International Journal of Mobile Computing and Multimedia Communications
Volume 14 • Issue 1

Biometric Authentication Methods on Mobile Platforms:

An Introduction to Fingerprint Strong Feature Extraction

Agnitè Maxim Wilfrid Straiker Edoh, University of Abomey-Calavi, Benin*
Tahirou Djara, University of Abomey-Calavi, Benin
https://orcid.org/0000-0002-8591-6610
Abdou-Aziz Sobabe Ali Tahirou, University of Abomey-Calavi, Benin
Antoine Vianou, Université d'Abomey-Calavi, Benin

ABSTRACT

In this work, the authors propose a new biometric authentication system on mobile devices, enhancing security at these terminals and preserving user privacy. The proposed system uses a method of extracting strong features from minutiae with refinement of the method with regard to the further elimination of false minutiae by the calculation of geometric information (orientations and distances between minutiae) to obtain true terminations and stronger bifurcations facilitating the recognition of individuals. A series of tests carried out using a recognition and authentication application allowed us to achieve a false rejection rate of 13.81% and a false acceptance rate of almost zero (0.021%). The authors also propose a security model using hash functions and a random number to make the recognition system revocable, more difficult to compromise and thus reducing the risk of usurpation.

KEYWORDS

Biometric Authentication, Fingerprint, Minutiae Extraction, Mobile Devices, Recognition, Strong Features

INTRODUCTION

With the current digitization of most administrative services, e-government, mobile payments, remote healthcare, the advent of COVID 19 where exchanges must be done mostly online and so on, and because of the large number of identity-theft cases, the authentication step is often considered the weakest link in computer security (Belguechi, 2015). For the authentication of an individual, the password is by far the most widespread method despite its obvious lack of security (password cracker, eavesdropping, etc.) and its very limited ease of use when the user wishes to access a multitude of services (use of several passwords for several applications).

DOI: 10.4018/IJMCMC.334130 *Corresponding Author

Biometric authentication, which is used to recognize an individual based on physiological or behavioral characteristics, is an interesting alternative. For example, it is extremely rare to lose one's fingerprints, unlike passwords. It is also easier for users to put their fingers on a sensor or to capture their faces than to enter a password. As far as smartphones are concerned, the means of biometric authentication are various, such as fingerprints, facial captures, graphic patterns, voice, gait, or even keyboard speed. However, users are not usually aware that they are storing their enduring physiological or behavioral characteristics on unsecured platforms (i.e., on cell phones or cloud storage), threatening the privacy of their biometric patterns and identities.

In recent years, biometric authentication has attracted much attention from academics and industries. The more people trust biometric authentication systems, especially on their personal devices such as smartphones, the more they reveal their identities to third parties. Due to the enduring characteristics of biometrics such as fingerprints, face, or behavioral traits, the increasing use of biometrics will increase the risk of identity theft. Therefore, secure, robust, privacy-preserving authentication systems are required to prevent unauthorized access to sensitive and personal information stored on mobile devices.

The main objective of this work is to strengthen biometric authentication methods on mobile phones, particularly by fingerprint. This objective has two sub-objectives: to provide methods to avoid identity theft with regard to fingerprint authentication and to strengthen authentication to avoid information leakage from the biometric model.

In this work, we present a novel privacy-preserving biometric authentication system for mobile users. The proposed system, unlike other research efforts, leverages the hardware security of smartphones and demonstrates its potential for secure authentication with faster and more accurate performance and low resource consumption. This work makes the following contributions: a new strong-minutiae extraction method for the elimination of false minutiae and completeness of the security model of authentication of mobile platforms by fingerprint by proposing a secure authentication system based on the strong-characteristics method and encryption using a random number and hash functions for information transformation after studying some of the authentication schemes used in the mobile-device domain for secure and fast authentication with respect to fingerprints.

LITERATURE REVIEW

Traditional Authentication Methods on Mobile Devices

The most popular authentication methods are PIN and password, pattern-lock, and physiological authentication.

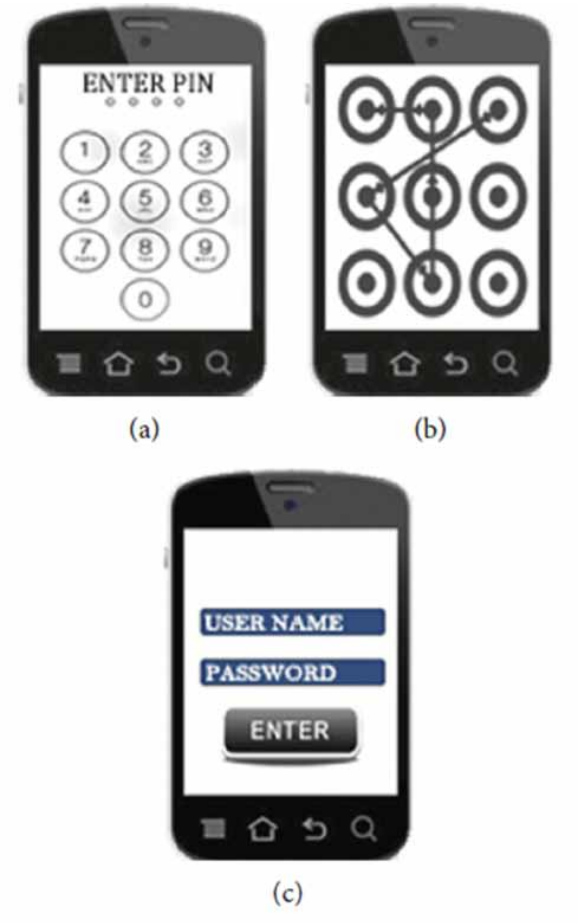
Password and PIN Authentication

A major difference between desktop and mobile authentication is that mobile users are not restricted to a particular location and settings; therefore, users are free to use their mobile devices to access and use password-protected services (e.g., online banking and email services) anytime and anywhere (Maydebura et al., 2013). In the process of these authentications, user credentials are verified at the beginning of the session. If the verification is successful (e.g., the correct password or PIN is entered), access is granted; otherwise, access is denied (Fig. 1). The session remains valid until the user logs out or closes the session.

