's respiratory motions have unique biometric information. For instance, Parreira et al. [24] find the significant differences in breathing patterns and thoracoabdominal motions among 109 participants. Moreover, it has been shown that the uniqueness of an individual's respiratory motion would remain the same for a long time despite the changes in ages, smoking habits, weight, and mild respiratory diseases [27]. The diaphragm contractions caused by breathing happen without conscious volition most of the time [7]. Thus, the distinct respiratory motion, which is a spontaneous thoracic movement, can be regarded as an ideal biometric for continuous user verification.

B. Capturing Unique Respiratory Biometrics Using WiFi

A few existing studies (e.g., [21], [32]) have shown the success of using CSI of existing WiFi signals to continuously track the user's breathing rate. Compared to the RSS-based approaches, the fine-grained CSI provides both amplitude and phase information of multiple OFDM subcarriers that respectively experience distinct multipath and shadowing effects, which can derive more accurate and respiratory patterns. In this work, we take one step further and find that the highly sensitive CSI can further capture the unique biometric information carried by the respiratory motions. Figure 3 shows the filtered CSI amplitude values at a subcarrier extracted from a mobile device (i.e., laptop) when two people are respectively sitting in front of the device and breathing normally. We observe that the CSI patterns corresponding to two people are significantly different in terms of the periodic patterns and morphological characteristics, such as pulse width, small fluctuations around the wave peak/trough in the figure, which motivates us to use pervasive WiFi signals to capture such unique respiratory motions for user verification.

System Challenges. 1) The system should be robust to interferences and noises so that it can reconstruct reliable respiratory patterns from WiFi signals in real-world wireless environments; 2) The system needs to extract users' unique respiratory biometrics from the wireless signals affected by the subtle respiratory motions to discriminate people; and 3) We need to develop an easy-to-deploy verification model that can accurately detect spoofing attacks and identify users' identities on mobile devices.

Applications. Respiratory motions, as a spontaneous activity and critical metrics for evaluating a person's health conditions, could be used to facilitate many emerging applications such as liveness detection, sleep monitoring, and early detection of diseases, etc. In this work, we take one step further and show the feasibility of using respiratory biometrics to contentiously authenticate and identify individuals, which can be used in various domains, such as customized services, surveillance system, and access management.

IV. Attack Model & System Overview

A. Attack Model

Random Attack. An adversary does not have any knowledge of the user's respiratory pattern. When attacking the system, the adversary stays in the same position as the user does and breathes in a randomly chosen style regarding the breathing rate, inhale/exhale rhythm, and depth.

Imitation Attack. An adversary has observed how the user passes the system using breath multiple times. The adversary stays in the same position as the user does and tries to mimic the user's breathing pattern to pass the system.

B. System Overview

The basic idea of our system is to examine the fine-grained CSI of WiFi signals and extract the unique biometric information rooted in users' respiratory motions. The flow

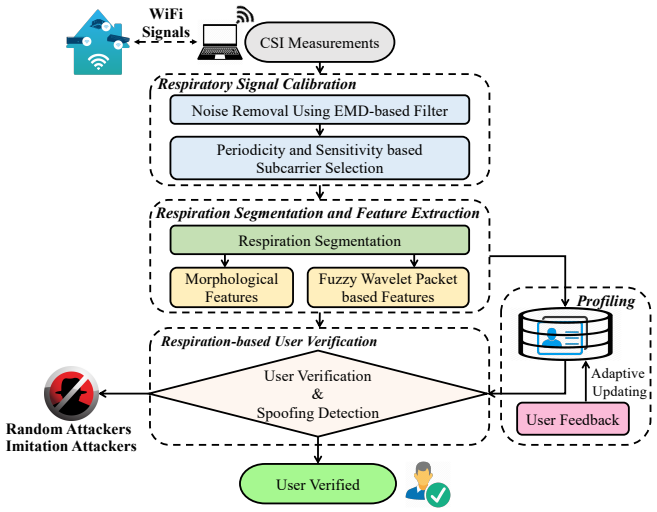
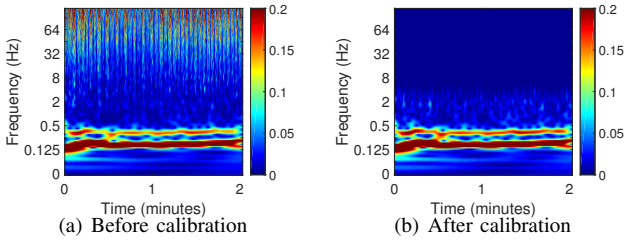


Fig. 4. Overview of system flow.

of our user verification system is illustrated in Figure 4. The system first collects time-series CSI measurements of 30 OFDM subcarrier groups from normal WiFi traffic via mobile devices (e.g., laptop). Once the system determines that the wireless signals contain repetitive respiratory patterns by finding the respiratory frequency components, it performs the *Respiratory Signal Calibration* to obtain reliable CSI measurements related to respiratory motions. The collected data is then processed to remove ambient noises via the *Empirical Mode Decomposition (EMD) based Filter*. The proposed EMD-based filter can adaptively remove the noisy components (e.g., immanent/environmental noises and irrelevant body interference) based on the data analysis and best preserve the frequency components related to respiratory motions. To obtain the most reliable respiratory signals, we utilize a *Periodicity and Sensitivity based Subcarrier Selection* strategy to select the subcarrier that is the most sensitive to minute human body movements by comparing the periodicity and variance of the CSI measurements.

