ORIGINAL RESEARCH

Submitted: 2.10.2022; Accepted: 21.10.2022; Published online: 25.12.2022

Analysis on specific biometric approaches: ECG as one of its trait

Mageshbabu M*, Mohana J, D.Gokulavani, Divya T.

ECE, SIMATS-Saveetha school of Engineering,Chennai, Tamilnadu

Corresponding author:
mageshbabum2002.sse@saveetha.com

Abstract

A biometric is in fact a pattern recognition system that uses biological traits like fingerprints, voice recognition, facial geometry, and hand geometry in addition to different patterns like iris and retina. The fact that different data protection codes like authentications and ID cards can be shared, stolen, or copied is what makes biometric so alluring. Physiological characteristics can be applied to improve the system's security and dependability. This paper provides an overview of the main biometric technologies, the fundamental techniques used, and the disadvantages of each. The paper then demonstrates how ECG operates and discusses various opportunities for ECG.

Keywords

Biometric, Recognition Methods,Access Control, Privacy, Safety.

Imprint

Mageshbabu M, Mohana J., D.Gokulavani, Divya T. Analysis on specific biometric approaches: ECG as one of its trait. Cardiometry; Special issue No. 25; December 2022; p. 1156-1160; DOI: 10.18137/cardiometry.2022.25.11561160; Available from: http://www.cardiometry.net/issues/no25-december-2022/analysis-specific-biometric

1. INTRODUCTION

The strongest link between a person's identity and their biometric characteristics is that they cannot be easily shared, lost, or duplicated. It is therefore more immune to social engineering attacks. This kind of system necessitates user presence during authentication. It may discourage users from asserting untrue things. As a result, it can be used in security applications. For forensic identification of criminals, law enforcement agencies all over the world rely on fingerprints. Access control, detecting multiple access controls, crossing international borders, and secure appropriate documentation are all dealt with by biometric traits. Each biometric characteristic has strengths and weaknesses of its own. Forensics, Automated teller machine banking, communication security[1], and other fields can all benefit from the technique of using bio – metric methods for identification.

Biometric Techniques:

Appearance-These physical characteristics include height, weight, gender, race, eye and skin colour, hair texture, physical markings, and height. speaking, habituated actions and visible handicaps. Bio-dynamics refers to a person's gestures, speech patterns, and keystroke dynamics, particularly in relation to login information and passwords Natural physiography. These include earlobe patterns, hand geometry, DNA, retina, and iris patterns, among many others. Imposed physical characteristics like dog tags, collars, bracelets and anklets, barcodes, embedded microchips.

2. BACKGROUND

A biometric is a computer that employs sensing, feature extraction, and matching modules to carry out biometric algorithms. The sensing component detects the traits, extraction of features removes extraneous data, and identical modules match the characteristics to references kept in the database. The authentication procedure is divided into two steps. As seen in Fig. 2.1, they are enrollment and verification. Verification is the process of comparing the extracted traits with references that are stored in the database. Registration is the method by which the traits in the database.

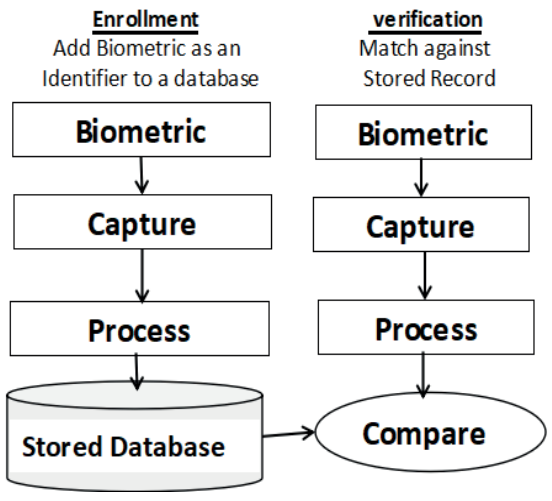

Fig2.1 BiometricSystem

Classification of biometric identification systems:

Biometric SystemsTypes:

Physical biometric:

This information obtained from precise calculates of human body parts. Some of the most popular physiological biometrics include facial recognition, iris, retina, iris, and fingerprints.

Behavioral characteristics:

The human is recognized based on his distinctive behavioural traits. These traits can include a person's walking gait, voice, speech, signature, and typing rhythm. Despite being influenced by an individual's actions, behavioural biometrics[2] is also determined by the physical makeup of the human body.

3. VARIOUS BIOMETRICS APPROACHES

- **Typing or Keystroke Recognition:**

The path in which a person types personalities on a keyboard is captured by keystroke dynamics. The period of time when a key is depressed is referred to as dwell time, and the period between pressing one key and pressing the next is referred to as flight time. This timing information is saved. The primary pattern that will be used for subsequent comparisons is then produced by processing the data using neural algorithms[3].

