

See discussions, stats, and author profiles for this publication at: <https://www.researchgate.net/publication/357962705>

Shared Weighted Continuous Wavelet Capsule Network for Electrocardiogram Biometric Identification

Conference Paper · December 2021

DOI: 10.1109/ICCWAMTIPS3232.2021.9674078

CITATIONS

4

READS

88

7 authors, including:



Happy Nkanta Monday

Oxford Brookes College of Chengdu University of Technology

53 PUBLICATIONS 584 CITATIONS

SEE PROFILE



Grace U. Nneji

Oxford Brookes College of Chengdu University of Technology

48 PUBLICATIONS 447 CITATIONS

SEE PROFILE



Edidiong Christopher James

University of Electronic Science and Technology of China

13 PUBLICATIONS 151 CITATIONS

SEE PROFILE



Leta Yobsan Bayisa

Southern University of Science and Technology

6 PUBLICATIONS 12 CITATIONS

SEE PROFILE

SHARED WEIGHTED CONTINUOUS WAVELET CAPSULE NETWORK FOR ELECTROCARDIOGRAM BIOMETRIC IDENTIFICATION

HAPPY NKANTA MONDAY¹, JIAN PING LI¹, GRACE UGOCHI NNEJI², EDIDIONG CHRISTOPHER JAMES², YOBAN BAYISA LETA², SAIFUN NAHAR³, AMIN UL HAQ¹

¹School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu, Sichuan 611731, China

²School of Information and Software Engineering, University of Electronic Science and Technology of China, Chengdu, Sichuan 611731, China

³School of Computer and Information Systems, University of Missouri St Louis MO, USA

E-MAIL: mh.nkanta@std.uestc.edu.cn, jpli2222@uestc.edu.cn, ugochinneji@std.uestc.edu.cn, edianajames@yahoo.com, yoban23@gmail.com, snnnm@umsl.com, khan.amin50@yahoo.com

Abstract:

In recent times, researchers are showing more interest in the subject of biometric identification, which uses biological traits to confirm a user's identity. Traditional authentication techniques are prone to damage, fraud, and negligence. We investigate a unique biometric based on electrocardiogram (ECG) signals generated from the heart as a biometric security attribute for access control verification. In this research, we propose a shared weighted continuous wavelet capsule network for ECG biometric identification, in which a continuous wavelet transform (CWT) is utilized to convert one-dimensional time-domain ECG signals into scalograms of two-dimensional images to obtain good quality training data. Then, a siamese capsule network framework is utilized to predict the right match or mismatch of ECG query samples using the extracted specific attributes from the scalograms. The dataset utilized in this work is collected from the Physionet MIT-BIH Normal Sinus Rhythm database. Experimental result shows that the proposed approach properly predicted ECG query samples with 99.2% accuracy, which makes our model more robust.

Keywords:

Biometric; Continuous wavelet transform; Electrocardiogram (ECG); Identification; Siamese capsule network; Security

1. Introduction

Despite various usability and security issues, conventional passwords remain the most used method of internet authentication [1-3]. Passwords are inconvenient for users since they must be remembered and preferably, be lengthy and distinct. As a result, it should come as no

surprise that many users choose weak passwords that they reuse across several platforms [4-5], resulting in account hack and personal data breaches. According to studies, over 50% of users use the same authentication credentials for several platforms [4] and over 80% of privacy breaches are caused by poor authentication credential behavior [6].

Alternative authentication techniques, such as push notifications [7], graphical passcodes [8], and trust scores [9], and gestures [10], have been investigated in attempt to replace or supplement standard passwords. Biometric authentication is of particular importance due to its unique characteristics of user identity. Biometrics enhances usability of the system by eliminating the need for users to remember passwords or move about with a token at all times. The simplicity with which biometrics can be used for authentication has sped up their adoption in both the private and public sectors, with the global market for biometric technology anticipated to hit \$59.31 billion by 2025 [11].

While much of the previous research has focused on standard biometrics like fingerprints, facial recognition, and iris scans, there has been little work done to investigate new biometrics. In this paper, we look at a biometric based on electrocardiogram (ECG) signals, which represent the electrical activity of the human heart. ECG has been shown to be adequately unique to every person in previous studies [12] and could be utilized for identity verification. In this paper, we proposed a hybrid scheme of continuous wavelet transform (CWT) and capsule network for biometric authentication based on ECG. CNN has made significant progress in a variety of applications, particularly in detecting anomalies in radiographs [13-16].

