Design and Development of a Novel Framework for the Secure Authentication of User

Vipula Madhukar Wajgade

APJ Abdul Kalam University Indore, Madhya Pradesh, India

Corresponding author: Vipula Madhukar Wajgade, Email: Vips.wajgade@gmail.com

The massive progression in the digital era has resulted in extensive use of technology following secure and robust authentication technologies. An incredible prerequisite for secure authentication techniques amongst various networks have been implemented. ECG Biometrics has been developed to encounter nonviolent input methods. This paper illustrates and proposes ECG biometric authentication technique and their applications. The main aim of the research is to develop a secure authentication system for preserving the secrecy of the user. The user's privacy will be conserved using the Electrocardiogram (ECG) signal since the external biometric modality is easily vulnerable to threats.

Keywords: Biometrics, Authentication, ECC algorithm, ECG-based biometrics, Depolarization.

2023. In Satyasai Jagannath Nanda & Rajendra Prasad Yadav (eds.), *Data Science and Intelligent Computing Techniques*, 517–523. Computing & Intelligent Systems, SCRS, India. https://doi.org/10.56155/978-81-955020-2-8-48

1. Introduction

Due to trustworthy authentication being needed, Biometrics is the best way of authentication in human beings. The extensive use of technology has a tremendous need for secure authentication techniques which can not be stolen, lost, or shared amongst networks. ECG Biometrics has been developed to overcome this challenge based on very safe input methods. This paper illustrates and proposed ECG biometric authentication technique and their applications. The main aim of the research is to develop a secure authentication system for preserving the privacy of the user. The user's privacy will be preserved using the Electrocardiogram (ECG) signal since the external biometric modality is easily vulnerable to threats, the cardiovascular or heart-based biometric ECG is introduced and studied through different aspects. The ECG signals are unique to humans and can not be replicated like other biometric authentication systems. We can achieve a high level of security through heart-based authentication. ECG signals from living human bodies are considered unique for authentication, which cannot be stolen, fake, or replaced. The ECG measures the electrical activity of the heart. The heartbeat pumps the blood to the body whereas the heartbeat is a series of events. The heartbeat consists of a P-wave, T-wave, and QRS complex. The P wave represents the representation of atria while the QRS complex represents the depolarization of ventricles and the T wave represents the depolarization of ventricles. The heart's electrical activity is measured in a graph as time versus voltage and is called as an electrogram. Ten electrodes are placed on the patient's limbs and chest. The overall goal of ECG is to check the electrical functioning of the heart[5].

1.1 Related work

The phenomenon of Biometric authentication emerges as a result of security and authenticity. The process of examining the physical and behavioral characteristics of human beings is called Biometric Authentication. William Herschel in 1858 was the first to use biometric characteristics or features. Alphonse Bertillon in 1870 used body measurements for criminals. Later with advancements authentication and matching strategies were developed. In the 19th and 20th centuries, the first developed authentication was the Fingerprint authentication. Over the counters, the shortfalls of systems came to know and more robust systems were developed. The ancient approach to authenticate and identify Tokens, code numbers, PINs, and some sort of Cards was used which has many drawbacks and couldn't provide security in depth. As time progresses the advancement in technology and researchers study as many approaches were developed[6]. The forensic use of biometrics is vital and the government offices where the critical database needs security must have a robust approach. Biometrics systems involve two main phases mainly enrolling the user and the next identification. Enrolling the user means creating a copy of the user in the biometric database where it can be again accessed. This process registers the user with any biometric feature and there will be conversion of this into a digital format. Next time when the same user tries to access the system with the biometric feature the new data is compared with the data stored in the database and accordingly access is given or rejected. The following table illustrates various types of biometrics used .Fingerprints ,retina recognition and iris recognition are some of the methods discussed[9].The table 1.1 shows evolution of biometrics.