The system then performs *Respiration Segmentation and Feature Extraction* to segment respiration cycles and extract corresponding distinctive respiratory features. To ensure that our system captures the unique biometric information in a complete respiratory cycle, the system performs the *Respiration Segmentation* to determine the segment of CSI measurements containing a respiratory trough-crest pattern by identifying the alternative increasing and decreasing trends (i.e., a down-up-down pattern) resulted from the inhalation and exhalation processes. Next, we use the *Respiration Feature Extraction* to derive unique respiration-related biometrics from the CSI measurements in each respiration segment. We particularly adopt two types of respiration features that can comprehensively describe the unique biometric information rooted in respiratory motions: *Morphological Features* and *Fuzzy Wavelet Packet Transform (FWPT) Features*. The morphological features focus on the shapes of the respiration-related CSI patterns and capture the physiological characteristics of respiratory motions (i.e., respiration depths and durations in different breathing stages). In addition, the FWPT features analyze the respiration segment in the frequency domain using the wavelets in different scales, which generates more fine-grained features that can reflect the complicated frequency characteristics of respiratory motions.



(a) Before calibration (b) After calibration

Fig. 5. Scalogram of a single subcarrier before and after EMD-based filtering.

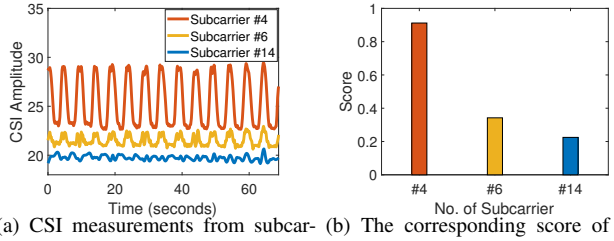
The extracted respiration features are used to construct profiles for legitimate users when they enroll in the system. After enrollment, the system takes the respiration features of the incoming respiration segments as the input to perform the *Respiration-based User Verification*. Specifically, during the verification phase, Breath ID determines as user access or not by checking a threshold to compute the feature distance between the incoming data and all users' profiles. Further, our system can recognize the legitimate user's identity by using the Deep Neural Network (DNN) classifier and defend against various types of attacks (e.g., random attacks or imitation attacks). We note that the user's breathing motions are usually stable in their daily lives. If the user's breathing pattern has a great change due to strenuous exercises or fluctuating emotions, our system is designed to take the user's feedback and perform an adaptive profile update to accommodate the changes.

V. Respiratory Signal Calibration

A. EMD-based Noise Removal

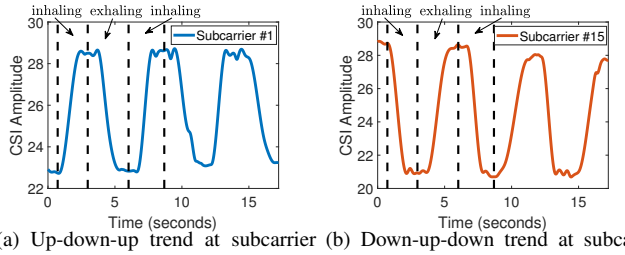
The CSI measurements collected in real environments usually contain interferences and noises introduced by communication hardware (e.g., unstable transmission power and frequencies) and environmental radio signals. Figure 5(a) shows an example of the scalogram of the time-series CSI measurements collected by a mobile device when a user is sitting in a typical lab room. We can observe that the scalogram exhibits high energy level in both respiratory frequency band (i.e., around 0.2-0.4 Hz [3]) and other frequency band (i.e., $>$ 4Hz).

To mitigate the impact of such noises, we use Empirical Mode Decomposition (EMD) based filter [12] to remove the irrelevant signals (i.e., signals out of the respiratory frequency band). Compared to the conventional de-noising methods (e.g., low-pass or band-pass filtering), EMD-based filtering is fully data-driven and can filter out the non-signal components dynamically based on the signal itself instead of the fixed cutoff frequency. Specifically, EMD first performs the decomposition of the collected CSI measurements $H_i(t)$ at the i^{th} subcarrier into a series of the intrinsic mode functions (i.e., $IMF_n(t), n = 1, 2, ..., M$) through the sifting process [12]



(a) CSI measurements from subcarrier #4, #6, #14 (b) The corresponding score of the three subcarriers

Fig. 6. Illustration of the periodicity and sensitivity based subcarrier selection.



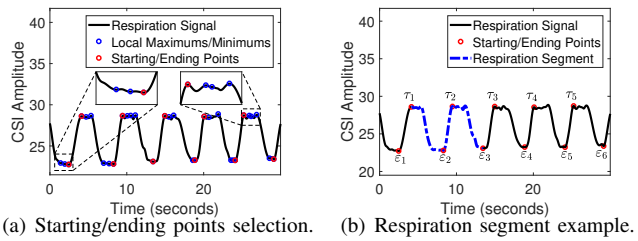
(a) Up-down-up trend at subcarrier #1 (b) Down-up-down trend at subcarrier #15

Fig. 7. Illustration of different CSI patterns corresponding to the same respiratory motions at two different subcarriers.

and a residual $r(t)$: $H_i(t) = r(t) + \sum_{n=1}^{M} IMF_n(t)$. Each decomposed IMF has the intrinsic time scale of the raw signal, starting from high-frequency modes to low-frequency modes. In order to keep the respiration related signals that are in a relatively lower-frequency band, we only keep the last $(M\text{-}K{+}1)$ IMFs with lower-frequency components to obtain the de-noised signals $\widetilde{H}_i(t)$: $\widetilde{H}_i(t) = r(t) + \sum_{n=K}^{M} IMF_n(t)$, where K is between $[1, M]$. To determine the optimal index K, we compute the mutual information [22] between the respiratory components (i.e.,$\sum_{n=K}^{M} IMF_n(t)$) and noise components (i.e., $\sum_{n=1}^{K-1} IMF_n(t)$) with all possible values of K. The index K corresponding to the maximum mutual information will be regarded as the optimal one. As illustrated in Figure 5(b), the CSI signals in the high-frequency band (i.e. $>$ 4Hz) are clearly eliminated after applying our EMD filtering with the optimal K.

