Torben Kuseler; Ihsan Lami; Sabah A. Jassim and Harin Sellahewa, " eBiometrics: an enhanced multi-biometrics authentication technique for real-time remote applications on mobile devices", SPIE 7708 Mobile Multimedia/Image Processing, Security, and Applications (April 28, 2010); doi: 10.1117/12.850022

(http://spie.org/x1125.xml)

eBiometrics: an enhanced multi-biometrics authentication technique for real-time remote applications on mobile devices

Torben Kuseler, Ihsan Lami, Sabah Jassim and Harin Sellahewa
Department of Applied Computing,
University of Buckingham, Buckingham, MK18 1EG, UK
{torben.kuseler,ihsan.lami,sabah.jassim,harin.sellahewa}@buckingham.ac.uk

ABSTRACT

Keywords: Biometrics, mobile devices, face recognition, verification, security

The use of mobile communication devices with advance sensors is growing rapidly. These sensors are enabling functions such as Image capture, Location applications, and Biometric authentication such as Fingerprint verification and Face & Handwritten signature recognition. Such ubiquitous devices are essential tools in today's global economic activities enabling anywhere-anytime financial and business transactions. Cryptographic functions and biometric-based authentication can enhance the security and confidentiality of mobile transactions.
Using Biometric template security techniques in real-time biometric-based authentication are key factors for successful identity verification solutions, but are venerable to determined attacks by both fraudulent software and hardware. The EU-funded SecurePhone project has designed and implemented a multimodal biometric user authentication system on a prototype mobile communication device. However, various implementations of this project have resulted in long verification times or reduced accuracy and/or security.
This paper proposes to use built-in-self-test techniques to ensure no tampering has taken place on the verification process prior to performing the actual biometric authentication. These techniques utilises the user personal identification number as a seed to generate a unique signature. This signature is then used to test the integrity of the verification process. Also, this study proposes the use of a combination of biometric modalities to provide application specific authentication in a secure environment, thus achieving optimum security level with effective processing time. I.e. to ensure that the necessary authentication steps and algorithms running on the mobile device application processor can not be undermined or modified by an imposter to get unauthorized access to the secure system.

1. INTRODUCTION

Recent advances in digital communication systems and the Internet have made a tremendous impact on the way humans interact and socialise, share and manage information, provide services and do business. Advances in science, technology and engineering have brought about super-fast Broadband connections enabling transmission of real-time, high-definition and 3D video content to personal homes. The emergence of Cloud Computing services has accelerated the need for much faster, more secure, and easier to handle data communications. The physical network infrastructure is complemented by wireless communication technologies such as 3G, WiFi and WiMax, providing wider coverage at an affordable cost.

The readily available access to communication networks has increased the usage of traditional internet-based web applications such as e-commerce and has provided a platform for exciting new applications. For example, the 25 March 2010 issue of Cellular news has reported that Mobile banking has overtaken Telephone banking in both the UK and USA. Most notable web-based applications are social networking, collaborative research, Telecare and online gaming. Mobile phones and smart phones, equipped with multiple sensor technologies, are two of the most widely used devices used for anywhere-anytime access to information and location-based services. Reliable, real-time user authentication techniques are a necessity for remote applications on mobile devices to provide security and confidentiality, to protect user privacy and to maintain user acceptability. Biometrics is an ideal tool for person authentication for applications on such mobile devices.

Nowadays-mobile devices such as cellular phones include an applications co-processor that is used to run various applications and interfaces to sensors on the platform. This is available in addition to the phone's Modem processor (handles the communications to the base station such as 3G and 2G modems) and various processors implemented within other functions such as WiFi, Bluetooth, GPS and etc. Application processors on the smart phone class of mobile devices are pretty powerful running at on average 500MHz with a plethora of resources available to ensure powerful performance (for e.g. iPhone 3GS has 600+MHz application CPU while the HTC-HD2 has a 1GHz CPU). As can be seen in Section 3, this study has concluded that these host processors are more than adequate to perform the authentication very fast (previous study concluded that a combined face recognition, handwritten signature and personal-pin authentication algorithm took on average half a second to complete on a 266MHz application processor[1]).

