VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
ÚSTAV INTELIGENTNÍCH SYSTÉMŮ

FACULTY OF INFORMATION TECHNOLOGY
DEPARTMENT OF INTELLIGENT SYSTEMS

SECURITY OF BIOMETRIC SYSTEMS

DISERTAČNÍ PRÁCE
PHD THESIS

AUTOR PRÁCE Ing. DANA LODROVÁ
AUTHOR

BRNO 2012

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
ÚSTAV INTELIGENTNÍCH SYSTÉMŮ

FACULTY OF INFORMATION TECHNOLOGY
DEPARTMENT OF INTELLIGENT SYSTEMS

BEZPEČNOST BIOMETRICKÝCH SYSTÉMŮ

SECURITY OF BIOMETRIC SYSTEMS

DISERTAČNÍ PRÁCE
PHD THESIS

AUTOR PRÁCE — Ing. DANA LODROVÁ
AUTHOR

VEDOUCÍ PRÁCE — Doc. Ing. MARTIN DRAHANSKÝ, Ph.D.
SUPERVISOR

BRNO 2012

Abstract

The main contributions of this thesis are two novel approaches for the increase of securing of biometric systems based on fingerprint recognition. The first approach is within the liveness detection and prevents the use of various fake fingers and other spoofing techniques during the capturing processes. This patented approach is based on a combination of change of papillary line color and width caused by pressing of a finger against glass plate. The resultant liveness detection unit can be integrated into an optical fingerprint sensor.
The second approach is within standardization and it increases the security and interoperability of minutiae extraction and comparison process. For this purposes, I have created the methodology to determine semantic conformance rates of minutiae extractors. The minutiae extracted by the tested extractors are compared against Ground-Truth-Minutiae obtained by clustering of data provided by dactyloscopic/forensic experts. This proposed methodology is included in the ISO/IEC 29109-2 Amd. 2 WD4.

Keywords

Biometrics, biometric system, fingerprint, sensor, security, liveness detection, fake finger detection, color and elasticity of fingers, semantic conformance testing, finger minutiae data, interoperability, standardization, Ground truth database.

Citation

Dana Lodrová: Security of biometric systems, PhD thesis, Brno, BUT FIT, 2012

Abstrakt

Hlavním přínosem této práce jsou dva nové přístupy pro zvýšení bezpečnosti biometrických systémů založených na rozpoznávání podle otisků prstů. První přístup je z oblasti testování živosti a znemožňuje použití různých typů falešných otisků prstů a jiných metod oklamání senzoru v průběhu procesu snímání otisků. Tento patentovaný přístup je založen na změně barvy a šířky papilárních linií vlivem přitlačení prstu na skleněný podklad. Výsledná jednotka pro testování živosti může být integrována do optických senzorů.

Druhý přístup je z oblasti standardizace a zvyšuje bezpečnost a interoperabilitu procesů extrakce markantů a porovnání. Pro tyto účely jsem vytvořila metodologii, která stanovuje míry sémantické shody pro extraktory markantů otisků prstů. Markanty nalezené testovanými extraktory jsou porovnávány oproti Ground-Truth markantům získaným pomocí shlukování dat poskytnutých daktyloskopickými experty. Tato navrhovaná metodologie je zahrnuta v navrhovaném dodatku k normě ISO/IEC 29109-2 (Amd. 2 WD4).

Klíčová slova

Biometrie, biometrický systém, otisk prstu, senzor, bezpečnost, detekce živosti, detekce falešných prstů, barva a elasticita prstů, sémantické testování shody, data markantů otisků prstů, interoperabilita, standardizace, databáze Ground truth.

Citace

Dana Lodrová: Bezpečnost biometrických systémů, disertační práce, Brno, FIT VUT v Brně, 2012

Security of biometric systems

Declaration

I hereby declare that this thesis is my genuine work, created under the guidance of my supervisors Prof. Christoph Busch, Assoc. Prof. Martin Drahanský, and Assoc. Prof. František Zbořil, CSc. (named in the alphabetical order). Further information was provided by Elham Tabassi (NIST). All information sources and publications used are properly cited.

....
Dana Lodrová
December 11, 2012

Acknowledgment

I would like to thank my supervisors Prof. Christoph Busch, Assoc. Prof. Martin Drahanský, and Assoc. Prof. František Zbořil, CSc. (named in the alphabetical order) for their guidance and valuable comments to my research work. I also would like to thank my friends and my colleagues at Brno University of Technology, Gjøvik University College and ISO/IEC JTC1/SC37 WG3 for their support. I would like to thank all volunteers, whose fingerprints have been tested, for their help and patience. Especially I would like to thank Ing. Michal Hradiš (for lending of camera for liveness detection) and dactyloscopic/forensic experts from Bundeskriminalamt in Germany (minutiae extraction), because they make my work possible.
This work has been partially supported by:

- **Biometric Authentication Systems based on Biometric Template Protection Schemes**, BioKeyS-Pilot-DB, BSI, 2010-2011.
- **Education of liveness testing in subject Biometric systems**, FRVŠ MŠMT, FR2525/ 2009 /G1, 2009.
- **Ground Truth Database for Finger Minutiae Data**, BKA, GTD, 2008-2013.
- **Information Technology in Biomedical Engineering**, GAČR, GD102/09/H083, 2009-2012.
- **TeamIT - Building Competitive Research Teams in IT**, MŠMT, CZ.1.07/2.3.00/ 09.0067, 2009-2012.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

Nowadays, there are increasing security needs influencing many parts of human life. The passports usually contain biometric data (e.g., fingerprints and face), frequent flyers can be identified using iris recognition, swipe fingerprint sensors are usually integrated into common laptops, etc. There are various biometric characteristics, which are/can be used as a biometric identifier, but the biggest market share belongs to various systems based on fingerprint recognition.

Nevertheless, the expansion of fingerprint recognition and the familiarity of people with this technology caused, that the fingerprints (and fingerprint sensors) are probably the most attacked biometric characteristic. There are a lot of studies of possible attacks on various fingerprint sensor technologies or description of weak places in the whole biometric system [3, 11, 43, 45, 58, 67] and there are also several published cases of attacks on systems based on fingerprint recognition (e.g., attempt to spoof pension dispensing system in South Africa [70] or a successful attack of South Korean woman to Japanese immigration screening [62]).

These analysis and described attacks show us the vulnerable places of biometric systems and the necessity of creation and functional implementation of new and more efficient method/technique of securing of biometric system. Therefore, the **objectives of this Ph.D thesis** were set as follows:

- Study of theories of biometric security systems.
- Design of a new way to protect biometric system according to the studied theories.
- Implementation of the proposed system.
- Experiments, results evaluation and proposal for further research.

The thesis is organized as follows. The Chapter 2 contains the theoretical introduction to the topic of biometric system and fingerprints. Because of the large amount of theory in these topics, only the parts needed as a theoretical background for the following chapters are described.

The Chapter 3 describes the security of biometric systems in general. There is the detailed overview of weak places of biometric systems together with the description of possible attacks and securing. This chapter contains description of spoofing and anti-spoofing possibilities, the software security of components of biometric system and communication channels, together with the securing of hardware (which is often neglected topic). This chapter also contains a short description of my contribution to the multi-modal biometrics

– proposal of a finger vein sensor, which could be integrated into an optical fingerprint sensor.

The Chapter 4 starts with the description of published methods of liveness detection together with their advantages and disadvantages. Later in this chapter, my new patented method of liveness detection is presented. At the end of this chapter, the results of detailed tests and proposals for the future research are presented.

The Chapter 5 describes my new methodology for semantic conformance testing for finger minutiae data, which was proposed to the oncoming Amendment No. 1 to the ISO/IEC[1] 29109-2 standard. This methodology has been developed to increase security and interoperability of fingerprint templates. At the end of this chapter, the description of tests and the influence of various parameters are discussed.

The last chapter is the conclusion. It contains the brief summary of my work/thesis and the proposal for the future work.

Moreover, this thesis contains several appendices. The first appendix contains example of Czech and US dactyloscopic/fingerprint card. Then there is the brief description of the process of standardization and the summary of the minutiae record format from ISO/IEC 19794-2:2005 standard, which is important for the topic of my thesis. The following appendix contains the description and screenshots of the program for the liveness detection used for the purposes of the proof-of-concept tests. The examples of used fake fingers are in the fifth appendix and the additional results of liveness detection are in the next appendix. The last two appendices present the structure of GTD[2] database and additional test results for the semantic conformance testing. The list of publications, research and teaching activities during my PhD study is attached in the pocket of hardcover.

[1] International Organization for Standardization/International Electrotechnical Commission.

[2] Ground Truth Database.

Chapter 2

Biometrics and fingerprints

At the beginning of this thesis, it is necessary to describe the operation of a biometric system and its individual parts as well as the differences among the most used biometric characteristic. Because every biometric characteristic has its specifics and requires unique approach, it is not possible to work on security of a biometric system in general. Therefore, I have to choose one of them. I chose fingerprints due to reasons given in Section 2.3. The detailed description of fingerprints and standardization can be found at the end of this chapter.

2.1 Biometric system

At first, it is necessary to describe the common biometric system, its schema and the function and the purpose of each component. Then the typical use-cases of biometric system have to be discussed, because each use-case has its specific advantages, disadvantages and ways of deployment.

2.1.1 Components

The common biometric system consists of five components: sensor (capture device), extractor (sometimes called extraction unit), comparator (or comparison unit), database and application (see Fig. 2.1) [30, 35, 43, 103, 104]. Sometimes the application is not included in the biometric system. However, I think that the application should be included in the biometric system from the security point of view. The communication channel to the application and the application itself have to be well secured because there is one of the major weak places and the inclusion of the application in the biometric system expresses the necessity of securing of these parts.

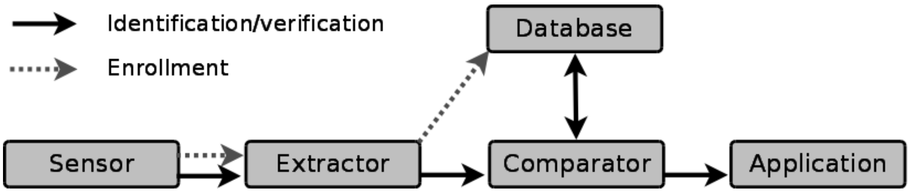


Figure 2.1: Schema of the enrollment and identification/verification process in the biometric system.

The biometric system is commonly used in three different modes. The first of them is an enrollment mode. This mode is used to an enrollment of applicants. In this case, the process/interconnection of components is a little bit different as in other two cases (see Fig. 2.1). The second mode is an identification mode. In this case, the captured biometric sample is processed and compared to all biometric references in the database. The third mode is a verification mode, where the captured sample is compared to the only one reference selected according to the identity claim. The description of behavior of each component during each mode follows [30, 35, 43, 103, 104]:

1. **Sensor/Capture device.** According to the general definition [130], sensor „measures the physical quantity" (in case of biometric system the biometric characteristic as fingerprint or voice) „and converts it into a signal" (e.g., image of fingerprint or audio record of voice). Thereafter, the captured sample (signal) of the biometric characteristic is sent to the extractor module.

   This part of biometric system can be also called a biometric capture device [104] and is defined as „device that collects a signal from a biometric characteristic and converts it to a captured biometric sample" [104]. In this case, the biometric capture device is understood to consist of one or more biometric sensors, possible illumination sources, etc.

2. **Extractor.** The extractor finds the characteristic points of input samples (e.g. minutiae in case of fingerprints). For this purpose, the input signal is usually pre-processed by several filters to noise reduction and to achieve better signal quality (so called intermediate biometric sample processing).

   Another part of the extractor module could be also the quality control. If the signal quality is not sufficient (according to the predefined threshold), the biometric sample is removed and the capture subject is asked to use the sensor again.

   If the system is in the enrollment phase, the extracted features are used to the creation of a reference, which will be stored in the database module. In case of the identification/verification phase, the extracted features are sent to the comparator module.

3. **Comparator.** In case of the identification process, this module takes the input set of features and compares it with the references of all enrollee stored in the database. It finds the enrollee with the highest comparison score (or the list of candidates with highest comparison scores). If the found score is above the predefined threshold, the output will be the ID of the found candidate; otherwise the output will be „not identified".

   The verification process is similar. The extracted features are compared with the template of the claimant and the result is a positive or negative claim of the specific identity (according to the threshold).

4. **Database.** The database module stores the references (biometric templates, samples or models) and other necessary information (e.g., ID or name) about enrollees.

5. **Application.** At the end of biometric system, there is the secured application itself. It can be the entrance door to the secured area, attendance system or another thing. It is necessary to link the application and the rest of biometric system wisely; otherwise

the attacker could circumvent other components of the biometric system and attack the application itself. In such case, the usage of biometric system would be futile.

2.1.2 Usage of biometric system

The biometric system is used for a lot of different purposes, e.g., for device access control, the attendance system or the physical access control. Every specific usage of the biometric system requires different approach for the physical placement of individual components and also different security requirements. In principle, we can find six different approaches to component placements [43]:

1. The first possibility is to have all components in one piece of equipment. This approach is called „System-on-Device“ (SoD) in case that all components are integrated in the biometric reader, which has a fixed location. The example of this approach could be the stand-alone touchless terminal TBSGuard 3D-Terminal from Touchless Biometric Systems AG [124].

   Similar approach is the placement of all components on the equipment, which is in the possession of the enrollee. This approach is called „System-on-Card“ or „System-on-a-Chip“ (SoC). The example of this approach could be the personal biometric token from Privaris, Inc. [115] (see Fig. a).

   These approaches are easy to implement in system without user management, but it is also possible to use them in case with necessity of proper central user management. In such case, the central database of enrollees does not contain the fingerprint templates but cryptographic keys.

2. The second possibility is the exclusion of the database module. The database of biometric samples could be located on a server or on the card (token). In case of database on server, the biometric reader often has its own copy of database and regularly synchronizes them. The example of this approach could be the Handkey II terminal from Ingersoll Rand Corp. (formerly IR Security & Safety Limited) [92].

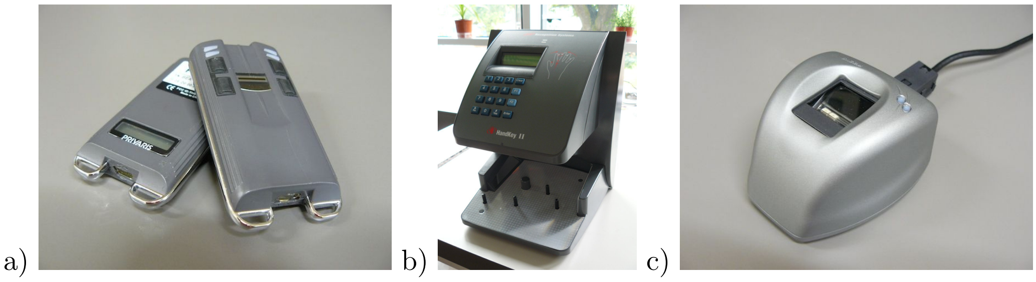


Figure 2.2: Examples of different usage of biometric system: a) System-on-Device (PlusID 90 from Privaris, Inc.), b) exclusion of Database module (Handkey II from Ingersoll Rand Corp.), c) separated sensor (Sagem MS0 300 from Morpho, Safran group).

3. The third approach is so called „Match-on-Card“ (MoC) [43] or On-Card-Comparison (OCC) [98]. In this case, the comparator and the database are located on some kind of a smart card. The example of this approach could be the Precise 250 MC system from Precise Biometrics, AB. [114]. This approach has often a problem with the insufficient memory size and also the implementation of comparison algorithm under constrained

resources of smart card is a challenge (e.g., alignment of fingerprints is very complex problem).

4. The fourth possibility is to combine the sensor and the extractor module in the biometric reader. The example of this approach could be the IrisPass terminal from OKI Electric Industry Co., Ltd. [109].

5. In the fifth approach, the sensor is separated and all the other components are included in one facility (probably PC or server). Typical usage of this approach is the common USB[1] sensor connected to the PC and used as a common access control system. The example of this approach could be the MorphoSmart (TM) USB fingerprint sensor from Sagem Morpho, Inc. [116] (see Fig. 2.2 c).

6. The last approach is very similar to the previous one. It is the combination of the extractor and the comparator module on one place and separation of database module. Typical usage of this approach is the USB biometric sensor connected to the PC (extractor and comparator) connected to the server (or other location of database).

2.2 Biometric characteristics

As it is mentioned earlier in this thesis, there are a lot of used biometric characteristics, e.g., fingerprint, iris, retina, finger veins and many others. On the human body, there can be found a lot of promising areas, which are currently not used as the biometric characteristic. This is because these properties do not meet the requirements to be the biometric identifier.

2.2.1 Requirements

Every biometric characteristic has to meet a lot of requirements/conditions. These requirements ensure that this biometric characteristic can be used in the real-world scenario; they reflect the demands on the sensor and the whole biometric system, the attitude of capture subjects, the robustness of biometric characteristic, etc. Usually, the requirements are divided in the following seven categories [30, 43]:

1. **Universality.** Everybody has to have this biometric characteristic, so its presence has to be independent on gender, age, race, etc.

2. **Distinctiveness.** Any two persons should be distinguished on the basis of this biometric characteristic.

3. **Permanence.** The used biometric characteristic has to be sufficiently invariant over the period of time.

4. **Collectability.** It has to exist some method for measuring this property by the help of present hardware equipment.

5. **Performance.** This requirement contains properties such as accuracy, speed, costs and possibilities of hardware and software application.

6. **Acceptability.** Capture subjects have to be willing to undergo measuring/collecting of this biometric characteristic (e.g., testing has to be noninvasive).

[1] Universal Serial Bus.

7. **Security.** It has to be difficult to spoof a sensor based on capturing of this biometric characteristic - to produce an artificial biometric characteristic.

2.2.2 Commonly used characteristics

The most often used biometric characteristics has been compared according to how much they meet the requirements described in the previous subsection. The compliance rate was described only simplified as High (H), Medium (M) or Low (L) (see Tab. 2.1).

Table 2.1: Overview of biometric characteristics according to the requirements described in Section 2.2.1. High, Medium and Low rates are denoted by H, M, and L, respectively [43].

	Universality	Distinctiveness	Permanence	Collectability	Performance	Acceptability	Security
Fingerprint	M	H	H	M	H	M	M
Iris	H	H	H	M	H	L	H
Retina	H	H	M	L	H	L	H
Thermoface	H	H	L	H	M	H	H
Veins	M	M	M	M	M	M	H
2D Hand-geometry	M	M	M	H	M	M	M
Face	H	L	M	H	L	H	L
Signature	L	L	L	H	L	H	L
Voice	M	L	L	M	L	H	L

Comparison of individual characteristics shows that a lot of characteristics have very unbalanced results and/or achieve poor results many times. In contrast, fingerprint has balanced results and does not reach poor results according to any requirement.

2.3 Fingerprints

Fingerprints are the most used biometric characteristic on the market of biometric sensors. In 2009, the technologies based on fingerprint capturing had 67 percent market share [84]. Fingerprints are among the biometric characteristics that best meet the previously described requirements.

Fingerprints of a child are fully formed approximately at seventh month of pregnancy [43]. The fingerprint can be defined as a pattern created by a papillary lines structure. Papillary lines are approx. 0.2–0.5 mm wide and approx. 0.1–0.4 mm high [20], so they are composed of ridges and valleys (sometimes called furrows).

The fingerprint identification is based on several fundamental rules (so-called biological principles of fingerprints [43] or dactyloscopic laws [20]):

- Every two fingerprints captured from different fingers have different ridge structure.
- The papillary line patterns are relatively unchanged during lifetime. The possible small changes are within the limits for systematic classification.

- The configuration and minutiae are permanent and unchanging.
- The papillary lines are permanently irremovable, unless the upper layer of dermis is not removed/damaged.

2.3.1 Fingerprint types and classes

The fingerprint analysis is necessary to begin by identifying the type of fingerprint. Each type of fingerprint has to be treated differently, because each type represents different group of problems to deal with.

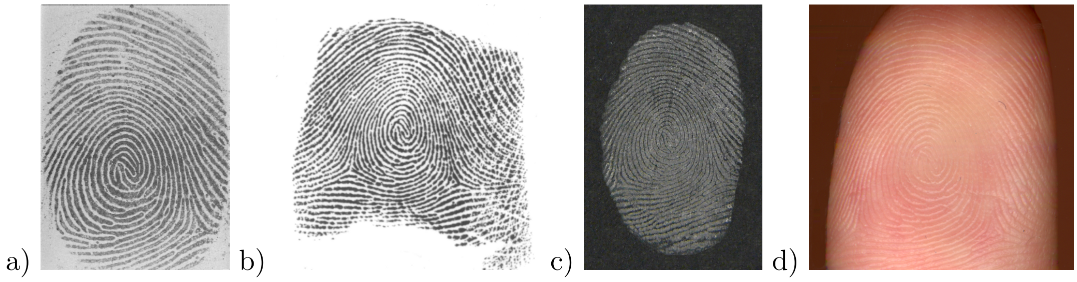


Figure 2.3: Examples of different types of impression of the same finger: a) live-scan plain, b) off-line rolled, c) latent, and d) photo/scan of corresponding fingertip (for comparison).

There are five possible types and combination of types of fingerprints (live plain, live rolled, off-line plain, off-line rolled, and latent). The description of these types is following [30, 35, 43]:

Plain. Sometimes also called flat, slapped or dab fingerprint. In this case, the finger touches the surface of the pad (e.g., sensor or dactyloscopic card) but is not rolled on it (see Fig. 2.3 a).

Rolled. Sometimes also called unwrapped fingerprint. To obtain this type of fingerprint, it is needed to roll a finger nail-to-nail on the pad (see Fig. 2.3 b). It is necessary to roll the finger only once (no scroll back), to have clean fingers without any dirt, and do not press finger strongly on the paper, otherwise the resultant impressions will be blurred and useless. This type of impression is mostly obtained off-line, but there are several fingerprint sensors with the ability to scan rolled fingerprints. In comparison with the plain fingerprint, the mutual position of important points (minutiae) is slightly deformed.

Live. Sometimes also called live-scan fingerprint. This type of fingerprint is obtained by the fingerprint scanner or other electronic device (see Fig. 2.3 a). Mostly, it is a plain impression, but there are several fingerprint sensors with the ability to scan the rolled fingerprint.

Off-line. Sometimes also called inked fingerprint (see Fig. 2.3 b). These fingerprints can be plain or rolled. Generally, the capturing of off-line impressions has always two phases: creation of a fingerprint and scanning of a fingerprint to the PC/database. Mostly, the off-line impressions are obtained by scanning of dactyloscopic card (for more details see Appendix A).

Latent. In comparison with the previous four types of fingerprints, this fingerprint is unintentionally left, e.g., on surface of object of daily use (see Fig. 2.3 c). Sometimes, it is included as a special case of the off-line fingerprints because of the two-phases processing. On the other hand, the first phase does not consist of creation of fingerprint, but it consists of finding and visualization of fingerprint. Therefore, these fingerprints are mostly presented separately.

Consequently, the fingerprints can be divided into several categories/classes according to their appearance. The first attempt to classify fingerprints was made by Jan Evangelista Purkyně in 1823 [43, 20]. He divided the fingerprints into nine classes: transverse curve, central longitudial stria, oblique stripe, oblique loop, almond whorl, spiral whorl, ellipse, circle, and double whorl. His work was followed by Francis Galton, Juan Vucetich and many others, who have created a lot of similar or different classification systems. Nowadays, the probably most used classification is the Galton-Henry classification system: arch, tented arch, left loop, right loop, and whorl (see Fig. 2.4).

For the purposes of facilitation of the classification process, two different singular points are used. The first one is a core. It is a center point, which can be defined as „the north most point of the innermost recurving ridge line“ [97]. In case of problems, the core can be also detected as „the point of maximum ridge line curvature“ [43]. The core is often marked as a green circle or a circle (see Fig. 2.4).

The second singular point is called delta. It can be defined as „a point on a ridge at or nearest to the point of divergence of two type lines, and located at or directly in front of the point of divergence“ [97]. The delta is often marked as a red triangle or a triangle (see Fig. 2.4).

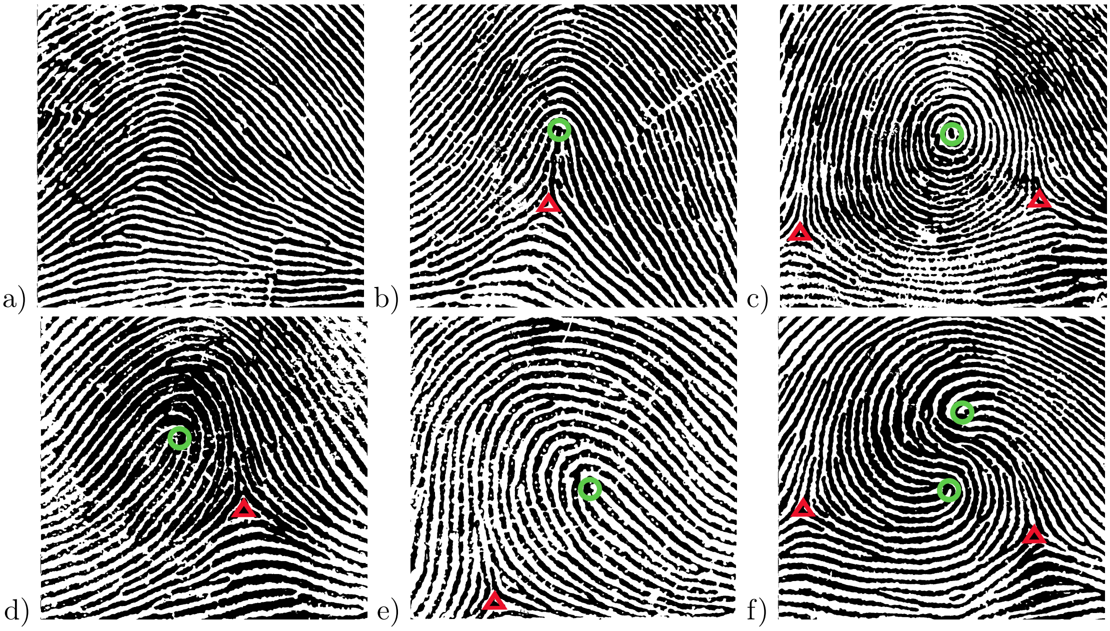


Figure 2.4: Examples of different classes of fingerprints [121]: a) arch, b) tented arch, c) whorl (plain whorl), d) left loop, e) right loop, and f) whorl (twin loop). The approximate positions of cores are marked by a green circle and the approximate positions of deltas are marked by a red triangle.

The Galton-Henry classification scheme with cores and deltas (see Fig. 2.4) can be described as follows [43]:

Arch. Sometimes it is called plain arch. This pattern contains the smallest changes in the ridge flow of all patterns (see Fig. 2.4 a). It contains neither core nor delta.

Tented arch. The tented arch is very similar to the plain arch - the difference is the central ridge(s), which causes a high ridge line curvature (see Fig. 2.4 b). This pattern contains one core and one delta situated under the core in the middle of the fingerprint. Sometimes the both classes (plain arch and tented arch) are merged into one: arch (A).

Left loop. Fingerprint belonging to this category contains one papillary line, which starts on the left side, continues to the center and returns back to the left side of fingerprint (see Fig. 2.4 d). This pattern mostly contains one core and one delta situated in the bottom-right part of fingerprint.

Right loop. The right loop is reversed in comparison with the left loop (see Fig. 2.4 e). Sometimes, both classes (left loop and right loop) are merged into one: loop (L). In some cases, classification on the left and right loop is replaced by the classification on the ulnar and radial loop. The loop starting on the thumb-side of finger is called radial loop by the bone called radius. The ulnar loop starts on the index finger-side of finger and it is called by the ulna bone. Nevertheless, the usage of this classification is limited, because often it is not possible to determine, whether the fingerprint belongs to the left hand or the right hand.

Whorl. The whorl (sometimes called whirl) pattern is the most complex pattern. It consists of at least one core and at least two deltas. Some classification systems distinguish among several different types of whorls, e.g., plain whorl (contains the central circle - see Fig. 2.4 c), twin or double loop (contains two loops twisted into one whorl - see Fig. 2.4 f), right/left pocket loop (similar to the loop, but there is another delta and circle/spiral [121]), accidental (e.g., containing two cores and three deltas [121]), etc.

As it was mentioned before, there are several different classification schemes. The probably simplest one divides fingerprints in only three classes: arch, loop and whorl. The most comprehensive systems distinguish, e.g., among several sub-patterns of whorl, so they can consist of ten or more classes in total.

2.3.2 Minutiae-based model

Although the classification of fingerprints to the different types of impressions and ridge patterns is important, it is not sufficient enough to enable reliable identification. For this purpose, it is necessary to use other fingerprint properties. One of them is the minutiae-based model, which will be discussed in this subsection. This model is probably the most used and most proved of all and also this model will be used in this work. Other models are not so important for this thesis, so they will be just briefly discussed at the end of this subsection.

The minutiae are the places of small changes of the ridge flow (e.g., ridge endings or bifurcations). Minutia can be defined as „point where a single friction ridge deviates from an uninterrupted flow“ [97].

In total, four minutia attributes are recorded: type t, position (x- and y-coordinates), orientation (θ), and quality q. Generally the minutiae M in a template T can be described as follows:

$$T = \{M_1, M_2, .., M_n\} \tag{2.1}$$
$$M_i = (t_i, x_i, y_i, \theta_i, q_i) \tag{2.2}$$

Unfortunately, several different approaches to detect and distinguish minutia type are used in practice. All systems (that I have ever seen) contained the minutiae types „ending“ and „bifurcation“, but other types were different (the examples of used types can be found in Fig. 2.5). According to my experience, even the dactyloscopic experts in different countries use different classification systems, e.g., German minutia „Insel“ (island) is called lake in English and English minutia called „island“ is called „Punkt“ (point) in German. Therefore, the possible international cooperation is necessary to begin by creating a dictionary/knowledge base (see Chapter 5.2.3).

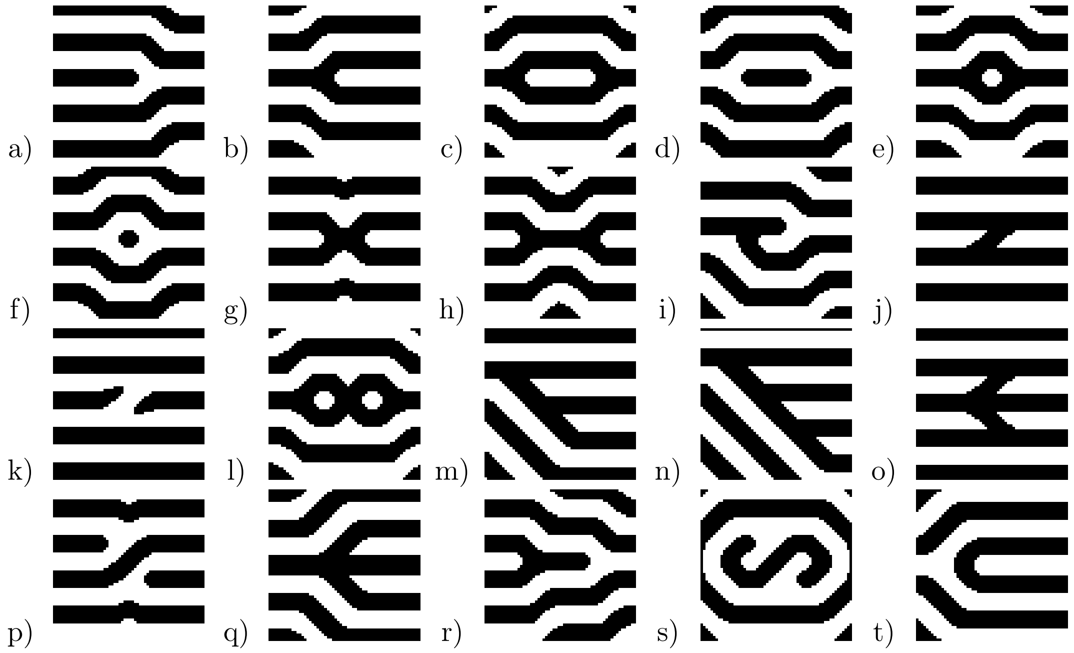


Figure 2.5: Examples of different minutiae types [14, 43, 64, 133]: a) ridge ending, b) ridge bifurcation, c) lake/enclosure/„Insel“ (island), d) interval/island/short ridge/independent ridge/„eingelagerte Linie“ (embedded line), e) simple whorl/„Auge“ (eye), f) point/island/dot, g) crossover/ridge crossing/x-line, h) opposed bifurcation, i) hook/spur, j) bridge/simple bridge/„Linienverästelung“ (branching lines), k) side contact/„ausweichende Endstücke“ (evasive endings), l) twofold whorl, m) twofold ridge bifurcation/double ridge bifurcation, n) threefold ridge bifurcation, o) twofold bridge, p) continuous line, q) trifurcation, r) opposed bifurcation-ending, s) „Sonderheit“ (special feature), and t) „eingelagerte Schleife“ (embedded loop). The ridges are drawn in black and furrows/valleys in white. The German names of minutiae types are listed only if they are semantically different from the English names.

Even the standards have different methodology. The American National Standards Institute (ANSI) uses the system of four types: ending (type A), bifurcation (type B), compound (crossover, trifurcation, etc. - type C), and undetermined (type D) [76]. On the other hand, the International Organization for Standardization (ISO) uses only three fingerprint types: ending, bifurcation and other, because it claims, that all different types can be disassembled to these basic types [97]. The ISO/IEC 19794-2:2005 standard [97] is used in this work and its detailed description is given in Chapter 2.4.1.

The second minutiae attribute is a position. It is recorded as x-coordinate and y-coordinate. According to my experience, there are different coordinate systems mostly based on the ISO coordinate system (axis in pixels, origin at the upper-left corner of image - see Chapter 2.4.1).

The third minutia attribute is the orientation θ. Usually the angle is measured counter-clockwise from the horizontal axis to the right. However, there is different approach [20], which defines the minutiae angle exactly the opposite way, so the angle of minutiae is increased (decreased) by 180 degrees.

The last recorded minutia attribute is the quality. It is also the most problematic attribute. Nowadays, there is no international standard defining how to determine the minutiae quality[2]. In case of work of dactyloscopic experts, the quality is sometimes defined as a percentage of certainty of expert about position, angle, type (and sometimes even the existence) of minutia.

The usage of minutiae differs in various countries not only in terms of usage of special types, but also in terms of required minutiae threshold for positive identification (see Tab. 2.2).

Table 2.2: Overview of required number of minutiae for positive identification in various countries [10].

Number of minutiae	Countries
8	Bulgaria
10	Spain, Netherlands, Hungary, Denmark
12	Germany, France, Czech Republic, Sweden, ...
14	Malta
16	Italy, Cyprus, Gibraltar

The automated processing and comparison of fingerprints is slightly different from the processing of fingerprints by dactyloscopic experts. The whole (but simplified) process has six phases. It begins with the caption of the fingerprint. The input image is enhanced by image filter(s) to reduce the noise. The fingerprint can also be segmented from the image background (if necessary). Then the orientation array is computed - the image is divided into small blocks and the orientation of papillary lines is computed in each of them. Later the papillary lines are extracted (mostly by the usage of Gabor filters). Then the extracted lines have to be thinned (omnidirectionally) down to one pixel width. After that, the extraction of minutiae is relatively simple: if the pixel has only one neighbor, it is the ridge ending, if it has three neighbors, it is the bifurcation; otherwise it is not the minutia. The illustration of the whole process can be found in Fig. 2.6.

The minutia-based model is not the only approach; other models have been described. Generally, they are based either on correlation of images or on non-minutiae feature extrac-

[2] Only three parts of ISO/IEC standard 29794 (Information technology – Biometric sample quality) has been published yet: Part 1 - Framework, Part 4 - Finger image data, and Part 5 - Face image data [95].

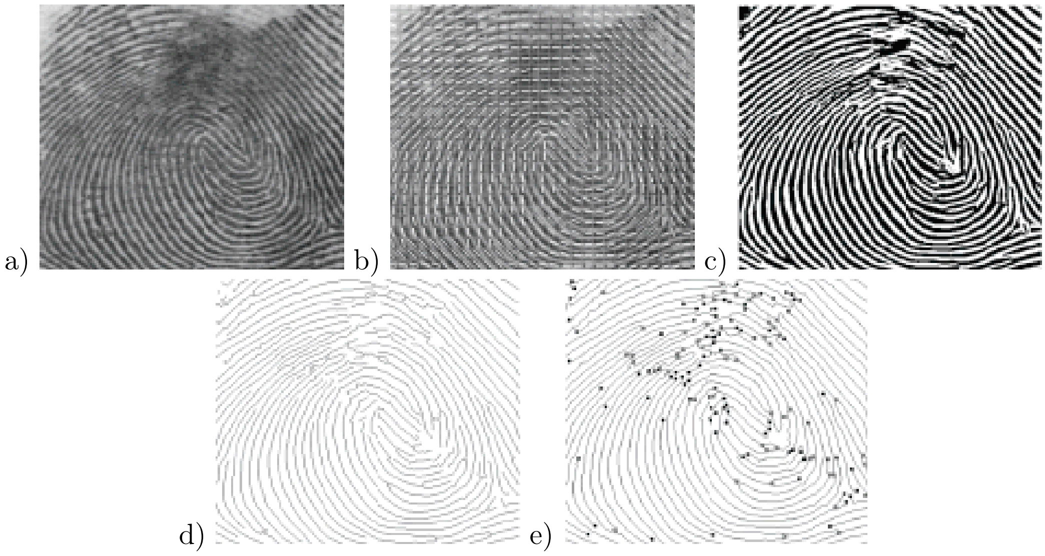


Figure 2.6: Example of fingerprint processing [14]: a) sensed and enhanced fingerprint, b) orientation array (mapped on fingerprint), c) papillary lines extraction, d) thinning, e) minutiae detection.

tion [43]. The correlation techniques are based on superimposement and correlation between fingerprint templates (e.g., [6]). The correlation techniques have to deal especially with the skin distortion [43], which makes every impression unique. The non-minutiae feature extraction based techniques use especially the sweat pores (e.g., combination of pores and ridge contour [29]), global and local texture information (e.g., ridge feature map [51]), etc. Nevertheless, the minutiae-based approach is still the most widely-used and most proved technique.

2.3.3 Fingerprint sensors

For the purposes of securing of a biometric (fingerprint) system, it is necessary to deeply understand the principles of fingerprint sensors, their advantages and disadvantages. There are two different approaches how to divide the sensors into different categories.

The first approach is to divide the sensors according to the usage [30, 35, 43].

1. **Touchless.** In this case, the finger of the capture subject is not in the contact with the sensor surface (see Fig. 2.7 a). The advantages of this type of sensor are the absence of latent fingerprint (which could be used for some type of attacks - see Section 3.2.1) and the more hygienic approach - better acceptance by the users. On the other hand, the problem could be the right focus and contrast of the captured image. In comparison with the plain fingerprint captured by touch sensors, the mutual position of important points (e.g., minutiae) is slightly deformed.

2. **Touch.** This sensor technology is the most used technology today. It requires the finger of the capture subject slightly pressed against the sensor surface (see Fig. 2.7 b). The advantage is the most user-friendly approach. The disadvantages are the latent fingerprints left on the sensor surface and (usually) the higher price in comparison with swipe fingerprint sensors.

