2009 Fifth International Conference on Intelligent Information Hiding and Multimedia Signal Processing

An Approach to Biometric Identity Management Using Low-Cost Equipment

Robert Mueller
Giesecke & Devrient GmbH
Prinzregentenstr. 159
D-81677 Muenchen, Germany
robert.mueller@gi-de.com

Raul Sanchez-Reillo
University Carlos III of Madrid
Univ. Group for Identification Technologies
Avda. Universidad, 30
E-28911 – Leganes (Madrid); SPAIN
rsreillo@ing.uc3m.es

***Abstract* – Digital identities are becoming increasingly popular. Professional implementation relies upon a secure embedded system and two-factor authentication for managing the important credentials. Although biometric user authentication is sometimes employed, it is still costly and difficult for the average user. The hardware currently available does not always use embedded processing or include a certified controller.**
We designed a system that allows digital identity management using two-factor authentication. This system considers typically existing IT infrastructure, relies upon on-card-biometric-comparison and operates from a portable device transparent to the host system.

Index Terms – biometrics, identity management, fingerprint, on-card-biometric-comparison, webcam

I. Introduction

A digital identity consists of the personal data of a user along with cryptographic keys and certificates. This digital identity allows the user to communicate authentically, use subscribed web services or file contracts with individuals she had never met before. The security and convenience is based on a Public Key Infrastructure (PKI), certification authorities and secure signature creation devices, i.e. smart cards. These embedded systems allow two-factor authentication to access cryptographic capabilities. To positively prove the legitimate owner of a smart card, biometric user authentication is important. In contrast to passwords, biometric characteristics cannot be stolen or transferred.

Today, various PKI tokens are available which implement fully embedded biometric user authentication. These devices usually have a form factor of a large USB flash drive and contain a fingerprint sensor with embedded processing. Some of these devices do not include a smart card chip and are therefore unsuitable for preventing spying on personal data. Other devices require driver and software installation on the host system which is often not possible for mobile users. None of these tokens are available today without a significant investment.

II. Requirements and Infrastructure

We first defined the requirements, which a system for secure identity management should satisfy. In addition, we analyzed the typical infrastructure that a mobile user is faced with in a networked world.

A. Requirements:

1) *Biometric user authentication:* Reliable user authentication is important for managing a digital identity. PINs and passwords have become no longer suitable for satisfying the security constraints. Biometric user authentication guarantees that the digital identity remains tied to the legitimate owner.
2) *On-card-biometric-comparison:* Biometric data is sensitive from a privacy point of view. As far as privacy and security aspects are concerned, The biometric reference template shall never leave the secure environment of a smart card chip both for privacy and security aspects. The full template matching process must be executed within a smart card chip.
3) *Zero footprint:* The user may not always operate on her own equipment, but instead, work in an Internet Café or on a PC or notebook of a friend. The system should not require any driver installation or administrator privileges.
4) *Portable:* A mobile user today does not want to carry a large device for managing her digital identity. Ideally, this token should not be larger than a USB mass storage device or a cell phone.
5) *Low-cost:* Whereas governmental institutions and large corporations can afford the hardware cost for a device integrating all the required technologies, the average user is expected to use standard low-cost equipment.

B. Infrastructure

The typical IT infrastructure today consists of notebooks or workstations featuring a USB interface. Some of the notebooks include an integrated fingerprint sensor, while the majority of new notebooks and even some workstations are equipped with a webcam.

978-0-7695-3762-7/09 $26.00 © 2009 IEEE
DOI 10.1109/IIH-MSP.2009.50

III. BIOMETRICS

A variety of biometric traits is used for personal identification. The following TABLE I. lists a selection of prominent technologies considered for the authentication of a claimed identity of an individual.

TABLE I. BIOMETRIC TECHNOLOGIES

Biometric trait	Characteristics		
	Privacy of data	Sensor available	Suitable for on-card-comparison
fingerprint image and related data	fair	in high-end notebook	yes
facial image	public	webcam	yes
iris image	fair	(webcam)	yes
dynamic signature	good	no	yes
keystroke dynamics	good	yes	yes
voice & lip movement	good	yes	no
DNA	good	no	?

The privacy column indicates the degree of difficulty for acquiring raw sample data of the specified biometric type without cooperation and knowledge of the individual. While the facial image can be easily grabbed while staring at a shop window, this method requires significantly more criminal energy, for example, lift a latent fingerprint from a touched glass and create a fake fingerprint.

Some technologies such as speaker recognition via the voice have the obvious advantage that a sensor – in this case a microphone – is usually available in the host machine. The algorithmic approach has an impact on whether biometric user authentication can be reliably carried out in a smart card chip.