Pattern-Lock Authentication

Pattern-based authentication is also a popular form of authentication on many mobile devices today. These authentication methods involve a user entering a pattern in order to authenticate. This typically involves connecting dots to complete the pattern, as shown in Fig. 1. If the wrong pattern is entered, the device will not authenticate the user, and if the pattern is increasingly incorrect, the device uses a

Figure 1. Biometric Authentication Methods on Mobile Devices (a) PIN code, (b) graphic scheme, and (c) password (Gupta et al., 2018)



pushback to retry entering the password after an increasingly long period of time. There are a number of rules that must be followed when using this method, including: (1) a pattern must consist of at least four points; (2) each point can only be visited once; and (3) a previously unvisited point will become visited if it is part of a horizontal, vertical, or diagonal line segment of the pattern.

Physiological Authentication

- **Fingerprint Authentication:** Authentication via fingerprints works because our fingers are made up of ridges and valleys on the surface of the finger that are unique to each human being (Uddin et al., 2011). It is this uniqueness of fingerprints that makes the use of fingerprint readers a viable biometric to use. Touchscreen devices such as smartphones and tablets allow fingerprints to be used or at least measure the size and shape of any part of the fingers in contact with the screen as a method of authentication. Biometric fingerprint authentication has attracted the most attention and is deployed mainly in mobile devices. This may be due to the convenience fingerprint authentication. One of the biggest problems with this authentication is fingerprint forgery.
- **Face-Recognition Authentication:** Faces are the most recognizable features of human biometrics. Facial recognition is popular because the hardware required for facial recognition is relatively cheaper than other biometric technologies such as iris scanning, making it a viable authentication

technique for mobile devices. Facial recognition meets efficiency criteria such as usability, security, and availability. It's easy to use, has a relatively high recognition rate, and does not require immense computer hardware to use (Vazquez-Fernandez and Gonzalez-Jimenez, 2016). However, facial recognition, as practical as it is, is subject to certain attacks. For example, an attacker can simply use a photo or video of the person they seek to attack and can gain unauthorized access to the user's device. This threat is increased with the availability of photos from social media sites like Facebook and Twitter (Vazquez-Fernandez and Gonzalez-Jimenez, 2016).

- **Voice-Recognition Authentication:** Voice recognition is also an authentication means that can be used on mobile devices. There are two main factors to consider for speech recognition to be used in authentication, which are the physiological component, known as the vocal tract, and the behavioral component, known as the vocal accent (Uddin et al., 2011). The advantages of speech recognition include the relative ease of installation and the minimal requirements (hardware and software) to use it. The only special equipment needed to make it work is a microphone. For voice recognition to be more secure, there are factors that come into play such as the performance of users when recording their voices. The ability to record the voices of authorized users can be used to try to bypass a speech recognition system (Shen et al., 2018).
- **Iris-Recognition Authentication:** Iris recognition is a biometric form of recognition in which an individual's iris is scanned in order to verify a user's identity. This is made possible because, like fingerprints, the iris has a unique pattern for each individual and also because the characteristics of the iris are extremely complex and random (Gragnaniello et al., 2015). Another benefit of iris recognition is that the iris is relatively unaffected by aging, making it a very viable form of authentication.

Iris recognition on mobile phones is different from conventional iris recognition in that once iris recognition is performed on mobile devices, factors such as the computing power of the mobile device, the space to place the LED illuminator, and the iris to be authenticated come into play (Kim et al., 2016). These problems can be solved in several ways, such as using fast eye-detection algorithms and using dedicated hardware to better detect the iris.

Mobile iris-recognition systems can be divided into three main categories: systems using dedicated devices to perform iris recognition, systems connecting additional hardware to the mobile device, and systems attaching a near-infrared (NIR) camera with illuminators (Kim et al., 2016). These near-infrared cameras are powerful devices that can capture iris images with sharp spectral patterns, even from dark-colored irises (Jung et al., 2017).

Behavioral Authentication Methods

- **The Gait:** This recognition technique is relatively new and relies on measuring and analyzing how an individual walks or runs using the acceleration signals produced by their mobile device. The gait feature lends itself to smartphones because of their built-in sensors, namely, accelerometer, gyroscope, and magnetometer. The main advantage of this technique is that it can be applied to the continuous authentication of users without requiring their intervention. However, factors such as the change in orientation of the device during walking (Muaaz and Mayrhofer, 2014), uneven ground, injuries, shoes, fatigue, and personal particularities may affect its accuracy (Murmuria et al., 2015).
- **Touch Gestures:** Touch gestures are hand-drawn shapes on the touchscreens of mobile devices that consist of single or multiple touches. Each key is a series of successive numerical coordinates. Characteristics such as direction and duration of touch, speed, and acceleration of movement are analyzed and measured alone or in combination with each other.

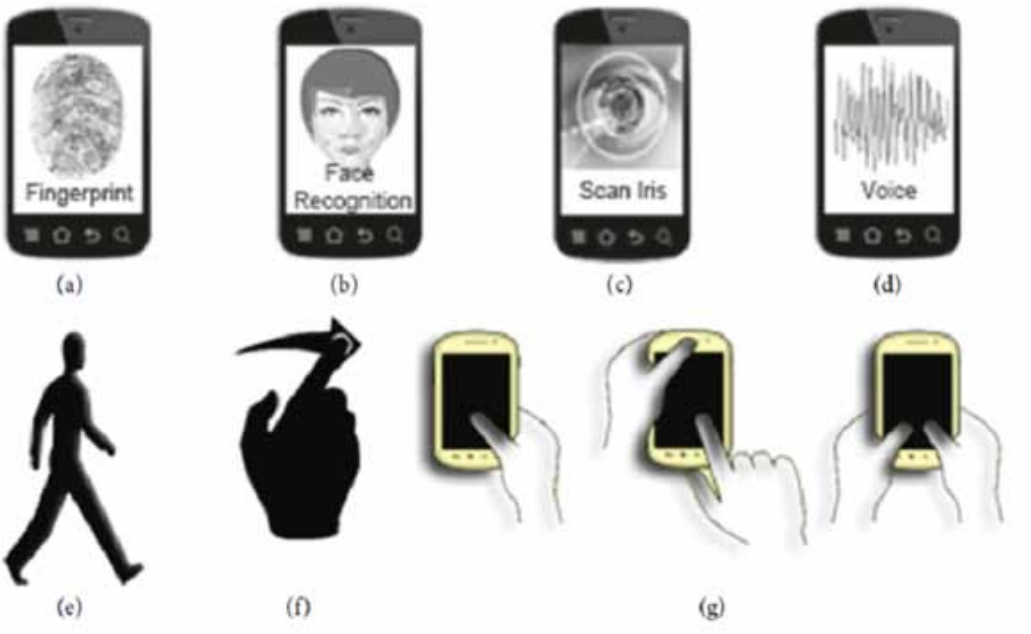
- **Keyboarding Dynamics:** We called typing dynamics the procedure of recording an individual's keyboard entries on a mobile device and the effort to identify them via analysis based on their typing habits (Mahfouz et al., 2017; Chang et al., 2016).
- **Behavioral Profile:** Mobile device usage data can be used for behavioral authentication of individuals on the basis that they generally follow a specific pattern when using their phone to interact with digital applications and services (Stylios et al., 2015). A user's behavioral profile can be constructed based on their interaction either with a network or with a host. In the first case, the behavior of users is monitored with regard to their connection patterns to Wi-Fi networks, service providers, etc., while in the second case, monitoring refers to the way of using applications in different places and at different times (Alzubaidi and Kalita, 2016).
- **Hand Waving:** Using the waving pattern of an individual's wrist, while interacting with their mobile phone or simply holding it, to identify users has recently attracted attention. This method does not require any additional action from the user besides holding the device. Several features can be used, such as wrist twist, speed, range, and wave frequency. Individuals can be distinguished since the hand gesture is different.