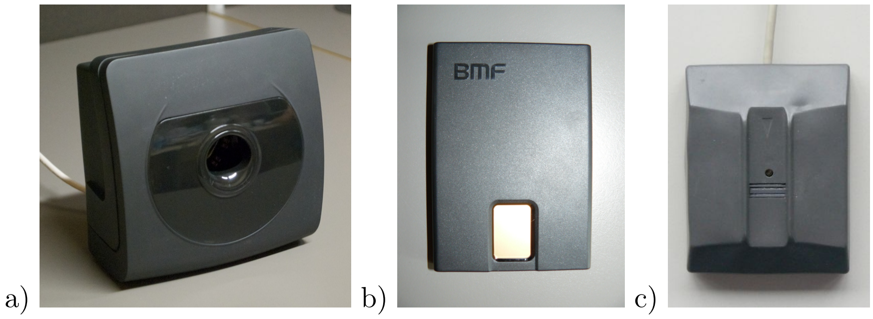


Figure 2.7: Examples of different types of fingerprint sensors: a) touchless sensor (optical direct reading sensor TBSGuard 3D-Enroll from Touchless Biometric Systems AG), b) touch sensor (pressure-sensitive sensor BMF EZF 650 from BMF Corp.), c) swipe sensor (thermal sensor Bergdata FCAT 100 from Bergdata Biometric GmbH).

3. **Swipe.** This type of sensor requires the swiping of the finger over the sensor unit (see Fig. 2.7 c). The advantage of this approach is the lower price and size of the sensor. On the other hand, the disadvantages are the problems with the image reconstruction (time-consuming and often not precise) and the most user-unfriendly and non-intuitive capturing.

The second approach is to divide the sensors by the used capturing technology [30, 35, 43].

1. **Optical.** This category of fingerprint sensors contains five technologies with optical-based capturing of fingerprints.

   (a) **FTIR.** Frustrated Total Internal Reflection (FTIR) is one of the oldest and the most common used sensor technology [43]. The acquired fingerprint image is gray scale or black-white, where dark (black) parts are fingerprint ridges and bright (white) parts are valleys (see Fig. 2.8 a).

   Principle of this technology is very easy. Finger is slightly pressed against glass plate-prism (sensors based on FTIR principle cannot be contactless) and illuminated through a glass prism by (a bank of) LED[3] diodes. Reflected light is focused through lens and captured by CCD[4] or CMOS[5] camera.

   For the purposes of miniaturization, the original glass prism can be replaced by a sheet prism (number of small prisms adjacent to each other [43]). The disadvantage of this approach is the lower quality of captured fingerprint.

   FTIR principle has often problems with dry or wet fingers. Manufacturers often try to avoid problems with dry fingers by applying conformal coating (i.e. silicon-based) to improve the optical contact.

   This type of sensors is produced, e.g., by Sagem Morpho, Inc. [116] or SecuGen Corp. [117].

   (b) **Optical fibers.** This type of sensor technology presents another approach to miniaturization. The finger is put on a fiber-optic platen and the CCD/CMOS sensor on the opposite part of the platen captures an emitted residual light.

[3] Light-Emitting Diode.

[4] Charge-Coupled Device.

[5] Complementary Metal Oxide Semiconductor.

    (c) **Direct reading.** Sensor based on direct reading principle uses the high-quality camera to take a picture of the finger directly. This approach is the only one optical sensor principle, which allows a touchless capturing of finger. This type of sensors is produced, e.g., by Touchless Biometric Systems AG [124].

    (d) **MSI.** Multispectral imaging technology (MSI) captures several images of a finger. Every image under different light conditions: different wavelengths, orientation and polarization of light. This technology is also capable to test liveness of the captured sample (see Section 4.1.1). This type of sensors is produced, e.g., by Lumidigm, Inc. [105].

    (e) **Electro-optical.** This type of sensor consists of two main layers. The first layer emits light in the areas of contact with papillary ridges. The second layer captures the emitted light. It is possible to use the standard lens and CMOS sensor for capturing of light, however (as mentioned before), this approach cannot be miniaturized. From this point of view, it is more suitable to use array of photodiodes. This type of sensors is produced, e.g., by Security First Corp. [118] (formerly Ethentica) or ELSYS Corp. (DELSY division) [88].

    A slightly modified electro-optical technology is used in the fingerprint sensors made by Integrated Biometrics, Inc. [94]. They use their patented LES[6] technology, which consists of multiple layers of fluorescent polymer film in combination with a new TFT[7] technology. Integrated Biometrics, Inc. also claims that this technology is able to detect liveness.

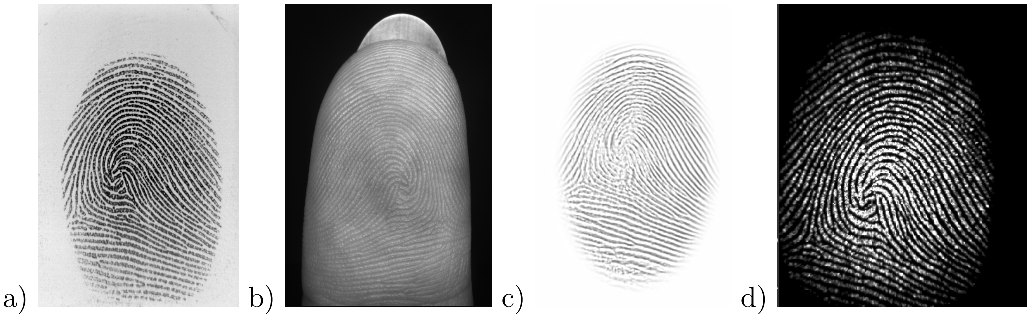


Figure 2.8: Example of same finger captured by a) FTIR (Biolink U-Match MB 3.5), b) direct reading (TBSGuard 3D-Enroll), c) MSI (Lumidigm Venus V100), and d) electro-optical sensor (Integrated Biometrics LES650).

2. **Solid-state.** These sensors (also known as silicon sensors) were designed to meet the market demands for size and price [43].

    (a) **Capacitive.** It is one of the most common types of sensors [43]. The surface of the sensor is created by the array of small plates covered with dielectric (e.g., silicon dioxide). Each plate has to be smaller than the width of papillary line (less than 0.2 mm). The papillary ridges of pressed finger create a „second plates“ of capacitors in the array. The resulting capacity of each capacitor in the array is directly proportional to the size of a papillary ridge over the plate. The disadvantage of this approach is the problem with wet and dry fingers and ease

[6] Light-Emitting Sensor.

[7] Thin Film Transistor.

to damage (mechanically or chemically) the sensor surface. Another problem is also the sensitivity to the electrostatic discharge (ESD), which can seriously damage the sensor. This type of sensors is produced, e.g., by Upek, Inc. [127] or Veridicom International, Inc. [128].

(b) **Thermal.** Thermal sensors are one of the most common used sensors today. This sensor technology exists only in the swipe version. The capture subject has to swipe its finger over a pyro–electric unit (with heating), which detects the finger surface on the basis of temperature differences between papillary ridges and valleys. The advantage of this type of sensor is the absence of latent fingerprint and the resistance to ESD, light flash or other type of interference. On the other hand, it is the most user-unfriendly approach, because the capture subject has to know how to swipe the finger over the pyro–electric unit - he/she has to be little bit handy. This type of sensors is produced, e.g., by Bergdata Biometrics GmbH. [81] or it is a part of common laptops. However, these final products are based on Atmel FingerChip from Atmel Corp. [77].

(c) **E-Field** (also known as RF[8] sensor or electric field sensor). This sensor technology uses a generator of sinusoidal RF signal and the matrix of active antennas to capture the signal modulated by epidermal layer of skin. For the correct functionality of sensor, the finger has to have good contact with both parts of the sensor (RF generator and antennas). The advantage of this technology is the ability to capture even the problematic fingers. On the other hand, the captured image is very small (often 128 × 128 px, 250 dpi). This type of sensors is produced, e.g., by AuthenTec, Inc. [78].

(d) **Pressure-sensitive.** Construction of pressure-sensitive technology allows two different approaches. The first of them is based on piezoelectric effect. The surface of sensor is covered by dielectric, which generates small electric current if the pressure is applied.

The second possibility is to cover the sensor by two conducting layers, between which is non-conducting gel. The pressure of the papillary ridges causes the displacing of non-conducting gel and contact of two conducting layers, which can be easily measured.

The advantage of this sensor technology is big sensor area and the ability to capture wet/dry/dirty fingers. However, this type of sensor has quite short operating lifetime and the problem could also be the black-white output (captured) fingerprint. This type of sensors is produced, e.g., by BMF, Corp. [85].

3. **Ultrasonic.** This type of sensor is created by a transmitter, which generates short ultrasound waves, and a receiver, which captures the reflected waves. The advantage of this sensor could be the possibility of capturing wet/dry/dirty fingers and finger through thin gloves. However, the disadvantage is the long capture time (a few seconds) and big and quite expensive sensor. This type of sensors is produced, e.g., by Optel Ltd. [112] or Ultra-Scan, Corp. [126].

[8] Radio Frequency.

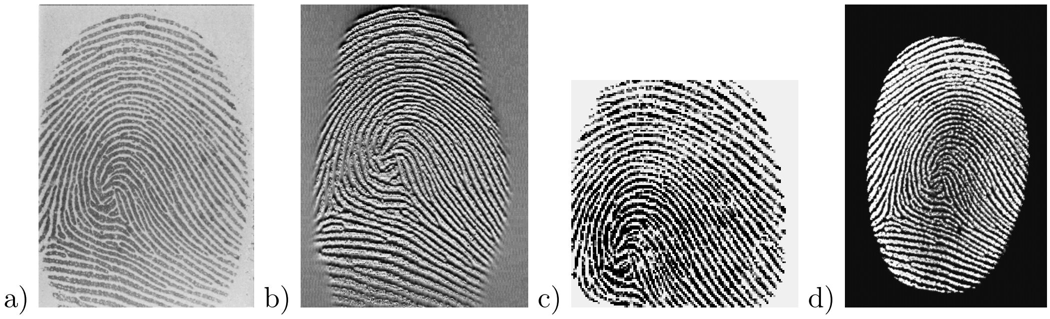


Figure 2.9: Example of a same finger captured by a) capacitive (Suprema SFM3050-TC1), b) thermal (Suprema SFM3010-FC), c) E-Field (Suprema SFM3000-FL), and d) piezoelectric sensor (BMF EZF 650).

2.3.4 Problematic fingers/fingerprints

Various fingerprint sensors, types of impressions and other situations (e.g., diseases) can cause problems with processing of fingerprints. The previous chapter contains eight examples captured by different fingerprint sensor technologies. All eight fingerprints are impressions of the same clean and healthy finger for the easier comparison. Every of these images has different combination of background color, ridge color and distribution of ridge thickness/quality. Various types of impression (see Fig. 2.3) increase the set of possible problems. Generally, all types of these problems can be divided into three categories: poor impression; injuries and diseases; and poor background:

1. **Poor impression.** This category describes fingerprints with poor quality due to environmental conditions or behavior of a capture subject. These problems can be mostly eliminated by applying of appropriate procedures.

   (a) **Dry finger.** This situation can be seen in Fig. 2.10 a). The fingerprint is light and the ridges are changed in the series of dots. This situation may cause problems mostly to the fingerprint area extractors and ridge extractors and therefore it can cause problems with the determination of correct minutiae type. The determination of minutiae type in the fingerprint of a dry finger is difficult even for the experienced dactyloscopic experts.

   According to my experience, this problem mostly occurs by the usage of optical fingerprint sensor. The problem can be easily eliminated by moistering of finger or by applying of slight pressure of the finger on the sensor surface (in case of touch sensor technology).

   (b) **Wet finger.** The example of this situation is shown in Fig. 2.10 b). The fingerprint is dark and it is difficult (or even impossible) to distinguish individual ridges. This situation is reversed compared to the previous one, but the consequences are the same.

   As far as I know, this problem mostly occurs to the optical fingerprint sensor and (if the extreme situations are neglected) the finger can be wet because of environmental conditions (e.g., rain) or excessive sweating.

   (c) **Bended skin/Wrinkles.** The fingerprints containing bended skin can have a few bended parts (or more) or it can be covered by such areas (see Fig. 2.10 c). This bends (sometimes called wrinkles) cause interruptions in the ridge flows, which can be interpreted by the minutiae extractors as the series of ridge endings. This problem can be reduced (or sometimes even eliminated) by the applying slight pressure against the sensor surface (in case of touch sensor technology).

(d) **Dirty finger.** This is a less frequent situation. It mostly occurs in case of special tests (e.g., test how high level of dirt the biometric system is able to deal with) or in case of problems with users (e.g., sabotage of the capturing process - see Chapter 3.6.1).

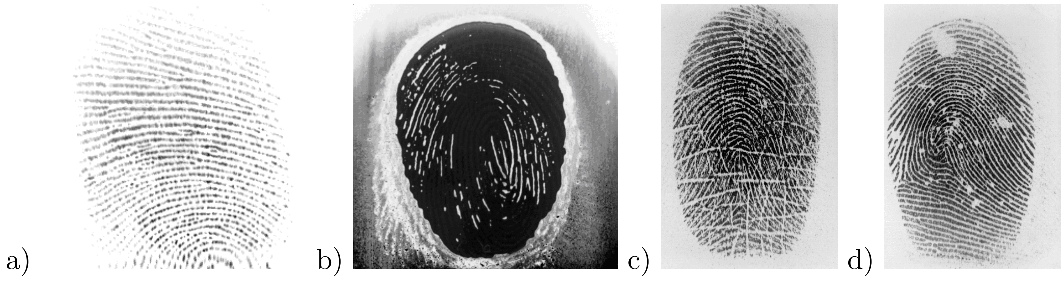


Figure 2.10: Examples of problematic fingerprints: a) dry finger, b) wet finger, c) bended skin, and d) dirty finger.

2. **Injuries and diseases.** Injuries and diseases are the separate category of fingerprint problems. Generally speaking, if the injury (or disease) did not affect the dermal part of skin, the fingerprint pattern can be fully recovered without visible changes in the ridge flow. However, if the injury or disease was deep enough to damage dermal skin layer, then the healed skin/papillary lines contains traces of previous damage. The chronic diseases may go through periods of improvement and remission and the different part (and size) of skin/fingerprint can be affected during these periods. This situation may cause the biometric performance drop, for example it was proved that even the small decrease of fingerprint area may cause a huge performance drop (for the further information see [43]). Several examples of fingerprints with injuries or diseases can be found in Fig. 2.11.

   (a) **Scar.** The first example (see Fig. 2.11 a) the finger with scar caused by a deep cut. The scar has jagged edges and seriously interrupts the ridge flow. This kind of injury is permanent.

   (b) **Burns.** The second example (see Fig. 2.11 b) shows the finger burned by chemical substances. Although this injury seems to be serious, only the epidermal skin layer was damaged and the finger has been fully recovered without any abnormalities in the ridge flow.

   (c) **Wart.** The third finger (Fig. 2.11 c) contains a wart (*verruca vulgaris*). The warts are common disease, which can interfere with dermal skin layer [31]. Lesions are usually located at hands (mostly fingertips and palms) and their size ranges from size of pinpoint to more than 1cm (most averaging 5mm). Nevertheless, this wart has been surgically removed and the skin has been fully recovered without any traces of past disease.

   (d) **Psoriasis.** The last impression (Fig. 2.11 d) belongs to the finger affected by psoriasis. The psoriasis is a common chronic recurrent disease, which can cause a huge discomfort [31]. The course of this disease involves periods of deterioration and remission, so the fingerprint is not affected exactly the same way over time. Affected skin is usually circumscribed, erythematous and lesions are usually covered by silvery white lamellar scales. It is assumed that the 1-2 % of US population is affected [31].

The skin diseases can affect fingers and therefore fingerprints in several ways. Not only the ridge flow can be affected, some diseases can change only the skin color, other can cause that it is not possible to capture ridge structure. Some drugs can even cause the disappearing of papillary lines (e.g., Capecitabine - cancer treatment [86]). Nevertheless, there is a variety of diseases and injuries, which can affect appearance of fingerprints, and their description is out of the scope of this thesis. For further information please see, e.g., paper [16], where this problem was described in detail.

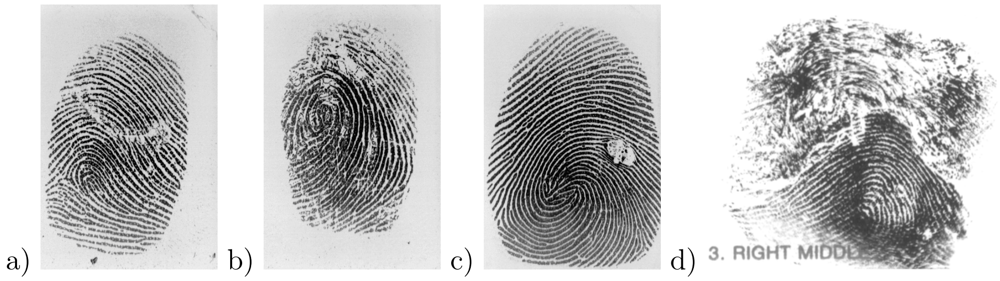


Figure 2.11: Examples of fingerprints affected by injuries and diseases: a) scar, b) burns (chemical), c) wart, and d) psoriasis.

3. **Poor background or whole image.** Due to the poor background image quality, the minutiae extractors can have a problem with the fingerprint area segmentation, which can lead to the false minutiae detection. The problems on the image background (or the whole image) can be caused by different removable or irremovable ways:

    (a) **Dirt.** In case of live impressions, the contamination of the image background by dirt can be caused by the environmental condition, the inadequate maintenance or it can indicate problems with users (e.g., a way to sabotage the capturing process - see Chapter 3.6.1). In case of off-line fingerprints, it can be mostly caused by contamination with dirt or ink drop, which can be hardly distinguishable from the fingerprint.

    (b) **Captured latent fingerprint.** This problem often happens by the usage of touch optical or capacitive fingerprint sensor technologies (see Fig. 2.10 b).

    (c) **Printed text or handwritten notes.** This situation often occurs in the off-line fingerprint impressions, mostly because of printed text and lines indicating the cell/box for impression and describing the finger in the dactyloscopic card (see Fig. 2.11 d), or because of the handwritten notes of dactyloscopic experts, which can interfere with the fingerprint area.

    (d) **Sensor problems.** The problems of sensor itself (design specific or malfunction) can cause the poor background quality or sometimes even poor fingerprint quality. The typical example is the fogging of glass of touch optical sensor due to the sweaty finger (see Fig. 2.10 b) or fogging of protective glass of touchless optical fingerprint sensor.

Another example is the sensor malfunction, which can cause disappearance or depreciation of some image part (e.g., black columns in image captured by malfunctioned sensor based on capacitive technology).

2.4 Used standards

The standardization is a very extensive topic. Given that the part of my work was created as a contribution in response to an ISO/IEC Call for contribution, it is necessary to give a short overview of possible categories of standards and describe the standards essential for my work in more detail.

In case of biometric system (see Fig. 2.1), there are three basic possible layers of communication and interfaces forming three categories of standards [20]: sensor connection (standardized drivers), transfer of the extracted features/references (standardized probes and references) and API[9].

Drivers. The standardization of drivers tries to solve the problem of incompatibility of sensor interface, e.g., USB standard.

Probes/References. The main purpose of standardization of biometric probes/references is to ensure the interoperability of extractors (and comparators), e.g., the multi-part standard ISO/IEC 19794 (Biometric data interchange formats) [95].

API. The goal of API standardization is to provide an interface appropriate for authentication based on arbitrary biometric characteristic, e.g., the BioAPI multi-part standard ISO/IEC 19784 [95].

In addition, there are various other categories of items, which have to be standardized [20], e.g.:

Tests. Usually, there are included the methodologies describing the correct way to do the interoperability testing, technology or scenario evaluation, modality-specific testing, etc. The example of this type of standard is the standard ISO/IEC 19795 (Biometric performance testing and reporting) Parts 1 – 7 [95].

Databases. This group contains the public databases of fingerprint samples, e.g., NIST SD14[10] [71] and SD29 [72] databases used as the base of our Ground Truth Database (GTD).

Security. In this group, there are only a few standards, e.g., Common Criteria (CC[11]) [96] or ISO/IEC 24745 (Biometric information protection) [95], and a lot of them is very general.

Forensic. This group includes standards related to the appearance and functionality of dactyloscopic cards, ID cards, e.g., standard ISO/IEC 24787 (On-card biometric comparison) [98]; or some standards for data interchange, e.g., WSQ[12] standard developed by FBI[13] and NIST, which I use as an input file format in case of semantic conformance testing.

[9] Application Programming Interface.

[10] National Institute of Standards and Technology (USA) Special Database 14.

[11] Common Criteria for Information Technology Security Evaluation.

[12] Wavelet Scalar Quantization [73].

[13] Federal Bureau of Investigation (USA).

Vocabulary. This group contains the standards, which create the harmonized vocabularies for the particular usage, e.g., DIS[14] ISO/IEC 2382-37 (Harmonized biometric vocabulary), whose terminology (version 12) I use in this work [104].

The following three subsections contain detailed description of standards ISO/IEC 19794-2:2005, 29109-1 and 29109-2, because their description is essential for my work. The short description of used parts from standardized databases is given in Chapter 5.2. The detailed description of standardization process is out of the scope of this work, but its brief overview is given in Appendix B. For further information about various standards see, e.g., [95] or [106].

2.4.1 ISO/IEC 19794-2

The international standard ISO/IEC 19794-2:2005 [97] is named „Information Technology - Biometric data interchange formats - Part 2: Finger minutiae data". This standard deals with the format of fingerprint data, specifically the data of minutiae, core and delta. Three types of fingerprint template formats are described: a format for general storage and transport and two formats for card-based systems (general and compact).

The standard begins with list of necessary terms, definitions and abbreviations. Then the possible approaches to detect minutiae are discussed. The formats for general storage and transport can extract minutiae as the ridge ending (encoded as valley skeleton bifurcation) and ridge bifurcation points. The card formats can use the same possibility or it can use ridge skeleton endpoints and ridge bifurcation points. The differences among these three approaches could be seen in Fig. 2.12.

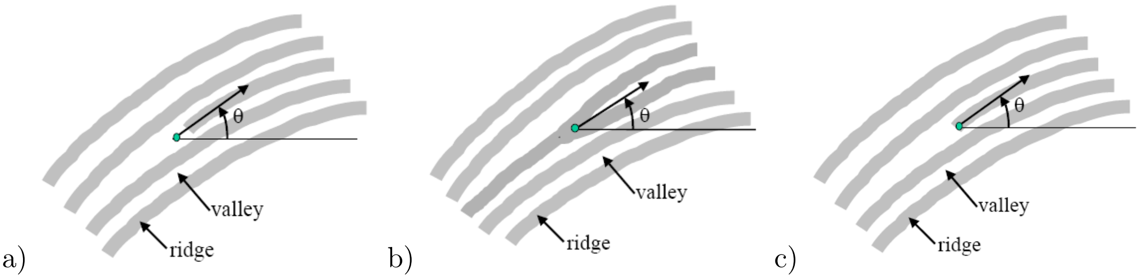


Figure 2.12: Position of minutia according to the ISO/IEC 19794-2:2005: a) the ridge ending (encoded as valley skeleton bifurcation), b) ridge bifurcation (encoded as ridge skeleton bifurcation point), c) ridge skeleton endpoint.

The ISO/IEC 19794-2:2005 standard recognizes only three types of minutiae: the ridge ending, ridge bifurcation and the type „other". It assumes that the most of minutiae can be described as a combination of ending and bifurcation and for the other minutiae, there is the type „other".

The position of minutia is given in pixels, but the coordinate system is a little bit unusual. The origin is in the upper-left corner. The x axis is increasing to the right and the y axis downward.

The determining of value of minutia angle is also a little bit unusual. As it has been mentioned earlier, the angle is measured counter-clockwise from the horizontal axis to the right. However, the measured value (in degrees) has to be converted to the 0 – 255 range. Therefore, the value of 180 deg means 128 and for example the value of 22.5 deg means 16.

[14] Draft International Standard (see brief description of standardization process in Appendix B).

The range of quality of minutia is 1 (as a minimum) to 100 (as a maximum). It is also possible to set the value of quality to 0, in case of usage of minutiae extractor without the capability to supply quality information. Nevertheless, the minutiae quality is the often discussed topic and any international standard describing the minutia quality determination methodology has not been published yet, so the ISO/IEC 19794-2:2005 standard does not ensure the comparability among minutiae quality values determined by different extractors or stored in different templates.

Moreover, the standard describes several information about the image, e.g., the image size or the possible values of x and y image resolution, or about the whole fingerprint, e.g., finger position (right thumb - left index finger) and impression type (e.g., plain, rolled, swipe). Important information is that the values of x and y image resolution should not be less than 98.45 pixels per centimeter (250 pixels per inch) and they are stored separately.

However, the standard itself contains a few inconsistencies. For example, the quality range: in one case the value of 0 means the unknown value and the value of 1 the lowest quality value, in other case the value 0 means the lowest quality value. Moreover, the maximum image size is 65 535 × 65 535 pixels, but according to the reduced amount of bits for minutia position data, the usable area of fingerprint is just 16 384 × 16 384 pixels.

The standard also contains the optional extended data fields, which may contain information about cores (type, position, and angle), deltas (type, position, and 3 angles), ridge counts or cell information. This standard allows recording data from 0 to 15 cores and the same amount of deltas.

Generally, the format can contain maximally 255 fingerprints (but only 16 sessions per each of 11 fingers) and 255 minutiae, 15 cores and 15 deltas per fingerprint. The detailed description of data field in mandatory data blocks is stated in Appendix C.

2.4.2 ISO/IEC 29109-1

The international standard ISO/IEC 29109-1 (Information Technology - Conformance Testing Methodology for Biometric Data Interchange Records defined in ISO/IEC 19794 - Part 1: Generalized Conformance Testing Methodology) has been published in 2009 [99].

Recently, there are many vendors claiming that their product conforms to the relevant part of the ISO/IEC 19794 standard. Nevertheless, there was no published or standardized methodology to confirm or refuse this claim. Therefore, the intention of this standard is to provide tests and methods, which will be able to give „the reasonable degree of assurance that a conformance claim has validity“ [99].

This standard describes test types, test levels and general methods for conformance testing purposes. The standard distinguishes two different types of conformance tests:

Type A. This type of conformance tests attests whether a unit (an extractor) generates a conformant biometric data interchange record (template).

Type B. This type of conformance tests attests whether a unit (an extractor) is capable to read a conformant biometric data interchange record (template) correctly.

This standard focuses on Type A of conformance tests and distinguishes three different levels of testing:

Level 1: Data Format Conformance. This level of test checks field-by-field and byte-by-byte conformance with the relevant biometric data interchange standard. It is a syntactic test and tests, e.g., whether the mandatory data fields are included and check the range of values in these fields.

Level 2: Internal Consistency Checking. This is also a syntactic test; nevertheless, it tests an internal consistency of data fields. It relates the values from one part to the values from the other part of the record and checks whether they are correctly related (e.g., whether the x and y minutiae positions fall within the specified image size).

Level 3: Content Checking/Semantic Testing. This level of test checks whether the generated biometric data interchange record (template) is a faithful representation of an input data (fingerprint).

2.4.3 ISO/IEC 29109-2

The international standard ISO/IEC 29109-2 (Information Technology - Conformance Testing Methodology for Biometric Data Interchange Records defined in ISO/IEC 19794 - Part 2: Finger Minutiae Data) has been published in 2010 [100]. This standard contains the guidelines to Level 1 and Level 2 conformance testing for measuring conformity to the international standard ISO/IEC 19794-2 [97]. Moreover, it defines procedures to be followed in case of the conformance testing.

Unfortunately, this document contains only a few remarks about Level 3 conformance testing and it does not contain any guideline or methodology for this purpose at all. Nowadays, the ISO/IEC JTC1/SC37 WG3[15] prepares a new amendment to the ISO/IEC 29109-2 standard, which should contain the methodology for Level 3 (Semantic) conformance testing (see Section 3.5.5 and Chapter 5).

[15] ISO/IEC Joint Technical Committee 1/Subcommittee 37 Working Group 3.

Chapter 3

Security of biometric systems

For the purposes of this thesis, it is essential to describe the state of the art in the area of security of biometric systems. At first it is necessary to analyze the possible vulnerabilities (weak places - see Section 3.1.1) of biometric systems and describe the threats (the possible attacks, their goals and motivation - Section 3.1.2) to the biometric system. The particular attacks and corresponding countermeasures/precautions are then described in Sections 3.2 – 3.6 of this chapter.

3.1 Introduction to the security of biometric systems

The introduction to the security of biometric systems begins with the analysis of the possible vulnerabilities (weak places, see Section 3.1.1) of biometric systems. The second part (see Section 3.1.2) consists of description of the threats (the possible attacks to the biometric system), their classification, goals and motivation.

3.1.1 Weak places of biometric system

For the identification and analysis of the vulnerabilities (weak places) of the biometric system it is necessary to deeply understand the functionality of each component and also the entire system (see Section 2.1). In Fig. 3.1, there are marked major weak places of a biometric system [3, 37, 43]. As it can bee seen, there is neither component nor channel, which is impossible to attack.

One of the major weak places and also the most easily attackable part is the place number 1, the sensor itself. An attacker can easily fool the sensor using an artificial finger or other spoofing method (see Section 3.2 for detailed description).

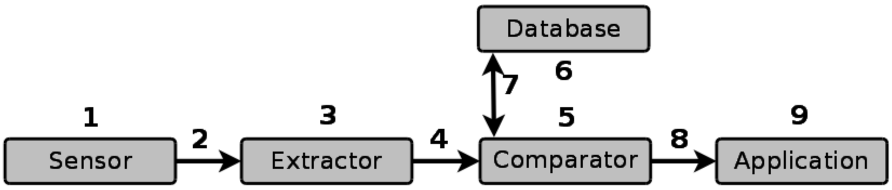


Figure 3.1: A diagram of biometric system. Weak places are marked by numbers [37].

The attacks can be also directed against other components (weak places number 3, 5, and 6) and/or communication channels (weak places number 2, 4, 7, and 8). In case of presence of hardware securing, the attack often begins with the attempt to bypass or destroy this hardware securing (see Section 3.4) and in case of success, it continues with the software attack, e.g., Replay attack, or Trojan horse (see Section 3.5).

The last weak place is an application itself[1]. If an attacker can input directly into this application and compels the access, then the usage of the whole biometric system is futile. If it is possible to use this attack (with reasonable effort and resources), it is not convenient to use biometric system for securing of such application [37].

3.1.2 Types of attacks

There are three basic types or goals of an attack: to obtain information/data, gain access or DoS[2] attack [30, 35, 43].

The DoS attack can have many forms [3], from the temporary attacks not causing a permanent damage to the serious damage of the hardware. The attacker can invade various communication channels or components, she/he can cause slowing down or stopping of the biometric system using various ways, e.g., by changing of threshold in extractor or comparator (see Section 3.5.1), by the overload of the communication network by forged messages (see Section 3.5.3) or by sabotage (see Section 3.6.1).

It does not matter, which channel or component has been attacked, because blocking of communication on each of them takes the whole system out of service. In such case, the biometric system has to be temporary replaced by other authentication procedure, which may be the goal of the attacker, because the substitute system can be more easily overpowered (e.g., a human supervisor can be corrupt). On the other hand, the easier circumvention may be only one of the possible reasons. The other reasons may be, e.g., extortion or the political reasons [3].

The second possible goal of an attack can be to obtain data, mostly the biometric reference of enrollees. In case that the particular person uses two or more biometric systems, then the attacker can try to obtain biometric reference from the least secured system and use them to gain access to the more secured system, e.g., by the generating of a fake finger structure using the minutiae data from obtained biometric reference (see Section 3.2.4) and subsequent creation of a fake finger (see Section 3.2.2). A possible precaution is the usage of cancelable/revocable biometrics (see Section 3.3.3).

The common goal of the attack is to gain access to the system or area protected by a biometric system. The simplest way to gain access is the spoofing (see Section 3.2). Many of the biometric sensors are vulnerable to this type of attack, but if the area/data is secured by the use of sensor with some of the anti-spoofing ability (see Section 3.3), it is still possible to use DoS attack or try to use more sophisticated hardware and/or software attacks (see Sections 3.4 and 3.5).

3.2 Spoofing of biometric sensor

Methods for spoofing of fingerprint sensors appeared simultaneously with sensors themselves. In previous years, researches demonstrated several very successful methods for fooling

[1] The application is sometimes (by some authors) considered to be part of the biometric system but it can be also understood as a part to which the biometric system is connected.

[2] Denial of Service.

of different types of fingerprint sensors. These methods can be divided into the following four categories [40] (see Section 3.2.1 - 3.2.4).

3.2.1 Reactivation of latent fingerprints

Reactivation of a latent fingerprint is the simplest and quickest way of spoofing of sensors. Thalheim et al. [67] proposed three ways how to fool capacitive fingerprint sensors:

Breathe. The breath on a sensor area can reactivate latent fingerprints left on the surface of capacitive sensors. The water vapor contained in the breath condenses on the sensor surface. The combination of condensed water vapor and grease from latent fingerprint causes the change of capacitance, which initiates the capturing process.

Plastic bag. The application of a thin-walled plastic bag filled with water on the sensor area is able to reactivate the latent fingerprint left on the surface of capacitive sensors. The principle of this method is the same as in case of the previous method. The resulting images have often the better quality than images captured with breath, because the water applied by plastic bag is spread more uniformly.

Dust. An attacker can also dust the latent fingerprint with an appropriate type of powder (e.g., graphite) and gently press an adhesive tape over it and spoof capacitive fingerprint sensors. Moreover, it is possible to use the latent fingerprint left on other place and dust it with the powder. Then it is necessary to press the adhesive tape thoroughly over it and transfer the fingerprint on the sensor surface.

All these methods were tested by Thalheim et al. [67] on capacitive sensors made by Infineon Technology AG[3] [91], STMicroelectronics Group [122] and Veridicom International, Inc. [128].

For the education purposes, I have personally tested the first approach (the breath on the sensor area) on capacitive sensor Suprema SFM3050-TC1. The test was successful beyond expectation (approx. 75% success rate), so I decided to show this approach to the students as an example of easy and free way to spoof the fingerprint sensor. Nevertheless, the success rate has declined over time and after three years of extensive use of this sensor, it was no longer possible to successfully demonstrate this approach.

3.2.2 Artificial fingers

There are two different approaches: professionally-made fingers and the home-made fingers. Professionally-made fingers represent a simple solution - an attacker does not make artificial fingers at home, but uses a service of some companies or common office machines.

One possibility is to use a printed structure of papillary lines or a picture of finger itself. This kind of fake should spoof optical fingerprint sensors. However, this kind of attack is rarely mentioned and it does not exist any serious study of its use and success rate.

Another possibility is that the attacker takes a picture of a latent fingerprint of an enrollee and enhances it by the help of Photoshop [38] (or another appropriate software). Then he/she goes into stationer's shop and orders creation of a stamp. The stamp is usually finished in two days and it costs approx. 4 EUR (in 2007). In Fig. 3.2 you can see that it is possible to spoof a thermal, optical, and capacitive fingerprint sensor using it.

[3] The tested capacitive sensor was integrated into Siemens ID Mouse. After these tests, Siemens published a paper [36] denying possibility to spoof their device using the above described techniques.

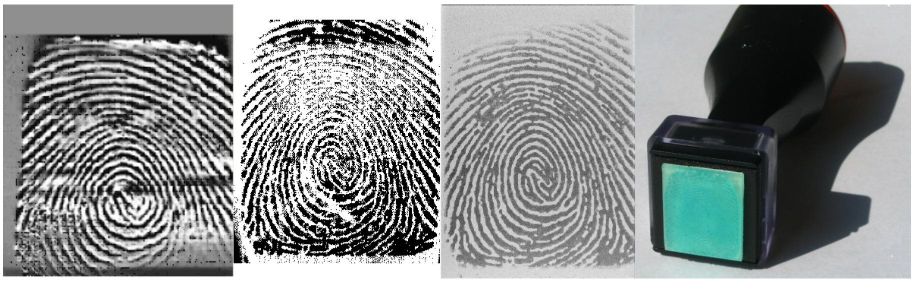


Figure 3.2: Stamp captured by different types of sensors [40]: left fingerprint - thermal sensor (Bergdata FCAT 100), middle fingerprint - optical sensor (Suprema SFM3020-OP), right fingerprint - capacitive sensor (Suprema SFM3050-TC1). Right picture: Picture of stamp of fingerprint.

The second option is the creation of home-made fingers. This way of spoofing of fingerprint sensors is probably most widely used. There are two different approaches for creation of these fingers: it is possible to create an artificial finger with or without assistance of an enrollee.

1. **With assistance of enrollee.** This solution is easier than the second one. The enrollee presses his/her finger against prepared material and thus he/she creates the mold, which is filled with appropriate material afterwards. This approach is very successful and there are a lot of possibilities, which material is appropriate for creation of mold and which is good for artificial fingers. For example, Matsumoto et al. [45] used free plastic for mold and gelatin for fingers (so called gummy fingers), Thalheim et al. [67] used a wax mold from tea candle and silicone for fingers and Prof. Schuckers et al. [59] created their mold from dental impression material and fingers from play-doh. In all cases, they achieved high successful rate.

2. **Without assistance of enrollee.** Creation of an artificial finger is more difficult, if an attacker cannot count with assistance of the enrollee. In this case, the attacker has to obtain a latent fingerprint of the enrollee, take a picture of it and enhance it, e.g., in Photoshop. Then he/she prints a resultant image on slide, puts it on photosensitive PCB[4] and illuminates it with UV[5] lamp. The illuminated PCB is developed by the help of dilutions of sodium hydroxide ($NaOH$) and iron trichloride ($FeCl_3$). This procedure was proposed by Prof. Matsumoto et al. [45] and was used for creation of mold in Biometric laboratory at the Brno University of Technology [40] (see Fig. 3.3).

The most dangerous types of homemade fingers are thin fingers. This kind of artificial finger can be glued on attackers own finger and it can be difficult to find this artificial finger even by supervisor or a camera system. This kind of attack was successfully used, e.g., against Japanese fingerprint immigration screening in 2008 [62].

The artificial fingers were also tested in the Life Finger project [11]. For these purposes, they have created the „BSI[6] Fake-Tool-Box“, which contains 25 different materials (and which should be regularly updated). These fake fingers were able to spoof not only all 12

[4] Printed Circuit Board.

[5] Ultraviolet.

[6] Bundesamt für Sicherheit in der Informationstechnik (Federal Office for Information Security - Germany).

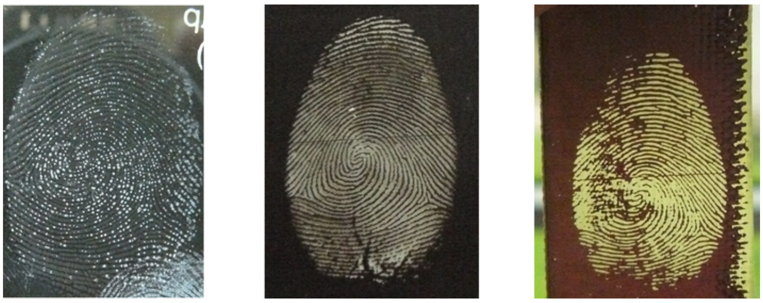


Figure 3.3: Process of creation of mold from latent fingerprint [40]: (left) the fingerprint enhanced by cyanoacrylate; (middle) the fingerprint enhanced in Photoshop and printed on a slide; (right) the photosensitive PCB after developing – the mold prepared for usage.

tested common sensors (5 different sensor technologies) but also all sensors with the liveness detection ability, which was possible to test [11].

