Paper

Usability Analysis of a Novel Biometric Authentication Approach for Android-Based Mobile Devices

Vincenzo Conti[1], Mario Collotta[1], Giovanni Pau[1], and Salvatore Vitabile[2]

[1] *Faculty of Engineering and Architecture, Kore University of Enna, Cittadella Universitaria, Enna, Italy*
[2] *Department of Biopathology and Medical and Forensic Biotechnologies, University of Palermo, Palermo, Italy*

Abstract—Mobile devices are widely replacing the standard personal computers thanks to their small size and user-friendly use. As a consequence, the amount of information, often confidential, exchanged through these devices is raising. This makes them potential targets of malicious network hackers. The use of simple passwords or PIN are not sufficient to provide a suitable security level for those applications requiring high protection levels on data and services. In this paper a biometric authentication system, as a running Android application, has been developed and implemented on a real mobile device. A system test on real users has been also carried out in order to evaluate the human-machine interaction quality, the recognition accuracy of the proposed technique, and the scheduling latency of the operating system and its degree of acceptance. Several measures, such as system usability, users satisfaction, and tolerable speed for identification, have been carried out in order to evaluate the performance of the proposed approach.

Keywords—fingerprints authentication, mobile device security, operating system, usability.

1. Introduction

In the actual technological scenario, where Information and Communication Technologies (ICT) provide advanced services, mobile computing systems need strong procedures to protect data and resource access from unauthorized users. The continuous advances of technology require high security levels, especially in mobile devices. More and more users are urged to enter proprietary data on these devices, in order to access to a greater number of services [1], [2].

Authentication procedures, based on the simple PIN or username/password pair, are not sufficient to provide a suitable security level for applications requiring high protection of data and services. Biometric based authentication systems represent a valid alternative to conventional approaches [3]. In this field, the identity management is related to the manipulation, storage and protection of personal biometric templates inside an electronic environment. Biometry represents a secure approach for identity management and personal authentication [4]. For trusted authentication, a secure infrastructure where each user could be reliably authenticated is required. Trustiness is an essential requirement when transactions must be executed without limits and compromises. Critical ICT services supplied to people (e.g. e-commerce or e-banking) need a high level of security [5]. A trusted biometric authentication system has to reduce the point-of-attacks in the recognition chain and has to give the capability to authenticate people with a high level of certainty. So, the eventual release of an application or a service is made through a biometric module (fingerprints control) on the basis of who the user is.

The main aim of this paper is to evaluate the feasibility and the acceptability of a biometric authentication system on a mobile device, addressing user reactions for the fingerprint acquisition, processing, and verification time. The results of these tests may be useful for future developers in order to find the optimization limit and the right trade-off for future biometric system implementations on mobile devices.

The paper has been structured as follows. Section 2 discusses the related works about authentication techniques and systems used on mobile devices. Section 3 describes the proposed approach. Section 4 reports the human-machine interaction evaluation techniques and the related experimental results in terms of user satisfaction. Finally, some concluding remarks are reported in Section 5.

2. Related Works

Android offers several techniques to protect the mobile device. These techniques are all related to screen lock and not to each application start. To configure this protection mode is enough to manage security settings. The latest versions of Android offer different possibilities to unlock:

- none – when the power button is pressed (even accidentally) the screen turns on and provides access to all device features (no security);
- numerical code (PIN) – the user chooses a numerical sequence of at least 4 digits. When the power button is pressed, the user must enter the sequence in the right way, in order to access to all device functions (medium security);

- password – the user chooses an alphanumeric case sensitive password. To unlock the device, the user must enter the characters in the exact sequence. In the event that the user enters an incorrect password five times, the device will be blocked for 30 seconds, in order to avoid attempts to unlock the device with brute force methods (high security);
- sequence type – this is a graphic unlock method. A grid with nine elements (3×3) is shown to the user. The release occurs only if the elements are touched in the right order and without lifting the finger from the screen (medium-low security);
- scrolling – when the button is pressed, different unlocking options are shown to the user in order to directly access to some device features, such as the camera or the homepage. This mode only protects against in adverting break outs (no security);
- face unlock (beta) – through a facial recognition algorithm and using the device's camera, the face of the user is recorded, specifically the eyes and mouth positions. Google considers this feature "unsafe" as the level of facial recognition has been lowered in order to enhance usability. In addition, after many users' reports related to the possibility to unlock the device using a photo of the owner, Google and Samsung have solved this problem by putting a parameter called "vitality control". In practice after facial recognition, the user must wink to unlock the device. In addition, this unlock function provides several customizations. For example it allows the user to enter four self-portraits in different conditions (with glasses, beard, with low light). In this way the user does not have to reconfigure the device to any appearance change.

The lock screen has various functions for security and it protects the mobile device from involuntary pressures of keys (for example when the device is in a pocket or in a purse). At the same time the lock screen provides protection both in case in which the device is left unattended and in case of theft or loss. In case of theft, the lock screen does not provide any protection against the device formatting, which determines all data loss and security settings reset.

In order to provide higher security, the unlock password should be saved online. The access to this password should happen only after the user enters the same password. This can make the devices theft more difficult but not impossible, because a formatting done by an experienced user could transform the device into another. In [6] the authors describe the permission-based security models. This system uses a computer security technique that allows the administrator and operating system to restrict applications to access specific resources. Throughout the analysis, they discover several phenomena that verify past research, and new potentials in permission-based security models that may provide additional security to the users. In [7] the authors, in cooperation with a security expert, carried out a case study with the mobile phone platform Android, and employed the reverse engineering tool-suite Bauhaus for this security assessment. During the investigation they found some inconsistencies in the implementation of the Android security concepts.