While biometrics are more usable than standard passwords, there are still issues about biometric data security and privacy [17]. Biometrics cannot be readily reversed once they have been infiltrated, as they are based on an individual's lasting physiological or behavioral features. Additionally, biometric recognition system operators may gain undesired information from a user's biometric data. Fingerprint patterns, for example, may be linked to certain disorders [18]. In conclusion, some biometric traits, such as a person's face, are difficult to conceal. As a result, even if a person wants to remain unknown, they may be recognized without their consent or knowledge [18].

The heart is a muscular organ that supplies blood to the body's tissues via blood vessels [19]. The heart muscle must contract in order to supply blood, resulting in an electrical impulse. During an electrocardiogram (ECG) examination, this impulse can be measured on the surface of the body using electrodes put on the skin. The process of depolarization and repolarization of the heart chambers, which causes them to contract and rest, is captured by an

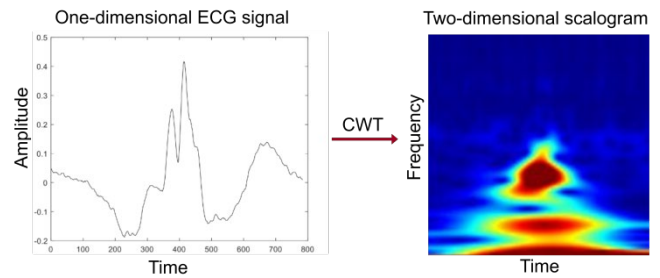


Fig.2 Conversion of one-dimensional traffic data to two-dimensional images using CWT

ECG tracing.

Various researchers have looked into the ECG's peculiarity and stability. The majority of these are based on a "on-the-person" approach "a method for signal acquisition in which electrodes are placed directly on the person [20]. There are limited researches that use "off-the-person" methodology "They use a different approach, but they show a real-life application scenario for ECG identification systems. Placing ECG sensors into a smartphone cover,