3.2.3 Dead fingers

The worst option is the usage of a human finger separated from a body. Prof. Schuckers et al. [58] tested this option by using of cadaver fingers. These tests were performed on the capacitive, optical and electro-optical fingerprint sensors. The success rate for 14 subjects was in the range of 40 to 94 percent depending on the sensor technology.

Possibilities of electronic fingerprinting of dead fingers (from the forensic point of view) were studied also by Rutty et al. [56]. They tested 45 subjects on a capacitive fingerprint sensor and proved that there is no problem to capture cadaver fingerprints and that this approach is dependent only on the status of the used finger.

3.2.4 Generated fingerprints

Previously it was thought that a stolen fingerprint template does not pose a big threat, because it is impossible to generate (good-quality) fingerprint from minutiae points and thus it is not possible to create fake finger on the basis of the stolen data.

In 2005, Assoc. Prof. Ross and his colleagues have published their preliminary results on reconstruction of fingerprints from minutiae points [53]. Their method was able to reconstruct the orientation map of the original fingerprint (see Fig. 3.4 a), however, the existence of only eight different angles in the orientation map resulted in angular papillary lines.

Later, this team has improved their method to produce a fingerprint containing smooth papillary lines [52]. They used selected group of minutiae as seeds and applied streamlines and Linear Integral Convolution on the estimated orientation field. The resultant image contains smooth papillary lines and can be used to spoof a biometric system. Nevertheless, this approach/fingerprint is not able to fool a human supervisor (see Fig. 3.4 b), especially due to the existence of areas within a fingerprint and without the papillary lines.

At the same time, Dr. Cappelli and his colleagues have created another approach to the fingerprint generation [13]. They used prototypes of ending and bifurcation as the seeds at minutiae positions. Thereafter, they applied Gabor-like filters to grow the seeds up. After several iterations, the empty regions of the image are filled and the fingerprint is completed (see Fig. 3.4 c). This generated fingerprint is fully capable to be a basis for creating a

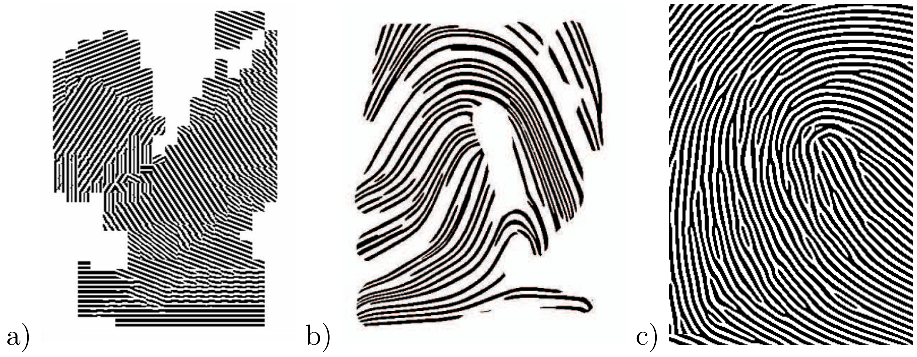


Figure 3.4: Examples of fingerprints generated from minutiae: a) fingerprint created on the basis of simple orientation map reconstruction [53], b) fingerprint created by the help of streamlines and Linear Integral Convolution [52], c) fingerprint created by the help of seed prototypes and Gabor-like filters [13].

high-quality fake finger, to spoof a biometric system and (in case of application of noise, etc.) to fool even the human experts.

Dr. Cappelli and his colleagues have improved their method and have created the SFinGe[7] program [82]. Their algorithm/program has also been used as a source of one of databases in the Fingerprint Verification Competition (FVC) since 2000 [89].

3.3 Anti-spoofing possibilities

Generally, there are four complementary approaches. The first two approaches are the liveness detection and the fake finger detection, which try to ensure that no fake finger will be considered (enrolled/identified/verified) as the live finger. The third approach is the usage of appropriate approach to multibiometrics, e.g., multi-modal biometric fusion. The fourth approach is the cancelable/revocable biometrics, which tries to secure the enrolled and processed templates that it will not be possible to extract important information (e.g., minutiae) from the template.

3.3.1 Liveness detection and fake finger detection

As it was mentioned earlier, both of these approaches try to ensure that no fake finger will be considered (enrolled/identified/verified) as the real one. Nevertheless, there is an important difference between them. The liveness detection (formerly called vitality detection) tries to detect whether the scanned sample belongs to the real live human finger. It tries to find the presence of some property/properties typical for the live human sample. The overview of recent liveness detection methods together with their advantages and disadvantages can be found in Section 4.1 and my patented approach to the liveness detection can be found in Sections 4.3 - 4.5.

For the purposes of liveness detection, it is not necessary to know the detailed characteristic of all types of fake fingers, because the fake fingers are necessary only for the testing purposes. From the testing point of view, the dead fingers and the very thin made-fingers are the most difficult detectable fakes. The very thin made fingers are dangerous because of

[7] Synthetic Fingerprint Generator.

its thickness. It can happen that some methods of liveness detection will penetrate through and will test the liveness of a real finger behind it.

The fake finger detection (spoof detection) has a different approach. It tries to find whether the tested sample is a fake/artificial finger. It means that these methods try to detect some properties characteristic for the fake/artificial fingers.

In the real-world scenario, the liveness detection and the fake finger detection are applied simultaneously, e.g., to set the threshold for some characteristic property.

3.3.2 Usage of additional biometric characteristic

Another approach to increase the security and reduce the chance of sensor deception is the usage of biometric fusion - multibiometrics [20, 35]. Generally, it is possible to distinguish six different approaches to multibiometrics [35]:

1. **Multi-sensor:** usage of several sensors to capture the same biometric characteristic. According to my experiences, the spoofing of two different fingerprint sensors is slightly more difficult and time-consuming than spoofing of one sensor, but it does not cause too much inconvenience to the attacker.

2. **Multi-algorithm:** usage of several algorithms to extract different features from a biometric sample (e.g., minutiae-base and correlation-based algorithm) or usage of different comparison algorithms. This approach cannot be used to reduce the chance of sensor deceiving. It is very likely that the good-quality fake finger, which can be captured and successfully identified/verified by one extractor/comparator, can be also successfully identified/verified by another extractor/comparator.

3. **Multi-instance:** usage of multiple instances of a biometric characteristic, e.g., both irises or several fingers. It can be assumed that if the attacker can get one biometric characteristic (e.g., one fingerprint) of a particular person, he/she is able to get the second one too.

4. **Multi-sample:** usage of several samples of the same biometric characteristic. The second capture of same fake finger is able to eliminate the bad-quality fake fingers, but it can have no influence on attack by usage of good-quality fake finger.

5. **Multi-modal:** usage of multiple biometric characteristics. This approach can significantly reduce the success rate of sensor spoofing attacks. In this case, the attacker has to obtain two different biometric characteristics of particular person and successfully spoof two different biometric capture device technologies.

6. **Hybrid:** combination of several of previous categories.

From the security point of view, the best of the above-described options is the application of multi-modal biometric fusion. This approach is the only one of the above described options of biometric fusion, which can significantly reduce the chance to sensor deceiving.

The capturing of two (or more) different biometric characteristics can cause a discomfort to the biometric enrollee, due to the necessity of capturing by two (or more) different sensors, the more time-consuming process and the resulting queue, etc. The solution can be the capture of both (or all) biometric characteristics at once, which means that the captured biometric characteristic should be present on the same body part. The capturing by the same sensor (integration of two or more different sensors in one) could also be more comfortable for enrollees and could lower the price of final solution.

In case of fingerprints, the additional biometric characteristic could be, e.g., finger/palm veins or 2D/3D hand geometry. For example, the combination of the finger veins and fingerprints is promising, because the vein pattern cannot be obtained so easily as fingerprint or hand geometry and because it could be quite easily integrated to the optical fingerprint sensor.

In 2008, we (me, Mr. Úlehla and Assoc. Prof. Drahanský) have worked on the pre-prototype of finger veins sensor. Several tens of LED diodes, several positions of these diodes and several finger positions were tested and finally we got this form of pre-prototype (see Fig. 3.5 a). This sensor could be used as the single-modal sensor or it could be integrated into an optical fingerprint sensor into one biometric solution.

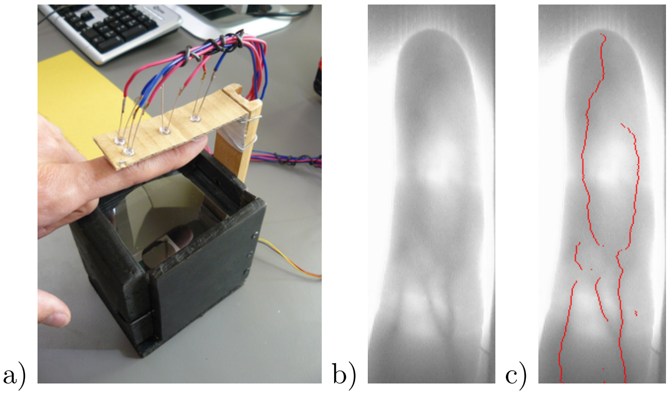


Figure 3.5: Example of finger vein detection: a) pre-prototype of finger vein sensor, b) captured vein image, and c) captured vein image with extracted vein skelet. (These images have been previously published, e.g., in [25].)

In 2009, we (me, Mr. Dvořák, Mr. Krajíček and Assoc. Prof. Drahanský in cooperation with Digitus s. r. o.) have developed an algorithm for detection of finger veins in image. This algorithm consists of several phases:

1. **Pre-processing.** It is necessary to remove noise and enhance specific features of the input image (see Fig. 3.5 b). For this purposes, common Median filter (5 × 5 px) and Smooth filter (3 × 3 px) are used.

2. **Edge detection.** For the purposes of edge detection, we use the convolution with special kernel. The usage of this kernel causes an effect similar to the side-illumination of finger veins.

3. **Thresholding.** The convolution is followed by thresholding (binarization) with $T = 1$.

4. **Post-processing.** The Median filter (7 × 7 px) is used for the purposes of removing of artifacts/small inaccuracies.

5. **Thinning.** The thinning algorithm is simple and very effective; it just finds the borderline between big black area and big white area.

6. **Post-processing.** The removal of small inaccuracies (e.g., undesirable isolated points) is done by a special type of median filter (3 × 3 px). The result can be found in Fig. 3.5 c).

Separately the finger contour is detected (by the usage of a similar pipeline) and it is used as a filter to remove the artifacts outside of the finger area. The top of the finger detection has been also used for the purposes of template comparison. The preliminary template consists only of absolute positions of finger vein pixels beginning on the row containing the top of the finger and the comparison score have been also an absolute number. Nevertheless, the results look promising.

Unfortunately, it is not possible to present the whole solution in this thesis. Our solution has been published on three international conferences and in one international journal [25], where the additional information can be found. Moreover, we have registered our solution as the Czech utility model No. 21548 [18] and the patent is pending.

In the meantime (in October 2009), the Sagem Morpho, Inc. and Hitachi, Ltd. unveiled their solution of multi-modal fingerprint-finger veins sensor „Finger VP" [83, 90, 116] and this sensor became the first multi-modal sensor in the market.

3.3.3 Cancelable/revocable biometrics

Recently, there are broadly discussed two theoretical possibilities, which are called cancelable/revocable biometrics [3, 43, 49, 125]. The goal of these methods is to store templates in non-reversible format. It means that it will be impossible to create a list of minutiae (or fingerprint) from the stored template. Another goal is to enable a creation of different identities per each person. These identities of one person could be used for different systems (e.g., health care, e-banking) so that there will not be any possibility to link them, and of course, there always has to be a possibility to cancel the identity or create another one.

One approach was proposed by Ratha et al. [49]. This approach is based on deformation of fingerprint image or minutiae coordinates. They proposed three different types of deformation: Cartesian, radial and functional. Nevertheless, there is still the problem with the vector of input parameters for deformation algorithm, because if an attacker will steal the vector, he/she can re-transform the template back.

Another approach is an intention to create some new one-way function [43]. In case of fingerprints or their templates, it is not possible to use commonly known hash functions, because of comparison principle. If we compare few captured images from one person, the sum of minutiae or their position is not the same in each case. Some minutiae are missing because of finger rotation; their position can change because of finger translation and deformation of skin, etc. The common comparison algorithm uses the rotation and translation of image (or coordinates) and looks for minutiae in some tolerated distance and this will not be possible after using hash function.

The demanded new hash function for fingerprint systems has to consider all these requirements and find a way how to meet them, and this was a main goal of the TURBINE[8] project [125]. They submitted seven template protection methods, which could meet the criteria of irreversibility, revocability and unlinkability [63]. Although the project ended in 2011, their work on template protection methods continues in the ISO/IEC JTC1/SC27 WG5, where they participated, e.g., in the creation of the standard ISO/IEC 24745 (Biometric information protection) [95, 125].

[8] Trusted Revocable Biometric Identities.

3.4 Security of hardware

The primary purpose of hardware securing is to block access to the device for possible attackers. Nowadays, there exist a lot of other approaches (anti-tamper mechanisms) [23, 47, 68], which can be successfully used for blocking, detection or response to the possible entrance of an attacker. These mechanisms can be divided into four groups according to their impact: tamper evidence (see Section 3.4.1), tamper resistance (see Section 3.4.2), tamper detection (see Section 3.4.3), and tamper response (see Section 3.4.4). The application of all these four principles can create a tamper proof device/module.

However, there is another problem; manufacturers of biometric solutions/sensors do not publish any information about securing of their devices. This situation can have two reasons, either they do not have any securing, or they think that they are increasing the security of sensor by keeping this information back (so called Security by Obscurity - see Section 4.2.2).

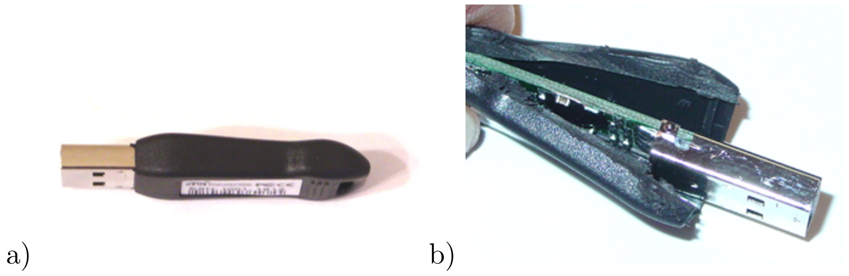
3.4.1 Tamper evidence

The main idea of tamper evidence techniques is to „left visible evidence behind the tampering“ [23]. Generally, the tamper evidence can be defined as „design and production techniques that aim to ensure that the act of tampering will result in an irreversible physical change to the device observable by subsequent audit“ [68]. These techniques are not intended to primarily block access to the protected parts of the device, their purpose is to cause the visible evidence of the security breach, but these two goals can be interconnected in many cases.

The basic tamper evidence are security seals or tapes [47]. They often contain some unique attribute (e.g., serial number) to make their replacement by an attacker more difficult.

The more advanced option is to use some special enclosure finishes, e.g., brittle packages, crazed aluminum or bleeding paint [23] to add the tamper evidence capability to the device. It is also possible to use the special glue with high melting point to glue the pieces of outer shell together. If the glue has higher melting point than the plastic enclosure, then the plastic melt before the glue, which creates a very good evidence of the attack. It means that this approach can present the tamper evidence and tamper resistance approach at once.

The other option is an ultrasonically-welded outer shell of device [23]. This industrial technique is based on applying of high-frequency ultrasonic acoustic vibrations to the material of outer shell (mostly plastic). After the application, the outer shell looks like made from one piece. In this case, the opening of outer shell can require destruction of device. An attempt to disassemble is shown in Fig. 3.6.


a)

b)

Figure 3.6: Example of an attack to the ultrasonically-welded outer shell: a) device before attack, b) device after attack [23].

3.4.2 Tamper resistance

The primary goal of tamper resistance approach is to „make tampering difficult“ [23]. This security approach can be generally defined as „the ability of device to defend against a threat that has the objective to compromise the device and or the data processed by the device“ [68]. As it was mentioned in the previous subsection, the tamper resistance ability is often connected with the tamper evidence ability.

The simplest way for securing of device using tamper resistance approach is to cast important parts (or whole interior of device) in epoxy (or other substance, e.g., urethane) [23, 47]. The epoxy encapsulation is very cheap and robust solution, because an attempt to remove epoxy will seriously damage the circuit itself. There are some general approaches, how to remove epoxy encapsulation, e.g., heating or usage of drilling machine with wooden skewer as a bit [47]. Nevertheless, these approaches are intended for general purposes and their usage on electrical circuits usually results in the destruction of PCB or components on it.

On the other hand, it is necessary to count with the fact, that the component casted in epoxy cannot be repaired. In case of malfunction, it is necessary to replace whole part (or whole reader). According to the opinion of experts (e.g., Ing. Martin Úlehla - MGM Compro and Ing. Petr Mikušek - DCSY FIT BUT[9]), it is also important to take into account the future epoxy encapsulation during the design of circuit because of cooling. The example of PCB cast in epoxy can be found in Fig. 3.7.

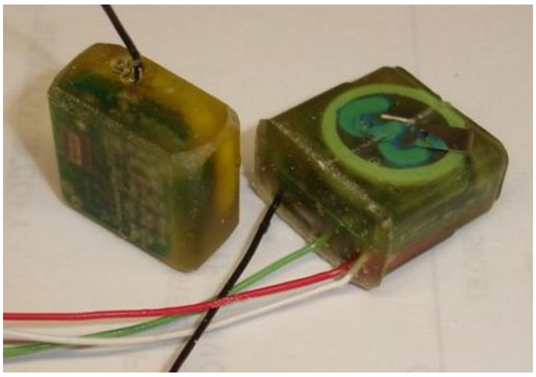


Figure 3.7: Example of PCB secured by the casting in epoxy [24].

The other and often used approach to add tamper resistance ability to the devices is the usage of specially shaped screws [23, 47]. On the other hand, this approach is so popular, that currently it is possible to buy security bits at common electronic stores.

3.4.3 Tamper detection

The tamper detection ability of device can be defined as: „Tamper detection is the ability of a device to sense that an active attempt to compromise the device integrity or the data associated with the device is in progress.“ [68]. The detection of the attack is the basic assumption to initiation of the tamper response mechanisms. However, the greatest design challenge in this area is to create mechanism sensitive enough to detect threat and tolerant enough to avoid false alarms.

[9] Department of Computer Systems, Faculty of Information Technology, Brno University of Technology (Czech Republic).

There are a lot of options of the tamper detection mechanisms and also a lot of approaches to disable these detections. Generally speaking, the successful tamper detection mechanism has to be active regardless to the state of the device to limit the possibilities of circumvention [68].

The first group of the tamper detection approaches contains the mechanisms based on direct detection of opening/removing of outer shell. For these purposes, various types of switches can be used [23], e.g., electric or magnetic switch. According to the opinion of experts (e.g., Ing. Martin Úlehla - MGM Compro and Ing. Petr Mikušek - DCSY FIT BUT), these methods are often quite cheap, but a lot of them can be easily fooled or bypassed.

The attacker can also try to enter into device without removing cover, e.g., by making a hole into it. In such case, it is possible to use some kind of vibration detector, e.g., mercury switch, or it is possible to use a barrier or matrix designed especially to detect drilling or similar type of attack [68].

The third approach to tamper detection is the indirect detection of entrance of the attacker - the detection of operational or environmental changes [47, 68]. For this purposes, it is possible to use sensors for detection of light or other radiation (x-rays, gamma rays), voltage, frequency, temperature, pressure or other variable. According to the opinion of experts (e.g., Ing. Martin Úlehla - MGM Compro and Ing. Petr Mikušek - DCSY FIT BUT), the most used method is the utilization of photodiode. This method is very cheap, but it is necessary to set a threshold very carefully, otherwise it cannot detect uncovering at night.

3.4.4 Tamper response

The last of four categories of anti-tamper mechanisms is the tamper response ability of device. It can be understood as the countermeasures in responses to the detected attack (initiated by tamper detection mechanism) [23, 68] or according to the general definition „the action that a device performs in order to prevent misuse or modification of the device, or the modification or disclosure of critical data contained in the device" [68].

There are a lot of possible approaches, how to react on the detected attack on the device. Generally, it is possible to shutdown, disable or destroy the device [23]. The event also can be logged or the device can send a message (e.g., some securing can send an SMS to the predefined cell phone in case of detected attack).

The often response to the detected attack is the zeroization of a critical memory [23, 47]. In case of a biometric system, it can be the memory containing the database of biometric references of enrollees. There are two possible approaches: a passive zeroization and an active zeroization [47]. In case of passive zeroization, the device disconnects power to the memory, so the data should be lost. Nevertheless, the previously stored data can remain in RAM[10] or other storage and there are several techniques to restore these data after power-off (e.g., usage of extreme temperature or voltage). However, the better solution is the active zeroization, where the data are actively overwritten.

Another approach is based on the combination of tamper detection and tamper response strategy. It is possible to use, e.g., the brittle components [47], so that the drilling or other attack mostly cause a destruction of the component or the whole device.

[10] Random-access memory.

3.5 Security of software

It is not possible to completely rely on the hardware securing and expect that the software/firmware part of a biometric device cannot be successfully attacked. It is generally known that every part of each system can be successfully attacked; it is just a manner of time, effort and resources.

3.5.1 Change of threshold

The sensor itself is not the only one target of possible attacks, there is another group of weak places containing the rest of components. For example, it is possible to attack the comparison unit by changing threshold value [3, 43]. If the changed value is too high, every identity will be rejected, which causes so called DoS attack. In such case, the biometric system has to be temporarily replaced by other authentication procedure, which can be easily overpowered by an attacker (e.g., a human supervisor can be corrupt).

Another situation occurs, when an attacker sets the threshold value too low [43]. In this case, every identity is accepted and it does not matter if it is an enrollee or an attacker. This change can be very dangerous, because it is not possible to reveal it in the common working condition without presence of a special test.

Similar method is the change of threshold value in an enrollment process [3]. In case of decreasing of threshold, it is possible to register even a very poor biometric sample, which can be easily imitated, and on the contrary, the increasing of this threshold causes the DoS attack.

3.5.2 Change of template

Another possible target of an attack could be a database of templates. One possible attack can be the stealing of a template [3]. Formerly, there was an opinion that it is impossible to reconstruct the fingerprint from minutiae data, but a few algorithms with this ability were developed in past years [42]. After the attacker reconstructs a fingerprint, he/she can use it for creation of some kind of artificial finger as described in Section 3.2.

Another possible attack on the database is a change of a template in database to the attacker's template. In this case, the enrollee cannot access to the system, but the attacker is able to.

3.5.3 Forged message

Generally, there are two possibilities to deceive biometric system by the usage of forged messages: Replay attack and pre-prepared message.

The first possibility of attack is so called Replay attack [3, 43]. In this case, an attacker connects to some channel and saves the sent information/message. At the moment of attack, he/she just sends the stored data.

The other way of attack is little more complicated. In this case, an attacker does not need to install some facility for saving messages; he/she just pre-prepares suitable information and sends it. The advantage of this method is that it is not necessary to wait for obtaining of message from successful identification/verification process of a capture subject. On the other hand, the disadvantage is that the attacker has to have a lot of necessary information about the used system to create a right format of the message, and in the case of attack on channels from/to extraction unit, he/she needs to have the fingerprint/template of some enrollee.

On the other hand, the forged/fake messages can have also other utilization than the deceiving of the biometric system. It is possible to send a huge amount of these messages, flood the system and cause the DoS attack.

3.5.4 Trojan horse

The last and most difficult way of an attack by communication channels is the usage of so called Trojan horse [43]. This facility/program can replace any component of a biometric system. For example, Trojan horse can pretend to be an extractor. In this case, it connects in an output from a sensor, sends its own output to a comparator and connects in the output from the comparator to get a comparison score.

The advantage of this kind of attack is that the attacker does not need any information (e.g., fingerprint) from the enrollee. On the other hand, for completion of this attack, it is necessary to have a lot of information about the biometric system.

The basic type of Trojan horse attack is a common brute force attack, when the program just generates templates in sequence and waits for results. At first sight, this method looks hopeless, but it is necessary to realize that positions of minutiae can fit only approximately, their order has not any influence on comparison and it is not necessary to find all of them. For a successful attack, the attacker just needs to acquire sufficiently high comparison score.

The brute force attack can be improved by including some known characteristic of minutiae positions [43]. For example, fingerprint usually does not fill the whole square of an image, so it is possible to generate minutiae positions only into an oval area in the middle of the image and it is also possible to take into account that minutiae positions have usually a uniform distribution.

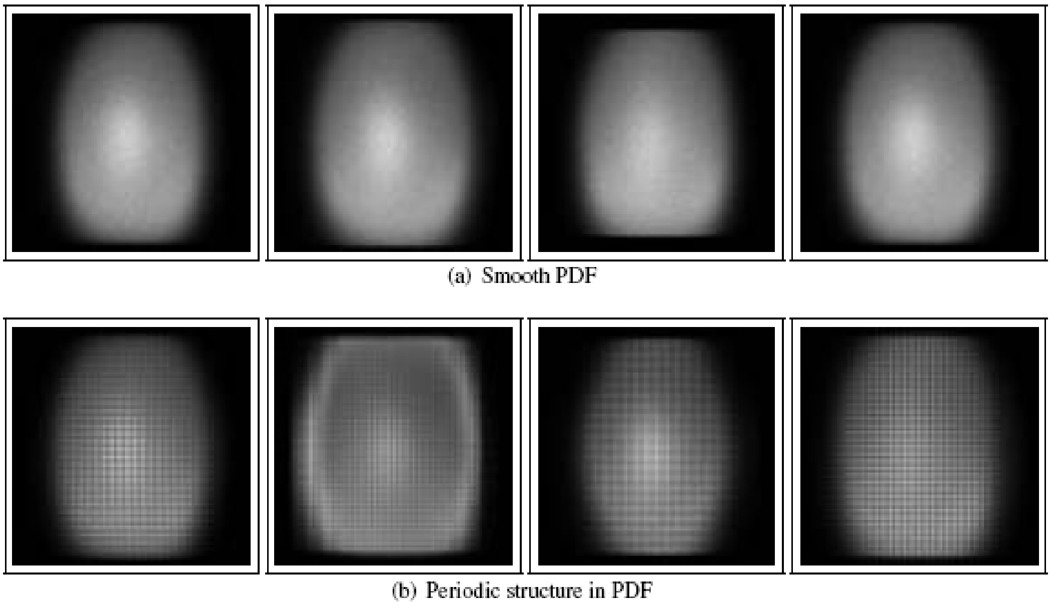
Moreover, it is possible to improve this attack by using of so called Hill-climbing algorithm [3, 43]. In this case, the program generates a random set of minutiae and saves its comparison score. Then it makes a small change and receives new comparison score. If new score is better than the old one the change is accepted, otherwise it is rejected. The program continues and does little changes until the score reach of a threshold value and an identity is accepted.

Another option to improve the brute force attack can be based on the knowledge of weak places of particular algorithm. The MINEX[11] project [66] tested the interoperability of various fingerprint extraction algorithms from different vendors and discovered that some algorithms do not place the minutiae in conformance with the standardized placement. The Minutiae Placement Density Function (MPDF) has shown that their placements created various periodic structures (grids with different spacing – see Fig. 3.8). The knowledge of a particular grid characteristic can greatly increase the success of the brute force attack. This implies that the placement of minutiae in the grid structure (the non-conformant behavior of algorithm) represents another vulnerable (weak) place of the biometric system.

3.5.5 Precautions

The most often mentioned way for securing of templates in database and communication channels is the usage of cryptography [43]. It is proposed to use an asymmetric cryptography for exchange of keys, which will be used afterwards for a symmetric algorithm. It is also

[11] Minutiae Interoperability Exchange Test - NIST's project.



(a) Smooth PDF

(b) Periodic structure in PDF

Figure 3.8: Examples of results of MPDF for different algorithms [66].

recommended to use a timestamp [43], because when the system will encrypt the timestamp together with the sent message (e.g., template), a resultant cipher-text will be different each time and an intruder cannot use the Replay attack.

Nevertheless, there are some problems, which are necessary to solve before using this solution in praxis. It is important to find a way for securing of private keys, consider usage of certification authority and other common cryptographic problems. All these problems have to be solved in relation to particular conditions, in which the biometric system will be used, and with respect to the type of system and reader. Sometimes it is even necessary to consider hardware claims of usage of cryptography. In case of using of the timestamp, it is also necessary to ensure a synchronization of all clocks, which is very difficult task in praxis.

Additional precaution against Hill-climbing attack on communication channels can be increasing of granularity score [43]. In such case, the attacker's algorithm cannot use the score for deciding, if the change was good or bad, and its successful rate will be same as in case of slightly enhanced way of brute force attack.

Another possible precaution is the usage of an extractor, which places the minutiae in conformance with the standardized placement. It is possible to check, whether the extractor places the minutiae in the grid structure, by the usage of the Minutiae Placement Density Function. Nevertheless, this function can detect only one of all possible non-conformant behavior/possible threat. It is necessary to use another approach/methodology, which does not check whether the tested extractor makes a particular error, but which checks whether the extractor places the minutiae in conformance with the standard. Unfortunately, such methodology was not published/created, so I have started my research in this area (see Chapter 5).

In case of the placement of some biometric system components in the PC, laptop or server, it is also necessary to secure these devices. Nevertheless, the securing of these devices is a very comprehensive topic. The individual steps to increase security of computer vary according to the used operating system, the security policy in the company, etc. Some of the security precautions are general enough to be applied almost on every situation [57], e.g., keeping all applications up-to-date, usage of an appropriate anti-virus system and a personal firewall, or do not open spam messages. Nevertheless, these recommendations provide just a basic guideline. The detailed description of this topic is out of the scope of this thesis. This securing of computer is so comprehensive and ever changing topic, so that some companies, people or institutions (e.g., some fingerprint departments) do not connect their computers to the Internet and do not allow file transfer among these computers and computers, which were/are connected to the Internet.

3.6 Problems with users

Attacks on biometric system are not caused only by persons without access to the system, but they can be done by enrollees or other users. In such cases, the goal of such attack is not to get an access to the system, but to discredit the system, grant the access to an unauthorized person or denial of the realized access and thus obtaining some profit.

3.6.1 Sabotage

The often described situation is a sabotage of a biometric system [3, 43]. In such case, users try to take the system or sensor out of service, e.g., by damaging of sensor surface or whole apparatus, by overloading of network or by simple sabotage of the power supply.

However, users can sabotage a particular system in a more hidden way, e.g., by sabotage of capturing process [3]. In case of solution based on capturing of fingerprints, the capture subject can wet the finger or put some dirt on it. The reason for this activity is simple. If the given biometric system has unacceptable high percent of FRR[12], it cannot be used in such conditions and it has to be replaced by other biometric system or removed without replacement.

These kinds of attacks belong in principle into the group of DoS attacks. The motivation of the attackers to a sabotage can be different [3, 43], e.g., extortion, political reasons, or just a personal antipathy to the used biometric system.

3.6.2 Coercion

Another possible attack caused by enrollees is the situation, when the enrollee intentionally grants an access for not-enrolled person [3, 43]. It can happen in case of some agreement between these two persons or because of blackmail.

Some sensors or liveness detection mechanisms have an ability to detect level of stress, e.g., ultrasound sensor, pulse or perspiration measurement.

Moreover, it is possible to give to the enrollee a chance to inform about this problem, e.g., by registering additional fingerprint in the database and using this finger for identification/verification only in crisis. These methods grant access for the capture subject, but also inform the administrator of the system about a possible problem.

3.6.3 Repudiation

Users also can attack the system because of obtaining of some profit. One of the possibilities can be the problem with repudiation [3, 43]. For example, if welfare benefits will be given on the basis of authentication by some kind of biometric system, an enrollee

[12] False Rejection Rate.

can obtain granted benefits and then he/she can claim that he/she did not obtain anything, and ask for it again.

3.6.4 Precautions

The recommended additional precaution is usage of a camera system. This system cannot stop an attacker, but it can be prevention from some kind of attacks. Especially, it can be the prevention of attacks of enrollees/employees, because these persons do not want to have a record of their activity for the system administrator/their employer, or it can be successfully used to avert the repudiation attack.

Chapter 4

Liveness detection

The liveness detection is the first area of the security of a biometric system, which I decided to devote in my Ph.D. thesis.

Nowadays, the easiest way to successfully attack a biometric system is to attack (spoof) the sensor. As it was mentioned earlier (see Section 3.3), there are basically three possible security precautions: usage of liveness/fake finger detection, usage of multiple biometric characteristics and partly also application of cancelable/removable biometrics. The usage of cancelable/removable biometrics protects the stored references against misuse and the biometric fusion reduces the success rate of sensor spoofing due to necessity of spoofing of two different biometric characteristics. It follows that the implementation of liveness/fake finger detection plays a crucial role in the sensor securing.

It is necessary to find answers to the following questions:

- Which approaches to the liveness detection have been published? Which sensors on the market have the ability to detect liveness?
- What are the advantages and disadvantages of the existing approaches/sensors?
- Which conditions should the liveness detection method meet?
- Is it possible/How to propose a method, which meets these conditions, which avoids the common errors of the existing approaches/sensors and which has better results than (or at least as good results as) the published test results of existing sensors/approaches?

4.1 Published methods

In the last years, researches developed several methods, which are or can be used for the liveness detection purposes. Generally, there are two approaches to sort them. The first approach was presented by Valencia et al. [70]. They divided all methods into three categories: intrinsic properties of live human body/finger (e.g., spectral or electrical properties), generated signals (e.g., pulse or perspiration) and responses to a stimulus.

Another approach was presented by Wei-Yun et al. [74]. They classified methods into purely software-based, purely hardware-based methods and methods, which need more information (pictures or measurements) for their function.

In this section, I present a brief overview of the known methods of liveness detection with their advantages and disadvantages. I did not divide these methods in any previously mentioned categories, because in a lot of cases, the methods can belong into more or no one of the mentioned categories.

4.1.1 Optical properties

There are several properties, which can be optically detected. The first of them is color of skin, the second are spectral properties of human tissue and the third is elasticity of human skin/tissue.

The detection of the color itself cannot be used as the liveness detection method, because it is very easy to create an artificial finger with the appropriate color of skin. The only one possibility is to use the detection of a color change caused by pressing the finger against a solid surface, because due to the pressure the color of finger is altering from reddish to whitish/yellowish [27, 34, 38, 70, 74].

Nowadays, there exist a few approaches to measure the color change. The first approach was patented by Igaki et al. [27]. They proposed an apparatus, which illuminated the pressed and not-pressed fingertip with the green light and measured reflectance in G and B component of the RGB (Red-Green-Blue) model of colors. As far as I know, this approach was not implemented in any fingerprint sensor on the market.

Another approach based partly on measuring of the color change was presented in my master thesis [38]. The color is measured in a slightly different way and its change is detected continuously and tested more complexly. This method is described in detail in Section 4.3.1.

An alternative approach was presented by Wei-Yun et al. [74] in summer 2007. They proposed simple sensor with a glass plate, camera in the bottom side (5Mpx resolution) and side illumination with white LED diodes (so that the captured samples of gelatin fake fingers look as their borders are slightly shining). They use one pressed and one not-pressed image of a finger, convert them from RGB to CIELa*b* color space and divide them into square blocks. For each square block, they compute a probability that the block belongs to the pressed or not-pressed finger or something else (by the use of chrominance component, homogeneity detection, etc.). Then they decide (according to the predefined threshold), whether the finger is alive or not. They have tested this method by the help of 25 volunteers and same amount of gelatin fingers and they achieved only 80% successful rate. On the other hand, they admit that the unspecified amount of fake fingers was rejected even before pressing due to exceeding of the inhomogeneity threshold (the bubbles in gelatin), so these fake fingers were not actually tested for the presence of color change.

The second optically detected group of properties are the spectral properties. Testing of spectral properties is one of few methods implemented in praxis. It was developed and patented by Lumidigm Inc. [22, 54] and its principle consists in testing of properties of various skin/finger layers. The finger is illuminated by LED diodes with various wavelengths in sequence. One from possible hardware configurations consists from 72 LED diodes and a common monochrome CCD camera. Wavelengths of diodes are carefully selected, so each of them penetrates into another depth and is reflected by another component of live finger.

Lumidigm Inc. calls this technology MSI (Multispectral imaging) and uses it in their fingerprint sensors in Venus series. Lumidigm claims that this technology is very successful and can work better than other sensors with dry, wet or only slightly-touched fingers. In one of their patents [55], they also claim that this method is capable to detect a level of alcohol in blood, which can be very useful in some employment.

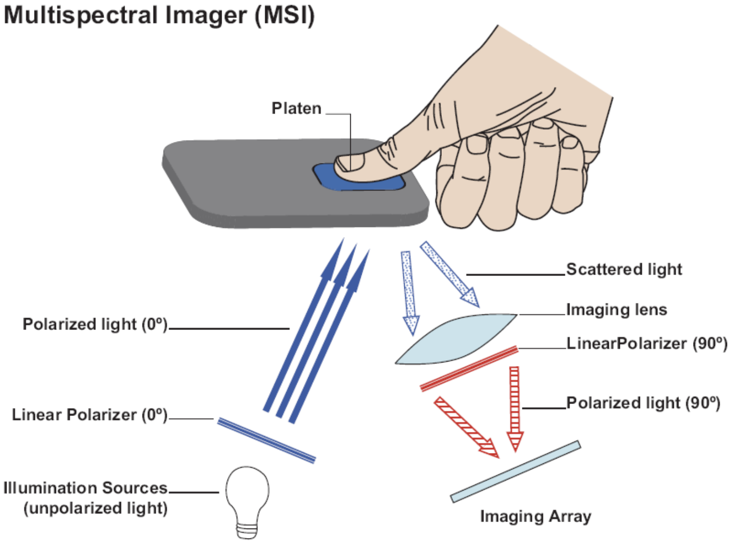


Figure 4.1: Schema of the Multispectral imaging process (MSI) [22].

On the other hand, Lumidigm does not describe any details of its method and it does not exist any independent test of this sensor. From this and other reasons, we prepare careful testing of this sensor/principle.

Another utilizable characteristic property of live human skin/tissue is the elasticity. The first method using this property for liveness detection purposes was patented by Brownlee et al. [12]. Their method uses prism (or micro-prism) and two light sources; the first one is the normal light source, which illuminates the plate in vertical direction, and the second one uses diffused light and illuminates the plate under the specific angle. The proposed sensor captures two images (each with different illumination) and compares appearance of pressed and not-pressed papillary lines. As far as I know, this approach was not implemented in any fingerprint sensor on the market and it was not published any test of this approach.

Another approach based partly on elasticity detection I have proposed in my master thesis [38]. I tested the elasticity of skin by continuous measuring of change of papillary lines width during the process of pressing of finger against glass plate. The detailed description of this approach can be found in Section 4.3.1.

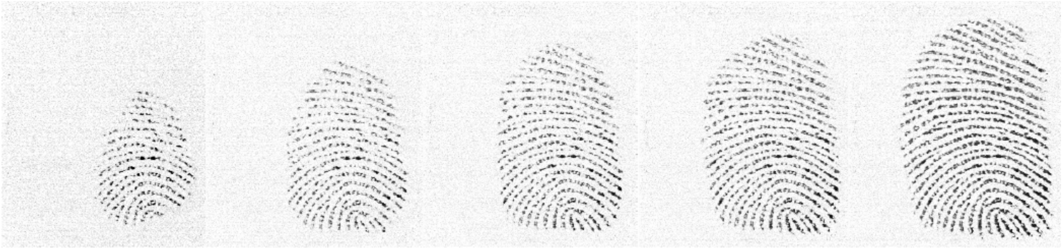


Figure 4.2: Sequence of fingerprint images illustrating elasticity of skin [32].