In [8], the authors present the current state of smartphone security mechanisms and their limitations in order to identify certain security requirements for proposing enhancements for smartphones security models. In [9] the authors present their upgraded Lock Screen system, which is able to support authentication for the user's convenience and provide a good security system for smartphones. They also suggest an upgraded authentication system for Android smartphones. All these considerations have led many researchers to study innovative techniques to improve security on all kind of devices. Different studies and implementations of biometric authentication systems based on different features were published in the literature. Usually, both software and hardware standard approaches are based on three main steps: image enhancement phase, extraction of biometric identifiers, and matching phase. In what follows, the most meaningful works are briefly described. In [10] the authors present a multimodal biometric identification system based on the combination of geometry and fingerprint features of the human hand. Hand images are acquired with a commercial scanner (150 dpi resolution) while support vector machines technique is used as verifier. In [11] the author makes new observation about fingerprint recognition that uses state of the single steak in the fingerprint image, because patterns of the veins in the fingerprint without notice of the fingerprint about person, and can be used for identified person. This algorithm can work on gray scanned photo and also its work very fine on the binary images. Whereas the insecurity of a system can be easily exaggerated even with little minor vulnerability, the security is not easily demonstrated.

In [12] the authors represent the system in terms of a state machine, elucidate the security needs, and show that the specified system is secure over the specified states and transitions. The authors expect that this work will provide the basis for assuring the security of the Android system. Multi-modal biometric fusion is more accurate and reliable compared to recognition using a single biometric modality, as said by author of [13]. Their goal is to advance the state-of-the-art in biometric fusion technology by providing a more universal and more accurate solution for personal identification and verification with predictive quality metrics. In [14] the authors focus their attention on the technical details and performance comparison of various available fingerprint sensors and explore the future direction and system development that states using similar techniques for chance or latent fingerprint enrolment. The study and experiments carried out indicate that the error occurred due to poor calibration causes a greater impact on the generated overall system output and serious usabil-

ity issues with respect to handling of fingerprint sensors. In [15] the authors proposed a novel fingerprint matching algorithm based on minutiae sets combined with global statistical features. The approach has the advantage of considering both local and global features for the fingerprint matching task. The above feature improves the accuracy of matching score without increasing of time and memory consuming.

In [16] the authors realized a software authentication system that refers to classical methods for fingerprint enhancement. Fingerprint is processed with two filters in order to enhance images quality. The first filter is based on two-dimensional Fourier transform for reducing low and high frequency noise. The second filter equalize fingerprint image grey levels. The last elaboration is then related to minutiae extraction. All the minutiae are sorted as to the distance by the image center. The processing time using a standard general purpose PC is 11.4 s. In [17] the authors proposed a hardware system using the pipeline technique to increase the final throughput. Various tasks were implemented on Altera FLEX10KE FPGA. An initial Gaussian filtering is used to enhance fingerprint quality and an edge-detection algorithm is applied to segment fingerprint ridges. Finally, a thinning algorithm is applied before the minutiae extraction task. The execution time is of 589.93 ms. In [18] the authors developed a prototype for fingerprint authentication through a Xilinx Virtex-II FPGA based board. The proposed architecture can be broken in 3 levels, where the lower level is constituted by hardware platform. In the enrollment phase, the extracted biometric template is stored into the FPGA memory. The execution time is about 5 s. In [19] the author presents and analyses the typical and known attacks against biometric systems and outlines several solutions to protect and design a secure biometric system. The advantages and disadvantages of each proposed technique was then discussed.

In [20] the authors make a biometric secured mobile voting. This is a novel technology and also first of its kind at present. Using fingerprint based biometric control information and encryption along with SSL using VeriSign would make the software involved in the voting process well secured. In addition tying the credentials to a mobile device will make the system even more robust. The next generation of banking applications won't be on desktop or mainframes but on the small devices we carry every day. In [21] authors have focused on how biometric mechanism provides the highest security to the mobile payment. The present security issues surround the loss of personal information through the theft of the cell phone. The authors present the proposed biometrics mechanism in order to make more secure the mobile payment and also to provide security at the wireless transmission level. In [22] the authors present a new way of generating behavioral (not biometric) fingerprints from the cellphone usage data. In particular, they explore if the generated behavioral fingerprints are memorable enough to be remembered by end users. They built a system, called HuMan that generates fingerprints from cellphone data. Android is one of the most popular and fully customizable open source mobile platforms that come with a complete software stack. One of the main reasons behind the rapid growth in adoption of smartphones is their capability to facilitate users with third-part applications. However, this rapid growth in smartphone usage and the ability to install third-part applications has given rise to several security concerns.

3. The Proposed Novel Approach

The fingerprinting is the basis of presented approach. In the market there are several sensor typologies:

- optical – the fingerprint is detected using the reflection law, in order to have a good contrast image;
- capacitive – a series of silicon sensors read a small part of the fingerprint and then join it in the complete image;
- ultrasonic – the sound waves strike the finger surface and based on the return signal valleys and ridges are defined;
- thermal – it uses the temperature difference between the valleys and ridges of the fingerprint.

In this approach the authors would like not use any fingerprint scanner since we have carried out a feasibility study for a future implementation. It will be possible to detect the fingerprint in any part of the screen, without the use of a specific sensor. In presented model, it is important that the fingerprint is detected directly through the screen, as detection must be almost invisible to the authorized user. Compared to other detection systems which deal with the device unlock only, a continuous control in order to check

Table 1
Device datasheet

Parameter	Value
Product name	LG Nexus 5
Wireless connectivity	Wi-Fi a/b/g/n/ac
Dimensions	$17.84 \times 69.17 \times$ 8.59 mm
Display	495 Corning Gorilla Glass 3 1080×1920 multi-touch 5 point
CPU clock frequency	2.26 GHz
Processor	Quad core Qualcomm Snapdragon 800
RAM	2 GB
Memory	32 GB integrated

user identity when each activity starts is inserted. An application for the Android platform has been developed in order to control the system. Every 500 ms a background application checks if running activities are in the authorized applications list. If an activity is not present, the system controls the user fingerprint. The list of authorized activities, is refreshed every 5 min and at every device rebooting. In the final version a variable will be included in order to count invalid fingerprint-based accesses. When the fifth failed attempt occurs, the device activates the lock-screen and delegates to Android policies the access management. The application was tested on a device whose data sheet is shown in Table 1.

