Biometric Security for Cell Phones

Adrian POCOVNICU
Academy of Economic Studies, Bucharest, Romania
pocovnicu@gmail.com

Cell phones are already prime targets for theft. The increasing functionality of cell phones is making them even more attractive. With the increase of cell phone functionality including personal digital assistance, banking, e-commerce, remote work, internet access and entertainment, more and more confidential data is stored on these devices. What is protecting this confidential data stored on cell phones? Studies have shown that even though most of the cell phone users are aware of the PIN security feature more than 50% of them are not using it either because of the lack of confidence in it or because of the inconvenience. A large majority of those users believes that an alternative approach to security would be a good idea.
Keywords: *biometrics, security, fingerprint, face recognition, cell phones.*

1 Introduction to Biometrics

The etymology of the word biometrics comes from the ancient Greek words: "bios" – life and "metros" – measure.

Biometrics is the science and technology used to uniquely identify individuals based on their physical, chemical or behavioral traits. Biometric systems are assuming that many of the physical, chemical and behavioral human traits are distinctive to each individual, that they can be accurately captured using sensors and devices and that they can be represented in a format appropriate for automatic decision making in regards with the identity of the individual.

Biometric security differentiate from the classic security methods because it identifies an individual based on what he is rather than on what he possesses or what he remembers. The advantage of biometric systems over traditional security methods is that they cannot be stolen or shared.

Traditional security practices often involve the use of two authentication methods: possession based and knowledge based. Knowledge based authentication requires that the users remember a user name and password or PIN numbers or answers to security questions. Possession based can use radio frequency IDs, Smart Cards, Interactive Tokens etc. Possession based authentication has the same usability issue as the knowledge based authentication, if the object used for authentication is forgotten at home, in the hotel room, in the car etc the authentication cannot be performed.

Biometric security systems are using:

- Physical human identifiers like fingerprint, face, iris, retina, DNA, hand geometry and vein geometry
- Behavioral identifiers like speech, signature, and keystroke timing
- Chemical identifiers like odor and body heat.

Biometric systems are used for two purposes. One is to verify that the user is genuine by comparing the acquired biometric trait with the one stored for that user. The other purpose the biometrics are used is to identify a user in which case the acquired biometric trait is compared with a collection of the same traits from multiple users.

2. Elements of a biometric system

A generic biometric system is comprised of the following units:

- A sensor unit that represents the interface between the user and the machine. This is the point where the biometric trait is acquired;
- A processing unit where the acquired biometric is sampled, segmented and features are being extracted. It also includes quality assurance to determine if the quality of the biometric is good enough to be used further in the process. If the quality of the acquired biometric is poor, the user may be asked to present the biometric again;
- A database unit where all the enrolled

biometric templates are being stored and where the templates are being retrieved from in the authentication process;

- A matching unit that compares the newly acquired biometric template with the templates stored in the database and based on decision rules determines either if the presented biometric is a genuine/impostor or if the user is identified or not.

The following image shows the enrolment and recognition process flow in a biometric system.