This paper proposes an enhanced, multi-biometric authentication system for real-time application on mobile devices. Recent work on biometrics on mobile devices has shown the feasibility of meeting some of the essential requirements of user authentication. SecurePhone[2], an EU funded project demonstrated the use of a non-intrusive multimodal biometric system for user authentication. It combines face, voice and handwritten signature verification for reliable user authentication. Su et al[3] proposed a fingerprint authentication system for mobile phones with an external fingerprint sensor. A feasibility study of using keystroke analysis to authenticate a mobile phone user is presented by Clarke and Furnell[4]. In[5], an accelerometer sensor, attached to a person's lower leg is used for authentication based on a person's gait.

Although a number of prototype biometric authentication systems have been successfully developed for mobile devices, these schemes are yet to meet satisfactory levels of reliability and user acceptance for real-life application scenarios. The novelty of this study is focused on devising an authentication solution based on combining biometric algorithms with automatic application-security configurability suitable for mobile devices. This solution automatically configures the appropriate authentication based on the available sensors on the host-platform and based on the application requirement, with minimum impact on the host device applications, usability, complexity, implementation and cost.

It is the focus of this work to ensure that, not only high degree of authentication confidence is achieved on a secure platform and is performed with minimum impact on mobile device functionality and cost, but also to easily integrate on the target device and automatically configure itself to meet the application requirements. For example, an application1 can be set, during the installation process, to require a combined face image and Personal Identification Number (PIN) authentication, while application2 can be set to require PIN authentication only, then the algorithms in this solution shall adopt automatically to these various requirements and perform the appropriate tasks in these requirements.

Section 2 explores the various Biometric techniques that can exist on current and future mobile devices, with a focus on the algorithm that can be adopted by this study for the implementation on the iPhone platform. Section 3 describes the criteria used to evaluate the best method to implement this solution on the mobile device that lead to the decision to opt in for a host based implementation. Section 4 describes the architecture adopted for this implementation, while section 5 describes how a built-in-self-test technique can be used to personalise the installation and authenticate the user, based on a PIN, on the mobile device before starting the Biometric authentication to ensure no tampering has taken place within the logic associated with the Biometric algorithm. Finally, section 6 draws the conclusion on this work thus far and highlights the ongoing/future objectives of this study.

2. MULTIMODAL BIOMETRIC AUTHENTICATION

Biometrics refers to measurable physiological and behavioural characteristics such as fingerprints, iris, face, voice and handwritten signatures that can be used to uniquely identify a person. Unlike passwords and PINs (something you know), biometrics are a part of you (something you are), therefore not easily guessed, forged or lost. Moreover, biometric-based authentication systems require the physical presence of the person at the time of authentication.

In automatic person authentication, a biometric template is initially created from one or more samples of the biometric characteristic (e.g. face) and it is typically stored on a database or on a token such as a smart card. During authentication, a live sample of the same biometric characteristic is captured and compared with the stored template to calculate a match score. The decision to accept or reject the claimed identity of a person is based on evaluating the match score against a predefined decision threshold.

2.1 Fingerprint recognition

Fingerprint is the oldest and the most widely used biometric characteristic for person recognition. Two fingerprints are compared by their patterns of ridges and furrows as well as minutia points[6,7]. Most common applications of fingerprint recognition are law-enforcements, forensics, border control and access control to buildings. Although very reliable, a drawback of using fingerprint verification on mobile devices is that it requires a sensor for the sole purpose of capturing fingerprint samples.

