

Mechanisms of Authentication toward Habitude Pattern Lock and ECG: An overview

Jose-Luis Cabra^{1*}, Carlos Parra², Diego Mendez², and Luis Trujillo²

¹Fundación Universitaria Compensar, Avenida (Calle) 32 No. 17 – 30. Bogota, 111311, Colombia
jlcabral.eng@gmail.com, jlcabra@ucompensar.edu.co

²Pontificia Universidad Javeriana, Ak. 7 #40 - 62. Bogota, 110231, Colombia
carlos.parra@javeriana.edu.co, diego-mendez@javeriana.edu.co, trujillo.luis@javeriana.edu.co

Received: August 10, 2021; Accepted: February 17, 2022; Published: June 30, 2022

Abstract

Smartphones contain access to user-sensitive information such as contacts, e-mails, e-payments among others. Therefore, it is imperative that proper smartphone authentication tools guarantee that only the smartphone proprietary has full control of its mobile features and data. Following this, this paper proposes an overview of smartphone authentication, with the purpose to delve into two biometric viable solutions: Habitude Pattern Lock and ECG unlocking services. For that aim, it is required to provide a clear meaning about the different forms how authentication can be performed. As the next step, an introduction to biometrics is offered, which includes behavioral, hidden, and physiological approaches with the purpose of addressing their scopes and weaknesses. Then, to enrich the smartphone authentication environment, we propose the study of Pattern Lock and ECG verification tools. The Pattern Lock section discusses the study of topics like measure of pattern strength, commonly suffered attacks, and our proposal Habitude Pattern Lock, which includes the user habit patterns while drawing the lock pattern. Then, the ECG authentication section covers the features of this potentiality technology, ongoing research and products related to the ECG authentication on mobiles devices, and research topics like current limitations, specific acquisition concerns, and improvement proposals.

Keywords: Smartphone Authentication, Mechanism of Authentication, Biometrics applications, Pattern Lock, ECG

1 Introduction

Smartphones have been designed to facilitate Internet functions, focusing on services in apps. These devices allow people to communicate and manage information wirelessly while attempting to maintain their privacy. There have been several milestones in the development of smartphones, the first of which was the Simon Personal Communicator in 1992 from IBM without success in sales. Then, in 2007 Apple launched the first iPhone [1] which kick-started the smartphone phenomenon. In 2016 and 2017 alone, smartphone sales skyrocketed 1.4 and 1.5 billion units per year [2]. Despite a drop in 2020, this market reached its peak with 1.5 billion units in 2019 and 2021 [2, 3, 4].

This handheld system has become society's remote control [5]. Our mobiles are capable of keeping personal contacts, emails, files, conversations, and user preferences. Phones can also perform sensitive

Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), 13(2):23-67, June 2022
DOI: 10.22667/JOWUA.2022.06.30.023

*Corresponding author: Department of Telecommunication Engineering, Fundación Universitaria Compensar, Avenida (Calle) 32 No. 17 – 30. Bogota, 111311, Colombia. Tel: +57-311-822-86-36

operations like making e-payments or performing specific operations through an app, for example, smart home services or e-health monitoring. Therefore, access to these devices by unauthorized people becomes a violation of the phone owner's privacy. The consequences of a data leak could be catastrophic depending on the type of information that was compromised and how it is used. There are multiple examples of authentication scams, such as the e-Transfer theft of 19,000 CAD [6] apparently as a result of a shoulder surfing attack. In the United States, the Federal Trade Commission (FTC) exists to prevent identity theft. This agency provides a series of recommendations [7]. In an attempt to mitigate the impact of identity theft, the FTC has created a web portal where victims can report cases, creating an identity recovery plan [8]. In the case of smartphones, the FTC suggests that the easiest way to avoid access by unidentified users is simply to lock down the device and to require a valid user verification request to unlock and reuse the phone features.

Nowadays, a sizeable group of users exist who do not lock their smartphones. These people prefer quick access over recognition methods such as PINs, passwords or pattern locks. This indicates that users prefer usability preference over privacy protection [9]. This trade-off between confidentiality and usability option opens a new variable parameter in user interaction studies. Overall, most people prefer usability over any slow locking service. Thereby, smartphone attributes like confidentiality and usability contain a time response restriction; it implies a compensation evaluation between performance and accuracy in the verification engine. Among the most common authentication techniques are a PIN code or secret pattern; unfortunately, both are susceptible to a spoofing attack [10]. Consequently, once the secret code is exposed and the verification step is broken, it renders unrestricted access to the mobile and the whole system is disclosed.

Regarding biometric authentication, their HW/SW market has grown from \$2.4 billion in 2016 with an expected growth of \$15.1 billion to 2025, all of it within a \$50 billion biometrics global business by 2024 [11]. Not limited to smartphones, camera biometrics will also grow to a market of \$19 billion by 2024 [12] and iris recognition \$4.1 billion by 2025, according to Tractica forecast [13]. In units, over 1 billion devices in 2020 contain facial and fingerprint recognition [14, 15]. However, some people do not trust or do not want to use biometrics in their smartphone [16]; consequently, they lock their phone with a password instead [16].

Popular methods such as fingerprint or facial recognition have the possible weakness of being copied to unlock the smartphone [17, 18, 19]. Indeed, each method under specific conditions can achieve its best rate of success. But, every single biometric method has its own kind of weakness. Between the conventional authentication techniques, none are fail-safe [20]. We have to take into account that biometric systems will inherit their sensor limitations.

In this paper, we intend to present some weaknesses and open gaps in current smartphone authentication. Indeed, our intention is not to discredit knowledge-based support or highly rated traits like fingerprint, iris, or face. On the contrary, we seek to raise awareness of the limitations of some unlocking methods and suggest alternative ways to verify a user. Besides, the goal of this paper is to provide a general map of smartphone authentication. In the last chapter, we will focus on two unusual proposals, one talking about enhanced proposals for pattern lock, taking advantage of smartphone current embedded sensors, and the other using ECG biosignal for user verification. Indeed, these proposed mechanisms do not have a technological limitation; furthermore, they can be implemented, providing a new possibility to support the current verification procedures cooperatively.

In the next list, we show the series of contributions of this text.

1. We will produce a comparative biometric performance table. Category descriptions including physiological, hidden, and behavioral approaches, making emphasis on each method's weakness. (Section 3)
2. Following biometric trait identification requirements by Dasgupta et al. [21] and Maltoni et al.

- [22], we will produce a comparative evaluation that includes together physiological, hidden, and behavioral approaches. (Section 3)
3. We will gather various studies studies on pattern lock. To the best of our knowledge, we have not found an article that collects multiple strands of research about it. It includes functionality, shapes proposals, entropy, preferability, attacks, and enhancements. (Section 4)
 4. We propose the term *habitude pattern lock* (HPL) in state of the art. (Section 4)
 5. Within our HPL proposal, time acquisition is highly essential. In this way, we made a study of the best Android function to perform this task. (Section 4)
 6. We contribute a comparative feature-based parallel between different researches in state of the art close to pattern lock and HPL. (Section 4)
 7. Regarding smartphone authentication with ECG, we will cover topics like thermal noise presence, leads quantity, an approach to T wave contribution, and verification of heart disease conditions. (Section 5)
 8. We submit a collection of current limitations, specific acquisition concerns and improvement proposals in *ECG biometrics* and *HPL*.



Figure 1: General paper sequence

The structure of this work (Figure 1) continue in section 2 with the *authentication* concept and mechanisms. We decided to introduce this concept because of different applications usage of the verification procedure, but they do not offer the same features in their services. Thus, it is necessary to discriminate each reach in user verification to understand and cover the authentication in mobile devices. In the next stage (section 3), we provide an invitation to understand the handset authentication with a biometric-based approach. Sections 2 and 3 have the purpose of knowing the current state in smartphone authentication, as an opening point for understanding the space of the initiatives of the next sections. Section 4 (pattern lock authentication) and section 5 (ECG authentication) both include current limitations, specific acquisition concerns, and improvement proposals. Lastly, we conclude this article our final opinion of the topics mentioned in this text.

2 Authentication types

This section in our article will categorise the different smartphone authentication attributes, creating a point of reference for further analysis. The importance of verifying the origin of any interaction makes the use of the word *authentication* necessary in different fields of study. One example is the definition of security in communications, where secure data transmission needs to be composed of three elements: confidentiality, integrity, and authenticity. The last component, a machine to machine context means to trust in the source/destination parties through encrypted message exchange. In the case of email

login, authentication comprises of a user/password and a token code number; the session is on until the account owner, signs-out. Similar to an ATM, the user trusts the PIN-code and the credit card acts as the token, but the session expires after the selected operation ends. For that reason, in the face of several authentication procedures, it is necessary to classify them and determine the best mechanism for their application. Consequently, the following subsections (2.1 and 2.2) define human-machine authentication ways and mechanisms oriented to the smartphone-perspective.

2.1 Human authentication strategies

There are three strategies [21, 23] to authenticate humans. Listed below:

- **Something you know:** With this technique, the device asks the user to enter some numerical, alphanumeric, or sequence code that ideally only the right user knows. The most common methods here are PIN code, password, or pattern lock (Figure 2). This method is the primary trust source for the operating system. An extension of knowledge-based validation is in section 4.

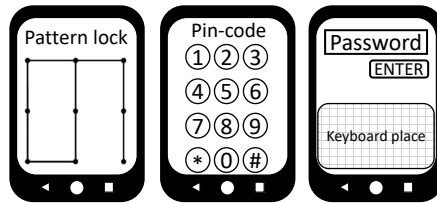


Figure 2: Knowledge-based authentication examples

- **Something you have:** Also known as token operation, it is used for instance, in financial operations when the user/password is enriched with a specific code provided by an external entity. This One Time Password (OTP) changes each verification request. Curiously, today's cellphones have included an option to incorporate bank tokens as apps [24, 25], or by way of supporting the opening of the email signature in non-common computers (Figure 3), among others. Therefore, in object-based validation, the smartphone is the entrance key but not the way to check the user proprietary; one more reason to be aware of phone-unlocking. Due to our scope, this work is oriented to protect a smartphone active session, and as such, this authentication method is not extended in this paper.



Figure 3: Object-based authentication examples

- **Something you are:** This study is geared towards the study of unique user patterns that can be physiological, hidden, or behavioral (Figure 4). Forgetting codes does not apply in this situation and the user presence is mandatory and highly appropriate for smartphone usage. This approach is extended in section 3.1.

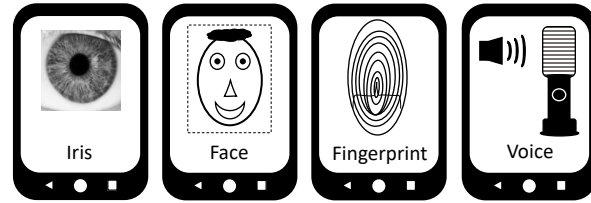


Figure 4: Biometric-based authentication examples [26]

2.2 Authentication mechanisms types

The smartphone can request user-authenticity credentials through a challenge or in a pervasive interaction. In a challenge oriented evaluation, the user needs a mandatory time while executing a requested operation, for example, taking a photo, device shaking, fingerprint reading, among others. This procedure often uses knowledge-based, physiologic biometrics, and some behavioural biometric methods. On the flip side, the pervasive oriented evaluation offers the user validation without interference in their daily dynamics. This implementation allows the device to evaluate the user validity but in a parallel way. In other words, the user and their context interacts with the device ubiquitously without interrupting the regular phone use or requiring any action from the user [27].

The different authentication mechanisms [23] that guide the user verification types are:

- **One-Shot authentication:** The user is validated before the session opening, and it finishes when the user closes the session.
- **Periodic authentication:** It incorporates one-shot authentication characteristics, but the session remains open until an idle time is over.
- **Single Sign-On authentication:** It manages a long-term open session that can be closed by the user anytime. If the system finds some change in the context (network, location, habits), a user re-authentication is required.
- **Multifactor authentication:** It can combine the different authentication strategies seen in section 2.1. One example could be to request a password and then request a fingerprint measure, or an OTP.
- **Static and Dynamic authentication:** Static authentication uses the same set of challenges as user verification. Meanwhile, dynamic authentication varies the challenges for each session opening.
- **Continuous authentication:** Regularly the user is validated through their habits during all the open-sessions, without interfering with their smartphone usage.
- **Transparent authentication:** With or without requiring a session opening, transparent authentication evaluates the user interaction with the smartphone in the background without a mandatory direct user operation being necessary. Transparent authentication can be used with other mechanisms like one-shot or continuous.
- **Risk-Based authentication:** According to the context, this mechanism evaluates a different set of variables pondering them to calculate a risk factor. This value is a threshold that determines if the entrance is valid or not.
- **Adaptive authentication:** It can reorganize its authentication criteria due to the changes in the environment because of different conditions or situations.

- Unimodal and Multimodal authentication: This modality is oriented to biometric approaches. Unimodal refers to acquiring one trait validation to verify someone; instead, multimodal works with two or more different traits to evaluate the owner's entry.

The previous list summarizes different authentication orientations in systems to deploy. However, maybe some readers could find some of these approximations unavailable to carry out. In that case, the next two pieces of evidence that could help to expand those implementations possibilities. First, Figure 5 shows a set of sensors that are already embedded in our smartphones. Indeed, each sensor generates enough data that can be turned into information. Consequently, different information sources allow it to collect enough knowledge to authenticate a user. For example, the camera can provide user categories like age, facial attributes, background-location, sex, and motion, all of them having discriminatory richness. Indeed, the camera example can be extrapolated to another sensor to extract complementary information. Therefore, the smartphone contains a plethora of sensors that provides sufficient data to authenticate a user. Second, Table 1 extends and depicts the authentication mechanism types and includes categories like request mode, session permanency, session close condition, and some related work.

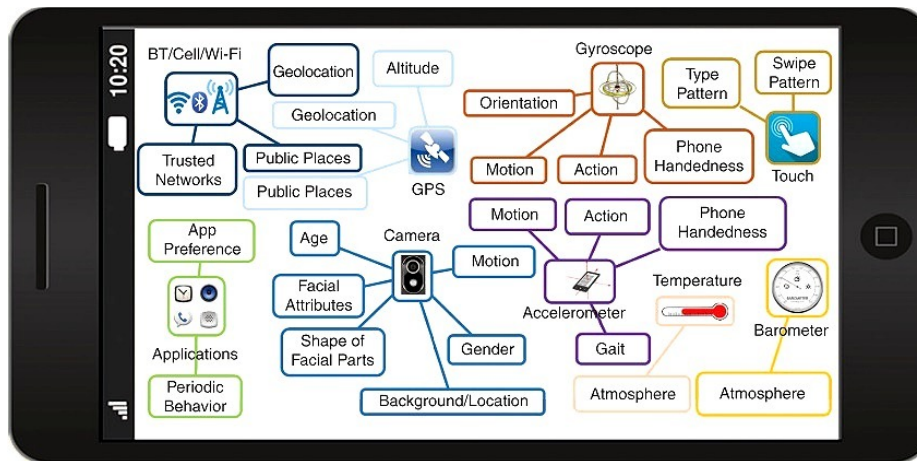


Figure 5: Information possibility from cellphone sensors [28]

3 Authentication for smartphones using biometric approaches

3.1 Overview

Biometric coverage, as an authentication tool that tests users to access all smartphone utilities, applications, and data, is still growing. Biometrics aims to measure specific and unique person bodily features unique to each individual; meanwhile, the knowledge-based approach requires it to keep some code in mind. Conversely, smartphone biometrics demand the user's presence, eliminating the need to memorize some code or sequence or the requirement to carry something (token).

The standard verification sequence consists of seven different blocks described briefly in Figure 6.

- The sensor module contains a transducer device that captures the signal of interest.
- The preprocessing component includes at least one of the next options like signal amplification and filtering to signal improvement and highlighting the region of interest (ROI).
- The Feature extraction block transforms the ROI to derive values that represent meaningful information that describe the smartphone user.
- The template generator component collects the set of calculated features, similarly to the user data reference in the registration and verification steps.
- The stored-templates element is a database that

Table 1: Brief of authentication mechanisms

Mechanism \ Category	Request	Session keep-alive	Session close condition	Examples
One-shot	Challenge or correct credential	No-condition	Screen-off	[29, 30, 31]
Periodic	One-shot variant	No idle state	Idle timeout	[29, 32]
Single Sign-On	Depends on the chosen method	- Aeonian. - If context change ->... re-authenticate	If spatial context change. Sign off	[33, 34, 35]
Multifactor	Two or more authentication strategies requested	Depends on the chosen method	Depends on the chosen method	[36, 37, 38]
Static and Dynamic	Fixed and shifting challenges approval	Depends on the chosen method	Depends on the chosen method	[39, 40, 41]
Continuous	Within session constant analysis	- Normal usage. - Under some abnormality ->... re-authentication prompt	Inconsistent usage and wrong re-authentication	[42, 43, 44]
Transparent	Various user sensing sources through their mobile interaction	Acceptable confidence level	Low device confidence	[45, 46, 47]
Risk-based	- Contextual risk-score profile evaluation. - If no risk, entry automatically. On the contrary, user must provide information	No risk after evaluation	Context change ->... risk found ->... wrong credentials	[48, 49, 50]
Adaptive	- Continuous user context learning. - Authentication method can change due to the environment. If the context is secure, it enters	Context safe	Unsafe context due to previous learning	[51, 52, 53]
Unimodal and multimodal	User trait/traits	No-condition	Screen-off	[54, 55, 56]

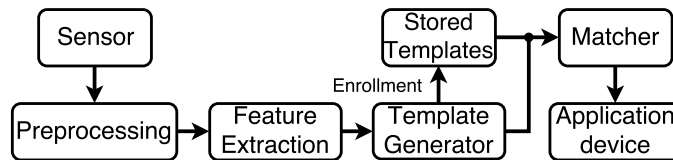


Figure 6: General architecture of a biometrics system

contains and stores the enrollment templates. vi) In a new smartphone entry attempt, the matcher section is responsible for numerically scoring the comparison between enrollment database samples and the new template. This evaluation considers a specific closeness metric, for both templates; near or far. vii) Application-device module uses the information provided by the Matcher and grants or denies access using a threshold criteria.