Figure 2 represents most biometric authentication methods on mobile devices.

PIN-Code, Password, and Graphic-Schemes Authentication

According to one report (Winnick, 2023), average smartphone users engage in 76 separate phone sessions per day, while heavy users (the top 10%) peak at up to 132 sessions per day. PINs, passwords, or graphical templates require users to memorize their previously set text to unlock their devices each time they want to initiate a session. Users encountered problems in remembering their passwords and, more specifically, in remembering multiple passwords correctly. This encouraged users to choose a simple or easy-to-remember password, but that opens many opportunities for attackers to guess

Figure 2. Various types of authentication methods: (a) Fingerprint, (b) face, (c) iris, (d) voice, (e) gait, (f) screen swipe, and (g) screen touch (Gupta et al., 2018)



or decrypt their passwords easily. When the system enforces strict password policies, users, due to memorization issues (Komanduri et al., 2011), allow their browsers or password managers to save their username/password information for easy future logins. However, users who trust their browsers or password managers are more susceptible to a wide variety of attacks (Bonneau et al., 2012; Silver et al., 2014). Overall, 82% of end users are frustrated with password management (Bhattasali et al., 2014). This clearly indicates the lack of usability, and, as a result, nearly 75 million smartphone users in the United States do not use any PINs, templates, or passwords because they consider them annoying and a barrier to quick access to their smartphones.

From a security perspective, PINs and passwords are vulnerable to various attacks such as guessing (Katsini et al., 2016), since some users choose their date of birth (Bonneau et al., 2012) or simple numbers (1111, 2222, etc.) (Thorpe, 2008) to set up their PIN. Alternatively, 40% of Android users prefer graphical patterns for unlocking the device. However, this approach requires users to remember the pattern; therefore, users choose simple and less secure templates. For example, if users connect at least four dots without repeating any of them in their templates, the maximum number of combinations is 389,112, which could be easily decrypted by brute force (Mali and Londhe, 2018). Ye et al. (2017) were able to decrypt 95% of 120 unique patterns collected from 215 independent users in only five attempts by recording their smartphone screens remotely while they unlocked their devices. Moreover, these patterns are more vulnerable to over-the-shoulder surfing than text-based passwords. Mehrnezhad et al. (2016) demonstrated the recovery of the entered PIN or password from the collected sensory data while the users were entering them. They installed PINlogger.js, a JavaScript-based side-channel attack that is capable of recording motion and orientation sensor streams without requiring user permission. The attack resulted in 94% accuracy in retrieving the correct PIN in just three rounds of testing.

Similarly, Sarkisyan et al. (2015) demonstrated an approach to exploit the motion sensors of smartwatches to retrieve entered PINs. They infected the smartwatches with malware to access the smartwatch motion sensors and the users' inferred activities and PINs. In a controlled scenario, the authors obtained PINs in five guesses with at least 41% accuracy using a random forest classifier on a dataset of 21 users.

Physiological-Biometrics Authentication

Mobile device manufacturers are increasingly integrating biometric sensors into their flagship smartphones for reliable and convenient user authentication with the intuition that biometric approaches are better than their conventional authentication schemes. For example, Apple, Huawei, Lenovo (currently owned by Motorola), Nokia (currently owned by Microsoft), Samsung, and many other major manufacturers have integrated fingerprint sensors, iris scanners, and facial-recognition algorithms into some of their high-end devices. These advances are akin to replacing a hay castle with a glass house to ward off attacks from sophisticated cyber hackers. Physiological biometrics are commonly used as single- or multi-factor/multi-model authentication schemes (in combination with other modalities) for smartphones.

Unexpectedly, biometric schemes have been found to be vulnerable to different types of attacks, e.g., spoofing, replay attacks, and escalation attacks (Bolle et al., 2013), exposing their security flaws. These schemes suffer from their data leakage; that is, a user's face can be easily found on social-media websites or their fingerprints can be extracted from photos based on their gestures, to mount a presentation attack (Ramachandra and Busch, 2017) against them. Recent research has shown that these systems can be hacked very easily with almost negligible investment and effort. For example, the iPhone X's Face ID was hacked with a 3D printed mask costing only about $150 (Titcomb, 2017), while the Samsung Galaxy S8's facial-recognition technology was duped simply with a photo of the owner (Kovach, 2017).

Similarly, the German Chaos Computer Club cracked the Samsung Galaxy S8's iris scanner (Hern, 2017) with a dummy eye made from photos of the iris, taken by a digital camera in night

mode, and covered it with a contact lens to match the curvature of the iris, less than a month after the launch of the S8. The same club had previously hacked the fingerprint sensor protection of the iPhone 5s within two days of the device going on sale worldwide (Charles, 2013). Their hacking team photographed the glass surface containing a user's fingerprint and created a fake fingerprint using thin film to unlock the phone. Japan's National Institute of Informatics (NII) researcher Isao Echizen (McGoogan, C., and Demetriou, D., 2017) (McGoogan, C., and Demetriou, D, 2017) demonstrated that fingerprints can easily be recreated from photos, taken from only three meters away, without using a sophisticated process and warned that casually making a peace sign in front of a camera could result in fingerprint theft.

