DOI:10.22413/ijatest/2021/v6/i3/5

A NOVEL TECHNIQUE FOR AUTHENTICATION USING ECG

[1]J.Himabindhu, [2]P.Jagruthi, [3]N.Bharath kumar, [4]A.Dharani, [5]S.Abdul kalam
[1]Assistant Professor, Dept of ECE, AITS, Rajampet, AP, India.
[2,3,4,5]Student, Dept of ECE, AITS, Rajampet, AP, India.

***Abstract:** The primary focus of this paper is to use ECG signals to authenticate the user. The electrocardiogram (ECG) is an electric signal that indicates heart activity and has highly discriminative capabilities for human identification. Although ECG-based authentication has already had a lot of success recently, selective extraction of features and effective classification techniques now have a long way to go. In the current environment, authentication systems have become an essential necessity for protecting the integrity of systems and confidential data. Passcodes have given a means of controlling sensitive data, but they have also revealed some fundamental flaws. We develop an authentication mechanism called "A novel technique for authentication using ECG" that can accurately grant access to the user. Using assessment metrics, this authentication primarily contains filtering type, segmentation, feature extraction, and health status on ECG biometrics.*

***Keywords:** ECG Biometric, Authentication.*

I. INTRODUCTION

Face detection, as the often used biometric attribute by human beings, has been a challenge for the researchers for ages, which has some applications in consumer goods and software. In comparison to many other biometric qualities such as fingerprint recognition or iris, the face has a distinction for being easy accessible and non-intrusive. Therefore, in mischievous situations, this benefit will become a drawback, allowing hackers to easily produce clones and fake face detection systems. The process of outwitting a biometric system by providing a false proof in terms of achieving identification is known as a spoofing attack. The images or videos of a valid user can be easily acquired from a distant or received through the network, it is quite easy to create such an attack for face recognition systems.

In the case of 3D facial mask attacks, approaches that rely on the assumptions of a planar surface for a fake face are made useless. Facial masks, made possible by advances in 3D printing technology, take malicious activities a step further and present new problems for countermeasure research. The safety of confidential data, services, or facilities can be accomplished by providing that only authorized individuals have access. Despite the fact that passcodes include some protection and security access, they are sometimes so weak that they can be quickly guessed. Complex passwords are more safe, but they're also more harder to recall, therefore they're frequently "stored" in less secure ways. Moreover, having similar passcode is frequently reused in several apps or devices, allowing a fraud to access multiple resources with a broken password. Biometric technology is an attractive approach for authentication.

Generally, biometric technologies operate in one of two modes: 1) verification or 2) identification. The goal of an authentication system is to validate or verify an user's identity but the goal of an identification system is to identify a particular person. In the last decade, live-ness identification has been a high priority, with several solutions to the problems described. ECG is an essential signal, and its availability confirms that the patient is alive. Stealing someone's ECG is significantly more challenging. But apart from its benefits, ECG accuracy is inferior to those of some other established biometrics such as fingerprints. Our ECG signals come from our fingertips. Fingertip ECG has two advantages: first, it removes the need for the user to undress in order to insert electrodes, and second, it makes the fingerprint a logical candidate for ECG fusion. The number of heartbeats captured is the same for all users, ignoring the fact that some individuals have a very constant ECG and do not require as many readings as others with a less stable ECG. Hence, ECG based authentication is most appropriate for authentication.

II.EXISTING METHOD

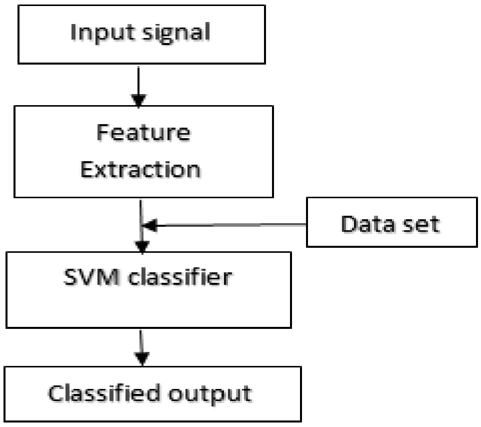

Fig.1. Existing System

The technique for intra-body communication was used to obtain intra-body propagation signals. For intra-body communication, three transmission mechanisms have been proposed: simple circuit type, electrostatic coupling type, and waveguide type. The waveguide type, in particular, considers the human body to be a waveguide via which an

DOI:10.22413/ijatest/2021/v6/i3/5

input signal at an input electrode pair is propagated as an electromagnetic wave to an output electrode pair. Furthermore, the waveguide type is resistant to environmental disturbances and can transfer signals over a wide frequency range.