Table 1: Evolution Of Biometrics

Year	Type	Author	Method	Place
19^{Th} century	Fingerprinting	Richard Edward Henry	Fingerscans	Scotlant
1935	Retina Authentication	Dr. Carleton Simon, Dr Isadore Goldstein	Retina Scans	---------
1993	Iris recognition	John Daugman	Iris scans	Cambridge University
2001	BAT	---------------------	Tangible recognition	kosovo

Biometric authentication mainly focuses on the behavioral or physiological characteristics of human beings. It is more calculated, latest, and information-sensitive. It is merely impossible to replicate biometrics so it protects sensitive data. So, there are two types of biometrics: Behavioral Biometrics and Physiological Biometrics. The table 1.2 discusses the comparison of biometrics on the basis of performance, output, and robustness.

Table 2: Comparison of Different Biometrics Systems

Type of Biometrics	Performance	Output	Robustness
Fingerprint Recognition	Medium	Best	High
Retina or Iris Recognition	High	Good	High
Facial Recognition	Medium	Good	High
Voice Recognition	Low	Good	Medium
Keystroke Dynamics	Low	Low	Medium
Signature	Medium	Low	Low

2. ECG Based Biometrics

The Heart-based biometric system works by receiving ECG signals from the receiver at the receiver end and then processing of signal and then transmitting it over the global network[2]. The previous systems do not provide security and can be attacked. Various methods and modes are tested to obtain the best output results[9]. Researchers used different types as follows. The following table shows a list of different methods and modes used.

Table 3: Different Modes of ECG Authentication Development

Researcher	Mode	Method
Zhao et al.	Intrinsic mode	ECG features
Singh et al.	End fiducials	Face and fingerprint
Silva et al.	ECG from fingers	ECG
Safie et al.	PAR	PPG
Niinuma et al	User's clothing and facial skin	
Ali et al. And Saevanee et al.	Text-based multimodal	Behavioural biometric
Frank et al.	Behavioral screen touch	--
Chan et al.	Behavioral screen touch	
Sitova et al.	Hand gestures	Smartphone authentication
Khan et al.	IA	Smartphones application
Rasmussen et al.	Pulse response	Radio based

The ECG is used to measure the electrical activity performed by the heart. The heartbeat is simply a series of events and the heart pumps the blood to the body. The heartbeat consists of a P-wave, T-wave, and QRS complex the P wave represents the representation of atria while the QRS complex represents the depolarization of ventricles and the T wave represents the depolarization of ventricles[9].The electrical activity of the heart which is measured in the graph as time versus voltage is called an electrogram [9].Ten electrodes are placed on the patient's limbs and chest. The overall goal of ECG is to check the electrical functioning of the heart[7][8].

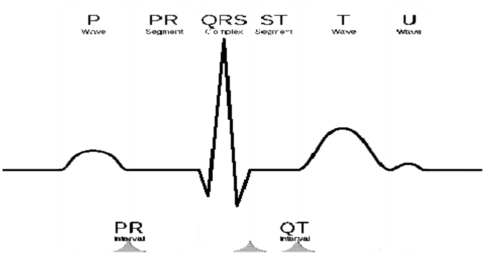


Fig. 1. Normal ECG[7]

The 5 steps of the electrical pathway of the heart are made up of 5 elements:[9]

The sino-atrial (SA) node.
The atrioventricular (AV) node.
The bundle of His.
The left and right bundle branches.
The Purkinje fibers.

Elliptic curve cryptography: ECC is a further defined cryptographic system. It has public and private keys same as RSA.A public key is used for the encryption of text and the private key is used for decryption purposes[1][2].

3. Proposed System

The main aim of the research is to develop a secure authentication system for preserving the privacy of the user. Here, the user's privacy will be preserved using the Electrocardiogram (ECG) signal since the external biometric modality is easily vulnerable to threats. The authentication will take place using two phases as registration phase and the signature phase. In the authentication phase, the ECG signal from the respective owner will be collected and then the preprocessing of the signal will be performed. ECG is a non-invasive test that records the electrical signals produced by the heart as it beats. The resulting ECG signal provides valuable information about the heart's rhythm, rate, and overall cardiac information. After collecting the ECG signal the preprocessing of the signal will be performed to reduce the noise present in the signal. From the preprocessed signals the features relevant to the heart such as Heart rate variability, Frequency features, statistical features, and Fiducial features will be extracted. Based on the features extracted the hash key generation will take place and this information will be encrypted using the Elliptic Curve Cryptography (ECC) algorithm. ECC is a public-key encryption algorithm that depends on the mathematics of elliptic curves over finite fields. It offers strong security with shorter key lengths compared to other encryption algorithms. Similarly, in the signature phase, the ECG signal from the user will be collected and then the preprocessing, feature extraction, and hash key generation will take place. The authentication between the data will be provided using the decrypted data from the registration phase and the hash key generated in the signature phase. If the information generated is similar then the access will be provided else the accessibility will be denied. The research will be carried out using the software Python and the efficiency will be proved using the metrics time, delay, and false user detection rate. The schematic representation of the framework is shown in Figure2.