2.2 Face recognition

Due to its unobtrusive nature and the easy of capturing face images, the face is naturally the most desired biometric trait for person identification. Common approaches to face recognition are geometrical feature-based approaches and statistical/holistic approaches[8-10]. The study in[11] proposes an efficient wavelet-based face verification scheme for mobile devices that uses the onboard camera of the mobile phone to capture face images for user authentication. The accuracy of face recognition systems is greatly affected by intra-class variations (e.g. illumination, pose and facial expressions) between enrolment and verification stages. As demonstrated in[12] face verification on mobile devices is particularly a challenging task as such devices are used in uncontrolled environments. Recent work on context-aware adaptive face recognition[13] can be adopted and enhanced for mobile platforms to provide robust face verification for uncontrolled environments.

2.3 Handwritten signature recognition

Online handwritten signature verification schemes use multi-dimensional feature vectors, which include velocity, acceleration, curvature and several other features for person recognition[14]. Such features can be easily captured from a mobile phone's touch sensitive screen. The features of handwritten signatures can be modelled by using continuous left-to-right Hidden Markov Models (HMM). One of the difficulties of signature verification on mobile devices is signal noise due to hand motion. However, advance sensors on today's smart phones could be used to correct such motion noise.

2.4 Speaker recognition

A typical speaker recognition system consists of a feature extraction module, a set of client speaker models and world model (background speaker model) and a classification unit. Spectral features such as the Linear Prediction Cepstral Coefficients (LPCCs) and Mel-frequency Cepstral Coefficients (MFCCs) obtained from speech signals are used as speaker-specific features. HMMs and Gaussian Mixture Models (GMMs) are commonly used techniques to encode temporal structure and/or statistical variations of these features to create client and world models[15]. In[1], a speaker verification system that uses MFCC features, modelled using GMMs, has been successfully implemented on a PDA.

2.5 Multimodal biometrics

Authentication systems based on multiple biometric characteristics are known to be more robust than systems that use a single biometric trait[16,17]. Information from multiple biometric sources can be fused at different stages/levels of the authentication process: (1) Feature level fusion - features of each biometric modality is combined into one feature set to represent the person (2) Score level fusion - match scores obtained from each biometric system for the same verification/identification attempt is combined into a single fused score and the claimed identity is accepted if this fused score falls within a predefined decision threshold (3) Decision level fusion - final decision (i.e. accept/reject or the claimed identity) of each biometric authentication system is combined to a single decision (e.g. by majority voting).

In SecurePhone, a multimodal biometric verification system is used to authenticate its owner in order to provide access to sensitive functionalities/applications on the phone. The system fuses the match scores of three biometric modalities: face, speech and voice in order to verify the owner of the phone. Experiments based on biometric data acquired using a PDA demonstrates that the multimodal verifier is capable of achieving an Equal Error Rate (EER) of less than 1%.

2.6 Inertial Sensors and face image 3-axis orientation

The proposed algorithm will take advantage of the presence of 3-axis Gyro and Accelerometer sensors commonly found on Smart-Phone class of mobile device platforms. The algorithm, in the pre-processing stage, will recognise the angle/orientation and movement of the camera at the time of the image and signature capture for the verification process. This information is used to improve the face location and scaling as well as remove motion noise. Thus achieving improved feature vectors for biometric traits.

3. HOST BASED SOLUTION FOR AUTHENTICATION

Various methods and environments for the implementation of Biometric authentication systems have been proposed over the last few years[1,2]. These methods intended to use hardwired implementations so to enhance the security of the authentication algorithm.

This study has evaluated if there are advantages of implementing a hardwired solution, such as an ASIC or FPGA, instead of using the host processor and resources available on the mobile device platform. This is to establish if the overheads associated with a chip implementation outweighs the security advantages associated with the gained security. This is especially critical since the authentication process is normally performed as a one-off task where the host application processor on the mobile device can be dedicated to do this task (i.e. in contrast to tasks such GPS navigation where a continuous real-time processing is required).

It is the target of this study to develop a practical and commercially viable solution to perform personal authentication on mobile devices, i.e. reducing the overheads of performing this authentication to a minimum. The authors expect that this part of the work shall establish a practical usable secure biometric authentication system on mobile devices in terms of cost and implementation complexity (size, adaptability, computational resources, memory, power, etc.). Table 1 shows the criteria used to evaluate a host-based Software implementation versus a chip device, focusing on wireless mobile devices authentication applications. This is important since most of the target platforms have these sensors onboard already.