Different approach was presented by Jia et al. [32]. They capture sequence of fingerprints during the process of putting of finger on sensor surface (see Fig. 4.2). Their algorithm computes a correlation coefficient of fingerprint area, average signal intensity and extension of fingerprint area, and on the basis of these coefficients it decides, if the captured sample is alive or not. They tested their approach using 15 volunteers/colleagues (1 finger and ten sessions per each volunteer) and 22 fake fingers made from gelatin on the Veridicom capacitive fingerprint sensor. Nevertheless, their Equal Error Rate was still quite high (EER 4.78%).

4.1.2 Electrical properties

There exist several electrical properties of live human skin/finger, which were broadly discussed. First of them is conductivity. Putte et al. [48] tested a possible usage of this property for liveness detection purposes and found out that the conductivity is dependent on type of skin and environmental conditions, so that an interval of possible values is too wide (from several $k\Omega$ for wet skin in summer to the several $M\Omega$ for dry skin in winter).

Another property tested by Putte et al. [48] was relative dielectric constant (RDC). They proposed a method for spoofing of liveness detection based on RDC measurement. They proposed to dip an artificial finger in dilution of alcohol (90%) and water (10%). The RDC of alcohol is lower than the RDC of water, and because alcohol evaporates more quickly, the RDC of dilution is growing. After some time the RDC will reach the value, which is typical for live human skin.

In 2001 Sony started to sell its optical sensor FIU-500 with liveness detection based on capacitance measurement [70]. Unfortunately, details are not known, but it seems that this idea was not successful. Nowadays, this sensor is not sold in the market any more and its successors do not have any liveness detection capability.

The promising property for liveness detection purposes is impedance. Nowadays, there are several ways to test it. One of them was proposed by Shimamura et al. [61]. They place a very small cross-shaped electrode in the middle of common capacitive fingerprint sensor (see Fig. 4.3). The sensor captures a fingerprint at first and then it measures the impedance. This two-phase way of work can be a problem, because an attacker can exchange an artificial finger with the real one.

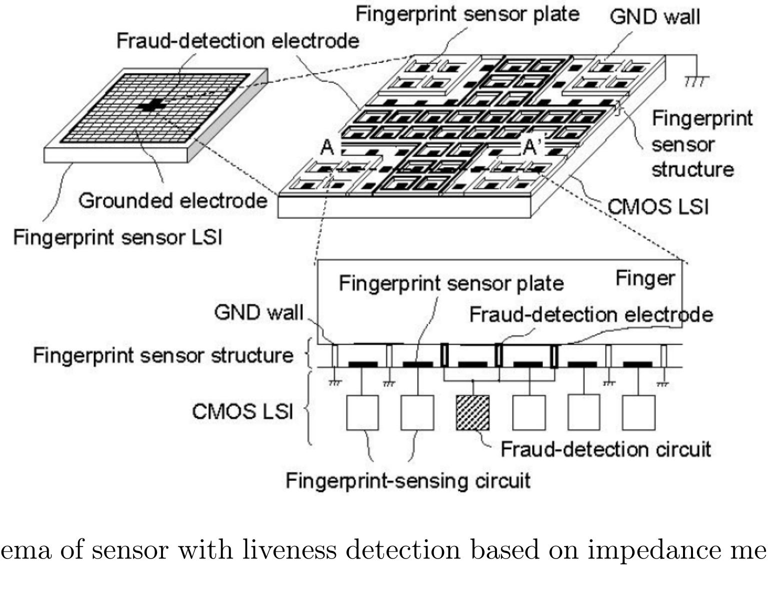


Figure 4.3: Schema of sensor with liveness detection based on impedance measurement [61].

Another method of liveness detection by impedance measurement was patented by Martinsen et al. [44]. They proposed a capacitive sensor, which contains at least 4 electrodes, which can work in at least two different four-point configurations. They claim that it is possible to measure impedance of different layers of skin by switching between these configurations and so to test the liveness.

4.1.3 Biomedical properties

Another group of properties for the purposes of liveness detection are the biomedical properties. This group includes the pulse, blood oxygenation, blood pressure, perspiration, etc.

Detection of the heart activity is often mentioned possibility how to test liveness. There exist several approaches to measure it; because the detection of pulse can be a side-effect of methods for detection of some characteristic properties of live human fingers, e.g., ultrasound waves reflection, spectral properties or blood oxygenation.

Novel method, which deals with detection of pulse, was proposed by Assoc. Prof. Drahanský et al. [17, 19]. They measure small volumetric changes caused by pulse. There are two approaches for measuring these changes. The first approach is optical-based (measuring distances between papillary lines in a video-stream) and the second approach is based on laser distance measurement (detection of volumetric changes – see Fig. 4.4). In both cases the measured distances are in μm.

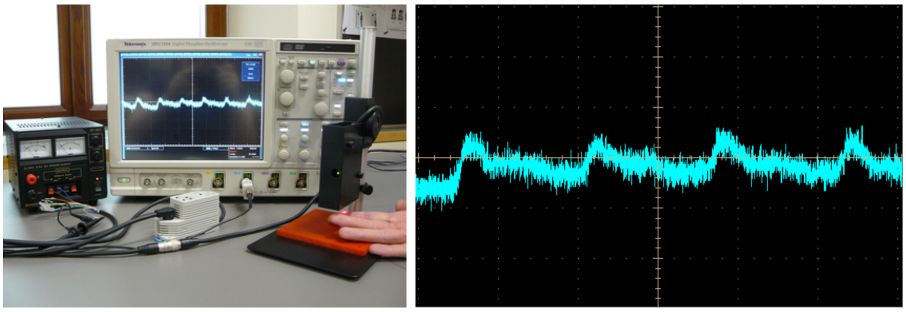


Figure 4.4: Left: the measurement of heart rate by the module for the detection of volumetric changes (laser distance sensor Panasonic LM10 ANR1250). Right: the resultant sample of heart rate displayed by the oscilloscope Textronics DPO 7254.

A possible problem of every liveness detection method based on pulse detection is a big difference in pulse frequency among people and also among different sessions of one human. These differences can be caused by health or emotional status or by previous physical activity (e.g., the capture subject running up the stairs or using an elevator). Another disadvantage is a long time necessary for detection of pulsation.

Detection of blood oxygenation can be measured by the help of a pulse oxymeter, which is commonly used in hospitals. Its principle is based on a Beer-Lambert's law [33], which relates absorbance of light at specific wavelengths to the concentration of corresponding substances. In case of pulse oxymeter, the absorption rate of wavelengths 660 nm and 940 nm corresponds to the concentration of reduced and oxygenated hemoglobin [33].

The advantage of this method is its wide use in praxis and also its possibility to detect pulse. On the other hand, the disadvantage is a long detection time (about 5 seconds) and the possibility to spoof this method by using a very thin artificial finger. As far as I know, it does not exist any fingerprint sensor on the market, which uses this method of liveness detection.

Another discussed property is blood pressure [48, 70]. Nowadays, this property cannot be used for fingerprint sensors, because current noninvasive techniques for measuring of blood pressure need to use two places at the human body.

Prof. Schuckers et al. [59] from BioSAL[1] laboratory proposed a liveness detection method based on detection of perspiration process. They measure a change of moisture of finger in time, as can be seen in Fig. 4.5. In the left fingerprint, we can see little dark areas – the sweat concentrated in neighborhoods of sweat pores. In next two fingerprints, it is possible to trace spreading of sweat (dark color) along papillary lines.

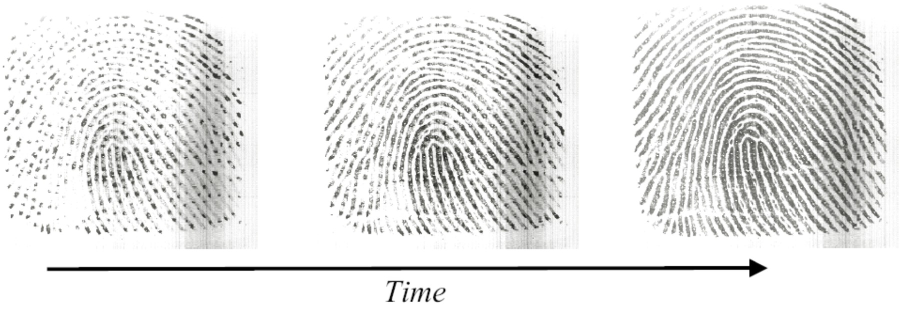


Figure 4.5: Spreading of sweat along papillary lines [59].

Although, the principle of this method looks easy, the algorithm itself is quite difficult. At first, two images are captured. The first image is captured at the beginning of perspiration process and the second image after a few seconds. Then both images are enhanced and transferred into a signal, which values indicate levels of gray in image. Afterward, several classifiers of images are computed (e.g., distance among sweat pores in each image or differences between both images). On the base of these classifiers, the algorithm will decide if the finger is alive or not.

The advantage of this method is its possible use on more types of fingerprint sensors (it was successfully tested on optical, capacitive and electro-optical sensors) and also its purely software-based implementation. But the problem is its higher False Acceptance Rate (approx. 10% FAR) and quite long time necessary for perspiration process.

4.1.4 Other possibilities

There exist a lot of other properties, which were discussed in connection with liveness detection by fingerprint sensors. One of them is temperature [48, 70], but there is a problem with big interval of possible values and also the possibility to heat up an artificial finger on the body temperature. Therefore, experts suggest using temperature gradient.

Mr. Bicz from Optel [9] claims that their ultrasound sensors have an inherent liveness detection capability. He claims that an ultrasound signal is in sentence reflected from different layers of skin/finger. He claims that the difference between signal from live finger and the artificial one can be seen in its amplitude and „character“, e.g., after FFT[2].

As an advantage of this sensor, he mentioned a capability of pulse detection and measurement of stress level. Unfortunately, it does not exist any independent test, which could confirm or disconfirm ability to test liveness and it is not possible to buy the described sensor in the market.

[1] Biomedical Signal Analysis Laboratory at Clarkson University and West Virginia University, USA.

[2] Fast Fourier Transform.

A method for testing of body odor was proposed by Baldisserra et al. [5]. They proposed to use an electronic nose, which consists from array of chemical sensors, which are able to detect molecules evaporated from the surface of tested object.

This method is cheap and innovative, but unfortunately, it has few serious problems. The first problem is the placement of sensors, because chemical sensors have to sense the same part of finger, which is captured for identification/verification purposes. Another problem is the low speed of scanning (10 - 15 seconds per sample), because sensors need to sense the background before scanning another sample. The most serious problem is the usage of common gelatin fingers, because in this case the response of chemical sensors is very similar to the live human fingers.

Another discussed methods are, e.g., a detection of skin exudation (shedding of dead skin cells) [70] or a patented method based on usage of radiation source and detector [7].

4.2 Analysis

Before creating a new method of liveness detection, it is necessary to analyze and compare the existing liveness detection methods (see Section 4.2.1), to study the principles/posibilities of sensors claiming to include some kind of liveness detection module (or software) together with published results of their tests (see Section 4.2.2) and try to find the requirements, which should be met (see Section 4.2.3).

4.2.1 Comparison of published liveness detection methods

The brief comparison of liveness detection methods described in Sections 4.1.1 – 4.1.4 is given in Table 4.1. It can be seen that a lot of methods have been published without test results mainly because the principle was described in patent, which was not followed by publication of test results in proceedings, journal or web pages of a particular company.

As far as I know, there are only a few methods with published test results and the number of their tested subjects and used materials of fake fingers varies significantly. Unfortunately, the authors often do not publish the statistical characteristic of group of tested subjects (e.g., age distribution, gender, ethnicity, presence of diseases or hobbies affecting fingerprints). The description of materials used for creation of fake fingers is also limited, which could cause a problem. The proportion of particular ingredients in some of the commercially available compounds varies from one country to another, which could cause the different optical or electrical parameters of created fake fingers.

4.2.2 Situation on the market of fingerprint sensors

Nowadays, more and more fingerprint sensors on the market include (or claim to include) some component/method for liveness detection (see Tab. 4.2). The manufacturers claim that their solution contains some kind of liveness detection mechanism. Unfortunately, the situation is not so good as it looks like. In many cases, the principle of their solution and the results of tests are unpublished and the sensors are (in some cases very easily) deceivable (according to my own experience and the results of independent tests [11]).

Some manufacturers assume that the security of their solution will be higher, if they keep its principle hidden (so called „Security by obscurity“ [37]). Unfortunately, it is a common mistake. If an attacker needs this information, he/she will find it, because there is always some way how to obtain it (e.g., unsecured place in computer network, or blackmail). An unpublished principle can hide some kind of mistake, which can create so called „back door“ for possible attackers. On the other hand, a possible error in published principle can be found and fixed, so that publishing can really improve the security of solution.

Table 4.1: Comparison of published (and previously described) liveness detection methods. The dash indicates that the approach has not been tested or the test results have not been published.

Authors	**Tested property**	**Error**	**Volunteers**	**Fakes (materials)**
Baldisserra et al. [5]	odor	EER 7.48%	15	9 (3)[3]
Benaron et al. [7]	radiation	-[6]	-	-
Bicz et al. [9]	ultrasound	-	-	-
Brownlee et al. [12]	elasticity	-[6]	-	-
Drahanský et al. [17]	pulse-optical	-	3	-
Drahanský et al. [17]	pulse-laser	-	7	-
Igaki, et al. [27]	color	-[6]	-	-
Integrated Biometrics [94]	electro-optical	-	-	-
Jia et al. [32]	elasticity	EER 4.78%	15	22 (1)
Lumidigm [105]	MSI	-[6]	-	-
Martinsen et al. [44]	impedance	-[6]	-	-
Putte et al. [48]	conductivity[4]	-	-	-
Putte et al. [48]	RDC	-	-	-[5]
Schuckers et al. [59]	perspiration	FAR 10%		
Shimamura et al. [61]	impedance	0	1	2 (2)
Sony [70]	capacitance	-	-	-
Wei-Yun et al. [74]	color	FAR 20%	25	25 (1)

Table 4.2: Overview of sensors with liveness detection capability [40]. The question mark means, that this company did not publish the principle of their solution.

Manufacturer	**Codename (tested property)**	**Sensors**
AuthenTec [78]	TrueFinger^{TM}(?)	EntrePad 1610
Dermalog [87]	(?)	ZF1
Integrated Biometrics [94]	LES (electro-optical)	LES650, ...
Lumidigm [105]	LightPrint^{TM}(spectral)	J110, Venus series
Optel [112]	(ultrasound)	ultrasound camera
Sagem Morpho [116]	(optronic ?)	MA521, MSO201, ...
Sony [70]	(capacitance ?)	FIU-500
TBS [124]	(?)	TBSGuard 3D-Terminal, ...
TST Biometrics [123]	optical (?)	BiRD 3
Upek [127]	(?)	TCS5

[3] The fake fingers made of organic materials (e.g., gelatin) are able to spoof this sensor.

[4] Huge interval of possible values of live fingers.

[5] This approach can be spoofed by fake finger soaked in an alcohol-water dilution.

[6] This approach is patented. Unfortunately, no test results have been published.

Nowadays, the standard for liveness detection ISO/IEC 30107 (Anti-Spoofing and Liveness Detection Techniques) is under preparation [95]. This standardization project is in the 3rd Working Draft phase[7] and it should contain (among others) necessary terms, concepts and error rate metrics [46].

4.2.3 Requirements

After careful study of known methods and their problems described in Section 4.1, I found some requirements/conditions, which a successful method has to meet, and some problems, which it has to avoid or solve.

The first group of requirements for method of liveness detection is very similar to the requirements for biometric characteristic (see Section 2.2.2). The requirements for universality, permanence, collectability and acceptability of liveness detection method/characteristic can be defined the same way as the corresponding requirements for biometric characteristics.

In case of requirement for distinctiveness, we do not need to differentiate between individuals. Samples from live human fingers create one class; gelatin fingers can create second class, silicon fingers may create the third one, etc. In this case, the tested property/method has to have high intra-class variability and low inter-class variability. This requirement is the reason, why the property with a wide range of accepted values (e.g., temperature) cannot be used for liveness detection purposes.

The performance requirement consists of same conditions in both cases, e.g., accuracy, speed, costs, or possibilities of application. Nowadays, the best accuracy has been achieved by perspiration detection method proposed by Prof. Schuckers et al. [59] (approx. 10% FAR) and by elasticity detection method proposed by Jia et al. [32] (EER 4.78%). Moreover, the time necessary for authentication has to be very short (2 seconds or even less), otherwise the application of this method will be very limited in praxis. The problem how to meet this criterion has, e.g., odor analysis proposed by Baldisserra et al. [5].

The most difficult requirement is the security requirement. It is impossible to claim, that some property and method of its testing is and will be forever 100% spoof-proof. On the other hand, it is necessary to ask for resistibility against known methods of spoofing.

Even if the property meets all previously described requirements, there is the second group of requirements, which result from integration of this method into some fingerprint sensor [38]:

1. **Measuring of same area.** In case of fingerprints, it is necessary to measure properties of a fingertip. For example, it is not appropriate to test a pupil dilatation, because an attacker using an artificial finger will pass this test without any problem. It is also problematic to test side part of a finger, because the attacker can have a very thin artificial finger glued only on fingertip.

2. **Concurrent measuring.** It is necessary to test liveness and capture fingerprint in the same time, otherwise an attacker can use artificial finger in the capturing process and his/her real finger in liveness detection process. In case of testing of some process (e.g., change of some characteristic), it is necessary to monitor and test this characteristic during the whole process, otherwise the attacker can create two different fingers, which simulate situation at the beginning and at the end of the process, and exchange them without any problem.

[7] See the brief description of standardization process in Appendix B.

3. **No interaction.** Because there are two measurements (liveness detection and fingerprint capturing) in the same time and place, it is necessary to use such pair of sensor and method, which will not interact with each other.

While using liveness detection, it is also necessary to think about privacy, because a side-effect of many possible liveness detection methods is the detection of some private things, e.g., health status, race, stress level. Such information can be easily misused, so if it is necessary to store them, then they have to be protected, e.g., by cryptography. At the end, it is necessary to publish the principle of securing to avoid effects of Security by Obscurity principle.

4.3 Novel liveness detection approach

After a thorough study of existing methods for liveness detection, it was possible to propose novel method/approach, which meets the proposed requirements and avoids the problems of existing solutions. The principle of this novel method is described in Section 4.3.1 in detail and the description of possible (and patented) hardware configurations is given in Section 4.3.2.

4.3.1 Principle

I proposed a novel approach based on combination of detection of two characteristics of live human fingers; change of color and elasticity due to pressing of finger against glass plate.

Under normal circumstances, a live human finger is reddish and its papillary lines are approx. 0.2 – 0.5 mm wide[8]. Due to the pressing of finger against glass plate, the height of papillary lines decreases so that the lines optically appear to be thicker and the blood is partly relocated from the pressed skin area so that the skin turn to yellowish/whitish [39]. Once the pressure on the finger is decreased (or eliminated), the papillary line color and optical thickness immediately come closer (returns back) to its original state. However, the percentage of extension of width of papillary lines and its color are not always the same. The rate of change is proportional to the force of finger pressing.

The color of finger (and also the color change) can be detected using various color models. During my proof-of-concept tests (see Section 4.4.1), I experimented with various color models [39], e.g., RGB, HLS[9] or CIEL*a*b*. The results of experiments with HLS color model shows that this model is not convenient for purposes of this liveness detection due to the high intra-class variability.

The results of proof-of-concept tests in case of CIEL*a*b* color model were much better. Due to pressing of finger against surface, the L* value (lightness) is increased. The chromatic value a*, which represents an axis from green to magenta, is significantly decreased and b* chromatic value, which represents an axis from blue to yellow, is increased. Nevertheless, I decided to not use this color model, because the initial b* chromatic value is highly dependent on the race of volunteer, and this dependency I consider inappropriate.

The results of RGB color model are more definite and proper. The biggest difference can be seen always between G components. The other differences are lower as follows:

[8] The width of papillary lines differ from one person to another, but it depends on various conditions, e.g., age of person.

[9] Hue-Lightness-Saturation color model.

$$(\bar{G_2} - \bar{G_1}) > (\bar{B_2} - \bar{B_1}) > (\bar{R_2} - \bar{R_1}) \tag{4.1}$$

where $\bar{X_2}$ is average value of X in center of image of pressed finger, $\bar{X_1}$ is identical calculation for image of non-pressed finger, where X is particular component in RGB color model.

The optical comparison between non-pressed and pressed finger for full RGB image and also decomposed individual components can be found in Fig. 4.6.

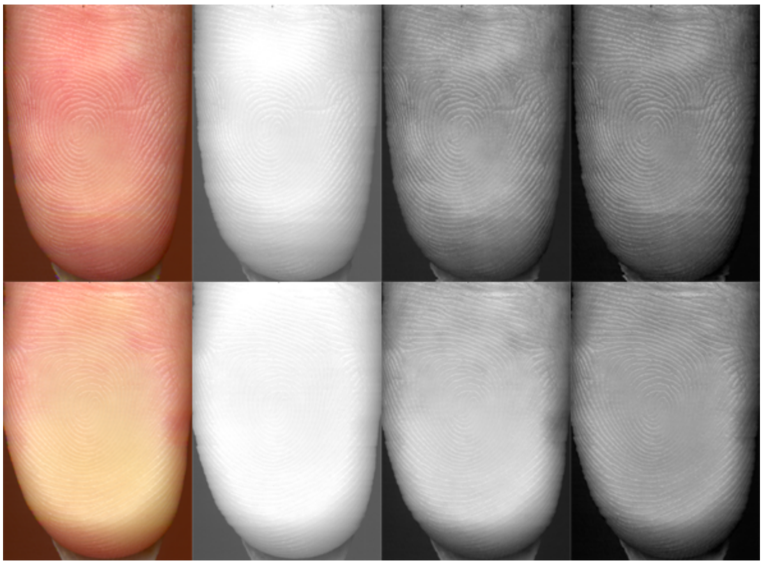


Figure 4.6: Comparison of the non-pressed finger (in the first row) and the pressed finger (in the second row). In the first column (from the left), there is the finger in all RGB colors. In the second column, there is only the R-channel, the G-channel is in the third and the B-channel is in the fourth column. The difference between average R values is 11, G 42 and B 20.

The width of papillary lines (and its change) could be detected in various ways. Above all, it will be necessary to choose an appropriate edge detector. There is a lot of edge detection methods, which are suitable for this purpose [26], e.g., Sobel filter, Gabor filter, or Canny edge detector. According to my opinion, the choice of appropriate method will be highly dependent on the used illumination source(s) mostly considering the angle of light. Moreover, the structure of used pipeline will be important, e.g., usage of appropriate image pre-processing/post-processing techniques.

As it was described in Section 4.2.3, the successful liveness detection mechanism should meet a lot of requirements. According to the described biological principle of both tested characteristics of live human finger, I suppose that the requirement for universality and permanence should be met. I do not expect any problems according to the acceptability requirement. Nevertheless, I decide to verify these assumptions (at least partly) during selected tests by choosing of volunteers of different age, gender and race, and by tests of larger group of volunteers. The requirement for collectability was tested (and met) during proof-of-concept test and the performance and distinctiveness will also be tested.

The requirement for concurrent measuring of the same area without interaction is met in the basis of the method proposal. The liveness detection measurements do not require any special illumination or other interfering hardware, so it is possible to run these measurements simultaneously with the capturing of fingerprint by common optical fingerprint sensor without any risk of negative interaction.

Regarding the requirement for security, it is necessary to ask for resistibility against the known methods of sensor spoofing. There is a lot of possible ways to create artificial finger of appropriate color, but (as far as I know) there is no skin-color material, which will be able to change color same way as the pressed finger.

The possible way to pretend the color change is to exchange two fake fingers[10], each of different color or to use two inks and to soak the stamp in the second ink during the capturing process. I have tested exchange of two samples using the Nikon camera (30 fps) and the speed of exchange was only 0.07 sec [38]. Nevertheless, this situation cannot spoof the proposed liveness detection unit, if the continuous monitoring of the color change will be implemented and the camera with high frame rate will be used.

Forgery of change of papillary lines width is also a non-trivial task. As far as I know, the elasticity of materials for fake finger creation has not been so widely tested. Thus, it is not possible to exclude the eventuality, that some of the commonly used materials can have similar properties to the live human skin.

Generally, the common materials usable for fake finger creation to imitate the elasticity of the live human skin can be divided into three groups: pressure resistant materials (e.g., sheet of rubber from a common office stamp), ordinary materials (e.g., gelatin or latex are often used), and soft (easily deformable) materials. In case of pressure resistant materials, the change of papillary line width should not be visible. It seems logical to use soft/easily deformable materials and to forge the change of papillary line width by controlling the pressing force. However, such fake finger often are not be able to forge the reverse change (decrease of the pressure and lifting of finger from the sensor surface) due to the slow or even non-existing memory effect of material. Nevertheless, it is necessary to test various materials during the tests of this approach.

Another possible approach to imitate change of width and color of papillary lines could be the usage of thin semi-transparent fake finger. Nevertheless, the creation and usage of such fake finger could be very difficult (or even impossible), because there are two opposing requirements for the level of transparency. These fake fingers have to be transparent enough to be possible to clearly see the color change, and non-transparent enough to be possible to clearly see the papillary lines on the fake finger surface non-interfering with the papillary lines from the live finger behind. Moreover, it is necessary to take into account that if the material is not as hard as glass; the finger has to be pressed significantly stronger to achieve same color change, which influences the change of width of papillary lines on the fake finger surface. Another possible complication for the attacker could be the fact that a lot of commonly used transparent (or semitransparent) materials often contain significant amount of bubbles.

One of the often discussed ways to spoof fingerprint sensor is the usage of dead finger. The capturing of the dead/removed finger may be difficult. Rutty et al. [56] proved that the fingerprinting in such situation depends on the status of the used finger. Nevertheless, it is also known that the color of human skin is conditioned by the circulation of the blood and that the skin due to the lack of blood circulation turns pale/grayish (*pallor mortis*) [28, 60]. According to the study of Dr. Shäfer [60], the paleness of skin develops rapidly and it can be

[10] It is not possible to use two printed fingerprints or two photographs of finger, partly due to continuous monitoring of the color and width of papillary lines change of course, but also partly because of insufficient resolution of such fake in these days.

easily optically distinguished from the common live skin color. The following post-mortem change of skin color is turning dark purple (*livor mortis*) [28]. This change is caused by gravity and thus it is present only in the lower part of the body. During first few hours after death, the dark purple parts of skin can turn whitish after applying pressure, but later, this effect is not observable.

According to the above described color changes of dead skin, I suppose that my liveness detection approach could be capable to identify the dead finger as a fake finger. Unfortunately, it was not possible to test my approach using the cadaver fingers as Prof. Schuckers et al. [58] did, although I intended to do it.

Generally speaking, the elasticity could be a little bit weaker than the color change, but coupled together they can create very strong barrier for the possible attacker. The proposed approach could also deal with the capturing of dry, wet or bended skin, which can be an advantage in comparison with other approaches. Another advantage of this approach is that this method needs not wait until some physiological process (e.g., perspiration or several heartbeats) takes place. When using the hardware with appropriate parameters, the speed of the whole system is limited only by the quality of algorithm implementation. On the other hand, there is also a disadvantage. The proposed approach can have a problem with a high percentage of skin contaminated by colored material (e.g., ink, chalk or some chemical substances), so the possibilities of deployment of this sensor could be slightly limited. On the other hand, a lot of sensors on the market has similar problem (according to my experiences).

4.3.2 Proposed hardware configuration

According to the previously described requirements and the software principle of new method, we (me in cooperation with Assoc. Prof. Drahanský) have proposed the hardware schema of the possible liveness detection unit. This unit can be integrated into an optical fingerprint sensor or it can be used as a sensor with the liveness detection ability (after a few necessary adjustments). In comparison with other partially similar approaches, the proposed liveness detection unit does not need any specific illumination sources (it is not necessary to have diffused light [12], green light [27] or side illumination of finger [74]), the common white LED diodes or other ordinary light sources in various locations should be sufficient.

As it can be seen in Fig. 4.7, the whole unit consists of two camera modules, prism, optics and glass plate. First camera (camera module) will be used for detection of papillary lines width. It is necessary to use the camera with good quality optics to achieve the sufficient magnification of papillary lines, but the camera can have lower image framerate and it can use gray-scale image/video stream.

The second camera has to follow the process of color change, so it has to produce a video stream with color images (lower resolution is possible). Nevertheless, this camera will be also used for detection of possible attacks (e.g., by switching two different artificial fingers). Because this kind of attack can be done in 0.7 s [38], it is necessary to have the camera with high image framerate (30 images per second or better).

It is possible to use only one camera module, but in such case, the „united module“ would have to meet all requirements for both separate camera modules. Such solution is currently more expensive and the possibilities of miniaturization (and therefrom resulting possibilities of integration into optical fingerprint sensors) are limited too.

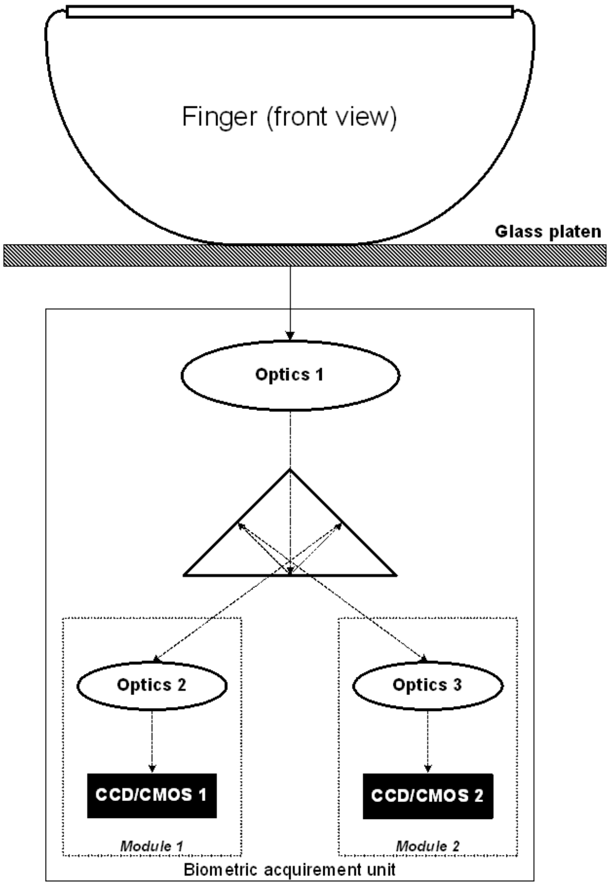


Figure 4.7: Schema of the proposed sensor [38].

During the work on this liveness detection unit, it appeared that it could be a good idea to apply for assigning of a utility model. Therefore, we created an application called: „Liveness testing on fingers by invocation of optical changes", where we proposed a liveness detection unit. The proposal has been accepted as the Czech utility model No. 19364 by Czech industrial property office in 2009.

For the purposes of testing of my approach, a new optical bench has been created (see Fig. 4.8 a). The bench consists of body, camera mounting module, camera (or other capturing device or other sensor generally), special fingerprint module, and mounting module. This optical bench is designed as multi-functional, so both mounting modules allow to set an arbitrary position (in the corresponding axis) and also to mount different sensors/fingerprint modules, so the whole unit can be used for testing of different configuration and even different ideas (not even for the liveness detection purposes).

I have designed a special fingerprint module (see Fig. 4.8 b) for the purposes of testing of my approach. This module is intentionally robust, because during preliminary tests, volunteers often feared that they could destroy the facility by pressing too hard. For higher user-friendliness, the module has an entrance for a finger from both sides.

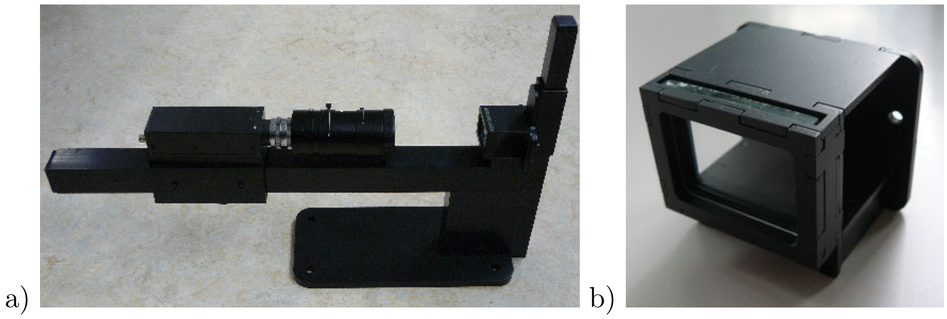


Figure 4.8: a) The special optical bench with fingerprint module. b) Detailed image of the fingerprint module.

4.4 Preliminary tests

I have conducted three consecutive preliminary tests for the purposes of thorough testing of basic ideas of the proposed liveness detection approach and testing of compliance with the basic requirements. The first test was a proof-of-concept test performed to test the basic idea of my approach by the use of minimal hardware equipment. The second test was performed on the large group of people to test mainly the acceptability of the approach and partly even universality, security and of course functionality of the newly built pre-prototype and correctness of the basic idea. The third test was focused on the possible improvements of the pre-prototype and the basic overview of possible algorithms for an automatic papillary line width detection.

4.4.1 Proof-of-concept test

Before I completed the optical bench and the pre-prototype of the liveness detection unit, I had performed the proof-of-concept test for checking of the basic idea of this approach.

I put together a small group of volunteers of different genders and races (Caucasian, African, and Asian). For capturing of fingerprints, I used common office scanner, and I captured 12 images per each volunteer; right thumb and index finger in 3 sessions and 2 images per each finger and session (pressed and non-pressed state). Due to the high resolution (1200 x 1200 dpi) the capturing of one fingerprint takes approximately half a minute, which was very uncomfortable for the volunteers.

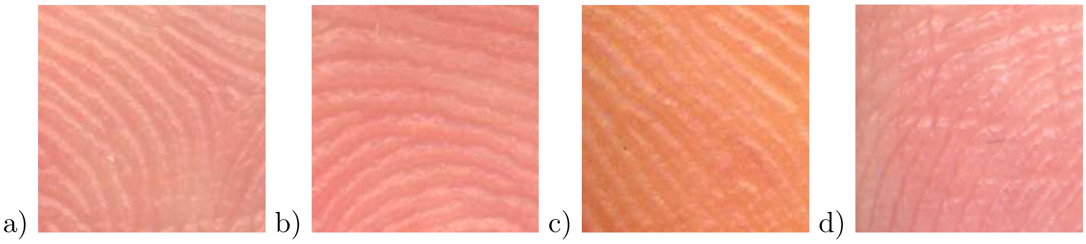


Figure 4.9: Similarity of finger color of different volunteers: a) woman, 25 years, Caucasian, b) man, 24 years old, Caucasian, c) man 24 years old, African, d) man, 25 years old, Asian.

The colors (and the color change) of papillary lines in case of different volunteers appear to be sufficiently similar, see Fig. 4.9. For the purposes of more detailed analysis of the captured fingerprints and demonstration of the functionality of my approach, I have created a simple program called „Demonstration of Liveness Testing Method“. The values of RGB components are determined using median, the papillary lines are visualized using Sobel operator and determined manually (the detailed description and screenshots can be found in Appendix D). Using this program, I experimentally determined the ranges of RGB components for pressed and non-pressed fingers captured by common office scanner (see Table 4.3). The changes of width of papillary lines were in the range from 10 to 40%. Nevertheless, the enlargement of papillary lines depends on the pressure force and also on the precision of the manual determining of papillary line width in loaded images.

Table 4.3: Experimentally determined ranges of RGB components for fingerprints captured by a common office scanner.

	R	G	B
non-pressed finger	225-240	155-175	125-140
pressed finger	235-255	200-220	150-165

Due to the very small number of volunteers and atypical illumination and capturing, these values cannot be perceived as mandatory for all people, various sensors and illumination types. These values serve as the preliminary confirmation of the collectability (and partly universality) claim and of course as the check of the basic principle.

4.4.2 Preliminary tests on a large group of people

The second test was performed on the large group of people to test mainly acceptability of the approach and partly even universality, security and of course functionality of the newly built pre-prototype and correctness of the basic idea.

This test was conducted in winter semesters 2009/10 and 2010/11. The capture subjects were 320 students (the statistical characteristics can be found in Table 4.4). Students worked with the new optical bench. The optical bench was equipped with Sony XCD-SX910CR color camera, Computar MLH-10X macro zoom lens and my special robust fingerprint module, which allows the entrance of finger from both sides. A captured finger was illuminated by two white LED diodes, which position (angle and distance) can be/was altered by students. The captured fingerprints were analyzed using the program „Demonstration of Liveness Testing Method“ (see Appendix D).

Table 4.4: Statistical characteristics of capture subjects in the second preliminary test.

	Study year			**Sex**		**Total**
Year	**1**	**2**	**3**	**M**	**F**	
2009	50	92	20	150	12	**162**
2010	45	93	20	154	4	**158**
Total	95	185	40	304	16	**320**

The testing was voluntary and each of the capture subjects had an opportunity to refuse the testing. According to the agreement with capture subjects, all fingerprints were erased after the analysis and no backup was created. However, the capture subjects could save their own fingerprints.

Results of tests of acceptability requirements were excellent. Nobody had objections or concerns about using this method, even the people, which had objections and concerns about capturing of other biometric characteristics (e.g., concerns about retina capturing process), did not have any problems with the capturing of the change of color and width of papillary lines.

The results of the security tests were also very good. The students tested the pre-prepared fake fingers (made of Durocast, Siligum, Siloflex, JaLatex, Latex Gedeo and stamp) or they had the opportunity to bring their own fake fingers. Nevertheless, none of the fake fingers was able to spoof this liveness detection unit.

The change of color and width of papillary lines was without any problem detected for all 320 volunteers. Nevertheless, it is necessary to say that the particular values of RGB components were highly dependent on the angle and distance of LED diodes and even on the light from the various sources in the environment. As it was expected, the illumination by LED diodes has different parameters than the illumination in a common office scanner, so the fingerprints illuminated by LED diodes appear darker than fingerprints captured by a common office scanner.

The change of papillary line width was detected for all 320 volunteers. However, it appeared that the detection of papillary lines by Sobel operator is not suitable for all fingerprints. Especially, the detected papillary lines of the wet fingers often contain a lot of noise, which could confuse the possible method for automatic detection of papillary line width. This implies that the third preliminary test should be more focused on the overview of possible algorithms for papillary line width detection.

4.4.3 Preliminary tests of pre-prototype

The third test was focused on the possible improvements of pre-prototype and the basic overview of possible algorithms for automatic papillary line width detection.

The first improvement of the pre-prototype of liveness detection unit was the exchange of camera module. The originally used camera Sony XCD-SX910CR with original software was not able to capture sequence of images or a short movie for an unknown reason, although it might be able to do it. Therefore, this camera module was replaced by Basler scA1600-14gc color camera module.

The other improvement and the tests/overview of possible algorithms for automatic papillary line width detection were performed by Ing. Homola (in his Master thesis under my supervision) [26].

Ing. Homola checked the dependency of values of RGB components on the angle and distance of LED diodes and on the light from environment and created a functional protective cover made of carton.

