Multifactor Biometric Sketch Authentication

Arslan Brömme and Stephan Al-Zubi

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

Abstract: In this paper we propose a multifactor biometric sketch authentication method based on biometric sketch recognition and a user's personal knowledge about the sketch's content, which is negotiated between the biometric authentication system and the user during enrollment. The used sketch recognition algorithm is based on the active shape structural model (ASSM) for analyzing the structural variability of sketches built up from a set of deformable shapes. For increasing the reliability of the biometric sketch authentication method the user's knowledge as authentication factor has been added by fulfilling specific sketching tasks of varying complexity given by the authentication system.

An evaluation and testing framework for biometric algorithms was used to prove the accuracy of the method. For this purpose the biometric sketch algorithm has been adapted to the framework, a compiled sample database for comparability testing between users has been generated, and attack classes ranging from none, over partial to complete knowledge about the user's sketch has been developed and used. The evaluation of the test results shows that particularly the user's knowledge as an added authentication factor leads the used sketch recognition algorithm to high accuracy.

1 Introduction

For increasing the reliability of authentication methods and systems, multimodal biometric authentication methods and combinations of (mono|multi)modal biometric algorithms with the additional authentication factors of knowledge, possession, time, and place is under scientific discussion and research.

In the actual rapid research of combining (single|multiple) biometric authentication methods with additional (single| multiple) authentication factors we are proposing a new *multifactor biometric sketch authentication method* which is using the biometrical characteristics of sketching in combination with the user's knowledge of a sketch's structural relations as an additional authentication factor for increasing the overall reliability of the proposed combined (multifactor) authentication method.

For enabling the evaluation and testing of (mono|multi)modal biometric algorithms within (single|multi)factor biometric authentication systems, the *biometric processes* of an *evaluation and testing framework for (mono|multi)modal biometric algorithms* are used [Brö03] in refinement and extension of a testing framework for monomodal biometric algorithms which is limited to operating systems' authentication [BKEK02]. The used sketch recognition algorithm is based on the active shape structural model (ASSM) [AZT02, AZT03]

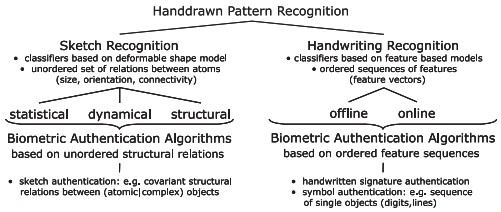

Figure 1: Classification of Biometric Sketch Authentication Applications

for analyzing the structural variability of sketches built up from deformable shapes.

Sketches were chosen for the biometric recognition algorithm because they are a very simple and intuitive way to represent secret information. They are easy to remember and draw. Sketches are gaining increasing importance with the shift to pen based interfaces as palm and tablet computers are proliferating. Currently sketching systems are employed in the field of design: Design of user interfaces [LNH00], recognizing mechanical designs [AD01] and content based image retrieval [VT00]. Many sketching systems are restricted to the usage of simple shape primitives like squares, circles, and polygons [AD01, FJ00]. ASSM describes sketches statistically allowing complex and uniform shape description.

We *define* a sketch as a set of structurally variable and statistically correlated drawing primitives of different complexity. As shown in figure 1, the structural component of a sketch (containing rich information in how the shapes relate to each other) is what differentiates sketches from handwritten signatures and symbols (simple fixed drawing) [LP94, ZTW96]. Taking into account the stroke directional information of handwritten characters and pictures (e.g. by analyzing the feature vectors of a pen's position, pressure, and inclination over time), related work with regard to the writer verification of hand written objects is given by [KHH02]. In our proposed method we are following a different approach which concentrates explicitly on the negotiated knowledge between user and authentication system represented on the algorithmic level as unordered structural relations within sketches given by the ASSM model.

