22

Access control system using dynamic handwriting features

Christiane Schmidt
Aachen University of Technology
Institute of Technical Computer Science, Ahornstr.55, 52074 Aachen, Germany, telephone:+49 241 803635 fax:+49 241 8888308
e-mail: schmidt@techinfo.rwth-aachen.de

Abstract

The increasing number of protected areas requires reliable methods of access control. Traditionally, computer systems rely on passwords for access security. To avoid unauthorized access, an access control might use biometric features such as fingerprints, irispatterns, voiceprints or signature. This paper presents a system for verifying a personal's identity by comparing signatures. Signatures are intrinsically more secure than passwords. Their invisible dynamics cannot simply be guessed. A pressure sensitive graphics tablet as the input device records the pen motion during signature and sends signals to a computer. From this data, characteristic parameters like horizontal and vertical trace, velocity and acceleration are determined. Depending on the variation of these values in comparison to reference datasets, the system classifies the signature to be an original or a forgery. A database has been constructed with 400 dynamic signatures to validate chosen features and procedures.

Keywords

access control, dynamic handwriting features, pen based input, signature, signature verification

1 INTRODUCTION

Access control tasks are well known and common practice in modern security applications. All systems use the same basic scheme in order to provide a selective mechanism which separates illegal from legal users. Such systems consist, as a rule, of two major com-

P. Horster (ed.), *Communications and Multimedia Security II*

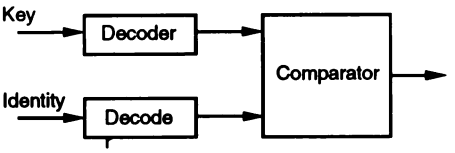

Figure 1 Principle of access control tasks.

ponents (Figure 1): The key component contains all information about the individual's identity. In today's security applications this component is often realized by using chip or magnetic cards. It is less often a physical key with mechanical attributes. The identity is a supplementary component like a password or identity number. Both components are coded and the verification is reduced to a simple comparison of the decoded components. The system only works if the information of the key and the identity exactly match. If the supplied information is not evident no access will be allowed at all (Horster, 1993).

The user has to subdue an installed access control system in two different ways: He has to take the key card and to remember the password. This may lead to certain problems in everyday life (Beutelspacher, 1993).

Nowadays, every person has a lot of identity cards with passwords and identity numbers. Some of these cards are used for normal services like starting a car, opening a door to a security area. Other, more abstract security mechanisms dealing, with bank accounts, e-mail and e-banking services, access to libraries, and interactions in world wide nets, get more fashionable day by day. This trend of society's evolution leads to an increasing number of security mechanisms. The user has to know exactly how to enter every service including passwords, identity cards, and other details.

A disadvantage of traditional access control systems may be, that persons with lots of passwords tend to note passwords on a piece of paper. If such note falls in the wrong hands, people have the possibility to illegally force an entry into the system.

However, there are other possible strategies which can replace nowadays access control interfaces by implementations and which work more intuitively. In order to create such systems, it is required to eliminate the abstract realization of the identity component and, if possible, to eliminate the key component by a direct measurement on the subject. This leads to access control systems that do not work with second hand materials like passwords or identity cards. Instead, these systems test the subject's personality itself (Jennings, 1992; Leggett, 1991; Sherman, 1992).

This can be realized by signal measurements from physiological and psychological processes which leads to biometric data acquisition (Guinier, 1990). Well-known biometric

