Advanced Studies on Reproducibility of Biometric Hashes

Tobias Scheidat[1], Claus Vielhauer[1,2], Jana Dittmann[1]

[1] Otto-von-Guericke University of Magdeburg, Universitätsplatz 2,
39106 Magdeburg, Germany
[2] Brandenburg University of Applied Sciences, PSF 2132,
14737 Brandenburg, Germany
[1] {tobias.scheidat | claus.vielhauer | jana.dittmann}@iti.cs.uni-magdeburg.de
[2] claus.vielhauer@fh-brandenburg.de

Abstract. The determination of hashes based on biometric data is a recent topic in biometrics as it allows to handle biometric templates in a privacy manner. Two main applications are the generation of secure biometric templates and cryptographic keys. Depending on these applications, there are different requirements with regard to possible errors. On one side, authentication performance based on biometric hashes as feature representation can be measured by common biometric error rates such as EER. Thus, generated hashes for each single person have to be only similar in a certain degree. On the other side, biometric hashes for cryptographic issues have to be identical and unique for each individual, although measured data from same person differs or data from different people may be similar. Therefore, we suggest three measures to estimate the reproducibility performance of biometric hash algorithms for cryptographic applications. To prove the concept of the measures, we provide an experimental evaluation of an online handwriting based hash generation algorithm using a database of 84 users and different evaluation scenarios.

Keywords: Biometrics, biometric hashing, collision, handwriting, measures, reproducibility, semantic fusion, verification

1 Introduction

In current biometric research, the generation of hash values based on biometric input is a recent topic. One goal of biometric hashing is the determination of a stable hash value based on a biometric trait of one person from its fuzzy input data in order to assure either authenticity and integrity, or confidentiality and privacy of biometric information. Another aim is the generation of unique individual values for cryptographic purposes ([1]), since the biometric information of a person is available anytime and anywhere, without the need to remember secret information or to present a special token.

In the following, a small selection from the variety of publications related to biometric hashing is presented, without neglecting others. In [2] the authors present a

method to calculate a cryptographic key based on a spoken password. Therefore, a 12-dimensional vector of cepstral coefficients is used as well as an acoustics model, which is speaker dependent. Based on these components, segmentation is carried out in order to create different types of features as basis of a so called feature descriptor which can be used as hash value. The biometric hashing method described by Vielhauer et al. in [3] is based on online handwriting biometrics and determines a feature vector of statistical parameters. These parameters are transformed into a hash value space using an interval mapping function, which results in a hash vector as feature vector representation. This method is described in more detail in section 2, since it was used as reference algorithm for the evaluation in this paper. Further methods for biometric hash generation can be found also for other biometric modalities, e.g. for face [4], fingerprint [5] or DNA [6].

This paper is structured as follows: The next section discusses relations between cryptographic and biometric hash functions and introduces the Biometric Hash algorithm, which is used as reference algorithm for our experimental evaluation. In the third section, new measurements are described to estimate the reproducibility performance of a biometric hash function motivated from [7]. The fourth section explains a fusion strategy of combining biometric hashes based on different handwritten contents. The evaluation database, methodology and the results with regard to biometric error rates and hash reproducibility are described in the fifth section. The last section concludes this paper and gives an overview of future work in this field of biometric research.

2 Biometric Hashing

Since the idea of a biometric hashing function is based on the principles of cryptographic hashing, the first part of this section discusses differences and similarities of cryptographic and biometric hash functions. In the second part, the reference algorithm used in our experimental evaluation is reintroduced shortly.

2.1 Cryptographic Hash Functions vs. Biometric Hash Functions

A cryptographic hash function ($h: A \rightarrow B$) has to fulfill different requirements ([8]): It has to be a so-called one-way function that provides the property of *irreversibility*, which describes the computational impossibility to determine any input data *a* from a hash value *h(a)*. Further, the *reproducibility* property of a hash function has to ensure that if any input data *a* and *a'* are equal, then also the output data *h(a)* and *h(a')* are equal. Contrariwise, in case *a* and *a'* are not equal, the corresponding hashes *h(a)* and *h(a')* have to be unequal. This requirement is called *collision resistance*. A fourth requirement of cryptographic hashes is the *bit sensitivity*. It states that small changes in the input data *a* (e.g. by alternating one bit) should lead to a big change in the output data *h(a)*.