Section 2 describes the main aspects of biometric authentication systems including their processes within IT security biometrics. In section 3 the sketch recognition algorithm based on the ASSM model will be mapped to the biometric processes of sensing, enrollment, authentication, and derollment within the evaluation and testing framework. The evaluation and testing will be done in section 4 by validating the biometric sketch recognition algorithm statistically (when users draw the same sketch), structurally (when users draw different sketches) and by imposter tests with different degrees of knowledge.

2 Biometric Authentication Systems

A biometric authentication system can be considered as a part of an IT infrastructure 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* [Brö03].

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. 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* 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 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*. In the phase of *derollment and authorization withdrawal* a person is derolled and the person's access rights are removed.

Biometric Processes Based on the general authentication process 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 [BKEK02] including enhancements concerning the clustering/classifying module (C) for the biometric en-/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 characteristics*, 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*, and 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[1]. If the biometric signature is hashed, the original raw data should not be reproducible from the hash values.

For en-/derollment the module C reclusters the space of biometric signatures 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

[1]The definition and classification of biometric signatures is given with [Brö03].

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*.

3 Biometric Sketch Recognition Algorithm

In this section the components of our proposed *biometric sketch recognition algorithm* based on the ASSM by Al-Zubi and Tönnies [AZT02, AZT03] is developed along it's mapping (see fig. 2) to the biometric processes of the evaluation and testing framework of biometric algorithms by Brömme [Brö03] for sensing, enrollment, authentication, and derollment. The following subsections describe each step of the algorithm in detail.

3.1 Sensor System Processes

Sensing Process & Human-Sensor System Interface. The sensing process depends on the chosen authentication system. For the herein used prototypical implementation under Windows XP a tablet screen with a digital pen by Wacom was used. A sketching program displaying the sketches drawn by the user (authentication GUI) including the possibility to manually revoke strokes and storing the strokes into a table of values was used.

Capturing/Scanning Process. A stroke is captured from the moment (event) the user puts his pen on the screen until he lifts it. Device coordinates of every point on the stroke as well as the time in milliseconds from the start of the stroke are recorded. Measurable values like pen pressure, pen azimuth and altitude *are not* recorded due to the fact that no dynamic (online) handwriting analysis will be applied like in [KHH02].

Biometric Raw & Sensor System Calibration Data. Every stroke is a sequence of points $((x_1, y_1, t_1), ..., (x_q, y_q, t_q))$ where (x_i, y_i, t_i), $i = 1...q$ are the (x_i, y_i) pixel coordinates of the pen and t_i is the time in milliseconds from the start of the stroke $t_1 = 0$.

3.2 Biometric Enrollment and Derollment Processes

(P) Preprocessing. During sampling, every stroke is converted to a parametric B-spline curve representation interpolating the sequence of device sampled points $s = ((x_1, y_1, t_1), (x_2, y_2, t_2), ..., (x_q, y_q, t_q)) \rightarrow x(t), y(t), 0 \leq t \leq t_q$ where t is the time in milliseconds. Time is used as the interpolating variable because it samples more of the curve at points of high curvature and detail.

(Q) Quality Check/Enhancement. Short strokes drawn by accident and stroke samples which are inferior in quality are removed.

(N) Normalization. An n-sampling of the stroke $\mathbf{sp}$ is a vector $\mathbf{x} = (x_1, x_2, ..., x_n, y_1, y_2, ..., y_n)^T$ where $(x_i, y_i) = \mathbf{sp}(\frac{(i-1)t_q}{(n-1)}), 1 \leq i \leq n$. Relations consist of multiple strokes represented as a list of splines $\mathbf{q} = (\mathbf{sp}_1, \mathbf{sp}_2, ..., \mathbf{sp}_m)$. $\mathbf{q}$ is statistically n-sampled by concatenating the corresponding n-sample vectors: $\forall \mathbf{sp}_i : 1 \leq i \leq m : \mathbf{x}_n = (\mathbf{x}_{1,n}^T, \mathbf{x}_{2,n}^T, ..., \mathbf{x}_{m,n}^T)^T$. A group of $\mathbf{p}$ stroke or relation samples $S = \{\mathbf{x}_1, \mathbf{x}_2, ..., \mathbf{x}_p\}$ are then iteratively aligned to each other using: translation and optionally rotation, scale or all three. The *rigid body alignment algorithm* is described in figure 5.