3.1. Model Processing Phases

The idea of the proposed system is shown in Fig. 1. The system checks if the user is trying to access to an authorized application. If the desired application is not in the authorized applications list, the system provides a biometric control based on fingerprint recognition. In case of recognized fingerprint, the system will insert the application in the authorized applications list allowing the access. Otherwise the system will lock the screen denying the access.

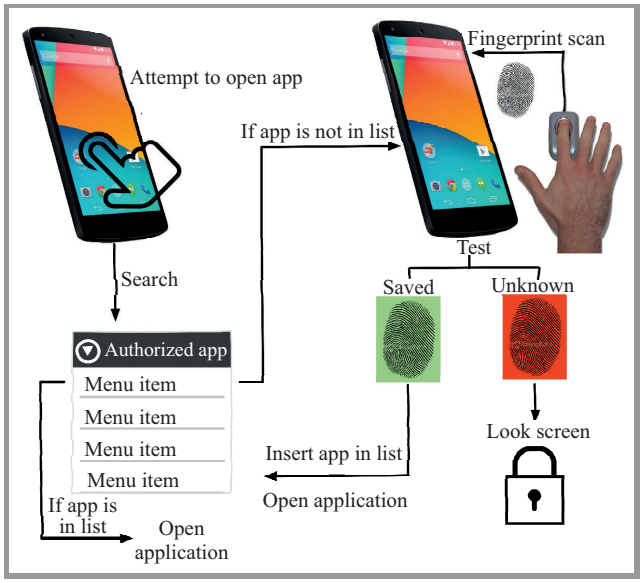

Fig. 1. The proposed system architecture.

Figure 2 describes the algorithm functioning. The number of possible access attempts is indicated by the variable *Number of attempts* (NoA), initially set to zero. The user will try to access to an application. The system controls if it is an enabled application or not. In the case of enabled application, the application will be launched. Otherwise, the system will check fingerprint to see if the access attempt has been made by the owner. If the fingerprint is recognized, the application will be included in the authorized applications list. Otherwise, the variable NoA will be incremented by one. The number of possible attempts

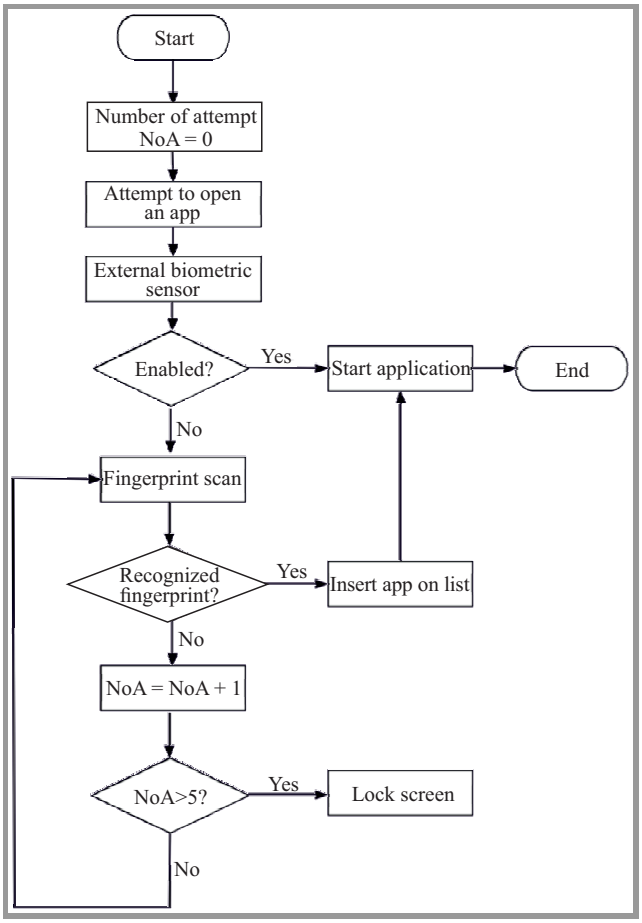

Fig. 2. Algorithm dataflow of the proposed approach.

is five. Exceeded five attempts, the system will lock the screen.

3.2. Fingerprint Authentication System

The goal of an authentication system is to compare two fingerprint images: a fingerprint captured and processed in the startup phase with the fingerprint acquired in real time. With more details, two steps, an off-line and on-line step, compose this model. In the off-line step the user's fingerprint is captured, processed and stored in the mobile device. In the online step the user gives its own fingerprint to verify the identity – the fingerprint is compared with one stored. The most used authentication systems are based on Minutiae or Singularity points.

In this work, three different authentication systems have been implemented using good quality fingerprint images. These authentication systems are characterized by different execution times and accuracy rates. Usually, authentication systems very strong in terms of accuracy rates have very high execution times and vice versa. Since the proposed biometric module is oriented to mobile devices, the final systems must be implemented in order to reduce the execution time maintaining a good accuracy level. Only one of these three systems, achieving the best compromise, will be used in the final mobile device.

First implementation: Algorithm 1

It is based on Singularity points extraction using the Poincaré indexes [23]. It is composed only by the following steps:

- directional image extraction – every element represents the local ridges orientation in the original grey-scale image;
- Poincaré indexes technique – it is computed by summing the orientation changes along a closed curve around the pixel of interest. Poincaré index, making a full counter-clockwise turn along the curve in the orientation field image, the direction angle is equal to $0°$, $\pm 180°$ or $\pm 360°$. So, according by the value of the Poincaré index (0 when orientation angle change is $0°$, $\frac{1}{2}$ when orientation angle change is $180°$, $-\frac{1}{2}$ when orientation angle change is $-180°$), the system is able to detect the singular points;
- matching technique [24] – two matching algorithms are applied: the single rotation matching and the multiple rotation matching. The single rotation matching is applied when the algorithm receives images with two singularity regions for each fingerprint and if the singularity regions are of same type and the difference of their relative distances is lower a threshold. The multiple rotation matching algorithm is applied when a fingerprint image has only a singularity region. The XOR operator is applied between the correspondent regions to obtain the similarity degree.