IV. TECHNICAL APPROACHES

Current systems have two main disadvantages. Firstly, they are normally quite expensive (e.g. fully self-contained USB devices equipped with sensor and embedded processing). Secondly, these solutions require that the software be installed on the host machine to enable, for example, operating a fingerprint sensor or smart card reader. The first disadvantage shall be overcome by using only existing sensor hardware for acquiring the biometric data. The second drawback we addressed with an embedded token that implements both a smart card interface without driver installation and a standard mass storage device to carry all the software.

Certain biometric traits are obviously not feasible as shown in TABLE I. . From a first point of view, face recognition and keystroke dynamics seem to be the best choice. However, our implementation of keystroke dynamics did not prove to implement a suitable discriminative power. Face recognition is subject to different lighting and environmental conditions [4] that could be overcome with a cooperative user. The main disadvantage of this technology is privacy. A face can easily be captured without notice of the user. People enrolled in social networks and online communities frequently disclose facial images on a web page.

Our approach first targeted the fingerprint sensors mounted in various high-end notebooks. If we could somehow manage to access these sensors and obtain a raw image, it would be possible to execute the rest of the authentication from the flash drive and process the template matching in the smart card chip. It turned out that it is nearly impossible to have low-level access to the integrated sensors in notebooks. These sensors are usually tied to a companion chip or TPM (Trusted Personal Module) for carrying out image processing and matching. Access at the application level might be possible but the privacy requirement does not allow the matching process to be shifted to another entity.

Another aspect to consider is that only a fraction of notebooks is equipped with a fingerprint sensor today. The webcam is much more prominent since the advent of IP telephony. We attempted to acquire a fingerprint simply with a regular webcam. The result in Fig. 1 shows that this is also not feasible.

Fig. 1. Fingerprint image acquired with a webcam

The camera is calibrated to work at a typical viewing distance. Due to insufficient light, the fingerprint image does not show a suitable ridge structure. Fingers are three-dimensional and can have large waves in the skin. It would be necessary to recalculate the finger sphere into a flat surface for measuring e.g. minutiae distances.

For capturing the fingerprint, the finger was pressed against a glass plate and an external light source was used to enhance the situation for insufficient lighting. The external light source must be placed sideways in order to avoid reflections on the glass plate. This yielded fingerprint images which one can start with. Further tests have shown that the glass plate is not required when the autofocus feature of the camera is deactivated. The low-cost devices Microsoft Lifecam VX3000 and Philips SPC630NC require manual adjustment of sharpness and produced suitable images without a glass plate. The advanced products Microsoft Lifecam VX6000 and Philips SPC1330NC could not be used since autofocus is included and limited to a minimum distance of approximately 30 centimeters.

The normal techniques such as histogram stretching and normalization [1][2] were not sufficient to work with the webcam images. The reason for this is that the images show significant shadows and regional overexposure. A common technique in image processing and graphing practice, the gamma correction [17] is applied to the fingerprint images from the webcam.

The pre-processing step is added to the existing image processing algorithm (see Fig. 4). The process continues by enhancing the gray scale image with directional Fourier filters and extracting data that is suitable for matching [2][8]. Normally, these features are fingerprint minutiae. We decided to use the hybrid algorithm introduced in [3], which relies on minutiae and skeleton data. Fig. 2 shows the result of processing a webcam image and extracting features.

The standardized fingerprint minutiae and skeleton as defined in [6][7] are used in our approach. For details on how to generate this data, [3] is suggested reading.

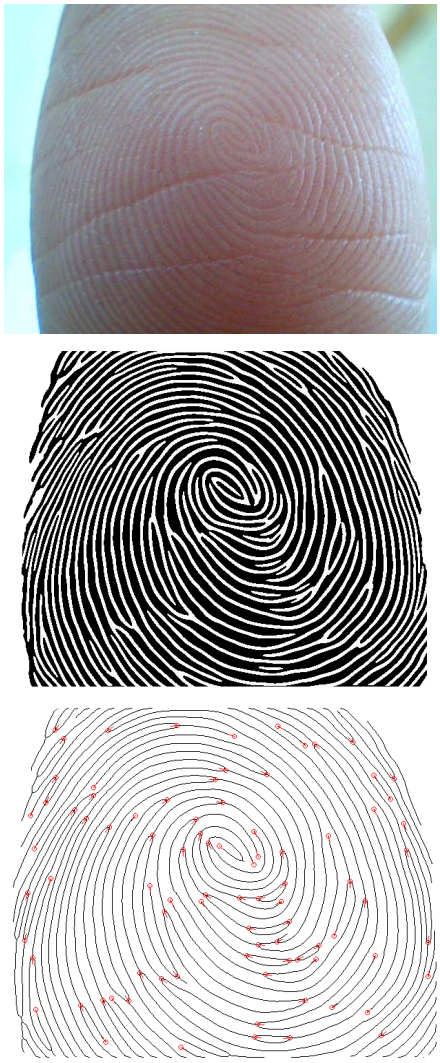


Fig. 2. Raw webcam image, processed and binarized image, extracted minutiae and skeleton

