Finger ECG-based Authentication for Healthcare Data Security Using Artificial Neural Network

Ying Chen
Biomedical Information Laboratory
The University of Aizu
Aizu-wakamatu, Fukushima
965-8580, Japan
Email: ychen@u-aizu.ac.jp

Wenxi Chen
Biomedical Information Laboratory
The University of Aizu
Aizu-wakamatu, Fukushima
965-8580, Japan
Email: wenxi@u-aizu.ac.jp

***Abstract*—Wearable and mobile medical devices provide efficient, comfortable, and economic health monitoring, having a wide range of applications from daily to clinical scenarios. Health data security becomes a critically important issue. Electrocardiogram (ECG) has proven to be a potential biometric in human recognition over the past decade. Unlike conventional authentication methods using passwords, fingerprints, face, etc., ECG signal can not be simply intercepted, duplicated, and enables continuous identification. However, in many of the studies, algorithms developed are not suitable for practical application, which usually require long ECG data for authentication. In this work, we introduce a two-phase authentication using artificial neural network (NN) models. This algorithm enables fast authentication within only 3 seconds, meanwhile achieves reasonable performance in recognition. We test the proposed method in a controlled laboratory experiment with 50 subjects. Finger ECG signals are collected using a mobile device at different times and physical statues. At the first stage, a "General" NN model is constructed based on data from the cohort and used for preliminary screening, while at the second stage "Personal" NN models constructed from single individual's data are applied as fine-grained identification. The algorithm is tested on the whole data set, and on different sizes of subsets (5, 10, 20, 30, and 40). Results proved that the proposed method is feasible and reliable for individual authentication, having obtained average False Acceptance Rate (FAR) and False Rejection Rate (FRR) below 10% for the whole data set.**

I. Introduction

To meet the worldwide increasing demand for healthcare, wearable and mobile medical devices have rapidly become a vital part of modern life over the past decades. These types of devices represent a promising platform for efficient, comfortable, and economic health monitoring, and enable a wide range of applications from daily to clinical scenarios. In that respect, management of the healthcare data and its security become critically important.

Biometric authentication has been attractive in recent decades for their usability in personal data security [1]–[3]. It measures unique features of human for identifying and authenticating approved users. Various biometrics have been introduced for application including face [4], fingerprints [5], iris [6], speech [7], and gait, etc. Electrocardiogram (ECG) is another potential distinctive characteristic for use in identify recognition problems. Unlike above external biometrics, ECG contains internal information that reflects how heart functions and its patterns reveal the anatomic structures of human heart and body. Because of this nature, ECG signals are highly personalized and appealing for authentication, as they are non-intrusive, continuously available, can only be measured in live subjects, and are not be simply imitated, or duplicated. It is particularly advantageous in clinical data protection because ECG data are sometimes already assessed as part of the patient regular physical exams and the measurements are nearly always guaranteed. Recent studies have revealed the validity of ECG signals for human identification [8]–[11], and specially applied for clinical data privacy [12]–[15].

The standard ECG recording using 12-lead apparatus guarantees high quality of signal collection, while its unfavorable property in data acquisition. It usually requires a professional operator to place the electrodes on the body, makes it inconvenient in practical application. One lead ECG, for example, finger-ECG, with only two electrodes (lead I), which is much more efficient and user-friendly in daily application.

ECG signal recognition are mostly based on fiducial and non fiducial features. Fiducial features include the amplitude, temporal, area, angle features from characteristic points on the ECG waveforms [8], [11], [16], [17], and non fiducial features such as wavelet coefficients or autocorrelation coefficients [18]. Most studies using fiducial features supposed that obtained ECG data are clean and with low level of noise. But in reality one-lead ECG signal, especially that collected by wearable devices sometimes are much more noisy compared to 12-lead ECG signals. In that case, authentication based on fiducial features, especially that requires accurate measurement of P, Q, R, S or T points, can not be simply applied to those real collected one-lead ECG signal. Here, we combined the use of both fiducial-based and non fiducial-based features. Fiducial feature includes the amplitude of QRST waveforms, which only requires the detection of R wave, and non fiducial features including QRST wave, QRS wave, the difference and kurtosis of QRST wave and QRS wave.