B. Periodicity and Sensitivity based Subcarrier Selection

Because each subcarrier experiences unique multipath and shadowing effects, we observe that the CSI of different subcarriers have different sensitivities to subtle respiratory motions. Our system needs to identify the subcarrier that captures the most unique biometric information to ensure the accurate user verification. Along with this direction, we propose to find the subcarrier having the strongest periodicity and sensitivity, and use it to extract the biometrics of respiration. The insight is that the time series of CSI significantly affected by respiration should present a continuous sinusoidal-like pattern with a high level of periodicity due to the periodical nature of human respiration. Moreover, the more sensitive the subcarrier is to respiratory motions, the more comprehensive characteristics of respiratory motions can be captured by CSI. Specifically, we quantify the i^{th} subcarrier's periodicity (i.e., ρ_i) using Fisher's Kappa [6],



(a) Starting/ending points selection. (b) Respiration segment example.

Fig. 8. Illustration of respiration segmentation.

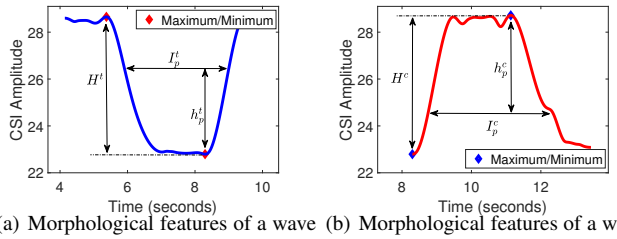
which is defined as: $\rho_i = \frac{max(PSD(\widetilde{H}_i(t)))}{\overline{PSD(\widetilde{H}_i(t))}}$, where PSD denotes the power spectral density of the signal. Higher ρ indicates stronger periodicity of the corresponding signals. In addition, we utilize the variance of CSI amplitude to quantify the i^{th} subcarrier's sensitivity (i.e., γ_i) to minute movements: $\gamma_i = \frac{\sum(\widetilde{H}_i(t) - \overline{\widetilde{H}_i(t)})^2}{N}$, where N denotes the length of the signal $\widetilde{H}_i(t)$. Higher variance means more significant amplitude changes in CSI and stronger impact of respiratory motions to the subcarrier. Finally, we add the normalized Fisher's Kappa and variance with same weight (i.e., 0.5) crossing all the subcarriers to select the most sensitive subcarrier for respiration analysis. As an illustration, Figure 6(a) depicts the extracted respiration signals from three subcarriers (i.e. #4, #6, #14). We can observe that the signal of subcarrier #4 has the greater periodicity and higher amplitude of fluctuation than other two subcarriers, which corresponds to the top score shown in Figure 6(b).

VI. Respiration Segmentation & Feature Extraction

A. Respiration Segmentation

Due to the multipath and shadowing effects, different subcarriers have different CSI amplitudes even when they are caused by the same respiratory motion. As shown in Figure 7, the derived respiration signals at subcarrier #1 exhibit an *up-down* trend during a complete respiration cycle (i.e., inhalation and exhalation), whereas the signals at subcarrier #15 exhibit an opposite trend. This observation indicates that the cause of the crests (i.e., *up-down* trend) or troughs (i.e., *down-up* trend) is not deterministic and could be either inhalation or exhalation. Therefore, we define the conjoint trough and crest (i.e., each *down-up-down* trend) as a *respiration segment*, which at least includes one inhaling-exhaling stage or one exhaling-inhaling stage.

Intuitively, the respiration segments can be determined by finding the local maximums/minimums in the respiration signals. However, multiple local maximums/minimums would be found on one crest or trough as illustrated in Figure 8(a) due to the signal fluctuation. To find the unique maximum/minimum points indicating the starting and ending times of inhalation or exhalation, we develop a *Starting/Ending Points Selection* approach , which applies two thresholds (i.e., T_{max} and T_{min}) to restrict the minimum distances between two neighboring maximums or minimums, respectively. The thresholds are determined by



(a) Morphological features of a wave trough (b) Morphological features of a wave crest

Fig. 9. Illustration of extracting morphological features from a respiration segment.

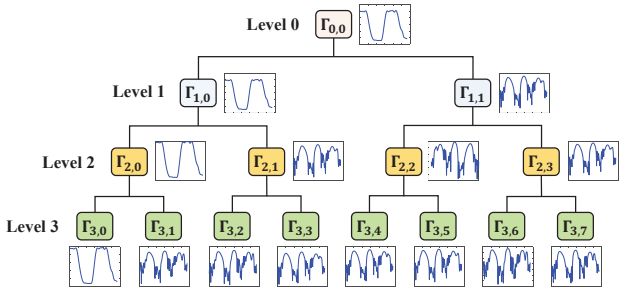


Fig. 10. Illustration of a 3-level fuzzy wavelet packet transformation.

the average distance between every two neighboring local maximums/minimums. Additionally, to make each segment consistent, the leftmost local maximum on a crest and the rightmost local minimum on a trough are selected as starting and ending point respectively. Based on the detected starting and ending point, the respiration segment (i.e., each *down-up-down* trend) can be obtained accordingly. For instance, the waveform between the starting point τ_1 and the second ending point after τ_1 (i.e., ε_3) is used to determine a respiration segment as illustrated in Figure 8(b).

B. Morphological Features

In order to obtain unique respiratory characteristics, we first perform morphology analysis in each respiration segment to extract representative features. We conduct multi-dimensional extraction of the morphological characteristics, resulting in total 100 features that characterize representative patterns in each respiration segment. Specifically, the *down-up-down* trend of each respiration segment consists of one wave trough and one wave crest, as shown in Figure 8(b). For the wave trough as illustrated in Figure 9(a), H^t represents the height of the wave trough defined as the difference between the maximum amplitude and the minimum amplitude. h_p^t denotes the $p\%$ of the height H^t from the minimum point and I_p^t is the intercept of the waveform at the height h_p^t. Therefore, the morphological feature at $p\%$ of the trough height is expressed as: $e_p^t = \frac{I_p^t}{h_p^t}$, which is able to reflect the relationship between the respiration depth and respiration time duration when a respiratory motion is finished $p\%$. Similarly, for the wave crest in the respiration segment as shown in Figure 9(b), the morphological feature at $p\%$ of the crest height is defined as: $e_p^c = \frac{I_p^c}{h_p^c}$. We take $p = \{2, 4, ..., 100\}$ to compute 50 morphological features for a wave trough and crest, respectively. The total 100 morphological features then can be obtained for each respiration segment.