The verification based on Euclidian distance is simple but insufficient for using the intra-body propagation signal for authentication in practical applications, so we incorporate the support vector machine (SVM) into the verification process to further improve the verification performance. The SVM has been proposed as a pattern classification approach based on supervised learning. The SVM learns a separating hyper plane that optimizes the distance (margin) between two classes and hence performs better separation for unlearned data of the classes. Figure 1 shows the separating hyper plane of two classes: C1 and C2. In practice, though, the two classes are practically linearly intertwined. As a result, they are linearly separable in higher dimensional space after being translated with a kernel function. Kernel functions such as the polynomial kernel, Gaussian kernel, and RBF kernel are commonly utilized.

The verification flowchart with the SVM is shown. The enrolling (learning) phase is completed prior to the verification. Intra-body propagation signals for all users are measured, then their spectra are removed, smoothed, and normalized to prepare learning data. The smoothing is done in the same way as before. The mean values of all amplitude spectra are adjusted to one during normalization. The classification of the user's own data and that of others to +1 and -1, respectively, is used to create user-specific models. During the verification (testing) phase, a user's spectrum is fed into the appropriate model, which is an already-learned SVM, and the SVM produces a prediction value. If the value is positive, the spectrum is considered to be that of a legitimate user. If the value is negative, however, the user is considered an imposter.

III.APPROACH FOR ECG BIOMETRIC AUTHENTICATION

This current approach is used to securely protect systems and data. We have two stages: enrollment and verification. The IIR butter-worth filter is then used to filter the data. For feature extraction, non fiducial is applied. The wavelet of Daubechies is carried out in two stages. Following that, DTW is used to perform biometric authentication. Due to changes in the lengths of their parts, two signals with similar features placed in the same order can appear significantly different. Dynamic time warping bends these durations so that the matching properties appears at the same time on a shared axis, emphasizing the signals' commonalities.

2.1. Butterworth filter

This signal processing filter is designed to have a frequency response in the pass-band that is as flat as feasible. A maximally flat magnitude filter is another name for it. However an ideal filter cannot be attained, Butterworth demonstrated that with increasing numbers of filter elements of the correct values, gradually better approximations may be created. Filters at the time produced a lot of ripple in the pass-band, and choosing component values was a lot of fun. Butterworth demonstrated that a low pass filter with a cutoff frequency of 1 radian per second and a frequency response (gain) was

$$G(\omega) = \frac{1}{\sqrt{1+\omega^{2n}}},$$

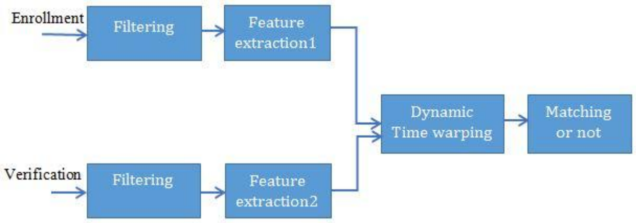

Fig.2. Approach for ECG biometric authentication.

Where ω is the angular frequency in radians per second and n is the number of poles in the filter equal to the number of reactive elements in a passive filter. If ω = 1, the amplitude response of this type of filter in the pass-band is 1/√2 ≈ 0.707, which is half power or −3 dB. Only filters with an even number of poles were addressed by Butterworth. He might not have realized that such filters could contain an odd number of poles. He used 2-pole filters isolated by vacuum tube amplifiers to construct his higher order filters. In his original graph, he labelled the frequency response of 2, 4, 6, 8, and 10 pole filters as A, B, C, D, and E.

The Butterworth filter's frequency response is absolutely flat (i.e., without ripples) in the pass-band and drops off to zero in the stop-band. The answer falls off linearly into negative infinity when examined on a logarithmic Bode plot. The responsiveness of a first-order filter decreases by 6 dB each octave. A second-order filter loses 12 decibels each octave, a third-order loses 18 decibels, and so on..

2.2 Daubechies wavelets

The Ingrid Daubechies wavelets are a group of orthogonal wavelets that define a discrete wavelet transform and are characterized by a maximum number of vanishing moments. There is a scaling function for each wavelet type in this class that produces an orthogonal multi resolution analysis. In general, for a given support width 2A, the Daubechies wavelets with the maximum number A of vanishing moments are chosen. The length or number of taps is referred to as DN, whereas the number of vanishing moments is referred to as dbA. As a result, D4 and db2 are the same wavelet transform. Among the 2A-1 feasible solutions of the algebraic equations for the moment and orthogonality constraints, the scaling filter with external phase is chosen. Daubechies wavelets are commonly utilized to solve a variety of difficulties, including signal self-similarity qualities, fractal problems, signal discontinuities, and so on.