Table 1. Comparison of host-based and hardwired authentication solutions

Criterion	Host-based solution	Chip implementation
Implementation Complexity	The implementation shall follow typical embedded SW design, implementation and test process. Development iterations are easier and platform installation is very simple	A similar complexity for the design and verification process, but much costly to change and even harder to integrate inside mobile platforms
Security	It was concluded that any special security features that can be implemented by a chip design, could be equally implemented using the host platform and existing resources	There are no tangible security advantages from implementing a dedicated chip to do this authentication. The chip can be harder to corrupt, but is not tamper-proof
Costs	The solution shall use existing host and resources platform, thus no additional hardware is needed, resulting in minimum overhead costs to implement the authentication on any mobile platform	Having a dedicated chip for this authentication involves high NRE costs, chip costs, and board level integration
Performance	Dependent on the target host platform, application processors running up to 1GHz are being used in modern smart phone platforms	Obviously this will always be a faster implementation as Dedicated circuits and optimised hardware algorithms allow maximum performance
Power Consumption	This implementation shall adopt the host platform power scheme as well as managing the authentication process to ensure that effective power compromise	Power consumption on the chip will be dependent on the manufacturing technology. It is expected that the chip will be consuming similar power to the

	and management is achieved when not engaged	host during the authentication process
Flexibility	Developing, installing and executing the authentication algorithms on the host are straightforward and very flexible to alterations. Software upgrades can be propagated and installed by the user any time	This is dependent on the task and the level of change in the process of designing, manufacturing and integration of the chip on the host platform. The process is rigid at large and changes at any stage involves large costs
Hardware requirements	No special hardware requirements are needed to develop or integrate the solution on the target platform. For e.g. Installation can be done by the subscriber	Requires chip / main board compatibility and integration of the chip into the host platform Once on the platform, then it is there even if not used by the subscriber
Space requirements	No additional space on the mobile device platform needed for any special hardware	Requires integration of the chip with rest of circuitry on the platform
Portability	Easy to port, platform independent algorithms can easily be adapted for different mobile device operating systems and sensors	Need to be tailored for every mobile platform implementation. Once done, it is fixed permanently
Memory	Uses host existing resources	Any required memory can be designed in the chip. If access to external memory needed by the chip, then additional resources and configuration has to be tailored to do this, e.g. flash memory

The host-based solution clearly outperforms the chip in most of the cases, for wireless mobile devices applications. Therefore, our evaluation has concluded there will be no additional security gained or meaningful added value to do a chip implementation of the authentication algorithm. For applications, such as surveillance cameras where continuous real-time authentication is required (e.g. to compare real-time images of people faces to large data-base of known individuals), a chip implementation would be more practical to perform multiple authentications and searches in parallel very quickly.

Furthermore, software implementation offers our development application the versatility to be tailored very quickly for various mobile platforms and various security level applications (see Section 4).

This study has therefore concluded that, even if there are hardwired techniques/options that might come to light in the future, then opting for the host based solution will allow us to implement these techniques in software with similar gains. This, coupled with intelligent power management scheme adopted in the implementation has resulted on negligible impact on the phone performance and battery.

4. OVERALL ARCHITECTURE WITH LAYERED AUTHENTICATION

Today's available mobile communication devices offer a wide range of different sensors and input options like camera, touchpad, GPS receiver or gyroscope, which can be used to enhance biometric based verification. Business, financial, medical or social applications require different levels of security to protect involved user data or to authorise transactions. Applications that can be protected by biometric authentication can range from participation in social networks, ecommerce and online shopping, banking applications to transfer of personal medical information to doctors or hospitals.

