Verifier-Tuple as a Classifier for Biometric Handwriting Authentication - Combination of Syntax and Semantics

Andrea Oermann, Jana Dittmann, and Claus Vielhauer

Otto-von-Guericke-University of Magdeburg,
Universitaetsplatz 2, 39106 Magdeburg, Germany
{andrea.oermann, jana.dittmann, claus.vielhauer}@iti.cs.uni-magdeburg.de

Abstract. In this paper, a new concept for classifying handwriting data and its analysis for biometric user authentication is presented. The concept's characteristic is the combination of syntax and semantics. It implies a determination of four distinct levels of syntax and semantics to lower complexity and structure information. We demonstrate the concept's impacts on on-line handwritings and the user verification, and clarify the benefit of applying information of higher levels of semantics within the authentication methods. As a result we are able to evaluate techniques for biometric user authentication. Furthermore, we precisely outline and reason a more accurate biometric user authentication system, due to the classification given by the Verifier-Tuple concept.

Keywords: Biometrics, Security of Multimedia Content, Identification and Authentication.

1 Motivation

The Verifier-Tuple (VT) is a new concept for classifying information to determine its origin and authenticity as it was originally presented for audio in [1]. It enables a scalable evaluation of techniques for biometric user authentication. The idea of the VT is originated in the field of forensics where the identification, localization and verification of an author of information are focus of recent research. Since there is a great degree of overlap in the goals on the methods between forensics and biometric user authentication, an application of VT appears adequate.

The goal of biometric user authentication is the automated verification of a living human beings identity. Biometric user authentication is becoming increasingly relevant for academic and industrial research. Biometrics will soon be generally implemented in different areas and applications from ID cards to security to applications of insurance companies. Therefore, biometrics improve the level of security in infrastructures and applications.

Two classes of biometric modalities exist. The first class includes behavioral-based modalities such as speech and handwriting. The second class includes physiological modalities such as fingerprint, face, iris, retina, or hand geometry.

J. Dittmann, S. Katzenbeisser, and A. Uhl (Eds.): CMS 2005, LNCS 3677, pp. 170–179, 2005.

We confine our study to the first class as we base our work on previous evaluations for another behavioral modality, speech authentication, in [1]. In this paper, handwriting is the focus. Because of its individual uniqueness and its usage as a deliberate declaration of consent, especially for signing contracts and agreements, handwriting is generally accepted and preferred as a method for biometric user authentication.

The major benefit of the VT is its ability to structure information into detail and combine different levels of information. Three distinct goals can be outlined when connecting levels of syntax and semantics. The first goal is obtaining more accurate results for biometric user authentication by incorporating information of a higher semantic level in the authentication process. The second goal is reducing complexity by restructuring information, and the third goal is using the tuple's function as a design criterion for future handwriting based biometric applications.

The paper is structured as follows: In section 2, the concept of the VT is introduced implying four levels of syntax and semantics. Section 3 gives a brief overview of sampling and data representation for handwriting biometrics from a signal processing perspective. This is followed by the tuple's application to handwriting including a detailed classification of the handwriting information in section 4. Furthermore, results of combinations of syntax and semantics levels are outlined. Results based on experimental evaluations will underline the correctness of the VT and provide the tuple's conceptual proof in section 5. Finally, section 6 concludes by summarizing the paper and providing a perspective on future work.

2 Concept of the Verifier-Tuple

As introduced in [1], we define the Verifier-Tuple (VT) as a concept for classifying information. Based on this, we are able to structurally analyze information by detail, classify features of interest, and evaluate existing techniques. The following descriptions and specifications are also presented in [1].

The idea of our VT is derived from the general concept of the explanation of programming languages [2]. The VT consists of four parts as it is shown in the formula below: the syntax, the executive semantics, the functional semantics and the interpretative semantics. Each part can be seen as a level of information which has to be analyzed to retrieve the whole context.

$$VT = \{SY, SE_E, SE_F, SE_I\} \tag{1}$$

SY = syntax
SE_E = executive semantics
SE_F = functional semantics
SE_I = interpretative semantics

The syntax is defined as the composition of certain signs within a selected alphabet. It is a systematic, orderly arrangement and it is rooted in linguistics.

In order to analyze the syntax of languages, formal logic is applied as presented in [3] and [4]. The syntax describes the processing of the elements of an alphabet by following certain rules, structures and regulations. The syntax functions to define valid and permitted constructs within an alphabet.