There are two famous biometrics trends on behavioral and physiological analysis, as explained by ISO/IEC 2382-37 [57] and NIST.SP.800-12 [58]; we extend this separation in a general map in figure 7. The behavioral approach focuses on the analysis of specific user movement habit patterns, even if different people perform the same action. One example is the trait of gait, which has demonstrated to be an unique characteristic among human beings [59].

In a formal way within the smartphone context, behavioral biometrics comprehend some of the next study fields: touch dynamics (gesture), keystroke dynamics, gait recognition, behavioral profiling, hand-waving authentication, voice, and signature. Setting aside the last two and in order to avoid the cross-use of contradictory meanings, each of these will be explained below.

1. Gesture-touch dynamics: It is a hand-drawn form over the smartphone touch-screen composed by a set of strokes that contains a group of ordered-pairs X and Y [60, 61, 62, 63, 64].
2. Keystroke dynamics: It studies how the user interacts during the use of the smartphone-keyboard typing service [65, 66, 67, 68, 69].
3. Gait recognition: It identifies the user following how the user walks [70, 71, 72, 73, 74].
4. Behavioral profiling: This field focuses on creating a user profile based on network-based technology. It can include app usage and location services [75, 76, 77, 78, 79].
5. Hand-waving: This orientation centres on how the user holds, rotationally moves, waves or shakes their smartphone [80, 81, 82, 83, 84].

Significant surveys have covered behavioral approaches like Mahfouz et al. [85], Alzubaidi et al. [86], Bhatt et al. [87], and Abuhamad et al. [88]. In our criteria, all of them cover the state-of-the-art around the behavioral authentication oriented to smartphones.

On the other hand, physiological biometrics also involve structural (static-external) and hidden user traits. Structural biometrics examples are face, retina, iris, and fingerprint with a minimal template variance over time, and their employment is profoundly expanded to more than just smartphones [89]. Hidden biometrics (HB) covers bio-signals such as Electroencephalography (EEG), Photoplethysmogram (PPG), and Electrocardiography (ECG), among others. Although these signals are used for health monitoring, different studies have found specific patterns among people which are suitable for verification approaches. We extend ECG hidden biometrics in section 5.

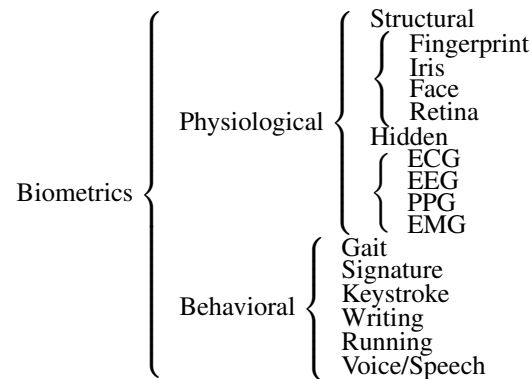


Figure 7: Biometric overview. Based on [90]

3.2 Current limitations

Smartphone biometric usage has increased in the last years in both market and research using different traits including behavioral, hidden, and physiological modalities. Biometrics mobile solutions gain trust between users [91]. However, it is advisable to know the features and scope of each technique, for instance, their weaknesses. In that sense, Table 2 provides a scope of different biometric characteristics, including evaluation score, the sensor used for signal acquisition, and the disadvantage column. The biometric score is a point of reference to understand the fulfillment of the biometric acquisition and processing engine. These values are the result of a series of tests in specific conditions evaluating the possible person verification states: genuine or impostor. The biometric engine evaluates the terms of probability represented within the parameters False Acceptance Rate (FAR), False Reject Rate (FRR),

and Equal Error Rate (EER). FAR counts the number of times a set of templates from a fake person is recognised by the system as an authentic one. Meanwhile, FRR counts the system rejection of the right user. Finally, EER is a performance indicator value of the process where FRR and FAR both meet, meaning the minimal and optimal point of the system. The letter $[x]$ in Table 2 means the absence of the category in the cited paper.

Each value such as accuracy, FAR, FRR, and EER correspond to a specific environmental condition that helps to reach the best classifying score. In that way, it is necessary to know the different variables that could interrupt, hinder, limit, condition, or decrease the trait evaluation. Some of these variables are in the last column in Table 2. For now, there is no unimodal fail-safe scheme covering all involved risks such as measurement quality, template reproduction, safe context, among others [20].

Another biometric trait comparison metrics suggested by different textbooks [22, 21] and experts [92], recommend the trait based categories described below: universality (people generality), distinctiveness (individually unique), permanence (stability), collectability (quantifiable), performance (recognition rate), acceptability (user comfort), and circumvention. These guidelines are in Table 3 based on authors' criteria [21] defining the qualification as high, medium, and low. Concerning hidden biometrics in Table 3, permanence column with a (pending) P mark, that assessment is to our criteria, due to missing long-term evaluation study [93, 94, 95].

Table 2: Evaluation of different biometric methods

Mod.	Biometric trait	Ref	EER(%)	Accuracy (%)	Frr (%)	Far (%)	Sensor	Disadvantage		
Behavioral	Voice	[96]	0.47	82.14	x	x	Microphone	Illness, ambient noise		
		[86]	15	x	x	x				
	Signature	[97]	6.2	x	x	x	Touch-sensor	Sensitive to friction		
		[98]	0.127	x	x	0.23				
	Gait	[99]	x	94.93	3.89	0	Accelerometer	Smartphone location, body injury, object carrying		
		[86]	7.3	86.3	x	x				
Hidden	ECG	[100]	0.87	96.2	x	x	Electrodes	Signal acquisition, usability, extend databases testing population		
		[101]	15	97	x	x				
	[102]	x	x	0.245	0.2475					
	[103]	x	81.6	x	x					
	PPG	[104]	x	96.1	x	x				
		[93]	[0.5-6]	x	x	x				
	EEG	[105]	x	100	x	x		Signal acquisition, usability, computational complexity		
		[106]	x	86.1	x	x				
Physiological	Face	[107]	x	x	x	1:1e6	Camera	Illumination, Power consumption, extra resource for liveness detection		
		[108]	x	90	x	x				
	Hand Geometry	[109]	0.3198	99	x	x				
		[110]	x	88.2	x	x				
	Iris	[111]	0.008	x	0.013	0.001				
		[112]	16.76	92.82	0.014	0				
	Retina	[113]	5.5	98.3	5	5				
		[21]	1:10e6	x	0.31	0.31				
	Fingerprint	[21]	2.07	x	x	x			FP-sensor	High exposition to be copied, situation awareness
		[21]	5	x	2	2				

In the following lines current acquisition methodology will be discussed. The first approach to classification is related to the kind of interaction between the user and the smartphone. That relationship can be a straight interaction or employing a propagation medium. While optical technology like cameras or sound sensors like microphones are examples of non-contact interaction, lock patterns focus on a straight contact with the touchscreen. In regards to camera and microphone performance, they are highly sensitive to the lack of light or noisy environments. Additionally, camera authentication in most cases,

Table 3: Biometric traits comparison according to identification requirements [22]

Biometric Technology	Universally	Distinctiveness	Permanence	Collectability	Performance	Acceptability	Circumvention
Voice	Medium	Low	Low	Medium	Low	High	High
Signature	Low	Low	Low	High	Low	High	High
Gait	Medium	Medium	Low	High	Medium	High	Medium
ECG*	High	Medium	Medium - P	High	High	Low	Low
EMG*	High	Low	Low - P	High	–	Low	Low
PPG*	High	Low	Medium - P	High	–	Low	Low
EEG*	High	High	High - P	High	High	Low	Low
Face	High	Low	Medium	High	Low	High	High
Hand Geometry	Medium	Medium	Medium	High	Medium	Medium	Medium
Iris	High	High	High	Medium	High	Low	Low
Retina	High	High	Medium	Medium	High	Low	Low
Fingerprint	Medium	High	High	Medium	High	Medium	Medium

requires the screen being on during the authentication process. For that reason, a mobile consumption description in Table 4 contains a list of smartphone components with their power estimation. This helps differentiate between the camera and display power [114]. Additionally, camera authentication needs a liveness-detection module with a minimal image quality that increases device price. Regarding the power description in Table 4, the camera consumes a large proportion of a device's battery, which is a disadvantage for consumers.

Table 4: Smartphone component consumption estimation. Based on [115]

Component	Consumption [mW]	%
Display	400	15%
Active cell radio	800	29%
Bluetooth	100	4%
Accelerometer	21	1%
Gyroscope	130	5%
Microphone	101	4%
GPS	176	6%
Camera, focusing and picture preview	1000	37%
Total	2728	100%

Regarding fingerprints, during the Mobile World Congress in 2016, the Chinese company Vkansee Technology Inc. experimented with iPhones supporting Touch ID recognition, debuting its authentication system with silicone clay and a piece of Play-Doh [116, 117]. Then, using a similar method with gelatin and Play-Doh, Goicoechea et al. managed to unlock five different smartphones working with people with no expertise in biometrics [19]. Moreover, there is another phenomenon involved with a fragmented fingerprint acquisition. In this case, the system took partial samples due to the small sensor size [18]. If the new partial sample matches with a stored partial sample, the unlocking process is approved. The risk in this scenario, owing to this partial acquisition, opens the possibility of other users of gaining a partial sample that could be similar to the owners'. Ray et al. evaluate this possible threat increasing the probability of failure acceptance when using additional finger samples of both hands to train the smartphone biometric model [18]. A further issue to deal with fingerprint technology is to validate the state of consciousness of the user prior to granting approval [16].

In the case of hidden biometrics, their advantage is the self-liveness-detection property, but they

contain several challenges to overcome, like acquisition and signal dynamics. For example, PPG being used in a daily living activity, needs an oximeter fixed steadily and its signal quality can depend on user's skin color. Another matter found in electrode-based HB is their sensor setup location since it demands a specific configuration to get an acceptable potential difference. As a consequence, placing the electrodes incorrectly will cause poor quality signal. As a matter of fact, ECG requires a mandatory configuration which is unattractive to most users. Besides, factors like humidity and muscle noise are highly demanding in the acquisition of these kinds of signals. The last challenge in the HB analysis is the signal fluctuation in relation to changes in posture and emotional state.

Another perspective for analyzing the verification phenomenon, is expanding how biometrics approaches human beings. Commonly, the user verification works in just one way to validate the user employing the unimodal approach. Admittedly, the physiological trait approach has been used as the preferred biometric validation. This approach is actually the most robust scheme implemented in smartphones. Nowadays, with the current sensors embedded in the smartphone or either with some external ones, it is possible to collect additional information. Also, it is expected that using them all together could help to improve the owner's verification process. Multimodal biometrics are an emerging option that could arguably enhance accuracy authentication by fusing different data according to the specific layer of work.

Taking into consideration company criteria in biometrics usage, NCC Group, a global expert in cyber-security and risk mitigation. Its technical director Matt Lewis commented that FRR is prioritized over FAR. Because, in case the system doubts the authenticity of the user, it would reject them temporary instead of granting access to an unknown one [107]. One particular example is Apple, upon checking the Face ID Security Guide they only provide FAR values for Face ID (1:1000000) and Touch ID (1:50000) [118]. Lewis proposed three security range measurements based on FAR values: 1:100 as low security, 1:10000 as medium security, and the highest security range as 1:1000000. Another principle is user acceptability. This aspect is bounded by user-experience and the time of the requested procedure. For example, the duration ranges for some code-based lock are: simple sequence pattern lock: $1.336s \pm 0.286s$, for a complex pattern: $2.313s \pm 0.420s$, and for a 4-digit PIN: $1.015s \pm 0.183s$ [10].

With the previous background (section 1-2-3), the smartphone authentication atmosphere is reachable. As we stated in section 1, the forwarding approaches (section 4-5) do not claim the place of smartphone owner recognition through fingerprint, face, voice or iris. Unlike mobile-biometric orientation it is robust, usable, reliable, scalable, but not perfect as mentioned in section 3. The authors are aware of the existing authentication gaps and view this situation as an opportunity to put forward the development of authentication engines that could overcome some of the current weaknesses. The next sections will present two emerging ways that can be implemented with current resources (section 4), or which still need to be inside the research field (section 5). The next two chapters include the introduction, current limitations, specific acquisition concerns and improvement proposals oriented to pattern lock, and ECG.

4 Authentication with Pattern Lock

4.1 Introduction

Knowledge-based authentication focuses on learning a personal text or code as a key to protect owner's data. Nowadays, this secret data-sequence input is user-supplied through the touchscreen with famous mechanisms like pattern-lock, PIN, and password. Text-based passwords enhance in strength as the character length increases, but human memory is limited, and people likely forget complicated passwords in the short-term. Moreover, regular long-text entries require more user interaction, increasing the digital friction usage. The typical user solution is to handle a short code that allows fast access but reduces the key strength. Indeed, 60% of North Americans do not have the habit of updating their passwords [119]

and their codes are short and not frequently updated. An example of low-strength passwords is the Chinese case in 2011, in which there were 100 million hacked accounts containing emails, usernames, and passwords [120]. Following this, Lin et al. studied password creation habits in China and found common characteristics like re-used passwords, birthdates of relatives, daily-usage words, personal information, and culturally common numerical sequences. Within the context of smartphones, the eavesdropping PIN code attack is an effective method as it is only necessary to learn four digits. According to Americans and Cybersecurity research, 35% of US citizens use PIN codes [119] and the smartphone unlocking risk increases up to 28%, with Americans that do not lock their smartphones.

To facilitate this memory issue with text-based and PIN lock methods, graphical passwords emerged. This change is based on the dual-code theory that suggests that there are two analysis components that exist in the brain, a verbal one and a non-verbal one. Drawing an image is easier for the brain than memorizing an alphanumeric code as there is no interpretation step in the middle [121]. The touch pattern was introduced in 2008 by Android, and according to Sun et al., by 2014 there have been few studies addressing their weaknesses [122]. Usually, the pattern is in the path `/data/system` with the name `gesture.key` turned in an SHA-1 key sequence [123].

The standard pattern lock is generally made up of nine nodes (Figure 8), connections, intersections, and overlaps. The visual code strength must face factors like user memorability, number of connections, input convenience, and privacy needs [122]. In short, an acceptable solid pattern must fulfill the following rules:

- The drawing must be continuous and should contain at least four dots.
- Each node can be connected just once.
- Straight lines should include middle dots [124].
- The pattern can be over a busy node but is not counted as a valid connection.

While the first rule applies for a minimal strength, the other rules eliminate ambiguity in the drawing [125].

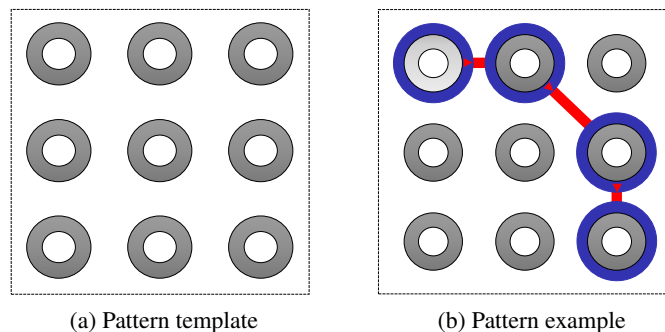


Figure 8: Pattern lock

Pi et al. calculates the total number of possible patterns to be 389,112 [126]. Lee et al. concluded that a total of $9.86e+5$ and $3.6e13$ is the number of visible nodes that can be reached by a point with patterns for 3x3 and 4x4 grids [127]. In 2013, researchers at the University of Notre Dame performed a predilection survey ($n = 150$) regarding smartphone unlocking methods. They found that approximately 51% of the sample population used pattern-lock, 14% used text lock, and 35% did not lock their smartphone at all [128]. Another poll with 8,286 participants that included eight countries (Australia, Canada, Germany, Italy, Japan, the Netherlands, the United States and the United Kingdom) found that 32%

of people proceeded to unlock the smartphone with pattern-lock, 32.1% with slide unlock, and 18.7% with PIN [129]. The same survey found that pattern-lock was the most popular unlocking method with 48% of participants using this method. Finally, analyzing different drawing sequence with 506 participants, 41.1% start the pattern in the top-left node and 20% finish in the bottom right node according to Zezschwitz et al. [130].

Looking for ways to assess the pattern-lock power, Uellenbeck et al. [125] were the first to study a strength metric oriented to the information theory, calculating the sequence entropy in 9.1 bits. Zezschwitz et al., through the Kolmogorov similarity, measured the strength among geometrical shapes, regardless of the orientation. Similarly, Sun et al. proposed a pattern-lock, entropy-based strength real-time visual indicator [122]. This score level is carried out with the next categories: size, physical length, number of intersection points and number of overlaps; all of them are criteria to perform equation 1.

$$P_{entropy} = \#dots + \log_2(\text{length}_{physical} + \#intersection + \#overlaps) \quad (1)$$

4.2 Current limitations

The previous subsection tackled categories like pattern-lock complexity and memorability; those are internal or user-related issues. In contrast, this section address external or intentional breach intrusion by an impostor. The main strategies for obtaining the pattern lock sequence are: smudge attacks, shoulder surfing, and side channel. The smudge vulnerability is due to oil remnants on the smartphone screen after finger swiping contact [131]. It becomes an attack when someone uses the oil remnants to guess the pattern, as can be seen in figure 9a.

The second attack is shoulder surfing; it is when a person or camera [132] close to the user to watch and learn the password [133]. The side-channel technique is another attack that is a type of reverse engineering that uses an external computational system to exploit the entity to attack[134]. Aviv et al. introduced a study about the side-channel, considering only the usage of the smartphones' accelerometer [135]. Using touch-related events to synchronize the software engine and collecting the accelerometer data in an uncontrolled condition, the model can predict the original pattern with a 40% of accuracy [135]. This study supports the importance of controlled access to the sensor layer and suggests suspending the sensor data exposure during sensitive operations. Another side-channel study by Zhang described a new way to predict sequences called wireless sniffing, which consists of measuring and detecting how the signal changes while the user draws their pattern-lock [136]. A further experiment proposed by Andriotis et al. describes using an optical camera and microscope looking for oil traces [121] as an additional way to perform a side-channel pattern detection. They used a thermal camera to analyze the heat distribution to determine the pattern, as illustrated in Figure 9b. In the second part of experiment of Andriotis et al.'s experiment, a psychological survey extracted the user's preferences and merged the results with the accelerometer data. Both the sensor and the survey data were used to infer several pieces of the pattern [121].