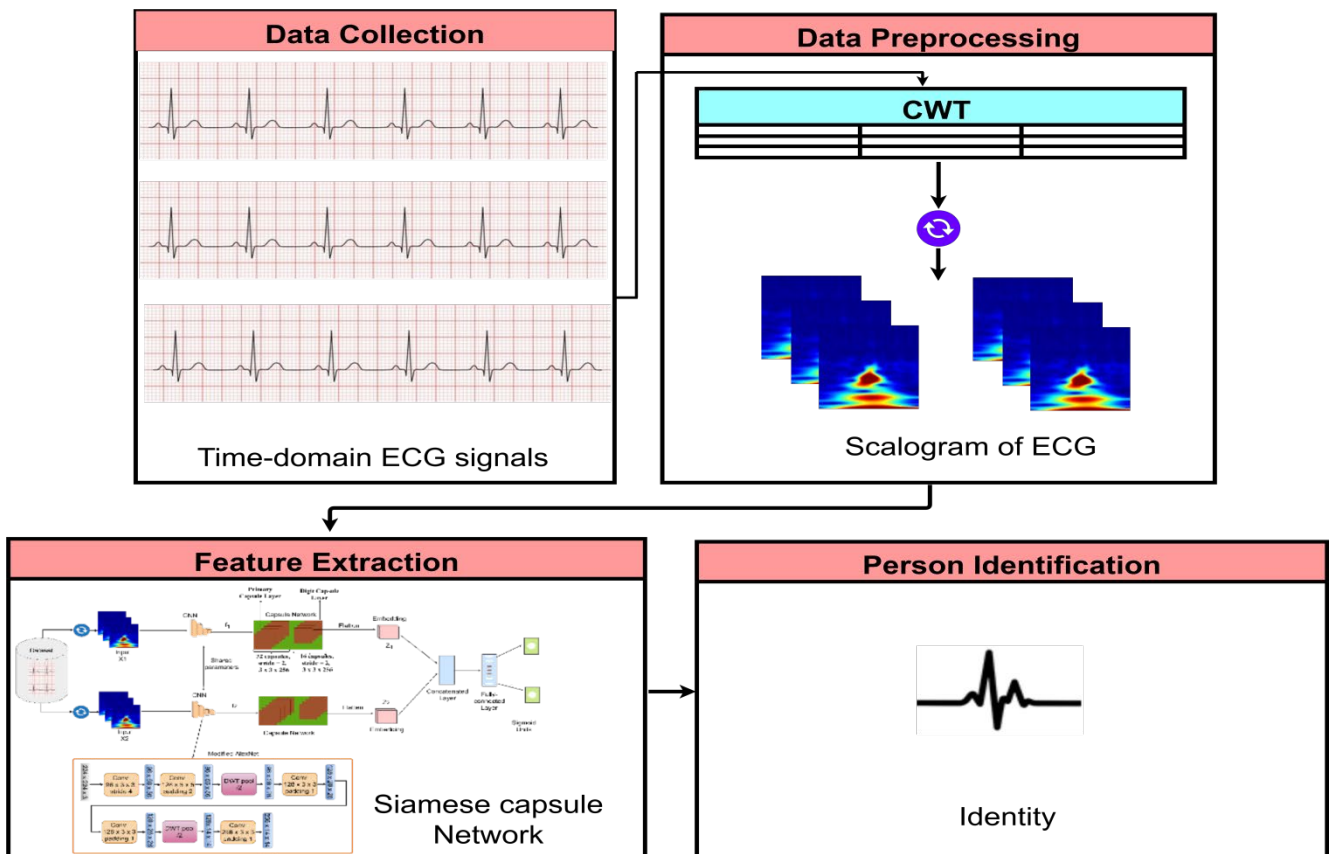


Fig.1 Proposed scheme for detecting DDoS attack on smart grid

wristbands, and car steering wheel are just a few instances. Additionally, as shown in [20], previous researches frequently employ data acquired from a single data acquisition session which are easy to develop.

In this paper, CWT is utilized to convert the 1-dimensional time-series signal of ECG to 2-dimensional time-frequency scalogram as input image of distinct features with growing sensitivity which makes it suitable for CNN model to extract feature for training. The image features obtained from CWT are utilized to train the proposed capsule network for biometric authentication. We adopted some well-known evaluation metrics to validate the performance of the proposed scheme.

Conclusively, we assess the effectiveness of the proposed scheme using public dataset and also presented some comparison with other methods of biometric

2. Methodology

The proposed method for biometric identification using ECG is described in this section. Fig.1 depicts the general framework of the proposed scheme for user identification. First, the dataset utilized in this study for ECG biometric identification is properly described.

2.1. Dataset

Instead of creating a new dataset, we used an already existed dataset. For this study, we used the MIT-BIH Normal Sinus Rhythm available on Physionet database. The Physionet MIT-BIH Normal Sinus Rhythm database consists of healthy ECG records of persons between the