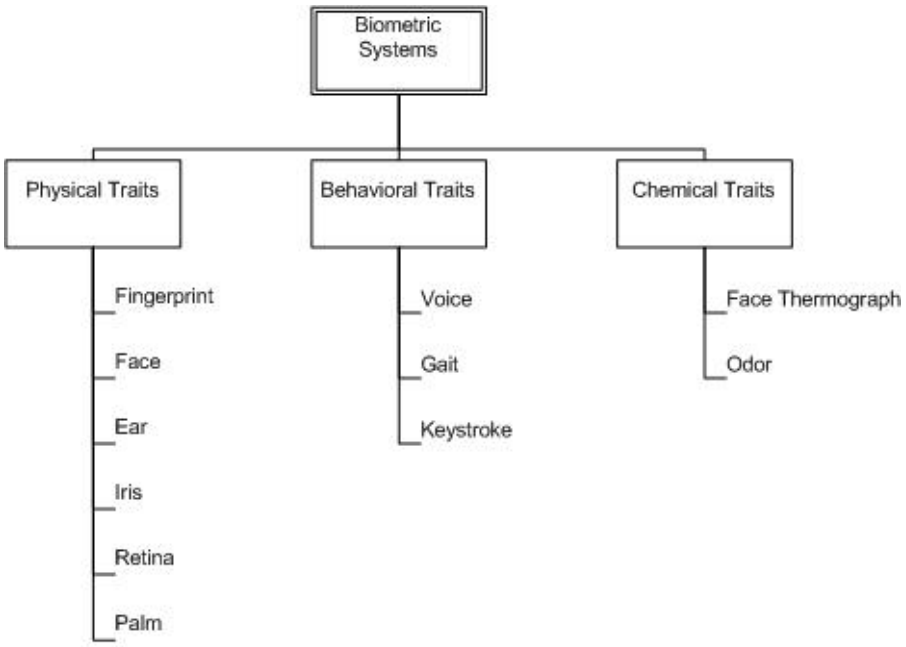


Fig. 1. Biometric Systems Classes

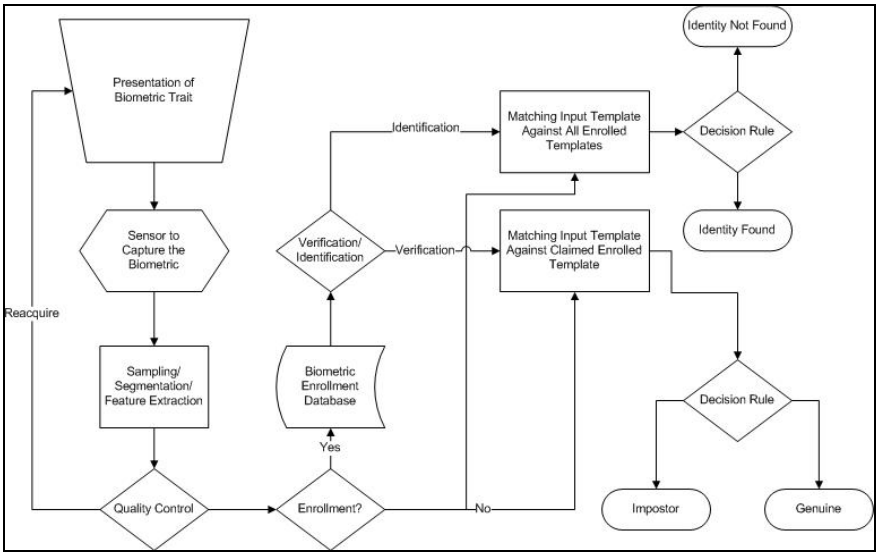


Fig. 2. Enrollment and Recognition in a Biometric System

3. Biometrics characteristics

Choosing between different biometrics is not an easy task. Each biometric has its own pros and cons and the selection of a biometric for an application should depend not only on its matching performance but also on other factors that determine if a biometric treat is suitable for the application or not. The following biometric characteristics should be evaluated in the selection process of a biometric system:

- Universality – each person that is using the biometric system should possess the biometric trait

- Uniqueness – measures how well the biometric trait separates one individual from another
- Permanence – measures how well a biometric trait resists aging
- Collectability – ease of acquisition of the biometric trait without causing inconvenience to the user
- Performance – accuracy, speed, robustness of technology used
- Acceptability – degree of approval of the biometric technology by the users
- Circumvention – ease of use of an imitation of the biometric treat.

No biometric is perfect. None of the biometrics would satisfy 100% the characteristics listed above. Depending on the application, decision makers should review the characteristics and determine which ones are a must for their organization.

Table 1. Comparison of various biometric technologies [2]

Biometrics	Universality	Uniqueness	Permanence	Collectability	Performance	Acceptability	Circumvention
Face	HIGH	LOW	MEDIUM	HIGH	LOW	HIGH	LOW
Fingerprint	MEDIUM	HIGH	HIGH	MEDIUM	HIGH	MEDIUM	HIGH
Hand geometry	MEDIUM	MEDIUM	MEDIUM	HIGH	MEDIUM	MEDIUM	MEDIUM
Keystrokes	LOW	LOW	LOW	MEDIUM	LOW	MEDIUM	MEDIUM
Hand veins	MEDIUM	MEDIUM	MEDIUM	MEDIUM	MEDIUM	MEDIUM	HIGH
Iris	HIGH	HIGH	HIGH	MEDIUM	HIGH	LOW	HIGH
Retinal scan	HIGH	HIGH	MEDIUM	LOW	HIGH	LOW	HIGH
Signature	LOW	LOW	LOW	HIGH	LOW	HIGH	LOW
Voice	MEDIUM	LOW	LOW	MEDIUM	LOW	HIGH	LOW
Facial thermograph	HIGH	HIGH	LOW	HIGH	MEDIUM	HIGH	HIGH
Odor	HIGH	HIGH	HIGH	LOW	LOW	MEDIUM	LOW
DNA	HIGH	HIGH	HIGH	LOW	HIGH	LOW	LOW
Gait	MEDIUM	LOW	LOW	HIGH	LOW	HIGH	MEDIUM
Ear Canal	MEDIUM	MEDIUM	HIGH	MEDIUM	MEDIUM	HIGH	MEDIUM

4. Biometric Systems Benefits

A biometrics security system offers the following benefits:

It doesn't require cooperation. Some biometric systems as face recognition, gait recognition, odor recognition or face thermograph don't require that the user cooperates so that the biometric is collected. Biometric systems prove useful in train stations, airports, stadiums etc., to identify wanted felons.