C. Fuzzy Wavelet Packet Based Features

In addition to the morphological features, our system performs fuzzy wavelet packet transform (FWPT) [16] on each respiration segment to construct the features that highly correlate with respiratory motions. The wavelet packet transform can realize fine-grained multi-resolution (i.e., time-frequency) analysis to differentiate the minuscule differences of respiratory motions from person to person. This trait can be utilized for analyzing the respiration-induced movements and vibrations of different parts of the body (e.g., thoracic movements, abdominal movements, and chest vibration caused by heartbeat) in varied frequency domains for better capturing the distinct respiration biometrics. Also, the wavelet analysis can locate the time periods for different stages of respiratory motion.

Specifically, FWPT is based on the wavelet packet decomposition, which is an expansion of the discrete wavelet transform (DWT) whereby both the approximation and detail subspaces are decomposed. In particular, Figure 10 shows an example of 3-level wavelet packet decomposition, where $\Gamma_{0,0}$ denotes the original signal space and $\Gamma_{j,k}$ denotes the decomposed subspace with j denoting the decomposition level and k denoting the subspace index at the j_{th} level. The signal space $\Gamma_{j,k}$ at the upper level is decomposed into two orthogonal subspaces, approximation subspace $\Gamma_{j+1,2k}$ and detail subspace $\Gamma_{j+1,2k+1}$. The efficacy of wavelet packet transform relies on choosing the proper wavelet basis, which determines whether the decomposed subspaces are highly distinguishable among individuals. To select the best wavelet basis in FWPT, fuzzy-entropy-based mutual information (MI) method [16] is applied. We finally perform 7 levels fuzzy wavelet packet decomposition which obtains $\sum_{j=0}^{7} 2^j$ (i.e., 255) wavelet subspaces. We then empirically choose the *standard deviation* and *skewness* of each subspace signal as the representative features for each subspace to generate total 510 FWPT based features for each respiration segment.

VII. Respiration-based User Verification

A. User Verification Approach

We first examine the feature distance between the incoming respiration segment and the legitimate user's profile to identify the user and detect spoofing attacks. Intuitively, if the incoming respiration segment is from the user, the feature distance should be small to the legitimate user's profile, otherwise, the feature distance should be large. In particular, we calculate the Euclidean distance in the feature space using the following equation: $(\lambda^x, \upsilon^n) = \sqrt{\sum_{i=1}^{M}(\lambda_i^x - \upsilon_i^n)^2}$, where $\lambda^x = \{\lambda_1^x, \lambda_2^x, ..., \lambda_M^x\}$ represents the feature vector of the incoming respiration segment, M=610 is the feature vector length. $\upsilon^n = \{\upsilon_1^n, \upsilon_2^n, ..., \upsilon_M^n\}$ denotes the feature set of the n_{th} legitimate respiration segment. We then select the top k smallest distances to the legitimate user's profile (i.e., respiration segments), and detect the presence of spoofer by comparing the mean value of the k smallest distances to

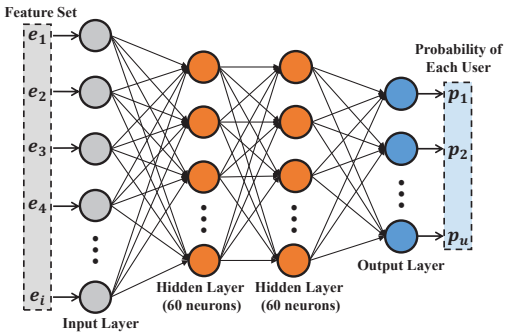


Fig. 11. Structure of the DNN model for legitimate user identification.

a pre-defined threshold η. In our case, we empirically set k=10, and the optimal threshold η for spoofing detection is decided by the ROC curve analysis, which is presented in Section VIII-A4. Note that our method could be easily extended to multiple users case, in which we select the top k smallest distances to all the legitimate users' profiles and compare the mean value of these distances to η.

B. Deep Learning based Legitimate User Identification

When multiple users enroll in the system, we adopt a neural-network-based classifier to differentiate the users. Considering to learn complex non-linear biometric abstractions, we develop a deep neural network (DNN) model [18] leveraging the extracted respiration features. The architecture of our DNN model is shown in Figure 11, which is a two-hidden-layer neural network with 60 neurons in each layer. The weights of hidden neurons are chosen randomly in the initial network. During training this neural network, the weights would be tweaked using scaled conjugate gradient (SCG) backpropagation algorithm [18] according to the training set.

Given an input of respiration feature vector to our trained DNN model, each neuron in the first hidden layer multiplies them by a weight factor and calculates the sum as the output: $o_i^{(1)} = b_i^{(1)} + \sum_j e_j \cdot \omega_{j,i}^{(1)}$, where $o_i^{(1)}$ denotes the output of the i_{th} neuron and $\omega_{j,i}^{(1)}$ represents the connecting weight from the j_{th} feature to the i_{th} neuron in the first hidden layer. $b_i^{(1)}$ is a bias added to the i_{th} neuron. The output of each neuron is then passed to the second hidden layer as the input through a non-linear sigmoid function: $\frac{1}{1+exp(o_i^{(1)})}$. After that, the model uses the same strategy as in first hidden layer to obtain the output $o_i^{(2)}$ in the second hidden layer. In the last output layer, the posterior probability p_u of u_{th} legitimate user is estimated based on $o_i^{(2)}$ by using the softmax function as follows: $p_u = \frac{exp(b_u^{(o)} + \sum_i o_i^{(2)} \cdot \omega_{i,u}^{(o)})}{\sum_i exp(o_i^{(2)})}$, where $\omega_{i,u}^{(1)}$ represents the connecting weight from the i_{th} neuron of the second hidden layer to the u_{th} user neuron in output layer. $b_u^{(o)}$ is a bias added to the u_{th} user neuron. Finally, the system identifies the legitimate user based on which class achieves the maximum posterior probability.