This study proposes a highly scalable architecture that defines different levels of security for varies applications, see Figure 1. This architecture automatically creates tailored solutions for a wide range of application with special security and usability requirements. The involved biometrics and verification techniques are automatically chosen, and if necessary combined, depending on the available device sensors and the type of application running by the user. Possible levels of protection are for instance; none authentication, PIN based authentication, combination of PIN and one biometric authentication, combination of PIN and several biometric modalities etc. This will lead to a maximum level of protection for security related applications with a minimum of additional impact to the user in non-critical applications. For example, a bank transaction authentication may require the use of a combination of PIN, fingerprint, face and voice verification to identify a legitimate user, whereas accessing a non-critical social network is protected only by face or voice verification.

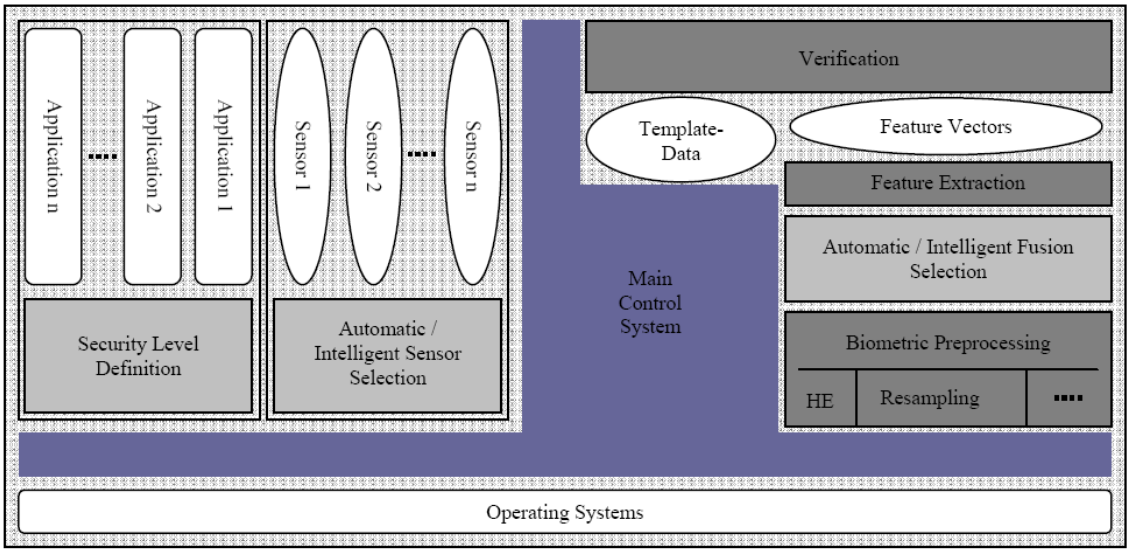

Figure 1. Layered Authentication Architecture

The target of this study is to create a complete authentication system ready for commercial markets with an integrated graphical user interface (GUI) and biometric authentication functionality. In the first stage, the system will be available on Apple iPhones, followed by a version for Google Android based mobile handsets. As this research project focus on commercial markets with the aim to produce a real-world working solution, the growing iPhone and Android popularity is an important factor. Analysts at Gartner expect a 700% growth of Android based systems by 2012 with a total of 150 million iPhone and Android handsets in 2012.

For example, the various sensors (Camera, Multi-Touch display, Accelerometer, Proximity sensor, Ambient light sensor, GPS, Digital compass) available on the iPhone, together with the iPhone OS Technology Layers structure, makes the iPhone a perfect first candidate for a complete secure biometric authentication system. Features like low-level memory allocation and access, iPhone security framework and direct access to sensors offer a flexible and secure framework.

The proposed layered authentication architecture can be configured by various parameters to meet application security and usability requirements and to address a wide range of mobile communication devices at the same time. In addition, the architecture offers a seamless continuity and upgradeability in terms of new hardware sensors available in future mobile devices or improved verification and authentication software algorithms.

4.1 Mobile device sensor availability

If a specific sensor for a biometric modality is not available on a particular mobile device (e.g. fingerprint sensor) the architecture offers to automatically substitute this feature by a single or a combination of other features (e.g. face and hand-written signature) existing on the device to achieve a similar level of accuracy.

