Semantic Conformance Testing for Finger Minutiae Data

Christoph Busch, Dana Lodrova
Gjøvik University College, Teknologiveien 22, 2815 Gjøvik, Norway
christoph.busch@hig.no,

Elham Tabassi
National Institute of Standards and Technology (NIST)
Gaithersburg, U.S.A.

Wolfgang Krodel
German Federal Criminal Police Office (BKA), ZD23/AFIS
Wiesbaden, Germany

Abstract

This paper describes a scheme for semantic conformance testing of standardized biometric interchange records. While conformance testing on a syntactical level has been formulated in the modality specific assertion test, there is yet no testing methodology being developed that could attest that a compact interchange record such as a minutiae template is indeed a faithful representation for the input signal. Thus we provide a testing methodology and outline to which extend this methodology can benefit from ground truth data being collected by forensic experts.

1. Introduction

Standardization in the field of information technology is pursued by a Joint Technical Committee (JTC1) formed by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). The international body for biometric standardization in JTC1 is the subcommittee 37 (SC37). An important part of SC37's work is the definition of data interchange formats into which the representation of a biometric characteristic can be encoded in a specified data structure. This data structure can then be stored as a reference on a SmartCard or in a database. In case of an open system this reference must be interoperable, e. g. different manufacturers must be able to read and understand the data interchange format and also to generate a good recognition performance on the basis of these data samples.

Within ISO/IEC JTC1 SC37 Working Group 3 (WG3) a series of interchange formats are developed. Among those standards is the feature based standard ISO 19794-2:2005 Finger minutiae data [3], which is relevant for numerous eID cards.

The current focus of WG3 is to develop for all interchange formats a conformance test [6][5]. The goal of such conformance testing for biometric data formats is to attest for a specific product of interest (referred to as "unit") that interchange records generated by the unit are not only field by field conformant to the ISO standard but also to attest that the generated record is a semantically correct representation of the input data.

This paper is organized as follows. In Section 2 the ISO levels of conformance testing and specificalities for finger minutiae data records are introduced. The efforts to generate a large scale database with ground truth data are discussed in Section 3 and relevant metadata associated with finger print minutiae are identified. While conformance testing on a syntactical level has been formulated in the fingerprint modality specific assertion test [5], there is yet no formulation for a semantic level. Thus in Section 4 we suggest a semantic conformance testing methodology that could attest that a compact interchange record such as a minutiae template is indeed a faithful representation of the input signal. Thus we provide a testing methodology for biometric interchange records that claim compliance with ISO 19792-2. We outline to which extend this methodology can benefit from ground truth data being collected by forensic experts.

2. Types and Levels of Conformance Testing

A generalized conformance testing methodology has been developed within ISO FDIS 29109-1[6]. This ISO project introduced test types, test levels and testing methodologies for units that claim compliance for their generated data interchange records according to ISO standards. Basically two test types are distinguished:

- **Type A:** Conformance tests of this type are attesting that a unit is *generating* conformant biometric data interchange records. In the case of fingerprint data this tests will verify that a unit (e.g. a minutia extraction algorithm) can create finger minutiae data records (templates) from appropriate fingerprint image data.
- **Type B:** With a conformance test of Type B a conformance claim is verified that the unit under test is capable to *read* conformant biometric data interchange records. For a fingerprint recognition system this test will show that the component is capable to interpret both the stored template and the probe correctly and to perform a desired function upon them, which could be the comparison of the two records and eventually the generation of a comparison score.