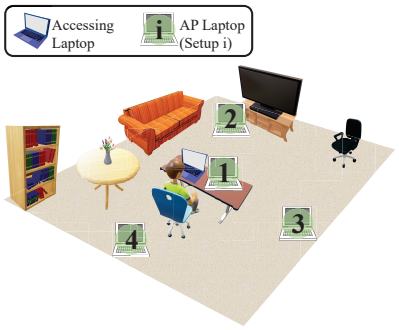


Fig. 12. Illustration of experimental setups.

C. Majority Voting Using Multiple Segments

To ensure the high verification accuracy, we devise a majority voting process to combine the results of multiple segments. In particular, for the user verification or legitimate user identification results of multiple respiration segments, if most of the segments are verified/identified as one subject (e.g., spoofer or a specific legitimate user), then our system would follow the majority voting decisions. This process can help to greatly reduce the verification errors and improve the robustness of our system.

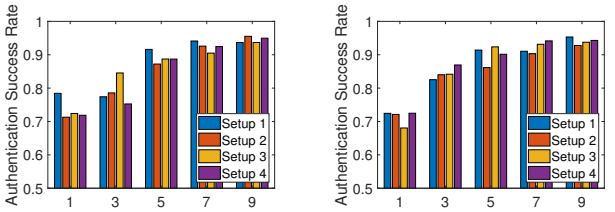
VIII. Performance Evaluation

A. Experimental Methodology

1) Devices and Network: We conduct experiments in an 802.11n WiFi network. Specifically, we deploy two Dell E6430 laptops to exchange WiFi packets periodically. Both laptops run Ubuntu 14.04 LTS with the 4.2.0 kernel and are equipped with an Intel WiFi Link 5300 card for measuring CSI. The packet transmission rate is set to 200 pkts/s in our experiments. We also studied the impact of packet transmission rate on the system in Section VIII-C.

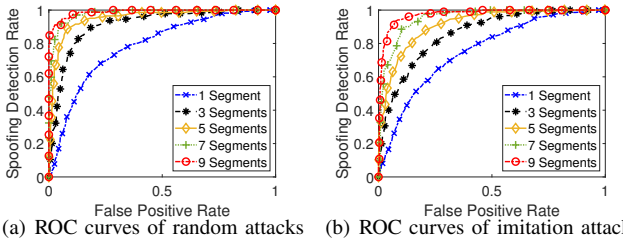
2) Setups of WiFi Devices: Our system is evaluated in a university office with the size of $17ft \times 9ft$, as shown in Figure 12, in which two laptops generate WiFi traffics continuously. One of them is used as the *Accessing Laptop* that the target user is operating. Another laptop (i.e., *AP Laptop*), emulated as the access point, is used to exchange WiFi traffic with the accessing laptop. The target user sits on a chair in front of *Accessing Laptop* and breath regularly during the experiment. The distance from the user to the accessing laptop is about 0.2 meter, which is a common distance that most people would use when operating the device (e.g., laptop, smart appliances). *AP Laptop* is placed at 4 different positions in the room to study the impact of various device setups in practical scenarios. Specifically, Setup 1 is the scenario where the two laptops are placed side by side at 180 degrees on the desk. For Setup 2, 3, 4, the AP laptop is placed 2 meters away from the participant's front, right side and back, respectively.

In order to explore the impact of different distances between the user and the accessing mobile device, we test the distances 0.4 meters, 0.6 meters, 0.8 meters and 1 meter under Setup 1. In addition, we also perform experiments



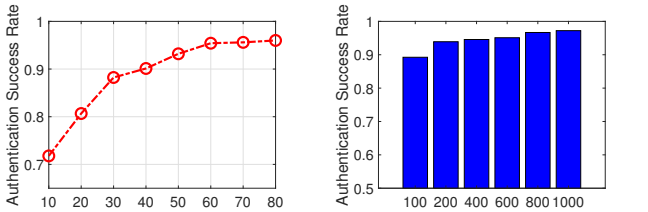
(a) One legitimate user (b) Five legitimate users

Fig. 13. Performance of user verification with different numbers of respiration segments for testing.



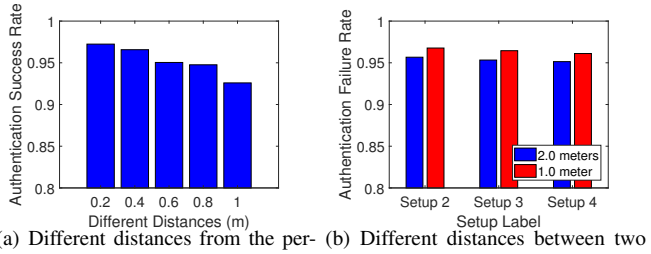
(a) ROC curves of random attacks (b) ROC curves of imitation attacks

Fig. 14. System performance under random attacks and imitation attackers with different numbers of respiration segments for testing.



(a) Impact of training size (b) Impact of packet transmission rates

Fig. 15. User verification performance with different training sizes and packet transmission rate.