Semantics is the study or science of meaning in language. Semantics implies the connection of characters, tokens or symbols and their relation to the meant object or information [5]. Semantics is associated with the interpretation of the facts given by the syntax. Thus, semantics enables to draw conclusions about the author of information and his or her intention. The interpretative characteristic of semantics is differentiated in three successive levels, the executive semantics, the functional semantics and the interpretative semantics.

The executive semantics can be defined as an application of a particular operation which determines a particular process sequence. Based on a certain input the operation effectively generates an output [2]. This level of semantics extracts connected, abstract syntactic elements as an output. The functional semantics includes a semantic algebra and evaluation functions as a further interpretative enhancement [2]. The functional semantics analyzes the impact of allocations of variables. Deriving from the syntax and the executive semantics, applied functions within the functional semantics specify measurement categories for analyzing the meaning of the information presented by the medium. The interpretative semantics is mostly provided by a human being but can also be integrated in a digital, automatic system. It is based on background knowledge and can be abstractly explained through methods of formal logic as presented in [2].

This concept of the VT enables a more detailed analysis and classification of information. With this structured division of information, it is not only possible to extract particular features, but also manipulations or attacks can be recognized and localized. Further, it allows drawing conclusions about the context which is not directly presented within the analyzed information such as certain metadata as we refer to later in this paper. A specified application of the VT for handwriting is demonstrated in section 4.

3 Sampling and Data Representation for Handwriting

The characteristics of the generation of a particular handwriting can be specified by the movement of the pen tip during the writing process. The main dimensions of this movement are pen position (horizontal/vertical), pen tip pressure and pen angle. Digitizer tablets provide sensor technology for the analog-digital conversion of these kinds of dynamics. PDAs or Tablet PCs as types of computers provide position information, represented as sequences of pen position points at discrete and continuous time intervals.

This representation of continuous information is also denoted as sampled signals, and for the case of position signal, we use the notation $x(t)$ for horizontal pen position signals and $y(t)$ for vertical pen position signals. The pen tip pressure signal can be either a binary pen-up/pen-down signal or describe pressure resolutions at a higher quantization level (typically up to 1024 levels) which is

denoted as $p(t)$. Finally, some current commercial digitizer tablets provide pen azimuth signals, denoted as $\Theta(t)$, the orientation of the vertical projection of the pen onto the writing surface, similar to a compass, as well as pen altitude signals $\Phi(t)$, describing the angle of the pen above the writing surface.

The goal of biometric user authentication using handwriting is the determination of similarities based on features derived from these sampled signals. For this purpose, different algorithms are applied [15] to bind the biometric data to an identity in order to authenticate a certain user.

4 Verifier-Tuple for Handwriting

The architecture of a biometric user authentication system is generally structured as follows: Initially, reference data is sampled during enrollment and stored in a database. Later, handwriting signals are sampled and analyzed for subsequent authentications. Authentication algorithms require certain parameters and reference data from the reference storage. In [7], [8], and [9], an overview of the variety of these authentication algorithms is provided. Well known algorithms are for example Dynamic time Warping (DTW), Hidden-Markov-Models (HMM), Neural Networks, Multi Level Approaches, or statistical approaches such as the Biometric Hash [10].

Two different goals of authentication can be outlined. The first goal is the verification of one particular known user of the reference storage. This implies a comparison of n signal samplings to *1* particular reference storage sampling ($1:1$ comparison). The second goal is the identification of a particular not known user which implicates a comparison of *1* signal samplings to n particular reference storage sampling ($1:n$ comparison). Depending on the desired authentication mode, the system parameters may change.

The application of the VT to handwriting biometrics results in the feature classification as demonstrated in the listing below. Features are differentiated and assigned to a particular level of the VT. Level 1 marks the syntactical properties of handwriting, level 2 the executive semantics, level 3 the functional semantics, and level 4 the interpretative semantics. Level 1 includes the original signal features, as provided from the sampling process. Level 2 classifies features derived from the original signals by applying feature extraction algorithms which lead to various abstraction levels. For this purpose, the biometric algorithm requires input from level 1 in any case but may additionally consider parameters from level 3 or 4. Level 3 presents the textual or visual presentation of information. In the particular case of handwriting, level 3 describes the content of the written sequence and its individual shape. Level 4 abstracts information about the context and background knowledge of the writing process. This may include for example environmental information, such as time and location of the sampling, as well as information about the hardware involved.