Conversely to most common optical and silicon fingerprint sensors, light pixels of the fingertip represent ridges while darker pixels indicate valleys. Image parts with insufficient contrast or ridge structure are excluded from the region of interest [2]. This is not visible in the sample image in Fig. 2 but important for the average finger image.

V. System Architecture

The system design is based on a Mobility Token MicroSD [16]. This product includes a smart card chip with an ISO-compliant On-card-biometric-comparison implementation described in [3]. Fig. 5 shows a photo of the Mobility Token MicroSD. The token runs without installing a host driver by translating mass storage commands into smart card APDUs [5][10]. It also includes sufficient flash memory and implements a mass storage device to carry all the software developed in this research. The webcam of the host computer system is used to acquire fingerprint images for processing.

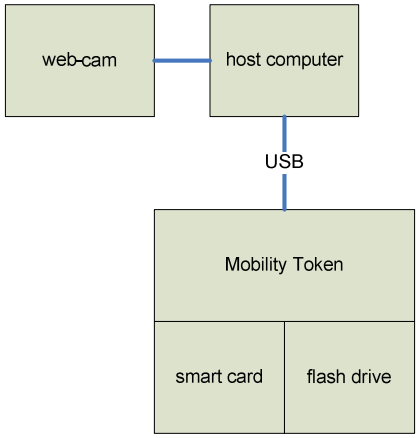


Fig. 3. System architecture: The Mobility Token includes both smart card with on-card-biometric-comparison algorithm and flash drive containing the software

The algorithmic approach shown in Fig. 4 is similar to the detailed description in [3] except that the additional pre-processing is required to cope with the webcam generated fingerprint images.

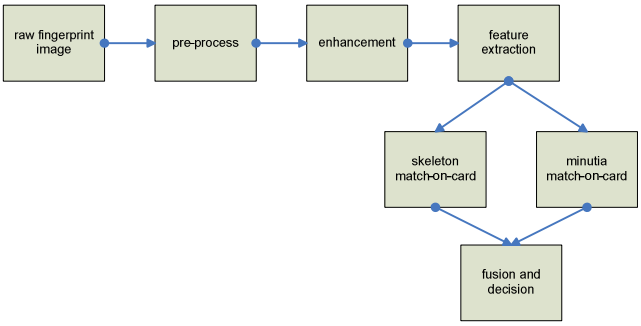


Fig. 4. Algorithm data flow. The matching and decision level fusion is executed in the smart card chip.

Fig. 5. StarSign Mobility Token MicroSD hardware, picture taken from [16]

VI. Experimental Results

A. *System operation:*

The token with MicroSD carrying the digital identity of the user in the smart card chip and authentication software in the flash mass storage runs without driver installation. The webcam is accessed via a system API (see discussion below) or generic camera driver of the operating system.

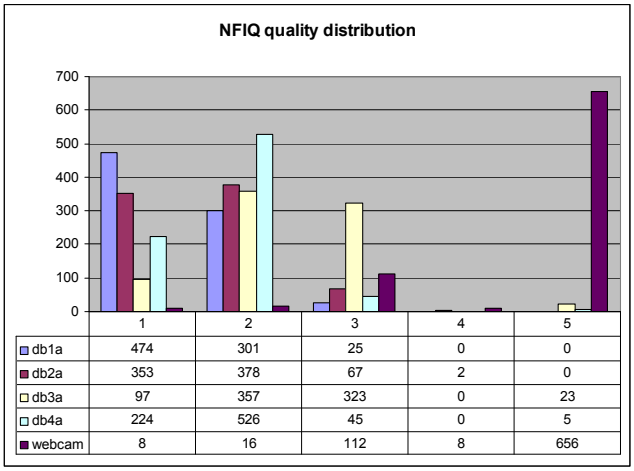
B. *Test data:*

For testing the system, a total of 400 fingerprint images from 36 fingers of 6 persons were generated with the webcams from Apple, Microsoft and Philips mentioned above. The first 4 impressions from every finger served as training set to configure the parameters of the matcher, whereas the second 4 impressions were used to compute error rates. All webcams had a resolution of 1280x1024 pixels but could be operated at 640x480 pixels without loss of accuracy. Regardless of the resolution, the lighting is critical and the feedback of a live image is mandatory to produce sufficient image quality.