Nevertheless, the major goal of this preliminary test was testing of the possible algorithms for automatic papillary line width detection. Ing. Homola tested and created a comparison of a large number of algorithms [26], e.g., Sobel, Robinson, Prewitt, and Kirsch operators, Gabor filter, Canny edge detector, Gaussian filter, or Median filter.

Moreover, Ing. Homola had created his own proposal for the possible pipeline of image processing algorithms for pre-processing of an image for detection of papillary line width. His pipeline consists of five steps: transformation to the grayscale, Canny edge detector (applied twice), combination of dilatation and Median filter (applied three times), combination of erosion and Median filter (applied three times), and Median filter (applied 35 times).

This algorithm was just a first proposal and is quite functional. Nevertheless, it is quite complicated, which means that its possible speed up is quite limited. This algorithm was tested on the group of volunteers (6 woman and 16 man from 22 to 28 years old), but it worked correctly only for 78% of captured samples. The rest of them were wrongly classified due to the insufficient quality of papillary lines.

4.5 Final tests

During the preliminary tests, I had enough experiences to start the final tests: the finalization of hardware unit (see Section 4.5.1) and necessary algorithms (see Section 4.5.2) by the help of training database, the creation of the testing database of live and fake samples (see Section 4.5.3) and results of tests (see Section 4.5.4).

4.5.1 Hardware configuration

The pre-prototype of liveness detection unit for the final tests was based on the optical bench with appropriate illumination covered by protective housing made of carton. The optical bench is equipped with a special fingerprint module (see Section 4.3.2), color camera Basler scA1600-14gc with Computar MLH-10X lens.

The glass, against which the finger is pressed, is illuminated by two LED diodes (white light, 4 000 mcd, 3.2 V) powered by laboratory power supply MATRIX MPS-3005L-3. The location of diodes is different than it was during the third preliminary test. Several different angles and also counts of LED diodes have been tested, but the resultant placement of two diodes (see Fig. 4.10) showed the best results.

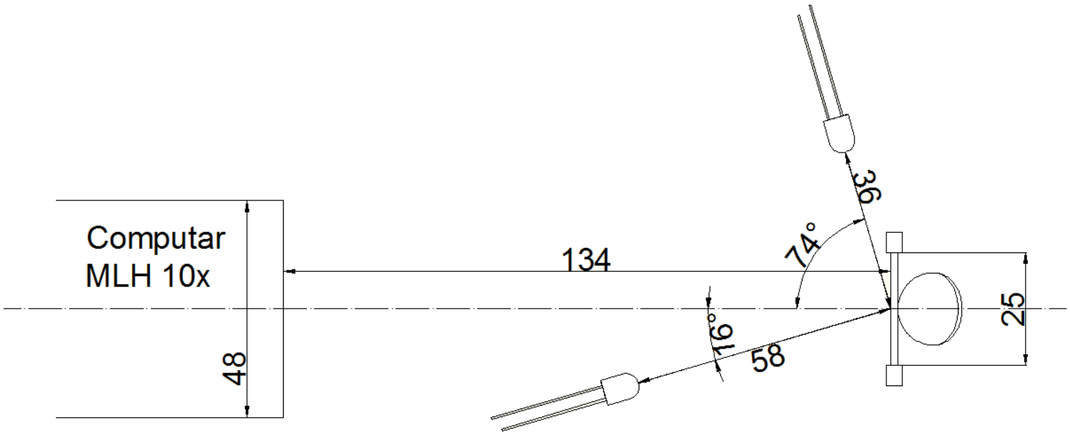


Figure 4.10: Position of LED diodes in the tested pre-prototype.

The protective cover (made by Ing. Homola) proved to be necessary, because the varying light conditions in laboratory affected the data (e.g., by reflection of light). On the other hand, the usage of this liveness detection unit with the protective cover is not as user-friendly as it was before.

The parameters of camera Basler scA1600-14gc were set in the same way as in the case of preliminary testing of the prototype (e.g., auto gain turn off, image type Bayer BG8), only the size and offset of the captured image was changed. The captured image has size 1284 × 930 px (instead of 800 × 600 px) and the offset was slightly altered to reflect the altered position of LED diodes.

For the purposes of the capturing of fingerprint samples, the common PC in Biometric laboratory has been used (Intel Core2 Duo E7400, 2048 MB RAM, NVIDIA GeForce 6600, OS Windows XP Professional SP3 installed on 9th September 2010). The liveness tests were conducted offline on my personal laptop Toshiba Satellite L40-14F (5 years old, Intel Dual-Core T2310, 1024 MB RAM, integrated graphics Intel GMA X3100, OS Windows XP Professional SP3 installed on 1st March 2009).

During the thorough checking of functionality of all hardware components before the start of capturing of training database, I have found out that the images of the same sample have various colors. The images look like they were illuminated by different intensities of light randomly alternating. Replacement of diodes did not solve the problem[11]. According to my opinion, this situation could occur in the real world scenario, so I have decided to alter the algorithm to deal with the various levels of illumination.

4.5.2 Algorithm

The liveness detection algorithm for the final tests was developed in C++ using Microsoft Visual Studio 2008, OpenCV 2.1 [110] and Pylon SDK 2.3 from Basler AG [79].

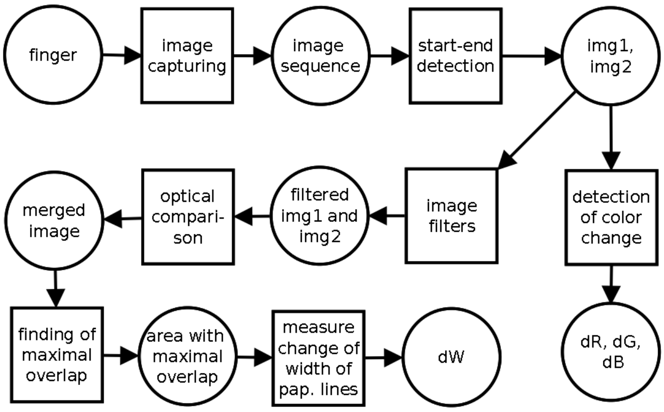


Figure 4.11: Workflow of my liveness detection approach.

As it was described earlier, the pipeline of algorithms has to be adjusted to the particular hardware configuration (especially in case of usage of different illumination sources). The selection of appropriate algorithms and its parameters for the above described hardware configuration (see Section 4.5.1) was done on the basis of test results of training dataset (3 persons: 1 woman, 2 men). The final liveness detection algorithm has seven phases (see Fig. 4.11):

Image capturing. The sequence of images is captured using the pre-prototype of liveness detection unit. During these final tests, I have used the pre-prototype described in the previous subsection and I captured the sequence of 75 BMP[12] images in every session. The captured images have size 1284 × 930 px and the camera is capable to capture approximately 12 frames per second, which means that the time of one

[11] The possible reason of this behavior was the malfunction of the power source unit.

[12] Bitmap image file.

session is approximately 6.25 s. During this time, the finger (real or artificial) has to be pressed against glass surface without any additional movement of finger.

The captured images are in the Bayer BG 8 file format [80]. It means that every pixel in each quadruple of neighborough pixels (2 rows of 2 pixels) contains only the value of one of the RGB colors (1st row: B, G; 2nd row: G, R). Because the images transformed in the BMP file format using accompanying algorithm did not have the expected color fidelity, I have decided to transform images by a simple algorithm, which reduces the size of image to half in both directions (from 1284 × 930 px to 642 × 465 px), but which complies the color fidelity. The RGB values of a new pixel are computed using the values of corresponding four pixels so that the R and B values are taken as they are and the G value of a new pixel is computed as the mean of both G values in the corresponding quadruple.

Start-end detection. The essential part of the liveness detection algorithm is the correct determination of images containing the non-pressed and pressed finger. For simplicity, it is expected that the capture subject will press the finger against the glass plate until the end of the capturing, so the image of the pressed finger is the last image in the image series see Fig. 4.12 c).

The detection of the non-pressed state of finger is more difficult. In Fig. 4.12, the mean RGB values of 100px (in line) in the center of each image are shown. The movement (and pressing) of finger was quite slow, so all phases of movement are easily distinguishable. In the first phase (approx. from 0 to 17), the finger is approaching to the glass. The images look dark and blurry, because the camera lens is focused on the glass.

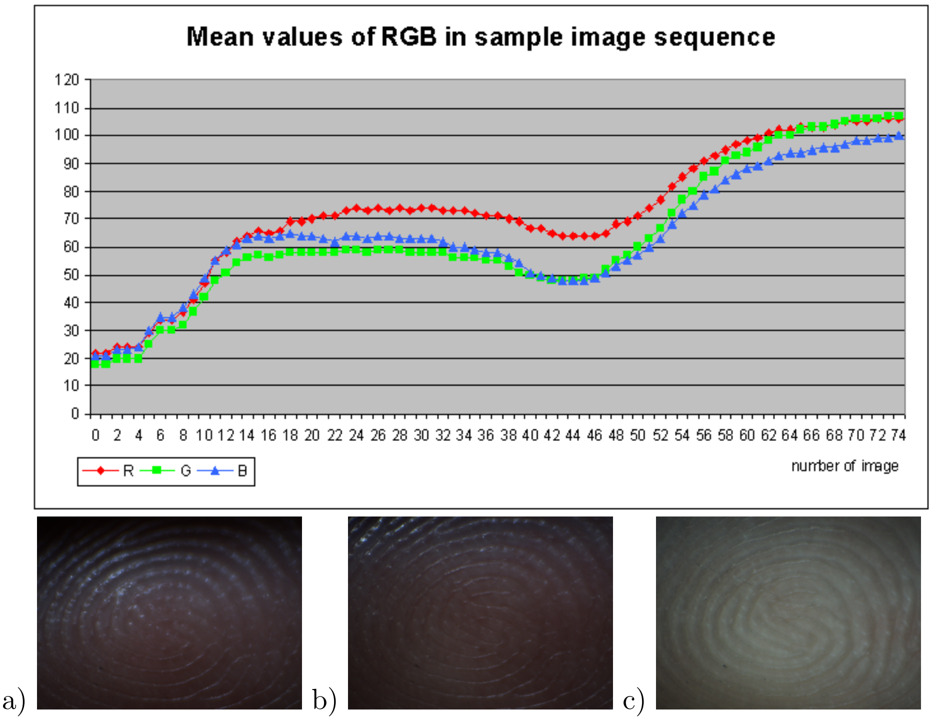


Figure 4.12: Graph of different phases during the pressing of finger and the sample images from diferent phases: a) image number 24, b) image number 43, c) image number 74.

The second phase (approx. from 18 to 38) is illustrated in Fig. 4.12 a). The finger is close enough to the glass to not be so blurred and there are reflections of the light on the papillary ridges. Nevertheless, not all of the papillary lines are visible (and only few of them are focused) due to rounded shape of the finger. During this phase, capture subjects often move their finger in various directions.

In the third phase (approx. from 39 to 47), the center of the finger slightly touches the glass (se Fig. 4.12 b). In the area of slight touch (the center of image), the reflection of light on the ridges is not visible, so the mean values of RGB colors decreased (as it is clearly visible in graph). The detection of this local minimum is used as the method to determine correct image of non-pressed finger.

The last phase (approx. from 47 to 74) is the pressing of finger against glass plate. The mean values of RGB increase quickly. The biggest increase can be seen in case of G values and the smallest in case of R values, which corresponds to the correct color change for the live human finger.

Nevertheless, the used camera is capable to capture only approximately 12 images per second and fingers of some people are moving quite fast. Therefore, I have decided to use backup method to determine the correct image of non-pressed finger. In case that it is not possible to detect the above described local minimum, the last image with mean G value equal to the half of G value of the image number 74 is considered to be an image of non-pressed finger.

Detection of color change. This step simply uses the average values of individual color channels computed for each image during the start-end detection and computes the difference of these average values for each color channel of both detected images (image before pressing and image after pressing finger against a glass plate).

Application of image filters. The sequence of image filters is applied on both images (image of non-pressed finger, i.e. img1, and image of pressed finger, i.e. img2). At first, both images are converted into grayscale color range. Then the Gaussian adaptive threshold[13] for blocks 85 × 85 is applied. Subsequently the Gaussian smooth filter (kernel 3 × 3) and threshold ($T = 128$) are applied.

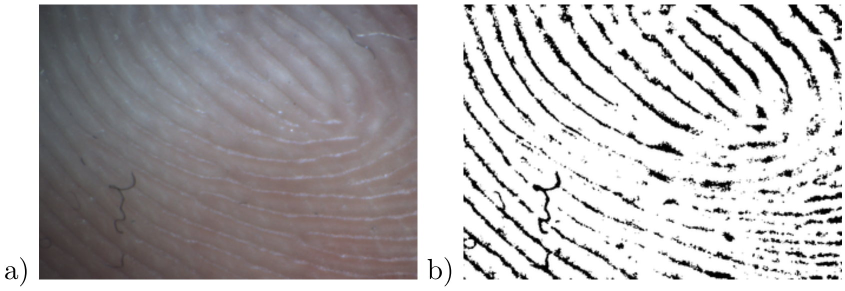


Figure 4.13: Examples of image filters in my liveness detection approach: image of pressed finger a) before and b) after application of sequence of image filters. This image has been excluded after capturing due to the higher amount of textile fibers, which could influence the results.

During the creation of the appropriate workflow for my liveness detection approach, a suitability of a lot of methods was tested/retested (e.g., Canny detector, Scharr filter,

[13] The Gaussian adaptive thresholding is the weighted mean of a neighborhood of pixel [110].

Median filter, dilatation, erosion) with various parameters, but the above-described sequence of methods with particular parameters proved the best capability to detect papillary lines in case of training images. Example of an application of image filters is given in Fig. 4.13.

Optical merging. This step merges two black and white images (image before pressing and image after pressing finger against glass plate, both after application of sequence of image filters). In case that both images have the same color of a particular pixel, the corresponding pixel in the merged image will have also this color. If the pixel is black in the first image and white in the second image, the corresponding pixel in the merged image will be green. In the opposite case, the resultant pixel will be red.

These contrasting colors (red and green) were chosen intentionally, because this module (optical merging) was used during the capturing of training and testing databases to check, whether the live/fake finger was moved during the pressing phase or whether it was not. In case of movement of finger, the merged image contains the separated green and red lines (with occasional crossing) on the white background so, that this problem can be easily and quickly recognized.

Finding of maximal overlap. Due to the distortion of the skin during the pressing of a finger against the glass plate, the papillary lines from the non-pressed and pressed fingerprints cannot be perfectly overlapped in the whole area of merged image. For the purposes of measuring of papillary line width, it is important to find the area of maximal overlap to avoid inaccuracies.

The source image for the finding of maximal overlap has 4 colors: white (overlapped ridges), black (overlapped valleys), green and red (non-overlapped valleys). In an ideal case (absence of noise), the overlapping is indicated by an absence of red pixels and high amount of black pixels in the area of overlapped valleys (surrounded by green pixels in case of live finger – see Fig. 4.14 a). On the other hand, the distortion of the skin is indicated by presence of green and red pixels (higher amount of green pixels than red pixels in case of slight distortion of a live finger – see Fig. 4.14 b) and absence of black pixels (or small amount in case of partial overlapping). The amount of white pixels does not entirely depend on the degree of overlapping. Therefore the area of maximal overlapping in image is computed as an area with maximal number of black minus red pixels.

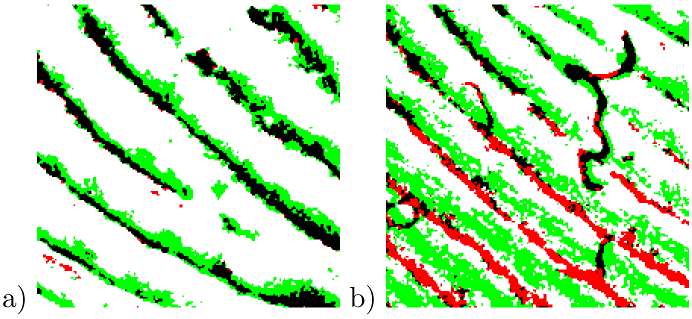


Figure 4.14: Examples of a) overlapping and b) distortion of papillary lines originating from the same merged image. The used image has been excluded after capturing due to the higher amount of textile fibers, which could influence the results.

Measuring of change of papillary line width. The original intention was to measure the width of papillary line using a similar approach as the algorithm used by Ing. Homola (see Section 4.4.3). The algorithm finds the white pixel (ridge) and tries to find the nearest black pixel (border of ridge - valley). The second black pixel is searched in the exactly opposite direction.

Nevertheless, the tests on the small training database showed that this simple approach has several disadvantages/problems. In case of very strong pressure of the finger, the valleys on the pressed finger are so thin that the detected lines of papillary valleys are slightly dashed. If the algorithm finding the opposite black pixel goes through the valley interruption, it will find the black pixel so, that the width of two adjacent lines (instead of one line) will be measured.

The papillary lines in the used magnification also do not have such smooth border as it may look on the images using smaller magnification rate. The line borders contain a lot of irregularities, e.g., small bays or protrusions. In case that the white pixel was found very close the border of a papillary line, it can happen that the algorithm measures the width of a bay instead of width of the papillary line. Moreover, the shape of some minutia (e.g., minutia called „point“ – see Section 2.3.2) or other irregularities (e.g., noise) could cause a problem, because the sample could be evaluated as a fake due to the insufficient width of papillary lines. In case of noise found as the first black pixel, it could theoretically happen that the opposite black pixel will be searched in the direction parallel with the papillary ridge flow.

These situations have been taken into account and the algorithm was redesigned. The starting white pixel has to be in distance at least 10px from the nearest black pixel to avoid, e.g., the measuring of width of the bay instead of the ridge width. Then the algorithm does not try to find the nearest black pixel and the second black pixel in the opposite direction, but it tries to find two opposing black pixels in 8 different directions[14]. The shortest width is considered to be correct. This approach minimizes the problem with dashed papillary valleys and the measuring of width in parallel with ridge flow. In this way, the ridge width is measured in 4 different places to avoid the problems with some untypical minutiae or other irregularities.

The results of the above described sequence of algorithms are the mean RGB values and width (four times) in image of pressed and non-pressed finger. The differences between corresponding means of RGB values have to meet the conditions given in Eq. 4.1. Nevertheless, I have decided to slightly reduce these requirements. Due to the lower level of illumination, the mean RGB colors of images in training database were nearer to the gray than mean RGB colors of images from preliminary tests using a scanner. Therefore, I have modified the equation so, that the values could be greater or equal (instead of greater). The minimal difference between one component of RGB color model in pressed and non-pressed image was set to 10.

At least three of four width pairs (width of papillary line in pressed and non-pressed finger) have to meet the conditions for the appropriate change of width. The conditions are simple: the width of pressed papillary line has to be in range [10, 70], the minimal change of width is set to 3px, the minimum amount of green pixels is 2 and if there are red pixels (noise), their amount has to be at least twice smaller than the amount of green pixels.

[14] This measurement is inspired by one phase of the automated processing of fingerprint (see Section 2.3.2). The array of orientation of papillary lines often contains also 8 different directions.

If the conditions for the appropriate color change are met and also (at least) three of four width measurement met the above described requirements, than the captured sample is considered to originate from a live human finger, otherwise it is considered to originate from a fake finger (or a dead finger).

4.5.3 Database

I tried to put together as much diverse group of people and fake fingers as possible. The final tests were performed on a group of 26 volunteers (18 men and 8 women) and 10 fake fingers made of different materials.

In the group of volunteers, only 18 volunteers graduated at Brno University of Technology. The rest of them have different professions, e.g., nurse, librarian, chemist (oil analysis), porter, technician. The distribution of nationality and ethnicity is not ideal (mostly Caucasians from the Czech and Slovak Republic), but the database contains also Asian from Vietnam. The age distribution is given in the Fig. 4.15. The age of volunteers is in the range from 20 to 68 years old (average 29 years old). I also tried to include persons with diseases or professions, which affect/may affect fingerprint color, elasticity or quality. There are volunteers having atopic eczema, anemia, or low blood pressure and manually working volunteers (see list of professions above) or volunteers with fingers damaged due to their hobby (judo, contrabass or hard work in the garden). In the group of volunteers, there is also a person (man, 25 years, Caucasian), whose fingers often caused problems to the various fingerprint sensors.

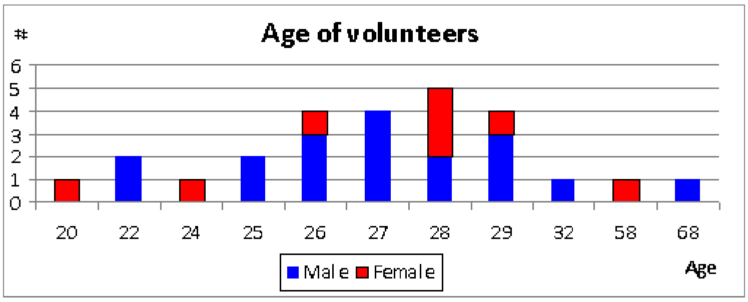


Figure 4.15: Age distribution and gender of volunteers in the final test of my liveness detection approach.

According to the necessity of usage of protective housing, the user-friendliness of the pre-prototype of liveness detection unit was much reduced. There were a lot of cases, where the images before and after pressing of finger against the glass were not corresponding due to the difficult access to the glass plate together with the nervousness of tested subjects (trembling or sweating fingers). Such images are not considered as correct samples; they were not included in the database and were immediately re-captured. Moreover, the samples containing higher amount of textile fibers were excluded. In the end, the testing database contains 3 correct samples per each live/fake finger.

In case of the fake finger part of database, I choose the fake fingers of different materials and colors. Because the elasticity of fake fingers made of various materials has not been widely tested, it is not possible to exclude potentially suitable candidate for the correct elasticity just because of the incorrect coloring. Naturally, it is also not possible to exclude candidate suitable to imitate the color of pressed or non-pressed finger just because of incorrect elasticity parameters or a lack of shape memory.

For the purposes of testing of my liveness detection approach, I have chosen the materials used in tests of competitive methods and the materials/fake fingers, which are successfully used in the biometric laboratory at Brno University of Technology. In total, 10 fake fingers in 3 sessions were captured:

- one pressure resistant material (sheet of rubber from a common office stamp),
- two soft materials without memory effect (special compound and gummy bears), and
- seven ordinary materials with varying softness (Siloflex, Siligum, Durocast, Latex Gedeo, JaLatex transparent, JaLatex skin-color, and gelatin).

The molds for all fake fingers were made of wax from common tea candles with assistance of an enrollee. As it was mentioned earlier, some of the used fake fingers have been used before; others (mostly the fake fingers made of material with rapidly deteriorating quality) were made only for this test. In all cases, I have used the thin variant of fake finger. The captured fake finger was always attached to the different live finger than the live finger, which was the model.

The characteristics of used materials and the set of photographs of used fake fingers are given in Appendix E.

4.5.4 Liveness test results

The captured sample is considered to be originating from a live human finger; it has to meet 3 criteria. The first criterion is the presence of a defined color change and the second criterion is the change of width of papillary line in at least three of four width measurements as it was described above. The last criterion was not directly stated before, but it simply results from the principle of this approach: the papillary lines have to be (at least partly) observable by person/algorithm, because the successful fake finger needs not only to deceive the liveness detection algorithm, but it also has to contain (at least some) papillary lines for minutiae extraction.

The third condition was easily met by almost all live finger samples. Only elder persons and person hardly working in the garden had not such perfect papillary lines (see Fig. 4.16), but most of their papillary lines were easily distinguishable, so they also met this requirement.

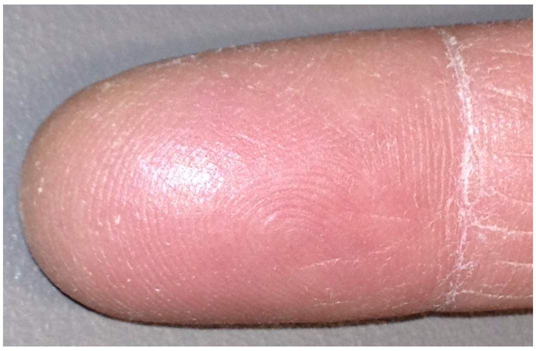


Figure 4.16: Example of finger of an elder manualy working person.

In case of captured samples of fake fingers, the third condition excluded several materials. Although the special compound is often very successful in spoofing of optical fingerprint sensors and it was capable to spoof one sensor with liveness detection capability, the captured samples of these fake fingers did not contain any papillary lines. The resultant images contains only the color dots of various substances used for creation of this material and it does not contain any signs of presence of papillary lines. This can be caused by the used magnification and/or the used illumination in combination with the characteristic properties of this compound (e.g., matte surface).

Another problem occurred at gelatin and gummy-bear fake fingers, although these fake fingers are widely used and capable to spoof variety of fingerprint sensors (e.g., see Fig. 4.17). The captured samples of these fake fingers contain a large amount of tiny bubbles. This problem was reported, e.g., by Wei-Yun [74], whose gelatin fake fingers often contained larger amount of bubbles. I have created many samples of gelatin and gummy-bear fake fingers[15] to choose the best (and the bubble-free) ones. Nevertheless, the presence of amount of tiny bubbles and the characteristic properties of material caused that the papillary lines were not distinguishable.

On the other hand, it is necessary to say that the tiny bubbles (in different quantities) were observable in all fake finger materials (except special compound). It can be said that the biggest problems with these inhomogeneities were observed in transparent or semi-transparent materials (probably due to the visibility of bubbles lying under the surface of a fake finger. The bubbles in non-transparent materials occur quite rarely and did not influence the detectability of papillary lines and the tests at all. It is also possible that the bubbles (and their influence on processed image) were highlighted by combination of magnification and illumination (and used sequence of image filters).

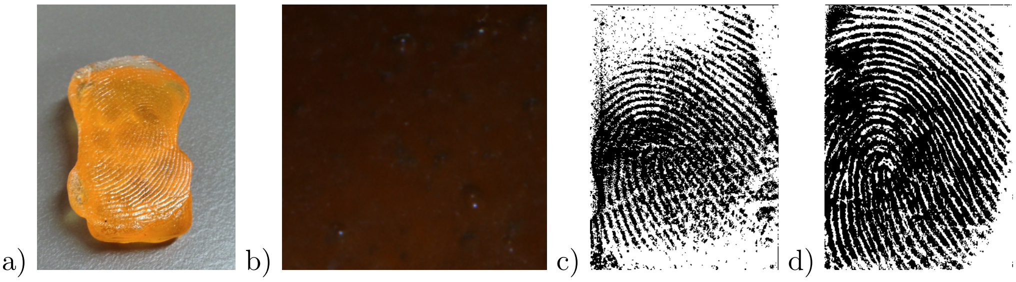


Figure 4.17: The a) fake finger made of orange gummy bear captured using b) presented liveness detection approach (see the presence of bubbles and absence of papillary lines), and by c) Suprema SFM3050-TC1. d) The corresponding live finger captured by the Suprema SFM3050-TC1.

According to the requirement for the proper color change, all live sample series contain the correct color change. Nevertheless, the liveness of these samples was evaluated using the simplified conditions created after on the basis of analysis of training database and insufficient lightning. If the data is evaluated using the equation used in case of preliminary tests on the scanner, 8 samples (10%) will be evaluated as originating from a non-live finger.

[15] During preparation of fake fingers for this testing, I have used gummy bears and gelatin in various color variants made by various companies to find whether the problem with bubbles is common. All of them contain bubbles, so I have chosen the material (producer), which reached best results in the past. More information is given in Appendix E.

All fake fingers (regardless the visibility of papillary lines) were tested, whether their pressing against the glass plate will have the color change similar to the live human finger. None of the tested fake fingers succeeded (even under the mild conditions). The graph of color changes of live and fake fingers is given in Fig. 4.18. The values of colors of non-pressed and pressed live human fingers are drawn smaller, because they serve as marking of the area of human-like color. The values of colors of fake fingers are so similar, that only their mean is displayed (to reduce amount of points in the graph). The additional graphs (graph of RG and GB colors) are given in Appendix F.

In Fig. 4.18, it can be seen that the direction of color change of live finger samples is in accordance with the presented equation: the change of red component is smaller than the change of blue component. It is clearly visible that live fingers before pressing were reddish and the pressed fingers were more whitish. Nevertheless, the consequences of the illumination instability are also visible: both groups of live finger samples (non-pressed samples and pressed samples) are not so homogenous as they could be, all samples are much more gray then samples captured on scanner during preliminary tests and some samples are even very dark.

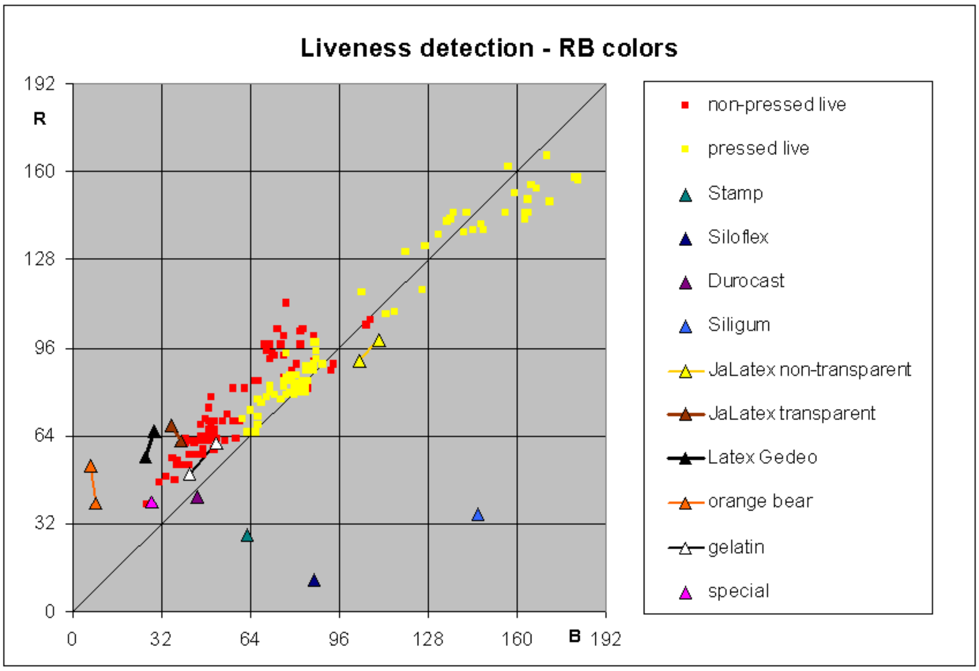


Figure 4.18: The graph of mean R and B colors of non-pressed and pressed samples.

Five of ten materials (stamp, Siloflex, Durocast, Siligum, and special compound) did not present any color change (in consistency with expectations). Nevertheless, the special compound confirmed, that its color can be considered as color of non-pressed live human finger[16]. Another material (non-transparent JaLatex) shows the small color change, which looks alright at first glance (see Fig. 4.18), but it has the opposite direction. This could be caused probably by higher amount of reflections of light in image of non-pressed sample.

Remaining four materials are transparent or semi-transparent, so it was expected that there will be some color change. In case of transparent JaLatex and orange gummy-bear,

[16] The mean color of special compound is slightly darker than mean color of live human finger due to the absence of reflections of light (surface of special compound is matt), but this is not a problem.

the color change has different direction than the color change of live human samples. The change of R component is presented but the value of change of blue component is negative. The Latex Gedeo has a better characteristic, the change of colors in positive direction is presented, nevertheless the change of red component is significantly higher than the change in blue component. The best results (from the spoofing point of view) were achieved by gelatin fake fingers. The results of changes of all RGB components almost meet the requirements, but the change of red component was always slightly higher than the change of blue component.

Nevertheless, it is necessary to say, that all changes presented by different fake fingers were very small. The changes of RGB components were about a few points in case of fake finger samples, but about a few tens points in case of live human fingers. It is possible that the change of color of live human finger behind the fake finger looks smaller because the material of fake finger is not transparent enough and absorbs the light, or it is possible that the finger does not present such significant color change due to the pressing against soft surface (fake finger), which absorbs part of the pressure force.

According to the detection of width of papillary lines, all samples of live fingers were classified as originating from the live human fingers (contained at least three correct width changes of four). The boxplot of correct widths of papillary lines of men/women can be found in Fig. 4.19. The mean width of non-pressed papillary lines is 24.2px for women and 26.7px for men. In case of pressed finger, the mean width increases to 32.1px for women and 34.9px for men. It seems that the mean width of papillary lines of women could be slightly smaller in general, but to confirm this hypothesis a much larger amount of test results (capture subjects) will be necessary.

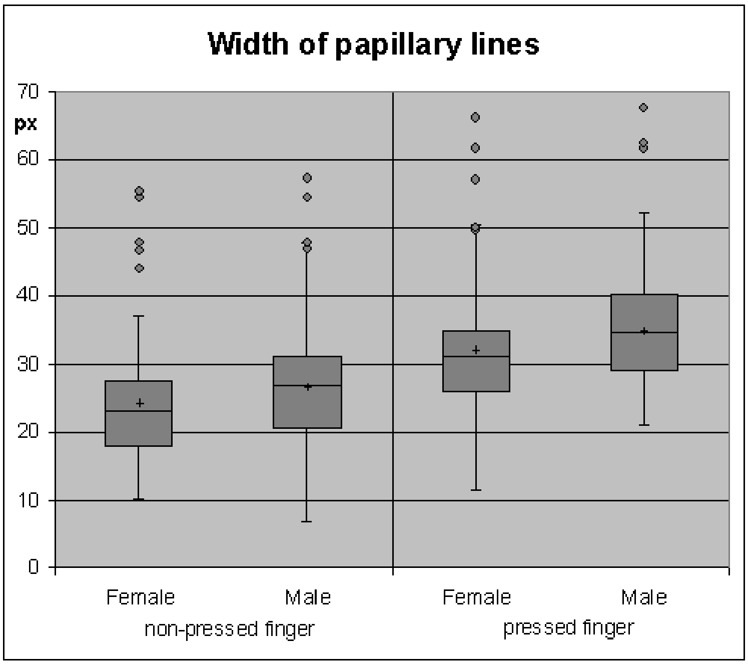


Figure 4.19: The boxplot of correct widths of papillary lines of men/women in pressed and non-pressed phase.

The outliers[17] (in Fig. 4.19) are mostly caused by extreme pressure of finger against the glass plate, which caused narrowing of valley so that the valley was hardly detectable and the algorithm measures the width of two papillary lines instead of one. Nevertheless, these values are still within the range of correct values.

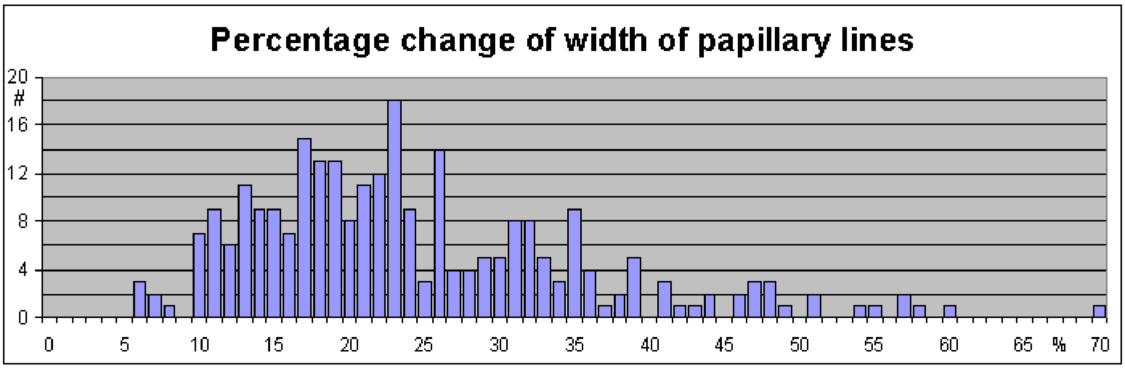


Figure 4.20: The graph of percentage change of width of papillary lines for live fingers.

The percentage change of width of papillary lines is given in Fig. 4.20. The mean value of change is 24.9%. In comparison with the results and suggested interval of width change given in the first preliminary test (change from 10 to 40%) based on only 12 width measurements, these new results show that 88.4% of correct measurements are in the same range. Another 9.3% of measurements exceed this range, which may be caused by different construction of the sensor (subjectively: people were often afraid to press a finger against a glass of common office scanner, but they were mostly not afraid to press their finger against a glass of the robust prototype).

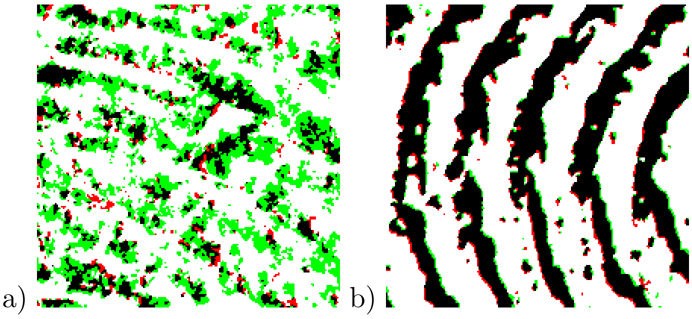


Figure 4.21: Example of merged images for livenes detection with test: a) papillary lines of elder manually working person (see photo in Fig. 4.16), b) papillary lines on the stamp.

As it was mentioned earlier, the quality of material was essential for the detection of papillary lines width. Therefore, three materials (special compound, gelatin and gummy bear) had to be excluded due to the impossibility to detect papillary lines and only seven materials (Siloflex, Siligum, Durocast, JaLatex skin-color, JaLatex transparent, Latex Gedeo and stamp) have been tested. The automatic detection of non-pressed and pressed finger expects the live human finger (the detection algorithm is based on the color change), so that algorithm was not able to find non-pressed sample or chose a sample containing the

[17] The outliers are defined as values, which are lower than $Q_1 - 1.5 \times (Q_3 - Q_1)$ or higher than $Q_3 + 1.5 \times (Q_3 - Q_1)$ [75].

black image from the beginning of image series (before the approaching of finger). Therefore I have decided to choose the image of non-pressed (fake) finger manually to fully avoid influence of color change to the width change detection.

According to the stamp fake fingers (see Fig. 4.21), the material was pressure resistant as it was expected – none of the captured samples showed any correct width change. Surprisingly, the fake fingers made of Siligum have also the same pressure resistance capability. The fake fingers made of skin-color JaLatex were also unsuccessful, only two of them contain one correct width change. On the other hand, the fake fingers made of Durocast, Siloflex and Latex Gedeo showed quite good results. In some cases, the captured samples contained two correct width changes. Due to the small amount of used samples, it is not possible statistically evaluate these results. Nevertheless according to my opinion, it could be possible to use some of these materials (fake fingers) to present three correct width changes, if the liveness detection unit allows sufficient (and quite high) amount of attempts.

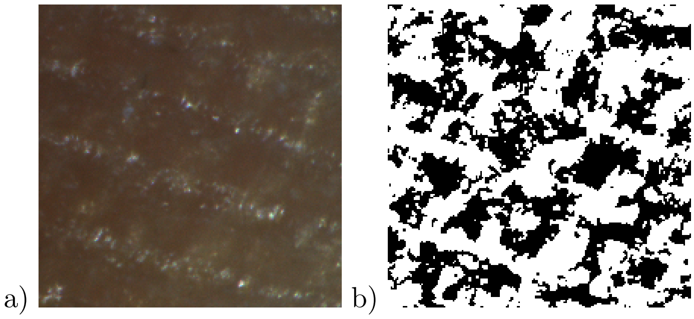


Figure 4.22: Example crossing of papillary lines of live and fake finger: a) captured image, b) image processed by series of image filters.