(a) Different distances from the person to accessing laptop (b) Different distances between two WiFi devices

Fig. 16. User verification performance with different distances.

with the longer distance (i.e., $d = 2.0m$) between the AP laptop and the accessing laptop using Setup 2, Setup 3, Setup 4, respectively. The aforementioned impacts of various distances will be discussed in Section VIII-C.

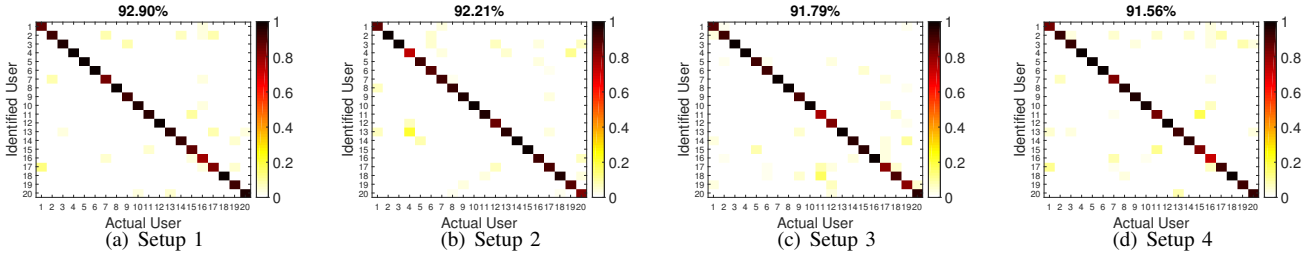
3) Data Collection: In the data collection, 20 subjects (i.e., 14 males and 6 females) aging from 21 to 32 are involved in the experiments. We collect around $200 - 300$ respiration segments for each subject sitting in the chair for each experimental setup. Each subject's respiration data are collected with multiple rounds in a long time span (i.e., four months), during which the participants perform normal breathing without any instructions and restrictions. Through our evaluation performance, we find that our system is robust to the changes in the users' emotion and physical conditions crossing different days. To construct the legitimate user profiles, 60 respiration segments of each legitimate subject are pre-stored for training and the rest of segments are used for testing. Moreover, we use the data collected in Setup 1 to evaluate our system under random attacks, in which 5 of the 20 subjects are considered as legitimate users and the other 15 subjects act as attackers. When the system is under imitation attacks with Setup 1, 1 subject acts as the legitimate user and 10 other subjects try to imitate the legitimate one's breathing style (e.g., breathe with similar breathing depth/duration and holding duration) to pass the system after watching a pre-recorded video of the legitimate user's breathings multiple times. We further collect around $200 - 300$ respiration segments for each attacker in this case.

4) Evaluation Metrics: (1) Authentication Success Rate. The percentage of legitimate instances correctly verified by our system; *(2) False Positive Rate.* The percentage of legitimate instances that are mistakenly detected as attacker instances; *(3) Spoofing Detection Rate (True Positive Rate).* The percentage of attack instances that are correctly detected. *(4) Receiver Operating Characteristic (ROC).* ROC curve shows the trade-off between the False Positive Rate and Spoofer Detection Rate under different values of threshold. The more the ROC curve hugs the point (0, 1), the better the performance. The minimum distance between the point (0, 1) of ROC space and any point on ROC curve gives the optimal threshold. *(5) Confusion Matrix.* The degree of color darkness in the matrix corresponds to the percentage of correctly identified instances of DNN.

B. Performance of User Verification

Figure 13 illustrates the user authentication success rate when different numbers of respiration segments are available for testing. Specifically, Figure 13(a) depicts the authentication success rate when the system only contains one legitimate user under different setups. We observe that all four setups achieve comparable authentication accuracy. The average authentication success rate achieves around 90% accuracy when five or more respiration segments are used for testing. When the system has multiple registered users for different setups, it can achieve similar authentication accuracy as illustrated in Figure 13(b).

Moreover, we evaluate our system under random attacks and imitation attacks. In the random attack experiment, we consider 5 of the 20 subjects as legitimate users and the other 15 subjects act as spoofers. Figure 14(a) depicts the ROC curves with different numbers of segments for testing. We can see that our spoofing detection rate reaches to over 92.14% with a false positive rate of around 5% when the system integrates the testing results of 9 respiration segments. While in the imitation attack, 1 participant acts as the legitimate user and 10 participants try to imitate the legitimate user's breathing style (e.g., breathe with similar breathing depth/duration and holding duration). We demonstrate that our system can also detect the imitation attacks with a high accuracy and a low false positive rate, which are presented



(a) Setup 1 (b) Setup 2 (c) Setup 3 (d) Setup 4

Fig. 17. Performance of deep learning-based legitimate user identification with 4 different setups.

in Figure 14(b). Specifically, we can achieve over 89.24% detection rate with 5% false positive rate when the system combines the testing results of 9 respiration segments. All the above results validate the great robustness of the proposed system under both random and imitation attacks.

Additionally, from the results above, we confirm the effectiveness of our majority voting algorithm using multiple respiration segments for testing. As we can see from the Figure 13, the average authentication success rate is greatly increased from around 72% to over 93%, given the number of respiration segments from 1 to 9. We have the same observation on the system performance under various attacks as shown in Figure 14. When there are more available respiration segments for testing, the ROC curve hugs the point (0,1) more, which indicates the system has better performance on the spoofing attack detection.

C. Impact of Various Factors

We then use Setup 1 to evaluate the user verification performance of our system with various factors while the system has 5 registered users.

Impact of Training Size. As shown in Figure 15(a), the average authentication success rate of 20 subjects shows the growing trend with the increasing training size. In particular, our system achieves an average authentication success rate of 71.78% with a small training size of 10. While increasing the number of training samples to 30, the average authentication success rate then grows dramatically to over 88%. If we set the training samples to over 60, the system can achieve a comparable authentication success rate of over 94%. Therefore, the training size is decided to be 60 in our system, which can achieve both good verification performance and reasonable training time duration.