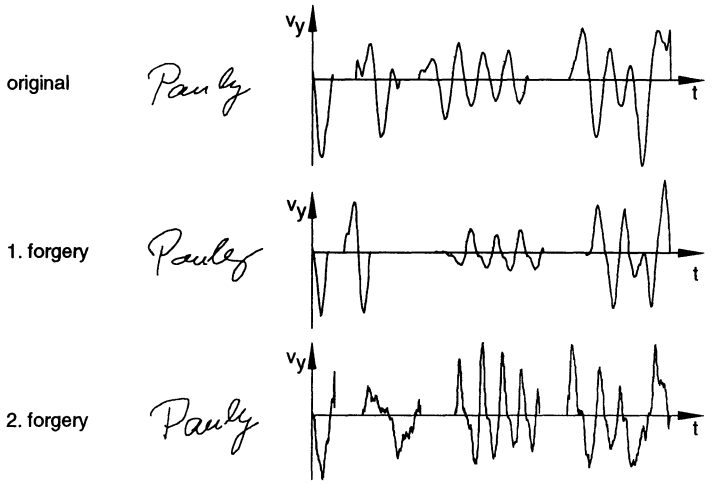

Figure 2 Illustrations on signatures as image and signal state. The first forger tried to imitate the dynamics and the second the picture of handwriting. The velocity diagrams are normalized to 150 sampling points.

data are fingerprints. Furthermore, irispattern, voiceprint, faces, and handwriting could be used as basis of an access control system. This biometric approach may lead to automatic identification and to simple verification systems that can be intuitively handled by the service user, and which provides full access control (Daugman, 1995; Hrechak, 1990; Konen, 1995; Matsuura, 1990; Plamondon, 1989; Schmidt, 1995).

In this paper we present an experimental access control system based on the dynamic features of handwriting. A specimen of a persons's handwriting is the signature. It is the common identification criterion and has the most undisputed importance in jurisdiction.

Every person develops a typical characteristic of his handwriting because the signature is often needed in life. Therefore, it is extremely difficult to copy. The dynamics of writing are very important for access control systems. Information about the sequence of the writing movement is taken into account (see Figure 2).

An access control system based on dynamics of signature gives the advantage that non-visible features in the script can be used. Forgers have only a chance to forge successfully, if they can precisely observe the writing movement.

In the next section, we discuss some aspects of handwriting and signature, and present

the data processing mechanism. Section 3 describes the concept of using handwriting as an access control system source. Section 4 illustrates experimental results and section 5 finally draws the conclusions of the presented work.

2 HANDWRITING AND SIGNATURES

Handwriting and signatures are biometrical features. They contain information about the writer as a subject emerged from information about his physiology and psychology, resulting for the writers arm and hand effectors and his personal mental model of handwriting. The analysis of static handwriting images is often used in forensic psychology. Especially the signature is a well practiced and confident security mechanism in everyday life.

Every writing process shows typical individual properties. A handwritten word seems to be constructed from a sequence of individual and rather invariant strokes, which can also be found in other words written by the same person (Teulings, 1993). These strokes are not exactly reproduced in any words written by another person. A model explaining this uses a motor program memory located somewhere between the central nervous system and the effectors of the writer's hand. The model describes the writing process as a controlled sequence of automatic pen movements, which corresponds to the experimental data acquired in psychological research. The parameters of this pen movements are fixed and looked up in motor program memory. This memory recall uses contextual information from proprioceptive and visual perception (Parizeau, 1989; Schomaker, 1990).

Every signature represents a handwritten text with special characteristics. A signature contains special stroke sequences which are not used in ordinary handwriting. These strokes are evolved from ordinary script to an individual style with strong geometric characteristics. The psychological result of handwriting as a grafical task, reasoned by small variances of spatial features, has a strong continuity to signatures. The overdone shapes of signatures letters are first of all grafical symbols with less similarity to ordinary handwriting. These shapes are evolved from routine and training, and the conscious and unconscious influence of the rule to create a unique and individual signature.

Because of training, normally a person needs little time to write its signature, whereas a forger usually needs more time. Although handwriting is usually rescalable in time and no fixed timing base in motor program memory's temporal information seem to exist, it can be used for verification. Direct time information like absolute value of writing duration at position (x,y) does not seem to be a good verification base. However, if we overlook the overall timing and force our consciousness to dynamic details of the process, we get useful information which is not easy to forge. This leads to a multivariate dynamic approach that contains temporal information as well as spatial information, which are todays favorites in handwriting image processing systems (Brost, 1994; Plamondon, 1992; Rieger, 1988).