It guarantees physical location of the user. It can be determined with certainty that the user was that the point where the biometric was collected at the time when the biometric was collected.

It has high-throughput. When there is a need to identify a person from a large population, automatic biometric identification may be the only efficient solution.

The biometric trait is unforgettable. Unlike the classic passwords that need to be remembered, biometric traits cannot be forgotten because they represent something that the user is: physically, behaviorally or chemically.

The biometric trait cannot be lost. Unlike authentication tokens, id cards or passwords written on a piece of paper, biometric traits cannot be lost.

It cannot be shared. Due to their nature biometric traits cannot be shared between users. This ensures that the user that logs in the system is the actual user and not a colleague

that is trying to help.

It is cost efficient. Sure there will be an up-front cost with the installation of the system and with user's education but in the long run it proves cost efficient due to the benefits listed above. It cannot be shared and it guarantees physical location; this way no employee can help-out a colleague that is late by punching-in in the time system on his behalf. And it cannot be lost or forgotten; this way costs of reissuing new identification tokens are reduced, the desktop support time is reduced because the need of resetting passwords will be less, if any, and the down-time of the employees because they've got locked out from the systems is also reduced.

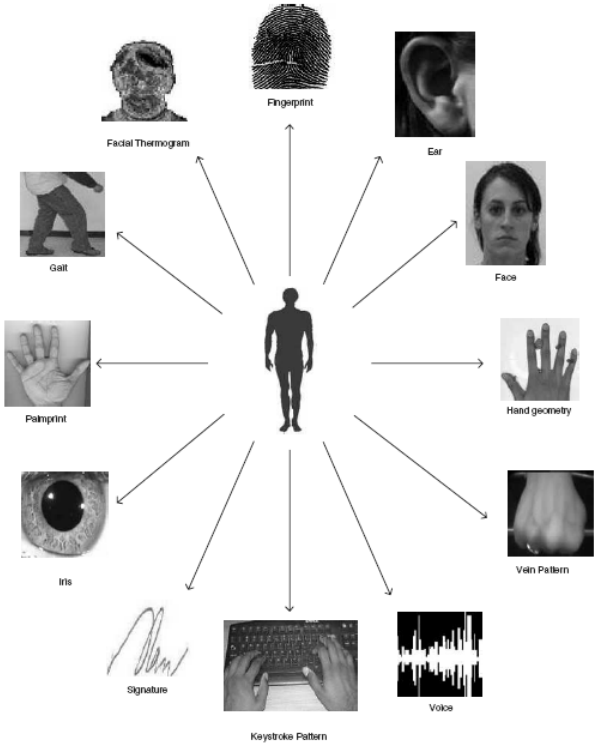


Fig. 3. Examples of Biometric Traits [1]

It can provide emergency identification. In those cases when a person cannot identify itself, using a biometric system may be the only way to find his identity.

It prevents identity theft. In the most cases of identity theft, the impostor used victim's name and personal identification number to create credit card accounts and use those in his behalf. Using biometric security systems makes it practically impossible for impostors to pretend they are somebody else.

It is appealing. Most people find biometric systems appealing because of the ease of use and because it is impressive how a door can be opened by just a swipe of a finger.

5. Cell Phone Devices

In October 13, 1983 first commercial cell phone call was made. The phone cost nearly $4000 and it was weighting about 2.5 pounds. It was a Motorola DynaTAC and only very wealthy people could afford it. Since then cell phones have benefited of an amazing evolution.

Fig. 4. Motorola DynaTAC – First Commercial Cell Phone [5]

Between 1992 and 2002 the main development goal of cell phones manufacturers was to reduce the size of the device. Around 2002 the phones were so small that that it wasn't practical from ease of use point of view to shrink them even more.

This was the time when development started focusing adding other features to the phone beside voice and SMS texting. The initial black and white displayed started being replaced by color displays and screen resolution became higher and higher. The new features that cell phones users started to benefit of are: multimedia, internet, email and personal organizer.

Today's cell phones can be classified in the following categories:

- Entry level cell phone
- Smartphone
- PDA

- Connected music players

Entry level cell phones are optimized for voice communication. Entry level cell phone are sold today in both developed markets and emerging economies. The functionality of such phones has not changed in the past decade but the prices have dropped dramatically due to higher volume production and fewer materials required for production (figure 9). These types of phones are using proprietary operating systems, have no or limited multitasking capabilities for applications.