4.2 Fusion of biometric modalities

In applications where more than one biometric modality is used (e.g. face and voice), the fusion of the different modalities is one of the key factors of the overall security and accuracy of the system. Using a reasonable fusion method for different combinations of biometric modalities and different application areas and environments is an important factor of verification accuracy. The proposed architecture allows a flexible combination and automatic selection of fusion techniques depending on used biometrics, the desired security level in terms of False Rejection Rate (FRR), False Acceptance Rate (FAR), EER and environmental conditions.

4.3 Flexible sensor integration

Today's state-of-the-art mobile handsets contain much more advanced sensors like CMOS-Image-Sensor (cameras), touch-pad-sensors (free-hand writing) or finger-print sensor at lower prices compared to standard handsets available a few years ago. New sensor and wireless technologies at lower costs and enhanced functionalities are finding their way into mobile devices at much faster design cycles (typical smartphone design cycle is currently 6-months compared to 24-months few years ago). These new sensors can be integrated as an additional biometric input source to the system architecture of this solution, or they can easily replace other previously used sensors or biometric modalities to improve the security, accuracy or performance of the system. No comprehensive adaptation of existing system parts is necessary which makes integration of new sensors a straightforward task.

4.4 Modular authentication algorithm integration

Various verification and authentication techniques based on a wide range of different biometrics have been proposed in the past and a lot of excellent active research from different groups is still going on in this area. Improved verification and authentication methods are developed every day. Flexible integration of new methods and algorithms is a key feature of the proposed layered authentication architecture. Individual parts of the verification process can be easily replaced by new or improved versions.

5. BUILT-IN SELF-TEST IMPLEMENTATION

The purpose of this algorithm is to ensure that the authentication software is clear of any defects generated by malicious software and/or hardware in the host system, or otherwise. This category of algorithms is typically used in the design of integrated circuits to ensure that all physical defects in the circuit are identified after manufacture and if they ever occur.

The implementation of this algorithm is based around inserting a number of Biometric Test Registers (BTR) at carefully selected positions in between the main function blocks of the authentication algorithm, as illustrated in Figure 2. The number of BTRs in the implementation can be chosen to be of any length. BTRs can be configured into 4 functional modes:

1. Scanpath mode: in this mode, a sequence of digital key can be shifted all through the BTRs path. This is used to input the test seed, which is typically a combination of the user's PIN input at the device GUI. At the end of this stage, all BTRs should have a unique value stored in them, and is unique to the user's device.
2. Signature mode: in this mode, the BTRs are run with the authentication algorithm for a predefined number of clocks, minimum 1, based on a specific digit value of the PIN or any chosen combination of the PIN. The residual value in these BTR constitutes the signature that shall be stored on the device during any of the Biometric/authentication enrolment stage. This signature can be shifted out of the BTRs via setting the BTRs in Scanpath mode and clocking the system for a number of clocks equal to the number of implemented BTRs. Typically, this signature is safely stored on the platform for comparison with a similar signature generated every time the authentication process starts.
3. Normal mode: in this mode, the BTRs are transparent to the authentication algorithm and have no part in the generation of the Feature Vector or whatever the authentication algorithm is doing.
4. Rest mode: in this mode, the BTRs can be set to whatever initial value that maybe required by the authentication process, if at all required.