Table 1 summarizes the application of the VT concept to different levels of features found in handwriting biometrics:

Table 1. Classification of Handwriting features

Level 1: Syntax	Dynamic features which are:
Additional:	o Horizontal pen position signal $x(t)$ o Vertical pen position signal $y(t)$ o Pen tip pressure signal $p(t)$ o Pen azimuth signal $\Theta(t)$ o Pen altitude signal $\Phi(t)$ o Horizontal pen acceleration signal $a_x(t)$ (via horizontal pen force) o Vertical pen acceleration signal $a_y(t)$ (via vertical pen force)
Level 2: Executive semantics	Features resulting from different classes of algorithms for verifying handwriting such as:
In Particular:	o Dynamic Time Warping (DTW) o Hidden-Markov-Models (HMM) o Neural Networks o Multi Level Approaches o BioHash with distance measures for extracting certain statistical parameters o Set of k statistical parameters derived from the syntax
Level 3: Functional semantics	Textual and visual information (what is written)
	o Word + its individual shape o Passphrase + its individual shape o Symbol + its individual shape o Number + its individual shape o Signature + its individual shape
Level 4: Interpretational semantics	Information about the context and background knowledge
	o Tablet o Pen o Device o Environment o Emotions o Metadata [11], [12] or Soft Biometrics [13], [14] o Acceptance

This new classification of handwritings for biometric user authentication is restructuring the authentication parameters. Parameters are now further differentiated according to the levels of syntax and semantics. The major benefit of this concept is the precise analysis of information. Certain defined classes pool information features. Thus, information can hardly get lost without being recog-

nized. Compared to other approaches of feature classification, that punctually and arbitrarily pick a particular feature to extract, our approach can structurally analyze more than one feature at the same time. Hence, with this structure the complexity of information and its analysis for user authentication can be reduced. Furthermore, the accuracy of techniques for verifying handwritings can be evaluated. The VT implies the assumption that, the more information can be applied to the technique, the better and more reliable results can be achieved for authentication.

The different levels and their relation to each other will now been explained into more detail. Level 1, the class of syntax, has already been elaborated in section 3. Especially level 2, the class of executive semantics is focus of current research investigations. Figure 1 demonstrates an example for the generation of information of level 2 by applying the biometric hash algorithm to information of level 1. Signals are used as the input as it can be seen on the left side.

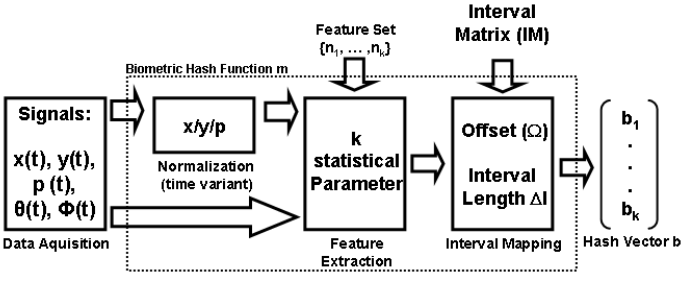

Fig. 1. Example for Level 1 and 2: Syntax and executive semantics [6], statistical representation.

Based on these signals, k statistical parameters are extracted such as the total writing time in ms, the total number of event pixels, the total absolute path length in pixels, or the total number of sample values. A complete description of the currently supported set of statistical parameters is provided in [6]. By applying an interval mapping function which implies the process parameter Interval Matrix IM, the Biometric Hash Vector b is generated which includes particular features. For authentication, this Biometric Hash Vector b will be compared with stored vectors of the database. Certain distance measures decide whether a user will be verified or not. These distance measures also belong to the class of level 2, the executive Semantics.

The class of level 3, the functional semantics is illustrated in Figure 2. This level 3 includes the classification of varying textual contexts used by the writers such as signatures, pin codes, passphrases, symbols, or numbers. Certain information such as "Sauerstoffgefäß" [oxygen container], as exemplified in Figure 2, written by two different writers is semantically equal within this level 3 of the VT model, while it differs from each other in level 1 and subsequently level 2. The meaning of the information is the same even if the signal distribution

Fig. 2. Handwriting examples of the German word "Sauerstoffgefäß" from two different writers [6].

is varying. This observation is a justification of our model with respect to the possibility to discriminate different writers, even if they write identical text.

Beside others, the interpretative semantics in level 4 classifies tablet categories or the interpretation of certain metadata [12] or soft biometrics [13], [14] such as cultural aspects [11] for the usage and acceptance of handwriting for biometric user authentication. The inclusion of this level 4 of information in biometric user authentication systems is a major subject of ongoing research.