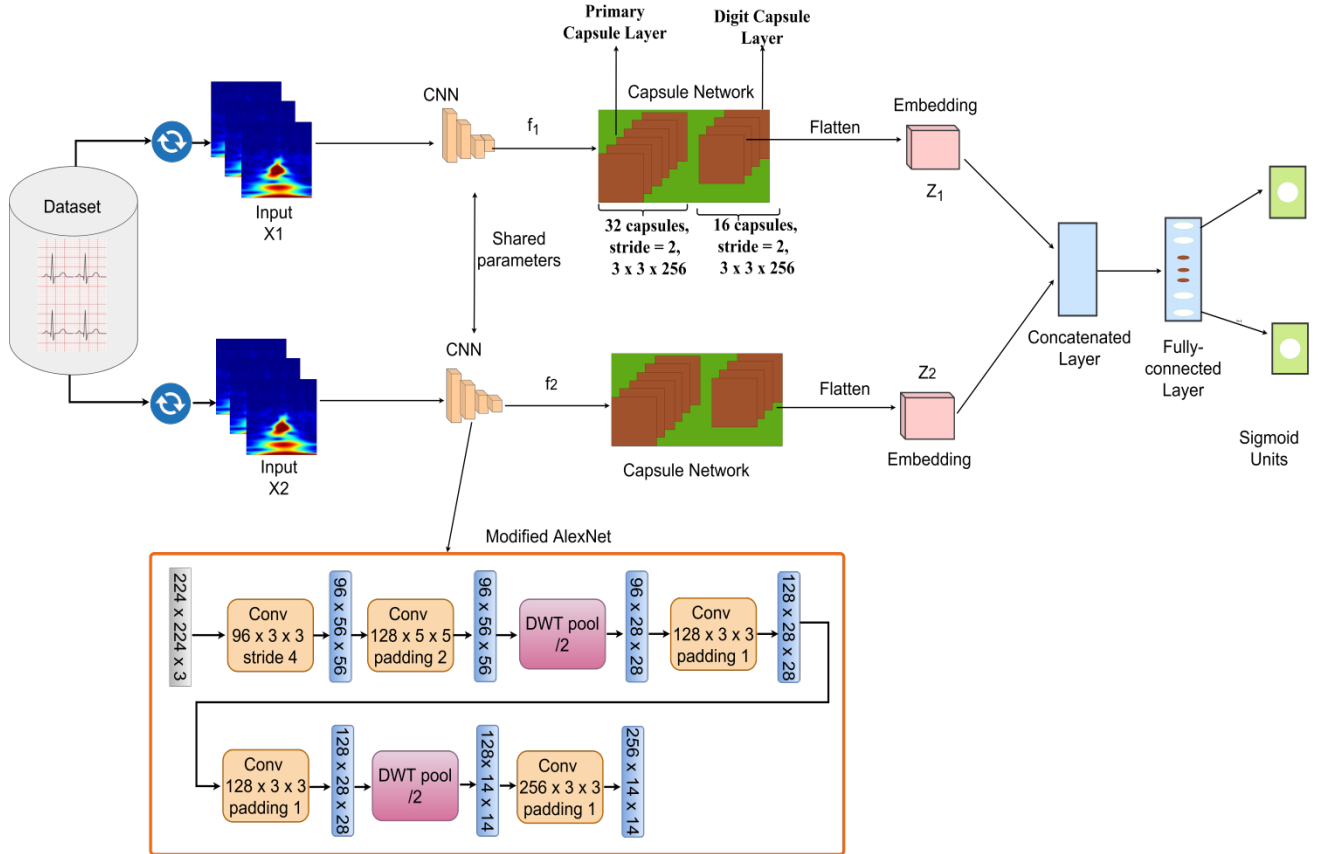


Fig.3 Proposed wavelet convolutional neural network for detecting DDoS attack on smart grid infrastructure

authentication. The remaining part of this paper is as follows: The dataset and the proposed scheme are presented in section 2. Section 3 presents the results and discussion. Conclusively, section 4 finalizes this study.

ages of 20 and 50 with no major arrhythmias collected at the Arrhythmia laboratory of Boston's Beth Israel Hospital [21]. Compared to other ECG dataset, Physionet MIT-BIH dataset has been utilized by most studies. Physionet

MIT-BIH dataset consists of 30 recordings of normal sinus rhythm signals.

2.2. Wavelet transform

Wavelet Transform (WT) is a technique for obtaining coefficients from signal data by transforming it into wavelets using wavelet function. WT is a signal processing approach that extracts details from data in order to disclose traits that aren't visible in the time domain [13]. Signals are broken down into coefficients and are presented in several scales. In this paper, we utilized continuous wavelet transform (CWT) for converting time-series signal to time-frequency images for biometric identification using ECG traits as depicted in Fig.2. Equation (1) expresses the numerical representation of CWT.

$$CWT_x^\psi = \frac{1}{\sqrt{|S|}} \int x(t) \psi^* \left(\frac{t-\tau}{S} \right) dt \quad (1)$$

where τ depicts the transition factor and S denote the scale factor. $x(t)$ represents the function of the mother wavelet. $\psi^* \left(\frac{t-\tau}{S} \right) dt$ depicts the derived function from the mother wavelet. τ is the shift term to move the mother wavelet. S is the frequency inverse. Low frequency corresponds to large S and small S leads to high frequency.

2.3. Proposed siamese capsule network (WavCapNet)

This research proposes a siamese capsule network, as shown in Fig.3. The model accepts two scalogram images as inputs, and then transmits them into a shared weighted framework. The obtained data is forwarded into the fully-connected layer, and the model then determines if the outcome is valid or invalid. Our proposed model's method

Table 1 Performance comparison of our proposed model with selected pre-trained models.

Model	ACC (%)	SEN (%)	SPE (%)	Time (Min)
ResNet-101	95.7	95.8	94.6	47
EfficientNet	94.7	94.3	95.8	40
MobileNet-V3	95.2	94.5	95.9	39
DenseNet	96.6	95.4	96.3	46
Ours	99.2	98.6	99.5	48

is based on a real-world security assessment of person identity.