Another attack is by brute force. The modus operandi is to input every possible combination of designs until it lands upon the owner's sequence. One brute-force approach proposed by Pi et al. has a GPU parallel thread modelling with an adjacent matrix and Hamiltonian Path problem to break the pattern [126]. Their break-time with the maximum number of nodes is 170 ms, as shown in table 5, and contains the relationship between dots, threads, and breaking off time.

In conclusion, obtaining the owner's lock pattern is possible through the different attacks highlighted in this section. These risks are an open gate to the data privacy exposure because once the secret code is known, the user data and their privacy are uncovered. Due to this weakness, different modifications have been evaluated and the habitude pattern-lock proposal (HPL) has been developed, like alternatives to enhance this system (section 4.4.2), joining behavioral biometric during the trace. One kind of data ac-

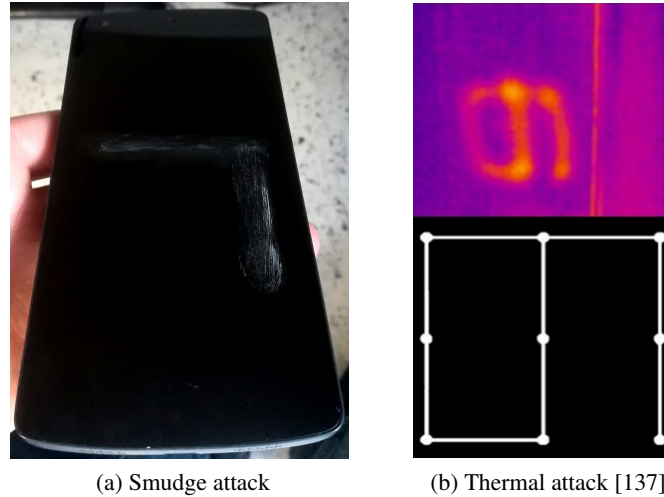


Figure 9: Example of pattern lock attacks

Table 5: Brute-force algorithm performance [126].

# of dots	# of threads	time [ms]
4	512	0.076
5	4,096	0.086
6	32,768	0.349
7	262,144	2.596
8	2,097,152	21.139
9	no-report	171.794

quisition in HPL is the between node drawing time. Consequently, the next section will discuss particular acquisition concerns to obtain the best precision in collecting time-based measures.

4.3 Specific acquisition concerns

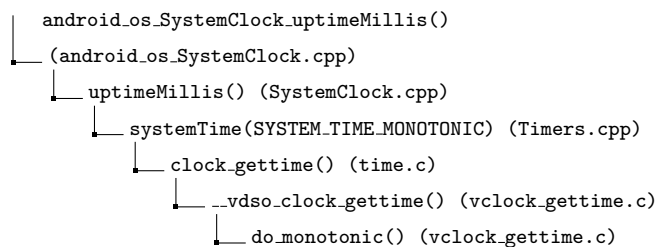
Throughout the pattern-lock entrance, each connection time between nodes is stored with labelled timestamps following a sampling rate. Each touch on a new dot is the synchronization mark for the analysis model. Although different operating systems have its epoch [138], the most famous timestamp is the Unix format which counts the number of seconds since January 1, 1970 (midnight UTC/GMT). Overall, the point of reference for examining the time passed is with the clocking options in any embedded system. According to the android.os package, the SystemClock class [139] contains three clocks:

- `System.currentTimeMillis()`: This expresses the time in milliseconds and can be configured by both mobile network or user. The time count can change unpredictably with leaps forward or backwards, depending on who updates it.
- `uptimeMillis()`: This counts in milliseconds from the time that the system is booted until the system goes into deep sleep mode. Usually, it is used in interval timing such as `thread.sleep`, `object.wait` and `system.nanoTime()`. However, we recommend using it when the routine interval execution is less than the deep-sleep time interlude. Unlike the `currentTimeMillis` method, the clock that guides `uptimeMillis` is monotonic.
- `elapsedRealtime()`: With their couple partner function `elapsedRealTimeNanos()` return the time

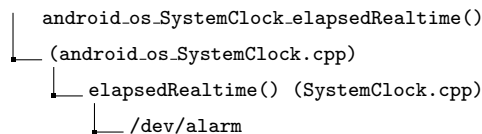
since the system was booted. Both counts even if the system enters in low-power mode. The oscillator that leads the count of `elapsedRealtime/Nanos` is monotonic. Finally, Android recommends this clocking scheme for interval timing purposes.

The functions, `currentTimeMillis`, `uptimeMillis`, `elapsedRealtime` are not constructed in Java; in consequence, they use the reference *native* for Java Native Interface [140], indicating that this function runs in another language. In this case, the functions run with C++ in a lower-layer scheme in the file `android_os_SystemClock.cpp`. With that design, it is expected for Java to reach an OS resource with a critical time response. By timing function, the next tree-kind references show the service calling chain with their containing file [141].

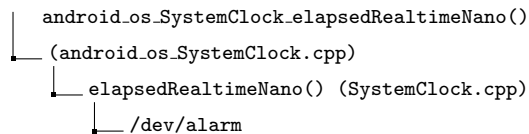
- `uptimeMillis()`:



- `elapsedRealtime()`:



- `elapsedRealtimeNano()`:



Among the different clocks available in Android, the least accurate is `currentTimeMillis` due to its unpredictable change in time. Regarding `uptimeMillis` and `elapsedRealtime/Nanos`, the Android literature affirms their monotonic behavior [139]; indeed, the Linux programming textbook confirms the monotonic clock behavior as being strongly trustworthy [142]. A steady oscillator possesses linear increments and allows a reliable counting since booting time (Android case), assuring a deterministic operation. Quote verbatim: *The important aspect of a monotonic time source is not the current value but the guarantee that the time source is strictly linearly increasing and thus useful for calculating the difference in time between two samplings* [142]. In summary, the accuracy in `uptimeMillis` and `elapsedRealtime` timing is guaranteed.

There is an extra factor to take into account regarding timing accuracy expectations during a function invocation. Linux and Android are not real-time operating systems [143, 144]; therefore, they are not deterministic. Non-RTOS (Android case) involves the function call procedure in Java; consequently, it gets a delay between the execution method and the returning value. Evaluating this OS nature, a test is performed with the Android smartphone ASUS ZenfoneGo 2 that contains a processor Snapdragon 200 Quad-Core 1.2GHz and 1GB of RAM. The experiment consists of evaluating the execution time response of `uptimeMillis()` and `elapsedRealTimeNanos()` including their mean and standard deviation.

Per function, the experiment is executed 100 times, getting the results presented in table 6; both services differ sharply in their std. In conclusion, the best timestamp is with `elapsedRealtimeNanos` on applications involved in continuous and pervasive authentication from the authors' concept. In contrast, timing extraction involved in one-shot and transparent authentication for pattern-lock, both `uptimeMillis` and `elapsedRealtime`, are useful Android methods.

Table 6: Function executing time

Function	mean time [ns]	σ [ns]
<code>uptimeMillis</code>	9847.63	5388.9
<code>elapsedRealtimeNanos</code>	10157.6	886.67

4.4 Improvement proposals

4.4.1 Pattern lock modifications

Pattern-lock weaknesses have favored different improvement proposals; in this subsection, a brief shape-based suggestion is covered. `TinyLock`, [145] created by Kwon et al., aims to prevent the smudge attack by reducing the distance between nodes without altering the operation time significantly compared to the usual matrix size. In this case, the finger can cover much of the area of interest, avoiding a clear pattern of smudges. Also, it includes the option to rotate the finger directly over the grid, deleting all traces of the smudge pattern.

For its part, Colley et al.'s methodology is focused on allowing already selected-nodes to break the one-usage node rule with the use of sequential duplication and time-based duplication. Accordingly, the dot permutation raises the pattern possibilities [146]. Instead, Lacharme et al. [147] synchronize an OTP using the pattern as the seed for a bio-hashing pseudo-random code generation.

As another option, Xiong et al. proposes discarding the use of some nodes randomly and changing the layout interface; as a result, this platform presents a system entropy increment [148]. Guerar et al. considers clicking as an alternative instead of swiping the pattern to bypass the smudge attack [10]. In this scheme, each dot in the application contains a row randomly numbered from 1 through 9 in the screen bottom-side. Then, the user selects the numeric sequence related to the pattern and it also has the option to turn numbers into colors, limiting eavesdropping.

4.4.2 Habitude pattern lock

This sections turns the sight to implement the pattern lock validation regarding user habits instead of extending the philosophy of memory-based key (Figure 10). The `Habitude` pattern lock seeks to join the knowledge of the pattern sequence with the evaluation of the user device interaction, creating a behavioral model with the data provided by the smartphone sensors. Citing for a while the behavior orientations in section 3.1, HPL belongs to gesture dynamics due to the hand-drawn form on the touchscreen, containing sequences of numerical coordinates. It consists of checking the user authenticity through its interaction with the device analyzing movement patterns. This kind of evaluation has been previously analyzed in typing. For instance, Schweitzer et al. used visualization techniques and studied custom practices during password input by keyboard and categorized them. They found common elements without using a dictionary attack [149]. Similarly, Frank et al. [150] dealt with touchscreen behavioral biometrics, using 30 features from movements like up-down and left-right getting an equal error rate less than 4% one week after the intra-session phase. Their test was with k-nearest neighbours (k-NN) and Support Vector Machines (SVM) implemented over 41 people.

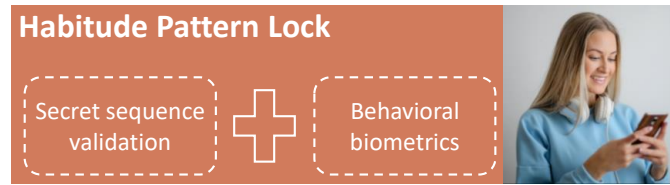


Figure 10: Habitude Pattern Lock

The next paragraphs address different contributions from authors that have had a close up extracting movement-user-features during their pattern-lock draw. One of them is Alpar [151]. He analyzed a four-node pattern measuring the touch-time by each dot as feature-set, creating a visual and a ghost password. Due to this, the classification was conducted with artificial neural networks, adaptive neuro-fuzzy inference and RGB histogram, getting an EER of 8.75%, 2.5%, and 7.5% [151]. On the other hand, Luo et al. with ten subjects, discriminated each one primarily with the embedded pressure sensor data, including x/y coordinates and time [152].

Equally important, an alternative input parameter with two fingers is proposed by Meng et al. [124] to achieve the pattern trace by reusing each dot expanding, the complexity. Then, with the use of an app developed in Android CyanogenMod, they extracted the touch timing, x/y coordinates, slide-down/slide-up inputs, and pressure values. Furthermore, the comfortability score was implemented with a survey where the users confirmed that pattern input was not as tricky, preferring a multi-touch option over the classical drawing. By the same token, De Luca et al. executed a long-term scheme in laboratory conditions outside without informing the users about the implicit verification, assuring natural conditions throughout pattern entering [61]. Afterwards, with 31 subjects, the attributes extracted were: XY-coordinates, pressure, size, time, and speed. Additionally, it was found that users who were informed about stroke-line analysis got better results. Alpar et al. [153] sought to configure the user identification from the distance and angle formed between the touched-node section and the operating-node central coordinate. The patterns were simulated in Matlab and classified with ANN and weight-optimized with Gauss-Newton and Levenberg-Marquardt. The score for LM was: {FAR=0% FRR 7.5%} and GM was: {FAR=22.5% FRR=0%}. They considered the epoch's number as a restriction to get a better classifier. On the other hand, Wajeeh et al. used singular value decomposition of the feature matrix composed of node timing, pressure, and finger area [154]. After that, the eigenvalues of eight subject samples were evaluated, getting an accuracy of 92.27% compared to the Naive Bayes approach with 76.16%.

Li et al. compared the use of pattern-lock and PIN-code using a smartphone and a tablet to obtain the user and device interactional attributes [155]. Then, with 16 individuals implementing DTW (Dynamic Time Warping) and Histogram approaches, they found that the Histogram method can stand aging templates better than DTW. Unfortunately, they do not evaluate memory and computational complexity. In contrast, Beton et al. separated samples of intra-class and inter-class entry attempts and evaluated the authentication with ten people through the Pearson Correlation coefficient and DTW [156]. Each technique performed an EER of 36% and 28%; then, fusing X and Y positions with time-based features obtained an EER of 17%.

Another proposal is a sequential scheme composed of phone angle, pattern shape, and drawing time suggested by Agrawal et al. [157]. In this study, the accuracy was between 60% and 95% with 20 individuals. Instead of the nine nodes grid, Ganesh et al. suggested a pentagon with ten dots that included the orientation and pressure data [158]. Besides, each node contained an associated number-label which changed its position after each new unlock. Then, with a set of fuzzy rules, the user-identification analysis was performed. A different strategy proposed by Liu et al. recommended adding orientation and acceleration sensor statistics [159]. After that, they classified the user posture with K-means reaching

an FAR of 4.36% and FRR of 5.03%. Then, with the identified posture (standing, sitting, and lying), they created a pattern drawing sample user-identification SVM model. Similarly, Nohara et al. used acceleration and angular velocity to differentiate by axis among touch, release, and distance attributes, with all seventeen attributes from the pattern trace [160]. Commonly, data processing was performed locally. However, their classification computing was achieved since the server-side, using self-organized maps for user-verification. This cloud-orientation is given when hard data processing is needed to save the smartphone [161].

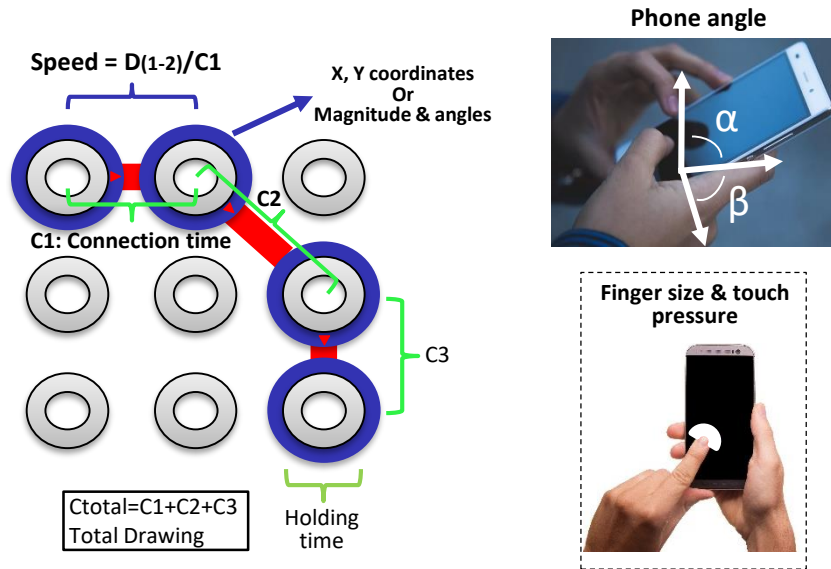


Figure 11: Lock pattern behavioral features. Photos from [162, 163]

For a general understanding of the information given in this section, Table 7 presents a summary of the papers related to pattern-lock current work. Then, considering state-of-the-art in the features linked with the user-dynamics during the pattern-lock trace, we generalize and cluster the values extracted composed of 5 data-sets: time, pressure, area, IMU and distance. In summation, the attributes extracted are: Pressure, holding time, finger-area size, movement, orientation, finger orientation, accelerometer, angular velocity (gyroscope), pressed-nodes location, inter-node time, and the phone waving model through pattern input. A graphic compilation of these attributes-sets is in Figure 11. Finally, Table 8 presents, with the five categories proposed separated by columns, a group of studies that implemented different dynamical-user-trace features during their investigations.

From this table, with an initial glance at the firsts four rows, we can conclude the predominance of time-based data. Likewise, from the fifth row until the end, there is a frequent relationship presence between pressure and finger area. Moreover, from the sixth row until the ninth, including the work of Agrawal et al. [157], there appears a new group that uses the IMU sensor. That category covers 45% of the presence in Table 8, followed by the distance-based category with 54%. Overall, in the work relayed in Table 8, the number of subjects does not exceed forty people; indeed, the best EER = 1.8% worked with 15 individuals [159]. To conclude, an optional option to validate future implementations is joining the different attributes of Figure 11. That fusion scheme can be evaluated by any of the next strategies: sensor-level, feature-level, with dynamic classifier selection, match-score level, and decision-level. This option assesses the discrimination capacity, choosing the best combination and enhancing this classic unlock system.