Impact of Packet Transmission Rate. Figure 15(b) presents an average authentication success rates of 20 subjects under various packet rates from $100pkts/s$ to $1000pkts/s$. We can observe that the system can maintain high accuracy across different packet rates. Particularly, the authentication success rate is up to 97.22% under the sampling rate of $1000pkts/s$. Moreover, our system can still achieve the accuracy over 89% even for the low sampling rates such as $100pkts/s$. The above observations confirm that the system can be applied to mobile devices with different sampling capabilities.

Impact of Distance. We further study the performance of user verification under various distances (i.e., $0.2m$ to $1.0m$) between the target user and the accessing laptop. As shown in Figure 16(a), even for the longer distances ($0.8m$ and $1.0m$), we can still achieve a high authentication success rate of 94.76% and 92.59%, respectively. In addition, we also evaluate our system with 10 subjects under longer distances (i.e., d=$2.0m$) between the accessing laptop and the AP laptop using Setup 2, Setup 3 and Setup 4, respectively. Figure 16(b) depicts the performance comparison of distances $1.0m$ and $2.0m$ under different setups. We observe that the authentication success rates of three setups with a $2.0m$ distance all kept great authentication performance of over 95%. It demonstrates that our system is applicable with various practical device setup requirements.

D. Performance of Legitimate User Identification

We further examine the system's legitimate user identification performance. Figure 17 plots the color-scale maps of the confusion matrices for the legitimate user identification with 9 respiration segments with four different setups of WiFi devices. We find that only few respiration segments are mistakenly identified as belonging to incorrect users in all setups. Setup 1 achieves the highest average identification accuracy of 92.90% because the two devices are placed close to each other, which guarantees the steady exchange of WiFi packets. Other three setups, which places the AP laptop apart from the accessing laptop, also have comparable high accuracies. In particular, the average accuracies are 92.21%, 91.79%, 91.56% for Setup 2, Setup 3, and Setup 4, respectively. This demonstrates that the system can accurately identify legitimate users under various practical scenarios.

IX. Conclusion

In this paper, we propose a continuous user verification system, which leverages the fine-grained respiratory biometrics captured by commodity WiFi devices. By in-depth study, we determine the unique representative CSI features that can best model users' respiratory motions by using the waveform morphology analysis and fuzzy wavelet transformation. We also develop a deep learning based user verification scheme as well as a unique respiration distance based spoofer detection approach to identify users and reject spoofers. We conduct extensive experiments with 20 subjects and various WiFi device setups regarding different practical applications. The results demonstrate that the proposed system can verify users with high accuracy and is resilient to spoofing attacks.

X. Acknowledgment

This work was supported in part by the National Science Foundation grants CNS1820624, CNS1826647, and Army Research Office grant W911NF-18-1-0221.

REFERENCES

[1] H. Abdelnasser, K. A. Harras, and M. Youssef. Ubibreathe: A ubiquitous non-invasive wifi-based breathing estimator. In *Proceedings of the 16th ACM International Symposium on Mobile Ad Hoc Networking and Computing (ACM MobiHoc)*, pages 277–286, 2015.

[2] A. Arakala, J. Jeffers, and K. J. Horadam. Fuzzy extractors for minutiae-based fingerprint authentication. In *Proceedings of the Springer International Conference on Biometrics*, pages 760–769, 2007.

[3] K. E. Barrett, S. M. Barman, S. Boitano, and H. Brooks. Ganong's review of medical physiology. 23. *NY: McGraw-Hill Medical*, 2009.

[4] J. Chauhan, Y. Hu, S. Seneviratne, A. Misra, A. Seneviratne, and Y. Lee. Breathprint: Breathing acoustics-based user authentication. In *Proceedings of the 15th Annual International Conference on Mobile Systems, Applications, and Services (ACM MobiSys)*, pages 278–291, 2017.

[5] O. College. *Anatomy and physiology*. Rice University, 2013.

[6] R. Cutler and L. S. Davis. Robust real-time periodic motion detection, analysis, and applications. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 22(8):781–796, 2000.

[7] S. I. Fox. *Human Physiology 9th Editon*. McGraw-Hill press, New York, USA, 2006.

[8] M. Frank, R. Biedert, E. Ma, I. Martinovic, and D. Song. Touchalytics: On the applicability of touchscreen input as a behavioral biometric for continuous authentication. *IEEE transactions on information forensics and security*, 8(1):136–148, 2013.

[9] J. Galbally, R. Cappelli, A. Lumini, G. Gonzalez-de Rivera, D. Maltoni, J. Fierrez, J. Ortega-Garcia, and D. Maio. An evaluation of direct attacks using fake fingers generated from iso templates. *Pattern Recognition Letters*, 31(8):725–732, 2010.

[10] M. Guennoun, N. Abbad, J. Talom, S. M. M. Rahman, and K. El-Khatib. Continuous authentication by electrocardiogram data. In *Proceedings of the 2009 IEEE Toronto International Conference Science and Technology for Humanity (IEEE TIC-STH)*, pages 40–42, 2009.

[11] X. Guo, B. Liu, C. Shi, H. Liu, Y. Chen, and M. C. Chuah. Wifi-enabled smart human dynamics monitoring. In *Proceedings of the 15th ACM Conference on Embedded Networked Sensor Systems (ACM SenSys)*, 2017.

[12] N. E. Huang, Z. Shen, S. R. Long, M. C. Wu, H. H. Shih, Q. Zheng, N.-C. Yen, C. C. Tung, and H. H. Liu. The empirical mode decomposition and the hilbert spectrum for nonlinear and non-stationary time series analysis. In *Proceedings of the Royal Society of London A: mathematical, physical and engineering sciences*, volume 454, pages 903–995, 1998.

[13] S. A. Israel, J. M. Irvine, A. Cheng, M. D. Wiederhold, and B. K. Wiederhold. Ecg to identify individuals. *Pattern recognition*, 38(1):133–142, 2005.