Classifications by template matching, using kNN, similarity or dissimilarity between ECG phase space portraits, or distance classification have been introduced to human identity verification. However, they are less advantage in authentication,

978-1-5090-6704-6/17/$31.00 ©2017 IEEE

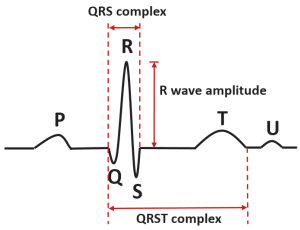

Fig. 1. A typical normal ECG pulse consists of a P wave, a QRS complex, and T/U waves.

when rejection of non-registered users becomes particularly important for better security. One of the reasons is that the threshold used in the final decision cannot be well- determined since it can just be either too loose or too strict.

Current algorithms for ECG authentication have shown promising results in user identification. But their recognitions required long data, normally from 10 to over 30 beats [19]–[21], which means users need to wait long to be recognized and get access. The algorithm proposed in this paper, is specifically designed for mobile devices, and the recognition requires only 3 beats, which is less than 3 seconds. To the best of our knowledge, this is the shortest time for authentication up to now in published studies.

We proposed a two-phase authentication method using artificial neural network (NN) models. Different with other works using ANN, this process is introduced as a two-stage identification which used two NN models, a "General" NN model for preliminary screening, and the "Personal" model for specific recognition. The performance of the proposed system is evaluated on sample sizes of 5, 10, 20, 30, 40, and 50.

II. Materials and Methods

The overall architecture of the proposed authentication system is shown in Fig. 2. The system is composed by three parts: pre-processing, enrollment and recognition. An ECG signal has to be pre-processed before being applied for authentication. This process involves removing the baseline drift and noise. Next, R peaks are detected, and QRS/QRST complexes are segmented. This step allows the alignment and normalization of the signal to avoid the influence of heart rate variability. After that, features are extracted from QRS/QRST complexes. In enrollment, both QRS/QRST template waveforms and NN models are generated and enrolled. NN models include a "General" NN model for the whole population, and the "Personal" NN model for each user. In recognition, test features are first matched with user's template, then the matching matrix is fed into "General" NN model and "Personal" NN model in sequence, as a two-phase identification. The final decision is made based on the outputs of the two types of models.

A. Pre-processing

1) Baseline Drift and Noise Removal: The baseline drift of ECG signal is first corrected by multilevel one-dimensional

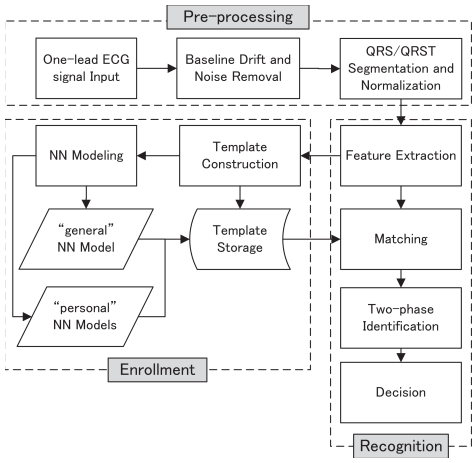

Fig. 2. The proposed ECG authentication system design. The method consists of three main processing parts: (a) pre-processing, (b) enrollment, and (c) recognition.

wavelet decomposition using one of Daubechies wavelets 'db8'. Raw ECG signal is decomposed into 7 levels, the final approximation coefficients is taken as the baseline drift and is subtracted from the original signal. A notch filter and a low-pass filter are then implemented to remove power-line noise and high-frequency distortions. Fig. 3(a)-(c) shows an example of pre-processed ECG signal.