The ISO FDIS 29109-1 focuses on Type A testing and so do we in this paper. Three different conformance testing levels are categorized in [6]:

- **Level 1** Basic Data Field Testing:
  This test level defines an assertion test that all data fields exist properly (e.g.in the correct encoding.) The conformance testing methodology for finger minutia data on this level [5] checks field by field and byte by byte conformance with the specification of the biometric data interchange record as specified in the base standard [3], both in terms of fields included and the ranges of the values in those fields. The focus of this test is on syntactic requirements of the base standard.
- **Level 2** Internal Consistency Testing:
  The subsequent test level defines an assertion test that all data fields are filled with meaningful values and the fields are internally consistent; values from one part or field of the biometric data interchange record are correctly related to values from other fields of the record. Again the focus on this level is to test syntactic requirements of the base standard.
- **Level 3** Semantic Testing:
  The ultimate test levels defines a semantic test to verify that a generated biometric data interchange record is a faithful representation of the initial digital representation (e.g. the fingerprint image) of the biometric characteristic (e.g. the finger pattern). Thus the conformance testing methodology needs to verify that the extracted features (e.g. minutia coordinates) are within tolerances bounds to real minutia coordinates. The focus on this level is to test semantic requirements of the base standard.

While progress in the definition of Level 1 and Level 2 has been made with ISO-projects FDIS 29109-1 [6] and FCD 29109-2 [5] and it is likely that corresponding conformance tests will be conducted soon, there is no concept yet for Level 3 testing. Nevertheless the existence of such conformance testing methodologies is of outmost importance for the market, as more and more biometric system operators are asking in their call for tender the vendors to submit with their offer conformant testing results.

2.1 The Challenges of Semantic Testing

For semantic conformance testing it is required to have a database of ground truth data that is composed by a sufficiently large number of *"ground truth minutia"* (referred to as "$gt - minutia$" or "gtm"). Then a Level 3 test can compare fields (location, angle etc.) of the automatic extracted minutiae data with the ground truth data. Composing a gt-minutiae database of sufficient size is a tremendous effort and it might - on the first glance - be a straightforward approach to apply a number of well known algorithms that have proven to result in a good biometric performance and compute automatic extracted minutia. As multiple algorithms are unlikely to produce one and the same data (coordinate / angle) the test database would be composed by computing the average over the results taking potential outliers into account. However results achieved with this approach can not be considered *ground truth* as the approach incorporates two fundamental drawbacks:

1. *Logic conflict*: Using the output of automatic processes to prove a conformance claim of an automatic process (the biometric feature extraction unit) is a conflict with fundamental principles of logic. This would correspond to a mathematical proof, in which a mathematical statement is proven by a series of inductive arguments, where one or more arguments contains the initial statement to be proven.
2. *Cartelization support*: The selection of "known algorithms" is likely to lead to a cartelization among the envolved vendors (algorithm developers). In consequence using the output generated by such a cartel technology for proof of a given conformance claim implies the risk that derivates of such cartel algorithms (i.e. new releases) have a high probability to pass the conformance test, where new and independent labs submitting an algorithm to the same test procedure have a lower probability. All in all this could be an undesired step towards monopolization of the biometric market.

An objective and reliable conformance test can only be achieved, if the ground truth data has been composed in an undoubtable independent manner.

3 Generating Ground Truth Data

As argued in the previous Section *real* ground truth data is a mandatory requirement for conformance testing on Level 3. The subsequent Sections will identify all necessary information for generation of such real ground truth data and define necessary requirements for the data collection.

3.1 Image Material

The fingerprint images needed to generate ground truth data has been provided by the National Institute of Standards and Technology (NIST). The fingerprint image data has been selected from special databases administrated by NIST such as SD14 (all rolled data and mostly ink with few live scanned images) and SD29 (flat data /plain impression but all ink). The selection of 5000 fingerprint image pairs avoids systematic effects. Fingerprint images selected are equally representing male and female data subjects. Furthermore the images do represent fingerprint image data at different image quality levels according to NFIQ [2].

The fingerprint recognition experts at NIST have provided a 5000 image pair selection, such that genuine comparison scores can be computed for fingerprint templates with regard to all biometric capture subjects. The images are stored in five equally sized bins with equivalent characteristics, such that 1000, 2000 or 5000 image pairs can be processed by a volunteering human expert crew - and therefore a contribution to the gt-minutiae database can be made by various institutions even though the individual extent of available resources and/or the effective time consumption might be quite different.