Second implementation: Algorithm 2

It is based on Minutiae extraction and a robust matching algorithm. It is composed by the following steps:

- binarization algorithm – this step aims to obtain a binary image, where pixels can assume a binary value;
- thinning algorithm – it aims to reduce ridge thickness to the unitary value;
- minutiae extraction algorithm – it is devoted to minutiae analysis (i.e. ending points and bifurcation points classification) and localization. As results, for each detected minutia, spatial coordinates are used to generate fingerprint template;
- alignment algorithm – it calculates roto-translation parameters if the value of Euclidean distance is lower than a threshold. The rotation parameter is based on the differences between the corresponding angles in the selected minutiae pairs. The translation parameter is based on the differences between the respective Cartesian coordinates in the selected minutiae pairs;
- matching technique [25] it is performed between the roto-translated test and template image. For each test image minutia, all template image ones are considered to calculate the differences between respective coordinates $x - y(\overline{diff}_{xy})$ and angles $\theta(\overline{diff}_{theta})$. Only when these differences are lower than two thresholds the first partial score is obtained and mapped into $[0, 1]$ range. Among all complete scores, only the greater is considered.

Third implementation: Algorithm 3

It is based on Minutiae extraction and a fast matching algorithm. It is composed only by the following steps:

- binarization algorithm – the same used for Algorithm 2;
- thinning algorithm – the same used for Algorithm 2;
- minutiae extraction algorithm – the same used for Algorithm 2;
- matching technique [26] off-line registration phase and one acquired during the authentication phase. It is based only roto-translation comparisons of Minutiae individualized.

4. Human-Machine Interaction Evaluation Techniques

Usability is defined in ISO 9241 standard, as "*the effectiveness, the efficiency and the satisfaction with which specified users achieve certain goals in determined contexts*". This standard provides a general definition applicable to digital interfaces and many other areas. In any case, an absolute definition of usability does not exist as usability is always compared to a user who needs to reach a certain goal. In the user-centered design context, usability is aimed to see how people relate with a certain product as objective as possible. The simplicity and standards compliance are essential to usability. The user's interest relates only to the product and its pure functionality. To find out if an application is usable it is necessary to know how a user can achieve a specific goal (effectiveness) in a reasonable amount of time (efficiency), finding comfortable and enjoyable this experience (satisfaction). The best way to understand it is through usability testing with users [27].

The main goal of the test is to study the behavior of users which interact with real products or prototypes [28]. Moreover it is really important to identify problems and bottlenecks of the interface, in order to be able to correct them during the design phase.

Another important point is to understand how the user moves and thinks its difficult reasons in order to address them in the design phase. The tests require that each user is observed individually, and not in group. Furthermore, the performed tasks must be coherent for each participant. These aspects are always present in all test methods and the rest will change depending on the constraints of each project. A very important step is the usability test planning [29]. This phase is focused on a number of factors on which the entire test is based: test objectives, user characteristics, tasks and questionnaire characteristics at the end of test.

Some requirements of usability test include:

- identification of all the variables involved in the interaction between user and product. Typically, they involve certain assumptions on the tested users, but also on the interface characteristics, and on what can vary and affect system performance;
- subjects recruitment – users can be divided in statistically equivalent groups;
- precise experimental hypothesis – the test is a real scientific experiment. Through the control of the involved variables the main aim is to verify a certain hypothesis;
- rigorous measurement of the experimental values – relevant data are collected for measurement and analysis of necessary variables (number of errors, number of clicks, execution time, etc.);
- statistical analysis – collected data are analysed and adjusted according to appropriate statistical techniques.

If necessary, during the test it is possible to record the session. However, the presence of a camera can embarrass the user and it is not always recommended. The test can be conducted through the think aloud technique [30], which asks users to verbalize aloud their thoughts, comments and emotions during the test. The think aloud method shows the differences between the designer and the user mental model. The main goal is to bring closer these two models as much as possible. In other cases it is possible to use the eye-tracking [31], a hardware and software technology that allows to track the user's eye movements while looking at the interface. The eye tracking is very useful when it is necessary to get very accurate and quantitatively significant data, for example to analyse the key pages of the application, to make comparative studies of different versions, to see the visual impact of the display.
The usability test on mobile touch devices must also take into account other technical constraints:

- sound – users may not feel it or, on the contrary, may have to disable it in order to avoid disturbing people around them;
- light conditions – mobility user might want to use the interface in non-optimal lighting conditions. So, it is very important the contrast between the background and text elements in the foreground;
- connection – it is necessary to optimize the loading time. For example, it is possible to load the main info immediately or define information architecture for this purpose;
- screen size: it is possible to optimize the interface in order to avoid unnecessary vertical or horizontal scrolling;
- touch: clickable elements must be sufficiently spaced.

4.1. Human-Machine Interaction Evaluation Test-bed

In order to validate presented approach a usability test has been implemented. The usability test involved 100 users for a qualitative and a quantitative test. With more details, user satisfaction and the percentage of tasks successfully completed (success rate) have been measured. After an initial briefing where the participants to the test goals have been introduced, each user was escorted to a separate room in order to feel at ease and concentrate on the goals of the test. The test does not provide audio or video recordings, it does not use the think aloud or the eye tracking methods. In order to collect feedbacks from users it has been prepared an analysis grid of critical situations accompanied by a short final questionnaire to gather tips. The Android application, installed on the mobile device, has been implemented in such a way to track user usage.
First of all, not having a device with a fingerprint detector, images acquired with external equipment have been used. With more details, to quantify the user satisfaction, it has been optimized the touches number on the various buttons and the number of applications starts. Figure 3 shows the user satisfaction after interacting with three different biometric recognition algorithms. The results show that the Algorithm 3 has received the greater number of positive feedback in order to execution time and accuracy rate.

