A CLASSIFICATION OF BIOMETRIC SIGNATURES

Arslan Brömme

Computer Vision Group
Department of Simulation and Graphics
Otto-von-Guericke University of Magdeburg, Germany
arslan.broemme@isg.cs.uni-magdeburg.de

ABSTRACT

The domain of biometrics lacks of a systematical approach for classifying biometric signatures for biometric authentication, detection, and reaction systems. This paper presents a first approach to fill this gap. Outlining the *general authentication process* and analyzing the meaning of the term *signature* from selected sciences, a definition of the term *biometric signature* as (bin|n-)ary coded representation of biometric characteristics is derived. To show the suitability of the suggested definition, its role within the core processes of biometric authentication systems (enrollment, authentication, derollment) is described.

1. INTRODUCTION

Each human being has static and dynamic physiological and behavioral biological characteristics, which can be used for biometric person recognition. Typical biological characteristics are fingerprints, iris patterns, face proportions, DNA short tandem repeats (static-physiological), pupil dilatation and contraction (dynamic-physiological), and voice, lips movement, handwriting (behavioral - based on statistical differences and/or trained knowledge) [1].

For proving the authenticity of a person against and for identification by IT systems with(out) reaction, several sets of methods (also called factors) can be combined: person knowledge (e.g. identifier, user name and password, passphrase), person possession (e.g. tokens, smartcards), person location (e.g. satellite based location), person attribute (e.g. face proportion, iris patterns, fingerprint minutiae), or time.

The domain of biometrics lacks of a systematical approach for classifying biometric signatures for biometric authentication, detection, and reaction systems. This paper presents a first approach to fill this gap. Outlining the *general authentication process* (sect. 2.1) and analyzing the meaning of the term *signature* from selected sciences, a definition of the term *biometric signature* is derived (sect. 4). To show the suitability of the suggested definition, its role within the core processes of biometric authentication systems (enrollment, authentication, derollment) is described.

2. BIOMETRICS IN IT SECURITY

For authentication purposes *IT security biometrics* uses the mathematical definitions of a *metric* and a *metric space*.

Definition: [A *metric* is] a nonnegative function $g(x, y)$ describing the "distance" between neighboring points for a given set. A metric satisfies the *triangle inequality* $g(x, y) + g(y, z) \geq g(x, z)$ with equality iff $x = y$, and is symmetric, so $g(x, y) = g(y, x)$.

Definition: [A *metric space* is] a set S with a global distance function (the metric g) which, for every two points x, y in S, gives the distance between a nonnegative real number $g(x, y)$. A metric space must also satisfy (1) $g(x, y) = 0$ if, and only if, $x = y$, (2) $g(x, y) = g(y, x)$, and (3) $g(x, y) + g(y, z) \geq g(x, z)$ *triangle inequality* [3]. The plane and three-dimensional space are metric spaces with the usual distance [4].

Based on these mathematical definitions it can be stated that biometrics in IT security makes use of metrics and metric spaces within distance calculations and comparisons of *biometric characteristics*, *biometric signatures*, and *biometric templates*.

Definition: *IT security biometrics* is defined as a person recognition method based on the sensing of a person's biological characteristics, measuring of the captured or scanned biometric characteristics (raw data and sensor calibration data), calculating of biometric signatures and biometric templates, and verifying and identifying against biometric templates and (hashed) biometric signatures with regard to the mathematical definitions of metrics and metric spaces. The (hashed) biometric signatures are used for authentication purposes against IT based authentication systems.

2.1. Biometric Authentication Systems

A biometric authentication system can be considered as a part of an IT infrastructure (for purposes which vary from IT based door control mechanisms over activation of electronic signature processes within smartcards up to identity verification within electronic business processes) where a

person is subjected to a general authentication process for receiving e.g. access rights to IT system resources, activity regulations and information non-repudiation within electronic business processes, or the permission to pass a gate or to enter a place or room.

The *general authentication process* can be divided into the five subsequent phases: *enrollment, (biometric) authentication, authorization, access control*, and *derollment and authorization withdrawal*.

During the phase of *enrollment* appropriate biometric raw data of a person is captured, the biometric signature (template) for the biometric authentication is computed, and the relevant biometric and personal data is stored in a biometric database [2]. A person's authenticity is checked by an identification (1:c) or verification (1:1) comparison of the actually computed biometric signature with the biometric signature class in the phase of *biometric authentication*[1] with(out) being combined with authentication methods based on a person's knowledge, possession, location, and time.