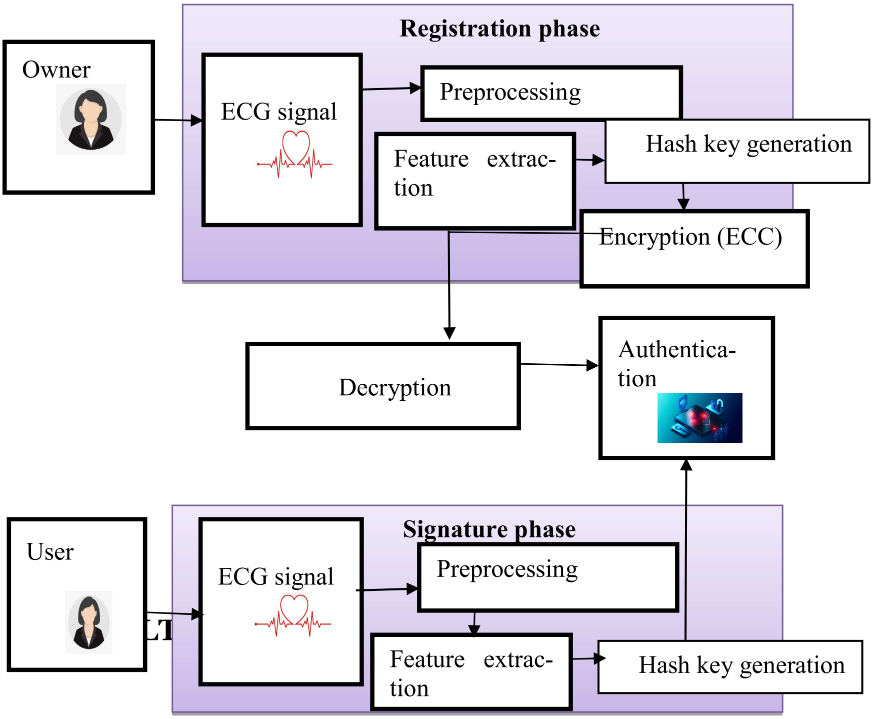


Fig. 2. Schematic Representation of the Framework

The authentication system is evaluated and tested with input as ECG signals that is cardiac cycles. The authentication is performed through ECC (Elliptic Curve Cryptography) for the encryption and decryption. The performance of the system is assessed with users and time graphs. ECC encryption algorithm is studied for different key size

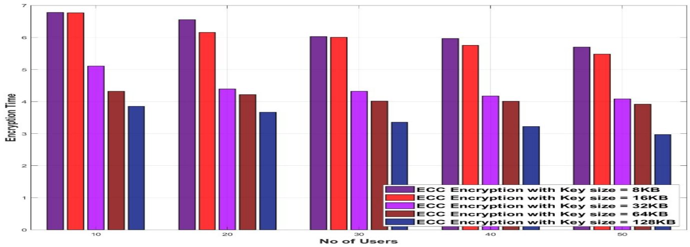
Hence the proposed system works efficiently and provides a robust and secure authentication method. Some of the best features of the above system are as follows-

1. The input given to the above system is permanent and not changed over time.
2. Provide a secure and robust approach as ECG signals can not be counterfeit.
3. The system is more accurate in terms of results.
4. The ECG signals and heartbeats are unique and thus result in exclusivity.

Table 4 shows different key size of ECC encryption versus time values and it is found that with increase in key size time increases.