Behavioral-Biometrics Authentication

Gait recognition is a process of identifying or verifying individuals based on their walking style. In clinical applications, the human gait has already been used for studies related to a person's health, and nearly 25 key gait patterns have been detected using different techniques such as image processing, floor sensors, and sensors placed on the body (Muro-De-La-Herran et al., 2014). Recently, smartphones and wearable devices have also started using it for authentication purposes (Welten, 2013). Since users are not required to perform explicit interaction with their devices, the walking modality can be collected unobtrusively, making it practical for a user-friendly access system (Muaaz and Mayrhofer, 2017).

Muaaz and Mayrhofer (2017) evaluated the security strength of a smartphone-based gait-recognition system against effortless and minimal live impersonation attacks in realistic scenarios and achieved an equal error rate (EER) of 13% on a dataset of 35 participants. However, additional testing is needed to verify robustness against impersonation attacks. Murao et al. (2015) proposed a grip-based authentication solution that profiles grip gestures using pressure sensors mounted on the sides and back of a smartphone and achieves an EER of 2%. In a study by Saevanee et al. (2012), unimodal systems, namely behavioral profiling, keystroke dynamics, and language profiling, were found to be less accurate; they yielded EERs of 20%, 20%, and 22%, respectively.

METHOD

Proposed Strong-Feature Extraction Method for Secure and Fast Fingerprint Authentication

The strong-feature extraction method is based on the selection of a strong feature—in this case, good-quality fingerprint images. Good-quality fingerprint images have a clear pattern of ridges and valleys; however, poor-quality fingerprint images have no easily distinguishable patterns. Poor-quality images result in spurious and missing features, degrading the performance of the overall system. An example of a poor-quality feature is abnormal ridges that are too close or too far apart. A block containing well-defined or high-quality ridges will have a considerably wider range of pixel intensities because there will be pixels ranging from bright in the middle of valleys to dark in the middle of ridges. Strong features are high-quality features that can be easily distinguished from other features in the biometric raw images.

Strong minutiae are obtained from fingerprint images and can be useful for secure and fast fingerprint authentication. To obtain them, eight fingerprint images of the same finger are recorded. These prints will have differences in finger placement (different vertical position, pressure of the finger against the sensor, degrees of skin distortion, rotation, humidity) that are taken into account in the FVC2004-DB4 fingerprint database (that we used in this paper) through the development of optical equipment.

Then, among these, we choose a reference impression whose image has the best quality and/or whose details are clearly visible. A number is then assigned to each minutia of the reference fingerprint (from 1 to the total number of minutiae of the fingerprint). The next step in this process is to find

the matched minutiae between the reference fingerprint and the other fingerprints. In doing so, for each minutia matched between the reference fingerprint and another fingerprint, we add one point to the score of the minutia number of the fingerprint. So if we have eight fingerprint impressions for each finger, we compare them seven times with each other, and each minutia of the reference fingerprint has a score from 1 to 8. Finally, with the number of points obtained for each minutia, one can determine the occurrence rate of the minutiae. Depending on whether the minutia is present on one, two, three, four, or even all eight prints, we obtain 50% strong, 63% strong, 75% strong, 88% strong, or 100% strong minutia. The higher this percentage, the stronger the minutia. Fig. 3 shows the overall process of extracting strong minutiae.

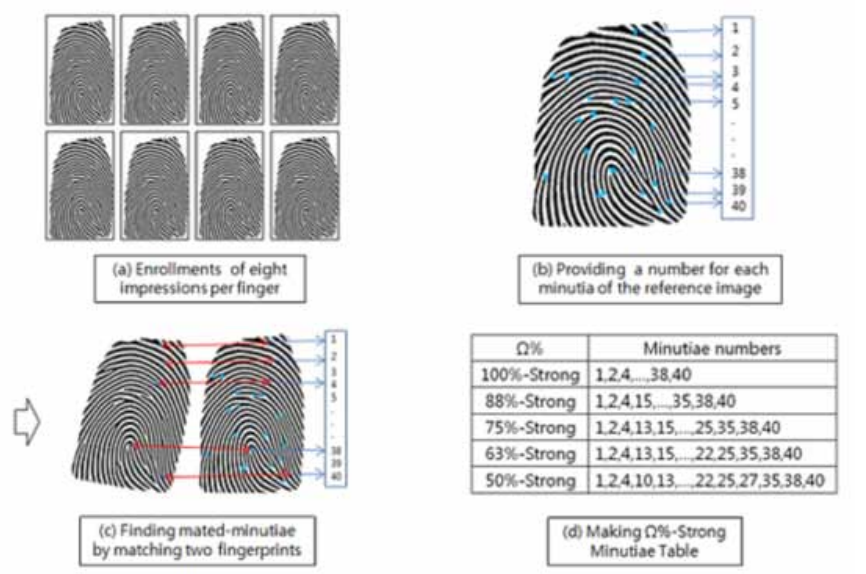
The process extracts from fingerprint images the most distinguishable and strong features of the minutiae. The strong features are the results of the *(w-k)Select* algorithm proposed by Han (2015), which is illustrated in Algorithm 1.

Here, w is the number of input fingerprint images and k is the minimum number of trials to find the features. F is the set of *(w-k)* strong features.