For implementing the normalization of a single user's sketch population, a sample queue within the normalization module (N) will be used to collect the different sketch samples given by the user during the enrollment procedure. After aligning we construct a data matrix $\mathbf{X} = (\mathbf{x}_1^T, \mathbf{x}_2^T, ..., \mathbf{x}_p^T)^T$.

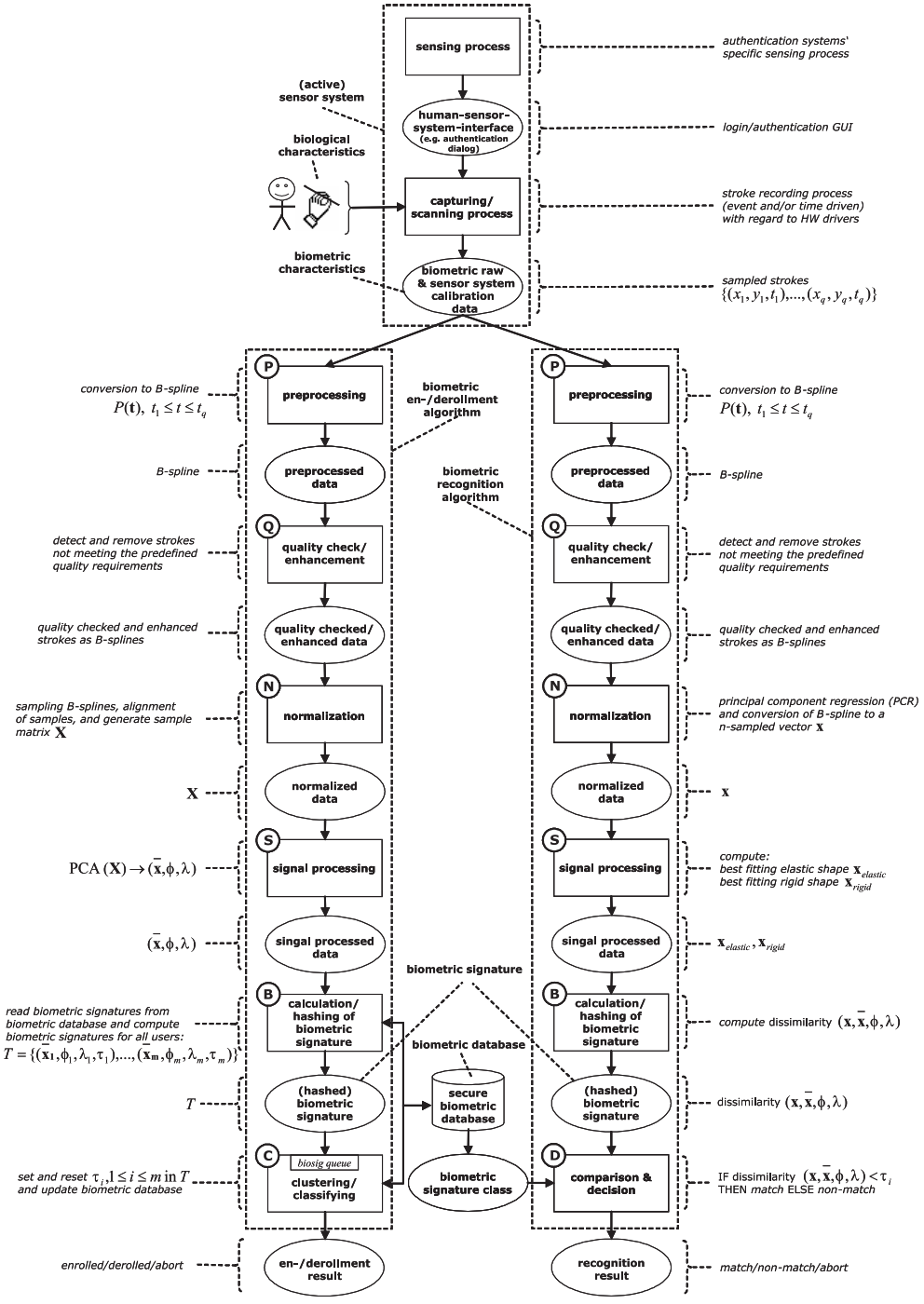

Figure 2: Biometric Sensing, Enrollment, Authentication, and Derollment Processes

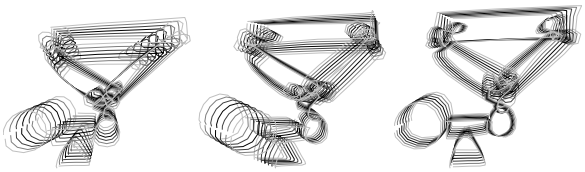

Figure 3: The effect of varying the first three shape parameters of an eleven-stroke shape ± 3 standard deviations

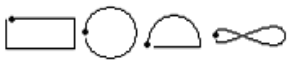

Figure 4: Shape types used to construct sketches: bar, wheel, base, and knot

1 $\bar{\mathbf{x}} \leftarrow \mathbf{x_1}$
2 **repeat**
3 **for** i=1 **to** p
4 find rigid body transform T that minimizes $\|\mathbf{T}(\mathbf{x_i}) - \bar{\mathbf{x}}\|$
5 $\mathbf{x_i} \leftarrow \mathbf{T}(\mathbf{x_i})$
6 $\bar{\mathbf{x}} \leftarrow \sum_{i=1}^{p} \frac{\mathbf{x_i}}{p}$
7 **until** $\bar{\mathbf{x}}$ converges

Figure 5: Sample rigid alignment algorithm