There are two kinds of impact the interpretative semantics in level 4 can have for an analysis of information. One impact can be outlined as follows: Based on the three preceding levels, one is able to derive assumptions about not particularly in the original handwriting sample included information within level 4 of the VT model such as soft biometrics. The other impact is determined through the additional consideration of information within in the interpretative semantics of level 4 as parameter input to processed operations in lower levels such as the authentication algorithms. Tests in section 5 will provide conceptual proof that, by this means of level 4 features, a more accurate result for biometric user authentication can be achieved.

These examples lead to the assumption that the more parameters can be applied to the analysis of handwriting information, the more accurate and reliable results can be achieved for biometric user authentication. Better recognition results can be achieved with the combination of signal analysis and metadata or soft biometrics, respectively the combination of syntax and semantics.

5 Tests for Evaluating the Verifier-Tuple

For evaluating the Verifier-Tuple we refer to some test results presented in [6]. Our goal is the exemplary demonstration of the tuple's benefits as a new classification of information and hence, showing the advantages of the combination of different classified levels of syntax and semantics.

The tests include algorithms for handwriting as a biometric user authentication. Evaluations of those algorithms are based on the Equal Error Rate (ERR), the point where False Match Rate (FMR) and False Non-Match Rate (FNMR) are identical [6], [15]. FNMR is the percentage probability of rejections by a biometric system of authentic user while FMR is the percentage probability of rejections of non-authentic user. Thus, ERR is one decision measure value at a specific operating point of a biometric system and implies the probability of great similarities as presented in Table 2 and 3.

Table 2. EER for different tablet categories, textual content Signature (n/a = not available) [6], MQED

	Equal Error Rate (EER)			
Tablet Category	EER_{Random}	EER_{Blind}	$EER_{LowForce}$	$EER_{BruteForce}$
StepOver+PRESS	0.1	0.26	n/a	0.34
Cintiq15	0,12	0,2	0,34	0,38
All	0,18	0,3	0,4	0,42
Midres-PQ	0.15	0.25	0.4	0.42

Table 3. EER for different tablet categories, textual content Signature (n/a = not available) [6], BioHash

	Equal Error Rate (EER)			
Tablet Category	Random	Blind	Low-Force	Brute-Force
All	15 %	14 %	11 %	18 %
Cintiq15	5 %	12 %	10 %	13%
Midres PQ	22 %	34 %	33 %	33 %
StepOver+PRESS	5 %	29 %	n/a	16 %

For our evaluation, we refer to those handwritings from the database, presented in [6] that have been collected with three classes of digitizer tablets: StepOver+PRESS, Cintiq15, Midres-PQ (collection of different tablets with a medium spatial resolution) and the joint set of all tablets, denoted as "All". Further, the MQED algorithm is applied for authentication in Table 2 and the BioHash algorithm in Table 3. For evaluating the VT, our focus is on the EER_{Random}, shown in the second column from right of both tables. Table 2 and Table 3 both represent Equal Error Rates for different tablet categories and the textual content *Signature*, but results shown in Table 3 are more accurate than in Table 2. In comparison to Table 2, the BioHash algorithm, whose test results are presented in Table 3, applies additional information of level 2, the executive semantics, since it abstracts to statistical features. Information of level 4, the interpretative semantics, is reflected by the four table rows, where each row represents a different scenario with respect to the hardware used for sampling of the handwriting signals. In particular, the algorithms consider knowledge about the used tablet in all cases except row "All". We observe that for both algorithms, the recognition accuracy improves, if the specific type of tablet is known to the authentication systems, i.e StepOver+PRESS and Cintiq15 have lower error rates than Midres-PQ and All. That is, knowing the type of digitizer (interpretative semantics level 4 in the VT model) can improve accuracy as compared to conditions, where there is uncertainty about the hardware.

We interpret this demonstration as a first proof of the concept of the VT as a classifier for biometric handwriting authentication. The approach of [6] has shown that considering more knowledge of semantics for analyzing handwritings more accurate and reliable results for user authentication can be achieved.

6 Conclusion and Future Work

This paper has shown the usability of the concept of the Verifier-Tuple as a new classifier for biometric handwriting authentication and the following aspects can be summarized:

The VT is a new concept to classify biometric information in a structured manner. Its major benefit is the ability to pool information together into one level of syntax and three levels of semantics. The concept enables an efficient combination of information of these levels in biometric applications. By applying our developed concept more accurate and reliable results for biometric user authentication can be achieved.