Algorithm 1

The (w-k)Select *Algorithm Specification*
Input: fingerprint samples ($\beta_1,\ldots,\beta_w$), w, k
Output: the strong features F
1: $k_i = 0$ ($i = 1,\ldots,N$) // N is the number of all features of original fingerprint β
2: for $j \leftarrow 1$ to w
3: ($f_1,\ldots,f_N$)←Find(β_j) //Find strong fingerprint features
4: for $i \leftarrow 1$ to N
5: if f_i exists then k_i++
6: $F \leftarrow f_i$ has k_i such that $k_i \geq k$
7: return F

Figure 3. Overall process of extracting strong minutiae (Han, 2015)



Ω%	Minutiae numbers
100%-Strong	1,2,4,....,38,40
88%-Strong	1,2,4,15,....,35,38,40
75%-Strong	1,2,4,13,15,....,25,35,38,40
63%-Strong	1,2,4,13,15,....,22,25,35,38,40
50%-Strong	1,2,4,10,13,....,22,25,27,35,38,40

The geometric information G, $G = \left(d_1,\ldots,d_{n-1},a_1,\ldots,a_{n-1}\right)$, consists, for example, of the distances (d_1,d_2,d_3,d_4) and the angles (a_1,a_2,a_3,a_4) between the strong features (F_1,F_2,F_3,F_4,F_5) that are the geometric information of five minutiae. Minutiae values are actual authentication data used in user verification. The original minutiae values M are $M = \left(m_1,\ldots,m_n\right)$. The fingerprint template proposed by Han is as follows:

$$FingTemp = \left(G \| M\right) \cdot \left(\| : binary\ \ concatenation\right)$$

Inspired by Han's model, our security model is given in Fig. 4.

We have proposed a scheme in which we simply use *Temp* and the random number a.

Enrollment

Given a security parameter k, let p be a prime number. The enrollment algorithm chooses a random number $a \in Z_p^*$ and hash functions H_1: $\{0,1\}^* \rightarrow Z_p^*$ and H_2: $Z_p^* \rightarrow \{0,1\}^k$. On enrollment, the steps are:

1. Calculate M from *Temp*, $M_{h1} = H_1(M)$.
2. Calculate $M' = M_{h1} \oplus a$. ($\oplus$: exclusive or XOR).
3. Calculate $a_{h2} = H_2(a)$.

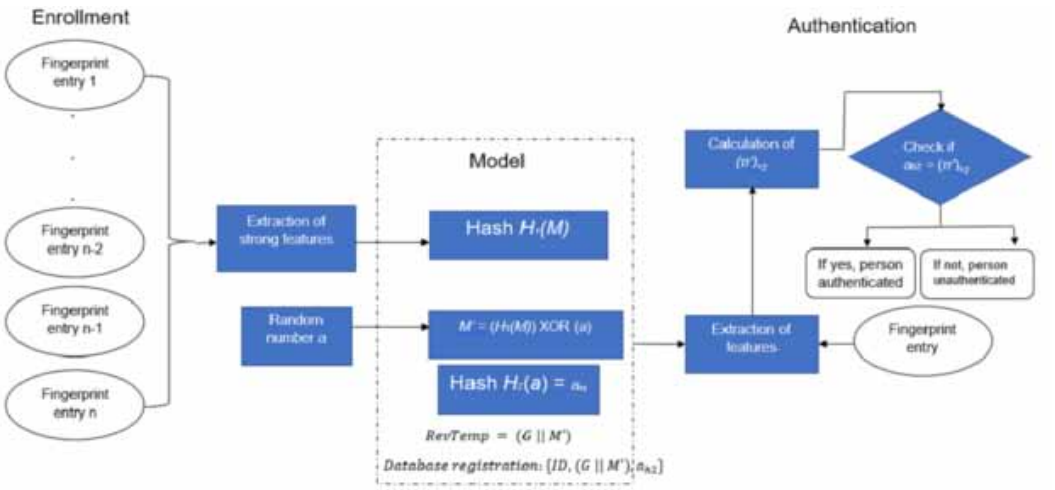
The randomized minutiae M' are taken to make a revocable template. The revocable model is $RevTemp = (G \| M')$.

If a user's ID is necessary for authentication in the device, *ID*, *RevTemp*, and a_{h2} are stored in a database as follows: Database registration: $\{ID, (G \| M'), a_{h2}\}$.

Authentication

The set of minutia values π of a person obtained from a scanner is sent to the authentication algorithm. At authentication, the steps are:

Figure 4. Our proposed security model



1. Calculate $\pi_{h1} = H_1(\pi)$.
2. Calculate $\pi' = \pi_{h1} \oplus M'$.
3. Calculate $(\pi')_{h2} = H_2(\pi')$.
4. If $(\pi')_{h2} = a_{h2}$, then the user is authentic; otherwise, they are not.

Each time user enrollment is implemented, the random number a is a different value, which is then used to transform the minutia information M differently. In short, the random number a is used as a one-time password, which adds a high level of security to the proposed authentication scheme. We can say that our one-time password-based authentication scheme is secure. The *(w-k)Select* algorithm produces strong features of a certain probability. Because we use only partial fingerprint characteristics, even when information is lost, the user's fingerprint data are safe.

Using an error-correction method as simple as quantification or normalization, we were able to compare the fingerprints with each other.

RESULTS

Implementation of Strong-Feature Algorithm on FVC2004 Database

Applying the strong-feature algorithm to one of the fingerprints of the FVC2004 fingerprint database gives us Fig. 5.

The number of minutiae has clearly decreased, so after the extraction of strong features, we have a selection of minutiae that have a high probability of being found on several fingerprint impressions of the same finger.

By using hash functions resistant to tampering (the slightest modification of the message results in a different hash value) and collisions (it should be impossible to find two different messages that produce the same hash value) for our authentication, we obtain a system with an almost zero FAR (0.021%) for a slightly high FRR (13.81%). That is to say, any fingerprint unknown to the system will certainly be rejected by the latter, but the downside is that even verified users may not be recognized during authentication.

Figure 5. Extraction of minutiae (left) and extraction of strong features (right)

Table 1. Error Rate According to Number of Strong Minutiae

Number of strong minutiae	FAR	FRR
1	-	-
2	-	-
3	0	0.00746269
4	0	0.05376344
5	0	0.09278351
6	0	0.13636364
7	0	0.16666667
8	0	0.19900498
9	0	0.23696682
10	0	0.28571429
11	0	0.32258065
12	0	0.36
13	0	0.38277512
14	0	0.42307692
15	0	0.45631068

Note: FAR is false acceptance rate; FRR is false rejection rate.