1 $\mathbf{x_0} \leftarrow \bar{\mathbf{x}}$
2 **do**
3 find a rigid body transform T that minimizes $\|\mathbf{T}(\mathbf{x}) - \mathbf{x_0}\|$
4 $\mathbf{x_1} \leftarrow \mathbf{T}(\mathbf{x})$
5 $\mathbf{b} = \mathbf{\Phi}^T(\mathbf{x_1} - \bar{\mathbf{x}})$
6 $\mathbf{x_2} \leftarrow \mathbf{x_0}$
7 $\mathbf{x_0} \leftarrow \bar{\mathbf{x}} + \mathbf{\Phi b}$
8 **while**$\|\mathbf{x_2} - \mathbf{x_0}\| > \varepsilon$
9 $\mathbf{x}_{elastic} \leftarrow \mathbf{x_0}, \mathbf{x}_{rigid} \leftarrow \mathbf{x_1}$

Figure 6: Deformable shape alignment algo

(S) Signal Processing. We apply *principal component analysis* on $\mathbf{X}$ to yield a t matrix of principal components $\mathbf{\Phi} = [\phi_\mathbf{1}, \phi_\mathbf{2}, ..., \phi_\mathbf{t}]$. The shape parameters are described by a vector $\mathbf{b}$ such that $\mathbf{x} = \bar{\mathbf{x}} + \mathbf{\Phi b}$. Figure 3 shows the first three variation modes of a complex 11-stroke shape analyzed from 20 samples. A biometric shape template is $(\bar{\mathbf{x}}, \mathbf{\Phi}, \lambda)$ where λ is the latent roots vector.