Table 4: Experimental result of ECC with different key siz

ECC Encryption with Key size = 8KB	ECC Encryption with Key size = 16KB	ECC Encryption with Key size = 32KB	ECC Encryption with Key size = 64KB	ECC Encryption with Key size = 128KB
3.309375	4.3953125	4.8578125	5.9484375	6.5625
3.1828125	4.20625	4.2828125	5.94375	6.4046875
3.1625	4.0125	4.178125	5.8234375	6.1859375
3.1546875	3.8796875	4.0875	5.5484375	6.0765625
3.10625	3.8296875	3.8984375	5.3640625	5.834375



Various encryption algorithms have been studied and evaluated and ECC encryption thus resulted most efficient and fast. Table 5 illustrates different encryption algorithms such as DES,AES,RSA,RC5 and ECC encryption. It is found and noted that ECC is more time efficient than any other algorithms studied.

Table 5: Computing ECC with variousalgorithms

DES Encryption	AES Encryption	RSA Encryption	RC5 Encryption	ECC Encryption
0.3125	0.265625	0.125	0.109375	0.09375
1.640625	1.21875	1.03125	0.53125	0.390625
1.9375	1.78125	1.3125	0.96875	0.5625
153.015625	124.4375	97.953125	76.296875	18.5
208.359375	153.703125	115.234375	97.78125	23.578125

4. Applications

The various applications of heart-based biometric authentication are as mentioned below

4.1 Medical and Healthcare:

To maintain the privacy of users as well as to give authenticity biometric authentication has become popular amongst healthcare professionals. Fast identification is useful in emergency conditions[3][4].

4.2 Defence Systems:

Government security forces should use the best authentication for the safety of the nation.

4.3 Banking And Financial:

The digital era involves financial online transactions on a frequent basis debit cards, credit cards, and Internet banking need the most secure method of transfer to limit online fraud.

References

[1] Vipula Madhukar Wajgade et al.: Review of steganographic techniques using Cryptography/ International Journal of Computer Science & Engineering Technology (IJCSET) ISSN: 2229-3345 Vol. 4 No. 04 Apr 2013 426

[2] Zhang Y., Wu J. Practical human authentication method based on piecewise corrected Electrocardiogram; Proceedings of the 7th IEEE International Conference on Software Engineering and Service Science (ICSESS); Beijing, China. 26–28 August 2016; pp. 300–303. [Google Scholar]

[3] Zhang Q., Zhou D., Zeng X. HeartID: A Multiresolution Convolutional Neural Network for ECG-Based Biometric Human Identification in Smart Health Applications. IEEE Access. 2017;5:11805–11816. doi: 10.1109/ACCESS.2017.2707460. [CrossRef] [Google Scholar]

[4] Zhang Y., Gravina R., Lu H., Villari M., Fortino G. PEA: Parallel electrocardiogram-based authentication for smart healthcare systems. J. Netw. Comput. Appl. 2018;117:10–16. doi: 10.1016/j.jnca.2018.05.007. [CrossRef] [Google Scholar]

[5] Biel L., Pettersson O., Philipson L., Wide P. ECG analysis: A new approach in human identification. IEEE Trans. Instrum. Meas. 2001;50:808–812. doi: 10.1109/19.930458. [CrossRef] [Google Scholar]

[6] Camara C., Peris-Lopez P., Gonzalez-Manzano L., Tapiador J. Real-Time Electrocardiogram Streams for Continuous Authentication. Appl. Soft Comput. J. 2018;68:784–794. doi: 10.1016/j.asoc.2017.07.032. [CrossRef] [Google Scholar]

[7] https://en.wikipedia.org/wiki/Electrocardiography#/media/File:EKG_Complex_en.svg

[8] https://www.nottingham.ac.uk/nursing/practice/resources/cardiology/function/conduction.php

[9] Vipula Madhukar Wajgade, Dr.Sharanabasappa C Gandage A Review Study Of Biometric Authentication Techniques IJCSPUB© 2022 IJCSPUB | Volume 12, Issue 2 June 2022 | ISSN: 2250-1770