Biometric hash functions should be also one-way functions to avoid obtaining the private user-related or relatable biometric input data from hashes. However, since biometric data is varying each time of acquisition even for the same user and trait

(intra-class variability), and data of different people may be similar (inter-class similarity), reproducibility and collision resistance have to be redefined for biometric hashing: On one side, *reproducibility* for the purpose of biometric hashing means the *identical hash reproduction for the same person and trait*, although the input data *varies within given bounds*. On the other side, the *collision resistance* of biometric hash functions describes the *ability to distinguish between (similar) data from different persons* to generate *different individual and unique hashes*. Consequently, due to the intra-class variability and inter-class similarity, the bit sensitivity property of cryptographic hashes cannot be mapped into the biometric hash methodology.

2.2 Biometric Hash Algorithm for Online Handwriting Biometrics

This subsection describes our Biometric Hash reference algorithm (see [3], [9]) based on online handwriting. Since we developed the new measures to quantify the degree of changes in an optimization process of the Biometric Hash algorithm, we use it as reference algorithm for our exemplarily evaluation based on these new measures. Figure 1 shows on the left side the enrollment process of the Biometric Hash algorithm. The first input data is a set of n raw data samples (D_1, …, D_n) derived from the handwriting acquisition sensor, e.g. tablet PC or PDA.

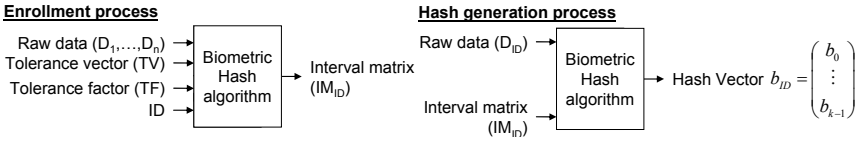

Fig. 1. Enrollment and hash generation processes of the Biometric Hash algorithm [3]

The aim of the enrollment process is to generate a so-called interval matrix *IM* for each user based on its raw data and several parameters. Generally, each raw data sample D_i ($i=1,\ldots,n$) consists of a temporarily dependent sequence of physical values supported by the device, such as pen tip coordinates $x(t)$ and $y(t)$, pressure $p(t)$ and pen orientation angles altitude ($\Phi(t)$) and azimuth ($\Theta(t)$). During the enrollment process, for each of the raw data samples D_i derived from a person, a statistical feature vector is determined with a dimensionality of k ($k=69$ in the current implementation). *IM* stores for each feature the length of an interval and an offset, where both values are calculated based on the intra-class-variability of the person, by using his/her statistical feature vectors. To parameterize the hash generation, the tolerance vector *TV* is used. The *TV* supports an element wise parameterization of the statistical features during the generation of hash values by the so-called interval mapping function. Thus, the dimensionality of *TV* is also k. The *TV* can be determined for each user individually or globally by a group of persons, either based on the registered users or a disjoint user set. The third input data is the tolerance factor *TF* as global hash generation parameter, which is a scalar value. Using the *TF*, it is possible to scale the mapping intervals for all feature components globally by one factor, thus affecting both reproducibility and collision resistance, where increasing values of *TF*

lead to the tendency of increasing reproducibility at cost of increasing collision probabilities. The user's identity *ID* is the fourth input for the enrollment process, which is linked to the reference data. Note that in our context, reference data is the output of the Biometric Hash algorithm's enrollment mode in form of the interval matrix IM_{ID} that provides information for the mapping of the individual statistical features to the corresponding hash values, but neither the original biometric input nor the actual feature vectors. The right side of Figure 1 shows the hash generation process of the Biometric Hash algorithm. Here, the input data consists of only one single raw data sample D_{ID} and the interval matrix IM_{ID} of a claimed identity *ID*. The raw data D_{ID} is used to determine a *k*-dimensional statistical feature vector. Based on this vector and the IM_{ID} the interval mapping function calculates a biometric hash vector b_{ID}, where interval lengths and offsets provided by IM_{ID} are used to map each of the *k* statistical features to a corresponding hash value. The biometric hash vector can be used either for cryptographic applications (e.g. key generation) or for biometric verification. In the latter case, the biometric hash vector b_{ID} generated from the currently presented authentication sample D_{ID} is compared against the reference hash vector $b_{ref\ ID}$ of the claimed identity ID, which in this case needs to be stored as additional information during the enrollment process. The classification can then be performed for example by some distance measurement and comparison to a given threshold *T*. On the other hand, for verification based on crypthographic hashes (e.g. message authentication codes, *MAC*) the reference hash and the hash generated for the currently presented data have to be identical, if and only if the hashes generated based on identical data.