Table 1 Dynamic global features of the signatures of Figure 2: Basis is the original

feature	*original*	*1. forger*	*2. forger*
total writing time	1.00	1.23	3.00
ratio total and actual writing time	1.00	1.15	1.02
pressure average	1.00	1.15	1.21
pressure variance	1.00	1.52	0.85
pressure changing	1.00	1.42	0.33
velocity absolute value	1.00	1.61	0.15
velocity x-direction	1.00	1.42	0.40
velocity y-direction	1.00	1.35	0.19
acceleration x-direction	1.00	1.51	0.03
acceleration y-direction	1.00	1.18	0.06

This dynamic representation contains information invisible in the static image of the handwriting. Figure 2 shows one genuine signature and two forgeries together with their produced velocity signal. Table 1 illustrates the relation between the original writer and the two forgers of Figure 2. The values of the features from the original writer represent the basis.

The spatial representation is a subset of the pure spatial processing, which can be reconstructed by elimination of the time parameter t. This approach seems to be more secure than pure image processing tasks, because a forger has to realize timing details not visible in the signature's image. The motor program theory leads to another kind of view because it defines the script as a sequence of strokes, transferred in time, and spatial domain. Thus we can work with the assumption, that there are differences in stroke timing between different persons caused by the habits and learning history of the writers (Parizeau, 1989).

3 ACCESS CONTROL SYSTEM

An access control simulation based on signatures has been developed to re-check the entry. The access control system consists of data acquisition, signal preprocessing, feature extraction, comparison and a decision process. If a person wants to get the legitimacy to enter the safety area, the system must generate reference data of this person. The person gives only his identity, the real name or a pseudonym, to the computer and writes his signature on the digitizing tablet (Figure 3).

Every writing produces a vector

$$s(t) = (x, y, p)(t) \tag{1}$$

of discrete time signals. In order to record these data, a pen with a special resonance circuit is positioned over a graphic tablet. The location (x,y) in the discrete coordinates of the graphic tablet and the pen pressure p transferred by the pen pit are acquired every 5 ms. The pressure is calculated from the resonance of the resonance circuit.

The system turns the received signature to be in the horizontal during signal preprocessing and computes temporal functions $f_k(t)$. The component k stands for horizontal and vertical deflection, writing pressure, changing writing pressure, velocity (absolute value, x-direction, y-direction), acceleration (absolute value, x-direction, y-direction) and course of direction vector.

A low pass filter eliminates noise in the components. The system is normalized to the sampling points of the temporal functions for a better comparison of the signature. The comparison of various signatures, based on the computation of cross correlation functions of the horizontal trace, shows a great similarity independent of whether it is an original

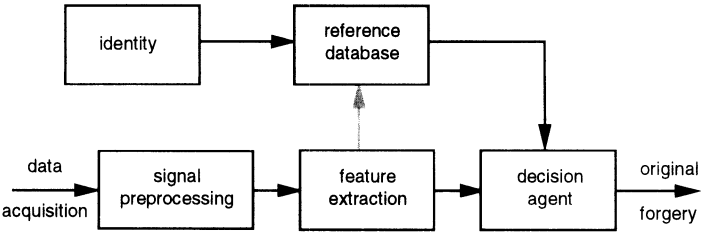

Figure 3 Overview of the access control system.

or a forged signature. The elimination of the linear part emphasizes the characteristic of the dynamic course (Figure 4).

The temporal function of the actual signature will be compared to the relevant reference data during the signal comparison. During the decision, the distance D_k between each temporal function of the actual signature and the reference data are compared to a threshold value S_k. If the distance D_k is less than the threshold value S_k, the signature will be classified as original, otherwise it is treated as a forgery. The overall decision of the system is based on the isolated decision of each temporal function.