The long term goal of this activity is to compose a gt-minutia database consisting of three segments: tenprint card fingerprint images, live scan images and latent print images (from crime scenes). However for the time being only the first segment is composed.

3.2 Expert Crew and Constraints

The dactyloscopic experts of the German Federal Criminal Police Office (BKA) have volunteered to provide support and to place real minutia data. The expert crew consists of 6 dactyloscopic experts. Those experts are highly experienced. The team started working on the image material in February 2009. Initial investigations of the human expert image assessment process indicated that the personal effort to complete the first bin of approx. 1000 images pairs (2000 images) is approximately one man year.

Each expert will specify minutia, core and deltas and correspondent assurance levels. These measurements are stored in a simple ASCII file (see figure 2)

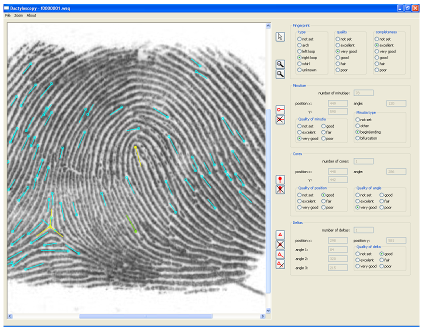
It is required to document for each gtm-file how the respective expert in general marks minutia, and what rule(s) he is used to follow with respect to the understanding of ridge endings as ridge-skeleton-end-point versus valley-skeleton-bifurcation. Along this line it is an essential meta information in the gt-minutia database to trace, whether an expert was stemming from an European ”minutia culture” (within which the expert has been trained to place a ridge ending coordinate as ridge-skeleton-end-point) or stemming from an American ”minutia culture” (within which the expert has been trained to place a ridge ending coordinate as valley-skeleton-bifurcation). As the ground truth database will grow the testing of various format types in 19794-2 will become possible. More specifically this is relevant for semantic conformance testing with respect to format types 25(0019 Hex) and 26(001A Hex) according to 19794-2:2005 COR 1 [4].

In order to minimize systematic effects in the ground truth data the expert crew has committed itself to independent operation: The experts that conduct the gt-minutia placements work fully independent and are not influenced by their colleagues. Furthermore any help from their day-to-day tool, which is an AFIS-client workstation, is not acceptable in this process. In order to avoid any unwanted influence on the test outcome there shall be no impact of any automatic or semi-automatic minutia extraction functionality of any AFIS system whatsoever. Automated minutia extraction algorithms would highly influence the minutia data and thus the Level 3 conformance testing result at most.

3.3 Graphical User Interface for Ground Truth Data Collection

The working environment should be efficient for the experts. However as any support of automatic AFIS functionality is not acceptable a simple Graphical User Interface was needed, to which dactyloscopic experts could adapt in a short period of time. Thus an independent GUI has been generated for the data collection (see figure 1). The GUI software is operational on WindowsXP SP2.

Dactyloscopic experts working with this GUI on the selected image material are expected in the first step to conduct global attributes for a fingerprint image, namely the fingeprint type, quality and completeness. In a second step the experts identify and mark each minutia, core and delta with its angle on the loaded image. Furthermore they asses metadata such as for instance the minutia quality assurance level. The full list of data fields is given in table 1.



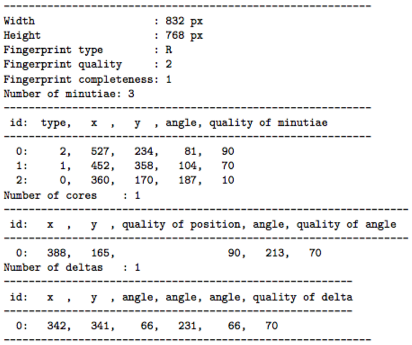
Fingerprint
type: ○ not set ○ arch ○ left loop ● right loop ○ whirl ○ unknown
quality: ○ not set ○ excellent ● very good ○ good ○ fair ○ poor
completeness: ○ not set ● excellent ○ very good ○ good ○ fair ○ poor