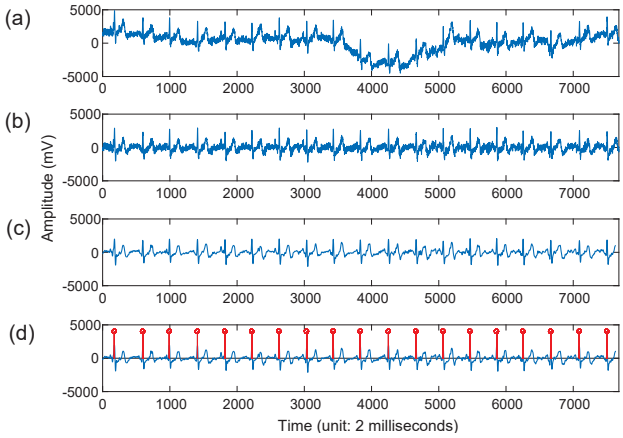

Fig. 3. Sample of a preprocessed ECG signal ((a) raw, (b) baseline drift removed, (c) noise eliminated, and (d) R peaks detected).

2) R Peaks Detection and QRS/QRST Segmentation: The QRS complex reflects the depolarization of the right and left ventricles and is the most prominent feature of the human ECG (Fig. 1). QRST complex includes more individual information over QRS complex. Thereafter, both QRS and QRST complexes are applied in feature extraction. R peak is the most distinguishable fiducial point on ECG signal which is also less affected by noise. For ECG signal sampled at 512Hz, all R peaks are detected and QRS complexes are segmented between 25 points (about 0.05s) before and after R peaks. Subsequently, QRST complexes are segmented between 70

points (about 0.14s) before and 180 points (about 0.35s) after R peaks. Now all the heartbeat waveforms have been aligned by their R-peaks instants.

3) Normalization: Segmented QRS and QRST complexes are normalized by the following equation:

$$N = \frac{x_i - \mu_x}{n_x} \tag{1}$$

where $x_i \in X, X = \{x_1, ..., x_t\}$, is the heartbeat waveform (QRS or QRST segment), μ_x is the mean of X, which is given by $\mu_x = \frac{1}{n}\sum_1^n x_i$. n_x is the length of x (data points). Normalization removes the mutual vertical shift of the segmentations.

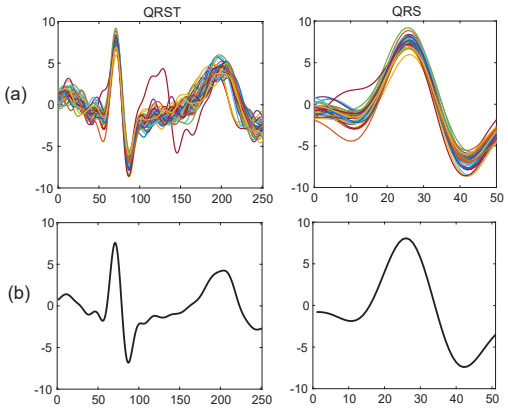

Fig. 4. Example of (a) segmented QRST and QRS complexes (normalized) and (b) the template QRST and QRS complexes for one subject using 30 seconds ECG signal.

B. Feature Extraction

After heartbeats alignment and normalization, unique features are extracted from QRS and QRST complexes. In Table I, seven features are selected based on preliminary studies. Features from QRS complexes include personal information while are robust to changes of heart rates. Features extracted from QRST complexes and R waveforms include more identifiable information of the individual.

TABLE I
FEATURE MEASUREMENTS.