Implicit and explicit authorizations are given to the person (represented as a user when accessing IT system resources) in the *authorization* phase with respect to strong and weak authorizations. In the *access control* phase the access to e.g. IT system resources or activity control within electronic business processes is granted by an *access management system*[2]. In the phase of *derollment and authorization withdrawal* a person is derolled and the person's access rights are removed.

2.2. Biometric Detection and Reaction Systems

For special purposes of fight against terror and criminality – not necessarily in the IT security domain – special biometric IT systems and infrastructures can be used which are based on *biometric identification processes* for biometric detection systems, and *biometric-collect-detect (biocode) processes* and *biometric-collect-detect-react (biocodeR) processes* for biometric reaction systems [1]. Biometric signatures can be used for these classes of biometric systems which are similar to those used within the core processes of biometric authentication systems. For this reason this paper focusses on the biometric signatures used within the three biometric processes of enrollment, authentication, and derollment for biometric authentication systems (cf. 4).

[1]The term biometric authentication is used in the international literature for different aspects of biometrics and authentication. A popular definition can be derived directly from the term biometric verification in distinction to biometric identification. From the process point of view it is necessary to have a more differentiated definition which means to have the above general biometric authentication process in the broader sense and the concrete algorithm for biometric verification/identification in the narrower sense [1].

[2]In the case of access to IT system resources the access management system can be based on a role based access control (RBAC) concept and the more technical concepts of mandatory access control (MAC) and discretionary access control (DAC) [2, 1].

3. BIOMETRIC SIGNATURES

For examining the meaning of identifying and characterizing signatures for biometrics applied in IT security, selected signatures from the fields of astrobiology, (type-)algebra, and (applied) cryptography will be briefly described followed by a generalized conclusion and definitions of biometric signatures and biometric templates (biometric signature clusters/classes). Three types of signatures will be considered: *biological signatures*, *algebraic signatures*, and *digital/electronic signatures*.

Biological signatures (biosignatures) in astrobiology can e.g. contain feature information based on spectroscopic analyses of electromagnetic signals or analyses of (rock | sediment) samples from (extra)terrestrial sites[3]. Within this paper a *biomarker* in close relation to a biosignature will be understood in two ways: Firstly, as a naturally given attribute and therefore as synonym to biosignature or secondly, as a biological characteristic which has been artificially established (e.g. within the (non-)coding part of the DNA or as fluorescent attributes of cells). Biosignatures are used as recognition characteristics based on measurable characteristics of biological lifeforms.

In type-algebra *signatures* are used for formally specifying the interface of *abstract data types* [6]. The complete formal specification of an abstract data type consists of a signature and axioms. A signature is defined as $\Sigma = (S, \Omega)$ with the set of sorts S and the definition of symbols for functions Ω. Linear algebra delivers for example a so called *matrix signature* (p, q) for a diagonal matrix of an $n \times n$ symmetric matrix with p 1s and q -1s [3][4]. Signatures for both, abstract data types and matrix signatures are thus describing characteristics of data and mathematical structures.

Digital signatures from cryptography applied for IT security are defined by [5] as follows:

Definition: A *digital signature* is a construct that authenticates both the origin and contents of a message in a manner that is provable to a disinterested third party.

In the legal context of *electronic signatures* in Germany special types of digital signature are used for authentication purposes [7]: *electronic signatures*, *advanced electronic signatures*, and *qualified electronic signatures*. An electronic signature is defined in [7] as follows:

Definition: [An electronic signature] is data in electronic form, which is attached and/or logically operated to other data for authentication.

Often the term electronic signature is used as synonym for digital signature and generally the term *signature* can be used. With the given definitions it can be derived that digital

[3]For further information please refer to the *NASA Astrobiology Institute (NAI)* at http://nai.arc.nasa.gov/ and the NAI Lead Team *Jet Propulsion Laboratory 1* at http://www.ipl.nasa.gov/ with regard to the actual research on definition and detection of biosignatures.

[4]Example: Matrix $A = [1000; 0100; 00\text{-}10; 0001]$ has signature (3,1)

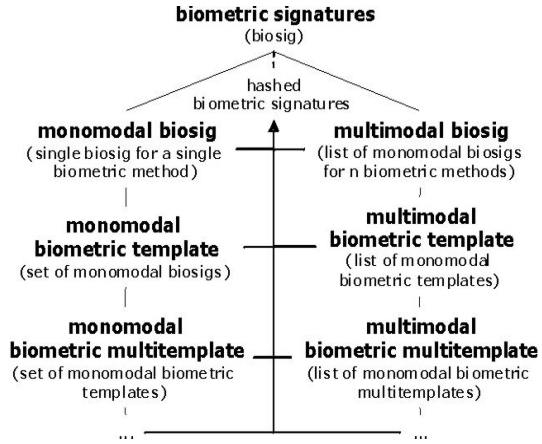

Fig. 1. Classification of Biometric Signatures

and electronic signatures include identifying information of subjects and objects in a digital or electronic form.