In this paper we study the performance of the Biometric Hash algorithm with regard to both, verification mode and hash generation mode, based on different setups, i.e. four different semantics and pair wise multi-semantic fusion.

3 New Performance Measures for Biometric Hashing

Based on the biometric data obtained, a hash generation method aims to generate identical hashes from data of the same person and/or different hashes from data of different users, respectively. In order to provide a measure for the degree of the reproducibility and/or false generation of such hashes, we suggest the Hamming Distance ([10]) as already shown in [9] and [7]. In context of the comparison of two biometric hashes *b* and *b'*, the Hamming Distance measure determines the number of positions, where the two hashes are different and returns a value between *0* and the number of elements.

$$hd(b,b') = \sum_{i=0}^{k-1} dist(b_i, b'_i) \qquad with\ dist(b_i, b'_i) = \begin{cases} 0, if\ b_i = b'_i \\ 1, else \end{cases} \tag{1}$$

In equation (1), b_i and b'_i are the corresponding elements of vectors *b* and *b'* at index *i*. The component-wise comparison of b_i and b'_i yields *0*, if the two elements are

equal and *1* otherwise. Then the Hamming Distance between the hashes *b* and *b'* is the sum of the results of all single comparisons.

Derived from the properties of cryptographic hashes, error rates to estimate the performance of biometric hash algorithms should be considered in the reproduction and the collision in addition to *FRR*, *FAR* and *EER*. In our Hamming Distance based histogram analysis, we compare all generated biometric hashes of each person to each other hash of the same person to calculate the *reproducibility rate* (*RR*). Therefore, a Hamming Distance *hd* of *0* is logged as a match, while any *hd* > *0* is logged as a non-match. Then, the Reproducibility Rate is the quotient of the number of matches by the number of comparisons. The *collision rate* (*CR*) is determined by the comparison of each single person's biometric hashes with the hashes of all other users. For the *CR*, a Hamming Distance of *0* is logged as a collision and all distances higher than *0* are logged as non-collision. The *CR* is calculated by the division of the number of collisions by the number of comparisons. In the ideal case, each comparison between hashes of the same person and semantic should be result in *hd=0*, while the comparison between hashes of any two different persons should yield *hd>0*. In order to refer to reproducibility requirement, the point of interest in the histogram is a Hamming Distance value of *0*. This means for *RR*, only the identical reproductions of hashes of the corresponding person are considered, while for the *CR* only identical generations of hashes of non identical persons are examined. However, for the optimization process of a biometric algorithm, the entire Hamming Distance based distribution should be taken in consideration. In order to have an indicator of the trade-off relation between *RR* and *CR*, an additional measure is introduced here: the *collision reproducibility ratio* (*CRR*) as result of the division of *CR* by *RR*. Since one aim of biometric hashing is to reproduce hashes of each person with a high degree, while hashes of different persons should be different, the *CRR* should be very small.

4 Multi-semantic Hash Fusion Approach

In this section we present a new biometric fusion strategy based on the pair wise combination of the biometric hash vectors of two semantic classes. In the context of biometric handwriting, semantics are alternative written contents in addition to the signature. Semantics can be based on the additional factors of individuality, creativity and/or secret knowledge, e.g. by using pass phrases, numbers or sketches. In [9], Vielhauer shows that the usage of such alternative contents may lead to similar results as the usage of the signature in context of online handwriting based authentication performance. Based on the number of biometric components involved in the fusion process, Ross et al. differentiate in [11] between the following five scenarios for automatic biometric fusion: multi-sensor, multi-algorithmic, multi-instance, multi-sample and multi-modal systems. Since the fusion proposed in this paper is executed on the feature extraction level in the hash domain based on different semantics, it is called multi-semantic hash fusion. It can be assigned to the multi-instance stage of the scheme suggested by Ross et al.

The first step is the data acquisition of two semantics, which form the input for the second step, the hash generation. In this process step, the statistical feature vector is

calculated from raw data of each semantic. Then, biometric hash vectors are derived from the semantics' statistical values, as described in the previous section. Although, the tolerance factor *TF* used for hash generation is identical for both semantics (*TF=3*), it is also feasible to tune the TF separately in dependency on corresponding semantic to optimize the fusion result. The global tolerance vector TV is determined globally based on disjoint user sets of the corresponding semantics. Thus, for both, statistical feature vectors and biometric hash vectors, the dimensionality is *k*. The fusion of the two hashes is the last process step, which is carried out as concatenation of both hashes and leads to a hash vector's dimensionality of *2*k*.