To get the legitimacy of entry for the first time, the user has to write several signatures on the digitizer. These signatures are needed to calculate the reference data for the user. The access control system calculates three reference signatures of each user (Hrechak, 1994). At the moment, the system works with 10 signatures of each user to compute the reference vector. This is a compromise between the available signatures in the database and the probability of 95% that the specimen of one's handwriting is included in the three shapes of individual handwriting.

The reference signature is represented by various normalized functions of time. Each temporal function is determined separately, and each individual component forms a correlation matrix. Figure 5 shows an example of such a correlation matrix of one specific component k of 10 signatures of one person.

The values in the correlation matrix of Figure 5 describe the degree of similarity between two signatures regarding component k, measured by the maximum value of the cross correlation function. They are calculated for each combination of signatures. For the computation of the reference data, the system selects a reference signature out of the 10 signatures in the matrix, which has the highest correlation value greater than a threshold value L in a row or in a column (e.g. $L = 0.9$).

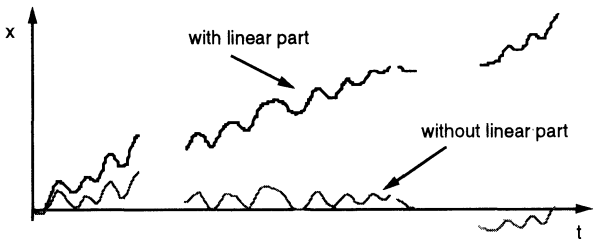

Figure 4 Horizontal trace of a signature with and without linear part.

signature no. :	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*
1	1	0.8	0.87	0.84	0.89	0.87	0.85	0.87	0.81	0.93
2	0.80	1	0.9	0.86	0.73	**0.90**	0.88	0.85	0.58	0.8
3	0.87	0.90	1	0.89	.87	**0.92**	.88	0.89	0.68	0.92
4	0.84	0.86	0.89	1	0.75	0.84	0.91	0.86	0.61	0.81
5	0.89	0.73	0.87	0.75	1	0.82	0.76	0.81	0.81	0.93
6	0.87	0.9	0.92	0.84	0.82	1	0.91	0.95	0.72	0.88
7	0.85	0.88	0.88	0.91	0.76	**0.91**	1	0.92	0.6	0.82
8	0.87	0.85	0.89	0.86	0.81	**0.95**	0.92	1	0.72	0.89
9	0.81	0.58	0.68	0.61	0.81	0.72	0.60	0.72	1	0.83
10	0.93	0.8	0.92	0.81	0.93	0.88	0.82	0.89	0.83	1

Figure 5 Example of a correlation matrix of the feature component k for 10 signatures.

In the matrix of Figure 5, signature no. 6 owns the largest number of correlation values greater than 0.9. Signature no. 6 is very similar to the signatures no. 2, 3, 7, and 8. The signature no. 6 is therefore the reference signature of this component k. Signatures no. 2, 3, 6, 7, and 8 can be deleted in the correlation matrix. A new matrix with the remaining signatures is formed.

signature no. :	*1*	*4*	*5*	*9*	*10*
1	1	0.84	0.89	0.81	0.93
4	0.84	1	0.75	0.61	0.81
5	0.89	0.75	1	0.81	0.93
9	0.81	0.61	0.81	1	0.83
10	0.93	0.81	0.93	0.83	1

Figure 6 Reduced correlation matrix of Figure 5.

In this reduced matrix (Figure 6), signature no. 10 is similar to the largest number of signatures. Therefore, signature no. 10 is the second reference signature of the component k. This process is repeated until all signatures are deleted in the matrix and the number of reference signatures is three. The system will raise the threshold value by increment if the number of the reference signatures is less than the desired number. The process of the generation of reference data is then started again. If the number of reference signatures is greater than three the system reduces the threshold value. The process terminates when the number of reference signatures is equal to three (Yoshimura, 1993). The resulting ref-

erence vector of a user signature consists of three reference vectors. Every single reference vector represents all components. Each calculated reference vector uses 112 bytes.