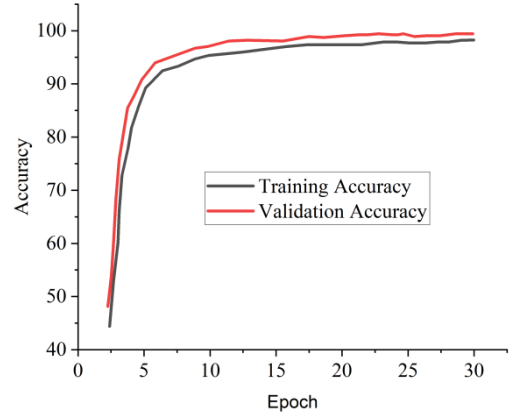


Fig.4 Training and validation accuracy curves showing the performance of our proposed

In a real-world scenario, tenants of a specific building or employees of a company with access control security equipment are normally asked to go through a security check. These persons' biometric templates must have been stored in the system. When a person attempts to enter an authorized building or organization, a comparison of both the template and the query input is performed to determine whether the request is valid or invalid. As a result, the idea of employing a siamese capsule network to receive both ECG trait images, access their attributes, and determine whether they are similar or not is proposed. In general, a siamese network is used to compare two input images with similar weights and parameters. The extracted feature vectors of the two inputs are then obtained from the last layer, and the Euclidean distance is computed. If the

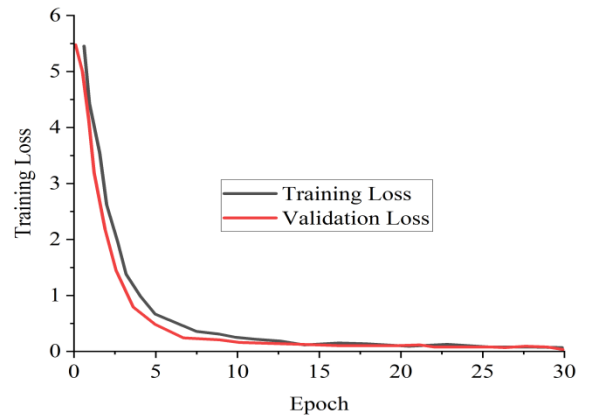


Fig.5 Training and validation loss curves of our proposed WavCovNet model showing steady reduction in loss

distance between the two images is large, they are different, otherwise, they are similar.

Computing the similarity of the ECG images will be

omitted in our investigation, and instead the relationship between the two images will be utilized to predict the outcome. As a result, the distance calculating aspect of our work is eliminated, as shown in Fig.3. For feature extraction, a shared weighted capsule network with modified AlexNet as the base neural network is used, then the retrieved features are fused and passed into the fully-connected layer, and ultimately, the ECG images are predicted using a sigmoid classifier. Instead of the usual max-pooling layer, we introduced discrete wavelet pooling to replace the first and second max-pooling layers for down-sampling operation whereas the third max-pooling layer is eliminated to arrive at a feature vector of $256 \times 14 \times 14$. The likelihood of which ECG trait matches the query or not is represented by the prediction result which is either 0 or 1.

2.5. Experimental detail and setup

The basic technique of the proposed scheme is split into two phases: data pre-processing and feature extraction. The pre-processing step begins with the collection of raw ECG signals from the Physionet database. The most essential and consistent fundamental characteristics are obtained in the pre-processing step by converting one-dimensional time domain ECG signal to time-frequency domain image of two-dimension using CWT. This work employed continuous wavelet transform and siamese wavelet capsule networks trained on Physionet MIT-BIH ECG dataset for biometric identification using Adam optimizer and dropout to prevent over-fitting, early stop strategies, and a learning rate of 10^{-4} to improve performance. Keras library with Tensorflow as the backend on a GeForce GTX 1080 GPU is used for the implementation of this work.

2.6. Performance Measures

Accuracy, sensitivity, specificity and AUC are some of the evaluation metrics applied on our proposed model. Equations (2)-(4) are the provided equation for the evaluation metrics.