Table 7: Pattern lock related work

Ref	Sample	Focus	Feature	Technique	Performance
[10]	51	Alternative drawing		Slide and random numeration	Time evaluation GM: FAR=22.5%
[151]		Authentication	Distance-Angles	Gauss-Newton; Levenberg-Marquardt	FRR=0% LM: FAR=0% FRR 7.5%
[157]	20	Authentication	Sequential: Phone angle, pattern, drawing time.	Do not say	[60-95]%
[128]	197	Behavioral	Amount of data, #sms, screen lock method, surveys.	Surveys and statistics	
[160]		Behavioral flicks	Acceleration, angular acceleration, distance, time=17.	SOM	N/A
[61]	31	Behavioral pattern	Pressure, xy coordinates, size (finger area), time, speed (time btwn 2 coordinates).	DTW	77%
[151]	35	Behavioral pattern	Touching nodes duration and connection time.	ANN; ANFIS; RGB Histogram	EER ANN: 8.75% ANFIS: 2.5% RGB: 7.5%
[156]	10	Behavioral pattern	x-y position, point position, time inside the node, time between nodes.	Correlation; DTW	EER Corr: 36% DTW: 28% Fusion: 17%
[158]		Behavioral pattern	Pattern shape, 3-axis orientation, pressure.	fuzzy if-then rule	
[154]		Behavioral pattern	Timing, finger pressure and area of finger pressure.	SVD	92.27 %
[159]	20	Behavioral pattern	11: Posture features 39: gesture feature based on x-y position, pressure, size, timestamp, 3-axis acceleration and orientation.	K-means	FAR = 4.36% FRR = 5.03%
[155]	15	Behavioral pattern; PIN	24 = x-y coordinates-magnitude-angle, pressure, size, 3-axis accelerometer, 3-axis angular acceleration and derivatives.	DTW; histogram	EER= 1.8;7.5
[147]	34	Biohashing; behavioral pattern	Pressure, x-y position, fingersize, tilt.	Hamming distance	Estimated EER=0%
[126]		Brute force		Hamiltonian Path problem	170 mS
[124]	45	Multitouch	Touch timing, x and y coordinates, press down and press up inputs and pressure.		Survey

Continued on next page

Table 7: Pattern lock related work

Ref	Sample	Focus	Feature	Technique	Performance
[146]	36	Node multiple inclusion.	Size: Dots number connected		
[122]	81	Pattern strength	physical length (min 1) # overlaps # intersections		
[132]	215	Shoulder surfing		Video	simple pattern: 60% complex: 87.5%
[135]	24	Side Channel	776= 3x3x86 [STATS (6), 3D-Poly-Deg (4), 3D-Poly-STATS (6), iFFT-Poly (35), iFFT-Acc (35)]	Logistics regression; HMM	40%
[121]		Smudge attacks		Thermal and optical camera	
[125]	584	Strength analysis		Entropy	
[130]	496	Strength analysis		Kolmogorov Similarity	
[164]	32	Time - Specific Patterns	6 fingers-in-dot; 5 finger-in-btwn-dots;	Random Forest	EER = 10.39% std = 3%

Table 8: HPL features compilation

Ref	Holding time	Connection time (C.T.)	Total C.T.	Pressure	3-axis	ACCLRM	Orientation	Finger area	Pixel distance	X,Y COORD	Velocity	MAG, Angle	Best evaluation	Technique	Sample
Agrawal2014			✓				△						Accy = [60-95]%	ANN; ANFIS; RGB	20
Alpar2015	✓	✓											EER = 2.5%	ANFIS	
Angulo2012	✓	✓											EER = 10.39% ± 3%	Random Forest	32
Beton2013	✓	✓											EER = 17%	Fusion: {DTW, Corr}	10
DeLuca2012		✓		▽				⊙		□	□		Accy = 77%	DTW	31
Ganesh2017				▽			△						Training Accy = 95%	Fuzzy	NR
Li2015				▽	△	△	⊙			□		□	EER = 1.8%	DTW	15
Liu2016		✓		▽	△	△	⊙			□			FAR = 4.36% FRR = 5.03%	k-means	20
Nohara2016			✓		△	△			□				Do not say	SOM	NR
Malek2006				▽								□	Accy = 92%	k-NN	37
Wajeeh2015		✓		▽			⊙						Accy = 92.27%	SVD	NR

✓ Time-based ▽ Pressure △ IMU-based ⊙ Finger area □ Distance based

5 Authentication with ECG

5.1 Introduction

Hidden biometrics (HB) is an emerging area that works with signals produced consistently by the human body. They must fulfill biometric requirements such as universality, uniqueness, and measurability. One important signal in HB is the electrocardiogram (ECG). This wave is generated by following the electrical activity of the heart through the use of electrodes, which are metal or gel pads, that make contact with the skin. The concept of difference in electrical potential is the foundation of ECG acquisition. The heart is a muscle, and each heartbeat produces an electrical current over the skin, which is captured by the conductive section of the electrode. To begin the measurement only requires a minimum of two electrodes in a function that involves time and voltage variation. The simplest connections are depicted in Figure 12.

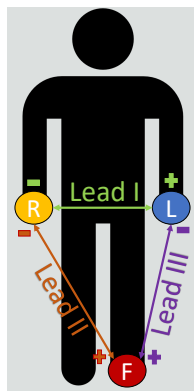


Figure 12: Bipolar Limb Leads

Lead I captures the signal between the points L and R, Lead II from F to R, and Lead III from F to L, taking into account the Einthoven triangle approach. Each heartbeat is the raw material to be evaluated, thereby, the elementary ECG signal analysis starts with the point of interest regions called fiducials. These peaks have the labels P, Q, R, S, and T, as Figure 13 shows. The Pan-Tompkins algorithm developed in 1985 is a well-known procedure to perform the fiducials search [165]. Real-time ECG-oriented applications implement this routine, achieving a $99.79\% \pm 0.34$ of sensitivity [166].

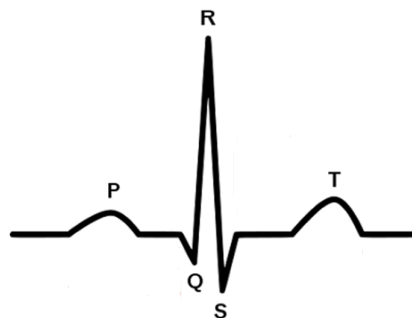


Figure 13: Fiducial PQRST. Based on [167]

A comprehensive study related to the ECG signal focuses on observing heart behavior and following cardiac abnormalities. In past years, newer ECG-related applications have emerged and have been implemented for cryptography [168], gender recognition [90], and biometrics [169], such as an option for

smartphone unlocking [90].

During the ECG study in this section, three aspects need to be covered. First, the possible features for which ECG authentication may be utilized as an emerging technology for smartphone authentication. Second, addressing some current applications that use ECG authentication in the context of smartphones. Third, current limitations, specific acquisition concerns, and improvement proposals for ECG as a biometric trait.

5.2 Motivation

ECG authentication, as it has potential to be ubiquitous, is appropriate for the Biometrics of Things applied in Smartphones. Additionally, ECG poses as an implicit liveness detection property. This promising smartphone authentication field could be used in continuous, transparent, or one-shot related schemes. Moreover, ECG signal reproduction is impossible to be suppressed by the user as those movements are involuntary. Nonetheless, the user may alter the signal cadence consciously or unconsciously given the daily activity dynamics, but that does not interrupt their generation. Each ECG-ROI poses a non-negligible variability as a challenge to overcome, especially for the classification training phase. But, this behavior simultaneously enriches the captured signal information, rendering it difficult to replicate. Between these sets of issues, the most challenging are the user sensor comfortability, computational complexity, and signal time acquisition. These demanding criteria, particularly the sensor ubiquity over the user's body, nowadays make the development of this technology non drop-down, advancing at a slow pace. However, once it overcomes these difficulties, ECG smartphone authentication may become a powerful biometric tool because in practice, ECG spoofing would require direct contact with the user's body, which renders this technique quite difficult to be hacked.

Independent of the processing unit (i.e., smartphone), during the last years, ECG focus on authentication has demonstrated an exciting evolution. Since Biel et al. started this research field [169], different approaches of evaluation have emerged. Among the conventional methods of evaluation are correlation [170, 171] and machine learning approaches such as Bayesian Networks (BN) [172], Neural Networks (ANN) [173], k-nearest neighbors (KNN) [174], Naive Bayes (NB) [175], Support vector machines (SVM) [176, 177], and deep learning [178]. Some examples of features to extract from heartbeats are the temporal or amplitude distance between distinct fiducials. Also, another set of possible attributes can be the application of space transformations like Fourier, Wavelet, Hilbert, among others. With these stack of values, a feature vector can be described.

There are noteworthy surveys that have dealt with ECG authentication, like the one proposed by Fratini [100], Agrafioti [179], Tantawi [180], and Pinto [181]. However, a common problem in ECG is the unbalanced comparison between most of researchers models with other classifiers. It happens because each work creates its own descriptor set and model, but the discrimination score is not widely contrasted. Cabra et al. [90] point out this problem and evaluate the same feature vector with 19 classifiers, including the model complexity variable estimation.

5.3 Ongoing research and products

This section tackles advances in ECG smartphone authentication oriented to both fields, research and market. The different set of investigations in Table 9 explore different approaches applied to mobile ECG authentication. From the hardware perspective, Cherupally et al. [182] and Yin et al. [183] develop a chip dedicated to user verification, that also includes acquisition, filtering, and a compressed neural network processing. Also, their chips achieve a power consumption of $62.37 \mu W$ [182] and $50.4 \mu W$ [183], a great advantage compared with $31.75 mW$ [184] with a implementation over a FPGA with a similar ECG chip solution.

Arteaga-Falconi et al. performed a low weight algorithm that uses a fiducial-based measure, classifying their user template with a hierarchical rule procedure [185], testing it with MIT/BIH and own measures. On the other hand, for prototypes creation and testing, Kang et al. [186] implemented a wristband and Chen et al. [187] a finger acquisition user validator, both with interesting approaches, using Lead I measure for their ECG authentication.

The studies in Table 9 include their databases capabilities and experiment variable design. These investigations demonstrate, that categories like silicon integration, power consumption, algorithms optimization, classification performance, and signal analysis could be integrated into a smartphone that has not been built yet.

Table 9: Mobile-related ECG authentication studies

Author	Year	Evaluation	Data source	Subjects number	Technique	Description
[182]	2020	EER %: ->1.36 (8X NNc) ->1.21 (4X NNc)	9 different Databases	741	Compressed ANN	->Hardware processor ->NN compression (NNc)
[183]	2017	EER %: 2.18	Database ECG-ID& in-house	645	Compressed ANN	Hardware processor
[184]	2015	EER %: 0.058	Database ECG-ID	90	Deep Learning	FPGA
[185]	2016	->TAR: 84.93% FAR: 1.29% ->TAR: 81.82% FAR: 1.41%	->MIT/BIH DB ->Own lead I acquisition	->76 ->10	Fiducial-based hierarchical scheme	Low weight algorithm for mobile devices
[186]	2016	FAR: 5.2% FRR: 1.9%	Own lead I acquisition	28	Non-fiducial-based degree of similarity	Wristband prototype
[187]	2017	FAR<10% FRR<10%	Own lead I acquisition	50	ANN	Handheld device prototype

One more category to consider is the electrode location. As the limbs used for smartphone usage are the hands (Figure 12), Lead I configuration was chosen for this kind of technology. Similarly, in terms of the comfort variable, Lead I is the most appropriate as confirmed by prototypes [186, 187]. This situation, with the current sensor technology available and variables considered, limits the mechanisms available to employ (Section 2.2). Continuous authentication requires a constant contact with the electrodes, and transparent connection needs the fingers free to face the implicit challenge. In consequence, those mechanisms can not be applicable for now. Therefore, supported by portable and wearable devices, one-shot related mechanism or challenge-based authentication are deployable and feasible methods for smartphone unlocking.

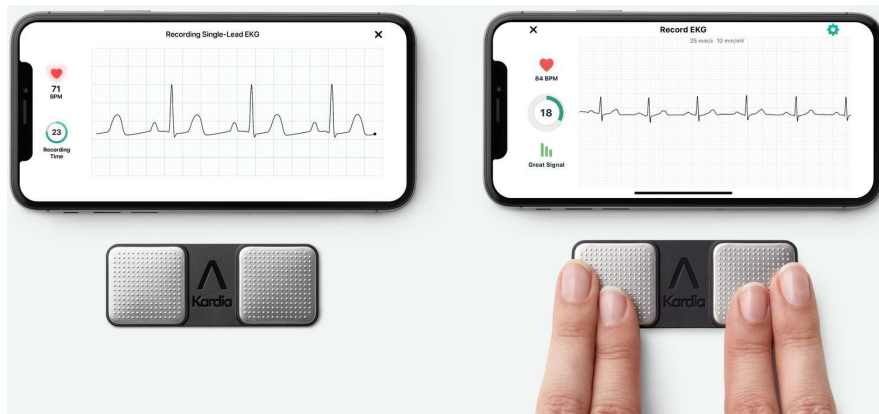


Figure 14: KardiaMobile - AliveCor [188]

There are different companies that have implemented their mobiles ECG services, overcoming the acquisition challenge and taking strong steps for direct communication with the smartphone through wearable or external accessories. For example, KardiaMobile (Figure 14) offers services of portable heart monitoring, approved by the FDA. KardiaMobile is based on HW and Machine Learning services and can detect heart abnormalities like arrhythmias and atrial fibrillation among others. It is compatible with Android and iOS smartphones; indeed, it has been tested as an acquisition instrument for mobile ECG user verification [185]. In addition, this device offers portability because of its size and weight, including a phone clip to attach to the back side of the smartphone (Figure 15). More details about KardiaMobile are in Table 10. AliveCor reported sales over 1 million units of KardiaMobile and funding of USD \$65 million by the Series E Financing in November 2020, including investors like Qualcomm Ventures and OMRON among others [189, 190].



Figure 15: KardiaMobile portable option [188]

Table 10: KardiaMobile specs [188]

Product	Price [USD]	Features	Photo
KardiaMobile	79	1.) Dimensions : 8.2 cm x 3.2 cm x 0.35 cm Two 3 cm x 3 cm stainless steel electrodes 2.) Weight: 18 grams 3.) Power: 3V CR2016 coin cell battery 200 hours operational time 12 months typical use 4.) EKG Characteristics: Single Lead ECG 10 mV peak-to-peak input dynamic range 300 samples per second sampling rate 16 bit resolution	

”Your Heart is smarter than you think” is the slogan of CardioID, a company with strong research background. With the goal to reduce road accidents, they provide Cardiowheel, (Figure 16) ”an Advanced Driver Assistance System that acquires the electrocardiogram (ECG) from the driver’s hands to continuously detect drowsiness, cardiac health problems, and biometric identity recognition”[191]. If an anomaly is detected, an alert emerges. Cardiowheel acquires the ECG signal during the driver’s journey through a cover over the wheel, also measuring the road attention (wheel hands-on) and fatigue status during the journey. The collected information is directed to the cloud for data aggregation analysis, which is reported via the central station on the dashboard. Their close partners have been Bosh and CEiiA. Likewise, CardioID requests Intellectual Property in Portugal, Japan, Korea, USA, among other countries.

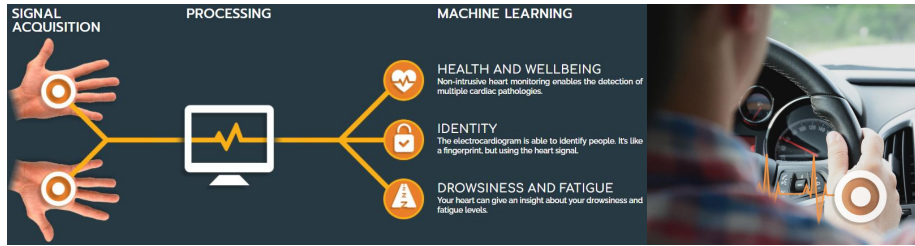


Figure 16: CardioID working sequence [191]

Extending CardioID person identification philosophy and technology (Figure 17), CardioID into their Internet of Things business line, propose that any object can be virtually reachable with their heart sensing technology, including smartphones [191], sports (Bikeyourheart), or gaming controllers. Coupled with it, sensors over the keyboard wristpad in critical office facilities monitor employees’ heart identification and fatigue condition classification, a valuable tool to reduce work accidents.



Figure 17: CardioID methodology in other contexts [191]

NYMI is a company from the University of Toronto that works with portable ECG authentication technology. NYMI has facilitated Lead I acquisition with their wristband design. The first electrode is on the back of the case, allowing for direct contact with the upper-side of the wrist. The second electrode is over the case and is activated when the user touches it with a finger of the opposite hand (one-shot mechanism).




Figure 18: NYMI Band [192]

The NYMI band can be linked with a smartphone through the NYMI app allowing unlocking service [193]. However, this service has increased to be used in access control in working environments. The NYMI band procedure starts by wearing the band for an on-body detection that includes both ECG

and fingerprint authentication (Figure 18). As a consequence, the session remains active until the user removes the band. Nevertheless, NYMI proposes a traceability environment solution connected with the entire company network. Taking advantage of the NFC tag also embedded in the NYMI band, that provides an object-based scheme to trigger local events. This NFC authentication allows activation of elevators, locked doors, computer session access, ping identity (company permission for information and applications), digital signature (i.e. turning on specialized machines), and bluetooth within range of presence recognition. More details about the NYMI band are presented in Table 11. Currently, NYMI's Technology Partner Program includes around 100+ companies like SAP, Intel, Siemens, ARM among others.

Table 11: Nymi specs [192]

Product	Price [USD]	Features	Photo
Nymi	199 [194]	1.) Biometric sensors: Fingerprint, ECG 2.) Secure Bluetooth Low Energy (BLE 4.2) 3.) Secure Near-Field Communication (NFC) 4.) Secure Credentials: FIDO2, FIDO (U2F), PIV, Nymi PKI, HID Seos 5.) Protection Ingress Ratings: IP66 & IP67 6.) Power: 3+ day battery life 7.) OLED monochrome display (48 x 64 px) 8.) Compliance: FCC, CE, IC, MIC, CMIIT, IMDA	

5.4 Current limitations

ECG user authentication is still a growing area that contains several challenges to overcome. One is the study of the signal variability due to body position. In this situation, a robust classifier would need a sharp detail in the enrollment phase due to the need to capture the distinct moments when the heartbeat rhythm changes. In this sense, Porée et al. find the standing position ECG-samples as an average position with the potential to cover the changing shape present in other postures [195]. Another approach seeks to estimate first the current posture and then apply a specific verification model; this approximation is extended in section 5.6.

A further open topic is to determine a proportion of how much the ECG-shape could change when different activities are done. That is to say, the intra-change study to establish a fiducial or morphological fluctuation criteria. An example of this idea is climbing up to the sixth floor. In this case, there is a constant movement but the body exerts more effort each time during the sympathetic nervous system activation, proportionally altering the heartbeat. An opportunity factor is to evaluate these transition changes because this variation rate needs a period until stabilization. On the other hand, it is missing a decision framework that includes a parallel model to follow cardiac behavior and another to establish the user-veracity. In this circumstance, to the best of our knowledge at this time, there is no study about the biometric-template modification in a person given a physiological variable change. For example, some experiments could capture the user heart-dynamics case in the middle-term of a user from their idle state to a fitness state.

Throughout section 5, we are evaluating the current work in this area and the challenges ahead. In this vein, a clue option for improving user verification is to add signals related to heart dynamics. In order to do this, some possible sensor adhesion over the user body might be PPG, accelerometer, or gyroscope. Besides, all of this data follows the same cardiac phenomenon, revealing relationships between them to increase the discrimination factor. The idea is to use signals to increase the recognition robustness.

5.5 Specific acquisition concerns

Assuming an optimal signal acquisition, the three major concerns in ECG recording are baseline wander, powerline interference, and muscle noise [196]. Other considerations to take into account are [197]:

- Electrode contact noise.
- Noise generated by electronic circuit devices.
- High-frequency noises in the ECG record.
- Breathing or bowel motion.

The joint solution for these kinds of noises is the use of filters. The main goal of eliminating noise is to improve the relationship between signal to noise without altering the desired information. The ECG spectrum is from 0.01 Hz to 100 Hz with 90% of spectral energy between 0.25 Hz and 35 Hz [196]. Nowadays, processing computing has increased, shifting the solution to the digital field with software filters over hardware filters [198].