Fig.3.1 Typing Recognition

- **Speakeror Voice Authentication:**

A voice biometric is are presentation of a person's voice's sound, rhythm, and pattern. As distinctive to a person as any other biometric technique is the voice biometric, or «voice print.» Voice verification[4] is a relatively easy process. When registering, a user takes a voice sample and stores it as a «voiceprint» in the authentication system. A sample of the user's voice is provided to the system to determine whether they want to access the resource. In order to confirm that the correct person is granted access to the resource, a difference between the input and voice print is made.

Fig.3.2VoiceAuthentication

- Fingerprint Recognition:

Fingerprint technology, It is an identification technique where two fingerprint samples are compared to see if they come from the same sources. This method involves comparing various fingerprint[5] characteristics that have been identified as being particular to an individual. An individual's ridges and minute points are distinctive. There are three different types of ridges: loop, whirl, and arch. Specific fingerprint features known as minutia points are essential for identification. With the aid of a scanner, these finger features are photographed, enhanced, and transformed into a template. The template is a mathematical formula or a biometric key that has been encrypted. The fingerprint's image is not saved. This template cannot be changed back into an image by the algorithm.

Fig.3.3FingerprintIdentification

- **Hand or Finger Geometry Recognition:**

Based on the distinctive trait of the hand, hand geometry can find a specific person. The unique measurements may be length of finger, its thickness, the distance between the finger joints and full of the bone. The system consisted of a camera that records the hand's image. Extractions, processing, and database

memory of the need features take place. After that, these saved elements can be used for verification.

- **Facial Recognition:**

Face recognition technology can recognize a person based on the different features of their face. The nodal points are a group of distinctive characteristics on the human face[6]. On the face, here 80 various nodal points present. The size of the nose, the separation between the eyes, the length of the jawline, the curve of the facial orient on the cheekbones, in profundity of the eye socketsis, and a number of other features. Suitable algorithms like PCA and LDA are used to measure the locations of these nodal points. 3D face recognition systems, which are more accurate than older systems, are a growing concept in face recognition.

Fig.3.4 FacialRecognition

4. DRAW BACKS OF VARIOUS APPROACHES

- **Fingerprint:**

Injury, trauma, wounds, or cuts may obfuscate the fingerprint[5]values. The likelihood of the identification being rejected increases with distortions brought on by grease, dirt, or leakage on finger tips. Scanners of the present day are still unable to distinguish between authentic and fake fingerprints. Gelatinized moulds placed over real finger prints can be used to trick fake fingerprint[5].

- **Facial Recognition:**

Pose variations and ageing continue to be the main barriers to accurate face recognition[7]. 2D scanners are sensitive to changes in light and shadow and are unable to handle variations in pose. Although using 3D scanners prevents these restrictions, doing so is costly and time-consuming.

- **Voice Recognition:**

When there is noise and outside sounds, these systems are prone to error. The accuracy rates are also impacted by the user's proximity to the microphone. Voice[8] that has been prerecorded can be accessed maliciously. These systems need a lot of memory to store voice files and take time to adapt to a person's voice.

- **Iris and Retinal Recognition:**

The effectiveness of the system is impacted by the subject's proximity to the camera. Errors may happen as a result of reflection from eyelashes, lenses, or spectacles. The subject must maintain complete stillness throughout[9] the scanning process. The tools employed cost a lot of money.

- **Hand Geometry based Recognition:**

It becomes problematic when used with many persons. The propagation of human pathogens could be fatal[10]. The equipment may operate as a result of potential hand form changes.

- **Signature**

The inconsistent signature is a restriction for these systems. A person without the need for a consistent signature might not be recognized, and someone with a muscular disorder[11] might have trouble proving their identity. Rejections could also be caused by poor paper and ink quality.

- **Keystroke:**

Low accuracy rates caused by the inconsistent typing rhythms are the main drawback. These differences may be brought on by illness, exhaustion, distractions, mood swings, or the negative effects of using alcohol, drugs, or both.

- **DNA Recognition:**

It may not be very correct among close relatives because it is a new technology, making it less well-liked in public. takes time to establish identity and process. expensive machinery is needed to process and analyse the samples.

5. ECGAS A BIOMETRIC

Latest research has focused on biometric that use an ECG. The ECG is a graphic representation of the heart's electrical pulses. The ECG signal is a representation of the heart's electrical function[12]. Without the subject's cooperation, it is achieving to capture the ECG signal. Consequently, it is difficult to create a wrong identity. The fact that the ECG takes into account a person's vitality is one of its most significant futures. As a result, the person must be physically present during the verification process. Comparing these factors to the other biometric that were previously discussed, they all guarantee big security. Therefore, in the future, ECG may turn out to be the most hopeful biometric.