All users were highly cooperative and aged from 19 to 44. Sufficient light conditions were achieved by attaching an inexpensive small lamp to the screen of the iMac computer. The cameras connected via USB did also work in normal daylight when carefully presenting the finger at the right orientation.

To assess the quality of fingerprint images acquired with a webcam, the NFIQ algorithm from NIST was used [18]. The NBIS software containing the algorithm is available free of charge at http://fingerprint.nist.gov/NBIS/index.html. This software assigns a quality score to fingerprint images ranging from 1 (best quality) to 5 (lowest quality). The same tool was applied to the FVC2002 databases db1a through db4a with 800 fingerprints, respectively. Results are shown in Fig. 6.

The quality score frequencies of the webcam images were scaled by a factor 2 since only 400 images were available. It is conspicuous from the diagram that any of the dedicated sensors and the artificial fingerprints (db4a) produces a significantly better image quality. The NFIQ algorithm seems to assign the score value 4 quite rarely.



	1	2	3	4	5
db1a	474	301	25	0	0
db2a	353	378	67	2	0
db3a	97	357	323	0	23
db4a	224	526	45	0	5
webcam	8	16	112	8	656

Fig. 6. NFIQ analysis of FVC2002 in comparison to webcam fingerprint images.

C. *Test execution:*

After proving that the system satisfies the predefined requirements (see discussion below), the webcam images were actually stored. The comparison was performed offline by simulating the smart card with a PC program in order to compute the error rates. The result is shown in TABLE II. .

To evaluate the practical use of the system, we include in the same table the results from running the algorithm with the FVC2002 databases. For this test, part of FVC2004 served as a training set.

TABLE II. Error Rates at Favourable Working Point

Database	FAR	FRR
webcam	0.18 %	10.29 %
FVC2002	0.02 %	6.54 %

It is quite evident that our method is inferior to a common fingerprint sensor database generated with a dedicated sensor. However, it is still in the same range as other common fingerprint systems and satisfies the listed requirements, namely use of low-cost equipment.

We intentionally do not show an ROC (Receiver Operating Characteristic) curve here because the test data set is very small and the results should not be misinterpreted as credible error rates of the system. The level of cooperation required by our proof-of-concept system goes beyond that of what can be expected from the average user. We consider, however, that the approach is feasible and the system has the potential to be improved and achieve better error rates.

D. *Life detection:*

In addition to the tests with live fingerprints, a printout of a binarized fingerprint image was held at the webcam and acquired again. As expected, the system could be fooled with this simple fake fingerprint since it does not implement any measures to detect artificial fingerprints. This is not considered a dramatic disadvantage of the system because it is

designed merely for privacy, and most dedicated fingerprint sensors can also be easily fooled [19]. However, it should be noted that the webcam approach is more vulnerable to fake fingerprints. It is suggested that high security applications combine biometric user authentication with password entry and smart cards – thus enabling a three factor authentication.

VII. Results and Outlook

An original system architecture has been designed to implement cost-efficient digital identity management with biometric user authentication. The proposed method is possible by acquiring fingerprint images with a webcam and pre-processing these before they undergo regular image processing and feature extraction algorithms. The matching is carried out in a smart card chip as required for privacy and security. Our system is based on a commercially available hardware token featuring flash memory and does not require a dedicated sensor.

The following requirements were fulfilled:

1) *Biometric user authentication: satisfied.* A fingerprint verification algorithm is used to authenticate the user.
2) *On-card-biometric-comparison: satisfied.* The matching algorithm runs in the smart card chip and combines minutia and skeleton matching results.
3) *Zero footprint: PARTLY satisfied.* The MobilityToken MicroSD used runs without hardware installation on the host machine. All software is carried in the mass storage. It was necessary to install a package on the host to directly access the webcam for image acquisition via an API.
4) *Portable: satisfied.* The only thing that a user has to carry with her is a Mobility Token MicroSD, having the form factor of a thumb drive.
5) *Low-cost: satisfied.* No specific hardware except for the token is required. In particular, no fingerprint sensor or other dedicated sensing device is required due to the webcam approach.

The experimental results with a small test data set show that the method is inferior but comparable to results achieved with common fingerprint databases. The technique has the potential to be enhanced with more tolerant image processing. The zero footprint requirement could possibly be satisfied when accessing the webcam through an open interface such as a browser plug-in. A portable browser would have to be delivered on the Mobility Token flash memory to realize the idea.