Wavelets ability to express polynomial behaviour or information in a signal is limited by their vanishing moment. D2, for example, efficiently encodes polynomials of one coefficient or constant signal components with only one vanishing moment. D4 encodes two-coefficient polynomials, such as constant and linear signal components, while D6 encodes three-coefficient polynomials, such as constant, linear, and quadratic signal components. The transform treats sub-sequences that reflect linear, quadratic, or other signal components differently depending on whether the points

DOI:10.22413/ijatest/2021/v6/i3/5

coincide with even- or odd-numbered sites in the sequence. Because of the significant attribute of shift-invariance, several alternative variants of a shift-invariant wavelet transform have been developed.

2.3. Dynamic time warping

Dynamic time warping (DTW) is a time series analysis algorithm for determining the similarity of two temporal sequences that differ in speed. DTW has been used to evaluate temporal sequences of video, audio and graphics data, but it may be used to study any data that can be converted into a linear sequence. In general, DTW is a method for finding the best match between two sequences under particular constraints and rules:

• Each index in the first sequence must be matched with one or more indices in the second, and vice versa.

• The first index in the first sequence must equal the first index in the second series.

• The first sequence's last index must be matched with the second sequence's last index.

A "warping path" is created in addition to a similarity measure between the two sequences; by warping according to this path, the two signals can be synchronized in time. The signal with the original points X (original), Y (original) is warped to X (warped), Y (warped). This can be used in genetic sequencing and audio synchronization. The DTW algorithm creates a discrete match between existing elements in one series and new elements in another. In other words, time-scaling of segments within the sequence is not possible.

2.4. Procedure for ECG based authentication

- To begin, we gather ECG-based data from a particular dataset. We can plot the signal using this information.
- We have two parts here: enrollment and verification, and both phases will follow the same procedure.
- Preprocessing is done first, and then the signal is filtered using an IIR butter-worth filter.
- After that, a non-fiducial feature extraction technique is used for feature extraction. The Daubechies wavelet process is employed in this method. Wavelet filtering is applied after that, and features are extracted.
- Following that, the verification phase follows the same procedure. After that, the matching procedure is carried out.
- The matching operation is carried out utilizing dynamic temporal warping (DTW). It calculates the difference between two phases' characteristics (enrollment, verification).
- If the difference between the features of two phases is zero, the dialogue box indicates that the biometrics are matched; otherwise, the dialogue box indicates that the biometrics are not matched.
- Finally, the accuracy of the suggested implementation between filtered signal and dynamic temporal warping is calculated. When compared to existing methods, our proposed method produces better outcomes.

2.5. Advantages

- Provides superior biometric authentication results.
- More accuracy.

2.6. Applications

There are several applications for biometric technology, but the following are the most common:

- Logical Access Control.
- Physical Access Control.
- Time and Attendance.

IV. RESULTS

The below diagram represent the generated ECG signal.

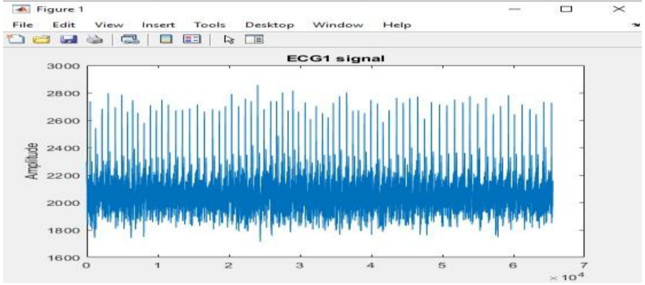

Fig.3. ECG1 signal

This signal processing filter is designed to have a frequency response in the pass band that is as flat as feasible. The IIR butterworth filter is depicted in the diagram below.

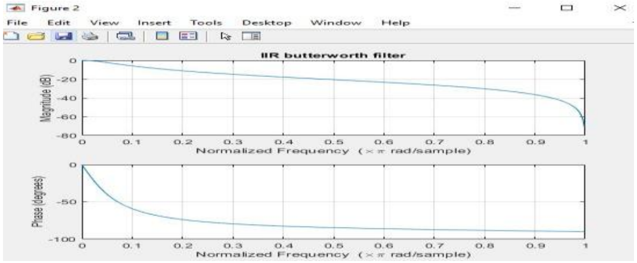

Fig.4. IIR butterworth filter

The generated ECG signal for the verification phase is depicted in the diagram below.