Muscle noise and the baseline wander are in the range of 0.05 Hz to 2 Hz; in the company of a high-pass filter, the attenuation task in this interval is completed. The powerline issue 50~60 Hz needs a notch or band suppressing filter. Other effects covered with a low-pass filter are the powerline harmonics and the anti-aliasing-filter with cut-off depending on the frequency sampling. Then, to reduce the computational complexity and adjust the system to apply to real-time systems, there are two proposals. First, to execute the filtering operation between the decimation and interpolation, if the system requirements allow this preprocessing task. Second, another approach is designing the filters with integer coefficients avoiding the use of floating point modules which would increase the processing time [198].

There are sophisticated methods for filtering the ECG signal such as neural networks [199], adaptive filters [200, 201], and wavelet-based filters [202, 200, 203], but those approximations are hardly applicable for real-time operations. However, there are innovations in adaptive filters for real-time applications [204, 196]. The most applied filters for real-time operations are FIR and IIR, choosing the best performance according to the phase, stability and order characteristics [205]. Moreover, assuming a white Gaussian additive noise, with the set of mentioned filters it is possible to reduce its bandwidth in respect to the ECG signal, improves the $\frac{\text{signal}}{\text{noise}}$ ratio.

During the ECG user sampling, not all measures have the same quality score; the cause can be noise, or electrode contact missing. Under this unavoidable scenario and the solution under low quality, this latter discards some affected ECG beats guided with some criteria. For example, the removal reference can be a correlation degree or the mean or median of some peak, or a temporal signal distance within some serial number of beats.

Regarding thermal noise, its behaviour inspection is with the ECG electrode model, that is a parallel impedance among a capacitor and a resistor. In consonance with the Association for the Advancement of Medical Instrumentation (AAMI), the ECG standard for a source impedance is 51 k Ω in parallel with 47 nF [206]. The thermal noise presence is expressed in equation 2 with the next parameters: i) T , temperature in Kelvins, ii) R is resistance, iii) Δf is frequency, iv) k is the Boltzmann constant ($1.38 \cdot 10^{-23} \frac{\text{joule}}{\text{Kelvins}}$), v) RMS voltage as e .

$$e^2 = 4kTR\Delta f \quad (2)$$

The impedance of the circuit RC after the conjugate complex separating the real and imaginary values is as follows in equation 3.

$$Z = \frac{R}{1 + (\omega RC)^2} - j \frac{\omega R^2 C}{1 + (\omega RC)^2} \quad (3)$$

With $\omega = 2\pi f$ and the equation 3, the square voltage is [207]

$$\begin{aligned} v_i^2 &= \int_0^\infty 4kT \operatorname{Re}(Z) \delta f = \int_0^\infty \frac{4kTR}{1+(2\pi fRC)^2} \delta f \\ &= \frac{2kT}{\pi C} \int_0^\infty \frac{\delta x}{1+x^2} = \frac{2kT}{\pi C} [\tan^{-1}]_0^\infty = \frac{kT}{C} \end{aligned} \quad (4)$$

Now, back to the electrode model with a capacitance of 47 nF [206] and a body temperature of 37°C (310.15°K), the thermal noise for one electrode is 301 nV. The typical ECG voltage range is between 0.1 and 2.5 mV [196]; in comparison with the thermal noise, ECG voltage is more prominent 8200 times. Therefore, although the thermal noise is a present phenomenon, its value does not affect the measure dramatically.

5.6 Improvement proposals

5.6.1 ECG verification including some postures and activities

As stated before, according to the body's needs, the ECG signal changes the heartbeat frequency, making it slower or faster. However, it is not only the time between each heartbeat that changes but also the amplitude and width of each fiducial within the PQRST complex that can suffer an alteration. From our perspective, this is the most challenging issue to face in an ECG authentication, especially during the training phase.

Commonly, in ECG authentication-related studies, the acquisition samples are taken from a resting position. Nevertheless, we present some work that expands this position variable for user verification. For instance, Porée et al. worked with three different testing conditions: supine rest, standing, and exercise [195], following up their participants for almost 20 months. In the same study, they provided a specific database by posture. Then, with the set of data collected, they designed an independent classification model by the three stances covered. The three stance conditions had an acceptable performance using the correlation coefficient with a shape analysis length between 300 and 800 milliseconds. Consequently, the next research goal was to study which of the three posture classifications already created could cover most of the possible heart variations. In this sense, for user verification, the experiments of Porée et al. suggest the standing-pose classification model that covers supine rest and exercise conditions. Lastly, to the best of our knowledge, no further work has been continued by Porée et al. in search of a general-pose that roofs other heart-rhythm postures for ECG user-authentication purposes.

On the other hand, applying machine learning algorithms instead of correlation, Shyan-Lung Lin et al. [208] evaluated the heartbeat of 26 people after exercise with SVM polynomial kernel, reaching a recognition rate over 80%. With respect to the use of wearable elements, Peter Christ et al. developed a WSN chest strap for walking and jogging experiments on a treadmill [209]. In the first scenario, the classifier obtained an accuracy of 98.1% within a speed between 3-9 $\frac{km}{h}$. Then, in a second session it reaches a rate of 11 $\frac{km}{h}$, with the recognition reduced to 93.8%. Moreover, in both cases, a fusion of either gait and ECG records were used with time and frequency features evaluated with ANN, SVM, and random forest classifiers. Table 12 presents the collection of Wahabi et al. [210], composed of different papers oriented to user-recognition, including different postures [211, 212, 213, 179]. In addition, table 12 contains a promising verification rate by work reaching an overall median of 79.5%, with data provided by the UofTDB database. In this study, the results indicate that ECG identification is possible in different positions and body activities, without denying the need for more population in new studies.

Table 12: Detection rate of different methods [210]

Method Posture	Sit	Stand	Supine	Tripod	Exercise
Chan et al. [211]	88%	94%	94%	96%	84%
Odinaka et al. [212]	66%	58%	84%	78%	90%
Irvine et al. [213]	78%	88%	84%	82%	92%
Agrafioti et al [179]	77%	75%	90%	94%	52%

5.6.2 ECG verification including heart disease and substance consumption

Not only can postures and activities alter the ECG signal, but the consumption of certain substances and some cardiac illness can as well. Odinaka et al. [212] conducted a notable study mixing 269 subjects with several categories where 40.15% had some heart-related disease, 46.84% used substances that might alter the ECG signal, and 27.88% were healthy. Among the three sessions, there was a separation from a week to seven months. The result within-session analysis was an EER of 0.37%; meanwhile, cross-session recording obtained an EER of around 5.2%.

5.6.3 About ECG lead I and more leads

Most of the current work focuses on Lead I signal acquisition for ECG biometric [179, 100]. However, there it is possible that in a dataset, when more electrodes and thus more data is available, the possibility of recognizing the desired category is higher. This section addresses some research that has worked with a configuration distinct from Lead I. To the best of our knowledge the first work in ECG biometric measuring with a 12-lead was proposed by Biel et al. Their procedure started with PCA for dimensionality reduction. Next, analysing the correlation matrix, they affirmed that the ECG signal contained redundant information, and only one lead configuration measure was necessary [169].

As for studies oriented to ECG-acquisition with multiple electrodes for user-recognition, Agrafioti et al. considered a data fusion experiment with a 12-Lead configuration. During the trial, they found that the performance in the feature level was not as high as expected, compared with Lead I disposition [179]. Later, they implemented fusion in the decision-level using a majority vote scheme achieving a better recognition performance. By the same token Fang et al. created coarse-grained structures with the phase space trajectory method [214], comparing either single-lead with three-lead, with a rate of 96% and 98%, respectively. In turn, Zhang et al. made use of the Mahalanobis distance with Bayes discrimination, containing measures from limb I-II and chest V1-V2 leads. Their best results were with V1 and V2 configuration (figure 19), possibly because these samples had a strong ECG signal by being near the heart, improving their quality. Alternatively, Jekova et al. [215] studied the optimization of 202 features using 12-lead. After a dimensionality reduction and a classification with LDA, only eleven features were the most representative, obtaining a sensitivity of 85.3% and a specificity of 86.4%. Their representative attributes corresponded to different leads: R-amplitude (I,II,V1,V2,V3,V5), S-amplitude (V1,V2), T_{neg} amplitude(aVR), and R-duration(aVF,V1).

In short, ECG 12-lead contains several features which can be represented in a small dimension. Although, in our opinion, based on the previous studies, Lead I configuration is enough for a regular performance during the person validation. For a proposal of hard acquisition conditions, we deem that the focus ahead must be on developing adequate materials for the electrodes. In case of a significant number of invalid heartbeats, it makes it necessary for the application to sacrifice comfort by adding one more lead. Due to its parallel scheme, an option with multiple Leads measuring is by doing a side by side authentication, ending with a majority vote evaluation method.

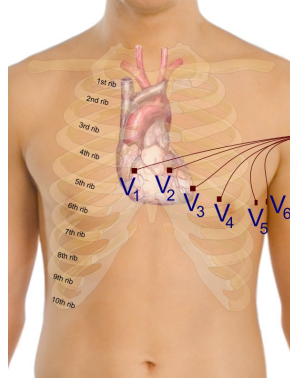


Figure 19: Positioning of the V1 to V6 leads. From [216]

5.6.4 An approach to T wave contribution

There are applications where the signal quality is low and only recognizable by the QRS complex. This is because this region contains a large portion of the heartbeat energy [173]. However, as depicted in Table 13, Lugovaya et al. compared different fragment contribution during the feature selection, showing that the segment P-QRS-T provides a more discriminative set [217].

Table 13: ECG identification fragments results of Lugovaya et al. [217]

Fragment	QRS	P-QRS	QRS-T	P-QRS-T
Recognition rate	77%	87%	76%	91%

In comparison, Kyoso et al. [218] extracted four attributes: P wave duration, PQ interval, QRS interval and QT interval. Then, the classification was done by discriminant analysis, using the Mahalanobis distance. As a result, the outstanding couples were QRS-QT and QRS-PQ, highlighting the influence of the fiducial T as described table 14.

Table 14: Results of discriminant analysis [218]

	P-QRS	P-PQ	P-QT	QRS-PQ	QRS-QT	PQ-QT
Accuracy mean [%]	76.57	56.55	57.41	85.12	94.20	68.02

On the contrary, Sidek et al. developed the recognition only with the QRS segment tackled in two papers [173, 219]. In their first work, they achieved a classification of 96.1%, with 30 people having a normalized QRS with MLP [219]. Then, in their second investigation, they applied the recognition over smartphones with NB, MLP and KNN, reaching a performance of 99.07% [173]. Unfortunately, both papers do not provide information on why the authors chose the QRS complex instead of the entire sequence. In contrast, Silva et al. located electrodes in a car steering wheel to compare the P-QRS-T and RS-T fragments, evaluating the driver recognition. The results suggest a better performance for the complete complex, with the second complex results being inside the confidence interval of the P-QRS-T [220].

The different related papers in this section and others, about the range of participation between the complex QRS and P-QRS-T are not conclusive [221, 222, 223, 224]. For this reason, we propose an experiment taking advantage of the scheme of Rezgui et al. scheme that has carefully mapped several features of the ECG signal [176]. So the purpose was to progressively eliminate the effect of the T

wave from the set of features, to register and compare the accuracy results. Then, with the attributes of Tables 15 and 16, the comparison was made with an SVM classifier, accounting for changes in the feature vector, including and discarding the T-based features. The test was applied to two subjects, each one against the templates of 89 people. In both cases, acceptance and rejection samples had the same amount. As a result, Table 17 contains the classifier accuracy discarding one feature at a time, modifying the feature vector.

Table 15: Temporal and amplitude features. Based on [176]

Extracted attributes					
Temporal	1. RQ	4. RL	7. RS'	10. S'T''	13. PT
	2. RS	5. RP''	8. RT''	11. ST	14. P'Q
	3. RP	6. RT	9. L'P''	12. PQ	15. ST''
Amplitude	16. PL'		17. PQ		18. RQ
	19. RS		20. TS'		21. TT''

Table 16: Morphological attributes. Based on [176]

Label	Description
Pp	Maximum amplitude of the positive peak
Pn	Maximum amplitude of the negative peak
ArP	Area of the positive samples
ArN	Area of the negative samples
Ar	Area of the QRS complex: $Ar = ArP + ArN$
Ima	Time interval from the QRS complex onset to the maximum positive peak
Imi	Time interval from the QRS complex onset to the maximum negative peak
No	Number of samples crossing a threshold of 70% of the highest peak amplitude
S1	QRS slope velocity calculated for the time interval between the QRS complex onset and the first peak
S2	QRS slope velocity calculated for the time interval between the first peak and the second peak

Table 17: Cumulative accuracy results discarding T features

	All	(-) RT	(-) RT''	(-) S'T''	(-) ST	(-) PT	(-) ST''	(-) TT''
P1 [%]	95.0	94.8	94.8	94.7	94.7	94.6	94.4	94.3
P2 [%]	93.7	93.5	93.4	93.3	93.3	93.1	92.7	92.9

In line with Table 17 in their first and last column, the confusion matrix in Table 18 contains the values of sensitivity, specificity, precision, and accuracy. Besides, during the classification, there is a constant value of false positives, which affects the specificity score. Consequently, as T fiducial is removed, the accuracy results with an SVM Gaussian kernel, decreased by 0.7% and 0.8% for person one and two. Therefore, this approach detects a minor T wave contribution through the SVM classifier. In comparison, the next experiment discards P and T contribution and uses only the QRS features of the same paper: $RQ, RS, RS', RQA, RSA, S1$ and $S2$. Therefore, the classification reaches 90% and 92.3% for person one and two following the results of table 19. In conclusion, the QRS complex is enough for recognition, but P and T fiducials have essential components that can complement the authentication rate.

6 Conclusions

From a smartphone authentication perspective, this paper provides a deep understanding of the different approaches in an authentication service. Thereby, an identity-based authentication orientation, a com-

Table 18: T contribution with Person #1 and #2

Condition	TP	TN	FP	FN	Sens.	Spec.	Prec.	Accy.
P1 with T	1235	1128	116	9	99.3%	90.7%	91.4%	95.0%
P1 without T	1237	1110	134	7	99.4%	89.2%	90.2%	94.3%
P2 with T	1237	1095	149	7	99.4%	88.0%	89.2%	93.7%
P2 without T	1236	1076	168	8	99.4%	86.5%	88.0%	92.9%

Table 19: QRS confusion matrix associated values

	TP	TN	FP	FN	Sens.	Spec.	Prec.	Accy.
P1	1221	1019	23	225	84.44%	97.79%	98.15%	90.03%
P2	1217	1079	27	165	88.06%	97.56%	97.83%	92.28%

parative description, and evaluation of existing biometric traits allowed different operational gaps to be recognized. This state creates the opportunity to extend the authentication environment with proposals such as Habitude Pattern Lock and ECG authentication. Habitude Pattern Lock integrates the standard use of the Pattern Lock but additionally analyze the user drawing habits to enrich the verification state. Finally, we present the smartphone ECG authentication study offering potential features, related products, and research topics such as current limitations, specific acquisition concerns, and improvement proposals. This study guides future investigations to make oriented decisions in the use of authentication services and smartphone biometric-based solutions. As future work for new investigations, we propose a fusion of dynamic and risk mechanisms, that depending on the peripheral context could prioritize the best evaluation tool for the user verification.

Acknowledgements

The authors would like to acknowledge the cooperation of all partners within the *Centro de Excelencia y Apropiación en Internet de las Cosas (CEA-IoT)* project. The authors would also like to thank all the institutions that supported this work: the Colombian Ministry for the Information and Communications Technology (*Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC*) and the Colombian Administrative Department of Science, Technology and Innovation (*Departamento Administrativo de Ciencia, Tecnología e Innovación - Colciencias*) through the *Fondo Nacional de Financiamiento para la Ciencia, la Tecnología y la Innovación Francisco José de Caldas* (Project ID: FP44842-502-2015). Besides, an additional acknowledgment corresponds to the Fundación Universitaria Compensar, including their Telecommunications Engineering Department, Research Department, English Area, and Bilingual Department for providing time and support to complete this paper.

References

- [1] S. Tweedie. World's first smartphone simon launched before iphone. <https://www.businessinsider.com/worlds-first-smartphone-simon-launched-before-iphone-2015-6>, July 2015. [Online; Accessed on 10/28/2021].
- [2] Statista. Number of smartphones sold to end users worldwide from 2007 to 2021. <https://www.statista.com/statistics/263437/global-smartphone-sales-to-end-users-since-2007/>, June 2021. [Online; Accessed on 10/28/2021].
- [3] C. Osborne. Smartphone sales stagnate in q4 2019, samsung still dominates. <https://www.zdnet.com/article/smartphone-sales-stagnate-in-q4-2019-samsung-still-dominates/>, March 2020. [Online; Accessed on 10/28/2021].