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \quad (2)$$

$$Sensitivity = \frac{TP}{TP+FN} \quad (3)$$

$$Specificity = \frac{TN}{TN+FP} \quad (4)$$

3. Results and discussion

The proposed ECG biometric identification scheme is built using the Keras framework and Tensorflow as the backend. We examined the proposed strategy for ECG biometric identification based on binary classification for both query match and mismatch in security access control systems during training and validation. The proposed

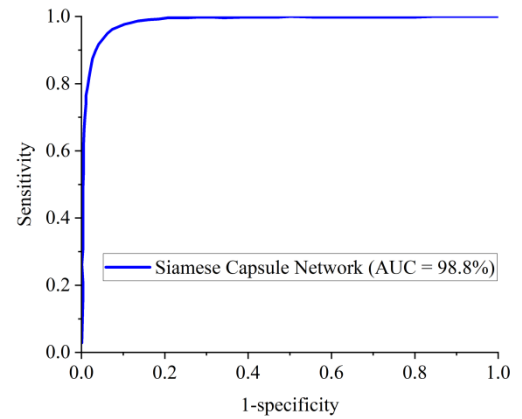


Fig.6 ROC curve showing the performance of our proposed model with respect to sensitivity and specificity

approach obtains 99.2% accuracy rate for identifying query match and mismatch. The proposed model's training and validation accuracy curves are depicted in Fig.4, which show that the model converges smoothly without over-fitting. The proposed scheme's training and validation loss curves are gradually and steadily reduced as shown in Fig.5. In general, the proposed siamese wavelet capsule network's performance is reasonable. It's crucial to evaluate the proposed model's validity using the receiver operating characteristic curve (ROC), which depicts the proposed scheme's overall accuracy in terms of area under the curve (AUC). Fig.6 illustrates that the proposed scheme has a high sensitivity combined with a high specificity, resulting in a low false positive rate and a high true positive rate.

As shown in Table 1, our proposed approach obtains 98.6% sensitivity and 99.5% specificity. The results of our proposed scheme versus certain pre-trained models are shown in Table 1. When it comes to correctly determining query match and mismatch of ECG characteristics, the proposed strategy clearly outweighed the selected pre-trained techniques by 2.6% in terms of accuracy. In addition, the proposed method achieved 2.6% increase in sensitivity and 3.2% increase in specificity when compared to pre-trained procedures. EfficientNet had the lowest

accuracy (94.7%) and sensitivity (94.3%) scores, whereas ResNet-101 had the lowest specificity score (94.6%). It is worth noting that the proposed scheme has a slightly higher computational time of about 48 minutes in training but achieves the best result, as shown in Table 1. Though MobileNet-V3 had the shortest training time of 39 minutes, our proposed model still achieves satisfactory performance.

4. Conclusions

Biometric identification systems provide several benefits that traditional techniques do not. We proposed an ECG-based biometric identification system for security access control in this research, in which a continuous wavelet transform (CWT) was utilized to convert one-dimensional time-domain signals into scalograms of two-dimensional images to obtain good quality training data. A siamese capsule network framework was utilized to predict the right match or mismatch of ECG query samples using the extracted specific attributes from the scalograms. The findings show that the ECG signal is a reliable biometric measure that is resistant to noise and artifacts. Furthermore, the proposed security system's efficiency was assessed using both classification metrics and the ROC-AUC measure. The proposed scheme properly predicted ECG query samples with 99.2% accuracy, which is 2.6% higher than the other models.

Acknowledgements

This work was supported by the National Natural Science Foundation of China (Grant No. 61370073), the National High Technology Research and Development Program of China (Grant No. 2007AA01Z423), the project of Science and Technology Department of Sichuan Province, the project of Science and Technology Department of Chongqing Municipality, Chengdu Chengdian Network Technology Co., Ltd., Chengdu Civil-military Integration Project Management Co., Ltd., and Sichuan Yin Ten Gu Technology Co.