Minutiae
number of minutiae: 78
position x: 449 angle: 120
y: 590
Quality of minutia: ○ not set ○ excelent ● very good ○ good ○ fair ○ poor
Minutia type: ○ not set ○ other ● begin/ending ○ bifurcation

Cores
number of cores: 1
position x: 448 angle: 286
y: 442
Quality of position: ○ not set ○ excelent ○ very good ● good ○ fair ○ poor
Quality of angle: ○ not set ○ excelent ● very good ○ good ○ fair ○ poor

Deltas
number of deltas: 1
position x: 298 position y: 581
angle 1: 84
angle 2: 320
angle 3: 215
Quality of delta: ○ not set ○ excelent ○ very good ● good ○ fair ○ poor

Figure 1. Graphical user interface for ground truth data collection.



```
-------------------------------------------------------------
Width                   : 832 px
Height                  : 768 px
Fingerprint type        : R
Fingerprint quality     : 2
Fingerprint completeness: 1
Number of minutiae: 3
-------------------------------------------------------------
 id:  type,   x  ,   y  , angle, quality of minutiae
-------------------------------------------------------------
  0:     2,   527,   234,    81,   90
  1:     1,   452,   358,   104,   70
  2:     0,   360,   170,   187,   10
Number of cores    : 1
-------------------------------------------------------------------
 id:   x  ,   y  , quality of position, angle, quality of angle
-------------------------------------------------------------------
  0:   388,   165,                 90,   213,   70
Number of deltas   : 1
----------------------------------------------------------
 id:   x  ,   y  , angle, angle, angle, quality of delta
----------------------------------------------------------
  0:   342,   341,    66,   231,    66,   70
-------------------------------------------------------------
```

Figure 2. Example of a ground truth minutiae record (gtm-file).

3.4 Ground Truth Database and Relevant Data Fields

The data fields in table 1 are considered as relevant information for any conformance testing Level 3 methodology and thus are requested from the expert. His assessment for each field is eventually stored in a gtm-file. Each of the fields in table 1 is mandatory and must be attributed to some value[1].

3.5 Calibrating Fingerprint Sample Quality Algorithms

Several additional benefits can be achieved with generated ground truth data. For many large scale applications such as the European Biometric Matching System (BMS) the assessment of fingerprint images being accepted by the system interfaces seems to be one of the most crucial factors and success criteria. In order to maintain acceptability of the biometric system both among system operators and biometric capture subjects a biometric sample should only then being rejected, if its associated quality score is below a predefined threshold [2][1]. Nowadays algorithms that create a quality score have demonstrated that such score values are correlated with genuine comparison scores and that the quality score can be considered as prediction of a successful processing of biometric image data. However studies on this matter such as the report of Fernandez et al. [1] have not yet shown that the quality score is also correlated to the signal quality assessment of an experienced human inspector. With the ground truth database as described in this paper the correlation of human sample quality assessment with automated sample quality assessment can be determined.

4 Testing Methodology

Conformance testing on various levels (1, 2, 3) and addressing various test types (A, B) is not associated with an equivalent effort. Moreover an intrinsic limitation of any conformance test is that the test can not be complete or perfect [6]. This results in the conclusion that it is only possible to $prove$ that a unit is non-conformant. Implicitly from the complement we can derive that a unit that has passed the conformance test (on the previous Level 1 and 2 as well as on the semantic level) is likely to be conformant to the base standard. In that line semantic conformance testing is primarily an $exclusive$ semantic gt-minutiae assertion test (gtm-test) with a resulting conformance rate above an expected threshold, which is defined as follows:

Exclusive gtm-test: An exclusive gt-minutiae assertion test is yielding a conformance rate cr_{gtm} as defined in Section 4.3 that is indicating the proportion of elements in the set of gt-minutiae for which a corresponding minutia exists [2] in the set of automatically generated minutiae (agm), such that values can be compared for each data field and differences can be measured.