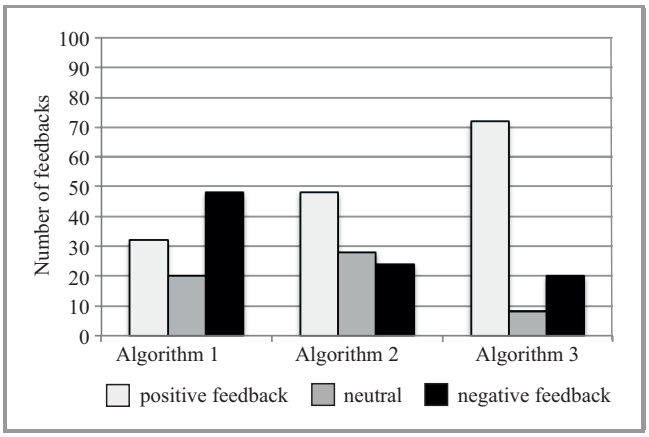

Fig. 3. User satisfaction feedbacks using the different implementation of the biometric recognition algorithm.

One of the most important Algorithm 3 phases is related to the minutiae identification and extraction. First of all, the thinning algorithm has been applied in order to obtain fingerprint ridges with size of 1 pixel. After, for the entire image, all 3×3 submatrices have been analyzed to calculate the number of black pixels. In every submatrix with a central black pixel, the following cases can be obtained:

– 1 black pixel – it is an isolated point;

– 2 black pixels – it is a minutia, said end-point;

– 4 black pixels – it is a minutia, said bifurcation.

In the proposed system, the minutia characteristics as position (spatial coordinates in Cartesian axes) and type have

Table 2
LG Nexus 5 processing times

No.	Binarization [ms]	Thinning [ms]	Minutiae extraction and post-processing [ms]	Matching algorithm [ms]	Total [ms]
1	66	1033	1474	87	2660
2	80	1282	1579	95	3036
3	46	1008	1474	85	2613
4	70	1227	1609	104	3010
5	73	1124	1506	101	2804

been considered. In addition, to decrease the number of false minutiae due to the noise presence, some choices have been made:

– all end-points and bifurcations located in the image edge are discarded;

– all end-points and bifurcations too close together are discarded.

The implemented fingerprint authentication system on the LG Nexus 5 has given the following experimental results in terms of minutia extraction (Fig. 4), execution time and accuracy. Table 2 shows the obtained processing time using the Algorithm 3 implementation on the Android device. The five rows correspond to tests carried out on five different fingerprints. The average time measured was 3 s. This is a tolerable value considering what expressed by users. Experimental results show good performance about the proposed system. Figure 5 shows tips provided by user regarding the Android application. Most of the users which participated at the usability test would like a biometric recognition speed improvement. This

Fig. 4. The proposed fingerprint authentication systems implemented on the LG Nexus 5: (a) the original fingerprint image, (b) the binarized fingerprint image, (c) the thinning fingerprint image, (d) detected minutiae, (e) the minutiae (end points and bifurcations) extracted after checking its distance.

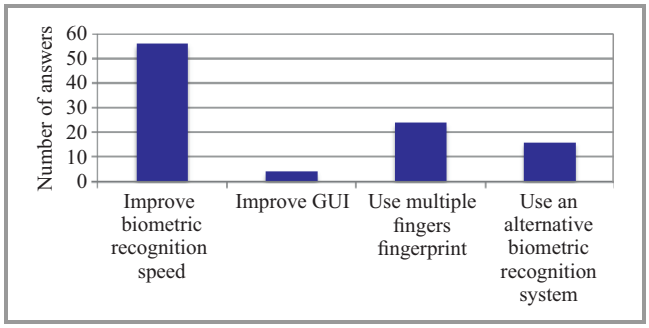

Fig. 5. Tips provided by users on the biometric application.

speed will be significantly improved when the biometric recognition system will be integrated directly into the mobile device.

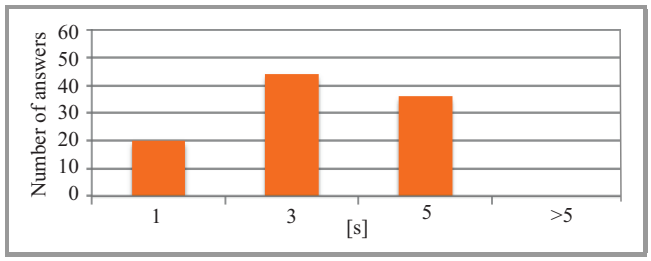

Fig. 6. Answers provided by users on the tolerable biometric recognition speed.

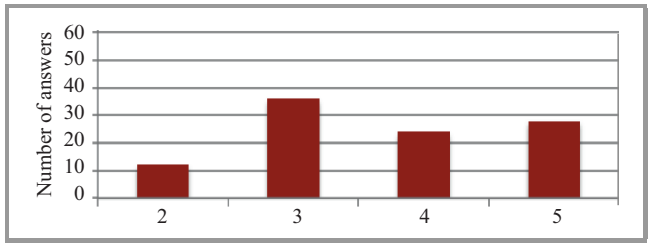

Fig. 7. Answers provided by users on the desired fingers acquisition number for biometric recognition.