From the presentation of selected signatures above it can be generally concluded that a signature is a kind of - (bin|n-)ary codable - identifier for special characteristics of objects and subjects based on attributes of biological, data, and mathematical structures and secret authentication information for security processes and protocols. Biometric signatures and templates can be now defined as follows:

Definition: A *biometric signature* is a (bin|n-)ary coded representation of biometric characteristics for (distributed) computing systems.

Definition: A *biometric template* is a biometric signature (class|cluster) describing a set of biometric signatures.

For authentication purposes biometric signatures can be hashed which results in *hashed biometric signatures*[5].

4. BIOMETRIC SIGNATURES WITHIN BIOMETRIC PROCESSES

Based on the general authentication process (sect. 2.1) for biometric authentication systems three core processes can be identified: *biometric enrollment process*, *biometric authentication process*, and *biometric derollment process*.

Figure 2 shows a refined version of the biometric authentication process in [9] including enhancements concerning the clustering/classifying module (C) for the biometric enrollment and derollment processes.

A *sensing process* within an *(active) sensor system* is used, which delivers an appropriate *human-sensor-system-interface* for capturing or scanning a person's biological characteristics. The *capturing/scanning process* results in *biometric raw data and calibration data*, called *biometric char-*

[5]In this paper, biometric signatures *are not* understood as handwritten signatures, whose static and dynamic characteristics are captured and analyzed. This research field, which can easily be confused with biometric signatures, is known as *biometric handwriting recognition* and a subdiscipline can be identified as *biometric handwritten signature recognition*.

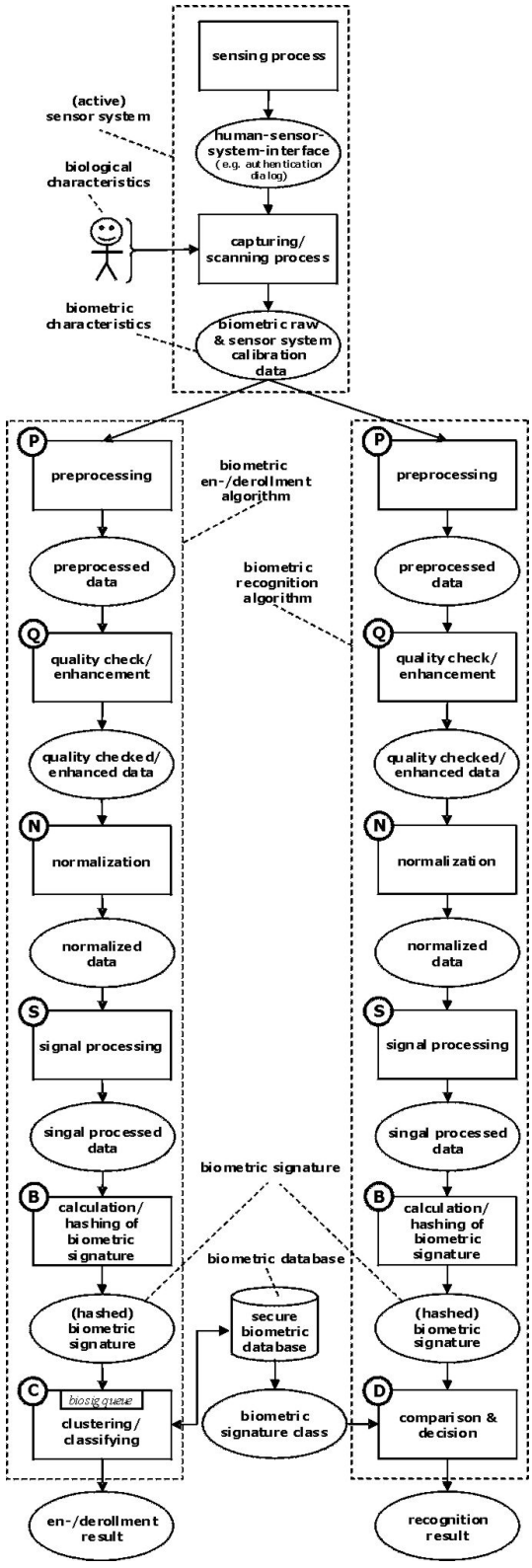

Fig. 2. Biometric Enrollment, Authentication, and Derollment Processes

acteristics, depending on the sensor system used for a specific biometric technique. After capturing the data is handed over to the biometric enrollment, recognition, or derollment algorithm. For authentication the authorized users are assumed to be already enrolled correctly, which means that calculated biometric templates have been stored in a secure biometric database.