(B) Calculation/Hashing of Biometric Signature. Given a population of m users, we calculate biometric signature classes for every user $\{(\bar{\mathbf{x}}_\mathbf{1}, \mathbf{\Phi_1}, \lambda_\mathbf{1}), ..., (\bar{\mathbf{x}}_\mathbf{m}, \mathbf{\Phi_m}, \lambda_\mathbf{m})\}$ from his input samples. We also compute the matching thresholds for each user $\tau_\mathbf{i}$, $1 \leq i \leq m$ such that they have minimal overlap. The (hashed) biometric signature is given by the biometric signature table $\mathbf{T} = \{(\bar{\mathbf{x}}_\mathbf{1}, \mathbf{\Phi_1}, \lambda_\mathbf{1}, \tau_\mathbf{1}), ..., (\bar{\mathbf{x}}_\mathbf{m}, \mathbf{\Phi_m}, \lambda_\mathbf{m}, \tau_\mathbf{m})\}$.

(C) Clustering/Classifying. For the clustering/classifying step two possibilities are considered:

1. *Clustering/classifying without accepting a decreasement of the authentication system recognition performance.* Once the user n will be enrolled in addition to the already $(n-1)$ enrolled users, his biometric signature $(\bar{\mathbf{x}}_\mathbf{n}, \mathbf{\Phi_n}, \lambda_\mathbf{n})$ is compared with all enrollment samples of the previous $(n-1)$ users. If the mean dissimilarity is less than three standard deviations from another user's samples, then user n has to re-enroll with a new sketch (pattern).
2. *Clustering/classifying with accepting a decreasement of the authentication system recognition performance.* If the user needs to be enrolled with a fixed set of samples and the dissimilarity is less then three standard deviations, then a higher false match rate can be used to enroll the new user by adjusting $\tau_\mathbf{n}$. To maintain the algorithm's performance another sketch can be enrolled - as part of *biometric multitemplates* [Brö03] - for discriminating users.

Enrollment/Derollment Result. For derolling a user's biometric signature his enrollment samples will be removed from the biometric database.

3.3 Biometric Authentication Process

A user claiming a specific identity draws his sketch which is converted to a spline representation for verification and is authenticated by comparison with the biometric signature he has enrolled with.

(P) Preprocessing. The input stroke s is converted to a B-Spline representation $\mathbf{p}$ as described for the biometric en-/derollment process (see 3.2).

(Q) Quality Check/Enhancement. Very short strokes or strokes consisting of a single point are removed from $\mathbf{p}$ to get $\mathbf{p}'$.

(N) Normalization. To determine the shapes a regression technique is employed predicting new shapes if only some are given [AZT03]. The *principal component regression* (PCR) uses the shape parameter space $\mathbf{b}$ as regression and observation variables. The list of input strokes $\mathbf{p}'$ is n-sampled and converted to a vector representation $\mathbf{x}$.

(S) Signal Processing. A fitting process between $\mathbf{x}$ and the biometric template $(\bar{\mathbf{x}}, \mathbf{\Phi}, \lambda)$ is executed. The *elastic alignment algorithm* is described in figure 6 which computes fitted elastic and rigid shapes $\mathbf{x}_{elastic}$, $\mathbf{x}_{rigid}$.

(B) Calculation/Hashing of Biometric Signature. The shape similarity measure is computed as the weighted sum of the deviation of $\mathbf{x}_{elastic}$ from its mean and the maximum distance between $\mathbf{x}_{rigid}$ and $\mathbf{x}_{elastic}$ as follows

$$\textit{dissimilarity}(\mathbf{x}, \bar{\mathbf{x}}, \mathbf{\Phi}, \lambda) = \textit{deformation}(\mathbf{x}, \bar{\mathbf{x}}, \mathbf{\Phi}, \lambda) + \alpha \cdot \textit{distance}(\mathbf{x}, \bar{\mathbf{x}}, \mathbf{\Phi}, \lambda),$$

$$\textit{deformation} = \sqrt{\sum_{i=1}^{t} (\frac{b_i}{\lambda_i})^2)} \quad where \quad \mathbf{b} = \mathbf{\Phi}^t(\mathbf{x}_{elastic} - \bar{\mathbf{x}}) = (b_1, b_2, ..., b_t),$$

$$\textit{distance} = max_{i=1}^{p} \|u_i - v_i\| \quad where \quad \mathbf{x}_{elastic} = (u_1, ..., u_p), \mathbf{x}_{rigid} = (v_1, ..., v_p)$$