- [4] Gartner. Gartner says global smartphone sales fell slightly in the fourth quarter of 2019. <https://www.gartner.com/en/newsroom/press-releases/2020-03-03-gartner-says-global-smartphone-sales-fell-slightly-in>, March 2020. [Online; Accessed on 10/28/2021].
- [5] J.M. Ospina, F.V. Quintero, O.L. García, M.S. Domínguez, N.M. Cáceres, and M.Y. Lobon. *La industria 4.0, desde la perspectiva organizacional*. Fondo Editorial Universitario Servando Garcés de la Universidad Politécnica Territorial de Falcón Alonso Gamero, 2019.
- [6] CTVNews.ca-Staff. e-transfer theft: How a calgary couple was robbed of \$19,000 — ctv news. <https://www.ctvnews.ca/business/e-transfer-theft-how-a-calgary-couple-was-robbed-of-19-000-1.2470032>, July 2015. [Online; Accessed on 10/28/2021].
- [7] L. Weintraub. Identity theft... by mobile phone. <https://www.consumer.ftc.gov/blog/2016/06/identity-theft-mobile-phone>, June 2016. [Online; Accessed on 10/28/2021].
- [8] Federal Trade Commission. Identity theft recovery steps. <https://identitytheft.gov/>, May 2015. [Online; Accessed on 10/28/2021].
- [9] S. Vongsingthong and S. Boonkrong. A survey on smartphone authentication. *Walailak Journal of Science and Technology*, 12(1):1–19, Jan 2015.
- [10] M. Guerar, A. Merlo, and M. Migliardi. Clickpattern: A pattern lock system resilient to smudge and side-channel attacks. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, 8(2):64–78, June 2017.
- [11] J. Lee. Report forecasts biometrics market to surpass \$50b by 2024. <https://www.biometricupdate.com/201708/report-forecasts-biometrics-market-to-surpass-50b-by-2024>, August 2017. [Online; Accessed on 10/28/2021].
- [12] C. Burt. Biometric hardware revenues forecast to hit \$19b by 2024 on access control and camera growth. <https://www.biometricupdate.com/201912/biometric-hardware-revenues-forecast-to-hit-19b-by-2024-on-access-control-and-camera-growth>, December 2019. [Online; Accessed on 10/28/2021].
- [13] J. Lee. Tractica report forecasts global iris recognition market to grow to \$4.1b by 2025 — biometric update. <https://www.biometricupdate.com/201703/tractica-report-forecasts-global-iris-recognition-market-to-grow-to-4-1b-by-2025>, March 2017. [Online; Accessed on 10/28/2021].
- [14] P. Sharma. More than one billion smartphones with fingerprint sensors will be shipped in 2018. <https://www.counterpointresearch.com/more-than-one-billion-smartphones-with-fingerprint-sensors-will-be-shipped-in-2018/>, September 2017. [Online; Accessed on 10/28/2021].
- [15] C. Burt. Counterpoint estimates more than 1 billion smartphones to be shipped with facial recognition in 2020. <https://www.biometricupdate.com/201802/counterpoint-estimates-more-than-1-billion-smartphones-to-be-shipped-with-facial-recognition-in-2020>, February 9. [Online; Accessed on 10/28/2021].
- [16] H. Kelly. Phones want to scan your eyes, face or fingerprints - what if users say no to these biometrics? <https://www.washingtonpost.com/technology/2019/11/15/fingerprints-face-scans-are-future-smartphones-these-holdouts-refuse-use-them/>, November 2019. [Online; Accessed on 10/28/2021].
- [17] V. Goel. That fingerprint sensor on your phone is not as safe as you think - the new york times. <https://www.nytimes.com/2017/04/10/technology/fingerprint-security-smartphones-apple-google-samsung.html>, April 2017. [Online; Accessed on 10/28/2021].
- [18] A. Roy, N. Memon, and A. Ross. Masterprint: Exploring the vulnerability of partial fingerprint-based authentication systems. *IEEE Transactions on Information Forensics and Security*, 12(9):2013–2025, September 2017.
- [19] I.G. Telleria, J.L. Jimenez, H.Q. Sandoval, and R.S. Reillo. Analysis of the attack potential in low cost spoofing of fingerprints. In *Proc. of the 52th International Carnahan Conference on Security Technology (ICCST'17), Madrid, Spain*, pages 1–6. IEEE, October 2017.
- [20] J. Pato and L. Millett. *Biometric Recognition : Challenges and Opportunities*. The National Academies Press, 1st ed. edition, 2010.

- [21] D. Dasgupta, A. Roy, and A. Nag. *Advances in User Authentication*. Springer, 1st ed. edition, 2017.
- [22] D. Maltoni, D. Maio, A. Jain, and S. Prabhakar. *Handbook of fingerprint recognition*. Springer, 2nd ed. edition, 2009.
- [23] S. Gupta, A. Buriro, and B. Crispo. Demystifying Authentication Concepts in Smartphones: Ways and Types to Secure Access. *Mobile Information Systems*, 2018(1):48–63, March 2018.
- [24] B. Bank. Internet: Portal banca personas. <https://www.bancodebogota.com/wps/portal/banco-de-bogota/bogota/teleton/canales/internet>, February 2015. [Online; Accessed on 10/28/2021].
- [25] B. Bank. Token movil. https://play.google.com/store/apps/details?id=com.bancodebogota.token&hl=es_EC, March 2019. [Online; Accessed on 10/28/2021].
- [26] M. Morse. Modified iris photo by michael morse from pexels. <https://www.pexels.com/photo/macro-photo-of-eye-1486641/>, October 2018. [Online; Accessed on 10/28/2021].
- [27] P.S. Teh, N. Zhang, A.B.J. Teoh, and K. Chen. A survey on touch dynamics authentication in mobile devices. *Computers and Security*, 59(1):210–235, June 2016.
- [28] V. Patel, R. Chellappa, D. Chandra, and B. Barbelo. Continuous User Authentication on Mobile Devices: Recent progress and remaining challenges. *IEEE Signal Processing Magazine*, 33(4):49–61, July 2016.
- [29] Android. Authentication. <https://source.android.com/security/authentication> [Online; Accessed on 10/28/2021], September 2020.
- [30] Android. Fingerprint hidl. <https://source.android.com/security/authentication/fingerprint-hidl>, September 2020. [Online; Accessed on 10/28/2021].
- [31] Android. Face authentication hidl — android open source project. <https://source.android.com/security/biometric/face-authentication>, October 2021. [Online; Accessed on 10/28/2021].
- [32] Android. Devicepolicymanager. [https://developer.android.com/reference/android/app/admin/DevicePolicyManager#lockNow\(int\)](https://developer.android.com/reference/android/app/admin/DevicePolicyManager#lockNow(int)), October 2021. [Online; Accessed on 10/28/2021].
- [33] P. Joshi, C. Jindal, M. Chowkwale, R. Shethia, S.A. Shaikh, and D. Ved. Protego: A passive intrusion detection system for android smartphones. In *Proc. of the 1st International Conference on Computing, Analytics and Security Trends (CAST'16), Pune, India*, pages 232–237. IEEE, December 2016.
- [34] Y. Kubo, R. Takada, B. Shizuki, and S. Takahashi. Exploring context-aware user interfaces for smartphone-smartwatch cross-device interaction. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, 1(3):69:1–69:21, September 2017.
- [35] Ilex International. Sign&go mobility center. <https://www.illex-international.com/en/iam-platform/sign-and-go-mobility-center>, January 2020. [Online; Accessed on 10/28/2021].
- [36] B. Maciej, E.F. Imed, and M. Kurkowski. Multifactor authentication protocol in a mobile environment. *IEEE Access*, 7(1):157:185–157:199, October 2019.
- [37] M. Azimpourkivi, U. Topkara, and B. Carbanar. Camera based two factor authentication through mobile and wearable devices. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, 1(3):35:1–35:37, September 2017.
- [38] Apple. Two-factor authentication for apple id. <https://support.apple.com/en-us/HT204915>, December 2020. [Online; Accessed on 10/28/2021].
- [39] A. Yohan, N.W. Lo, and H.R. Lie. Dynamic multi-factor authentication for smartphone. In *Proc. of the 27th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC'16), Valencia, Spain*, pages 2448–2453. IEEE, September 2016.
- [40] S. Barra, G. Fenu, M.D. Marsico, A. Castiglione, and M. Nappi. Have you permission to answer this phone? In *Proc. of the 6th International Workshop on Biometrics and Forensics (IWBF'18), Sassari, Italy*, pages 1–7. IEEE, June 2018.
- [41] Y. Albayram and M.M. Khan. Evaluating smartphone-based dynamic security questions for fallback authentication: A field study. *Human-centric Computing and Information Sciences*, 6(1):72:1–72:35, September 2016.
- [42] Hugo Gascon, Sebastian Uellenbeck, Wolf Christopher, and Konrad Rieck. Continuous authentication on mobile devices by analysis of typing motion behavior. In *Proc. of the 6th Series Sicherheit, Schutz und Zuverlässigkeit (Sicherheit'14), Vienna, Austria*, pages 1–12. Gesellschaft für Informatik, March 2014.

- [43] C. Shen, Y. Zhang, Z. Cai, T. Yu, and X. Guan. Touch-interaction behavior for continuous user authentication on smartphones. In *Proc. of the 3rd International Conference on Biometrics (ICB'15), Phuket, Thailand*, pages 157–162. IEEE, May 2015.
- [44] M.P. M, D. Ramotsoela, and G. Hancke. Continuous user authentication in smartphones using gait analysis. In *Proc. of the 44th Annual Conference of the IEEE Industrial Electronics Society (IECON'18), Washington DC, USA*, pages 4656–4661. IEEE, October 2018.
- [45] J. Zhang and D. Tao. Implicit identity authentication mechanism based on smartphone touch dynamics. In *Proc. of the 6th International Conference on Consumer Electronics (ICCE-TW'19), Yilan, Taiwan*, pages 457–458. IEEE, May 2019.
- [46] H. Crawford and K. Renaud. Understanding user perceptions of transparent authentication on a mobile device. *Journal of Trust Management*, 1(1):7:1–7:7, June 2014.
- [47] H. Crawford, K. Renaud, and T. Storer. A framework for continuous, transparent mobile device authentication. *Computers and Security*, 39(1):127–136, November 2013.
- [48] S. Ghogare, S. Jadhav, A. Chadha, and H. Patil. Location based authentication: A new approach towards providing security. *International Journal of Scientific and Research Publications*, 2(4):1–5, April 2012.
- [49] S. Wiefling, L.L. Iacono, and M. Durmuth. Is this really you? an empirical study on risk-based authentication applied in the wild. In *Proc. of the 34th International Conference on Information Security and Privacy Protection (IFIP SEC'19), Lisbon, Portugal*, volume 562 of *IFIP Advances in Information and Communication Technology*, pages 134–148. Springer, June 2019.
- [50] I. Traore, I. Woungang, M. Obaidat, Y. Nakkabi, and I. Lai. Online risk-based authentication using behavioral biometrics. *Multimedia Tools and Applications*, 71(2):575–605, July 2014.
- [51] C. Mi, R. Xu, C.T. Lin, and R.Y. Meng. An active smartphone authentication method based on daily cyclical activity. *CoRR*, abs/1909.00045(1):1–14, September 2019.
- [52] M. Tanviruzzaman and S.I. Ahamed. Your phone knows you: Almost transparent authentication for smartphones. In *Proc. of the 38th Annual Computer Software and Applications Conference (COMP-SAC'14), Vasteras, Sweden*, pages 374–383. IEEE, July 2014.
- [53] R. J. Hulsebosch, M. S. Bargh, G. Lenzini, P.W.G. Ebben, and S.M. Iacob. Context sensitive adaptive authentication. In *Proc. of the 2nd European Conference on Smart Sensing and Context (EuroSSC'07), Kendal, United Kingdom*, volume 4793 of *Lecture Notes in Computer Science*, pages 93–109. Springer, October 2007.
- [54] Q. Zhang, H. LiMan, Z.Z. He, Z. Sun, and T. Tan. Fusion of face and iris biometrics on mobile devices using near-infrared images. In *Proc. of the 5th Chinese Conference on Biometric Recognition (CCBR'15), Tianjin, China*, volume 9428 of *Lecture Notes in Computer Science*, pages 569–578. Springer, November 2015.
- [55] M. Marsico, C. Galdi, M. Nappi, and D. Riccio. Firme: Face and iris recognition for mobile engagement. *Image and Vision Computing*, 32(12):1161–1172, December 2014.
- [56] L. Wu, J. Yang, M. Zhou, Y. Chen, and Q. Wang. Lvid: A multimodal biometrics authentication system on smartphones. *IEEE Transactions on Information Forensics and Security*, 15(1):1572–1585, September 2020.
- [57] ISO. Information technology - Vocabulary - Part 37: Biometrics. Technical Report ISO/IEC 2382-37:2017, ISO, 2017.
- [58] M. Nieves, K. Dempsey, and V.Y. Pillitteri. Nist special publication 800-12 revision 1 - an introduction to information security. *NIST Special Publication*, 1(1):1–101, June 2017.
- [59] A. Fantana, S. Ramachandran, C. Schunck, and M. Talamo. Movement based biometric authentication with smartphones. In *Proc. of the 49th International Carnahan Conference on Security Technology (ICCST'15), Taipei, Taiwan*, pages 235–239. IEEE, September 2015.
- [60] M. Montgomery, P. Chatterjee, J. Jenkins, and K. Roy. Touch analysis: An empirical evaluation of machine learning classification algorithms on touch data. In *Proc. of the 4th International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage (SpaCCS'19), Atlanta, GA, USA*, volume 11611 of *Lecture Notes in Computer Science*, pages 147–156. Springer, December 2019.
- [61] A.D. Luca, A. Hang, F. Brudy, C. Lindner, and H. Hussmann. Touch me once and i know it's you!:

- implicit authentication based on touch screen patterns. In *Proc. of the 31th Conference on Human Factors in Computing Systems (CHI'12)*, Austin, TX, US, pages 987—996. ACM, August 2012.
- [62] S. Sahdev, C. Forlines, R. Jota, B. Araujo, B. Moseley, J. Deber, S. Sanders, D. Leigh, and D. Wigdor. Ghostid: Enabling non-persistent user differentiation in frequency-division capacitive multi-touch sensors. In *Proc. of the 36th Conference on Human Factors in Computing Systems (CHI'17)*, Denver, US, pages 15–27. ACM, May 2017.
- [63] Q. Liu, M. Wang, P. Zhao, C. Yan, and Z. Ding. Behavioral authentication method for mobile gesture against resilient user posture. In *Proc. of the 3rd International Conference on Systems and Informatics (ICSAI'17)*, Shanghai, China, pages 324–331. IEEE, November 2017.
- [64] M.M. Diaz, J. Fierrez, and J. Galbally. Graphical password-based user authentication with free-form doodles. *IEEE Transactions on Human-Machine Systems*, 46(4):607–614, August 2016.
- [65] B.S. Saini, N. Kaur, K.S. Bhatia, and A.K. Luhach. Analyzing user typing behaviour in different positions using keystroke dynamics for mobile phones. *Journal of Discrete Mathematical Sciences and Cryptography*, 22(4):591–603, September 2019.
- [66] B.S. Saini, N. Kaur, and K.S. Bhatia. Authenticating mobile phone users based on their typing position using keystroke dynamics. In *Proc. of 2nd International Conference on Communication, Computing and Networking (ICCCN'19)*, Chandigarh, India, volume 46 of *Lecture Note in Networks and Systems*, pages 25–33. Springer, March 2019.
- [67] H. Lee, J.Y. Hwang, D.I. Kim, S. Lee, S.H. Lee, and J.S. Shin. Understanding keystroke dynamics for smartphone users authentication and keystroke dynamics on smartphones built-in motion sensors. *Security and Communication Networks*, 2018(1):125–134, December 2018.
- [68] A. Primo. Keystroke-based continuous authentication while listening to music on your smart-phone. In *Proc. of the 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON'17)*, New York, NY, USA, pages 217–225. IEEE, Oct 2017.
- [69] C. Praher and M. Sonntag. Applicability of keystroke dynamics as a biometric security feature for mobile touchscreen devices with virtualised keyboards. *International Journal of Information and Computer Security*, 8(1):72—91, March 2016.
- [70] Q. Zou, Y. Wang, Q. Wang, Y. Zhao, and Q. Li. Deep learning-based gait recognition using smartphones in the wild. *IEEE Transactions on Information Forensics and Security*, 15(1):3197–3212, December 2020.
- [71] M. Muaaz and R. Mayrhofer. Smartphone-based gait recognition: From authentication to imitation. *IEEE Transactions on Mobile Computing*, 16(11):3209–3221, November 2017.
- [72] I. Lamiche, G. Bin, Y. Jing, Z. Yu, and A. Hadid. A continuous smartphone authentication method based on gait patterns and keystroke dynamics. *Journal of Ambient Intelligence and Humanized Computing*, 10(11):4417–4430, November 2019.
- [73] R. Ferrero, F. Gandino, B. Montrucchio, M. Rebaudengo, A. Velasco, and I. Benkhelifa. On gait recognition with smartphone accelerometer. In *Proc. of the 4th Mediterranean Conference on Embedded Computing (MECO'15)*, Budva, Montenegro, pages 368–373. IEEE, June 2015.
- [74] M. Gadaleta and M. Rossi. Idnet: Smartphone-based gait recognition with convolutional neural networks. *Pattern Recognition*, 74(1):25–37, February 2018.
- [75] S. Alotaibi, A. Alruban, and S. Furnell. A novel behaviour profiling approach to continuous authentication for mobile applications. In *Proc. of the 5th International Conference on Information Systems Security and Privacy (ICISSP'19)*, Prague, Czech Republic, pages 246–251. SCITEPRESS, February 2019.
- [76] S.M.Z. Mohammed, A.R.M. Shariff, and M.M. Singh. An authentication technique: Behavioral data profiling on smart phones. In *Proc. of the 1th International Conference on Computational Science and Technology (ICCST'17)*, Kuala Lumpur, Malaysia, volume 488 of *Lecture Notes in Electrical Engineering*, pages 88–98. Springer, November 2017.
- [77] U. Mahbub, S. Sarkar, V. Patel, and R. Chellappa. Active user authentication for smartphones: A challenge data set and benchmark results. In *Proc. of the 8th IEEE International Conference on Biometrics: Theory, Applications, and Systems (BTAS'16)*, Niagara Falls, NY, USA, pages 1–8. IEEE, September 2016.
- [78] F. Li, N. Clarke, M. Papadaki, and P. Dowland. Active authentication for mobile devices utilising behaviour profiling. *International Journal of Information Security*, 13(3):229—244, June 2014.