While in the test scenario discussed in this paper, information of a higher semantic level, such as the type of digitizer tablet was known a-prior, it might be of interest in future investigations to perform analysis of signals and classes of algorithms towards determination of such higher level of information. For example, to identify the type of sampling device used during recording of the biometric data. Furthermore, by applying and evaluating metadata and soft biometric features such as the cultural origin, ethnicity and education, hypotheses of the user acceptance of a biometric user authentication system can be possibly derived in future. Future work will also include the analysis of compression of data by its entropy in order to figure out how far the data can be compressed and still discriminative features of interest can be extracted to grant accurate and secure authentication systems.

Comprising our earlier work on the forensic background, we can conclude that Verifier-Tuples are not only adequate to analyze an on-line handwriting into detail but also we can give more reliable assumptions about user authentication in general. With this paper we have shown the Verifier-Tuple's characteristics as a scalable concept for different media.

Acknowledgements

The information in this document is provided as is, and no guarantee or warranty is given or implied that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability. The work described in this paper has been supported in part by the Federal Office for Information Security (BSI), Germany, in particular the development of the tuple, and partly by the EU-India project CultureTech, especially the hardware independency tests. The German Government is authorized to reproduce and distribute reprints for Governmental purposes notwithstanding any copyright notation there on. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the Federal Office for Information Security (BSI), or the German Government.

References

1. A. Oermann et al.: Verifyer-Tupel for Audio-Forensic to determine speaker environment, accepted at ACM Multimedia and Security (2005)
2. H.R. Nielson, F. Nielson: Semantics with Applications: A Formal Introduction, revised edition, John Wiley & Sons, original 1992 (1999)
3. N. Chomsky: Syntactic Structures, Mouton and Co., Den Haag (1957)
4. N. Chomsky: Aspects of the Theory of Syntax, MIT Press, Massachusetts Institute of Technology, Cambridge, MA (1965)
5. S. Löbner: Semantik: eine Einführung, De Gruyter Studienbuch Berlin (2003)
6. C. Vielhauer: Biometric User Authentication For IT Security: From Fundamentals to Handwriting, Springer, New York, U.S.A., to appear 2006 (2006)
7. R. Plamandon, G. Lorette: Automatic Signature Verification and Writer Identification - the State of the Art, Pergamon Press plc., Pattern Recognition, 22, Vol. 2 (1989) 107 - 131
8. F. Leclerc, R. Plamondon: Automatic Verifictaion and Writer Identification: The State of the Art 1989-1993, International Journal of Pattern Recognition and Artificial Intelligence, Vol. 8 (1994) 643 - 660
9. J. Gupta, A. McCabe: A Review of Dynamic Handwritten Signature Verification, Technical report at James Cook University, Australia (1997)
10. C. Vielhauer, R. Steinmetz, A. Mayerhöfer, Biometric Hash based on Statistical Features of Online Signatures, In: Proceedings of the IEEE International Conference on Pattern Recognition (ICPR), Canada, Vol. 1 (2002) 123 - 126
11. S. Schimke, C. Vielhauer, P.K. Dutta, T.K. Basu, A. De Rosa, J. Hansen, B. Yegnanarayana, J. Dittmann: Cross Cultural Aspects of Biometrics, in Proceedings of Biometrics: Challenges arising from Theory to Practice (2004) 27-30
12. C. Vielhauer, T. Basu, J. Dittmann, P.K. Dutta: Finding Meta Data in Speech and Handwriting Biometrics, to appear in: Proceedings of SPIE (2005)
13. A. K. Jain, S. C. Dass and K. Nandakumar: Soft Biometric Traits for Personal Recognition Systems, in Proceedings of International Conference on Biometric Authentication (ICBA), LNCS 3072, Hong Kong, July (2004) 731-738
14. A. K. Jain, S. C. Dass and K. Nandakumar: Can soft biometric traits assist user recognition?, in Proceedings of SPIE Vol. 5404, Biometric Technology for Human Identification, Orlando, FL, April (2004) 561-572
15. C. Vielhauer, T. Scheidat: Fusion von biometrischen Verfahren zur Benutzerauthentifikation, In: P. Horster (Ed.), D-A-CH Security 2005 - Bestandsaufnahme, Konzepte, Anwendungen, Perspektiven (2005) 82 - 97