An approximative measure of the proportion of true minutia missed by the automatic minutia extractor under test is given by $1 - cr_{gtm}$. Note that a unit that generates multiple false minutiae may well pass the exclusive gtm-assertion test. False minutia could occur i) outside the fingerprint area as indicated in figure 3, where they are caused by i.e. noise in the background or ii) inside the fingerprint area due to scars, dirt on the finger, skin diseases and bented skin.

However this semantic testing methodology does also contain an $inclusive$ semantic automatically generated

[1] It is possible that some images do not result in a data field for core or delta.

[2] The gtm-assertion requires the corresponding minutia to be in the vicinity.

Table 1. Relevant data fields for ground truth data collection. Data fields in *italics* are defined in correspondance to ISO 19794-2:2005 Clauses 7.4.2.1, 7.4.2.2, 7.4.2.3, 7.4.2.4, 7.5.3.1, 7.5.3.3, 7.5.3.4, 7.5.3.5, 7.5.3.7 and 7.5.3.8 respectively.

Data field	Description
Pattern type	1st Level classification according to the following Classification Codes: A = Arch; L = Left Loop; R = Right Loop; W = Whirl; U = Unknown.
Sample quality level	The level of difficulty to analyze the fingerprint is assessed as sample quality level according NFIQ[2] ranging from 1 "excellent", 2 "very good", 3 "good", 4 "fair" down to 5 "poor".
Sample completeness level	The level of completeness of the finger pattern.
Minutia type	The type can be ridge ending, ridge bifurcation or other (undetermined).
Minutia Position	The coordinates of the minutia (horizontal X and vertical Y).
Minutia Angle	Absolute angle of the minutia.
Minutia Quality	The quality figure for both position and angle.
Number of Cores	The number of core points represented.
Core Position	The coordinates of the core.
Core Position Quality	The quality (accuracy) figure.
Core Angle	The angle of the core is recorded.
Core Angle Quality	The quality (accuracy) figure.
Number of Deltas	The number of delta points represented.
Delta Position	The coordinates of the delta.
Delta Angle	The three angle attributes of the delta.
Delta Quality	The quality figure for both position and angle.

minutiae assertion test (agm-test) that is designed to asses the number of false minutiae, which is defined as:

Inclusive agm-test: An inclusive ag-minutiae assertion test is yielding a conformance rate cr_{agm} that is indicating the proportion of elements in the set of ag-minutiae[3] that are inside or at the borderline of the fingerprint area.

In this proposed methodology the conformance testing is conducted in three phases:

1. *Data sanitization*: None of the human experts will work without any errors. Thus in the first phase, outliers with respect to the average assessment among the expert group member must be identified.

2. *Threshold definition*: This phase will determine the tolerance bounds for potential dislocations of the minutia coordinates, differences in the minutia angle or differences in the minutia quality assessment.

3. *Attest semantic conformance*: This phase will verify, whether a unit under test is reaching a conformance rate and thus is operating within tolerances.

The first two phases are about data sanitization and threshold computation procedures and define tolerance parameters and thus the turning key for the conformance test. In the last phase the unit under test is tested with respect to the tolerances as defined in phase 2.

4.1 Computing gt-minutia (phase 1)

With a larger number of experts contributing to the gt-minutiae database a new challenge arises: The edited values in the minutia data fields are unlikely to be identical. In a first approach the gt-minutia coordinate, angles and assurance level will be computed as the mean expert placements[4]. In a more sophisticated manner the coherence of the expert placements will be investigated. This approach is currently under development

[3] Note that the set of ag-minutiae may or may not contain false minutiae.

[4] The variance of values can indicate trustworthiness of this gtm for further processing.

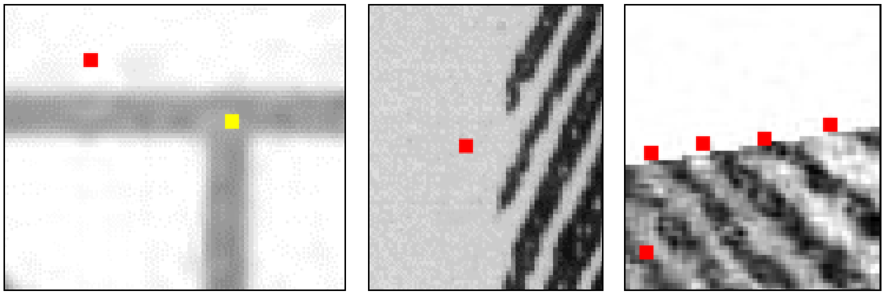


Figure 3. False minutiae at the edge of a ten-print card or at the border line of a fingerprint area. Minutiae are extracted with $mindtct$ from the NBIS-package[8].