DISCUSSION

With a threshold setting, we can retrieve features with only a certain percentage. Here we took a threshold of 0.7 (70%), so we retrieved the characteristics having a percentage greater than or equal to 70%. We found that from 200 bifurcations we went to 63 and from 51 terminations we went to 9. For this experiment, we determined 100% strong minutiae when all eight fingerprints had the same minutiae, 88% strong minutiae when seven prints had the same minutiae, 75% strong minutiae with six prints, 63% strong minutiae with five, and 50% strong minutiae with four. These results are significant, given that these FVC2004 DB4 fingerprints were created for a worldwide fingerprint authentication system competition. Therefore, through this experiment, we have demonstrated how strong minutiae can be extracted using Han's method.

As shown by our experimental results, we expect 100% strong minutiae to be achieved with a proper process to register fingerprints. Moreover, we know that our information G is the information of the relative distances d_i $(1 \leq i \leq n)$ and the angles a_i $(1 \leq i \leq n)$ between the strong features. When G is compromised by an attack, the old G can be revoked and a new fingerprint template with a new G can be enrolled, which means that other strong features will be selected for this new template.

The datasets in Table 2 show the average runtime of our application on different fingerprints of the database according to the number of minutiae.

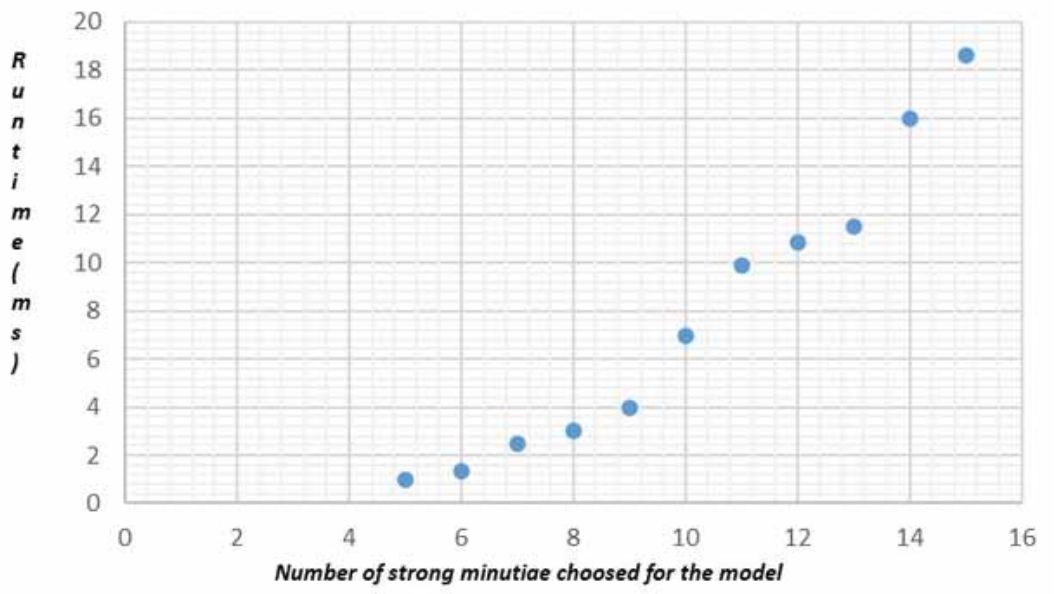
In Fig. 6, we note that the more the number of minutiae chosen increases, the more the execution time of the program also increases.

In France, the judicial system considers that it takes 12 minutiae sufficiently close to the original to declare that two fingerprints match. Overall, this figure fairly well represents the average in Europe. In the United States, on the other hand, it is set at eight (Raspberry Pi FR, 2023). On average, the execution time of our application varies between 1 ms and 20 ms at most (for 5 to 15 strong minutiae) compared to four other algorithms (The Secure Enclave for Apple iPhone X, Samsung Exynos 64-bit octa-core Secure Processor for Samsung Galaxy S9, Google Pixel Imprint for Google Pixel 3, Kirin 980 NPU

Table 2. Datasets of the runtime of our application according to the number of strong minutiae

Number of Minutiae	Average Runtime (in Milliseconds)
5	4.51932556
6	5.68706989
7	6.28604889
8	7.00606667
9	8.70168209
10	10.0565195
11	14.1998291
12	15.6626225
13	18.8696384
14	22.4766493
15	26.0155678

Figure 6. Runtime of our application according to the number of strong minutiae chosen



for Huawei Mate 20 Pro) whose average runtime is between 0.2 and 0.4 s (Table 3). This proves the performance of our application based on the strong feature algorithm (the algorithms whose execution time is compared being those of mobile devices considered to be high-end models with powerful processing chips).

Please note that these values are given as an indication and based on hypothetical estimates, so they may vary depending on the conditions of use of the device and other factors such as the size of the database, the quality of the prints, and the computing power of the device used.

Table 3. A few matching minutiae algorithms and their average runtimes

Matching Minutiae Algorithms	Average Runtime
Fingerprint Verification SDK (Software Developer's Kit)	0.1 to 1 second
VeriFinger SDK	0.2 to 1 second
DigitalPersona	0.1 to 0.5 second
Touch N Go	0.1 to 0.5 second
The Secure Enclave (Apple)	0.3 second
Samsung Exynos 64-bit octa-core Secure Processor	0.2 second
Google Pixel Imprint	0.4 second
Kirin 980 NPU	0.3 second
Our Algorithm	0.004 to 0.1 second

CONCLUSION AND PERSPECTIVES

Starting from the conventional authentication methods, we enumerated the biometric authentication methods on mobile platforms and specified the probable attacks and shortcomings of the different methods. Then we explained the proposed method, which is the extraction of strong features from fingerprint images and which will be useful to build bit strings from a fingerprint.

A series of tests carried out using a recognition and authentication application allowed us to achieve a false rejection rate of 13.81% and a false acceptance rate of almost zero (0.021%).

The average execution time (user authentication by fingerprint) of our application compared to some mobile devices considered high-end current models with powerful processing chips showed that our application's speed is average and therefore quite efficient.

With this revocable model and the simple binary operations used (not taking too much space to execute on the device used) in the study model, the authentication method is secure and fast and thus suitable for mobile platforms. In the future, we plan to realize a web application in real time and why not on a chip of real mobile devices to better evaluate the performance of our model against existing systems.

Although our proposed method is also applicable to other resource-constrained devices, biometric authentication on internet-of-things devices can be studied in the future to evaluate its performance and show its limits.