	Features	Difference Matching
F1	QRST segment	Euclidean distance
F2	QRS segment	
F3	difference of QRST segment*	
F4	difference of QRS segment*	
F5	amplitude of R wave	Manhattan distance
F6	kurtosis of QRST segment	
F7	kurtosis of QRS segment	

*first order difference

C. Template Construction

When a user registers for the first time, template waveforms are generated from the first recorded ECG signal. This refers to both template QRS waveform and QRST waveform. Then, features described in Table I are extracted from the template waveforms. To be specific, all QRST/QRS complexes are first segmented, and normalized, then 70% of the segments that closest to μ_x in (1) are selected, estimated by calculating the Euclidean distance (d) of each individual segment x_i to μ_x :

$$d(x_i, \mu_x) = \sqrt{\sum_{r=1}^{n}(y_r(x_i) - y_r(\mu_x))^2} \tag{2}$$

where $y_r(x_i)$ is the value of the rth attribute of instance x_i. Then QRST/QRS template waveform is constructed by averaging above selected 70% segments (Fig. 4(b)).

Template features can be expressed by the following seven variables (for ECG sampled at 512Hz):

- $\overline{QRST_T} = \langle qt_1, qt_2, ..., qt_{251}\rangle$, qt_i is the data point of template *QRST* waveform;
- $\overline{QRS_T} = \langle q_1, q_2, ..., q_{51}\rangle$, q_i is the data point of template *QRS* waveform;
- $\overline{QRST\_dif_T} = \langle qt\_d_1, qt\_d_2, ..., qt\_d_{250}\rangle$, qt_i is the data point of the difference waveform of the template *QRST* waveform;
- $\overline{QRS\_dif_T} = \langle q\_d_1, q\_d_2, ..., q\_d_{50}\rangle$, q_i is the data point of the difference waveform of the template *QRS* waveform;
- $\overline{R\_amp_T}$, is the peak amplitude of template QRST wave;
- $\overline{QRST\_kurt_T}$, is the kurtosis of template QRST wave;
- $\overline{QRS\_kurt_T}$, is the kurtosis of template QRS wave;

D. NN Modeling

1) Training Data: Before NN modeling, we need to prepare for the training data. The training data includes input data and target data. Input data is a data matrix $Z = \{D_1, D_2, D_3, ..., D_n\}$, consisting of series of difference vectors, which can be expressed by $D_i = \langle d_1; d_2; d_3; d_4; d_5; d_6; d_7\rangle$, where d_i refers to the difference (value) between test and template feature. Features of each segmented heartbeat are compared with that of the template features. Difference vectors can be estimated using methods described in Table I. Target data is the corresponding label for each difference vector D, labeled as "Selves" or "Others". Specifically, by comparing features with that of the same individual's template, the obtained difference vector D is labeled as "Selves", while by comparing with that of other individuals' templates, D is labeled as "Others". The difference distributions for each feature and between every two features are shown in Fig. 5 and Fig. 6, respectively. To get train data, for each individual, features from all segments in 30 seconds ECG signal are compared with that of his/her own template to get difference vectors labeled as "Selves", and features of 2 randomly selected segments are compared with that of other all templates respectively to get difference vectors labeled as "Others". The number of segments per individual to get training data for "Others" class has been limited to 2 since segments more than 2 make performance worse because of over-learning.

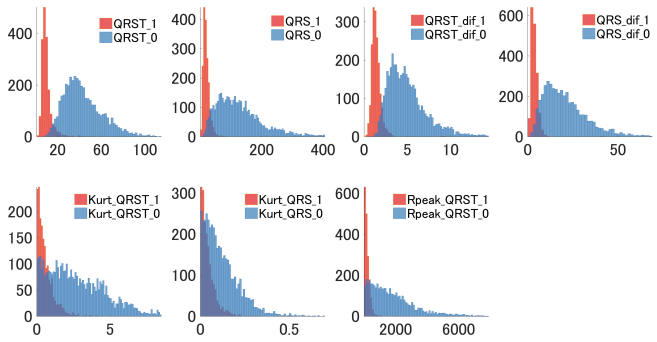

Fig. 5. Difference distributions of the "Selves" and the "Others" groups for each feature. "x_1" refers to the "Selves" group, and "x_0" refers to the "Others" group.