- [79] Y. Ashibani and Q.H. Mahmoud. A behavior profiling model for user authentication in iot networks based on app usage patterns. In *Proc. of the 44th Conference of the IEEE Industrial Electronics Society (IECON'18)*, Washington D.C., USA, pages 2841–2846. IEEE, October 2018.
- [80] F. Hong, M. Wei, S. You, Y. Feng, and Z. Guo. Waving authentication: Your smartphone authenticate you on motion gesture. In *Proc. of the 33rd Annual ACM Conference Extended Abstracts on Human Factors in Computing Systems (CHI EA'15)*, Seoul, Republic of Korea, pages 263—266. ACM, April 2015.
- [81] A.N. Filina and K.K. Kogos. Continuous authentication over hand-waving for android smartphones. In *Proc. of the 1st Advanced Technologies in Robotics and Intelligent Systems (ITR'20)*, Moscow, Russia, volume 80 of *Mechanisms and Machine Science*, pages 413–424. Springer, January 2020.
- [82] A. Filina and K. Kogos. Mobile authentication over hand-waving. In *Proc. of the 2nd IEEE Conference on Quality Management, Transport and Information Security, Information Technologies (IT&MQ&IS'17)*, St. Petersburg, Russia, pages 69–74. IEEE, September 2017.
- [83] A. Buriro, B. Crispo, F. Delfrari, and K. Wrona. Hold and sign: A novel behavioral biometrics for smartphone user authentication. In *Proc. of the 5th IEEE Symposium on Security and Privacy Workshops (SPW'16)*, San Jose, CA, USA, pages 276–285. IEEE, May 2016.
- [84] L. Yang, Y. Guo, X. Ding, J. Han, Y. Liu, C. Wang, and C. Hu. Unlocking smart phone through handwaving biometrics. *IEEE Transactions on Mobile Computing*, 14(5):1044–1055, May 2015.
- [85] A. Mahfouz, T. Mahmoud, and A.S. Eldin. A survey on behavioral biometric authentication on smartphones. *Journal of Information Security and Applications*, 37(1):28–37, December 2017.
- [86] A. Alzubaidi and J. Kalita. Authentication of smartphone users using behavioral biometrics. *IEEE Communications Surveys and Tutorials*, 18(3):1998–2026, March 2016.
- [87] G. Bhatt and B. Bhushan. A comprehensive survey on various security authentication schemes for mobile touch screen. In *Proc. of the 9th International Conference on Communication Systems and Network Technologies (CSNT'20)*, Gwalior, India, pages 248–253. IEEE, April 2020.
- [88] M. Abuhamad, A. Abusnaina, D. Nyang, and D. Mohaisen. Sensor-based continuous authentication of smartphones' users using behavioral biometrics: A contemporary survey. *IEEE Internet of Things Journal*, 8(1):65–84, August 2020.
- [89] A. Jain, K. Nandakumar, and ArunRoss. 50 years of biometric research: Accomplishments, challenges, and opportunities. *Pattern Recognition Letters*, 79(1):80–105, August 2016.
- [90] J.L. Cabra, D. Mendez, and L.C. Trujillo. Wide machine learning algorithms evaluation applied to ecg authentication and gender recognition. In *Proc. of the 2nd International Conference on Biometric Engineering and Applications (ICBEA'18)*, Amsterdam, Netherlands, pages 58—64. ACM, May 2018.
- [91] J. Snyder. Using biometrics for authentication in android. insights.samsung.com/2021/04/21/using-biometrics-for-authentication-in-android-2/, April 2021. [Online; Accessed on 10/28/2021].
- [92] K. Plataniotis. Biometric signals and systems. <http://www.ipsi.utoronto.ca/docs/ECE1517-Intro-Lecture.pdf>, November 2009. [Online; Accessed on 10/28/2021].
- [93] U. Yadav, S. Abbas, and D. Hatzinakos. Evaluation of ppg biometrics for authentication in different states. In *Proc. of the 5th International Conference on Biometrics (ICB'18)*, Gold Coast, QLD, Australia, pages 277–282. IEEE, February 2018.
- [94] C. Carreiras, A. Lourenço, A. Fred, and R. Ferreira. Ecg signals for biometric applications - are we there yet? In *Proc. of the 11th International Conference on Informatics in Control, Automation and Robotics (ICINCO'14)*, Vienna, Austria, pages 765–772. IEEE, September 2014.
- [95] E. Maiorana, D.L. Rocca, and P. Campisi. On the permanence of eeg signals for biometric recognition. *IEEE Transactions on Information Forensics and Security*, 11(1):163–175, 2016.
- [96] A. Das, O. Manyam, M. Tapaswi, and V. Taranalli. Multilingual spoken-password based user authentication in emerging economies using cellular phone networks. In *Proc. of the 2nd IEEE Spoken Language Technology Workshop (SLT'18)*, Goa, India, pages 5–8. IEEE, December 2008.
- [97] M.M. Diaz, J.Fierrez, R. Krish, and J. Galbally. Mobile signature verification: feature robustness and performance comparison. *IET Biometrics*, 3(4):267–277, May 2014.
- [98] F.J. Zareen and S. Jabin. Authentic mobile-biometric signature verification system. *IET Biometrics*, 5(1):13—19, March 2016.

- [99] T. Hoang, D. Choi, V. Vo, A. Nguyen, and T. Nguyen. A lightweight gait authentication on mobile phone regardless of installation error. In *Proc. of the 11th International Conference Security and Privacy Protection in Information Processing Systems (SEC'13), Auckland, New Zealand*, volume 405 of *IFIP Advances in Information and Communication Technology*, pages 83–101. Springer, July 2013.
- [100] A. Fratini, M. Sansone, P. Bifulco, and M. Cesarelli. Individual identification via electrocardiogram analysis. *BioMedical Engineering OnLine*, 14(1):78:1–78:23, August 2015.
- [101] J. Sriram, M. Shin, T. Choudhury, and D. Kotz. Activity-aware ecg-based patient authentication for remote health monitoring. In *Proc. of the 11th international conference on Multimodal Interfaces and Machine Learning for Multimodal Interaction (ICMI-MLMI'09), New York, NY, United States*, pages 297—304. ACM, November 2009.
- [102] H. Yamaba, T. Kurogi, K. Aburada, S.I. Kubota, T. Katayama, M. Park, and N. Okazaki. On applying support vector machines to a user authentication method using surface electromyogram signals. *Artificial Life and Robotics*, 23(1):87–93, November 2018.
- [103] S. Shin, J. Jung, and Y.T. Kim. A study of an emg-based authentication algorithm using an artificial neural network. In *Proc. of the 16th IEEE SENSORS, Glasgow, UK*, pages 1–3. IEEE, October 2017.
- [104] V. Jindal, J. Birjandtalab, M.B. Pouyan, and M. Nourani. An adaptive deep learning approach for ppg-based identification. In *Proc. of the 38th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC'16), Orlando, FL, USA*, pages 6401–6404. IEEE, August 2016.
- [105] S.K. Yeom, H.I. Suk, and S.W. Lee. Person authentication from neural activity of face-specific visual self-representation. *Pattern Recognition*, 46(4):1159—1169, April 2013.
- [106] I. Jayarathne, M. Cohen, and S. Amarakeerthi. Survey of eeg-based biometric authentication. In *Proc. of the 8th International Conference on Awareness Science and Technology (iCAST'17), Taichung, Taiwan*, pages 324–329. IEEE, November 2017.
- [107] D. Bradbury. Sure, face id is neat, but it cannot replace a good old fashioned passcode. https://www.theregister.co.uk/2017/11/14/is_facial_recognition_good_enough/, November 2017. [Online; Accessed on 10/28/2021].
- [108] J.O. Mercado, K.T. Medina, G.S. Perez, H.P. Meana, and M.N. Miyatake. Face recognition system for smartphone based on lbp. In *Proc. of the 5th International Workshop on Biometrics and Forensics (IWBF'17), Coventry, UK*, pages 1–33. IEEE, April 2017.
- [109] B. Aghili and H. Sadjedi. Personal authentication using hand geometry. In *Proc. of the 1st International Conference on Computational Intelligence and Software Engineering (CiSE'09), Wuhan, China*, pages 1176–1179. IEEE, December 2009.
- [110] A. Bapat and V. Kanhangad. Segmentation of hand from cluttered backgrounds for hand geometry biometrics. In *Proc. of the 5th IEEE Region 10 Symposium (TENSYP'17), Cochin, India*, pages 218–221. IEEE, July 2017.
- [111] M.R. Rajput and G.S. Sable. Iris biometrics survey 2010–2015. In *Proc. of the 1st IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT'16), Bangalore, India*, pages 2028–2033. IEEE, May 2016.
- [112] G.S. Bindra, A. Agrawal, and P. Sharma. Feature based iris recognition system functioning on extraction of 2d features. In *Proc. of the 2nd IEEE International Conference on System Engineering and Technology (ICSET'12), Bandung, Indonesia*, pages 102–106. IEEE, September 2012.
- [113] J. Fatima, A. Syed, and U. Akram. A secure personal identification system based on human retina. In *Proc. of the 5th IEEE Symposium on Industrial Electronics & Applications (ISIEA'13), Kuching, Malaysia*, pages 90–95. IEEE, September 2013.
- [114] X. Chen, Y. Chen, Z. Ma, and F. Fernandes. How is energy consumed in smartphone display applications? In *Proc. of the 14th Workshop on Mobile Computing Systems and Applications (HotMobile'13), New York, NY, United States*, pages 1–6. ACM, February 2013.
- [115] S. Tarkoma, M. Siekkinen, E. Lagerspetz, and Y. Xiao. *Smartphone Energy Consumption: Modeling and Optimization*. Cambridge University Press, 2014.
- [116] LifeHacks. Your iphone's touch id is very easy to hack with this simple trick! it's easier to break in than you think! <https://www.tips-and-tricks.co/lifehacks/iphone-touch-id/>, May 2018. [Online;

- Accessed on 10/28/2021].
- [117] BBC News. Clay digit fools smartphone fingerprint sensors. <https://www.bbc.com/news/av/technology-35642747>, February 2016. [Online; Accessed on 10/28/2021].
 - [118] Apple Inc. Security of apple platforms. <https://manuals.info.apple.com/MANUALS/1000/MA1902/esES/apple-platform-security-guide-y.pdf>, May 2021. [Online; Accessed on 10/28/2021].
 - [119] K. Olmstead and A. Smith. Americans and cybersecurity. *Pew Research Center*, 1(1):1–43, January 2017.
 - [120] C. Yang, J.L. Hung, and Z.X. Lin. Loose password security in chinese cyber world left the front door wide open to hackers: an analytic view. In *Proc. of the 14th Annual International Conference on Electronic Commerce (ICEC'12), Singapore, Singapore*, pages 121–126. ACM, August 2012.
 - [121] P. Andriotis, T. Tryfonas, G. Oikonomou, and C. Yildiz. A pilot study on the security of pattern screen-lock methods and soft side channel attacks. In *Proc. of the 6th ACM conference on Security and privacy in wireless and mobile networks (WiSec'13), Budapest, Hungary*, pages 1–6. ACM, April 2013.
 - [122] C. Sun, Y. Wang, and J. Zheng. Dissecting pattern unlock: The effect of pattern strength meter on pattern selection. *Journal of Information Security and Applications*, 19(4):308–320, November 2014.
 - [123] B.H. Padma and G.V.S. Raj Kumar. Design and analysis of an enhanced sha-1 hash generation scheme for android mobile computers. *International Journal of Applied Engineering Research*, 11(4):2359–2363, March 2016.
 - [124] W. Meng. Evaluating the effect of multi-touch behaviours on android unlock patterns. *Information and Computer Security*, 24(3):277–287, July 2016.
 - [125] S. Uellenbeck, M. Dürmuth, C. Wolf, and T. Holz. Quantifying the security of graphical passwords: the case of android unlock patterns. In *Proc. of the 20th ACM SIGSAC conference on Computer & communications security (CSS'13), Berlin, Germany*, pages 161–172. ACM, November 2013.
 - [126] J. Pi, P. De, and K. Mueller. Using gpus to crack android pattern-based passwords. In *Proc. of the 19th International Conference on Parallel and Distributed Systems (ICPADS'13), Seoul, Korea (South)*, pages 450–451. IEEE, December 2013.
 - [127] J. Lee, J.W. Seo, K. cho, P.J. Lee, J. Kim, S.H. Choi, and D.H. Yum. A visibility-based upper bound for android unlock patterns. *IEICE Transactions on Information and Systems*, E99.D(11):2814–2816, November 2016.
 - [128] D.V. Bruggen, S. Liu, M. Kajzer, A. Striegel, C.R. Crowell, and J. D'Arcy. Modifying smartphone user locking behavior. In *Proc. of the 9th Symposium on Usable Privacy and Security (SOUPS'13), Newcastle, United Kingdom*, pages 1–14. IEEE, July 2013.
 - [129] N. Malkin, M. Harbach, A.D. Luca, and S. Egelman. The anatomy of smartphone unlocking: Why and how android users around the world lock their phones. *GetMobile: Mobile Computing and Communications*, 20(3):42–46, July 2017.
 - [130] E.V. Zezschwitz, M. Eiband, D. Buschek, S. Oberhuber, A.D. Luca, F. Alt, and H. Hussmann. On quantifying the effective password space of grid-based unlock gestures. In *Proc. of the 15th International Conference on Mobile and Ubiquitous Multimedia (MUM'16), New York, NY, United States*, pages 201–212. ACM, December 2016.
 - [131] J. Davin, A. Aviv, F. Wolf, and R. Kuber. Baseline measurements of shoulder surfing analysis and comparability for smartphone unlock authentication. In *Proc. of the 21th Conference Extended Abstracts on Human Factors in Computing Systems (CHI'17), Denver, Colorado, USA*, pages 2496–2503. ACM, May 2017.
 - [132] G. Ye, Z. Tang, D. Fang, X. Chen, K.I. Kim, B. Taylor, and Z. Wang. Cracking android pattern lock in five attempts. *NDSS*, 25(1):1–15, February 2017.
 - [133] A.A. Abdulwahid, N. Clarke, S. Furnell, I. Stengel, and C. Reich. The current use of authentication technologies: An investigative review. In *Proc. of the 1st International Conference on Cloud Computing (ICCC'15), Riyadh, Saudi Arabia*, pages 239–246. IEEE, April 2015.
 - [134] Tech design forum. Side-channel attacks. <http://www.techdesignforums.com/practice/guides/side-channel-analysis-attacks/>, June 2012. [Online; Accessed on 10/28/2021].
 - [135] A.J. Aviv, B. Sapp, M. Blaze, and J.M. Smith. Practicality of accelerometer side channels on smartphones. In *Proc. of the 28th Annual Computer Security Applications Conference (ACSAC'12), New York, NY, United States*, pages 41–50. ACM, December 2012.

- [136] J. Zhang, X. Zheng, Z. Tang, T. Xing, X. Chen, D. Fang, R. Li, X. Gong, and F. Chen. Privacy leakage in mobile sensing: Your unlock passwords can be leaked through wireless hotspot functionality. *Mobile Information System*, 2016(1):52–65, April 2016.
- [137] Y. Abdelrahman, M. Khamis, S. Schneegass, and F. Alt. Stay cool! understanding thermal attacks on mobile-based user authentication. In *Proc. of the 37th Conference on Human Factors in Computing Systems (CHI'17), Denver, Colorado, USA*, page 3751–3763. ACM, May 2017.
- [138] Computer Hope. What is epoch? <https://www.computerhope.com/jargon/e/epoch.htm>, November 2018. [Online; Accessed on 10/28/2021].
- [139] Android Developers. Systemclock. <https://developer.android.com/reference/android/os/SystemClock.html>, February 2021. [Online; Accessed on 10/28/2021].
- [140] Oracle. Java native interface overview. <http://docs.oracle.com/javase/6/docs/technotes/guides/jni/spec/intro.html#wp725>. [Online; Accessed on 10/28/2021].
- [141] A. Lutomirski. `arch/x86/vdso/vclock_gettime.c` - kernel/mediatek. https://android.googlesource.com/kernel/mediatek/+refs/heads/android-mediateg-sprout-3.4-kitkat-mr2/arch/x86/vdso/vclock_gettime.c, March 2012. [Online; Accessed on 10/28/2021].
- [142] L. Robert. *Linux System Programming*. O'Reilly, 2013.
- [143] L.T. Thang. Comparing real-time scheduling on the linux kernel and an rtos. <https://www.embedded.com/comparing-real-time-scheduling-on-the-linux-kernel-and-an-rtos/> [Online; Accessed on 10/28/2021], April 2012.
- [144] B. Cole. Real-time android: real possibility, really really hard to do - or just plain impossible? <https://www.embedded.com/real-time-android-real-possibility-really-really-hard-to-do-or-just-plain-impossible/>, May 2012. [Online; Accessed on 10/28/2021].
- [145] T. Kwon and S. Na. Tinylock: Affordable defense against smudge attacks on smartphone pattern lock systems. *Computers & Security*, 42(1):137–150, May 2014.
- [146] A. Colley, T. Seitz, T. Lappalainen, M. Kranz, and J. Häkkinen. Extending the touchscreen pattern lock mechanism with duplicated and temporal codes. *Advances in Human-Computer Interaction*, 2016(1):1–12, November 2016.
- [147] P. Lacharme and C. Rosenberger. Synchronous one time biometrics with pattern based authentication. In *Proc. of the 11th International Conference on Availability, Reliability and Security, (ARES'16), Salzburg, Austria*, pages 260–265. IEEE, September 2016.
- [148] X.S. Chun, Y. Chao, M.A.J Feng, and Z.J. Wei. Android unlock pattern scheme through random point exclusion. *Ruan Jian Xue Bao/Journal of Software*, 28(2):361–371, February 2017.
- [149] D. Schweitzer, J. Boleng, C. Hughes, and L. Murphy. Visualizing keyboard pattern passwords. In *Proc. of the 6th IEEE Symposium on Visualization for Cyber Security (VizSec'09), Atlantic City, NJ, USA*, pages 69–73. IEEE, October 2009.
- [150] M. Frank, R. Biedert, E. Ma, I. Martinovic, and D. Song. Touchalytics: On the applicability of touchscreen input as a behavioral biometric for continuous authentication. *IEEE Transactions on Information Forensics and Security*, 8(1):136–148, January 2013.
- [151] O. Alpar. Intelligent biometric pattern password authentication systems for touchscreens. *Expert Systems with Applications*, 42(17):6286–6294, October 2015.
- [152] J.N. Luo, M.H. Yang, and C.L. Tsai. A mobile device-based antishoulder-surfing identity authentication mechanism. In *Proc. of the 10th International Conference Network and System Security (NSS'16), Taipei, Taiwan*, volume 9955 of *Lecture Notes in Computer Science*, pages 37–46. Springer, September 2016.
- [153] O. Alpar and O. Krejcar. Pattern password authentication based on touching location. In *Proc. of the 16th Intelligent Data Engineering and Automated Learning – (IDEAL'15), Wroclaw, Poland*, volume 9375 of *Lecture Notes in Computer Science*, pages 395–403. Springer, October 2015.
- [154] H.M. Wajeeh and S. Hameed. User authentication based on touch dynamics of pattern unlock. *International Journal of Computer Science and Mobile Computing*, 4(5):622–634, May 2015.
- [155] Y. Li, J. Yang, M. Xie, D. Carlson, H.G. Jang, and J. Bian. Comparison of pin- and pattern-based behavioral biometric authentication on mobile devices. In *Proc. of the 34th Military Communications Conference (MILCOM'15), Tampa, FL, USA*, pages 1317–1322. IEEE, October 2015.