Description of ECG waveform:

ECG signal traits different segments of signal waves denotes the symbol of P,Q,R,S,T. Figure 5.1 displays information on the cardiac cycle. A conductor for current is the body. With the aid of an ECG, the electrical activity of the heartbeat can be seen on the skin. To monitor voltages changes in cells here between electrodes, electrodes are placed on the skin. On an analyzer and graph paper, these voltage variations are visibly enlarged and shown. An ECG records the heart's electrical activity from a particular "view" through a series of pulses and aberrations. Vertical analysis from fixed electrodes at various locations on the body are monitored by many screens, each of which is referred to as a lead. Bipolar leads I, II, and III each feature two electrodes with opposing polarities (positive and negative). Other sources' electrical activity is reduced by a third (ground) electrode. single lead with an one positive terminal and a reference point are AVR, AVL, and AVF (having zero potential). It is at the center of the heart's electrical field. Leads V1-V6 are single lead and consist of a single positive electrode with a negative reference point found in the electrical center of the heart. An ECG tracing looks different in each lead because the recorded angle of electrical activity changes in each lead.

A range of perspectives enable a more accurate understanding than just one. Any skin electrode can be made positive or negative by adjusting the Output device. The lead that the device registers determines the orientation. For an inspection system, a wire linked to the patient has three, four, or five coloured wires, or ten for just a 12-lead Electrocardiogram. A electrocardiogram reading might become aberrant by having the electrodes placed incorrectly.

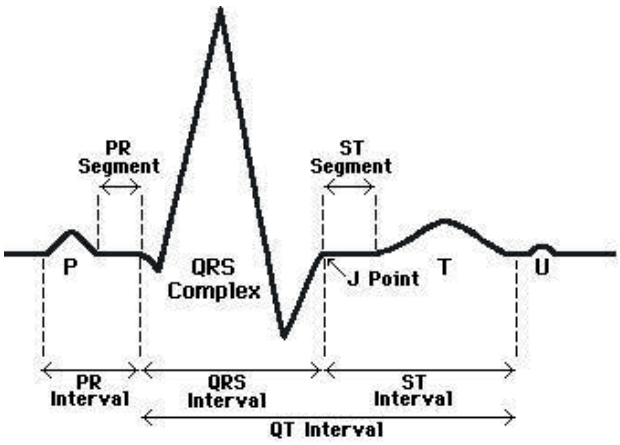

Fig5.1 Basic ECG signal

Features that make ECG unique:

The ECG is special because the morphology and signaling of the heart rate depending on the size, shape, and place of the heart. Heartbeat[8] is a characteristic of the heart that varies greatly. The average heartbeat of an individual is sixty to eighty beats per minute. The heart rate might reach two hundred beats per minute during times of stress or excitement.

This change could shorten the diastole and decrease ventricular depolarization[13]. The amplitude of a R wave may also be attenuated as a result. But there are only less variation in the length of the QRS complex. Typically, noise absorbs the ECG signal, necessitating preprocessing to remove the interference. Following preprocessing, Feature must be extracted in order to perform authentication.

6. APPLICATIONS OF ECG AS BIOMETRIC

The following areas are where we can conduct an ECG based authentication process. ID cards are typically used in attendance monitoring system systems to validate a person's presence. A guy could forget the ID at home, but it's quite unlikely that he would forget his heart home. Additionally, utilizing ECG to find duplicate attendance is challenging. ECG can be a crucial component of a single vote in electronic voting devices. One vote may be cast per person. Multiple votes or the addition of fictitious votes can be quickly found and disregarded. In the locking system found in automobiles, home doors, bank lockers, mobile phones, etc..It is The condition of a patient could be observed from a large distances utilizing telemedicine [15] by using the patient's ECG as an identifying feature.used in applications that include fund transactions, such as online platforms, ATM systems, and net banking.Used as a digital signature for delivering and receiving encrypted emails, electronically procuring goods and services, and filing tax returns, among other things. Useful for UID cards. Each Indian resident is given a 12-digit ID card called an UID cards. With the broader presence of banking sectors and error-free delivery of governmental schemes, this one source of truth will aid in financial inclusion. Irises and fingerprints[5] were photographed for the card.

These biometric equipment are susceptible to forgery. However, the individuality of a person can be tough to clone if ECG-based Reconization[17] is applied. Can be utilized as a factor in a person's identity while moving an international border[18] to prevent

future instances of illegal trespassing, smuggling, and other anti-social behaviour.

Acquire access control over computer programmes and data files that include sensitive information that is important to the military[19], inspection agencies, revenue, the defence, and other governmental agencies. keeping secrecy[20] for that kind of agency is crucial.