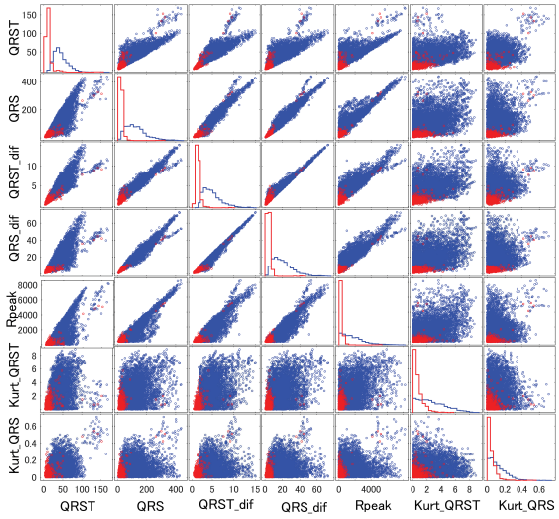

Fig. 6. Difference distributions of the "Selves" and the "Others" groups for every two features. The red refers to the "Selves" group, and the blue refers to the "Others" group.

2) "General" NN Model: The "general" NN modeling used difference vector data from all individuals (users), with a data size around 5000. A two-layered feed-forward network is used as the pattern matching tool (MATLAB Neural Network Toolbox). The number of hidden neurons is configured to 10. This network can be trained to classify inputs according to target classes. The network is trained with scaled conjugate gradient back-propagation. Training automatically stops when generalization stops improving, as indicated by an increase in the cross-entropy error of the validation samples. The performance of the trained "General" NN model is evaluated on around 5000 heartbeats from 50 individuals by Equal Error Rate (EER). The ROC curve is shown in Fig. 7, and the EER is 2.61%.

3) "Personal" NN Models: The "Personal" NN model is trained by using difference vector data from a single individual, about 140 length of data. Each individual (user) will have his/her own "Personal" NN model.

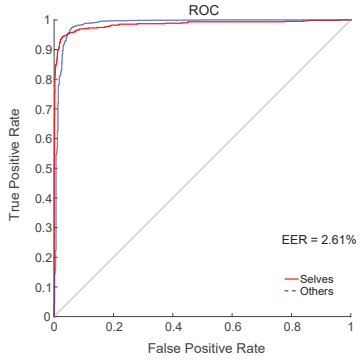

Fig. 7. ROC curve of the "General' NN model.

E. Identification

The identification process can be described as a two-phase authentication. For each test heartbeat, features are first extracted and a difference vector is computed by comparing those features with that of reference user's template. The input difference vector is then fed into and classified by "General" NN model (first phase) and "Personal" NN model (second phase) in sequence, an individual is accepted if the outputs of both "general" NN model and "personal" NN model are superior to a given threshold, while he/she is rejected if either output of the two models is below the threshold. Here, a threshold of 10% and 70% are used for "general" NN model and "personal" NN model separately. This value is decided based on a preliminary study, which can have a best balance between true matches and true rejections. A final decision is made if 2 out of 3 heartbeats of the individual are accepted by both NN models.

III. Results and Discussion

A. Experiment

1) Data Acquisition: Laboratory experiment is conducted, and the ECG signal recording is performed using a BMD_Starter_Kit with a built-in BMD101 chip (NeuroSky Japan Inc.) at a sampling rate of 512Hz. ECG signal acquisition is through a single lead setup at the fingers. The measurement apparatus prototype is depicted in Fig. 8. The right hand thumb is used as the negative electrode, and the left hand thumb simultaneously as the positive electrode. Transmit of the data is through a Bluetooth wireless connection to a mobile App installed on a smartphone or a tablet. Data are then transmitted to PC by USB cable.

50 individuals participate in this experiment, aged between 20 and 70 years old. Detailed information of the subjects are listed in Table. II. Informed concents are obtained from all subjects before data collection.