5 Evaluation

This section firstly describes the test data used in our evaluation. Following, our methodologies are presented, which are used to determine the results of biometric handwriting verification as well as biometric hash generation. Finally, the results for both, verification and hashing are presented and discussed.

5.1 Evaluation Database

The entire test set is based on *84* users, each of them having donated *10* handwriting samples for four different semantics (total of *3,440* samples). The *PIN* is given as a sequence of the five digits '77993'. Using this semantic, the individual style of writing plays a more important role than the content, since all test subject write the same numbers. The semantic *Place* represents the individual answer to the question "Where are you from?", written by each test person. This answer includes individual knowledge in a certain degree which, however, is not absolutely secret. We use the semantic *Pseudonym* as anonymous substitution of the individual signature, due to the fact that most of the test subjects refrained from donating their original signature due to privacy concerns. The *Pseudonym* is a name freely chosen by the writer, which had be trained several times before the acquisition. The freely chosen *Symbol* holds individual creative characteristics and additionally provides a knowledge based component in form of the sketched object.

In order to determine a global tolerance vector *TV* as hash generation parameter and to carry out the biometric error rate analysis and the Hamming Distance histogram analysis, a training set (hereafter set *T*) of *15* users and an evaluation set (hereafter set *E*) of *69* users are extracted from the entire set of *84* persons. Both sets are entirely disjoint with respect to the subjects and structured as follows: From the *10* handwriting samples $D=D_1,\ldots,D_{10}$ of each person and each semantic, the first *5* samples $D_1,\ldots,D_5$ are taken to create *5* sets, using a leave-one-out strategy. This means a combination of *5* choose *4*, i.e. *5* different sets are created, containing *4* handwriting samples each. Each of the 5 sets is used to create a user dependent interval matrix (IM_{ID}) and consequently, we yield reference data $R_i=(ID, IM_{i,ID})$ with $i=1,\ldots,5$. Based on these interval matrices and the remaining samples $D_6,\ldots,D_{10}$, *5* biometric hashes are created for each user of set *T* and set *E* respectively. The determination of the tolerance vector *TV* is conducted globally, based on all users of

set *T*, whereas the biometric error rate analysis and a Hamming Distance based histogram analysis are carried out on disjoint set *E*.

5.2 Evaluation Methodology

In this paper, we use the equal error rate (*EER*) to show the verification performance of the reference algorithm in comparison to the reproducibility performance of biometric hashes based on dynamic handwriting. For the latter evaluation, we analyze the Biometric Hash algorithm (see section 2.2) by using the new measurements Reproducibility Rate (*RR*), Collision Rate (*CR*) and Collision Reproducibility Ratio (*CRR*) to compare the reference and current hashes as described in section 3.

Note that for the evaluation of the multi-semantic fusion, we assume that there is no temporal dependence between semantic 1 and semantic 2 (i.e. *EER*, *RR*, *CR* or *CRR* of fusion of semantic 1 and semantic 2 is equal to *EER*, *RR*, *CR* or *CRR* of fusion of semantic 2 and semantic 1). Thus, the outcome of the fusion is symmetric with respect to the sequence semantics taken into account, and results to the triangular layout of Table 1 and Table 2.

In our previous work, we optimized the tolerance factors *TF* for verification as well as for hash generation in a certain degree. We observed, that for verification the best integer *TF* is *1*, while for hash generation *TF=3* was relatively good. Thus, we use in this initial study these both values for the corresponding evaluations. The hash generation for both applications is also based on a global *TV* determined on a disjoint set of users per semantic. However, it is also possible to use alternative parameterizations for *TF* and *TV* to optimize both, verification and hash generation performance.

5.3 Results

This subsection describes the results of the verification and the hash reproducibility. The corresponding tests are carried out on the single semantics as well as on their pair wise fusion. In tables 1 and 2 the best single results are printed in bold, while the best fusion results for *EER*, *RR*, *CR* and *CRR* are marked with a gray background.

Biometric Error Rate Analysis. Table 1 shows the results of the biometric error rate analysis. While the second column (*single*) presents the *EERs* of the individual semantics, the last three columns are showing the pair wise fusion results. The fusion is carried out on the matching score level and is based on a simple mean rule. This strategy weights the scores of the two fusion components involved with the same value (*0.5*) and summates the results to a final fused score. For the verification, the best single-modal result with respect to the *EER* is determined for the *Symbol* with *EER=3.199%*. The worst *EER* of *4.969%* is based on semantic *Pseudonym*. Another observation from Table 1 is that all pair wise fusion combinations improve the results determined by the corresponding semantics. Here the lowest *EER* of *1.143%* is calculated based on the combination of *Place* and *Symbol*.