REFERENCES

Alzubaidi, A. A., & Kalita, J. K. (2016). Authentication of smartphone users using behavioral biometrics. *IEEE Communications Surveys and Tutorials*, *18*(3), 1998–2026. doi:10.1109/COMST.2016.2537748

Belguechi, R. O. (2015). *Sécurité des systèmes biométriques: Révocabilité et protection de la vie privée*. [Doctoral thesis, Higher National School of Computer Science]. HAL Theses.

Bhattasali, T., Saeed, K., Chaki, N., & Chaki, R. (2014). A survey of security and privacy issues for biometrics based remote authentication in cloud. In K. Saeed & V. Snášel (Eds.), *Computer information systems and industrial management* (pp. 112–121). Springer. doi:10.1007/978-3-662-45237-0_12

Bolle, R. M., Connell, J. H., Pankanti, S., Ratha, N. K., & Senior, A. W. (2013). *Guide to biometrics*. Springer. doi:10.1017/S0263574704221130

Bonneau, J., Preibusch, S., & Anderson, R. (2012). A birthday present every eleven wallets? The security of customer-chosen banking PINs. In A. D. Keromytis (Ed.), *FC 2012: Financial Cryptography and Data Security* (pp. 25–40). Springer. doi:10.1007/978-3-642-32946-3_3

Chang, T. Y., Tsai, C. J., Tsai, W. J., Peng, C. C., & Wu, H. S. (2016). A changeable personal identification number-based keystroke dynamics authentication system on smart phones. *Security and Communication Networks*, *9*(15), 2674–2685. doi:10.1002/sec.1265

Charles, A. (2013, September 23). iPhone 5S fingerprint sensor hacked by Germany's Chaos Computer Club. *The Guardian*. https://www.theguardian.com/technology/2013/sep/22/apple-iphone-fingerprint-scanner-hacked

Gragnaniello, D., Sansone, C., & Verdoliva, L. (2015). Iris liveness detection for mobile devices based on local descriptors. *Pattern Recognition Letters*, *57*, 81–87. doi:10.1016/j.patrec.2014.10.018

Gupta, S., Buriro, A., & Crispo, B. (2018). Demystifying authentication concepts in smartphones: Ways and types to secure access. *Mobile Information Systems*, *2018*(Special Issue), 1–16. doi:10.1155/2018/2649598

Han, J. (2015). Fingerprint authentication schemes for mobile devices. [IJECE]. *Iranian Journal of Electrical and Computer Engineering*, *5*(3), 579–585. doi:10.11591/ijece.v5i3.pp579-585

Hern, A. (2017, May 23). Samsung Galaxy S8 iris scanner fooled by German hackers. *The Guardian.* https://www.theguardian.com/technology/2017/may/23/samsung-galaxy-s8-iris-scanner-german-hackers-biometric-security

Jung, Y., Kim, D., Son, B., & Kim, J. (2017). An eye detection method robust to eyeglasses for mobile iris recognition. *Expert Systems with Applications*, *67*, 178–188. doi:10.1016/j.eswa.2016.09.036

Katsini, C., Belk, M., Fidas, C. A., Avouris, N. M., & Samaras, G. (2016). Security and usability in knowledge-based user authentication: A review. In *Proceedings of the 20th Pan-Hellenic Conference on Informatics* (p. 63). ACM. doi:10.1145/3003733.3003764

Kim, D., Jung, Y., Toh, K. A., Son, B., & Kim, J. (2016). An empirical study on iris recognition in a mobile phone. *Expert Systems with Applications*, *54*, 328–339. doi:10.1016/j.eswa.2016.01.050

Komanduri, S., Shay, R., Kelley, P. G., Mazurek, M. L., Bauer, L., Christin, N., Cranor, L., & Egelman, S. (2011). Of passwords and people: Measuring the effect of password-composition policies. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 2595–2604). ACM. doi:10.1145/1978942.1979321

Kovach, S. (2017, March 31). Samsung's Galaxy S8 facial recognition feature can be fooled with a photo. *Business Insider*. https://www.businessinsider.com/samsung-galaxy-s8-facial-recognition-tricked-with-a-photo-2017-3

Mahfouz, A., Mahmoud, T. M., & Eldin, A. S. (2017). A survey on behavioral biometric authentication on smartphones. *Journal Information Security and Applications*, *37*, 28–37. doi:10.1016/j.jisa.2017.10.002

Mali, P. R., & Londhe, V. (2018). Single input multi factor user authentication protocol for smartphone. *International Journal of Engineering and Techniques*, *4*(3), 284–291.

Maydebura, S. V., Jeong, D. H., & Yu, B. (2013). Understanding environmental influences on performing password-based mobile authentication. In C. Zhang, J. Joshi, E. Bertino, & B. Thuraisingham (Eds.), *Proceedings of the IEEE 14th International Conference on Information Reuse & Integration* (pp. 728–731). IEEE. doi:10.1109/IRI.2013.6642543

McGoogan, C., & Demetriou, D. (2017, January 12). Peace sign selfies could let hackers copy your fingerprints. *The Telegraph*. https://www.telegraph.co.uk/technology/2017/01/12/peace-sign-selfies-could-let-hackers-copy-fingerprints

Mehrnezhad, M., Toreini, E., Shahandashti, S. F., & Hao, F. (2018). Stealing PINs via mobile sensors: Actual risk versus user perception. *International Journal of Information Security*, *17*(3), 291–313. doi:10.1007/s10207-017-0369-x PMID:31929770

Muaaz, M., & Mayrhofer, R. (2014). Orientation independent cell phone based gait authentication. In S. L. Wang, Y. Tao, L. Chen, & C. Lee (Eds.), Proceedings of the 12th International Conference on Advances in Mobile Computing and Multimedia (MoMM '14) (pp. 161–164). ACM. https://doi.org/doi:10.1145/2684103.2684152 doi:10.1145/2684103.2684152

Muaaz, M., & Mayrhofer, R. (2017). Smartphone-based gait recognition: From authentication to imitation. *IEEE Transactions on Mobile Computing*, *16*(11), 3209–3221. doi:10.1109/TMC.2017.2686855

Murao, K., Tobise, H., Terada, T., Iso, T., Tsukamoto, M., & Horikoshi, T. (2015). Mobile phone user authentication with grip gestures using pressure sensors. *International Journal of Pervasive Computing and Communications*, *11*(3), 288–301. doi:10.1108/IJPCC-03-2015-0017