(D) Comparison & Decision. Every user i who enrolled into the system has a biometric signature $(\bar{\mathbf{x}}_\mathbf{i}, \mathbf{\Phi}_\mathbf{i}, \lambda_\mathbf{i})$ which is compared with his input $\mathbf{x}$ using the dissimilarity measure. If $\textit{dissimilarity}(\mathbf{x}, \bar{\mathbf{x}}, \mathbf{\Phi}, \lambda) < \tau_i$ we authenticate the user, otherwise we reject him.

Matching Result. The algorithm results in a match or non-match.

4 Evaluation and Tests of the Biometric Algorithm

The biometric signatures are used to characterize the input of users in two ways:

1. Statistically (quantitative features): If a population of users is asked to draw exactly the same shape, then the set of biometric signatures can be used to some extent for identification of users based on the characteristic way they draw these shapes. By increasing the complexity of the shape, the identification performance increases.
2. Structurally (qualitative features): A sketch additionally contains connectivity, scale and orientation relations between shapes. These relationships are represented in the biometric templates of single users and substantially improve discrimination performance in comparison to statistical features only.

Three types of tests were done to evaluate these two claims:

1. Handwritten PIN number tests: Testing the statistical claim.
2. Sketch tests: Testing the structural claim.
3. Imposter tests: Testing to what extent an intruder with no, partial or full knowledge about user sketches can be falsely authenticated.

task	description	objects	error %
1	Draw three connected wheels of different sizes	3	1.3%
2	Draw 3 connected bars with one bar is bigger than the others. Connect the bars to 3 knots	6	0.9%
3	Draw 2 connected wheels with one wheel is bigger than the others. Connect the wheels to a small bar. Connect bar to a big base.	4	0.7%
4	Draw Task 2 and task 3 and connect them with a knot.	11	0.0%

Figure 7: Sketching tasks given to users and their recognition errors

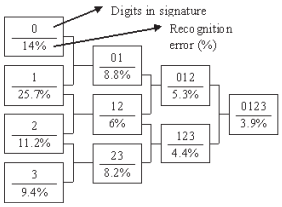

Figure 8: Recognition error rates decrease as more digits are combined

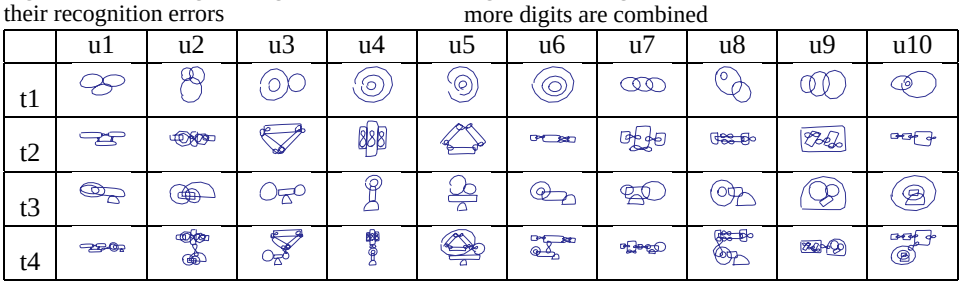

Figure 9: Mean sketches drawn by some users

Handwritten 4-Digit PIN Number Tests. A population of 10 users was asked to draw 30 times the PIN number *0123*. Each test used 20 randomly selected samples for training and the remaining 10 for testing. Each test was cross validated 10 times and the average error rate was computed. Each stroke was sampled by 32 points. The number of principle components was set to represent (explain) 98% of the samples and ranged between 11 to 15 principal components. Figure 8 shows how the recognition error rate drops from worst case 25.7% for digit *1* to 3.9% for the complete PIN. The conclusion is that the error rate of a combined structure is less than the error rates of its substructures.