Table 1. Equal error rates in % per semantic class and their pair wise fusion (*TF=1*)

		Multi-semantic fusion		
	single	Symbol	Pseudonym	Place
Semantic	**EER**	**EER**	**EER**	**EER**
PIN	4.763	1.719	2.249	1.982
Place	3.541	1.143	1.632	-
Pseudonym	4.969	1.382	-	
Symbol	**3.199**	-		

Hamming Distance based Histogram Analysis. The results of the Hamming Distance based histogram analysis for single semantics as well as for their pair wise fusion are presented in Table 2. In the rows of Table 1 labeled with RR the reproducibility rate of genuine hashes by the corresponding genuine users is shown in dependency of the semantic class. The rows labeled with CR are showing the collision rate, while the CRR rows present the collision reproducibility ratio.

Table 2. Reproducibility and collision rate in % and collision reproducibility ratio for single semantics and pair wise semantic hash fusion (*TF=3*)

			Semantic 2		
Semantic 1	**Measurement**	**single results**	**Symbol**	**Pseudonym**	**Place**
	RR	76.580	60.000	55.304	55.536
PIN	**CR**	5,818	0.346	0.685	1.207
	CRR	0.076	0.006	0.012	0.217
	RR	72.116	57.217	52.696	
Place	**CR**	5.115	0.319	0.484	-
	CRR	0.070	0.006	0.009	
	RR	70.551	56.290		
Pseudonym	**CR**	4.923	0.223	-	
	CRR	0.070	0.004		
	RR	**77.101**			
Symbol	**CR**	**2.392**	-		
	CRR	**0.031**			

As shown in the third column of Table 2, the best reproducibility rate of genuine hashes is calculated for *Symbol* with a *RR* of *77.101%*. A similar result is calculated based on the *PIN* with *RR=76.580%*. However, since *PIN* is the given sequence of the digits '77993' written by all persons, the collision rate (*CR=5.818%*) is the highest. Thus, also the collision reproducibility ratio for *PIN* (*CRR=0.076*) is higher than the *CRRs* for the other semantics. From the point of view to choose the semantic having the best ratio between *RR* and *CR*, the semantic *Symbol* should be taken in consideration (*CRR=0.031*).

Since the multi-semantic hash fusion is carried out as simple concatenation (see section 4) of two hashes based on different semantics, the reproducibility of the new fused hash depends only on the individual reproducibility of the two hashes involved. Based on this fact, it is obvious that the *RR* of the fused hashes cannot be higher than the worst individual reproducibility rate of the two hashes used for the fusion. Table 2 shows also the results of the pair wise multi-semantic hash fusion. The intersections of rows and columns of the different semantics are showing the corresponding fusion results for reproducibility rate (*RR*), collision rate (*CR*) and collision reproducibility

ratio (*CRR*). As assumed, a general observation is, that the fusion results for the reproducibility rate are worse than the results obtained based on the single semantics (see second column of Table 2). For example, the best fusion result is based on the concatenation of the hashes for *PIN* and *Symbol* where the *RR* is equal to *60%*, while the single results amount *76.58%* for *PIN* and *77.101%* for *Symbol*, respectively. This corresponds to a relative degradation of approx. *22%* in comparison to the best single result determined for the *Symbol*. On the other hand, the collision rates are significantly lower than those of the single semantics involved. Here the relative decline lies between *77%* and *90%*. The best *CR* of *0.223%* was determined for the fusion of semantics *Pseudonym* and *Symbol*, while the corresponding *RR* amounts *56.29%*. The greatest improvement of the fusion we see in the decrease of the *CRR*. In case of the best fused *RR* of *60%* the *CRR* is reduced to one fifth (*0.006*) of the *CRR* of the best single result calculated for symbol (*0.031*). Thus, the fusion may provide the opportunity to reach a higher *RR* at an acceptable *CR*.

The results of biometric error rate as well as Hamming Distance based histogram analysis show that there is a dependency between *EER* and/or *RR* and *CR*, and the written content. Based on these results it can be stated, that the choice of a semantic depends on the requirements of the verification and/or hashing application. It can be decided on best equal error rate performance or on best reproducibility, best collision resistance as well as on the best ratio between them.