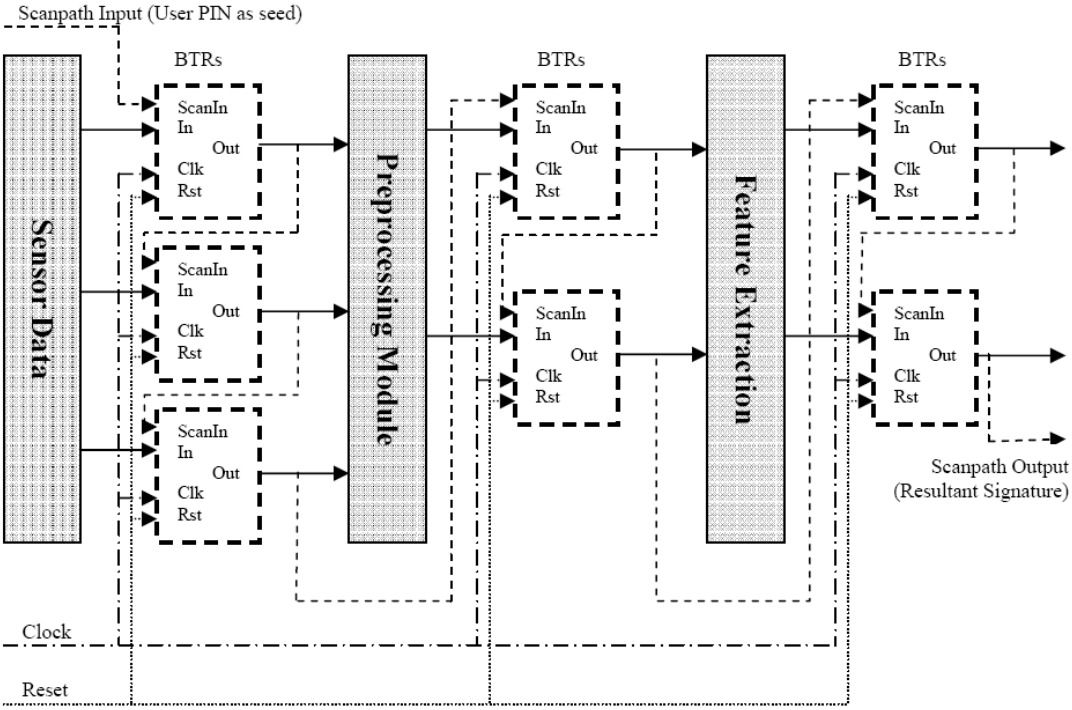

Figure 2. Self-Test Scheme for biometric authentication

Note that, during the enrolment stage, the user shall select the length of the BTRs (see (1) above) or the number of clocks to generate the signature (see (2) above) based on suggested options by the application at the GUI stage. Thus, further diversify the BTR's implementation on the device to ensure that intruder hardware and/or software shall be deterred even further.

It is the intention of this study to use the BTR implementation methodology to further introduce varied mapping of the authentication algorithm on the host platform's memory, and so avoid being target for attacks by hacking (forcing a specific memory location/area to be a specific value or bypassing the authentication) and attackers who pray on the uniformity of the layout of the program register locations in memory. I.e. devise more real-time diversification in the algorithm. I.e. ensures that all pre-designed attacks are void by making the software relocate in memory to ensure that the process of authentication is clean (free from intruders).

6. CONCLUSIONS

This study has investigated hardware and software based solutions for multimodal biometric verification systems on mobile devices. Number of hardware and software implantations for secure biometrics has been compared and evaluated against a set of performance and usability criteria.

The authentication accuracy achieved using both Biometric and PIN authentication is suitable for most Cloud Computing services. This implementation does not only offer an easy to install and use solution for all kinds of mobile device platforms, but also ensures that the authentication is performed within a secure environment. This makes it harder for imposters to compromise parts or the overall authentication process.

This solution is based on a popular mobile handset platform. This focused approach makes it even more commercially desirable. An advantage of the solution is the use of the phone's inertial sensors (accelerometer and Gyro) to recover the acquisition of the user's face image. Therefore achieving improved authentication accuracy.

This study is ongoing to establish a practical authentication process on mobile devices based on amalgamation of enhanced-Biometric algorithms and implementation techniques. The target of this work is to ensure that the overhead associated with implementing complex, secure and accurate authentication solutions, in terms of authentication accuracy, security level, real-time performance, and cost of implementation and procuring is kept to a minimum and is commercially viable.