4 CLASSIFICATION AND EXPERIMENTAL RESULTS

The classifier is based on a combination of various functions. The system computes cost values of global features and dynamic time warping of each component. The results are the basis for the general decision. Every partial classification is based on an individual combination of dynamic handwriting features.

The average of the current and reference data and the variance of the reference data define the cost function of the global features E_i. The cost function is computed for every component of the global features i. These are the ratio of total and real writing time, derivation of pressure, velocity, and acceleration of the signature. The value of the cost function is compared to a threshold, that depends on the selected feature i:

$$E_i = \frac{(actual_i - reference_{average_i})^2}{reference_{variance_i}} \tag{2}$$

The dynamic time warping defines a mapping function, which assigns equal events like maximum or minimum value to the same event. The distance D_k between the components is calculated by the sum of the absolute difference between related sampling points. Since every component has been three reference values computed, the system calculates three distance values D_{k_i} with $i = 1, 2, 3$. The decision function compares the minimum value of the three reference values $D_{k_{min}} = min(D_{k_i})$ with a threshold value S. This is the borderline between original and forgery. The parameters are the vertical and horizontal trace, the pressure, and the derivation of pressure, velocity, and acceleration.

The validation of the classification system was carried out using a handwriting database of 400 signatures from 20 persons. After a training on the special pen and the digitizing tablet, every person wrote 20 signatures on various days. The first five signatures were obtained at the first day, the next five signatures were written on the following five days. The last 10 signatures were collected within the next two to three weeks at different times (for instance in the morning, after lunch, in the evening, after discussion).

The system calculated the global reference data vector and the personal specific threshold from the first signatures of every person. With the signatures no. 11 to 20 the right acceptance rate (RAR) was computed, i.e. the probability of acceptance as original. With all individual components, the system achieves a RAR between 61.5% and 81.5% (Table 2). The overall classification of original with a combination of the components results at 90.5%.

Table 2 Recognition rate using dynamic time warping

feature	*RAR* (%)	*RRR* (%)
vertical trace	71	99.8
horizontal trace	80	85.8
pressure	71	98
velocity	65	98.5
velocity (v_x)	71	97
velocity (v_y)	61.5	100
acceleration	72	98
acceleration (a_x)	81.5	79
acceleration (a_y)	72	72.5
dynamic time warping	90.5	98.9

A second criterion of judgment is the detection of unauthorized persons (right rejection rate, RRR). For this judgment it is necessary to make forgeries with the input utilities. The result of the classification depends on the quality and the talent of the forgering person. "Professional" forgers were not available. So the usability of the presented method was tested by another evaluation. Twenty persons got the task to write the word "Grünschnabel" ten times. We evaluated whether the system was able to tell two persons apart or not. Only similar specimen handwriting were compared. The system classified the person B on the reference data of the person A. These reference data were computed by 10 "Grünschnabel" signatures with the same combination of components as the original classification system. The system recognized 98.9% as forgery. This result bases on 190 classified specimen handwritings.

5 SUMMARY

Computer aided holding of business transaction or automatic supervision of entrance to safety areas gain importance. To avoid the admittance of unauthorized person, the entitlement of this person for this area has to be checked. Traditionally, this is achieved by input of passwords or the use of chipcards.

In this paper a signature-based access control system has been presented. The society accepts signatures as identity information on almost every document. An access control mechanism based on signature verification might lead to good acceptance and high customer learning rates because it is already common practice in everyday life.

The main result of this study is that the basic authorization scheme depends on multivariate differences between individual handwritings. The presented experimental results gave evidence that the selected dynamic features of signature and the selected methods to calculate the reference data vector are suitable to test the identity of persons by biometric features.

The classification steps have been discussed. A scheme for computation of the reference signature has been presented that forms the basis for the recognition. The final classification task is carried out by a cost function system depending on dynamic time warping.

In order to increase the recognition rate and system performance, the database will be enlarged during the next time. Further work is needed on an optimal structure of the database, methods for generating forgeries and for the comparison between conventional recognition approaches and neural networks methods.