The user's tolerance level about the biometric recognition speed is shown in Fig. 6. Users tolerate a biometric recognition speed ranging between 3 and 5 s. Figure 7 shows the answers provided by users regarding the desired fingers number for biometric recognition. It is clear that users want to use fingerprints from multiple fingers. Figure 8 shows the answers provided by users regarding to an alternative biometric recognition system. Among the various proposed

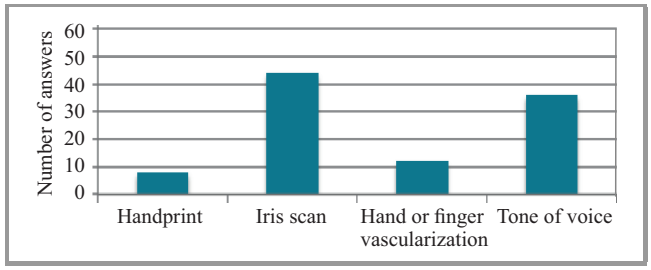

Fig. 8. Answers provided by users on an alternative mobile biometric recognition system.

systems users would be more willing to use an iris scan system or a tone of voice recognition system.
Finally the Success Rate (SR), related to tasks to be performed by each user, has been evaluated using the following equation [32]:

$$SR = \frac{Successful\_trials + (Partially\_Successful \cdot 0.5)}{Total\_trials} \quad (1)$$

Two parameters are also considered. The Precision (also known as positive predictive value) is the fraction of retrieved instances that are relevant, and the Recall (also known as sensitivity) is the fraction of relevant instances that are retrieved. Precision and Recall [33] are then defined through the Eqs. 2 and 3, respectively:

$$Precision = \frac{TP}{TP+FP}, \quad (2)$$

$$Recall = \frac{TP}{TP+FN}, \quad (3)$$

where TP is the True Positive value, TN is the True Negative value, FP is the False Positive value, and FN is the False Negative value. Specifically, the instance is negative and it is predicted negative in TN, the instance is positive and it is predicted positive in TP, the instance is positive but it is predicted negative in FN, and, finally, the instance is negative but it is predicted positive in FP.

Table 3
Hit and failure percentages

Task	Success [%]	Partial success [%]	Failure [%]
1	92	8	0
2	94	6	0

As shown in Table 3, the usability test has been carried out considering two specific tasks: the search of the application to launch in the list of enabled applications (Task 1) and the fingerprint control (Task 2). Moreover, the percentages of success and failure are also shown in Table 3. Using Eq. 1, the success rate of both tasks has been calculated as:

$$SR = \frac{172 + (28 \cdot 0.5)}{200} = 93\% \quad (4)$$

Then the Precision and Recall parameters, always considering 100 users, have been calculated. The measured occurrences of TP, FP, TN and FN are shown in Table 4. Moreover, Precision and Recall rates have been calculated for both tasks, using Eqs. 2 and 3 and the results are listed in Table 5.

Table 4
Authentication system: Precision and Recall

Parameter	Task 1	Task 2
TP	88	84
TN	0	4
FP	4	8
FN	8	4

Table 5
Precision and Recall of Task 1 and Task 2

Parameter	Task 1 [%]	Task 2 [%]
Precision	95.6	91.3
Recall	91.7	95.4

A statistical analysis has been also carried out through the MedCalc software [34] suite. This analysis focused on the inter-rater reliability (or even "agreement between judges") that measures the degree to which the ratings of two or more judges are consistent beyond the case. In the first analysis the Intraclass Correlation Coefficient (ICC) [35], [36], a measure of the reliability of measurements or ratings, has been calculated. For the purpose of assessing inter-rater reliability and the ICC, two or preferably more raters rate a number of study subjects. In this case different users rate the three algorithms. It is necessary to made a distinction between two study models: (1) each algorithm is rated by a different and random selection of a pool of raters/users, and (2) each algorithm is rated by the same raters/users. In the first model, the ICC is always a measure for "absolute agreement"; in the second model a choice can be made between two types: "consistency" when systematic differences between raters are irrelevant, and "absolute agreement", when systematic differences are relevant.

Table 6
Intraclass Correlation Coefficient

	Intraclass Correlation	95% confidence interval
Single measures	0.6037	0.2653 to 0.9841
Average measures	0.6037	0.2653 to 0.9841

In the presented analysis, the authors considered this last case and the results are shown in Table 6. In detail, the "Intraclass Correlation" represents the degree of absolute agreement among measurements, the "Single measures" estimates the reliability of single ratings (an index for the reliability of the ratings for one, typical, single rater) and the "Average measures" estimates the reliability of averages of k ratings (an index for the reliability of different raters averaged together, always higher than the Single measures ICC).

5. Conclusions

In new generation mobile devices, biometrics can be a safe approach for user identity and authentication management. However, in this context, a biometric authentication system must have an authentication capacity with a high level of security. Moreover, the biometric approaches are involved into the tasks scheduling of the operating system that can causes latency and then the user satisfaction can

be compromised. So, some real-time operations concerning human-machine interactions can slow down due to biometric authentication process. In this paper the feasibility of a trusted biometric authentication system has been evaluated. A deep analysis has been performed in order to evaluate users reactions towards the delay times for acquisition, processing and verification of fingerprints. The obtained results provide a clear guidance on the users' satisfaction about used algorithms and on the tolerable speed for identification. This information can be the main starting point for developers in order to find the optimum trade-off for future implementations.

References

[1] C. Militello, V. Conti, S. Vitabile, and F. Sorbello, "Embedded access points for trusted data and resources access in HPC systems", *The J. of Supercomput.*, vol. 55, no. 1, pp. 4–27, 2011.

[2] S. Vitabile, V. Conti, M. Collotta, G. Scatà, S. Andolina, A. Gentile, F. Sorbello, "A real-time network architecture for biometric data delivery in Ambient Intelligence", *J. Ambient Intelligence and Humanized Computing*, vol. 4, no. 3, pp. 303–321, 2013.

[3] C. Militello, V. Conti, S. Vitabile, and F. Sorbello, "An Embedded Iris Recognizer for Portable and Mobile Devices", *International Journal of Computer Systems Science & Engineering*, vol. 25, no. 2, pp. 119–131, 2010.