4.2 Defining thresholds (phase 2)

In a straightforward approach the tolerance bounds for the distance between gtm and agm can be derived from the fingerprint frequency. Assume an agm has been identified in the agm-set as the closest neighbor to some gtm of interest then their distance d should be within the tolerance tol_d, which is given by

$$tol_d = \frac{W}{4} \tag{1}$$

where W is some global metric for the source fingerprint image and quantifies on average the shortest distance between the skeleton of one ridge line and the skeleton of the parallel ridge line. In a more sophisticated manner the quality level of the source (gtm or agm) could increase tol_d and thus allow a wider separation of mates in low quality image areas. Furthermore if the mates are assigned with different minutia types, then the tolerance d should also be increased.

Tolerances for minutia angle and quality differences are chosen as

$$tol_{\Delta\theta} = \frac{\pi}{4} \tag{2}$$

where $\Delta\theta$ is the difference among the mates with regard to the angle.

4.3 Attesting semantic conformance (phase 3)

The semantic conformance is attested based on an exclusive gtm-assertion test or inclusive agm-assertion test which verifies that an agm generated by the unit under test is within tolerances when compared to a gtm.

4.3.1 Exclusive gtm-assertion

The exclusive gtm-assertionspecifies the relevant metric cr_{gtm} as a gt-minutiae conformance rate, which is given by

$$cr_{gtm} = \frac{\sum_{i=1}^{ngtm} mcs_i}{ngtm} \tag{3}$$

where $ngtm$ is the number of elements in the gtm set and mcs_i is the minutia conformance score for the i-th gt-minutia that indicates the similarity between a gtm and the nearest minutia from the automatically generated minutiae set. The mcs is non-zero, if the distance d between the minutiae positions is within the tolerance bounds tol_d and the relevant data fields yield similar values.

The minutia conformance score mcs expresses the overall similarity of a minutia pair with regard to angle and minutia type:

$$mcs = \begin{cases} 0 & \text{if } d \geq tol_d \\ 1 - p & \text{otherwise} \end{cases} \tag{4}$$

where p is a potential "punishment" for an agm-minutia

$$p = p_{\Delta\theta} + p_{\Delta t} \tag{5}$$

regarding a dissimilarity in angle θ or minutia type t. Note that the field minutia quality q should be considered here but was intentionally omitted as there is no universally agreeable method on defining minutia quality yet.

The punishment $p_{\Delta\theta}$ is given by

$$p_{\Delta\theta} = \begin{cases} 0,5 & \text{if } |\theta_{gtm} - \theta_{agm}| \geq tol_{\Delta\theta} \\ 0 & \text{otherwise} \end{cases} \tag{6}$$

and the punishment p_t is given by

$$p_{\Delta t} = \begin{cases} 0,25 & \text{if } t_{gtm} \neq t_{agm} \\ 0 & \text{otherwise} \end{cases} \tag{7}$$

4.3.2 Inclusive agm-assertion

The inclusive agm-assertion specifies the metric cr_{agm} as an agm-conformance rate, which is given by

$$cr_{agm} = \frac{\sum_{i=1}^{nagm} mps_i}{nagm} \tag{8}$$

where $nagm$ is the number of elements in the agm set and mps_i is the minutia position score for the i-th ag-minutia that indicates the homogenious distribution of ag-minutia with respect to the fingerprint area. This metric will reflect a ”punishment” for those agm that are on the borderline or outside the fingerprint area according to:

$$mps = \begin{cases} 0 & \text{if } agm \text{ is outside the fingerprint area} \\ 0,5 & \text{if } agm \text{ is at the borderline} \\ 1 & \text{otherwise} \end{cases} \quad (9)$$

This assertion is an indicator for the number of false minutia in the automated generated minutia set and thus important for the conformance of the unit under test with the standard. This importance has been shown recently by the Minutiae Template Interoperability Testing (MTIT) Project as an increasing number of false minutia does degrade the interoperability performance [7].