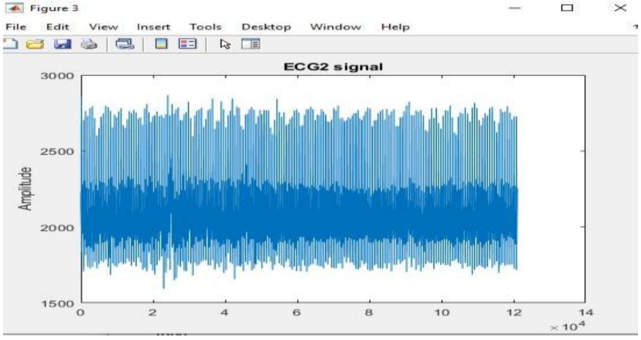

Fig.5. ECG2 signal

The IIR butterworth filter for the verification step is depicted in the diagram below.

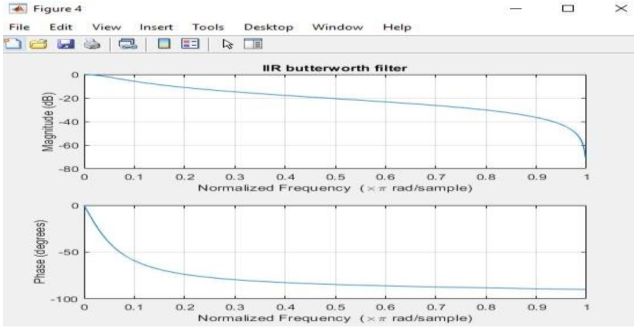

Fig.6. IIR Butterworth filter

Dynamic Time Warping (DTW) is a technique for comparing two sequences that do not have to be identical in length. After then, the matching process begins.

Not Matched

Fig.7. Dialog box represents matching or not.

V. CONCLUSION AND FUTURE SCOPE

The impact of filtering type, segmentation, feature extraction, and health state on ECG biometrics is thoroughly examined in this work. The ECG dataset is used for authentication to protect the devices and data. To put it another way, various experiments were carried out to assess the influence of significant methodologies for ECG biometric systems. When compared to the previous strategy, our new proposed methodology performs better, according to this research.

In future work, by taking the biometrics ECG signals in live and by using segmentation technique we can perform the biometric authentication.

REFERENCES

[1] Nesli Erdogmus and Sebastien Marcel. Spoofing face recognition with 3d masks. IEEE transactions on information forensics and security, 9(7):1084–1097, 2014.

[2] Abdenour Hadid, Nicholas Evans, Sébastien Marcel, and Julian Fierrez. Biometrics systems under spoofing attack: an evaluation methodology and lessons learned. IEEE Signal Processing Magazine, 32(5):20–30, 2015.

[3] Neslihan Kose and Jean-Luc Dugelay. On the vulnerability of face recognition systems to spoofing mask attacks. In 2013 IEEE International Conference on Acoustics, Speech and Signal Processing, pages 2357– 2361. IEEE, 2013.

[4] Javier Galbally, Raffaele Cappelli, Alessandra Lumini, Guillermo Gonzalez-de Rivera, Davide Maltoni, Julian Fierrez, Javier Ortega-Garcia, and Dario Maio. An evaluation of direct attacks using fake fingers generated from iso templates. Pattern Recognition Letters, 31(8):725–732, 2010.

[5] Zahid Akhtar, Christian Micheloni, and Gian Luca Foresti. Biometric liveness detection: Challenges and research opportunities. IEEE Security & Privacy, 13(5):63–72, 2015.

[6] Majid Komeili, Narges Armanfard, and Dimitrios Hatzinakos. Liveness detection and automatic template updating using fusion of ecg and fingerprint. IEEE Transactions on Information Forensics and Security, 13(7):1810–1822, 2018.

[7] Patrick PK Chan, Weiwen Liu, Danni Chen, Daniel S Yeung, Fei Zhang, Xizhao Wang, and Chien-Chang Hsu. Face liveness detection using a flash against 2d spoofing attack. IEEE Transactions on Information Forensics and Security, 13(2):521–534, 2017.

[8] Nima Karimian, Zimu Guo, Mark Tehranipoor, and Domenic Forte. Highly reliable key generation from Electrocardiogram (ECG). IEEE Transactions on Biomedical Engineering, 64(6):1400–1411, 2016.

[9] José Vicente, Pablo Laguna, Ariadna Bartra, and Raquel Bailón. Drowsiness detection using heart rate variability. Medical & biological engineering & computing, 54(6):927–937, 2016.