[4] V. Conti, C. Militello, F. Sorbello, and S. Vitabile, "A frequency-based approach for features fusion in fingerprint and iris multimodal biometric identification systems", *IEEE Trans. Syst., Man, and Cybernet. Part C: Applications & Reviews*, vol. 40, no. 4, pp. 384–395, 2010.

[5] S. Vitabile, V. Conti, C. Militello, and F. Sorbello, "An extended JADE-S based framework for developing secure multi-agent systems", *Comp. Stand. Interfsace J.*, vol. 31, no. 5, pp. 913–930, 2009.

[6] I. Rossameeroj and Y. Tanahashi, "Various approaches in analyzing android applications with its permission-based security models", in *Proc. IEEE Int. Conf. Electro/Inform. Technol. EIT 2011*, Mankato, MN, USA, 2011, pp. 1–6, 2011.

[7] B. J. Berger, M. Bunke, and K. Sohr, "An Android security case study with bauhaus", in *Proc. 18th Work. Conf. Reverse Engin. WCRE 2011*, Lero, Limerick, Ireland, 2011, pp. 179–183.

[8] S. Khan, M. Nauman, A. T. Othman, and S. Musa, "How secure is your smartphone: an analysis of smartphone security mechanisms", in *Int. Conf. Cyber Secur., Cyber Warfare and Digit. Forensic CyberSec 2012*, Kuala Lumpur, Malaysia, 2012, pp. 76–81.

[9] K. Il Shin, J. S. Park, J. Y. Lee, and J. H. Park, "Design and implementation of improved authentication system for Android smartphone users", in *Proc. 26th Int. Conf. Adv. Inform. Netw. Appl. Worksh. WAINA 2012*, Fukuoka, Japan, 2012, pp. 704–707.

[10] M. A. Ferrer, A. Morales, C. M. Travieso, and J. B. Alonso, "Low cost multimodal biometric identification system based on hand geometry, palm and finger print texture", in *Proc. 41st Ann. IEEE Int. Carnahan Conf. Secur. Technol.*, Ottawa, ON, Canada, 2007, pp. 52–58.

[11] B. Saropourian, "A new approach of finger-print recognition based on neural network", in *Proc. 2nd IEEE Int. Conf. Comp. Sci. Inform. Technol. ICCSIT 2009*, Beijing, China, 2009, pp. 158–161.

[12] W. Shin, S. Kiyomoto, K. Fukushima, and T. Tanaka, "Towards formal analysis of the permission-based, security model for Android", in *Proc. 5th Int. Conf. Wirel. Mob. Commun. ICWMC'09*, Cannes, France, 2009, pp. 87–92.

[13] Y. Tong, F. W. Wheeler, and X. Liu, "Improving biometric identification through quality-based face and fingerprint biometric fusion", in *Proc. IEEE Comp. Soc. Conf. Comp. Vision and Pattern Recog. Worksh. CVPRW 2010*, San Francisco, CA, USA, 2010, pp. 53–60.

[14] B. Ashwini, J. S. Digambarrao, and S. P. Patil, "Performance analysis of finger print sensors", in *Proc. 2nd Int. Conf. Mechan. Electron. Engin. ICMEE 2010*, Kyoto, Japan, 2010, pp. 169–174.

[15] P. Shi, J. Tian, Q. Su, and X. Yang, "A novel fingerprint matching algorithm based on minutiae and global statistical features", in *Proc. 1st IEEE Int. Conf Biometrics: Theory, Appl. and Syst.*, Washington, USA, 2007, pp. 1–6.

[16] M. Zsolt and V. Kovacs, "A fingerprint verification system based on triangular matching and dynamic time warping", *IEEE Trans. Pattern Anal. and Machine Intell.*, vol. 22, no. 11, pp. 1266–1276, 2000.

[17] V. Bonato, R. F. Molz, J. C. Furtado, M. F. Ferraao, and F. G. Moraes, "Propose of a hardware implementation for fingerprint systems", in *Field Programmable Logic and Application*, *LNCS*, vol. 2778, pp. 1158–1161, Springer, 2003.

[18] P. Schaumont and I. Verbauwhede, "ThumbPod puts security under your thumb", *Xilinx Xcell J.*, Winter 2004.

[19] P. Ambalakat, "Security of biometric authentication systems", in *Proc. 21st Computer Science Seminar*, Hartfort, USA, 2005.

[20] D. Gentles and S. Sankaranarayanan, "Biometric secured mobile voting", in *Proc. 2nd Asian Himalayas Int. Conf. Internet AH-ICI 2011*, Kathmandu, Nepal, 2011, pp. 1–6.

[21] M. Belkhede, V. Gulhane, and P. Bajaj, "Biometric mechanism for enhanced security of online transaction on Android system: A design approach", in *Proc. 14th Int. Conf. Adv. Commun. Technol. ICACT 2012*, PyeongChang, South Korea, 2012, pp. 1193–1197.

[22] P. Gupta *et al.*, "HuMan: Creating memorable fingerprints of mobile users", in *Proc. IEEE Int. Conf. Pervasive Comput. Commun. Worksh. (Percom Workshops)*, Lugano, Switzerland, 2012, pp. 479–482.

[23] H. Zhang, Y. Yin, and G. Ren, "An improved method for singularity detection of fingerprint images", in *Book Advances in Biometric Person Authentication*, *LNCS*, vol. 3338, pp. 516–524, Springer, 2004.

[24] V. Conti, C. Militello, S. Vitabile, and F. Sorbello, "Introducing pseudo-singularity points for efficient fingerprints classification and recognition", in *Proc. 4th IEEE Int. Conf. Complex, Intell. Softw. Intens. Syst. CISIS 2010*, Krakow, Poland, 2010, pp. 368–375.