Third party developers don't have access to the operating system and the only way they can extend the capabilities is by using java programming.

Fig. 5. Nokia 2135 [6]

Fig. 6. Nokia 9300 Smartphone [7]

A **smartphone** is a cell phone with advanced features like internet and email capabilities. Smartphones often use an open operating which allows applications development either by the manufacturer, service provider or third parties.

PDA Phones are an evolution of PDAs. They use operating systems like Microsoft Windows Mobile, Palm OS, Symbian etc. and they include office applications, task scheduling and personal organizer. The differences between PDA phones and Smartphones are becoming smaller but the PDAs tend to keep the original shape.

Fig. 7. HTC Touch Diamond 2 [8]

Fig. 8. iPhone [9]

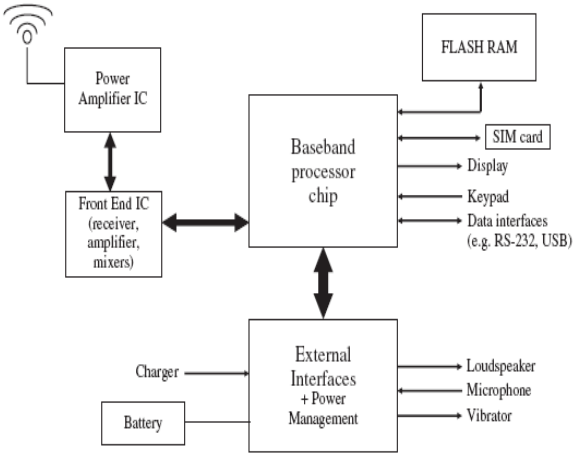


Fig. 9. Block diagram of a voice-optimized mobile phone hardware platform.[10]

Music Player Phones are portable music player phones. They may have integrated internet connectivity (3G), integrated web browser. A very popular example of a device within this category is Apple's iPhone.

6. Biometrics and Cell Phones

Biometric systems can be integrated with cell phones in two ways: As a biometric collecting device or as a stand-alone system to protect unauthorized use of the cell phone. In the first case cell phones are collecting the biometric and then they are passing it via internet or via voice communication to a remote location where it is processed and matched. This proves useful for remote transactions when the identity of the caller has to be proven. As an example, the user calls his bank to make a transaction, he is going to introduce himself as John Smith and in order to verify

his identity he is asked to recite a passphrase. The voice recording is then processed and compared with the sample that was collected when the user enrolled in the system. Face, fingerprint, signature or key stroke are other biometric traits that today's cell phones have the capabilities to collect and transfer them to a remote location.

The other implementation of biometric systems on cell phones is that the entire biometric system resides on the cell phone and it serves the purpose of preventing unauthorized access to cell phone's functions and data.

Biometric systems can replace the annoying PIN security and with a swipe of a finger the phone can be unlocked and used. Today's implementations of biometric systems on cell phones include fingerprint recognition, voice recognition, face recognition, signature recognition and keystroke recognition.

Fingerprint. AuthenTec is a world leader in providing fingerprint recognition biometric systems.

AuthenTec's suite of technologies includes: TruePrint®, TouchStone™, TrueMatch™, TrueFinger™, TrueNav™, TrueYou™.

TruePrint® is used to capture the fingerprint image from the live layer of skin beneath the surface. This has reduces the risk of not accepting a fingerprint because the skin surface has worn-out. TouchStone™ is a technology to create waterproof sensors.

TrueFinger™ is a technology that ensures that only real fingerprints are being read. TrueNav™ is a technology that tracks the motion of the finger on the sensor and it is translated in the move of a cursor on the screen. TrueYou™ technology allows starting different applications depending on the finger that is swiped [11].

Pantech was the first manufacturer to put a fingerprint scanning technology on its GI 100 mobile phone.

Lenovo have integrated fingerprint security in its P960 phone to protect the sensitive data such as VIP recordings, address book information, call history, text messages etc. Fujitsu launched first waterproof fingerprint-enabled mobile phone using TouchStone™ technology from AuthenTec.

Face recognition. ClassifEye and Omron are between the companies that have developed face recognition technology for use as security system in camera-enabled cell phones. The advantage of this technology is that it doesn't require any additional hardware because cameras already exist in most of the phones. The minimum required camera resolution for the system to work is 100,000 pixels [13].