The last material (JaLatex transparent) was also unsuccessful, but the image analysis showed one interesting result. As you can see in Fig. 4.22, this material was transparent enough to cause an interference of papillary lines on fake finger and on live finger behind. Nevertheless (as it was mentioned above), this material was not transparent enough for the sufficient amount of light and thus present the correct color change. Moreover, it is necessary to ask, whether this image is a correct sample due to the absence of correct papillary lines and consequently the significantly decreased possibility to find the correct minutiae.

Moreover, the statistics show a few interesting values. The 48.7% of images of non-pressed finger was selected using the detection of local minimum, in the rest of cases (51.3%) this method was unable to select an image, so these images were chosen by included backup alternative method. It could appear that the finding or not finding of local minimum is a random phenomenon with an equal probability. In that case, the probability of detection of local minimum in all three sessions will be 12.5% and the same is the probability of detection of local minimum in none of all three sessions. Nevertheless, these two cases occur in 61.5% (equal probability in both cases). These results could confirm the assumption given after the analysis of training database that the curve of means of RGB values could be influenced by captured subject.

Another observation has been made. The live and fake fingers often contain various amounts of textile fibers. Some of the fibers were so small, that they are not visible to the naked eye. Live human fingers (and also tested fake fingers made of harder materials) contain only a few of fibers, so this situation did not influence the capturing process or algorithm. The fake fingers made of soft material (gelatin, gummy bear and special compound) had a tendency to contain more of these fibers and it was very difficult to remove the fibers from their surface, because fibers were like glued. These fake fingers had to be kept and transported in the very clean environment to avoid contamination and to do not influence tests due to covering by higher amount of textile fibers. According to my opinion, this property of some materials could also slightly increase the difficulty of an attack.

4.6 Summary

The content of previous sections answers the questions asked at the beginning of this chapter. I analyzed the liveness detection methods published in papers, patents or on web pages of various companies and tried to find advantages and disadvantages of the presented approaches. On the basis of this analysis, I created a list of conditions, which the successful liveness detection method should meet. I also created a novel method for the liveness detection, which meets these requirements and which can be integrated into a common optical fingerprint sensors.

The presented novel liveness detection method is patented in the Czech Republic (Utility model No. 19364 [41]). This method was widely tested (three preliminary tests and a final test by the help of 374 volunteers and fake fingers made of various materials) and it shows better results than other[18]. The advantage of this method is the possibility of correct capturing of wet, dry or bended skin and also the type of tested characteristic properties of live human body, so it is not necessary to wait until some physiological process (e.g., perspiration or several heartbeats) takes place. The disadvantage is the impossibility of correct evaluation of skin with high percentage of contamination by colored material (e.g., ink, chalk or some chemical substances).

There are a few possibilities for the future research or improvements. The first possibility is the creation/invention of an algorithm for the automatic rotation, movement and especially correct deformation of papillary lines. This algorithm should reduce the unwanted side effects of elasticity of fingers and create a higher amount of overlapping of papillary lines of non-pressed and pressed samples to enable the measuring of papillary lines in all image areas.

The second possibility of improvement is the hardware change. According to the test results, the user-friendliness of a unit/sensor with this liveness detection method is significantly higher, if the glass is accessible from all sides (e.g., glass of open office scanner or optical sensors produced various companies). Placing a finger inside a sensor, finding a glass there and then pressing a finger against that glass often causes a slipping or movement of a finger especially in case of nervousness or wet fingers, which can cause a repeating of capturing process.

Other possibility of future research is the defining of area of colors belonging to the live human fingertip in non-pressed and pressed state regardless of skin color, gender, age, etc. I partly opened this topic during the first preliminary test, but it was just a start. The existence of definition of area of colors belonging to the live human fingertip could significantly help to the liveness detection in general. The appropriate application of such research could help to exclude magenta or green fake fingers, which commonly reaches high successful rate or to exclude the theoretical attack on my liveness detection approach by a substance capable of color change with the correct change ratio but with the incorrect start and end color (e.g., from dimgray to aquamarine).

[18] Nevertheless, only a few of other methods published results of their tests.

Chapter 5

Semantic conformance testing

The semantic conformance testing is the second area of the security of biometric systems, which I decided to devote in my Ph. D. thesis. As it is mentioned earlier (see Section 3.5.5), the development of semantic conformance testing is a consequence of results of MINEX [66] and similar projects, which have confirmed that some automatic minutiae extractors have not followed the intensions of the ISO/IEC 19794-2:2005 standard [97] and have placed the minutiae in some kind of grid instead of placing them at the faithful location according to the standard. These results point to a possible interoperability and security problem and it was decided to solve this problem (and also a lot of other problems) by creating of conformance testing procedures and methodology.

The conformance testing (generally) has been divided into three levels of testing in ISO/IEC 29109-1 standard [99] (see Chapter 2.4.2). The first two levels were quite easily created and implemented[1], but there was no proposal or existing method to create Level 3 (Semantic) conformance testing, which tests whether the generated biometric data interchange record (template) is a faithful representation of an input data (fingerprint). This situation led to the call ISO/IEC SC37 N3058 [102] (Call for Contributions on Metric for Measuring Accuracy of Minutiae Placement) and my methodology was created as a contribution in response to it.

It is necessary to find answers to the following questions:

- What are the common errors and problems of the minutiae extraction algorithms? Are these problems equally serious?
- How to deal with the problematic fingerprints (poor impression, injuries, diseases, image problems)?
- How to define the reference set of minutiae (Ground Truth Minutiae)? How to collect GTMs?
- Is it possible to use all GTMs from one source? Or how to cluster data from different sources to achieve GTMs? How to solve the problem of inconsistent opinion of data sources?
- Is it possible to create (and implement and test) a sufficiently clear/understandable methodology covering all these aspects?

[1] Level 1 (Data Format Conformance) and Level 2 (Internal Consistency Checking) are syntactic tests. They test, e.g., the presence of all mandatory fields or correctness of relation among various values/fields - whether the minutiae coordinates are not bigger than image size.

5.1 Analysis

At first, it was necessary to analyze possible problems or situations, where the minutiae extraction algorithms could fail or could produce inaccurate results. Moreover, it was necessary to find a way to define and create the reference set - the ground truth minutiae.

This analysis was based on my experience with the fingerprint minutiae extraction algorithms and the results of proof-of-concept tests. The input fingerprints for these tests were the images from my private fingerprint database and several images from the NIST SD14 database [71]. The tested set of images included images scanned from dactyloscopic cards, images from the crime scene, fingerprints with some skin diseases or scars, images of dirty fingers, etc. This set of fingerprints was the input of the minutiae extraction algorithm `mindtct` from NIST [73]. The results of tests confirmed that there are basically three different types of problems: minutiae outside the appropriate area, imprecisely placed minutiae and minutiae found in the problematic areas.

5.1.1 Minutiae outside the appropriate area

The first group of errors of minutia placement are the possibilities that the minutiae extraction algorithm finds a minutia outside of the fingerprint area or at the border. Although it seems to be a theoretical problem, it occurred very frequently during the proof-of-concept tests.

This problem is a consequence of improper foreground/background masking. The reason of this failure can be noise, dirt, drawing or written characters in the background of an image or some specific problems of a particular algorithm. The examples of the minutiae detected outside or at the border of the fingerprint area can be found in Fig. 5.1.

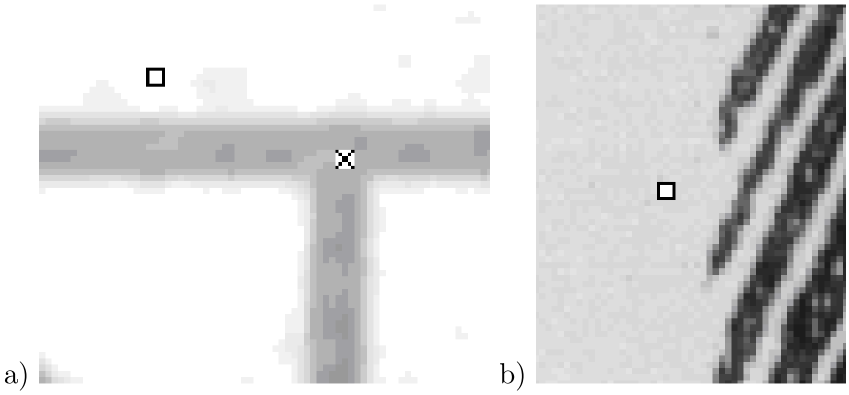


Figure 5.1: Minutiae detected a) outside the fingerprint area (noise on the background and the border of scanned dactyloscopic card) or b) at the border of the fingerprint area. The ridge endings are drawn as squares and ridge bifurcations are drawn as crosses.

5.1.2 Imprecisely placed minutiae

The second group of problems are the imprecisely placed minutiae. According to the description of minutiae data given in the ISO/IEC 19794-2:2005 standard [97] (see Section 2.4.1), there can occur four different problems:

- inaccurate minutiae position;

- false minutia type;
- inaccurate angle of minutia; and
- different value of quality of minutia.

Of course, several of these problems can occur simultaneously. For example, if the minutia type is wrongly determined, then there is a strong likelihood that the position of minutia will be imprecise too (see Fig. 5.2). It can happen that a minutiae extraction algorithm wrongly evaluates the difference of gray level of papillary ridge and assumes that two ridges are not joined. In such case, it also assumes that the remaining ridge ends in the middle of distance between neighbor papillary lines and places the minutia position there, which causes the simultaneous problem with inaccurate minutia type and position.

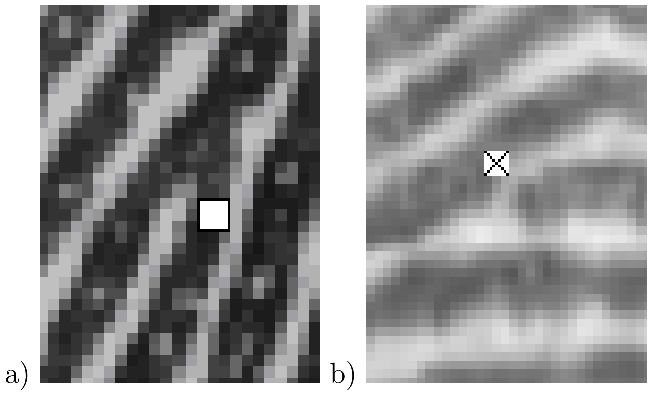


Figure 5.2: Examples of imprecisely placed minutiae: a) the ridge bifurcation detected as the ridge ending, b) the ridge ending detected as ridge bifurcation. The ridge endings are drawn as squares and ridge bifurcations are drawn as crosses.

On the other hand, there are algorithms, which intentionally do not set the minutiae type (set the type of all minutiae as „other“ type). This approach is not only the problem from the ISO standards point of view but also it is a problem from the security point of view, because an attacker can more easily use the brute force attack.

As it is written in the beginning of this chapter, the imprecisely set value of minutia quality is one of the possible problems. Beside to the other three inaccuracies, this inaccuracy was not taken into an account during the process of creation of the methodology. The reason is that all three other attributes of minutiae (type, position, and angle) are standardized, but there is no standardized quality metrics yet. Therefore, I decided to omit the assessment of quality faithfulness from the methodology.

5.1.3 Problematic areas

The last set of problems are the minutiae detected inside the problematic areas in the fingerprint. These areas are created by specialties distorting the standard flow of papillary lines in image. These problematic areas (causes of their occurrences and sometimes even the possible approaches to enhance quality of the resultant fingerprint) are described in Section 2.3.4. A lot of these problematic fingerprints were tested during the proof-of-concept tests. The false minutiae were detected by used extractor in three different situations:

1. **Fake ridge endings.** The regular ridge flow can be interrupted, e.g., by bended skin, scar or dirt on the captured finger. Another example is the fingerprint of dry finger, where the papillary lines may appear as the series of papillary dots. These situations may cause the fake minutia (mostly fake ridge ending) detection (see Fig. 5.3).

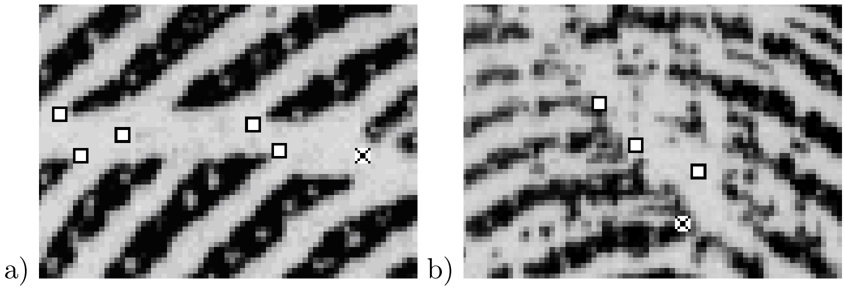


Figure 5.3: Examples of the minutiae found in the problematic areas of fingerprints: a) bent skin, b) scar. The ridge endings are drawn as squares and ridge bifurcations are drawn as crosses.

2. **Fake ridge bifurcations.** This situation is an opposite to the previous one. In case of the wet fingers (e.g., caused by higher sweat production) or the very hard pressing of finger against the sensor surface, the papillary lines may optically join and create fake minutiae.

3. **Fake ridge pattern.** In more complicated cases, the affected part of the fingerprint can contain the completely new (fake) ridge pattern. This situation may occur mostly in case of some skin diseases[2]. The correct minutiae detection in such areas is very difficult. Even the human dactyloscopic experts can have problems with such minutiae because it cannot be easily determined whether the ridge ending or bifurcation is caused by a disease or it is natural. The example of several fingerprint areas with skin diseases and false minutiae can be found in Fig. 5.4.

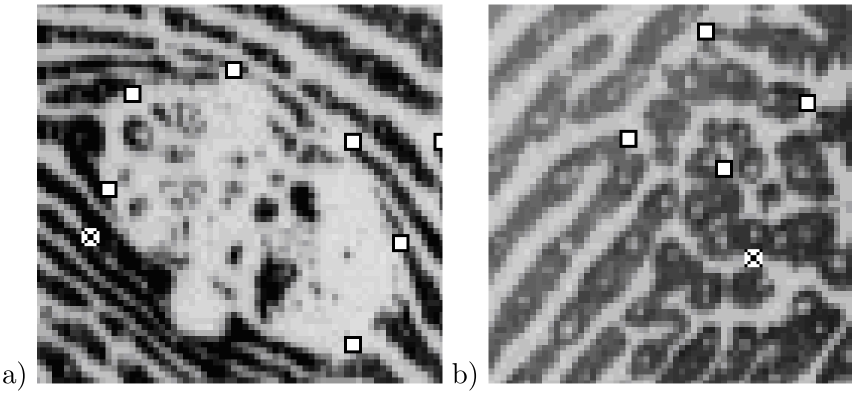


Figure 5.4: Examples of minutiae found in fingerprints affected by skin diseases: a) wart, b) papillary dots. The ridge endings are drawn as squares and ridge bifurcations are drawn as crosses.

[2] The influence of different skin diseases for comparison results is studied in the project „Influence of skin diseases for recognition by fingerprints" in cooperation with University Hospital in Olomouc.

The problematic areas presented in this subsection often occur in many of current fingerprint databases. Whereas the experts have difficulties to recognize true minutiae from the false minutiae in these areas, it is not possible (and not fair) to judge the minutiae extraction algorithms according to the amount of false minutiae detected inside of these areas.

5.1.4 Determination of the ground truth

For the purposes of computation of semantic conformance rates, it is essential to have the reference set - so called the Ground Truth Minutiae (GTMs). It is evident that the determination of the ground truth has to be done by the independent institution and on a large scale and carefully selected fingerprint database. It is not possible to choose one (or more) vendor(s)/fingerprint extraction algorithm(s) to generate ground truth minutiae, because it is not possible to assure, that it is (they are) 100% accurate and does not make any errors. Moreover, it is necessary to count on the fact that the selection of one (or more) vendor(s)/algorithm(s) would create monopoly on the market and disadvantage the other vendors/algorithms.

The ground truth minutiae also could not be set by an inexperienced person/institution, so the only one solution was to ask dactyloscopic (forensic) experts for help. The best situation would occur if the experts were from different countries, because the variability of their training and placement practices would minimize the risk of systematic errors. However, the experts are still human beings, so it is necessary count with possible errors and inconsistencies in their opinions.

5.2 Ground Truth Database

As it has been discussed previously, it is necessary to create database of fingerprints together with their GTMs. This database has been called Ground Truth Database (GTD). At the beginning, it was necessary to carefully choose the fingerprint samples (see Section 5.2.1). Then it was necessary to create a program for collecting data from dactyloscopic experts (see Section 5.2.2). Finally, the Harmonized dactyloscopic dictionary was created (see Section 5.2.3) to avoid errors arising from different approaches of experts from different countries.

5.2.1 Fingerprint samples

The fingerprint samples were carefully selected by Ms. Elham Tabassi (NIST). These images came from the NIST SD14 [71] and SD29 [72] fingerprint databases and they were carefully selected to represent the variability of fingers, fingerprint types, quality (NFIQ[3]), position and consist of the approximately same amount of male and female fingerprints. Nevertheless, it is not possible to create the fully balanced database, because the sources are limited and the representation of patterns in the population is not uniform.

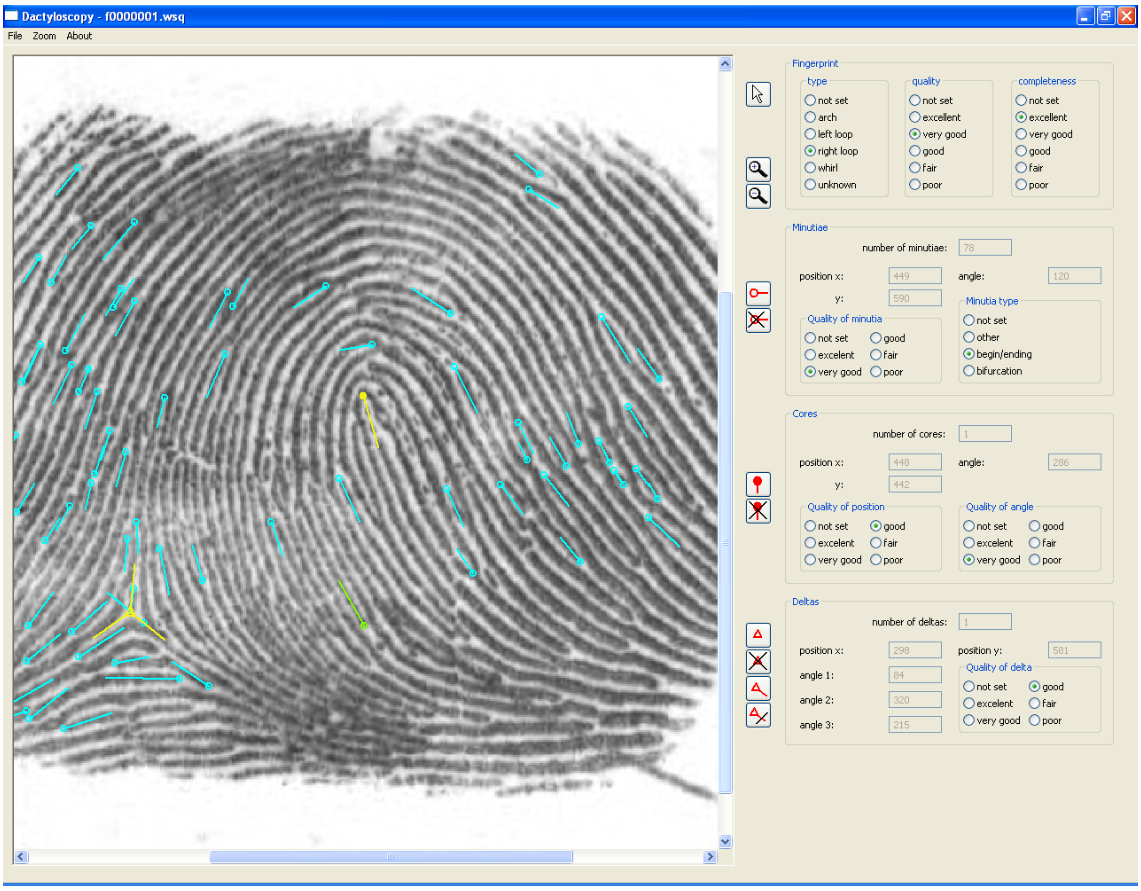
The final GTD database consists of 9 638 fingerprints, 6 800 of them come from the SD14 database and the rest comes from the SD29 database (to enrich the final GTD with plain impressions). The images from SD14 contain information about sex, finger position, fingerprint type, category, and quality. In contrast, a fingerprint from the SD29 database

[3] NIST Fingerprint Image Quality [73].

contains only the information about finger type, position and fingerprint quality. The statistical characteristic of the final database can be seen in Appendix G.

5.2.2 GUI for dactyloscopy

The Ground Truth Minutiae (GTMs) are the minutiae found by the dactyloscopic experts. For the purpose of GTMs collection, I have prepared the program „GUI[4] for dactyloscopy“ (see Fig. 5.5).



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

y: 590

angle: 120

Quality of minutia: ○ not set ○ good ○ excelent ○ fair ● very good ○ poor

Minutia type: ○ not set ○ other ● begin/ending ○ bifurcation

Cores

number of cores: 1

position x: 448

y: 442

angle: 286

Quality of position: ○ not set ● good ○ excelent ○ fair ○ very good ○ poor

Quality of angle: ○ not set ○ good ○ excelent ○ fair ● very good ○ 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 ● good ○ excelent ○ fair ○ very good ○ poor

Figure 5.5: Screenshot of GUI for dactyloscopy.

This GUI has been programmed in C++ language using wxDev-C++ framework v. 6.10.2 (extension of Dev-C++ framework by wxWidgets - cross-platform GUI Library [132]).

The GUI can load fingerprints in BMP or WSQ[5] file formats. It supports the setting of fingerprint type, quality and completeness. It is possible to zoom in/out fingerprint in the interval from 10 % to 500% and also it is possible to select each of the inserted objects to see its properties.

The GUI allows inserting, modifying and deleting of minutiae (and setting their type and quality). The last inserted minutia or the selected minutia is neon green (RGB: 127, 255, 0) and the previously inserted (or not-selected) minutiae are cyan (RGB: 0, 255, 255). The symbol of inserted minutia is an empty circle with a line representing the angle of minutia.

[4] Graphical User Interface.

[5] Wavelet Scalar Quantization [73].

The minutia is inserted by pressing the left mouse button; the angle of the minutia is set by the movement of the mouse, and the releasing of the mouse button will save all information in the internal database.

It also allows inserting, modifying and deleting cores (with information about quality of their position and angles). The last inserted core or the selected core is neon yellow (RGB: 243, 243, 21) and the previously inserted (or not-selected) cores are red (RGB: 255, 0, 0). In comparison to the minutiae, the symbol of core is the full circle, but it also contains the line representing the angle of core. The process of inserting core is same as in case of inserting minutia.

The last group of objects allowed to insert are deltas (with value of delta quality). The deltas are same color as cores, but their appearance is different. The delta is inserted as an empty triangle with three lines representing angles of delta. The direction of each line can be changed by drag and drop principle (the line has to be taken in the end-part). It is also possible to remove or add an angle/line but there can be only two or three angles and the missing angle value is filled by one of the rest values (according to the ISO/IEC 19794-2:2005 [97]).

The quality (fingerprint quality, quality of minutia, quality of core position and angle, quality of delta) should be the value in the interval from 1 to 100 according to the ISO standard. However, it is impractical and time-consuming to write the value manually. Therefore, the setting of the quality is (as required by experts) limited to the five possibilities (excellent, very good, good, fair, poor) and value „not set“. These possibilities determine the values 90, 70, 50, 30 10 and 0 respectively.

Although, the used colors seem to be unusual, they have been carefully selected in cooperation with the German dactyloscopic experts to provide the maximal contrast among used objects, maximal contrast between objects and fingerprint on the background and show the biggest user-friendliness.

The resultant minutiae, core and delta record is stored in the *.gtm file format (see Fig. 5.6). This format is human readable ISO-like record of set properties. All values are stored in ranges defined by the ISO/IEC 19794-2:2005 standard, but they are placed so, that it is easy to apply batch processing but also the result can be easily human-readable in any common text editor.

5.2.3 Harmonized dactyloscopic specification

For the purposes of international cooperation, it was essential to create a harmonized dactyloscopic specification/knowledge base. Due to the fact, that the various countries use different fingerprint classes (see Section 2.3.1) and various minutiae types (see Section 2.3.2), it was necessary to illustrate, how to classify various fingerprints and how to place minutiae and set their parameters (type and angle) in various specific situations.

This base was given in the document „Daktyloskopisches Basiswissen im Rahmen des Kooperationsprojektes Ground-Truth-Database“ (Dactyloscopic Knowledge Base in the Context of the Cooperation Project Ground-Truth-Database) [8] by Ms. Bernhardt from Department ZD23-1 (AFIS-Planung, Entwicklung, Qualitätssicherung) at BKA[6] Wiesbaden in 2009. This document has been reviewed by various dactyloscopic experts and academic researchers. This dictionary was also enhanced after the analysis of the preliminary tests (see Section 5.5.1).