6 REFERENCES

Beutelspacher, A. (1993) *Kryptologie.* Vieweg Verlag, Braunschweig/Wiesbaden.

Brost, M. (1994) *Entwicklung eines Verfahrens zur Benutzerverifikation unter Berücksichtigung der Schreibdynamik.* Master's thesis, RWTH Aachen.

Daugman, J. (1995) Face recognition by feature demodulation, in *International Workshop on Automatic Face- and Gesture-Recognition* (ed. M. Bichsel). 350–355. Multi Media Laboratory, Department of Computer Science at the University of Zurich.

Guinier, D. (1990) Identification by biometrics: An introduction and a survey. *SIGSAC Review,* **8(2)**, 1–11.

Horster, P. (1993) Sicherheitsmechanismen. *Datenschutz und Datensicherung,* **9**, 511–520.

Hrechak, A.K. and McHugh, J.A. (1994) Automated fingerprint recognition using structural matching. *Pattern Recognition,* **23(8)**, 893–904.

Jennings, C. (1992) Biometrics: When the person is the key. *Sensor Review,* **12(3)**, 9–11.

Konen, W. and Schulze-Krüger, E. (1995) Zn-face: A system for access control using automated face recognition, in *International Workshop on Automatic Face- and Gesture-*

Recognition (ed. M. Bichsel). 18–23. Multi Media Laboratory, Department of Computer Science at the University of Zurich.
Leggett, J. and Williams, G. and Usnick, M. (1991) Dynamic identity verification via keystroke characteristics. *International Journal Man-Machine Studies*, **35(6)**, 859–870.
Matsuura, T. (1990) Handwriter identification based on acceleration of handwriting motion, in *Signal Processing V: Theories and Applications* (ed. L. Torres, E. Masgrau, and M. A. Lagunas). 1635–1638. Elsvier Science Publishers.
Parizeau, M. and Plamondon, R. (1989) What types of scripts can be used for personal identity verification?, in *Computer Recognition and Human Production of Handwriting* (ed. R. Plamondon, C. Y. Suen, and M. L. Simner). 77–90. World Scientific Publ. Co.
Plamondon, R. and Lorette, G. (1989) Automatic signature verification and writer identification - the state of the art. *Pattern Recognition*, **22(2)**,107–131.
Plamondon, R. and Yergeau, P. and J.J. Brault, J.J. (1992) A multi-level signature verification system. in *From Pixels to Features III: Frontiers on Handwriting Recognition* (ed. S. Impedovo and I. C. Simon). 363–370. Elsevier Society Publisher.
Rieger, R.B.(1988) *Analyse von Schreibsignalen*. PhD thesis, J.W. Goethe Universität Frankfurt/Main.
Schmidt, C. and Hünermann, R. (1995) Handwriter identification based on dynamic word independent features. in *7th Biennial Conference of the International Graphonomics Society* (ed. M.L. Simner). 140–141.
Schomaker, L.R.B. and Plamondon, R. (1990) The relation between pen force and pen point kinematics in handwriting. *Biological Cybernetics*, **63**, 277–289.
Sherman, R.L. (1992) Biometrics futures. *Computer and Security*, **11**, 128–133.
Teulings, H.-L. (1993) Invariant handwriting features useful in cursive-script recognition. in *From Pixels to Features III: Frontiers on Handwriting Recognition* (ed. S. Impedovo and I. C. Simon). 1–20. Elsevier Society Publisher.
Yoshimura, I. M. and Yoshimura M. (1993) On-line signature verification incorporating the direction of pen movement. in *From Pixels to Features III: Frontiers on Handwriting Recognition* (ed. S. Impedovo and I. C. Simon). 353–361. Elsevier Society Publisher.

7 BIOGRAPHY

CHRISTIANE SCHMIDT received her diploma in Electrical Engineering from the Technical University of Ilmenau in 1992. She is currently engaged with her Ph.D. project at the Institute of Technical Computer Science at Aachen Technical University. Her research is on biomterical access control systems.