Future work will include a multi-modal system combining fingerprint and face on-card-biometric-comparison. The parameters for the fingerprint system can be set less strict if the additional face comparison is carried out with a fusion of results on the score level. The dynamic color change when pressing a finger against the glass plate looks quite unique. Resistance against fake fingerprints may be realized when examining this behavior in detail.

The IEEE paper [20] describes the use of low-cost cameras for fingerprint biometrics. This paper was detected only after submission. While part of the initial idea is similar to our proposal, the architecture and algorithmic approach are different. Qualitative results are comparable in terms of algorithm performance. The hardware system architecture is not addressed in [20]. The paper provides valuable background information for researchers.

Further investigations on the use of low-cost equipment for digital identity management are suggested future work.

References

[1] D. Maltoni, D. Maio, A.K. Jain, S. Prabhakar, Handbook of Fingerprint Recognition, *Springer, New York, 2003.*

[2] R. Mueller, "Fingerprint Verification with Microprocessor Security Tokens" *Ph.D. thesis, Munich University of Technology, Utz Verlag Muenchen, May 2001.*

[3] R. Mueller U. Martini, "Decision Level Fusion in Standardized Fingerprint Match-on-Card" *, ICARCV2006, IEEE.*

[4] Belen Fernandez-Saavedra, Raul Sanchez-Reillo, Raul Alonso-Moreno, R. Mueller, "Evaluation Methodology for Analyzing Environment Influence in Biometrics" *ICARCV2008, IEEE.*

[5] ISO/IEC: Information technology – Identification cards – Integrated circuit(s) cards with contacts, International Standard ISO/IEC 7816 Part 3: Electronic Signals and Transmission Protocols
Part 4: Interindustry Commands for Interchange

[6] ISO/IEC: FDIS 19794-2, Biometric data interchange Formats — Part 2: Finger minutiae data, *ISO/IEC JTC1 SC37, 2005*

[7] ISO/IEC: FDIS 19794-8, Biometric Data Interchange Formats – Part 8: Finger Pattern Skeletal Data, *ISO/IEC JTC1 SC37, 2006*

[8] A. K. Jain, L. Hong and R. Bolle: On-line Fingerprint Verification, *IEEE Transactions on PAMI, Vol. 19, No. 4, pp. 302-314, 1997.*

[9] A. K. Jain, S. Prabhakar and S. Chen: Combining Multiple Matchers for a High Security Fingerprint Verification System, *Pattern Recognition Letters*, *Vol 20, No. 11-13, pp. 1371-1379, 1999*

[10] W. Rankl, W. Effing: Smart Card Handbook, *John Wiley & Sons, New York, 1997*

[11] A. Ross, A. Jain, J. Reisman: A Hybrid Fingerprint Matcher, *pattern recognition vol. 36, 2003 pp. 1661-1673, Elsevier Science*

[12] J. Fierrez-Aguilar, Y. Chen, J. Ortega-Garcia, A. K. Jain, Incorporating Image Quality in Multi-Algorithm Fingerprint Verification, *to appear in ICB06*

[13] J. Daugman, Combining Multiple Biometrics, http://www.cl.cam.ac.uk/users/jgd1000/combine/combine.html

[14] P. Grother et al, NISTIR 7296 MINEX, Performance and Interoperability of the INCITS 378 Fingerprint Template, *NIST, March 2005*

[15] ISO/IEC: FDIS 19794-3, Biometric Data Interchange Formats – Part 3: Finger Pattern Spectral Data, *ISO/IEC JTC1 SC37, 2006*

[16] Giesecke & Devrient GmbH: StarSign USB Token MicroSD datasheet, 2008

[17] J. Dijk, P.W. Verbeek: Lightness Filtering in Color Images with Respect to the Gamut, *CGIV 2006, Proc. Third European Conference on Colour in Graphics, Imaging, and Vision*

[18] Craig I. Watson, Michael D. Garris, Elham Tabassi, Charles L. Wilson, R. Michael McCabe, Stanley Janet, Kenneth Ko: User's Guide to NIST Biometric Image Software (NBIS).

[19] T. Matsumoto, H. Matsumoto, K. Yamada, S. Hoshino: Impact of Artificial Gummy Fingers on Fingerprint Systems, *Proc. of SPIE Vol. #4677, Optical Security and Counterfeit Deterrence Techniques IV, 2002*

[20] Vincenzo Piuri, Fabio Scotti: Fingerprint Biometrics via Low-cost Sensors and Webcams, *Biometrics: Theory, Applications and Systems, 2008. BTAS 2008. 2nd IEEE International Conference on*