5 Conclusion

The data collection described in this paper is composed to provide the missing ground for semantic fingerprint conformance testing. The overall database will be split in two separated fractions - a public one and a sequester fraction. It is intended that the mix between live scan (but roll) and plain (but inked) should be approx. the same in the public as in the sequester fraction.

The *public* fraction should contain approx. 30 percent of the total data and will be available in the public domain in order to be used by any interested body of the biometric community. Thus this fraction will be available to the industrial sector.

The *sequester* fraction should contain approx. 70 percent of the total data and will be provided under strong restriction to accredited testing institutions only, which are involved in conformance testing - be it in the academic sector or in the governmental sector. It is essential that the sequester fraction is never made available to stakeholders of the industrial sector in order to avoid that commercial algorithms are tuned to the data. In the mid-term perspective it is expected that ISO/IEC JTC1 SC37 will establish a testing lab accreditation process and procedures to authorize testing institution to receive a copy of the sequester database. The developed testing methodology verifies that the extracted feature data from some unit is in deed a faithful representation of the biometric characteristic. Initial experiments show that the proposed testing methodology and the suggested conformance rates are indicating the semantic conformance of a unit with respect to a test database. This assumption is currently validated with the composed ground truth database with the intent to develop a reliable test criteria for automated minutia extraction algorithms.

6 Acknowledgment

The authors would like to express their sincere appreciation for the expert teams at the National Institute of Standards and Technology that kindly provided the image material and at the AFIS department of the German Federal Criminal Police Office. Those experts devoted a significant share of their personal resources and made this work possible. Further thanks to Patrick Grother, Mike McCabe, Charles Wilson, John Campbell and Patrick Bours that provided valuable comments.

References

[1] F. Alonso-Fernandez, J. Fierrez, J. Ortega-Garcia, J. Gonzalez-Rodriguez, H. Fronthaler, K. Kollreider, and J.Bigun. A comparative study of fingerprint image-quality estimation methods. *IEEE Transactions on Information Forensics and Security*, 2(4):734–743, December 2007.

[2] M. Garris, E. Tabassi, and C. Wilson. Nist fingerprint evaluations and developments. *Proceedings of the IEEE*, 94(11):1915–1926, November 2006.

[3] ISO/IEC JTC1 SC37 Biometrics. *ISO/IEC 19794-2:2005 Information Technology - Biometric Data Interchange Formats - Part 2: Finger Minutiae Data*. International Organization for Standardization, June 2005.

[4] ISO/IEC JTC1 SC37 Biometrics. *ISO/IEC 19794-2:2005 Information Technology - Biometric Data Interchange Formats - Part 2: Finger Minutiae Data - Technical Corrigendum 1*. International Organization for Standardization, Jan. 2008.

[5] ISO/IEC JTC1 SC37 Biometrics. *ISO/IEC FCD 29109-2 Information Technology - Conformance Testing Methodology for Biometric Interchange Formats defined in ISO/IEC 19794 – Part 2: Finger Minutiae Data*. International Organization for Standardization, Feb. 2009.

[6] ISO/IEC JTC1 SC37 Biometrics. *ISO/IEC FDIS 29109-1 Information Technology - Conformance Testing Methodology for Biometric Interchange Formats defined in ISO/IEC 19794 – Part 1: Generalized Conformance Testing Methodology*. International Organization for Standardization, Feb. 2009.

[7] MTIT Consortium. Minutia Template Interoperaility Testing (MTIT). STREP Project funded by the European Commission, June 2007. Last visited: January 14, 2009.

[8] NIST. Nist biometric image software (nbis).