Sketch Tests. Each user was given 4 tasks (t1,...,t4) of increasing complexity to complete in his way as shown in figure 7. Figure 9 shows some mean sketches drawn. Each stroke was sampled by 16 points. For every sketch, the number of principal components was set to explain 95% of the samples. The number of principal components ranges between 10 for task 1 and 15 for task 4. The experiments were conducted on 10 users (u1,...,u10). Each user sketched each task 30 times. For every user task, 20 randomly selected samples were used for training and the remaining 10 were used for testing. The tests were cross validated 10 times and averaged. As seen in figure 7, the average recognition error decreases as the complexity of the structures increases. Task 4 consisting of 11 objects had no error within this laboratory test setup.

Imposter Tests. These tests verify at what rate an enrolled user is falsely rejected and an imposter is falsely accepted within authentication. Three kinds of tests were considered:

1. The imposters have full knowledge of the sketch and try to copy it.
2. The imposters have partial knowledge of the sketch structure.
3. The imposters have no knowledge of the sketch structure at all.

The full knowledge test was conducted with two imposters who tried to copy 20 times task 4 of user 8. The results were compared with 10 user samples and cross validated 50 times. Figure 10 (top) shows the false match and non-match rate graph that resulted by adjusting the threshold on the dissimilarity measure. As we see the point of equal error rate is about

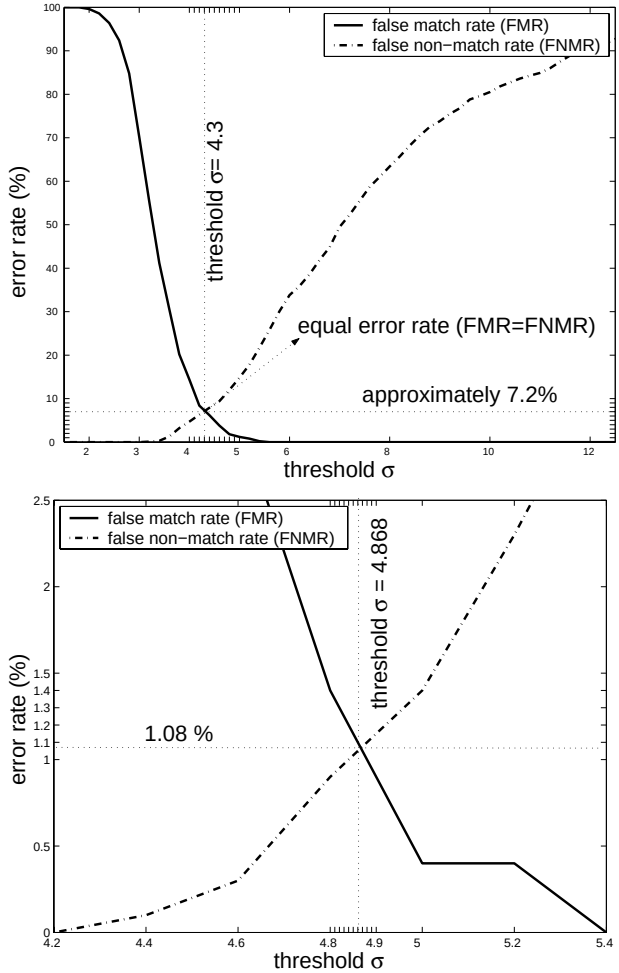

Figure 10: Imposter tests **top:** direct copying (task 4) **bottom:** last knot unknown (task 4)

7.2% which is due to the statistical properties differentiating the user from imposters. For the partial knowledge test two imposters were given all the knowledge about task 4 of user 8 except the position of the last knot which had to be guessed. 20 samples were drawn and the results are depicted in figure 10 (bottom). The point of equal error decreases to about 1%. Further tests with even less knowledge showed no error which validates the assumption that structural information is difficult to duplicate by an imposter when he has no knowledge about it.