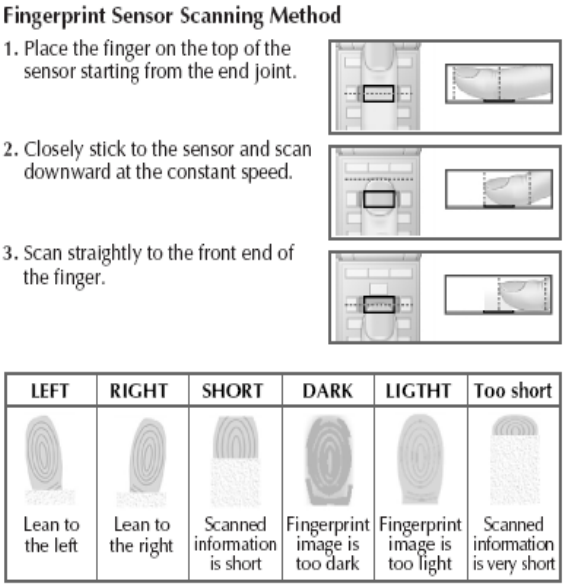


Fig. 10. Pantech GI 100 Scanning Method and Capture Fail Icons [12]

Sharp has integrated face recognition software in its mobile phones. To unlock the device it has to match user's face captured by live camera against a saved portrait.

Fig. 11. Face Recognition Vectors [1]

Dynamic Signature Analysis relies on the manner in which a signature is written rather

than the physical appearance of the signature. Using a PDA users sign in their name multiple times. Features like pressure, direction or velocity are recorded during enrollment [14].

Conclusions

Biometric systems are offering a more convenient way to secure private information stored on mobile phone. Biometrics systems are also adding security to remote transactions initiated using a phone.

Voice recognition, face recognition, signature recognition or keystroke recognition are biometric security systems that can be implemented on most of the mobile phones since they don't require any additional hardware.

Fingerprint recognition systems require additional hardware, a fingerprint scanner, but that sensor has more technologies built in it, like screen cursor movement or having favorite applications starting at a touch of a finger, that is making the devices which have a fingerprint sensor very appealing.

Biometric security systems for cell phone are not only making cell phones more secure but they are also are making cell phones use easier and even more entertaining.

References

[1] A. K. Jain, P. Flynn, A. ROSS, *Handbook of Biometrics*, Springer, USA, 2008.

[2] A. K. Jain, A. Ross, S. Prabhakar, "An introduction to biometric recognition", *IEEE Transactions on Circuits and Systems for Video Technology,* Vol. 14, No. 1, pp. 4-20, January 2004.

[3] K. Revett, PhD, *Behavioral Biometric A Remote Access Approach*, Wiley, UK, 2008.

[4] S. Holtmanns, V. Niemi, P. Ginzboorg, P. Laitinen, N. Asokan, *Cellular Authentication For Mobile And Internet Services,* Wiley, UK, 2008.

[5] *Motorola DynaTAC 8000X – World's First Mobile Phone* [Online]. Available: http://www.tech-fresh.net/motorola-dynatac-8000x-worlds-first-mobile-phone

[6] *Nokia USA – Nokia 2135* [Online]. Available: http://www.nokiausa.com/link?cid=PLAIN_TEXT_842095

[7] *Nokia USA – Nokia 9300 Smartphone – Phones* [Online]. Available: http://nokiausa.com/find-products/phones/nokia-9300-smartphone

[8] *HTC – Products –HTC Touch Diamond2* [Online]. Available: http://www.htc.com/www/product/touchdiamond2/overview.html

[9] *Apple–iPhone – Gallery* [Online]. Available: http://www.apple.com/iphone/_gallery/#image3

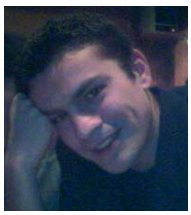
[10] M. Sauter, *Beyond 3G – Bringing Networks, Terminals and the Web Together,* Wiley, UK, 2009.

[11] *Authentec | Technology* [Online]. Available: http://authentec.com/technology.cfm

[12] *Global – Pantech – Manual* [Online]. Available: http://global.pantech.com/fup/support/manual/60_30232759.pdf

[13] *Technology News – PCWorld's Technology news and Reviews* [Online]. Available: http://pcworld.about.com/news/Mar0120 05id119850.htm

[14] *Emerging Biometric Technologies – Crime, Law Enforcements and Corrections* [Online]. Available: http://www.allbusiness.com/crime-law/law-biometrics-fingerprinting/1054 6671-1.html



Adrian POCOVNICU is a PhD Candidate at Academy of Economic Studies. His main research areas are: Multimedia Databases, Information Retrieval, Multimedia Compression Algorithms and Data Integration. He is a Data Integration Consultant for ISA Consulting, USA.