[6] Automated Fingerprint Identification System-Planning, Development, Quality assurance at German Federal Criminal Office (Bundeskriminalamt).

```
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 5.6: Example of *.gtm file format.

5.3 Methodology

The semantic conformance testing methodology was proposed in order to determine whether or not a minutiae extractor is conformant to the ground truth minutiae. This methodology was created on the basis of my experiences with minutiae extraction algorithms and the results of proof-of-concept tests presented in Section 5.1.

For the purposes of semantic conformance testing, I have proposed three conformance rates, which will be described in the following subsections. The conformance rates values are in the range 0 to 1, where 0 means the lowest score (non-conformant result) and 1 means the one hundred percent compliance between GTM[7] set and AGM[8] set.

5.3.1 First conformance rate

The first conformance rate is marked as cr_{gtm}. This conformance indicates the preciseness of placements of AGMs detected by the automatic minutiae extraction algorithm according to the GTMs.

The process of computation of cr_{gtm} conformance rate is not so difficult. At first, the algorithm tries to find the closest AGM to every GTM. If the distance between the found AGM and original GTM is smaller than or equal to a tolerated distance tol_d, the minutia is further processed, otherwise it is rejected and the algorithm considers this AGM as missing. This process is described in the Equation 5.1:

$$cr_{gtm} = \frac{\sum\limits_{i=1}^{n_{gtm}} mcs_i}{n_{gtm}} \tag{5.1}$$

$$mcs_i = \begin{cases} 0 & \text{if} \quad d \geq tol_d \\ 1 - p & \text{otherwise} \end{cases} \tag{5.2}$$

$$tol_d = \frac{W}{4} \tag{5.3}$$

where n_{gtm} is the number of GTMs, d is the Euclidean distance[9] between GTM and the nearest AGM, tol_d is a maximum tolerated distance, W is a space between parallel thinned papillary lines, p is a general punishment (general cost-factor), and mcs_i is the so called „minutia conformance score“ of the i-th minutia. The value of tol_d was intentionally chosen to be equal to $W/4$ since this is the maximal possible radius around a GTM, such that two areas of commonly located neighbored GTM (e.g., two opposite ridge endings) will not overlap each other.

Afterwards, the general cost-factor p for each found minutiae pair (GTM - AGM) is evaluated using the following equations:

$$p = p_{\Delta\theta} + p_{\Delta t} \tag{5.4}$$

$$p_{\Delta\theta} = \frac{|\theta_{gtm} - \theta_{agm}| * 0.5}{\pi} \tag{5.5}$$

$$p_{\Delta t} = \begin{cases} 0.25 & \text{if} \quad t_{gtm} \neq t_{agm} \\ 0 & \text{otherwise} \end{cases} \tag{5.6}$$

[7] Ground Truth Minutiae.

[8] Automatically Generated Minutiae.

[9] Euclidean distance between two points in 2D space is computed using Pythagorean formula [131].

where $p_{\Delta\theta}$ is a punishment for imprecise setting of the minutiae angle, $p_{\Delta t}$ is a punishment for imprecise setting of the minutiae type, θ_{gtm} is an angle of reference GTM, θ_{agm} is an angle of assessed AGM, t_{gtm} is a type of reference GTM and t_{agm} is a type of assessed AGM.

According to the proposed Equations 5.4 - 5.6, several cost-factors (punishments) can be obtained for each minutiae pair (GTM - AGM). As it was discussed earlier, there is no punishment for different minutiae quality value, because there is no standardized algorithm or procedure to determine the quality of particular minutiae yet.

The first cost-factor ($p_{\Delta\theta}$) describes the difference between angle of GTM (θ_{gtm}) and angle of corresponding AGM (θ_{agm}). The value of this punishment is not constant, but it is calculated according to the distance between these two angles (see Equation 5.5). The maximal value of this cost-factor is 0.5 and the minimal is 0. The value of the second cost-factor is constant (0 or 0.25). This value describes whether or not the type of GTM is the same as the type of AGM (see Equation 5.6). These two values are summed and the result is the final cost-factor for the particular minutiae pair.

The different maximal value of punishment for different deficiencies (see Equations 5.5 and 5.6) was chosen intentionally. The results of recent studies have shown that the strongest impact on interoperability, i.e. the results of automatic minutiae extraction and comparison algorithms, has the inaccuracy in minutia location, less relevant is the inaccuracy in minutia angle and the least relevant is the inaccuracy in the minutia quality.

This conformance rate expresses the quality of minutiae placement and quality of assessment of minutiae parameters according to the clustered opinion of human dactyloscopic experts (GTMs).

5.3.2 Second conformance rate

The second conformance rate cr_{agm} describes the proportion of false minutiae placed outside or at the border of fingerprint area.

$$cr_{agm} = \frac{\sum_{i=1}^{n_{agm}} mps_i}{n_{agm}} \tag{5.7}$$

$$mps_i = \begin{cases} 0 & \text{if} \quad agm \quad \text{is outside the fingerprint area} \\ 0.5 & \text{if} \quad agm \quad \text{is at the borderline} \\ 1 & \text{otherwise} \end{cases} \tag{5.8}$$

where n_{agm} is a number of AGMs and mps_i is the so called „minutia position score“ of the i-th minutia.

This conformance rates express the quality of fingerprint area extraction algorithm, which is an essential part of each automatic minutiae extraction algorithm. The false minutiae located at the borderline are considered of be less severe mistakes, because they can be caused by inaccuracies of the fingerprint area extraction part of the tested algorithm (unit under test). On the other hand, the false minutiae outside the fingerprint area can point to a more severe problem - the absence of whole fingerprint area extraction part.

5.3.3 Third conformance rate

The third conformance rate cr_{amf} is the complement to the previous two conformance rates. It can be calculated using Equation 5.9:

$$cr_{amf} = 1 - \frac{n_{iagm}}{n_{agm}} \tag{5.9}$$

where n_{iagm} is a number of AGMs, which are inside the fingerprint area and does not correspond to any GTM and n_{agm} is a number of all AGMs.

This conformance rate gives us an overview, how many unpaired AGMs are inside the fingerprint area. This conformance rate is very easy to compute, but it is an essential part/complement to the first two conformance rates. If this rate was omitted, the automatic minutiae extraction algorithm would place minutiae in every pixel in the fingerprint area in image and the first two conformance rates would rate it as the conformant algorithm.

5.4 Process of computation of conformance rates

The computation of the conformance rates is not a simple process. Its whole workflow can be seen in Fig. 5.7.

The input data is the image containing fingerprint and the data (templates in *.gtm file format) collected from experts. Generally, it can be said that there are four processes that have to be performed before the start of the final computation of conformance rates:

Automatic minutiae extraction. The minutiae extraction algorithm under test is used to generate the set of AGMs for each fingerprint image in the GTD database. The AGMs stored in the vendor specific template or ISO template are converted to the *.gtm file format for greater clarity.

Fingerprint area extraction. For the purposes of computation of the second conformance rate cr_{agm}, it is necessary to precisely determine the fingerprint area in the image. This process is described in Section 5.4.1.

Determination of the space between ridges. It is necessary to know the space between two thinned parallel papillary lines (labeled as W) for the purposes of computation of first and second conformance rate and also for the purposes of clustering of data from experts.

Originally, it was intended that this task would be done automatically by an appropriate algorithm. The first tests of the conformance rates computation were performed with the manual determination of the papillary line width. During these tests, it was found that the difference among the values of papillary line width from one image is practically the same as the difference among various fingerprints. All these values are very similar (approx. in the interval from 9 to 13 pixels, that we decided to set (to round) the value of papillary line width as a constant value $W = 12px \Rightarrow W/4 = 3px$.

Clustering of the data from experts. This is the most complex part of the whole process of computation of conformance rates. It is necessary to cluster the minutiae from templates provided by dactyloscopic experts, compute the cluster centers and create so called Ground Truth Minutiae (GTMs). This process is described in Sections 5.4.2 and 5.4.3.

Finally, the results from previously described processes (AGMs, fingerprint area, space between parallel ridges, and GTMs) are taken as the input to the computation of the semantic conformance rates.

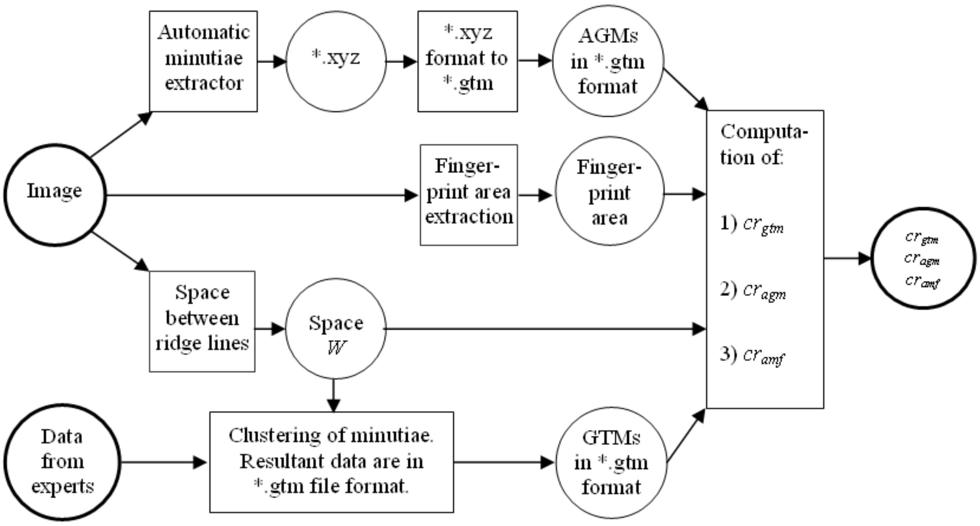


Figure 5.7: Process workflow to determine conformance rates.

5.4.1 Fingerprint area detection

The fingerprint area detection pipeline was designed by Mr. Doležel under my leadership and in my cooperation. The pipeline was based on the approach proposed by Alonso-Fernandez et al. [4]. The final pipeline consists of 6 phases:

1. **Fingerprint pre-processing.** This phase is used to enhance the input fingerprint image and to make a segmentation methods more accurate (see Fig. 5.8 a, b). In this phase, three pre-processing algorithms are used. At first, the gray-scale conversion is used to make the pipeline resistant to the incorrect inputs (color images). Then the contrast stretching (to deal with too bright or too dark images) and semi-thresholding (for the noise elimination) are used.

2. **Application of Gabor filters.** This phase is based on method proposed by Alonso-Fernandez et al. [4]. Our approach also uses the computation of magnitude Gabor feature g:

$$g(x, y, \theta, f, \sigma_x, \sigma_y) = \left| \sum_{x_0=-\frac{W}{2}}^{\frac{W}{2}-1} \sum_{y_0=-\frac{W}{2}}^{\frac{W}{2}-1} I(x + x_0, y + y_0) h(x_0, y_0, \theta, f, \sigma_x, \sigma_x) \right| \tag{5.10}$$

   where X and Y are coordinates of center of block, θ is rotation, f is frequency, σ_x and σ_y are parameters of the Gaussian envelope, W is the size of block (even number), $I(X, Y)$ is level of gray for pixel at (X, Y) coordinates and h is the 2D Gabor function.

   Nevertheless, our approach contains several improvements to achieve smoother and more precise fingerprint segmentation:

   - Smaller blocks (6 × 6 px).
   - Maximal overlapping (5px) in both directions.

- Computation of average magnitude Gabor features for every pixel.

The result of this phase can be seen in Fig. 5.8 c).

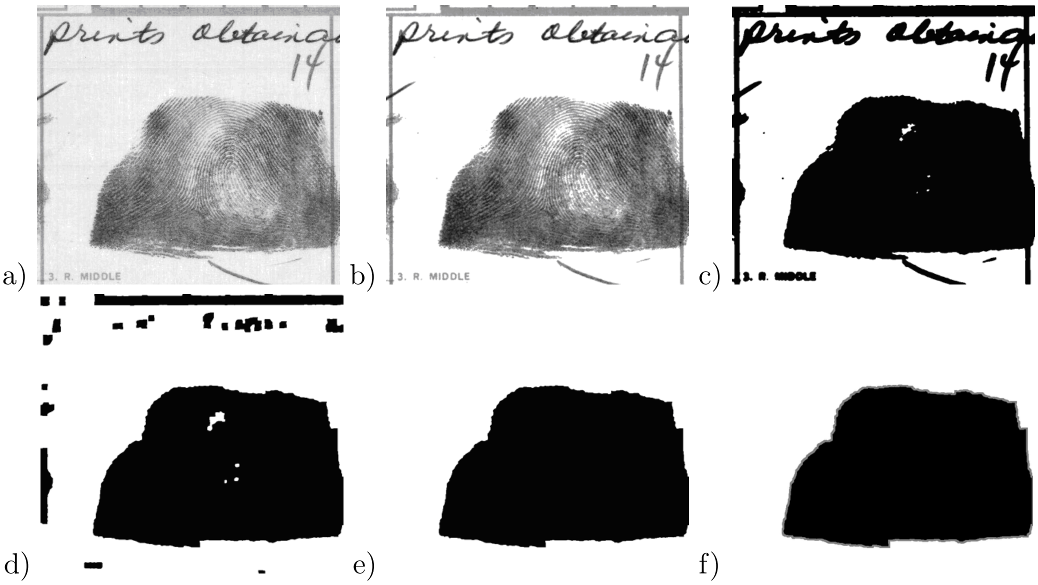


Figure 5.8: Fingerprint area extraction pipeline: a) original fingerprint, b) after the preprocessing phase c) application of Gabor filters, d) artifacts removal, e) holes and insignificant areas removal, and f) fingerprint border detection.

3. **Erosion.** The segmented area is slightly larger than the original fingerprint, so the omnidirectional morphological erosion [21] 6 × 6px is used to solve this problem.

4. **Artifacts removal.** It is necessary to remove artifacts like drawing or lines in the dactyloscopic card, which were identified as fingerprint area. For this purposes, it is created a copy of processed image and the binary opening [21] (specifically binary erosion 15 × 15px and dilatation 17 × 17px) is applied to it. The result of this phase is a logical conjunction of the enhanced copy of processed image and the processed image itself (see Fig. 5.8 d).

5. **Removal of holes and insignificant areas.** The image after application of artifacts removal process may contain several holes inside the fingerprint area and also several insignificant area/noise identified as small foreground areas. At first all white areas (background areas) are identified and their size in pixels is computed by the usage of the flood seed fill algorithm [129]. Then the largest area(s) is (are) marked as background and other areas are filled with black using flood seed fill algorithm. The removal of insignificant foreground areas is done similarly. The example of the result can be seen in Fig. 5.8 e).

6. **Fingerprint border detection.** The final phase is quite easy. It is necessary to draw a gray line (RGB: 128, 128, 128) around the detected fingerprint area. The line is 6 px thick, which corresponds to the average width of papillary line in GTD database. This color scheme (white background, gray border of fingerprint area, black inside fingerprint area) is chosen intentionally to simplify the process of computation of second conformance rate cr_{agm}. The detection whether the AGM is outside, at

the border or inside the fingerprint area can be done by using of AGM position and reading of color at the same coordinates in the fingerprint area image. The resultant detected fingerprint area can be seen in Fig. 5.8 f).

5.4.2 Clustering of data from experts

Every fingerprint is evaluated by several dactyloscopic experts. It can be expected that the records describing one fingerprint by different experts will be similar, but they will not be identical. Even a dactyloscopic expert is a human being and she/he can make a mistake, can have different opinion than his colleagues or can find minutiae overlooked by her/his colleagues. It is not possible to determine whether the particular minutia is correct on the basis of fingerprint image and one or two *.gtm files, but it is possible to determine the confidence percent of minutiae occurrence by the clustering of the data from experts and quality of the cluster calculation.

The procedure is quite comprehensive. In the first phase, it is necessary to create several auxiliary sets of clusters with different cardinalities $A_1 - A_{n_{exp}}$. The resultant set of clusters C is created on the basis of the auxiliary sets. The second phase consists of computation of cluster centers according to positions, types, orientation and quality of cluster members. The last phase is the determination of the quality/reliability of clusters and the determination of the threshold for cluster centers to be a ground truth minutia.

The clustering of minutiae from experts is a nontrivial task, because the number of clusters is not known. To solve this problem, I have proposed an approach inspired by the Apriori algorithm [75] and general principle of hierarchical clustering [75]. All elements in the resultant cluster have to meet the following two conditions:

- Each element (minutia) is placed by different dactyloscopic expert.
- The Euclidean distance of an arbitrary pair of elements (minutiae) in cluster is less or equal to $W/2$ (all elements have to be approximately in the circle with radius $W/4$[10]).

The clustering procedure is quite simple. At first the auxiliary sets of n-set are created. Then the set of minutiae clusters is computed on the basis of auxiliary sets. At the end, the cluster center is computed.

Lets begin with the description of creation of auxiliary sets. The principle is quite simple. At the beginning, the set A_1 is designed to contain all minutiae from all experts. Then the set A_2 is created to contain 2-sets, where both elements (minutiae) follow the above-mentioned rules.

$$A_1 = \left\{ a \;\middle|\; a \subset \bigcup_{u=1}^{n_{exp}} T_u,\ |a| = 1 \right\} \tag{5.11}$$

$$A_2 = \left\{ a \;\middle|\; a \subset \bigcup_{u=1}^{n_{exp}} T_u,\ |a| = 2,\ \forall r \in \{1,2,3,..,n_{exp}\} : a \not\subset T_r,\ d(a) \leq \frac{W}{2} \right\} \tag{5.12}$$

where T_u is a template created by the expert u and $d(a)$ is the Euclidean distance between two elements in 2-set a.

[10] It is necessary to mention that all values are in pixels and the circle is very serrate, especially because the $W/4$ is equal to 3px.

Generally, the Euclidean distance $d(\{e_1, e_2\})$ between two elements $e_1 = (x_1, y_1)$ and $e_2 = (x_2, y_2)$ is computed simply by the Pythagorean formula [131]:

$$d(\{e_1, e_2\}) = \sqrt{(x_1 - x_2)^2 + (y_1 - y_2)^2} \tag{5.13}$$

Then the set A_3 is constructed to contain 3-sets where the same rules as in case of set A_2 are applied.

$$A_3 = \left\{ a \;\middle|\; a \subset \bigcup_{u=1}^{n_{exp}} T_u,\ |a| = 3,\ \binom{a}{2} \subset A_2 \right\} \tag{5.14}$$

The other auxiliary sets are constructed in the same way (see Equation 5.15). The maximal index of auxiliary set is equal to the n_{exp} (number of participating experts), because it is not possible to create a set containing more than n_{exp} elements when every two elements have to be given by different experts.

$$\forall i \in \{3, .., n_{exp}\}:\ \ A_i = \left\{ a \;\middle|\; a \subset \bigcup_{u=1}^{n_{exp}} T_u,\ |a| = i,\ \binom{a}{i-1} \subset A_{i-1} \right\} \tag{5.15}$$

After the creation of auxiliary sets, it is possible to proceed to creation of the resultant set of clusters C. This set consists of all elements from sets $A_1 - A_{n_{exp}}$, which was not a subset of any element with higher cardinality:

$$\forall r \in \{1, 2, 3, .., n_{exp} - 1\}:\ \ C = \{c \mid c \in A_r,\ \forall b \in A_{r+1} : c \not\subset b\} \cup A_{n_{exp}} \tag{5.16}$$

The implementation of the clustering algorithm described in Equations 5.11 - 5.16 is adjusted to achieve higher robustness and speed. At the beginning, the array of all minutiae[11] A_1 from all experts is created. Then the array A_2 of minutiae pairs is created according to the above-described rules. If the element from array 1 is used for the creation of a minutiae pair in the array 2, then it is marked as „used“.

The adjustment is made in the process of creation of arrays number 3 or more. For the purposes of simplifying and clarification of the source code and the whole process, it was not suitable to check whether all possible combinations of the n-set are present in the array number $n - 1$ (e.g., in case of $n = 11$, eleven possible combinations of the elements from 11-set in 10-set can be found). The adjustment consists in finding of two $(n-1)$-sets, which contain $n - 2$ identical elements (minutiae) and computation, whether the two elements outside the intersection of these two sets meet the conditions described at the beginning of this section. The graphical example of creation of 3-set and 4-set is given in Fig. 5.9).

5.4.3 Determination of cluster center - ground truth minutia

Determination of the cluster center and its characteristic is a non-trivial task. It is necessary to compute the x- and y-coordinates, type, angle and quality of the cluster center.

[11] In this case, minutia is a struct with values: expert ID, type, x-coordinate, y-coordinate, angle, quality, and boolean marker used/not used with default value „not used“.

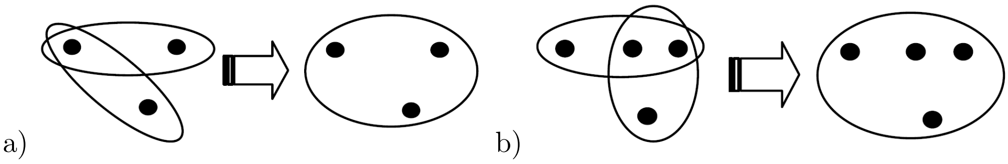


Figure 5.9: Example of the process of a) 3-set and b) 4-set creation.

Lets start with the computation of x- and y-coordinates of the cluster center. Generally, there are two different approaches to compute the coordinates of the cluster center. The first approach is the computation of average value of x-coordinate (and the y-coordinate) of all minutiae in this cluster. The second approach computes just the average of the minimum and maximum value of x-coordinates of all minutiae in this cluster (and y-coordinates respectively). The impact of these two methods in an extreme situation is illustrated in Fig. 5.10. The first method (see Fig. 5.10 b and d) sets the cluster center position according to the prevailing opinion of experts. Nevertheless, the newly created point would not include the tested point in its neighborhood, although the tested point could be included in the original cluster.

The second method includes our hypothetical tested point both in the original cluster and in the neighborhood of the cluster center position. On the other hand, this method does not respect the prevalent opinion of experts and ignores the possibility of an error of the single expert. In case of usage of the second method, the wrong position from one expert could devalue the work of several dozen experts. These reasons led to the usage of the first method in my work.

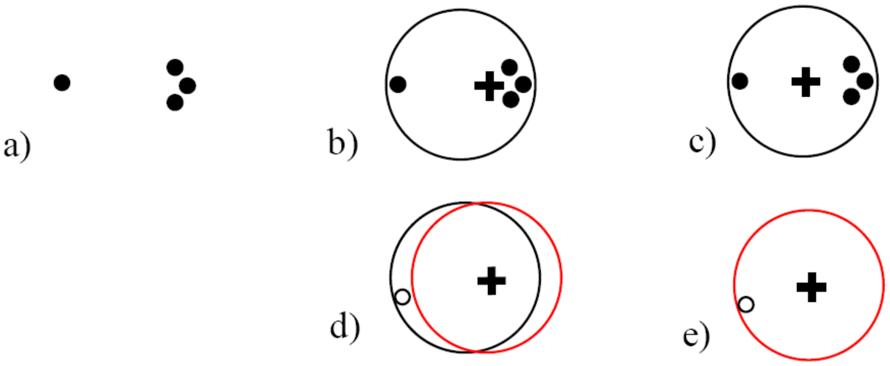


Figure 5.10: Comparison of two methods for computation of the cluster center. a) The clustered minutiae. b, d) Cluster center computed as an average of all x-coordinates. c, e) Cluster center computed as an average of minimum and maximum of x-coordinates. The minutiae placed by experts are drawn as black dots, the tested point as the white dot and the cluster centers as black crosses. The area of cluster with radius $W/4$ is drawn as black line and the circle with radius $W/4$ centered at cluster center is drawn by red line.

Secondly, it is needed to determine the type of the cluster center. It is not possible to compute an average value of minutiae type. Because the semantic conformance testing has been developed primarily for the purposes of ISO standard, the determination of cluster center type is based on the ISO directives: the type is assigned, if more or equal to the 2/3 of the experts assigned the same type to the cluster members, otherwise the cluster center type (and thus ground-truth-minutia type) is set to UNKNOWN (numbered as 4). In case of computation of cr_{gtm} conformance rate, the punishment for wrong minutia type is not applied.

Then it is necessary to compute the angle of cluster center. The computation is not as easy as it looks like, because it is not possible to use the common average. Lets assume that there are two angles from experts $\theta_1 = 0°$ and $\theta_1 = 180°$, or three angles from experts $\theta_1 = 0°$, $\theta_2 = 120°$ and $\theta_3 = 240°$. What should be the average angle in such situations?

The method for computation of the angle of the cluster center has to deal with such situations and also it has to be robust and has to allow to determine, whether the consensus[12] is achieved.

During the algorithm programming, I did not know and I was not able to find any method that could meet these criteria, so I created my own. The principle is simple:

1. Imagine that all angles of all minutiae in cluster are unit vectors (vectors with length equal to one) so, that the endpoints of these vectors lie on the circle with radius equal to one.

2. Compute the average x-coordinate and average y-coordinate of these vectors (Eq. 5.17 and 5.18).

$$x_\theta = \frac{\sum\limits_{u=1}^{n_{cl}} \cos\theta_u}{n_{cl}} \tag{5.17}$$

$$y_\theta = \frac{\sum\limits_{u=1}^{n_{cl}} \sin\theta_u}{n_{cl}} \tag{5.18}$$

   where n_{cl} is the number of minutiae in this cluster.

3. The resultant coordinates (x_θ, y_θ) can be imagined as the endpoint of the resultant vector.

4. Whether the length of the resultant vector is greater or equal to 1/3, then the angle of this vector is the angle of the cluster center, otherwise the angle is marked as UNKNOWN (numbered as 256[13]).

$$_c\theta = \begin{cases} \arccos\left(\frac{x_\theta}{\sqrt{x_\theta^2+y_\theta^2}}\right) & \text{if } \sqrt{x_\theta^2+y_\theta^2} \geq \frac{1}{3} \wedge y_\theta \geq 0 \\ 360° - \arccos\left(\frac{x_\theta}{\sqrt{x_\theta^2+y_\theta^2}}\right) & \text{if } \sqrt{x_\theta^2+y_\theta^2} \geq \frac{1}{3} \wedge y_\theta < 0 \\ UNKNOWN & \text{otherwise} \end{cases} \tag{5.19}$$

The threshold $T = 1/3$ corresponds to the previously described consensus (2/3 majority). For example, the experts may set the angles of minutia at $\theta_1 = 0°$, $\theta_2 = 180°$, $\theta_3 = 0°$. In such borderline case, the average coordinates will be $(x_\theta = 1/3, y_\theta = 0)$ and the length of such vector will be equal to 1/3.

[12] A majority of 2/3 of national bodies (or committee members) manifests consensus (according to the ISO directives).

[13] The values of angles contained in *.gtm file format are ISO/IEC 19794-2:2005 compatible. It means that all values in degrees are converted into values in interval from 0 to 255 and thus the value 256 can be used as the indication of UNKNOWN angle.

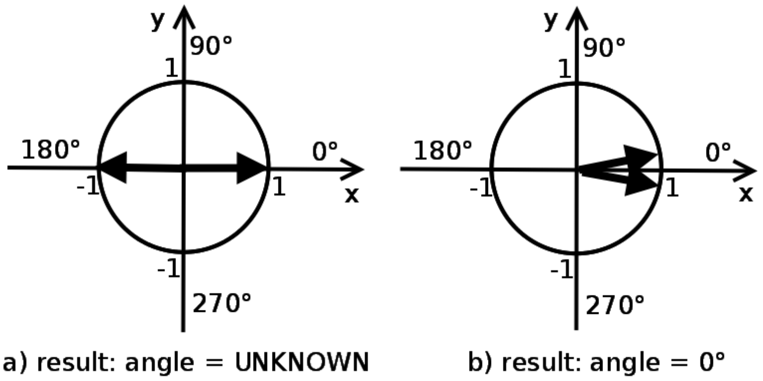


Figure 5.11: Example of computation of average angles. a) The input angles are opposite, so the resultant angle is UNKNOWN. b) The input angles are not too distant and resultant angle is equal to 0°.

At the end, it is necessary to determine the quality of cluster. Whereas the quality of minutia is understood as the percentage of certainty of experts concerning the minutia, it can be stated, that the expert, who did not find this particular minutia, stated the quality value as zero. It follows that the quality of cluster can be computed as the average of values from all experts contributing to this image (including experts, who do not contribute to this particular cluster):

$$q_{cl} = \frac{\sum\limits_{u=1}^{n_{cl}} q_u}{n_{exp}} \tag{5.20}$$

where q_{cl} is the quality of cluster and q_u is the quality of the u-th minutia in this cluster.

5.5 Evaluation results

During the methodology development and after its finalization, many tests were performed. It started with the tests, which were used as one of the basis for analysis of the situation (see Section 5.1). Then the preliminary tests of the methodology were conducted on the limited fingerprint dataset (see Section 5.5.1). Whereas the tests were successful, the evolution continued by the development of the fingerprint area extraction algorithm (see Section 5.4.1) and its proper testing (see Section 5.5.3). These tests were followed by the proper tests of the whole methodology on the extended fingerprint dataset (see Section 5.5.5) and the tests of influence of reliability of clusters (see Section 5.5.4).

For the testing purposes, three minutiae extraction algorithms were used:

- `mindtct` from NIST NBIS[14] package (Rel 1.1.0)[15] [73],
- Innovatrics ANSI and ISO SDK[16] v 1.52[17] [93],

[14] NIST Biometric Image Software.

[15] It has to be said that the NIST algorithm was developed independently on the special databases (SD14 and SD29), and these databases are publicly available.

[16] Software Development Kit.

- VeriFinger 6.1 SDK from NeuroTechnology[17] [108].

5.5.1 Preliminary tests

Preliminary tests were performed on a small fragment of GTD database. Only 17 images were used, but they were processed by 11 dactyloscopic/forensic experts from German Federal Criminal Police Office (BKA). These tests were focused on the tests of implemented programs (programs for generation of AGMs in *.gtm file format, clustering of data from experts, computation of the cluster center, and computation of the conformance rates). The fingerprint area, space between and threshold for the cluster quality ridges were computed/chosen manually. The intention of these preliminary tests was also to check, whether the values of conformance rates are meaningful and whether there are any problems or misunderstanding on our side or by experts.

The tests were successful. There were no problems with the above mentioned programs and the values of conformance rates were as expected (see Tab. 5.1). Unfortunately, the licenses for extractors from Innovatrics and NeuroTechnology were not available at that time; so all tests were performed only for `mindtct` from NIST.

Table 5.1: The results of preliminary tests of semantic conformance testing methodology for `mindtct` from NIST. The threshold of cluster quality was set to the 37.

Average (std. dev.)	cr_{gtm}	cr_{agm}	cr_{amf}	n_{gtm}	n_{agm}
NIST	0.353 (0.179)	0.885 (0.066)	0.338 (0.178)	59 (-)	100 (-)

During the studying of the test results, I found that there are some misunderstandings among us and dactyloscopic experts regarding the definition of some minutia types and their marking (e.g., difference between dot and short ridge has been clarified), which led to the refinement of the harmonized dactyloscopic dictionary.

5.5.2 Tested dataset

The GTD database is continuously processed by dactyloscopic/forensic experts from BKA (Germany) and other institutions (countries).

For the purposes of careful testing, we have received the first part of GTD (1 180 images) processed by experts from BKA. The dataset was processed by six different dactyloscopic experts. Unfortunately, not all of the processed images could be used. Some of the images were processed by only two experts, which makes them unusable, because it is not possible to establish consensus based on the opinion of two persons (see Tab. 5.2).

Another problem was discovered during the manual fingerprint area extraction. A lot of fingerprint images were cut from the dactyloscopic card automatically without any manual correction. In case of images originating from SD14 database it sometimes happen, that the fingerprint is not impressed exactly in the middle of appropriate box, but it overlaps in the next box and thus the automatically cut fingerprint-box contains (part of) two different fingerprints. This situation is not considered to be correct and such fingerprints have to be excluded from the tested database.

[17] The algorithms from NeuroTechnology and Innovatrics were chosen, because they are often used for the testing purposes. They are not specialized on a particular type of fingerprints and they declare to be able to work with impressions captured by broad spectrum of sensors/technologies.

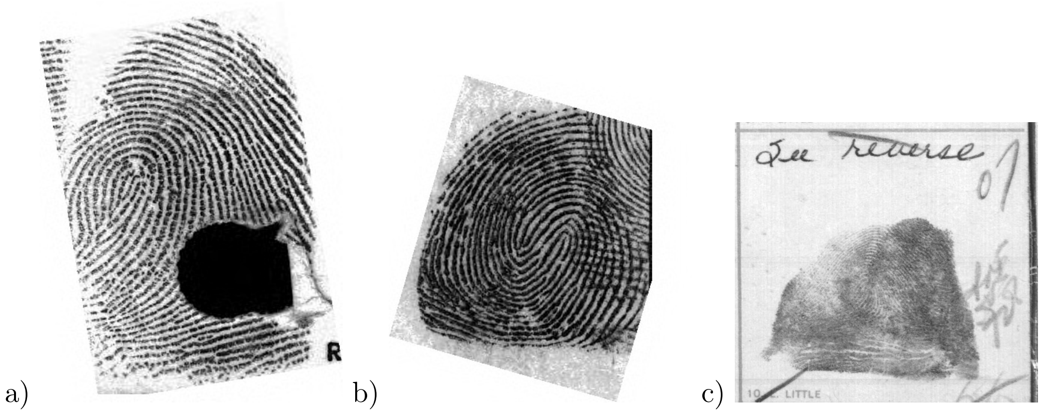


Figure 5.12: Image problems occurred in the GTD: a) black circle, b) two fingerprints in one image, and c) low quality fingerprint (resulted in template problem).

The fingerprints originating from SD29 database sometimes tend to have another problem. The images can contain the big black circle (mostly located in the middle of fingerprint and covering a large part of fingerprint area - see Fig. 5.12 a). In my opinion, this black circle may be caused by a common office punching machine, which corresponds to the distance between the black circles on the dactyloscopic card (see Fig. A.3).

Table 5.2: The tested database: number of fingerprints excluded from the processing and the reason of removal.

	GTD-SD14	**GTD-SD29**	**GTD**
Processed images	**700**	**480**	**1 180**
Image processed by less than 3 experts	6	199	205
Two fingerprints in one image	201	16	217
Image problem: black circle	0	17	17
Template problem[18]	7	1	8
Total	**486**	**247**	**733**

5.5.3 Tests of fingerprint area extraction

The developed segmentation pipeline was compared with/tested against five well known fingerprint segmentation algorithms:

- `Segmentor` from NIST NBIS package (Rel 1.1.0) [73]:

  This algorithm is provided by NIST. It uses a special thresholding based on local and global pixel intensity, erosion and edge detection. The result is the fixed size rectangle, which makes this algorithm useless for our purposes.

- NFIQ from NIST NBIS package (Rel 1.1.0) [73]:

[18] In a few isolated cases, one or more algorithms have a problem with the template creation. These images were excluded, because the goal of these (or future) tests is not an assessment of biometric performance of a particular algorithm, but the creation of a correct database.

NFIQ is fingerprint image quality value developed and used by NIST. The NFIQ values are in range 1 (highest quality) to 5 (lowest quality).

- Ratha algorithm [50]:

  This algorithm uses the orientation field to compute dominant ridge direction. Then the variance of the gray level is computed. The variance of foreground areas is very high but the variance of background is quite low.

- Alonso-Fernandez Gabor filter based algorithm [4] (basic and enhanced version):

  Alonso-Fernandez et al. proposed a new application of Gabor filters. At first the so-called magnitude Gabor features are computed using several differently oriented Gabor filters. The fingerprint is segmented using a threshold, which is equal to the standard deviation of the magnitude of Gabor filters for each block. This algorithm works quite well (small problem is a serrated border of fingerprint area) in case of good-quality fingerprint placed on clean background. Nevertheless, it does not work well for the images scanned from dactyloscopic cards (see Fig. 5.13 e). The enhancement proposed by Alonso-Fernandez et al. (e.g., half block overlapping or ridge frequency computation) were also implemented, but the results were even little bit worse (see Fig. 5.13 f).

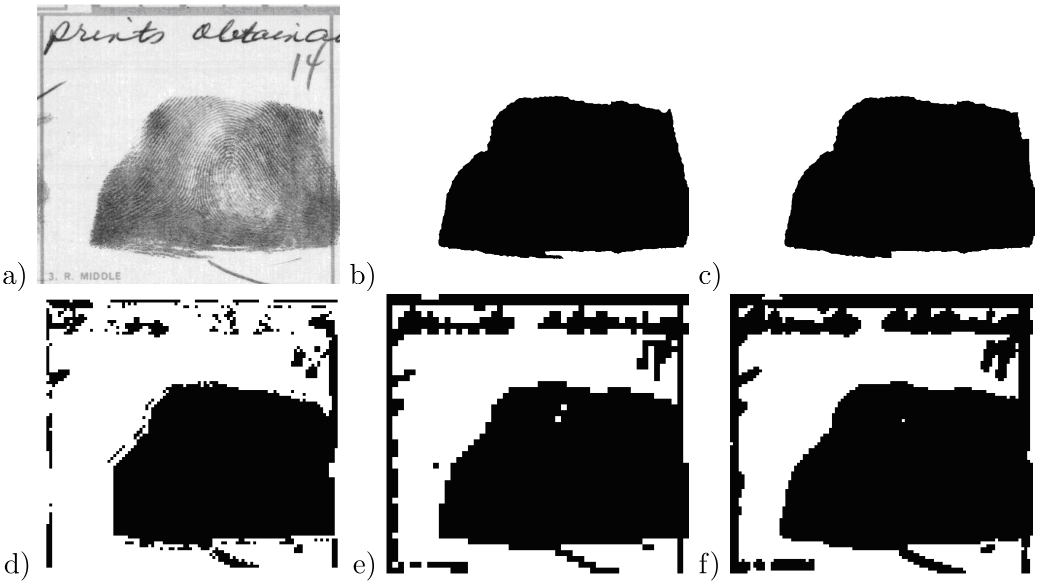


Figure 5.13: Comparison of results of different fingerprint area extraction methods: a) tested fingerprint, b) fingerprint area extracted manually, fingerprint area extracted c) by our algorithm/pipeline, d) by NIST NFIQ quality map with threshold $T = 2$, e) by basic Gabor filter-based algorithm [4], and f) by enhanced Gabor filter-based algorithm (enhancement proposed by Alonso-Fernandez) [4].

The comparison of our pipeline with different fingerprint segmentation algorithms can be found in Table 5.3. It can be seen that our segmentation pipeline gives several times better results than other algorithms. In case of tests on the GTD-SD14 database, the second best results are given by NFIQ algorithm from NIST NBIS package [73]. Nevertheless, in case of GTD-SD29 database, the NFIQ algorithm and the basic Gabor filter based algorithm are the second bests. In all cases, the enhanced Gabor filter based algorithm achieves worse results than the basic variant. Moreover, it has been shown that the default threshold value of NFIQ determination algorithm is not the best choice for these purposes.

Table 5.3: The results of tests of different fingerprint segmentation algorithms based on the comparison with the manual fingerprint extraction. The value of 0% indicates the absolute overlap between the manually extracted area and the automatically extracted area and 100% indicates absolute difference, i.e. inverted selection.

Database	GTD-SD14		GTD-SD29	
Method/Algorithm	Mean (%)	Median (%)	Mean (%)	Median (%)
Our segmentation pipeline	5,531	3,324	4,407	2,775
NFIQ best threshold[19]	10,519	10,195	7,502	6,907
NFIQ default threshold $T = 3$	11,867	10,844	16,639	15,637
Gabor Filter-Based algorithm [4]	13,830	13,453	7,538	6,662
Gabor Filter-Based algorithm (with enhancement proposed by Allonso-Fernandez) [4]	15,766	15,438	8,637	7,653

Although our fingerprint area extraction algorithm/pipeline proved to be much better than the competing algorithms, we decided to use manually extracted fingerprint areas to increase preciseness. The results of our fingerprint area extraction pipeline (without the border detection phase) were used as the base for manual extraction. The original fingerprint and the automatically extracted area (as a semi-transparent mask) were loaded into the GSegmentator program (author: Mr. Doležel [15]) and then we have manually corrected the particular part of detected area. At the end, the borders of fingerprint area in the manually extracted results were detected and drawn.

5.5.4 Tests of reliability of clusters

The importance of process of minutiae clustering, quality of cluster determination and thresholding (creation of GTMs) is illustrated in Fig. 5.14 (the visualized data comes from preliminary tests - see Section 5.5.1 for more information). In the first part (see Fig. 5.14 a), the minutiae placed by dactyloscopic experts are drawn. It can be seen that the minutiae in the bottom-right corner of the image create nice cluster with the almost perfect consensus regarding minutia position and type (ridge ending). This cluster is created by 7 of 8 contributing experts and its quality is equal to 64. In the upper-left corner of image, the different situation can be seen. There are two minutiae of „other“ type quite distant to each other. The minutiae are set by different dactyloscopic experts and it is very likely that they did not mean the same minutiae.

The second image (see Fig. 5.14 b) illustrates the situation after clustering; only cluster centers are drawn. There are three cluster centers, because two minutiae located in the upper-left image corner were too distant from each other to create one minutiae cluster.

The third image (see Fig. 5.14 c) shows us the situation after application of the quality of cluster threshold ($T = 37$ - see Section 5.5.1). The cluster centers in the upper-left corner disappeared, because the quality was equal to 6 (in both cases). On the other hand, the

[19] The best results are given using the threshold $T = 2$ for GTD-SD14 database and the threshold $T = 1$ for GTD-SD29 database.

cluster center in the bottom-right image corner is considered to be a ground-truth-minutia, because its quality ($q = 64$) exceeded the threshold.

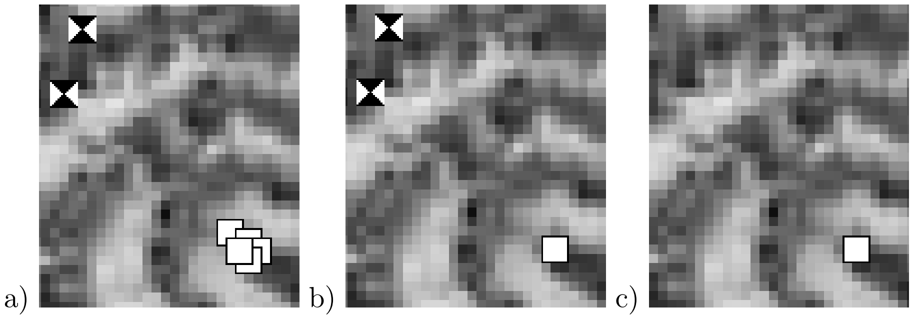


Figure 5.14: Process of creation of ground-truth-minutiae: a) Clustering of minutiae placed by dactyloscopic experts. b) Computation of cluster centers. c) Selection of high quality clusters as the ground-truth-minutiae. The ridge endings are drawn as squares and minutiae of „other" type are drawn as square filled by black and white triangles.

The detailed influence of application of the cluster quality threshold can be seen in Fig. 5.15. The data used for these tests are equal to the dataset used for the final tests in Section 5.5.5. The maximal value of cluster quality threshold is 90, because this is the highest value that can be set by dactyloscopic experts. The lowest value of cluster quality threshold is 0, because this value is understood as an indication of a missing minutia during the computation of cluster quality. It means that the quality of cluster can be even lower than the lowest value that can be inserted by an expert using „GUI for dactyloscopy" program.

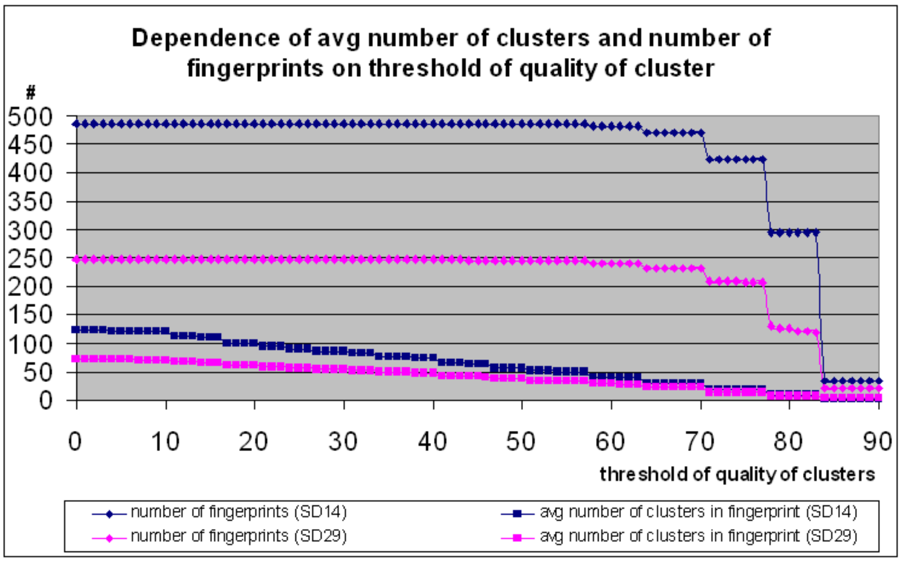


Figure 5.15: Dependence of number of fingerprints and average number of clusters in fingerprints on threshold of cluster quality. Fingerprints without any cluster are not counted.