6 Conclusions

In this paper, we suggest the analysis of the biometric hash reproducibility and collision rates based on the Hamming Distance, in addition to the typical verification error rates. The reproducibility rate (*RR*) shows, how is the performance of a hash generation algorithm with respect to generate stable has values for the same persons and the same written content. The collision rate (*CR*) is a measure for the probability of generation of biometric hashes by non-authentic users. Further, the collision reproducibility ratio (*CRR*), as third introduced measure, indicates the tradeoff relation between *CR* and *RR*. In order to find a suitable working point for a biometric hash generation algorithm for practical applications, one solution can be to minimize the *CRR*. Further, we have suggested a novel concept in the domain of multi-biometrics: Multi-semantic fusion of biometric hashes generated using different writing contents.

In the experimental evaluation, we have practically shown the feasibility of the new measurements based on online handwriting biometrics. On one side, the evaluation of the multi-semantic hash fusion has shown that the concatenation of two hashes using different semantics leads to a significantly worse reproducibility rate than the individual semantics. Here the best fusion result is calculated for the combination of *PIN* and *Symbol* (*RR=60%*), while the individual *RRs* for *PIN* and *Symbol* amount *76.580%* and *77.101%*, respectively. On the other side, a significant improvement of the collision rate can be observed. The best *CR* of *0.223%* is determined based on the semantics Pseudonym and *Symbol*. This leads to the best collision reproducibility ratio of the entire evaluation (*CRR=0.004*) and this

significantly improved trade-off between *RR* and *CR* provides potential for optimized parameterization towards better *RR* at acceptable *CR* level.

To do so, the parameterization can be adjusted to any user registered in the database by optimizing user specific tolerance vectors, which are used to calculate the mapping interval of the Biometric Hash algorithm. In order to improve the *RR* even more, other methods have to be studied, e.g. alternative mapping functions or error correction mechanisms. In this case, one has also to keep track of the expansion of *CR* as counterpart of *RR*. Finally, although in this paper we have focused on biometric hashes for handwriting, it appears quite possible to apply the methodology to hashes generated based on other biometric modalities in the future.

Acknowledgements. The work on biometric hashes with regard to verification and reproducibility is partly supported by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation, project WritingPrint).

References

1. Dittmann, J., Vielhauer, C.: Encryption Related Issues. Joint COST 2101 and BioSecure Industrial and End-user Committee Workshop on “Smart Cards and Biometrics”, Lausanne (2007)
2. Monrose, F., Reiter, M. K., Li, Q., Wetzel, S.:, Using Voice to Generate Cryptographic Keys. A Speaker Odyssey, the Speech Recognition Workshop, Crete (2001)
3. Vielhauer, C., Steinmetz, R., Mayerhöfer, A.: Biometric Hash based on Statistical Features of Online Signature. In: International Conference on Pattern Recognition, Quebec City (2002)
4. Sutcu, Y., Sencar, H. T., Memon, N.: A Secure Biometric Authentication Scheme Based on Robust Hashing. In: 7th workshop on Multimedia and security, ACM Press, New York (2005)
5. Tulyakov, S., Farooq, F., Govindaraju, V.: Symmetric Hash Functions for Fingerprint Minutiae. In: International Workshop on Pattern Recognition for Crime Prevention, Security and Surveillance, Bath (2005)
6. Korte, U. et al.: A cryptographic biometric authentication system based on genetic fingerprints, In: Alkassar, Siekmann (Eds.): Sicherheit 2008 - Sicherheit, Schutz und Zuverlässigkeit; Beiträge der 4. Jahrestagung des Fachbereichs Sicherheit der Gesellschaft für Informatik e.V., Saarbrücken (2008)
7. Scheidat, T., Vielhauer, C.: Biometric Hashing for Handwriting: Entropy based feature selection and semantic fusion. In: SPIE - Security, Steganography and Watermarking of Multimedia Contents X, IS&T/SPIE Symposium on Electronic Imaging, San Jose, California (2008)
8. Bishop, M.: Computer Security: Art and Science. Addison-Wesley, Reading, Mass (2003)
9. Vielhauer, C.: Biometric User Authentication for IT Security: From Fundamentals to Handwriting. Springer, New York (2006)
10. Hamming, R.W.: Error-detecting and error-correcting codes. Bell System Technical Journal XXVI (2) (1950)
11. Ross, A., Nandakumar, K., Jain, A.K.: Handbook of Multibiometrics. Springer, New York (2006)