CONCLUSION

This paper evaluates the rationale for using an ECG-capable biometric identification system. In contrast to conventional biometric, which are neither firm nor robust sufficientin opposition to falsification, ECG is inherited by a person and is extremely secure and impossible to be falsified. The ECG's very very important feature is the real-time vitality feature. This makes the person's presence at the time of authentication necessary and prevents the acquisition of an ECG from a less persons. The ECG is the most innovative, useful, and widely applicable biometric identification. Its durability is a crucial component for it to quickly develop into a top-notch biometric system.

References:

1. B Rodger Jamieson, Ph.D., CA, Greg Stephens andSanthoshKumar"Fingerprint Identification: An Aidto the Authentication Process", Information SystemsAuditandControlAssociation.
2. NicosMaglaveras, Telemachos Stamkopoulos, Konstantinos Diamantaras, Costas Pappas, Michael Strintzis "ECG pattern recognition and classification using non-line art rans formation sand neural net works: A review", International Journal of MedicalInformatics52(1998)191-208
3. Fahim Sufi, Ibrahim Khalil, and Jiankun Hu, "ECG-BasedAuthentication",Chapter17,Handbookof-InformationandCommunicationSecurity(Eds.)
4. Abhishek Kumar Sinha, "Financial Transactions getpersonalizedandsecurewithbiometrics",DigitalTransformation.
5. P.SasikalaandDr.R.S.D.Wahidabanu,"Identification of IndividualsusingElectrocardiogram", IJCSNS International Journal of Computer Scienceand Network Security,VOL.10No.12,December2010
6. Dr.Neil Townsend, "Medical Electronics", MichaelmasTerm2001foundatpno 7
7. StevenA.Israel,JohnM.Irvine,AndrewCheng, MarkD.Wiederhold, Brenda K. Wiederhold "ECG toidentify individuals", PatternRecognition, The journalofpatternrecognitionsociety.
8. I.Goodfellow et al., "Generative adversarial networks," Communica-tionsoftheACM,vol.63,-no.11,pp.139–144,2020.
9. J.C.Carrillo-Alarco´netal.,"Ametaheuristicoptimizationapproachfor parameter estimation in arrhythmia classification from unbalanceddata,"Sensors,vol.20,no.11,p.3139,2020.
10. X. Zhai et al., "Semi-supervised learning for ecg classification withoutpatient-specific labeled data," Expert Systems with Applications, vol.158,p.113411,2020.
11. Z.Zhou,X.Zhai,andC.Tin,"Fullyautomaticelectrocardiogramclassificationsystembasedongenerativeadversarialnetworkwithauxiliary classifier," Expert Systems with Applications, vol. 174, p.114809,2021.
12. T. Golany and K. Radinsky, "Pgans: Personalized generative adver-sarial networks for ecg synthesis to improve patient-specific deep ecgclassification," in Proceedings of the AAAI Conference on ArtificialIntelligence,vol.33,no.01,2019,pp.557–564.
13. S.Pathoumvanhetal.,"Robustness studyof ecg-biometric identi-ficationinheartratevariabilityconditions,"IEEJTransactionsonElectricalandElectronicEng.,vol.9,no.3,pp.294–301,2014.
14. O. Boumbarov et al., "Ecg personal identification in subspaces usingradial basis neural networks," in 2009 IEEE international workshop onintelligent data acquisition and advanced computing systems: technologyandapplications.IEEE,2009,pp.446–451.
15. D.-H. Shih et al., "An embedded mobile ecg reasoning system forelderly patients," IEEE Transactions on Information Technology inBiomedicine,vol.14,-no.3,pp.854–865,2009.
16. R. Zhou et al., "Ecg-based biometric under different psychologicalstress states," Computer Methods and Programs in Biomedicine, vol.202,p.106005,2021.
17. Y. Xia et al., "Quick detection of qrs complexes and r-waves using awavelet transform and k-means clustering," Biomedical Materials andEng.,vol.26,no.s1,pp. S1059–S1065,2015.
18. H. Chen and K. Maharatna, "An automatic r and t peak detectionmethodbasedonthecombinationofhierarchicalclusteringanddiscretewavelettransform,"IEEEjournalofbiomedicalandhealthinformatics,vol.24,no.10,pp.2825–2832,2020.
19. Y. Zhang and S. Yu, "Single-lead noninvasive fetal ecg extraction bymeans of combining clustering and principal components analysis,"Medical & Biological Eng. & Computing, vol. 58, no. 2, pp. 419–432,2020.
20. J.Gordon,M.Norman,M.Hurst,T.Mason,C.Dickerson,B.Sandler,K.G.Pollock,U.Farooqui,L.Groves,C. Tsangetal.,"Usingmachine learning to predict anticoagulation control in atrial fibrillation:A uk clinical practice research datalink study," Informatics in MedicineUnlocked,vol.25,p.100688,2021.