Murmuria, R., Stavrou, A., Barbará, D., & Fleck, D. (2015). Continuous authentication on mobile devices using power consumption, touch gestures and physical movement of users. In H. Bos, F. Monrose, & G. Blanc (Eds.), *Research in Attacks, Intrusions, and Defenses: RAID 2015 Proceedings* (pp. 405–424). Springer. doi:10.1007/978-3-319-26362-5_19

Muro-De-La-Herran, A., Garcia-Zapirain, B., & Mendez-Zorrilla, A. (2014). Gait analysis methods: An overview of wearable and non-wearable systems, highlighting clinical applications. *Sensors (Basel)*, *14*(12), 3362–3394. doi:10.3390/s140203362 PMID:24556672

Ramachandra, R., & Busch, C. (2017). Presentation attack detection methods for face recognition systems: A comprehensive survey. *ACM Computing Surveys*, *50*(1), 1–37. doi:10.1145/3038924

Saevanee, H., Clarke, N. L., & Furnell, S. M. (2012). Multi-modal behavioural biometric authentication for mobile devices. In D. Gritzalis, S. Furnell, & M. Theoharidou (Eds.), *Information security and privacy research* (pp. 465–474). Springer. doi:10.1007/978-3-642-30436-1_38

Sarkisyan, A., Debbiny, R., & Nahapetian, A. (2015). WristSnoop: Smartphone PINs prediction using smartwatch motion sensors. In *IEEE International Workshop on Information Forensics and Security (WIFS)* (pp. 1–6). IEEE. doi:10.1109/WIFS.2015.7368569

Shen, J., Gui, Z., Ji, S., Shen, J., Tan, H., & Tang, Y. (2018). Cloud-aided lightweight certificateless authentication protocol with anonymity for wireless body area networks. *Journal of Network and Computer Applications*, *106*, 117–123. doi:10.1016/j.jnca.2018.01.003

Silver, D., Jana, S., Boneh, D., Chen, E., & Jackson, C. (2014). Password managers: Attacks and defenses. In *Proceedings of the 23rd USENIX Conference on Security Symposium* (pp. 449–464). ASM.

Stylios, I. C., Chatzis, S., Thanou, O., & Kokolakis, S. (2015). Mobile phones & behavioral modalities: Surveying users' practices. In *TELFOR 2015 International IEEE Conference.* IEEE Communications Society.

Thorpe, J. K. (2008). *On the Predictability and Security of User Choice in Passwords*, [Doctoral thesis, Carleton University, Ottawa, Ontario, Canada]. http://thorpe.hrl.uoit.ca/publication/thorpePDFS/thorpe_thesis.pdf

Titcomb, J. (2017, November 13). Hackers claim to beat iPhone X's face ID in one week with £115 mask. *The Telegraph*. https://www.telegraph.co.uk/technology/2017/11/13/hackers-beat-iphone-xs-face-one-week-115-mask/

Uddin, M. N., Sharmin, S., Ahmed, A. H. S., Hasan, E., Hossain, S., & Muniruzzaman (2011). A survey of biometrics security system. *IJCSNS, 11*(10), 16–23.

Vazquez-Fernandez, E., & Gonzalez-Jimenez, D. (2016). Face recognition for authentication on mobile devices. *Image and Vision Computing*, *55*, 31–33. doi:10.1016/j.imavis.2016.03.018

Welten, S. M. (2013). *Sensing with smartphones: Light authentication, heavy personalization, and medical applications*. Hartung-Gorre Verlag.

Winnick, M. (2023). *Putting a finger on our phone obsession*. dscout. https://dscout.com/people-nerds/mobile-touches

Ye, G., Tang, Z., Fang, D., Chen, S., Kim, K. I., Taylor, B., & Wang, Z. (2017). Cracking Android pattern lock in five attempts. In *Proceedings of the 2017 Network and Distributed System Security Symposium.* Internet Society. doi:10.14722/ndss.2017.23130

Agnitè Maxim Wilfrid Straiker Edoh is a PhD student at the University of Abomey-Calavi, Benin. His research interests include information security, computer networking, internet of things, industrial applications, and programming. He is a member of the Laboratory of Electronics, Telecommunications and Applied Computing (LETIA/EPAC) and the Laboratory of Analysis and Processing of Image and Speech of the Institute of Technological Innovation (LATIP/IITECH). He graduated as a computer network engineer in 2008 and obtained his master's degree from the Polytechnic School of Abomey-Calavi in the University of Abomey-Calavi in 2018. He is a consultant in the fields of information security, computer networking, mobile computing, and desktop and mobile applications development.

Tahirou Djara is a senior lecturer at the Polytechnic School of Abomey-Calavi located in the University of Abomey-Calavi, Bénin. His research interests include biometrics, signal and image processing, computational intelligence, industrial applications, and symbolic programming. He is a member of the Laboratory of Electronics, Telecommunications and Applied Data Processing Technology (LETIA/EPAC). He received a PhD in signals and image processing from the University of Abomey-Calavi in 2013. He is a consultant in quality assurance in higher education and a consultant in the field of science and engineering technology.

Abdou-Aziz Sobabe Ali Tahirou holds a PhD in engineering sciences from the University of Abomey-Calavi in Benin. He conducts his research at the Laboratory of Electrical Engineering, Telecommunications and Applied Computing (LETIA/EPAC). His research interests include biometrics, signal and image processing, affective computing, and software engineering. His areas of specialization include multimodal biometrics, non-contact biometrics, score fusion, and user-specific parameters in biometric systems. In the area of software engineering, he is interested in object-oriented programming and relational databases for applications. In the field of artificial intelligence, he uses machine learning methods applied to computer security (biometric authentication), e-agriculture, and e-health.

Antoine Vianou is a full professor of engineering sciences and techniques at the University of Abomey-Calavi. He is an engineer from the School of High Technology Montreal Canada (1980). He obtained his diploma of advanced studies in energy systems and master's in energy from the University of Paris XII (1989). He has a PhD in engineering from the University of Dakar (1992), a PhD in physical sciences (1994) from the University of Évry Val d'Essonne, France, and is a knight of the National Order of Benin (2012). He is a founding member of the National Academy of Sciences, Arts and Letters of Benin (ANSALB) (2013).