For each individual, one minute ECG data is recorded in sitting position 15min before (data A) and 15min after (data B) a Master two-step test, respectively. The Master two-step

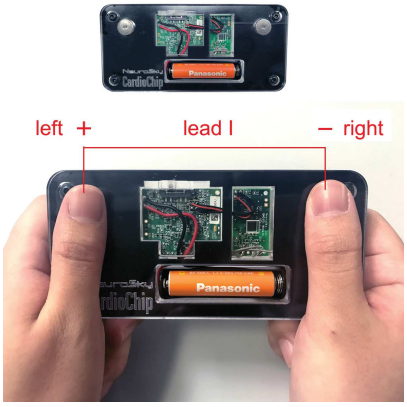

Fig. 8. ECG measurement device.

TABLE II
INFORMATION OF SUBJECTS.

Age (years)	Male	Female
20∼29	5	5
30∼39	6	4
40∼49	5	5
50∼59	5	5
60∼69	9	1
Total	30	20

test is a standardized heart stress exercise which permits ECG recording immediately after the exercise terminates [22]. Pulse and blood pressure can be elevated after the test. In 90s, the subject walks up and down a foot stool repeatedly following a metronome. The step rhythm (speed) is determined by the age and weight of each subject. It is assumed that ECG data are collected under different physical statuses.

From data A, 30s ECG data are extracted for enrollment (template construction and NN modeling). The starting 3 heartbeats of data B is used for authentication.

2) Authentication: The performance of the algorithm is evaluated by False Acceptance Rate (FAR) and False Rejection Rate (FRR). To evaluate the FAR, every single user is taken at a time for testing, and FAR is computed by dividing the number of correct identifications by the total number of users. Leave-one-out (LOO) cross-validation is applied to estimate the FAR. A single individual is taken at a time as unregistered user for authentication, and the remaining individuals are taken as registered users. This process is repeated until each individual has been taken for authentication. We evaluate our algorithm on sample sizes of 5, 10, 20, 30, 40 and 50. For each subset, individuals are randomly selected from initial population at a time, and the LOO cross-validation process described above is conducted. This process is repeated 100 times for each subset, and FAR and FRR are estimated by averaging the results of 100 iterations.

B. Evaluation

The authentication performance results on different sample sizes are plotted in Fig. 9 and summarized in Table III. From the figure, average FAR and FRR are below 10% for different sample sizes. The obtained results are compared with two recent published works about finger ECG authentication on mobile platforms. Comparisons are summarized in Table IV. Arteaga-Falconi et al. [17] test their algorithm on 10 subjects. The authentication takes only 4s to achieve a 1.41% FAR, however, the FRR reaches 18.18%. In [23], they use 5 beats for authentication and reduce the FAR and FRR to 5.20% and 1.90%, respectively, which is promising. But the data used for enrollment and authentication are collected at one time, which means, there are no time intervals between enrollment and authentication. Since the permanency of ECG patterns has not yet been proved and it has shown that the variability of ECG cycles takes place within even one hour [24], the error rates will possibly rise if it is evaluated on different data set. It is worth emphasizing that, our method gives a reasonable authentication using only 3 beats within 3 seconds, the fastest as we know up to now. This is especially desirable for practical applications implemented in mobile or wearable devices.

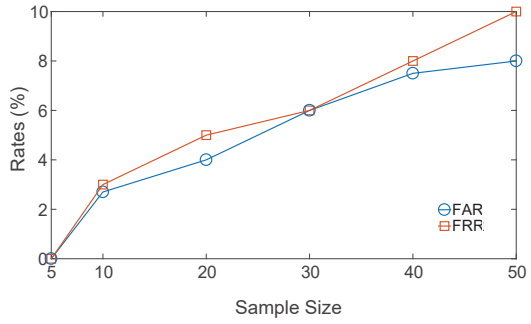

Fig. 9. The average errors of the authentication with different sample sizes.

TABLE III
AVERAGE PERFORMANCE RESULTS.