[25] V. Conti, G. Vitello, F. Sorbello, and S. Vitabile, "An advanced technique for user identification using partial fingerprint", in *Proc. 7th Int. IEEE Conf. Complex, Intell. Softw. Intens. Syst. CISIS 2013*, Taichung, Taiwan, 2013, pp. 236–242.

[26] V. Conti, S. Vitabile, G. Vitello, and F. Sorbello, "An embedded biometric sensor for ubiquitous authentication", in *Proc. AEIT Ann. IEEE Conf.*, Mondello, Italy, 2013, pp. 1–6.

[27] G. Chao, "Human-computer interaction, the usability test methods and design principles in the human-computer interface design", in *Proc. Int. Conf. Comp. Sci. Inform. Technol. ICCSIT 2009*, Beijing, China, 2009, pp. 283–285.

[28] M. Lv, W. Hou, and C. Zhao, "Research of usability test mode based on the implicit user behavior lib", in *Proc. 9th Int. Conf. Comp.-Aided Indust. Des. Concept. Des. CAID/CD 2008*, Kunming, China, 2008, pp. 157–161.

[29] W. P. Brinkman, R. Haakma, and D. G. Bouwhuis, "Component-specific usability testing", *IEEE Trans. Syst., Man and Cybernet., Part A: Systems and Humans*, vol. 38, no. 5, pp. 1143–1155, 2008.

[30] L. Cooke, "Assessing concurrent think-aloud protocol as a usability test method: A technical communication approach", *IEEE Trans. Profess. Commun.*, vol. 53, no. 3, pp. 202–215, 2010.

[31] H. Fengpei, "The Studies of Eye Tracking and Usability Test", in *Proc. 7th Int. Conf. Comp.-Aided Indust. Des. Concept. Des. CAID/CD 2006)*, Hangzhou, China, 2006, pp. 1–5.

[32] T. Tullis, B. Thomas, and W. Albert, *Measuring the User Experience: Collecting, Analyzing, and Presenting Usability Metrics*. Morgan Kaufmann, 2010.

[33] D. L. Olson and D. Delen, *Advanced Data Mining Techniques*, 1st ed. Springer, 2008.

[34] MedCalc – User-friendly statistical software [Online]. Available: http://www.medcalc.org/index.php

[35] P. E. Shrout and J. L. Fleiss, "Intraclass correlations: uses in assessing rater reliability", *Psycholog. Bull.*, vol. 86, pp. 420–428, 1979.

[36] K. O. McGraw and S. P. Wong, "Forming inferences about some intraclass correlation coefficients", *Psycholog. Meth.*, vol. 1, pp. 30–46, 1996.

Vincenzo Conti is an Assistant Professor with the Faculty of Engineering and Architecture at the Kore University of Enna, Italy. He received his Laurea cum Laude degree and his Ph.D. in Computer Engineering from the University of Palermo in 2000 and 2005, respectively. His research interests include biometric recognition systems, programmable architectures, bio-inspired processing system, and user ownership in multi-agent systems. He has chaired and participated at several national and international conferences, coauthoring over 50 scientific publications, journals and conferences. Moreover, he has participated to several research projects funded by industries and research institutes in his research areas. Currently, he collaborates too with the Department of Chemical Engineering, Management, Mechanics and Computer Science (DICGIM) of the University of Palermo and with Council National of Researches (CNR) of Cefalú (Palermo).

E-mail: vincenzo.conti@unikore.it
Faculty of Engineering and Architecture
Kore University of Enna
Cittadella Universitaria
94100 Enna, Italy

Mario Collotta is an Assistant Professor with tenure in the Faculty of Engineering and Architecture at the Kore University of Enna, Italy, and since 2011 he is scientific responsible and director of Telematics Engineering Laboratory. His research activity is mainly focused on the study of real-time networks and systems. His interests concern the realization of strategies and innovative algorithms in order to ensure a flexible management of resources (band/CPU or resource allocation, battery consumption, etc,) in real-time systems and networks. The flexibility refers to the ability of the system to dynamically adapt to changes in its operating conditions, without reconfiguration need. He is a member of IEEE and has published 2 book chapters, and over 40 refereed international journals and conference papers.

E-mail: mario.collotta@unikore.it
Faculty of Engineering and Architecture
Kore University of Enna
Cittadella Universitaria
94100 Enna, Italy

Giovanni Pau is a Ph.D. student at the Kore University of Enna. He received his Bachelor degree in Telematic Engineering from Catania University in 2008 discussing a thesis entitled "Study and development of an algorithm for the assignment of cardinality in low power wireless networks" and then in 2010, his Master degree summa cum laude in Telematic Engineering from the Kore University of Enna discussing a thesis entitled "A dynamic control approach to manage real-time traffic light timing through a wireless sensor network". His research interest includes wireless sensor networks, soft computing techniques and real-time systems. In each of these research fields, he has produced several publications in international conferences and journals.

E-mail: giovanni.pau@unikore.it
Faculty of Engineering and Architecture
Kore University of Enna
Cittadella Universitaria
94100 Enna, Italy

Salvatore Vitabile received the Laurea degree in Electronic Engineering and the doctoral degree in Computer Science from the University of Palermo, Italy, in 1994 and 1999, respectively. He is currently an assistant professor with the Department of Biopathology, Medical and Forensic Biotechnologies, University of Palermo, Italy. In 2007, he was a visiting professor in the Department of Radiology, Ohio State University, Columbus, USA. His research interests include computational intelligence, biometric authentication systems, architecture design and prototyping, real-time driver assistance systems, multi-agent system security, and medical data processing and analysis. He has chaired, organized, and served as member of the organizing committee of several international conferences and workshops. He is also the editor in chief of the International Journal of Adaptive and Innovative Systems, Inderscience Publishers, and a member of the board of directors of SIREN (Italian Society of Neural Networks) .

E-mail: salvatore.vitabile@unipa.it
Department of Biopathology and Medical
and Forensic Biotechnologies
University of Palermo
Via del Vespro 129
90127 Palermo, Italy