References

- [1] Anne Adams, Martina Angela Sasse, and Peter Lunt. Making passwords secure and usable. In *People and Computers XII*, pages 1–19. Springer, 1997.
- [2] Joseph Bonneau, Cormac Herley, Paul C Van Oorschot, and Frank Stajano. The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In *2012 IEEE Symposium on Security and Privacy*, pages 553–567. IEEE, 2012.
- [3] Steven Furnell and Leith Zekri. Replacing passwords: in search of the secret remedy. *Network Security*, 2006(1):4–8, 2006.
- [4] Anupam Das, Joseph Bonneau, Matthew Caesar, Nikita Borisov, and XiaoFeng Wang. The tangled web of password reuse. In *NDSS*, volume 14, pages 23–26, 2014.
- [5] Blake Ives, Kenneth R Walsh, and Helmut Schneider. The domino effect of password reuse. *Communications of the ACM*, 47(4):75–78, 2004.
- [6] Verizon. Verizon Data Breach Investigations Report. <https://enterprise.verizon.com/resources/reports/dbir/#report>, 2017. Accessed: 2021-11-10.
- [7] Aleksey Sanin, Matt Ricketson, Ryan Newlman, Andrew LeBlanc, and Eric Stern. Systems and methods for push notification based application authentication and authorization, January 2 2014. US Patent App. 13/915,475.
- [8] Susan Wiedenbeck, Jim Waters, Jean-Camille Birget, Alex Brodskiy, and Nasir Memon. Passpoints: Design and longitudinal evaluation of a graphical password system. *International journal of human-computer studies*, 63(1-2):102–127, 2005.
- [9] Bjorn Markus Jakobsson, Mark J Grandcolas, Philippe JP Golle, Richard Chow, and Runtong Shi. Implicit authentication, November 13 2012. US Patent 8,312,157.
- [10] Michael Sherman, Gradeigh Clark, Yulong Yang, Shridatt Sugrim, Arttu Modig, Janne Lindqvist, Antti Oulasvirta, and Teemu Roos. User-generated free-form gestures for authentication: Security and memorability. In *Proceedings of the 12th annual international conference on Mobile systems, applications, and services*, pages 176–189. ACM, 2014.
- [11] Grand View Research. Biometrics technology market analysis report by end-use. <https://www.grandviewresearch.com/industry-analysis/biometrics-industry>, 2017. Accessed: 2021-10-10.
- [12] Carlos Carreiras, André Lourenço, Hugo Silva, Ana Fred, and Rui Ferreira. Evaluating template uniqueness in ECG biometrics. In Joaquim Filipe, Oleg Gusikhin, Kurosh Madani, and Jurek Sasiadek, editors, *Informatics in Control, Automation and Robotics*, pages 111–123, Cham, 2016. Springer International Publishing.
- [13] G. U. Nneji et al., “A Super-Resolution Generative Adversarial Network with Siamese CNN Based on Low Quality for Breast Cancer Identification,” in 2021

- 4th International Conference on Pattern Recognition and Artificial Intelligence (PRAI), 2021, pp. 218–223, doi: 10.1109/PRAI53619.2021.9551033.
- [14] H. N. Monday et al., “The Capability of Multi Resolution Analysis: A Case Study of COVID-19 Diagnosis,” in 2021 4th International Conference on Pattern Recognition and Artificial Intelligence (PRAI), 2021, pp. 236–242, doi: 10.1109/PRAI53619.2021.9550802.
- [15] G. U. Nneji et al., “Enhancing Low Quality in Radiograph Datasets Using Wavelet Transform Convolutional Neural Network and Generative Adversarial Network for COVID-19 Identification,” in 2021 4th International Conference on Pattern Recognition and Artificial Intelligence (PRAI), 2021, pp. 146–151, doi: 10.1109/PRAI53619.2021.9551043.
- [16] H. N. Monday et al., “Improved Convolutional Neural Multi-Resolution Wavelet Network for COVID-19 Pneumonia Classification,” in 2021 4th International Conference on Pattern Recognition and Artificial Intelligence (PRAI), 2021, pp. 267–273, doi: 10.1109/PRAI53619.2021.9551095.
- [17] Salil Prabhakar, Sharath Pankanti, and Anil K Jain. Biometric recognition: Security and privacy concerns. *IEEE security & privacy*, (2):33–42, 2003.
- [18] John D Woodward. Biometrics: Privacy’s foe or privacy’s friend? *Proceedings of the IEEE*, 85(9):1480–1492, 1997.
- [19] The Johns Hopkins University. Basic Anatomy of the Heart. https://www.hopkinsmedicine.org/healthlibrary/conditions/cardiovascular_diseases/basic_anatomy_of_the_heart_85_P00192. Accessed: 2021-11-10.
- [20] L. Biel, O. Pettersson, L. Philipson, and P. Wide. ECG analysis: a new approach in human identification. *IEEE Transactions on Instrumentation and Measurement*, 50(3):808–812, Jun 2001.
- [21] The MIT-BIH Normal Sinus Rhythm Database. Available online: <https://physionet.org/physiobank/database/nsrdb/> (accessed on 15 November 2021).