- [156] M. Beton, V. Marie, and C. Rosenberger. Biometric secret path for mobile user authentication: A preliminary study. In *Proc. of the 1st World Congress on Computer and Information Technology (WCCIT'13)*, Sousse, Tunisia, pages 1–6. IEEE, June 2013.
- [157] A. Agrawal and A. Patidar. Smart authentication for smart phones. *International Journal of Computer Science and Information Technologies*, 5(4):4839–4843, August 2014.
- [158] M. Ganesh, P. Vijayakumar, and D. Jegatha. A secure gesture based authentication scheme to unlock the smartphones. In *Proc. of the 1st International Conference on Recent Trends and Challenges in Computational Models (ICRTCCM'17)*, Tindivanam, India, pages 153–158. IEEE, February 2017.
- [159] Q. Liu, M. Wang, P. Zhao, C. Yan, and Z. Ding. A behavioral authentication method for mobile gesture against resilient user posture. In *Proc. of the 3rd International Conference on Systems and Informatics (ICSAI'16)*, Shanghai, China, pages 324–331. IEEE, November 2016.
- [160] T. Nohara and R. Uda. Personal identification by flick input using self-organizing maps with acceleration sensor and gyroscope. In *Proc. of the 10th International Conference on Ubiquitous Information Management and Communication (IMCOM'16)*, New York, NY, United States, pages 1–6. ACM, January 2016.
- [161] P. Gasti, J. Šeděnka, Q. Yang, G. Zhou, and K. Balagani. Secure, fast, and energy-efficient outsourced authentication for smartphones. *IEEE Transactions on Information Forensics and Security*, 11(11):2556–2571, November 2016.
- [162] Niekverlaan. Hand swiping across a cellphone screen image. <https://www.goodfreephotos.com/business-and-technology/hand-swiping-across-a-cellphone-screen.jpg.php>, Good free photos. [Online; Accessed on 10/28/2021].
- [163] K. Baeza. Person holding white smartphone. <https://www.pexels.com/photo/person-holding-white-smartphone-141362/>, August 2016. [Online; Accessed on 10/28/2021].
- [164] J. Angulo and E. Wästlund. Exploring touch-screen biometrics for user identification on smart phones. In *Proc. of the 7th PrimeLife International Summer School, (PRIMELIFE'12)*, Trento, Italy, volume 375 of *IFIP Advances in Information and Communication Technology*, pages 130–143. Springer, September 2012.
- [165] J. Pan and W. Tompkins. A real-time qrs detection algorithm. *IEEE transactions on biomedical engineering*, 32(3):230–236, March 1985.
- [166] R.A.Á. Arturo, J.M. Penín, and X.A.V. Sobrino. A comparison of three qrs detection algorithms over a public database. *Procedia Technology*, 9(1):1159–1165, December 2013.
- [167] A. Thompson. Long qt syndrome part ii. <http://paramedicine101.blogspot.com/2009/07/long-qt-syndrome-part-ii.html>, July 2009. [Online; Accessed on 10/28/2021].
- [168] N. Karimian, Z. Guo, M. Tehranipoor, and D. Forte. Highly reliable key generation from electrocardiogram (ecg). *IEEE Transactions on Biomedical Engineering*, 64(6):1400–1411, June 2017.
- [169] 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, June 2001.
- [170] I. Jekova and G. Bortolan. Personal verification/identification via analysis of the peripheral ecg leads: Influence of the personal health status on the accuracy. *BioMed Research International*, 135676(1):1–13, October 2015.
- [171] 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*, 23(6):805–808, June 2016.
- [172] S. Ergin, A.K. Uysal, E.S. Gunal, S. Gunal, and M.B. Gulmezoglu. Ecg based biometric authentication using ensemble of features. In *Proc. of the 9th Iberian Conference on Information Systems and Technologies (CISTI'14)*, Barcelona, Spain, pages 1274–1279. IEEE, June 2014.
- [173] K.A. Sidek, V. Mai, and I. Khalil. Data mining in mobile ecg based biometric identification. *Journal of Network and Computer Applications*, 44(1):83–91, September 2014.
- [174] C. Camara, P.P. Lopez, and J.E. Tapiador. Human identification using compressed ecg signals. *Journal of Medical Systems*, 39(11):148:1–148:10, November 2015.
- [175] N.I.M. Nadzri, K.A. Sidek, and D.H.B. Wicaksono. Development of an electrocardiogram based biometric identification system: A case study in the university. *Journal of Telecommunication, Electronic and Computer Engineering*, 8(4):115–120, January 2016.

- [176] D. Rezgui and Z. Lachiri. Ecg biometric recognition using svm-based approach. *IEEJ Transactions on Electrical And Electronic Engineering*, 11(1):S94–S100, June 2016.
- [177] S. Keshishzadeh and S. Rashidi. Single lead electrocardiogram feature extraction for the human verification. In *Proc. of the 5th International eConference on Computer and Knowledge Engineering (ICCKE'15), Mashhad, Iran*, pages 118–122. IEEE, October 2015.
- [178] B. Pyakillya, N. Kazachenko, and N. Mikhailovsky. Deep learning for ecg classification. *Journal of Physics: Conference Series*, 913(1):012004:1–012004:5, September 2020.
- [179] F. Agrafioti and D. Hatzinakos. Fusion of ecg sources for human identification. In *Proc. of the 3rd International Symposium on Communications Control and Signal Processing (ISCCSP'08), Saint Julian's, Malta*, pages 1542–1547. IEEE, March 2008.
- [180] M. Tantawi, K. Revett, A.B. Salem, and M.F. Tolba. Electrocardiogram (ecg): A new burgeoning utility for biometric recognition. *Intelligent Systems Reference Library*, 70(1):349–382, June 2014.
- [181] J.R. Pinto, J.S. Cardoso, and A. Lourenço. Evolution, current challenges, and future possibilities in ecg biometrics. *IEEE Access*, 6(1):34746–34776, June 2018.
- [182] S.K. Cherupally, S. Yin, D. Kadetotad, G. Srivastava, C. Bae, S.J. Kim, and J. Seo. Ecg authentication hardware design with low-power signal processing and neural network optimization with low precision and structured compression. *IEEE Transactions on Biomedical Circuits and Systems*, 14(2):198–208, April 2020.
- [183] S. Yin, M. Kim, D. Kadetotad, Y. Liu, C. Bae, S.J. Kim, Y. Cao, and J. Seo. A 1.06 uw smart ecg processor in 65 nm cmos for real-time biometric authentication and personal cardiac monitoring. In *Proc. of the 31th Symposium on VLSI Circuits, Kyoto, Japan*, pages C102–C103. IEEE, June 2017.
- [184] A. Page, A. Kulkarni, and T. Mohsenin. Utilizing deep neural nets for an embedded ecg-based biometric authentication system. In *Proc. of the 10th IEEE Biomedical Circuits and Systems (BIOCAS'15), Atlanta, GA, USA*, pages 346–349. IEEE, October 2015.
- [185] J.S.A. Falconi, H.A. Osman, and A.E. Saddik. Ecg authentication for mobile devices. *IEEE Transactions on Instrumentation and Measurement*, 65(3):591–600, March 2016.
- [186] 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*, 23(6):805–808, June 2016.
- [187] Y. Chen and W. Chen. Finger ecg-based authentication for healthcare data security using artificial neural network. In *Proc. of the 19th International Conference on e-Health Networking, Applications and Services (HealthCom'17), Dalian, China*, pages 187–192. IEEE, October 2017.
- [188] AliveCor. Kardiamobile ekg monitor - instant ekg on your phone. <https://store.kardia.com/products/kardiamobile>, October 2020. [Online; Accessed on 10/28/2021].
- [189] K. Wiggers. AliveCor raises \$65 million to detect heart problems with ai. <https://venturebeat.com/2020/11/16/alivecor-raises-65-million-to-detect-heart-problems-with-ai/>, November 2020. [Online; Accessed on 10/28/2021].
- [190] Digital Health News. AliveCor raises \$65 million for remote cardiology platform. <https://mercomcapital.com/alivecor-raises-65-million-for-remote-cardiology-platform/>, November 2020. [Online; Accessed on 10/28/2021].
- [191] CardioID. Every heart has a beat, but the way we use it is unique! <https://www.cardio-id.com/>, December 2016. [Online; Accessed on 10/28/2021].
- [192] Nymi. Nymi workplace wearables. <https://www.nymi.com/nymi-band>, June 2021. [Online; Accessed on 10/28/2021].
- [193] A. Sacco. Nymi band uses your heartbeat to secure mobile payments. <https://www.cio.com/article/244782/nymi-band-uses-your-heartbeat-to-secure-mobile-payments.html>, August 2015. [Online; Accessed on 10/28/2021].
- [194] Vandrico Inc. The nymi band. <https://vandrico.com/wearables/device/nymi-band.html>, June 2020. [Online; Accessed on 10/28/2021].
- [195] F. Porée, G. Kervio, and G. Carrault. Ecg biometric analysis in different physiological recording conditions. *Signal, Image and Video Processing*, 10(2):10:267–10:276, January 2015.

- [196] J. Li, G. Deng, W. Wei, H. Wang, and Z. Ming. Design of a real-time ecg filter for portable mobile medical systems. *IEEE Access*, 5(1):696–704, October 2017.
- [197] D. Bansal S. Nayak, M.K. Soni. Filtering techniques for ecg signal processing. *International Journal of Research in Engineering & Applied Sciences*, 2(2):474–475, February 2012.
- [198] M. L. Ahlstrom and W.J. Tompkins. Digital filters for real-time ecg signal processing using microprocessors. *IEEE Transactions on Biomedical Engineering*, BME-32(9):708–713, September 1985.
- [199] S. Pongponsoi and X.H. Yu. Electrocardiogram (ecg) signal modeling and noise reduction using wavelet neural networks. In *Proc. of the 3rd IEEE International Conference on Automation and Logistics (ICAL'09)*, Shenyang, China, pages 394–398. IEEE, August 2009.
- [200] Q. Haibing, L. Xiongfei, and P. Chao. Discrete wavelet soft threshold denoise processing for ecg signal. In *Proc. of the the International Conference on Intelligent Computation Technology and Automation (ICICTA'10)*, Changsha, China, pages 126–129. IEEE, May 2010.
- [201] S. Pongponsoi and X.H. Yu. An adaptive filtering approach for electrocardiogram (ecg) signal noise reduction using neural networks. *Neurocomputing*, 117(1):206–213, October 2013.
- [202] W.S. Kang, S. Yun, and K. Cho. Ecg denoise method based on wavelet function learning. In *Proc. of the 11th IEEE SENSORS, Taipei, Taiwan*, pages 699–702. IEEE, October 2012.
- [203] M. Alfaouri and K. Daqrouq. Ecg signal denoising by wavelet transform thresholding. *American Journal of Applied Science*, 5(3):276–281, March 2008.
- [204] I. Tudosa and N. Adochiei. Lms algorithm derivatives used in real-time filtering of ecg signals: A study case on performance evaluation. In *Proc. of the 1st International Conference and Exposition on Electrical and Power Engineering (EPE'12)*, Iasi, Romania, pages 565–570. IEEE, October 2012.
- [205] Massachusetts Institute of Technology. Iir, fir filter structures. <https://ocw.mit.edu/courses/electrical-engineering-and-computer-science/6-341-discrete-time-signal-processing-fall-2005/lecture-notes/lec07.pdf>. [Online; Accessed on 10/28/2021].
- [206] Association for the Advancement of Medical Instrumentation. *Diagnostic electrocardiographic devices*. Advancing Safety in Health Technology, 2001.
- [207] L. Jack. Thermal noise analysis in ecg applications. <http://www.ti.com/lit/an/sbaa185/sbaa185.pdf>, May 2011. [Online; Accessed on 10/28/2021].
- [208] S.L. Lin, C.K. Chen, C.L. Lin, W.C. Yang, and C.T. Chiang. Individual identification based on chaotic electrocardiogram signals during muscular exercise. *IET Biometrics*, 3(4):257–266, December 2014.
- [209] P. Christ and U. Rückert. Identification of athletes during walking and jogging based on gait and electrocardiographic patterns. In *Proc. of the 6th International Biomedical Engineering Systems and Technologies (BIOSTEC'13)*, Barcelona, Spain, volume 452 of *Communications in Computer and Information Science*, pages 62–77. Springer, February 2014.
- [210] S. Wahabi, S. Pouryayevali, S. Hari, and D. Hatzinakos. On evaluating ecg biometric systems: Session-dependence and body posture. *IEEE Transactions on Information Forensics and Security*, 9(11):2002–2013, November 2014.
- [211] A.D.C. Chan, M.M. Hamdy, A. Badre, and V. Badee. Wavelet distance measure for person identification using electrocardiograms. *IEEE Transactions on Instrumentation and Measurement*, 57(2):248–253, February 2008.
- [212] I. Odina, P.H. Lai, A. Kaplan, J. O'Sullivan, E. Sirevaag, S. Kristjansson, A.K. Sheffield, and J.W. Rohrbaugh. Ecg biometrics: A robust short-time frequency analysis. In *Proc. of the 2nd IEEE International Workshop on Information Forensics and Security (WIFS'10)*, Seattle, WA, USA, pages 183–187. IEEE, December 2010.
- [213] J.M. Irvine, S.A. Israel, W.T. Scruggs, and W.J. Worek. eigenpulse: Robust human identification from cardiovascular function. *Pattern Recognition*, 41(11):3427–3435, April 2008.
- [214] S.C. Fang and H.L. Chan. Qrs detection-free electrocardiogram biometrics in the reconstructed phase space. *Pattern Recognition Letter*, 34(5):595–602, April 2013.
- [215] I. Jekova, V. Krasteva, R. Leber, R. Schmid, R. Twerenbold, C. Müller, and T. Reichlin R. Abacherli. Intersubject variability and intrasubject reproducibility of 12-lead ecg metrics: Implications for human verification. *Journal of Electrocardiology*, 49(6):784–789, December 2016.

- [216] M. Häggström. Precordial leads in ecg. https://commons.wikimedia.org/wiki/File:Precordial_leads_nECG.svg, September 2020. [Online; Accessed on 10/28/2021].
- [217] T.S. Lugovaya. Biometric human identification based on ecg. <https://physionet.org/physiobank/database/ecgiddb/biometric.shtml>, 2005. [Online; Accessed on 10/28/2021].
- [218] M. Kyoso and A. Uchiyama. Development of an ecg identification system. In *Proc. of the 23th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC'01), Istanbul, Turkey*, pages 3721–3723. IEEE, October 2001.
- [219] K.A. Sidek, I. Khalil, and M. Smolen. Ecg biometric recognition in different physiological conditions using robust normalized qrs complexes. In *Proc. of the 25th Computers in Cardiology (CinC'12), Krakow, Poland*, pages 97–100. IEEE, September 2012.
- [220] H. Silva, A. Lourenço, and A. Fred. In-vehicle driver recognition based on hand ecg signals. In *Proc. of the 20th ACM international conference on Intelligent User Interfaces (IUI'12), Lisbon, Portugal*, pages 25—28. ACM, February 2012.
- [221] T.W. Shen, W.J. Tompkins, and Y.H. Hu. One-lead ecg for identity verification. In *Proc. of the 15th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC'02), Houston, Texas, USA*, pages 62–63. IEEE, October 2002.
- [222] R. Palaniappan and S. M. Krishnan. Identifying individuals using ecg beats. In *Proc. of the 1st International Conference on Signal Processing and Communications, (SPCOM'04), Bangalore, India*, pages 569–572. IEEE, December 2004.
- [223] G. Wübbeler, M. Stavridis, D. Kreiseler, R.D. Bousseljot, and C. Elster. Verification of humans using the electrocardiogram. *Pattern Recognition Letters*, 28(10):1172—1175, July 2007.
- [224] M.M. Tawfik, H. Selim, and T. Kamal. Human identification using time normalized qt signal and the qrs complex of the ecg. In *Proc. of the 7th International Symposium on Communication Systems, Networks and Digital Signal Processing, (CNSDSP'10), Newcastle Upon Tyne, UK*, pages 755–759. IEEE, July 2010.

Author Biography



Jose-Luis Cabra López received the BSc. Eng. in Electronics Engineering in 2011 from the Universidad Nacional de Colombia, Colombia, and the MSc. in Electronics Engineering in 2015 from the Pontificia Universidad, Bogotá, Colombia. From 2020 to the current date, he is a full-time professor of the Telecommunication Engineering Department at the Fundacion Universitaria Compensar. Currently, he is pursuing his doctorate degree at the Pontificia Universidad Javeriana, Bogotá. His research interests include Real Time Operating Systems, Digital Electronics, Embedded Hardware & Firmware Design, IoT, Biomedical Embedded Systems, and Embedded Machine Learning.



Carlos Alberto Parra Rodríguez is a full professor in the Department of Electronics at the Pontificia Universidad Javeriana, Colombia. He is PhD from the Universite De Toulouse III (Paul Sabatier), Francia. Prof. Parra has experience in the application of data science in robotics, perception, intelligent systems, and real-time computer vision. He has published over fifty papers.



Diego Méndez Chaves is an associate professor in the Department of Electronics Engineering at the Pontificia Universidad Javeriana, Bogotá, Colombia. He received his PhD. (2012) and his MSc. (2011) in Computer Science from the University of South Florida, Tampa FL, USA, his ME. (2008) from the Universidad de Los Andes, Bogotá, Colombia, and his BSc. (2005) in Electronics Engineering from the Universidad Nacional, Bogotá, Colombia. Diego's research interests include Internet of Things (IoT), embedded systems, wireless sensor networks, participatory sensing, digital systems design, operating systems and high-level systems design.



Luis Carlos Trujillo Arboleda is an assistant professor in the Department of Electronics Engineering at the Pontificia Universidad Javeriana, Bogotá, Colombia. He received his MSc. (2005) in Telematics from the Universidad del Cauca, Cali, Colombia, his ME. (2008) from the Universidad de Los Andes, Bogotá, Colombia, and his BSc. (1992) in Electronics Engineering from the Universidad del Cauca, Cali, Colombia. Currently he is the general manager of the CEA-IoT. His research interests include Internet of Things (IoT), wireless sensor networks, network design and software defined networks.