5 Conclusions and Future work

In this paper we have developed a *multifactor biometric sketch authentication method* based on biometric sketch recognition and a user's personal knowledge about the sketch's content. The developed and used *biometric sketch recognition algorithm* is based on the *active shape structural model* for analyzing the structural variability of sketches built up from deformable shapes. The extension and adaption of the algorithm to the different *biometric processes* of biometric authentication systems has been done along an *evaluation and testing framework for (mono|multi)modal biometric algorithms and systems*. Within the evaluation and testing of the biometric algorithm it could be shown that the reliability of the used biometric sketch recognition algorithm has been increased for authentication purposes by systematically adding the user's knowledge about the sketch's content as an authentication factor. The robustness of this approach was validated against a test database by conducting imposter tests with varying knowledge about the user's sketch. The evaluation of the laboratory test results shows that mainly the factor of the user's knowledge as an added authentication factor leads the used sketch recognition algorithm to high accuracy.

Future work involves the further evaluation and testing of the proposed method against a large test database, the study of the intra- and inter-user variability of sketches in combination with knowledge, and the integration of the proposed multifactor biometric sketch authentication method into different authentication systems.

References

[AD01] C. Alvarado and R. Davis. *Resolving ambiguities to create a natural computer-based sketching environment*. International Joint Conference on Artificial Intelligence, 2001.

[AZT02] S. Al-Zubi and K. Tönnies. *Extending Active Shape Models to incorporate a-priori Knowledge about Structural Variability*. DAGM Pattern Recognition, 2002.

[AZT03] S. Al-Zubi and K. Tönnies. *Generalizing the Active Shape Model by Integrating Structural Knowledge to Recognize Hand Drawn Sketches*. CAIP 2003, 2003.

[BKEK02] A. Brömme, M. Kronberg, O. Ellenbeck, and O. Kasch. *A Conceptual Framework for Testing Biometric Algorithms within Operating Systems' Authentication*. ACM SAC 2002, Madrid, Spain, 2002.

[Brö03] A. Brömme. *A Classification of Biometric Signatures*. IEEE International Conference on Multimedia & Expo (ICME), Baltimore, USA, 2003.

[FJ00] M. Fonseca and J. Jorge. *Using Fuzzy Logic to Recognize Geometric Shapes Interactively*. IEEE International Conference Fuzzy Systems (FUZZIEEE), 2000.

[KHH02] Y. Kato, T. Hamamoto, and S. Hangai. *A Proposal of Writer Verification of Hand Written Objects*. IEEE International Conference on Multimedia & Expo (ICME), 2002.

[LNH00] J. Lin, M. Newman, and J.I. Hong. *DENIM: Finding a Tighter Fit Between Tools and Practice for Web Site Design*. CHI: Human Factors in Comp. Systems, 2000.

[LP94] F. Leclerc and R. Plamondon. *Automatic Signature Verivication: The State of the Art 1989-1993*. International Journal of Pattern Recognition and Artificial Intelligence, 1994.

[VT00] R. Veltcamp and M. Tanase. *Content-Based Image retrieval Systems: A Survey.* Tech. Rep. UU-CS-2000-34. Dep. of Computing Science, Utrecht Univ., 2000.

[ZTW96] R. Zhu, T. Tan, and Y. Wang. *Biometric Personal Identification based on Handwriting*. National Lab. of Pattern Recognition (NLPR), Chinese Academy of Sciences., 1996.