Sample Size	FAR (%)	FRR (%)
5	0.00	0.00
10	2.70	3.00
20	4.00	5.00
30	6.00	6.00
40	7.50	8.00
50	8.00	10.00

We notice that the performance decreases slightly with number of users increasing. This tendency is accordance with the identification result of one previous study [25]. One possible reason might be related to the uniqueness property of ECG as discussed in [25], suggesting that application of the ECG authentication is more suitable in a relatively small pre-determined groups, such as family, small company, nursing home, or clinic, etc. To find out features that reflect the intrinsic nature of ECG patterns become particularly important. In

our study, the difference distributions of "Selves" group and "Others" group are observed to be distinctive in all features except the kurtosis of QRS/QRST patterns, which are found less distinguishable between the two groups (Fig. 5 and Fig. 6). In order to spread our scheme to a larger population, more specific features should be included.

TABLE IV
ALGORITHM COMPARISONS.

Algorithm	No. of Subjects	FAR (%)	FRR (%)	Authent. Length	Enroll and Authent. at one time ?
Arteaga-Falconi et al. [17]	10	1.41	18.18	4s	No
Proposed Method	10	2.70	3.00	$\leq$ 3s	No
Kang et al. [23]	28	5.20	1.90	5 beats	Yes
Proposed Method	30	6.00	6.00	3 beats	No

The reason why a two-phase identification applied is that it enables efficient recognition while guarantees a high specificity. A "Personal" NN model is constructed based on data from a single person. ECG patterns are shown to slightly vary with time even for the same individual. In practical application, when only limited training data are available at a time, the only use of a "Personal" NN model is less distinguish for individual detection and may reduce false acceptance. At the same time, the "General" NN model is constructed based on data from a certain number of individuals. It can neutralize individual differences at a certain level so that it is more tolerant of the variations on the same person. The only use of the "General" NN model or the "Personal" NN models can still obtain an efficient recognition with 92% accuracy, but with a FAR rise to 26%. Combined use of above two models can get a good balance between the usability and security. Thresholds for the two models can be also adjusted according to different intents (1:1 or 1:N authentication).

IV. CONCLUSION

This study proposes a two-phase authentication algorithm with two trained NN models, which can balance the error performance of acceptance and rejection. Considering the ease-of-use for practical applications, it shows promising results by using only 3 beats, within 3 seconds for authentication. The proposed algorithm is tested with a sensor designed for mobile environment and achieves average FAR and FRR below 10% on a group of 50 subjects. This performance is more promising on small groups of cohort (less than 30), having obtained both FAR and FRR under 5.00%. Nonetheless, further improvements are still needed to optimize accuracy while maintaining a short acquisition time for authentication.

REFERENCES

[1] A. Jain, R. Bolle, and S. Pankanti, *Biometrics: personal identification in networked society*. Springer Science & Business Media, 2006, vol. 479.

[2] J. L. Wayman, "Fundamentals of biometric authentication technologies," *International Journal of Image and Graphics*, vol. 1, no. 01, pp. 93–113, 2001.

[3] J. Chirillo and S. Blaul, *Implementing biometric security*. Hungry Minds, Incorporated, 2003.

[4] H. Sellahewa and S. A. Jassim, "Image-quality-based adaptive face recognition," *IEEE Transactions on Instrumentation and Measurement*, vol. 59, no. 4, pp. 805–813, 2010.

[5] N. K. Ratha, R. M. Bolle, V. D. Pandit, and V. Vaish, "Robust fingerprint authentication using local structural similarity," in *Applications of Computer Vision, 2000, Fifth IEEE Workshop on.* IEEE, 2000, pp. 29–34.

[6] J. Daugman, "New methods in iris recognition," *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics)*, vol. 37, no. 5, pp. 1167–1175, 2007.

[7] A. Graves, A.-r. Mohamed, and G. Hinton, "Speech recognition with deep recurrent neural networks," in *Acoustics, speech and signal processing (icassp), 2013 ieee international conference on*. IEEE, 2013, pp. 6645–6649.

[8] L. Biel, O. Pettersson, L. Philipson, and P. Wide, "Ecg analysis: a new approach in human identification," *IEEE Transactions on Instrumentation and Measurement*, vol. 50, no. 3, pp. 808–812, 2001.