REFERENCES

1. A. C. Morris, J. Koreman, H. Sellahewa, J. Hendrik-Ehlers, S. Jassim, L. Allano, and S. Garcia-Salicetti, "The SecurePhone PDA database, experimental protocol and automatic test procedure for multimodal user authentication," http://www.coli.uni-saarland.de/SecurePhone/documents/PDA_database_and_test_protocol.pdf (20/08/2006), January 2006.
2. R. Ricci, G. Chollet, M. V. Crispino, S. Jassim, J. Koreman, M. Olivar-Dimas, S. Garcia-Salicetti, and P. Soria-Rodriguez, "Securephone: a mobile phone with a biometric authentication and e-signature support for dealing secure transactions on the fly," in Mobile Multimedia/Image Processing for Military and Security Applications, Proc. SPIE 6250, p. 625009, April 2006.
3. Q. Su, J. Tian, X. Chen, and X. Yang, "A fingerprint authentication system based on mobile phone," in AVBPA, pp. 151-159, 2005.
4. N. L. Clarke and S. M. Furnell, "Authenticating mobile phone users using keystroke analysis," International Journal of Information Security 6, pp. 1-14, January 2007.
5. D. Gafurov and E. Snekkenes, "Gait recognition using wearable motion recording sensors," EURASIP Journal on Advances in Signal Processing 2009, pp. 1-16, 2009.
6. A. K. Jain, L. Hong, and R. Bolle, "On-line fingerprint verification," IEEE Transactions on Pattern Analysis and Machine Intelligence 19, pp. 302-314, April 1997.
7. S. Pankanti, S. Prabhakar, and A. K. Jain, "On individuality of fingerprints," IEEE Transactions on Pattern Analysis and Machine Intelligence 24, pp. 1010-1025, August 2002.
8. R. Brunelli and T. Poggio, "Face Recognition: Feature vs. Templates," IEEE Transactions on Pattern Analysis and Machine Intelligence 15, pp. 1042-1053, October 1993.
9. M. Turk and A. Pentland, "Eigenfaces for Recognition," Journal of Cognitive Neuroscience 3(1), pp. 71-86, 1991.
10. P. N. Belhumeur, J. P. Hespanha, and D. J. Kriegman, "Eigenfaces vs. Fisherfaces: Recognition Using Class Specific Linear Projection," IEEE Transactions on Pattern Analysis and Machine Intelligence 19, pp. 711-720, July 1997.
11. S. Jassim and H. Sellahewa, "A wavelet-based approach to face verification/recognition," in Unmanned/Unattended Sensors and Sensor Networks II, Proc. SPIE 5986, p. 598609, October 2005.
12. H. Sellahewa and S. A. Jassim, "Performance Evaluation of Wavelet-based Face Verification on a PDA recorded database," in Mobile Multimedia/Image Processing for Military and Security Applications, Proc. SPIE 6250, p. 62500A, April 2006.
13. H. Sellahewa and S. A. Jassim, "Image-quality-based adaptive face recognition," IEEE Transactions on Instrumentation and Measurement 59, pp. 805-813, April 2010.
14. J. G. A. Dolfing, E. H. L. Aarts, and J. J. G. M. V. Oosterhout, "On-line Signature Verification with Hidden Markov Models," International Conference on Patter Recognition 14(2), pp. 1309-1312, 1998.
15. D. A. Reynolds, "Speaker identification and verification using gaussian mixture speaker models," Speech Communication 17, pp. 91-108, August 1995.
16. A. Ross and A. Jain, "Information fusion in biometrics," Pattern Recognition Letters 24, pp. 2115-2125, September 2003.
17. L. Allano, A. C. Morris, H. Sellahewa, S. Garcia-Salicetti, J. Koreman, S. Jassim, B. Ly-Van, D. Wu, and B. Dorizzi, "Non intrusive multi-biometrics on a mobile device: a comparison of fusion techniques," in Biometric Technology for Human Identification III, Proc. SPIE 6202, p. 62020P, April 2006.