The biometric algorithms are subdivided into modules:

P: *preprocessing*
Q: *quality check/enhancement & decision*
N: *normalization*
S: *signal processing*
B: *calculation/hashing of biometric signature*
D [authentication]: *comparison & decision*
C [en-/derollment]: *clustering/classifying*

The module P passes the preprocessed data to the module Q for quality check and appropriate enhancement, followed by the module N for normalization. If the quality meets the defined requirements, N hands over the normalized data to the main processing module S. Subsequently S begins processing the data depending on the core part of a biometric algorithm and hands over the signal processed data to the module B. Next B calculates the (hashed) **biometric signature**. If the biometric signature is hashed[6], the original raw data should not be reproducible from the hash values.

For en-/derollment the module C clusters the space of **biometric signatures** new depending on the added or removed biometric signature (clusters|classes). The secure biometric database will be read and updated for this purpose. It is to be kept in mind that the recognition performance can be influenced after this step has been done.

In module D the **biometric signature** is mapped to the biometric signature classes by a verification (1:1) or identification (1:c) comparison on a secure biometric database. From this comparison a decision will be generated which yields a *match* or *non-match*.

5. A CLASSIFICATION OF BIOMETRIC SIGNATURES

For increasing the reliability of authentication methods and systems, multimodal biometric authentication and the combination of biometrics with knowledge, possession, place, and time is under research and scientific discussion.

The presented usage of biometric signatures within the biometric enrollment, authentication, and derollment processes shows mainly two classes of biometric signatures in use for monomodal biometric processes: *monomodal biometric signatures* for single biometric signatures and *monomodal biometric templates* representing sets/classes of single biometric signatures.

[6]The implemented calculation of *biometric hashes* for a PDA derived from the statistical features of signals from online handwritten signatures is given with [8]. Hashing algorithms applied to biometric signatures/templates for authentication processes are addressed in [2].

Taking multimodality into account figure 1 shows the outcome for two more classes of biometric signatures: *multimodal biometric signatures* as lists of monomodal biometric signatures for more than one biometric method used and *multimodal biometric templates* for lists of monomodal biometric templates.

On the superset level with regard to (mono|multi)modal biometric processes for changing environmental conditions or changing biological characteristics (e.g. aging), other high level classes will arise (fig.1): *monomodal biometric multitemplates* for sets of monomodal biometric templates and *multimodal biometric multitemplates* for lists of monomodal biometric multitemplates.

6. CONCLUSIONS

Based on the presented *general authentication process* for biometric IT systems with regard to the introduced processes of *biometric enrollment, authentication, and derollment* it could be shown that the discussed and presented definition for *biometric signatures* enables a classification of biometric signatures of various complexity for monomodal and multimodal biometric IT systems from the classes of biometric authentication, detection, and reaction systems.

7. REFERENCES

[1] Brömme, A.: A Classification of Biometric Applications Wanted by Politics - Passports, Person Tracking, and Fight Against Terror, IFIP World Computer Congress (WCC) 2002, Montréal, QC, Canada, 2002

[2] Brömme, A.: A Discussion on Privacy Needs and (Mis)Use of Biometric IT-Systems, IFIP WG 9.6/11.7 SCITS-II, Bratislava, Slovakia, 2001

[3] Weisstein, E.W.: CRC Concise Encyclopedia of Mathematics, Chapman & Hall, London, UK, 1999

[4] James, R.C. and James, G.: Mathematics Dictionary, 5th edition, Chapman & Hall, New York, USA, 1992

[5] Bishop, M.: Computer Security - Art and Science, Addison-Wesley International, Boston, USA, 2003

[6] Liskov, B. and Zilles, S.: Programming with Abstract Data Types, ACM SIGPLAN Symposium on Very High Level Languages, Santa Monica, California, USA, 1974

[7] Bundesrepublik Deutschland, Gesetz über Rahmenbedingungen f. elektronische Signaturen [...], 16-05-2001, BGBl-2001-I-22; Verordnung zur elektronischen Signatur, 21-11-2001, BGBl-2001-I-59, Germany, 2001

[8] Vielhauer, C., Steinmetz, R. and Mayerhöfer, A.: Biometric Hash based on Statistical Features of Online Signatures, IEEE ICPR, Québec City, QC, Canada, 2002

[9] Brömme, A., Kronberg, M., Ellenbeck, O., and Kasch, O. : A Conceptual Framework for Testing Biometric Algorithms within Operating Systems' Authentication, ACM SAC 2002, Madrid, Spain, 2002