[9] S. A. Israel, J. M. Irvine, A. Cheng, M. D. Wiederhold, and B. K. Wiederhold, "Ecg to identify individuals," *Pattern recognition*, vol. 38, no. 1, pp. 133–142, 2005.

[10] Y. Wang, F. Agrafioti, D. Hatzinakos, and K. N. Plataniotis, "Analysis of human electrocardiogram for biometric recognition," *EURASIP journal on Advances in Signal Processing*, vol. 2008, no. 1, p. 148658, 2007.

[11] S. I. Safie, J. J. Soraghan, and L. Petropoulakis, "Electrocardiogram (ecg) biometric authentication using pulse active ratio (par)," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 4, pp. 1315–1322, 2011.

[12] J. C. Sriram, M. Shin, T. Choudhury, and D. Kotz, "Activity-aware ecg-based patient authentication for remote health monitoring," in *Proceedings of the 2009 international conference on Multimodal interfaces.* ACM, 2009, pp. 297–304.

[13] H. Silva, A. Lourenço, A. Fred, and J. Filipe, "Clinical data privacy and customization via biometrics based on ecg signals," in *Symposium of the Austrian HCI and Usability Engineering Group*. Springer, 2011, pp. 121–132.

[14] K. Wang, Y. Shao, L. Shu, C. Zhu, and Y. Zhang, "Mobile big data fault-tolerant processing for ehealth networks," *IEEE Network*, vol. 30, no. 1, pp. 36–42, 2016.

[15] Y. Shao, K. Wang, L. Shu, S. Deng, and D.-J. Deng, "Heuristic optimization for reliable data congestion analytics in crowdsourced ehealth networks," *IEEE Access*, vol. 4, pp. 9174–9183, 2016.

[16] Y. Singh and P. Gupta, "Biometrics method for human identification using electrocardiogram," *Advances in Biometrics*, pp. 1270–1279, 2009.

[17] J. S. Arteaga-Falconi, H. Al Osman, and A. El Saddik, "Ecg authentication for mobile devices," *IEEE Transactions on Instrumentation and Measurement*, vol. 65, no. 3, pp. 591–600, 2016.

[18] T.-W. Shen, W. Tompkins, and Y. Hu, "One-lead ecg for identity verification," in *Engineering in medicine and biology, 2002. 24th annual conference and the annual fall meeting of the biomedical engineering society embs/bmes conference, 2002. proceedings of the second joint*, vol. 1. IEEE, 2002, pp. 62–63.

[19] G. Wübbeler, M. Stavridis, D. Kreiseler, R.-D. Bousseljot, and C. Elster, "Verification of humans using the electrocardiogram," *Pattern Recognition Letters*, vol. 28, no. 10, pp. 1172–1175, 2007.

[20] Y. N. Singh and S. K. Singh, "Evaluation of electrocardiogram for biometric authentication," *J. Information Security*, vol. 3, no. 1, pp. 39–48, 2012.

[21] Y. N. Singh and S. K. Singh, "Identifying individuals using eigenbeat features of electrocardiogram," *Journal of Engineering*, vol. 2013, 2013.

[22] A. M. Master, "The master two-step test," *American heart journal*, vol. 75, no. 6, pp. 809–837, 1968.

[23] S. J. Kang, S. Y. Lee, H. I. Cho, and H. Park, "Ecg authentication system design based on signal analysis in mobile and wearable devices," *IEEE Signal Processing Letters*, vol. 23, no. 6, pp. 805–808, 2016.

[24] T. S. Lugovaya, "Biometric human identification based on ecg," 2005.

[25] C. Carreiras, A. Lourenço, A. Fred, and R. Ferreira, "Ecg signals for biometric applications-are we there yet?" in *Informatics in Control, Automation and Robotics (ICINCO), 2014 11th International Conference on*, vol. 2. IEEE, 2014, pp. 765–772.