[14] N. Karimian, Z. Guo, M. Tehranipoor, and D. Forte. Human recognition from photoplethysmography (ppg) based on non-fiducial features. In *Proceedings of the 2017 IEEE International Conference on Acoustics, Speech and Signal Processing (IEEE ICASSP)*, pages 4636–4640, 2017.

[15] N. Karimian, M. Tehranipoor, and D. Forte. Non-fiducial ppg-based authentication for healthcare application. In *Proceedings of the 2017 IEEE EMBS International Conference on Biomedical & Health Informatics (BHI)(IEEE EMBS)*, pages 429–432, 2017.

[16] R. N. Khushaba, S. Kodagoda, S. Lal, and G. Dissanayake. Driver drowsiness classification using fuzzy wavelet-packet-based feature-extraction algorithm. *IEEE Transactions on Biomedical Engineering*, 58(1):121–131, 2011.

[17] A. Kumar and A. Passi. Comparison and combination of iris matchers for reliable personal authentication. *Pattern recognition*, 43(3):1016–1026, 2010.

[18] Y. LeCun, Y. Bengio, and G. Hinton. Deep learning. *nature*, 521(7553):436, 2015.

[19] F. Lin, C. Song, Y. Zhuang, W. Xu, C. Li, and K. Ren. Cardiac scan: A non-contact and continuous heart-based user authentication system. In *Proceedings of the 23rd Annual International Conference on Mobile Computing and Networking (ACM MobiCom)*, pages 315–328, 2017.

[20] J. Liu, C. Wang, Y. Chen, and N. Saxena. Vibwrite: Towards finger-input authentication on ubiquitous surfaces via physical vibration. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (ACM CCS)*, pages 73–87, 2017.

[21] J. Liu, Y. Wang, Y. Chen, J. Yang, X. Chen, and J. Cheng. Tracking vital signs during sleep leveraging off-the-shelf wifi. In *Proceedings of the 16th ACM International Symposium on Mobile Ad Hoc Networking and Computing (ACM MobiHoc)*, pages 267–276, 2015.

[22] S. Liu, R. X. Gao, D. John, J. Staudenmayer, and P. Freedson. Tissue artifact removal from respiratory signals based on empirical mode decomposition. *Annals of biomedical engineering*, 41(5):1003–1015, 2013.

[23] X. Liu, J. Cao, S. Tang, and J. Wen. Wi-sleep: Contactless sleep monitoring via wifi signals. In *Proceedings of the 2014 IEEE Real-Time Systems Symposium (IEEE RTSS)*, pages 346–355, 2014.

[24] V. F. Parreira, C. J. Bueno, D. C. França, D. S. Vieira, D. R. Pereira, and R. R. Britto. Breathing pattern and thoracoabdominal motion in healthy individuals: influence of age and sex. *Brazilian Journal of Physical Therapy*, 14(5):411–416, 2010.

[25] J. R. Pinto, J. S. Cardoso, A. Lourenço, and C. Carreiras. Towards a continuous biometric system based on ecg signals acquired on the steering wheel. *Sensors*, 17(10):2228, 2017.

[26] K. N. Plataniotis, D. Hatzinakos, and J. K. Lee. Ecg biometric recognition without fiducial detection. In *Proceedings of the 2006 Biometrics Symposium: Special Session on Research at the Biometric Consortium Conference*, pages 1–6, 2006.

[27] M. Ragnarsdóttir and E. K. Kristinsdóttir. Breathing movements and breathing patterns among healthy men and women 20–69 years of age. *Respiration*, 73(1):48–54, 2006.

[28] Y. Ren, Y. Chen, M. C. Chuah, and J. Yang. User verification leveraging gait recognition for smartphone enabled mobile healthcare systems. *IEEE Transactions on Mobile Computing*, 14(9):1961–1974, 2015.

[29] P. Samangouei, V. M. Patel, and R. Chellappa. Attribute-based continuous user authentication on mobile devices. In *Proceedings of the 7th International Conference on Biometrics Theory, Applications and Systems (IEEE BTAS)*, pages 1–8, 2015.

[30] C. Shi, J. Liu, H. Liu, and Y. Chen. Smart user authentication through actuation of daily activities leveraging wifi-enabled iot. In *Proceedings of the 18th ACM International Symposium on Mobile Ad Hoc Networking and Computing (ACM MobiHoc)*, page 5, 2017.

[31] I. Traore, I. Woungang, M. S. Obaidat, Y. Nakkabi, and I. Lai. Combining mouse and keystroke dynamics biometrics for risk-based authentication in web environments. In *Proceedings of the Fourth International Conference on Digital Home Digital Home (IEEE ICDH)*, pages 138–145, 2012.

[32] H. Wang, D. Zhang, J. Ma, Y. Wang, Y. Wang, D. Wu, T. Gu, and B. Xie. Human respiration detection with commodity wifi devices: do user location and body orientation matter? In *Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing*, pages 25–36. ACM, 2016.

[33] W. Wang, A. X. Liu, and M. Shahzad. Gait recognition using wifi signals. In *Proceedings of the ACM International Joint Conference on Pervasive and Ubiquitous Computing (ACM UbiComp)*, pages 363–373, 2016.

[34] W. Wang, A. X. Liu, M. Shahzad, K. Ling, and S. Lu. Understanding and modeling of wifi signal based human activity recognition. In *Proceedings of the 21st ACM Annual International Conference on Mobile Computing and Networking (ACM MobiCom)*, pages 65–76, 2015.

[35] Y. Wang, J. Liu, Y. Chen, M. Gruteser, J. Yang, and H. Liu. E-eyes: device-free location-oriented activity identification using fine-grained wifi signatures. In *Proceedings of the 20th annual international conference on Mobile computing and networking (ACM MobiCom)*, pages 617–628, 2014.