The graph in Fig. 5.15 shows that the average value of GTMs (clusters with the quality exceeding threshold) is almost constantly decreasing. On the other hand, all files (except one) contain at least one GTM for the threshold $T < 58$. Then the number of files containing at least one GTM is rapidly decreasing and in case of threshold $T = 84$, there are last few images (33 images from GTD-SD14 and 21 images from GTD-SD29) containing at least one GTM.

5.5.5 Final tests

Three conformance rates were performed on the dataset described in Section 5.5.2, it means 486 images from GTD-SD14 and 247 images from GTD-SD29 processed by 6 different dactyloscopic experts (3 opinions per image).

The series of tests was made. In many cases, the results computed for GTD-SD14 and GTD-SD29 are so different that it was necessary to display the results separately.

The first graph (see Fig. 5.16) shows the results of first semantic conformance rate cr_{gtm} for all used algorithms on GTD-SD14 database depending on threshold of quality of cluster.

The first part of all curves (the lower threshold values) shows the influence of inconsistence of opinions of experts. At the beginning ($T = 0$), all clusters are considered to be ground truth minutiae. Even the minutiae found by only one expert, low quality minutiae/clusters and minutiae located too far apart (inconsistence of experts opinion - minutiae form separate clusters) are included. This situation increases the number of ground truth minutiae and thus decreases the first conformance rate cr_{gtm}.

During the increase of threshold the value of first conformance rate is also increasing and the maximum value is reached approximately in the interval $T \in [45, 65]$. In the final part of conformance curves $T > 78$ the significant decrease of conformance rate is achieved and the curves have a staircase shape. This is caused by the significant (and staircase shaped) decrease of the number of appropriate-quality data in the dataset (see Fig. 5.15).

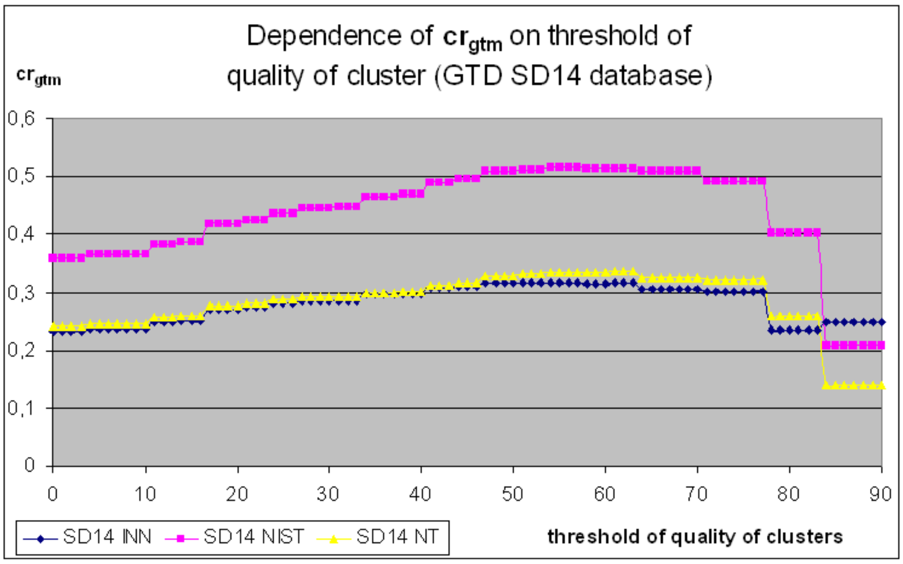


Figure 5.16: Dependence of cr_{gtm} on quality of cluster threshold for GTD-SD14 database. The algorithms from NIST, Innovatrics and NeuroTechnology are marked as NIST, INN and NT, respectively.

The example of the curves of all conformance rates for one algorithm and one database (NIST algorithm and GTD-SD29 dataset) is given in Fig. 5.17. It can be seen the almost constant value of the second conformance rate cr_{agm}. This rate assesses the degree of minutiae outside or at the border of fingerprint area and thus it is independent on the applied quality of cluster threshold (see Equation 5.8). The small oscillation is caused by the enormous decrease of used fingerprints. On the other hand, this oscillation is so small, that it proves the stability of second conformance rate. (The difference between the stable value and the highest oscillation is from one hundredth to several thousandths of cr_{agm} value for all used algorithms - see Appendix H.)

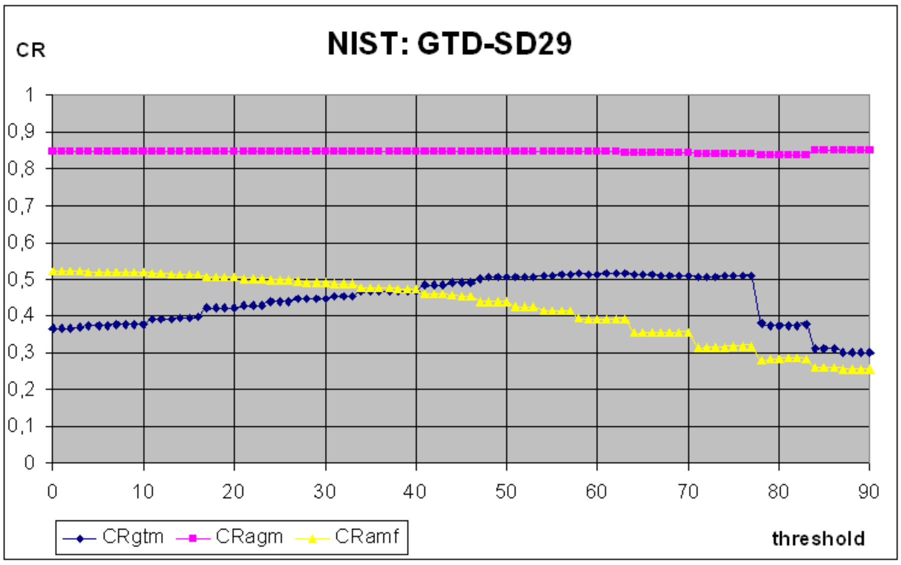


Figure 5.17: Dependence of conformance rates on quality of cluster threshold for GTD-SD29 database and algorithm from NIST.

The third conformance rate cr_{amf} is slowly decreasing during the increase of the threshold of cluster quality (see Fig. 5.17) as expected. This situation is caused by the decrease of the number of GTM, which causes the slight decrease of the GTM-AGM minutiae pairs and thus the slight decrease of third conformance rate (see Equation 5.9).

The short summary of results can be found in Table 5.4. The results for all conformance rates on both datasets (GTD-SD14 and GTD-SD29) are given for the thresholds of cluster quality $T = 60$ (consensus) and $T = 37$ (backward compatibility with the preliminary tests).

In case of first conformance rate cr_{gtm}, the NIST algorithm achieves much better results than the others. The results of other two algorithms are balanced, but it can be said that the algorithm from Innovatrics achieves slightly better results from GTD-SD29 dataset and the algorithm from NeuroTechnology is slightly more successful in case of GTD-SD14 dataset. Nevertheless, the difference is almost negligible.

The results for second conformance rate cr_{agm} are more surprising. In case of GTD-SD14 dataset, the first is algorithm from Innovatrics, the second one from NIST and the third one from NeuroTechnology. Nevertheless, the results of all used algorithms are balanced and the difference is very small. On the other hand, the results for GTD-SD29 database are very different. The algorithms from Neurotechnology and Innovatrics probably prefer this type of fingerprint images and their results are very good and better than in case of GTD-SD14 dataset. However, the algorithm from NIST has problems with this type of dataset (probably a problem with the fingerprint area extraction in these fingerprints). Its results are much worse than results of other algorithms and they are even worse than in case of GTD-SD14 dataset.

Table 5.4: The results of tests of semantic conformance testing methodology for `mindtct` from NIST, SDK from Innovatrics and Verifinger from NeuroTechnology. The threshold of cluster quality is marked as T.

			Average (std. dev.)				
Vendor	DB	T	cr_{gtm}	cr_{agm}	cr_{amf}	n_{gtm}	n_{agm}
NIST	14	37	0,464 (0,092)	0,857 (0,063)	0,355 (0,123)	76 (29)	202 (49)
INN	14	37	0,296 (0,075)	0,876 (0,078)	0,293 (0,097)	76 (29)	160 (39)
NT	14	37	0,300 (0,098)	0,839 (0,103)	0,333 (0,119)	76 (29)	147 (36)
NIST	29	37	0,468 (0,122)	0,847 (0,085)	0,478 (0,152)	49 (23)	89 (32)
INN	29	37	0,299 (0,100)	0,937 (0,054)	0,330 (0,118)	49 (23)	64 (24)
NT	29	37	0,295 (0,117)	0,974 (0,040)	0,308 (0,135)	49 (23)	54 (22)
NIST	14	60	0,514 (0,130)	0,857 (0,063)	0,286 (0,112)	41 (22)	202 (49)
INN	14	60	0,315 (0,106)	0,876 (0,078)	0,231 (0,095)	41 (22)	160 (39)
NT	14	60	0,335 (0,133)	0,838 (0,103)	0,273 (0,119)	41 (22)	147 (36)
NIST	29	60	0,514 (0,156)	0,847 (0,085)	0,393 (0,150)	28 (16)	89 (32)
INN	29	60	0,323 (0,138)	0,938 (0,055)	0,246 (0,111)	28 (16)	64 (24)
NT	29	60	0,317 (0,151)	0,974 (0,040)	0,215 (0,123)	28 (16)	54 (22)

In case of the third conformance rate cr_{amf}, the results of all three algorithms on both parts of dataset are very similar except one value. The value of conformance rate cr_{amf} for algorithm from NIST on GTD-SD29 database is much better than the others and generally it can be said that the algorithm from NIST is the best in this test - it extracts the minimal number of „false minutiae“ in proportion to the number of all extracted minutiae.

These conformance rates could also have other application than it was requested. The usage of three different rates allows to point out the strengths and/or weaknesses of tested algorithms. The additional graphs and results can be found in Appendix H.

5.6 Summary

The content of previous sections answers the questions asked at the beginning of this chapter. I analyzed the common problems of minutiae extraction algorithms and subsequently I proposed and tested methodology of the semantic conformance testing, which is able to deal with the described problems. In the meantime, I created the program „GUI for dactyloscopy“ for the purposes of the collection of opinions of experts. Moreover, I proposed and implemented the methods for clustering of these opinions and deal with their inconsistencies.

The semantic conformance testing methodology presented in this chapter was created as a contribution in response to the ISO/IEC SC37 N3058 (Call for Contributions on Metric for Measuring Accuracy of Minutiae Placement). The reaction was accepted well and I was invited to present the proposed methodology in the ISO/IEC JTC 1/ SC37 WG3 meeting in Moscow in June 2009. After the presentation, I (as a Czech National Body) created and submitted a New Work Item Proposal. It was decided that this topic will be intended to publish as an Amendment 2 of the international standard ISO/IEC 29109-2. Due to the big requirements to travel, I had to refuse a position of an editor and I am working as a co-editor since January 2010.

Nowadays (May 2012), the document ISO/IEC 29109-2 Amd. 2 is in the preparatory stage as the Fourth Working Draft (WD4[20]) and there is still much work to do before it will be published. In the meantime, my work was incrementally published, cited several times (see Appendix H) and was followed by Mr. Abt[21] (Germany) in his research (e.g., his work concerning clustering [2] or quality score [1]).

[20] For the description of standardization process see Appendix B.

[21] According to my knowledge, the work of Mr. Abt will probably be integrated into the Amd. 2 too.

Chapter 6

Conclusion and future work

The objectives of this thesis were to study theories of biometric systems security and to propose, create and test a new way to the protection of biometric systems. These objectives were met and I have presented two new securing of biometric systems.

My first contribution is the novel method of liveness detection based on the detection of changes of color and width of papillary lines. This method was patented (Czech utility model No. 19364), widely tested and the resultant liveness detection unit can be integrated into an optical fingerprint sensor. The advantages of this method are the capability of correct capturing of wet, dry or bended skin and also the short time necessary for capturing of the process of change. The disadvantage is the impossibility of correct capturing of contaminated skin (e.g., dyed by ink). Moreover, I proposed one future hardware improvement and two possibilities for the future research. The first possible direction of the future research could be the creation of an algorithm, which will be capable correctly deform papillary lines to reduce the unwanted effect of finger elasticity. The second possible direction of research is the definition of area of colors belonging to the live human fingertip in non-pressed and pressed state regardless to the skin color, gender, age, etc.

The second contribution is within standardization. I created a methodology to determine semantic conformance rates of minutiae extractors to increase security and interoperability of minutiae extraction and comparison process. Moreover, I prepared program „GUI for dactyloscopy“ for collection of opinions of forensic/dactyloscopic experts. I proposed and implemented methods to cluster these data and to deal with their inconsistencies, so the resulted data could be used as a part of Ground-Truth Database. Nowadays (May 2012), these equations are included into ISO/IEC 29109-2 Amd. 2, which is in the preparatory stage as WD4 and my work on this topic is followed by Mr. Abt in his research.

In this thesis, I have also shortly presented my other two smaller contributions to the securing of biometric systems and better understanding of fingerprints. The first topic is the patented unit for the finger vein detection (Czech utility model No. 21548 – co-author), which was intended to use separately or integrated into a common optical fingerprint sensor according to the principle of multi-modal biometrics. I have also presented the second topic; the short overview of the work about diseases (co-author) and other situations, which may influence the quality of captured fingerprint.

All of presented contributions were incrementally published in international journals and conference proceedings, and these papers were cited several times (see attached list of author's publications and research activities).

Bibliography

[1] ABT, S., BUSCH, C., BAIER, H.: A quality score honoring approach to semantic conformance assessment of minutiae-based feature extractors. In: *Proceedings of the Special Interest Group on Biometrics and Electronic Signatures* [BIOSIG2011]. Darmstadt (Germany): GI, 2011. pp. 21–32. LNI 191, ISBN 978-3-88579-285-7.

[2] ABT, S., BUSCH, C., NICKEL, C.: Applikation des DBSCAN Clustering-Verfahrens zur Generierung von Ground-Truth Fingerabdruck-Minutien [Application of DBSCAN Clustering Method to Generate Ground-Truth Fingerprint Minutiae]. In: *Proceedings of the Special Interest Group on Biometrics and Electronic Signatures* [BIOSIG2010]. Darmstadt (Germany): GI, 2010. pp. 95–106. LNI 164, ISBN 978-3-88579-258-1.

[3] ADLER, A.: Biometric System Security. In: JAIN, A. K., FLYNN, P., ROSS, A. A. (Eds.): *Handbook of Biometrics.* New York (USA): Springer, 2008. pp. 381–402. ISBN 978-0-387-71040-2.

[4] ALONSO-FERNANDEZ, F., FIERREZ-AGUILAR, J., ORTEGA-GARCIA, J.: An Enhanced Gabor Filter-Based Segmentation Algorithm for Fingerprint Recognition Systems. In: *Proceedings of the 4th International Symposium on Image and Signal Processing and Analysis* [ISPA2005]. Zagreb (Croatia): IEEE, 2005. pp. 239-244. ISBN 953-184-089-X.

[5] BALDISSERA, D., FRANCO, A., MAIO, D., MALTONI, D.: Fake Fingerprint Detection by Odor Analysis. In: *Proceedings of the International Conference on Biometrics* [ICB2006]. Hong-Kong: Springer, 2006. pp. 265–272. LNCS 3832/2005. ISBN 978-3-540-31111-9.

[6] BAZEN, A. M., VERWAAIJEN, G. T. B., GEREZ, S. H., VEELENTURF, L. P. J., ZVAAG, B. J. van der: A Correlation-Based Fingerprint Verification System. In: *Proceedings of 11th Annual Workshop on Circuits Systems and Signal Processing* [ProRISC 2000]. Veldhoven (Netherlands): Technology Foundation STW, 2000. pp. 205-213. ISBN 90-73461-24-3.

[7] BENARON, D., PARACHIKOV, I. H., FIERRO, M. R.: *Metabolism-or Biochemical-based Anti-spoofing Biometrics Devices, Systems, and Methods.* International patent WO 2008/113024. 2008.

[8] BERNHARDT, S.: *Daktyloskopisches Basiswissen im Rahmen des Kooperationsprojektes Ground-Truth-Database* [Dactyloscopic Knowledge Base in the Context of the Cooperation Project Ground-Truth-Database]. Wiesbaden (Germany): BKA, 2009.

[9] BICZ, W.: *The Impossibility Of Faking Optel's Ultrasonic Fingerprint Scanners.* Wrocław (Poland): Optel, 2003. http://www.optel.pl/index_en.htm [accessed August 24, 2010].

[10] BOLLE, R. M., CONNELL, J. H., PANKANTI, S., RATHA, N. K., SENIOR, A. W.: *Guide to Biometrics.* New York (USA): Springer, 2004. ISBN 0-387-40089-3.

[11] BREITHAUPT, R., TEKAMPE, N.: Spoof Detection and the Common Criteria. In: *Proc. of the International Biometric Performance Conference* [IBPC2010]. Gaithersburg (USA): NIST, 2010. p. 17.

[12] BROWNLEE, K., ALTO, P.: *Method and Apparatus for Distinguishing a Human Finger from a Reproduction of a Fingerprint.* US Patent 6,292,576. 2001.

[13] CAPPELLI, R., LUMINI, A., MAIO, D., MALTONI, D.: Can Fingerprints be Reconstructed from ISO Templates?. In: *Proceedings of International Conference on Control, Automation, Robotics and Vision* [ICARCV2006]. Singapore: IEEE, 2006. pp. 191–196. ISBN 1-4244-0341-3.

[14] COHEN, F.: *Portability of Fingerprinting Systems Across Different Platforms and Different Fingerprinting Collection Protocols.* Philadelphia (USA): Drexel University, 2007. http://www.pages.drexel.edu/ aws29/Proposal.htm [accessed September 18, 2011].

[15] DOLEŽEL, M.: *Detection of Fingerprint Area in Image.* Brno (Czech Republic), 2010. Master thesis, Brno University of Technology, Faculty of Information Technology.

[16] DRAHANSKÝ, M., BŘEZINOVÁ, E., HEJTMÁNKOVÁ, D., ORSÁG, F.: Fingerprint Recognition Influenced by Skin Diseases. In: *International Journal of Bio-Science and Bio-Technology* [IJBSBT], Vol. 2, No. 4. Korea: SERCS, 2010. pp. 11–22. ISSN 1976-118X.

[17] DRAHANSKÝ, M., HEJTMÁNKOVÁ, D.: New Experiments with Optical Liveness Testing Methods. *Journal of Information Hiding and Multimedia Signal Processing* [JIHMSP], Vol. 1, No. 4. USA: Ubiquitous International, 2010. pp. 301–309. ISSN 2073-4212.

[18] DRAHANSKÝ, M., HEJTMÁNKOVÁ, D., DVOŘÁK, R., KRAJÍČEK, J., NEZHYBA, O.: *Biometric security device for acquirement and recognition of finger veins of a human hand*, Czech utility model No. 21548. 2010.

[19] DRAHANSKÝ, M., NÖTZEL, R., FUNK, W.: *Method and Apparatus for Detecting Biometric Features.* International patent WO 2007/036370. 2007.

[20] DRAHANSKÝ, M., ORSÁG, F., DOLEŽEL, M., DVOŘÁK, R., HÁJEK, J., HANÁČEK, P., HEJTMÁNKOVÁ, D., HERMAN, D., KNĚŽÍK, J., MARVAN, A., MRÁČEK, Š., STRUŽKA, J., VÁŇA, J.: *Biometrie* [Biometrics]. Brno (Czech Republic): Computer Press, 2011. p. 294. ISBN 978-80-254-8979-6.

[21] EIDHEIM, O. C.: *Introduction to Mathematical Morphology.* Trondheim (Norway), 2007. Norwegian University of Science and Technology, Department of Computer and Information Science. http://www.idi.ntnu.no/emner/tdt4265/lectures/lecture3b.pdf [accessed September 2, 2012, presentation].

[22] ENNIS, M. S., ROWE, R. K., CORCORAN, S. P., NIXON, K. A.: *Multispectral Sensing for High-Performance Fingerprint Biometric Imaging.* Albuquerque (USA): Lumidigm, Inc., 2007. http://www.lumidigm.com/lightPrint.html [accessed January 12, 2009].

[23] GRAND, J.: *Advanced Hardware Hacking Techniques.* In: DEFCON 12. Las Vegas (USA): Great Idea Studio, Inc., 2004. p. 59. http://grandideastudio.com/wp-content/uploads/advanced_hardware_hacking_slides.pdf [accessed September 2, 2012, presentation].

[24] HASHEMI, K.: *SCT Encapsulation.* Massachusetts (USA): Open Source Instruments Inc. & Brandeis University, 2008. p. 51. http://www.opensourceinstruments.com/Electronics/A3013/Encapsulation.html [accessed September 2, 2012, presentation].

[25] HEJTMÁNKOVÁ, D., DVOŘÁK, R., DRAHANSKÝ, M., ORSÁG, F.: A New Method of Finger Veins Detection. *International Journal of Bio-Science and Bio-Technology* [IJBSBT], Vol. 1, No. 1. Korea: SERSC, 2009. pp. 11–15. ISSN 1976-118X.

[26] HOMOLA, A.: *Detekce šířky papilární linie u otisků prstů* [Detection of papillary line width by fingerprints]. Brno (Czech Republic), 2011. Master thesis, Brno University of Technology, Faculty of Information Technology.

[27] IGAKI, S., SHINZAKI, T., YAMAGISHI, F., HIROYUKI, I.: *Biological Object Detection Apparatus.* US Patent 5,088,817. 1992.

[28] ISERSON, K. V.: Rigor Mortis and Other Postmortem Changes. In: KASTENBAUM, R. (Ed.): *Macmillan Encyclopedia of Death and Dying.* USA: Macmillan Reference, 2002. ISBN 978-0028656892.

[29] JAIN, A., CHEN, Y., DEMIRKUS, M.: Pores and Ridges: Fingerprint Matching Using Level 3 Features. In: *Proceedings of International Conference on Pattern Recognition* [ICPR2006]. Hong Kong: IEEE, 2006. pp. 477–480. ISBN 0-7695-2521-0.

[30] JAIN, A. K., ROSS, A.: Introduction to Biometrics. In: JAIN, A. K., FLYNN, P., ROSS, A. A. (Eds.): *Handbook of Biometrics.* New York (USA): Springer, 2008. pp. 1–22. ISBN 978-0-387-71040-2.

[31] JAMES, W. D., BERGER, T. G., ELSTON, D. M.: *Andrews' Diseases of the Skin: Clinical Dermatology.* 10th edition. Philadelphia (USA): Saunders Elsevier, 2006. ISBN 0-7216-2921-0.

[32] JIA, J., CAI, L., ZHANG, K., CHEN, D.: A New Approach to Fake Finger Detection Based on Skin Elasticity Analysis. In: LEE, S.-W., LI, S. (Eds.): *Advances in Biometrics* [ICB2007]. Berlin (Germany): Springer, 2007. pp. 309–318. LNCS 4642/2007. ISBN 978-3-540-74548-8.

[33] KAMAT, V.: Pulse Oximetry. In: *Indian Journal of Anaesthesia* [IJA], Vol. 46, No. 4. Mumbai (India): Medknow Publications, 2002. pp. 261–268. ISSN 0019-5049.

[34] KLUZ, M.: *Liveness testing in biometric systems.* Brno (Czech Republic), 2005. Master thesis, Masaryk University Brno, Faculty of Informatics.

[35] LI, S. Z. (Ed.): *Encyclopedia of Biometrics*. New York (USA): Springer, 2009. ISBN 978-0-387-73003-5.

[36] LIGON, A.: *An Investigation Into the Vulnerability of the Siemens ID mouse Professional Version 4*. Siemens, 2002. http://www.bromba.com/knowhow/idm4vul.htm [accessed September 2, 2012].

[37] LODROVÁ, D.: *Bezpečnost nesenzorové části biometrických systémů* [Security of non-sensor part of biometric systems]. Brno (Czech Republic), 2008. Brno University of Technology, Faculty of Information Technology. [project in Information System Security and Cryptography].

[38] LODROVÁ, D.: *Rozpoznávání živosti otisků prstů* [Liveness Testing by Fingers]. Brno (Czech Republic), 2007. Master thesis, Brno University of Technology, Faculty of Information Technology.

[39] LODROVÁ, D.: *Security of Biometric Systems*. Brno (Czech Republic), 2009. Treatise of Ph.D. thesis, Brno University of Technology, Faculty of Information Technology.

[40] LODROVÁ, D.: *Spoofing and anti-spoofing methods for fingerprint sensors*. Oslo-Fornebu (Norway): IDEX ASA, 2008. p. 16. [technical report].

[41] LODROVÁ, D., DRAHANSKÝ, M.: *Liveness Detection on Fingers by Causation of Optical Changes*. Czech utility model No. 19364. 2009.

[42] MALTONI, D.: Fingerprints. Recognition, Performance Evaluation and Synthetic Generation. In: *Summer School for Advanced Studies on Biometrics for Secure Authentication*. Alghero (Italy), 2008. [presentation].

[43] MALTONI, D., MAIO, D., JAIN, A. K., PRABHAKAR, S.: *Handbook of Fingerprint Recognition*, 2nd ed. London (UK): Springer, 2009. ISBN 978-1-84882-253-5.

[44] MARTINSEN, O. G., NYSAETHER, J., RIISNAES, K., MOSTAD, G., PEDERSEN, R., CHRISTIE, N. W., CLAUSEN, S.: *Live Finger Detection by Four-Point Measurement of Complex Impedance*. International patent WO 2004/049942. 2004.

[45] MATSUMOTO, T., MATSUMOTO, H., YAMADA, K., HOSHINO, S.: Impact of Artificial „Gummy“ Fingers on Fingerprint Systems. In: *Proceedings of SPIE, Optical Security and Counterfeit Deterrence Techniques IV*, Vol. 4677. San Jose (USA): Society of Photo Optical, 2002. pp. 275–289. ISBN 978-0819444172.

[46] NEWTON, E.: Overview of the ISO/IEC 30107 Project Anti-Spoofing and Liveness Detection Techniques. In: *International Biometric Performance Conference* [IBPC2012]. Gaithersburg (USA): NIST, 2012. p. 13. http://biometrics.nist.gov/cs_links/ibpc2012/presentations/Day2/228_Newton.pdf [accessed September 2, 2012, presentation].

[47] ORTEGA CHAMORRO, A. : Physical protection: Anti-tamper mechanisms in CC security evaluations. In: *10th International Common Criteria Conference*. Tromsø (Norway), 2009. p. 27. http://www.yourcreativesolutions.nl/ICCC10/proceedings/doc/pp/ALVARO_ORTEGA_EPOCHE&ESPRI_Physical_protection_Anti_tamper_mechanisms.pdf [accessed September 2, 2012, presentation].

[48] PUTTE, T. van der, KEUNING, J.: Biometrical Fingerprint Recognition: Don't get your fingers burned. In: *Fourth Working Conference on Smart Card Research and Advanced Applications.* Norwell (USA): Kluwer Academic Publishers, 2000. pp. 289–303. ISBN 0-7923-7953-5.

[49] RATHA, N., CONNELL, J., BOLLE, R. M., CHIKKEUR, S.: Cancelable Biometrics: A Case Study in Fingerprints. In: *Proceedings of the 18th International Conference on Pattern Recognition* [ICPR2006]. Washington (USA): IEEE, 2006. pp. 370–373. ISBN 0-7695-2521-0.

[50] RATHA, N. K., CHEN S., JAIN, A. K.: Adaptive Flow Orientation-Based Feature Extraction in Fingerprint Images. *Pattern Recognition*, Vol. 28, No. 11. Amsterdam (Netherlands): Elsevier, 1995. pp. 1657-1672. ISSN 0031-3203.

[51] ROSS, A., JAIN, A., REISMAN, J.: A Hybrid Fingerprint Matcher. In: *Proceedings of International Conference on Pattern Recognition* [ICPR2002]. Quebec (Canada): IEEE, 2002. pp. 795–798. ISBN 0-7695-1695-X.

[52] ROSS, A., SHAH, J., JAIN, A. K.: From Template to Image: Reconstructing Fingerprints from Minutiae Points. *IEEE Transactions on Pattern Analysis and Machine Intelligence* [TPAMI], Vol. 29, No. 4. Los Alamitos (USA): IEEE, 2007. pp. 544–560, ISSN 0162-8828.

[53] ROSS, A., SHAH, J., JAIN, A. K.: Towards Reconstructing Fingerprints From Minutiae Points. In: *Proceedings of SPIE Conference on Biometric Technology for Human Identification II*, Vol. 5779. Orlando (USA): SPIE, 2005. pp. 68–80. ISBN 9780819457646.

[54] ROWE, R. K.: A Multispectral Sensor for Fingerprint Spoof Detection. *Sensors*, Vol. 22, No. 1. Newton (USA): Questex Media Group, 2005. pp. 2–4. ISSN 0746-9462.

[55] ROWE, R. K., HARBOUR, R. M.: *Noninvasive alcohol sensor.* US Patent 7,386,152. 2008.

[56] RUTTY, G. N., STRINGER, K., TURK, E. E.: Electronic fingerprinting of the dead. *International Journal of Legal Medicine*, Vol. 122, No. 1. Berlin (Germany): Springer, 2007. pp. 77–80. ISSN 0937-9827.

[57] SCHNEIER, B.: Safe Personal Computing. *Crypto-gram*, May 2001. Counterpane Internet Security, 2001. http://www.schneier.com/crypto-gram-0105.html [accessed September 20, 2011].

[58] SCHUCKERS, S. A. C.: Spoofing and Anti-Spoofing Measures. *Information Security Technical Report*, Vol. 7, No. 4. Netherlands: Elsevier, 2002. pp. 56-62. ISSN: 1363-4127.

[59] SCHUCKERS, S., HORNAK, L., PARTHASARADHI, S., DERAKHSHANI, R.: Time-Series Detection of Perspiration as a Liveness test in Fingerprint Devices. In: *Biometric Consortium Conference* [BC2003]. Arlington (USA), 2003, p. 23. http://www.biometrics.org/bc2004/CD/PDF_PROCEEDINGS/Microsoft%20Power Point%20-%20SchukersS.ppt%20%5BRead-Only%5D.pdf [accessed September 2, 2012, presentation].

[60] SHÄFER, A. T.: Colour measurements of pallor mortis. *International Journal of Legal Medicine*, Vol. 113, No. 2. Berlin (Germany): Springer, 1999. pp. 81–83. ISSN 0937-9827.

[61] SHIMAMURA, T., MORIMURA, H., SHIMOYAMA, N., SAKATA, T., SHIGEMATSU, S., MACHIDA, K., NAKANISHI, M. : A Fingerprint Sensor with Impedance Sensing for Fraud Detection. In: *IEEE International Solid-State Circuits Conference* [ISSCC2008]. San Francisco (USA): IEEE, 2008. pp. 170-171. ISBN 978-1-4244-2010-0.

[62] SHIMBUN, Y.: S. Korean woman 'tricked' airport fingerprint scan. *Daily Yomiuri Online.* January 2009. http://www.yomiuri.co.jp/dy/national/20090101TDY01303.htm [accessed February 14, 2009].

[63] SIMOENS, K.: TURBINE Security Assessment: How to Build Trust. *The TURBINE Final Workshop.* Brussels (Belgium): 2011. p. 23. http://www.turbine-project.eu/dowloads/Day1.4.3.TURBINE_Workshop_17012011_K.Simoens.pdf [accessed September 2, 2012, presentation].

[64] STEINERT, U.: *Kriminalistik/Kriminaltechnik - Daktyloskopie* [Criminology/Forensics - Dactyloscopy]. Oranienburg (Germany), 2008. Fachhochschule der Polizei des Landes Brandenburg. p. 23. [textbook on the subject Criminology/Forensics].

[65] TABASSI, E.: *What is What. Description on selection process and selected fingerprint images for level 3 conformance test.* NIST, 2008. p. 5. [document on CD with GTD database].

[66] TABASSI, E., GROTHER, P., SALAMON, W., WATSON, C.: Minutiae Interoperability. In: *Proceedings of the Special Interest Group on Biometrics and Electronic Signatures* [BIOSIG2009]. Darmstadt (Germany): GI, 2009. pp. 13–30. LNI 155, ISBN 978-3-88579-249-9.

[67] THALHEIM, L., KRISSLER, J., ZIEGLER, P.-M.: Body Check, Biometric Access Protection Devices and their Programs Put to the Test. In: *c't magazine*, November 2002. Germany: Heinz Heise publishing house, 2002. ISSN 0724-8679.

[68] TILBORG, H. C. A. van, JAJODIA, S. (Eds): *Encyclopedia of Cryptography and Security*, 2nd ed. New York (USA): Springer, 2011. ISBN 978-1-4419-5905-8.

[69] U.S. DEPARTMENT OF JUSTICE, FBI: *The Science of Fingerprints: Classification and Uses.* USA: Diane Publishing, 1988. ISBN 1-56806-839-5.

[70] VALENCIA, V. S., HORN, Ch.: *Biometric Liveness Testing.* In: WOODWARD, J. D., ORLANS, N. M., HIGGINS, P. T. (Eds.): Biometrics. New York (USA): Osborne McGraw Hill, 2003. pp. 139–149. ISBN 978-0072222272.

[71] WATSON, C. I.: *NIST Special Database 14. Mated Fingerprint Cards Pairs*, v. 2. NIST, 2008. p. 40. http://www.nist.gov/srd/upload/Spec-db-14.pdf [accessed September 2, 2012].

[72] WATSON, C. I.: *NIST Special Database 29. Plain and Rolled Images from Paired Fingerprint Cards.* NIST, 2003. p. 32. http://www.nist.gov/srd/upload/nistsd29.pdf [accessed September 2, 2012].

[73] WATSON, C. I., GARRIS, M. D., TABASSI, E., WILSON, C. L., MCCABE, R. M., JANET, S., Ko, K.: *User's Guide to NIST Biometric Image Software (NBIS).* NIST, 2007. [document on CD with NBIS SW].

[74] WEI-YUN, Y., HOANG-THANH, T., EAM-KHWANG, T., JIAN-GANG, W.: Fake Finger Detection by Finger Color Change Analysis. In: *Advances in Biometrics, Proceedings of the International Conference on Biometrics* [ICB2007]. Berlin (Germany): Springer, 2007. pp. 888–896. LNCS 4642/2007. ISBN 978-3-540-74548-8.

[75] ZENDULKA, J., BARTÍK, V., LUKÁŠ, R., RUDOLFOVÁ, I.: *Získávání znalostí z databází* [Knowledge Discovery in Databases]. Brno (Czech Republic), 2009. Brno University of Technology, Faculty of Information Technology. [textbook on the subject Knowledge Discovery in Databases].

[76] ANSI/NIST-ITL 1-2000: *Information Technology: American National Standard for Information Systems-Data Format for the Interchange of Fingerprint, Facial, SMT Information.* [NIST Special Publication 500-245] American National Standards Institute/National Institute of Standards and Technology, 2000.

[77] Atmel, Corp. http://www.atmel.com/ [accessed August 24, 2010].

[78] AuthenTec, Inc. http://www.authentec.com/ [accessed August 24, 2010].

[79] Basler AG. http://www.baslerweb.com/ [accessed September 2, 2012].

[80] Basler Scout: The user's manual for GigE version cameras. Basler AG, June 2007. http://www.bnl.gov/atf/systems/diagnostics/scout-g_users_manual.pdf [accessed September 2, 2012].

[81] Bergdata Biometrics GmbH. http://www.bergdata.com/ [accessed August 24, 2010].

[82] Biometric System Laboratory at University of Bologna. http://biolab.csr.unibo.it/research.asp?organize=Activities&select=&selObj=12&pathSubj=111||12&Req=& [accessed September 10, 2011].

[83] Biometrics 2009: Sagem Sécurité and Hitachi introduce multi-modal finger vein and fingerprint device. *Infosecurity magazine.* October 2009. http://www.infosecurity-magazine.com/view/4631/biometrics-2009-sagem-scurit-and-hitachi-introduce-multimodal-finger-vein-and-fingerprint-device-/ [accessed November 9, 2011].

[84] Biometrics Market and Industry Report 2009-2014. International Biometric Group, 2009. http://www.biometricgroup.com/reports/public/market_report.php [accessed January 16, 2009].

[85] BMF, Corp. http://www.bm-f.com/index.html [accessed August 24, 2010].

[86] Cancer drug erases fingerprints. *BBC News*, May 27, 2009. http://news.bbc.co.uk/2/hi/health/8064332.stm [accessed September 20, 2011].

[87] DERMALOG Identification Systems GmbH. http://www.dermalog.de/uploads/files/PM_ZF1_CeBIT08_ENGL_final_030308.pdf [accessed January 16, 2009].

[88] ELSYS Corp. http://www.elsys.ru/delsy_e.php [accessed August 24, 2010].

[89] Fingerprint Verification Competition. http://bias.csr.unibo.it/fvc2006/databases.asp [accessed September 10, 2010].

[90] Hitachi, Ltd. http://www.hitachi.com/ [accessed November 9, 2011].

[91] Infineon Technologies AG. http://www.infineon.com/cms/en/product/index.html [accessed August 24, 2010].

[92] Ingersoll Rand Corp. http://security.ingersollrand.com/Pages/default.aspx [accessed August 24, 2010].

[93] Innovatrics, s. r. o. http://www.innovatrics.com/ [accessed October 5, 2011].

[94] Integrated Biometrics, Inc. http://integratedbiometrics.com/ [accessed January 3, 2012].

[95] International Organization for Standardization. http://www.iso.org [accessed March 19, 2011].

[96] ISO/IEC 15408: *Information technology – Security techniques – Evaluation criteria for IT security* [so called Common Criteria]. International Organization for Standardization, 2009.

[97] ISO/IEC 19794-2:2005: *Information technology – Biometric data interchange formats – Part 2: Finger minutiae data*. International Organization for Standardization, 2005.

[98] ISO/IEC 24787:2012: *Information technology – Identification cards – On-card biometric comparison*. International Organization for Standardization, 2010.

[99] ISO/IEC 29109-1:2009: *Information technology – Conformance testing methodology for biometric data interchange formats defined in ISO/IEC 19794 - Part 1: Generalized conformance testing methodology*. International Organization for Standardization, 2009.

[100] ISO/IEC 29109-2:2010: *Information technology – Conformance testing methodology for biometric data interchange formats defined in ISO/IEC 19794 - Part 2: Finger minutiae data*. International Organization for Standardization, 2010.

[101] ISO/IEC Directives, Part 1: *Procedures for the technical work*. International Organization for Standardization, 2011. http://www.iso.org/directives [accessed March 19, 2011].

[102] ISO/IEC SC37 N3058: *Call for Contributions on Metric for Measuring Accuracy of Minutiae Placement*. International Organization for Standardization.

[103] ISO/IEC SC37 N3972 Standing Document 11 Part 1: *Overview Standards Harmonization Document*. International Organization for Standardization, 2010.

[104] ISO/IEC SC37 Standing Document 2: *Harmonized biometric vocabulary*, Version 12. International Organization for Standardization, 2009.

[105] Lumidigm, Inc. http://www.lumidigm.com/ [accessed August 24, 2010].

[106] National Institute of Standards and Technology. http://www.nist.gov/ [accessed March 19, 2011].

[107] Nestlé Česko s. r. o. http://www.nestle.cz/ [accessed September 2, 2012].

[108] NeuroTechnology, s. r. o. http://www.neurotechnology.com/ [accessed October 5, 2011].

[109] OKI Electric Industry Co., Ltd. http://www.oki.com/en/ [accessed August 24, 2010].

[110] OpenCV 2.1 C++ Reference. http://opencv.willowgarage.com/documentation/cpp/index.html [accessed September 2, 2012].

[111] OpenGL, The Industry's Foundation for High Performance Graphics. http://www.opengl.org/ [accessed November 8, 2012].

[112] Optel, Ltd. http://www.optel.pl/index_en.htm [accessed August 24, 2010].

[113] Pebeo, SA. http://www.pebeo.com/ [accessed April 6, 2012].

[114] Precise Biometrics, AB. http://www.precisebiometrics.com/ [accessed January 5, 2012].

[115] Privaris, Inc. http://www.privaris.com/ [accessed August 24, 2010].

[116] Sagem Morpho, Inc. http://www.morpho.com/ [accessed August 24, 2010].

[117] SecuGen Corp. http://www.secugen.com/ [accessed August 24, 2010].

[118] Security First Corp. http://www.securityfirstcorp.com/ [accessed August 24, 2010].

[119] Sirchie Fingerprint Laboratories. http://www.sirchie.com/ [accessed April 6, 2012].

[120] SpofaDental, a.s. http://www.spofadental.cz/ [accessed April 6, 2012].

[121] Statewide Fingerprint Imaging System in California, USA. http://www.sfis.ca.gov/pattern_types.html [accessed September 18, 2011].

[122] STMicroelectronics Group. http://www.st.com/stonline/ [accessed August 24, 2010].

[123] TST Biometrics GmbH. http://www.tst-biometrics.com [accessed August 24, 2010].

[124] Touchless Biometric Systems AG. http://www.tbs-biometrics.com/ [accessed March 10, 2012].

[125] TURBINE project. http://www.turbine-project.eu/ [accessed January 16, 2009].

[126] Ultra-Scan, Corp. http://www.ultra-scan.com/ [accessed August 24, 2010].

[127] Upek, Inc. http://www.upek.com/ [accessed August 24, 2010].

[128] Veridicom International, Inc. http://www.veridicom.com/ [accessed August 24, 2010].

[129] Wikipedia, Flood fill. http://en.wikipedia.org/wiki/Flood_fill [accessed November 8, 2012].

[130] Wikipedia, Sensor. http://en.wikipedia.org/wiki/Sensor [accessed November 8, 2012].

[131] Wolfram Mathworld, Distance. http://mathworld.wolfram.com/Distance.html [accessed November 8, 2012]

[132] WxWidgets project. http://www.wxwidgets.org/ [accessed March 19, 2011].

[133] ZK Software, Inc. http://usa.zksoftware.com/view.do?id=51 [accessed September 18, 2011].

List of abbreviations

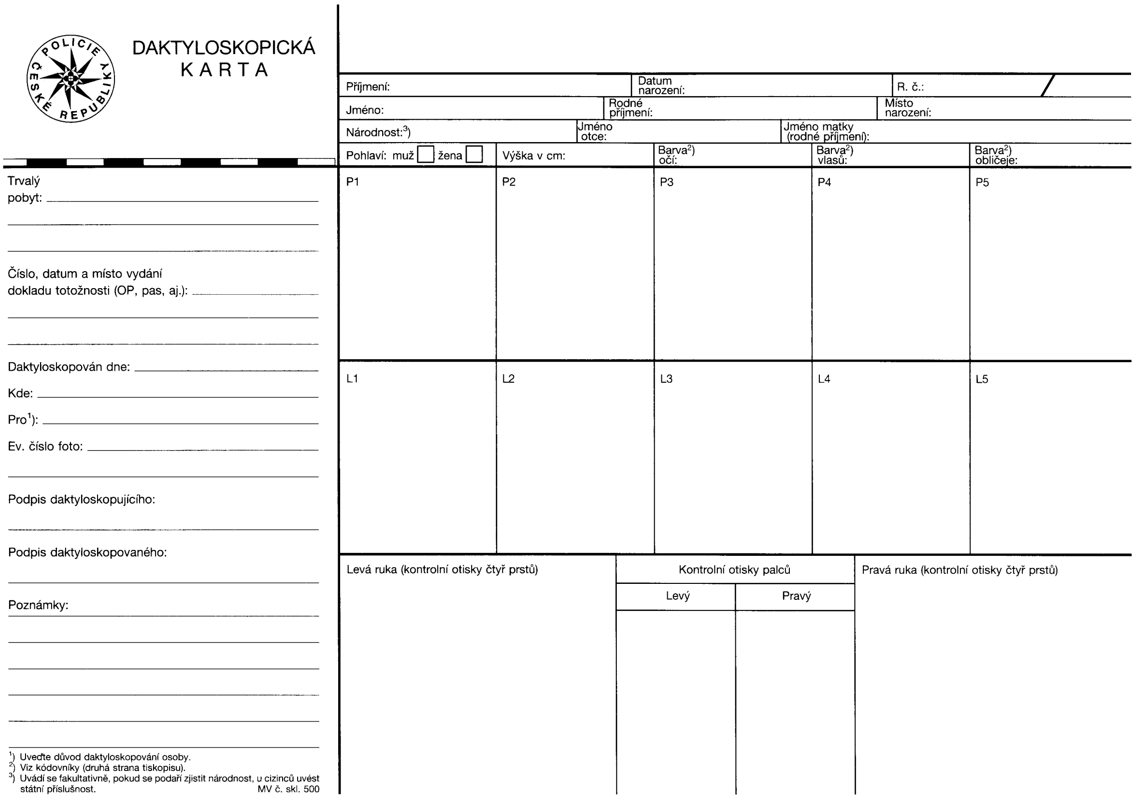
AFIS	Automated Fingerprint Identification System.
AGM	Automatically Generated Minutia.
ANSI	American National Standards Institute.
API	Application Programming Interface.
BioSAL	Biomedical Signal Analysis Laboratory, Clarkson University and West Virginia University - USA.
BKA	Bundeskriminalamt [German Federal Criminal Office].
BMP	Bitmap image file.
BSI	Bundesamt für Sicherheit in der Informationstechnik [Federal Office for Information Security] - Germany.
BUT	Brno University of Technology - Czech Republic.
CIEL*a*b*	CIE color model.
CC	Common Criteria for Information Technology Security Evaluation.
CCD	Charge-Coupled Device.
CD	Committee Draft [process of standardization].
CDV	Committee Draft for Vote [process of standardization].
CMOS	Complementary Metal Oxide Semiconductor.
DCSY	Department of Computer Systems - BUT FIT, Czech Republic.
DIS	Draft International Standard [process of standardization].
DoS	Denial of Service.
EER	Equal Error Rate.
ESD	Electrostatic Discharge.
FAR	False Acceptance Rate.
FBI	Federal Bureau of Investigation - USA.
FDIS	Final Draft International Standard [process of standardization].
FFT	Fast Fourier Transform.
FIT	Faculty of Information Technology - BUT, Czech Republic.
FRR	False Rejection Rate.
FRVŠ	Fond rozvoje vysokých škol [Czech Fund for Higher education growth].
FTIR	Frustrated Total Internal Reflection.
FVC	Fingerprint Verification Competition.
GAČR	Grantová Agentura České Republiky [Czech Grant Agency].
GTD	Ground Truth Database.
GTM	Ground Truth Minutia.
GUI	Graphical User Interface.
HLS	Hue-Lightness-Saturation (color model).
IEC	International Electrotechnical Commission.
ISO	International Organization for Standardization.

JTC	Joint Technical Committee [process of standardization].
LED	Light-Emitting Diode.
LES	Light-Emitting Sensor.
MINEX	Minutiae Interoperability Exchange Test [NIST's project].
MoC	Match-on-Card.
MPDF	Minutiae Placement Density Function.
MSI	Multispectral imaging.
MŠMT	Ministerstvo školství, mládeže a tělovýchovy [Czech Ministry of Education, Youth and Sports].
NB	National Body [process of standardization].
NBIS	NIST Biometric Image Software.
NBU	Národní Bezpečnostní Úřad [Czech National Security Agency].
NFIQ	NIST Fingerprint Image Quality.
NISlab	Norwegian Information Security laboratory.
NIST	National Institute of Standards and Technology - USA.
NWIP	New Work Item Proposal [process of standardization].
OCC	On-Card-Comparison.
OpenGL	Open Graphics Library.
OpenCV	Open Source Computer Vision.
PCB	Printed Circuit Board.
PWI	Preliminary Work Item [process of standardization].
RAM	Random-access memory.
RDC	Relative Dielectric Constant.
RF	Radio Frequency.
RGB	Red-Green-Blue color model.
SC	Subcommittee [process of standardization].
SD	Special Database [NIST].
SDK	Software Development Kit.
SFinGe	Synthetic Fingerprint Generator.
SoC	System-on-a-Chip or System-on-Card.
SoD	System-on-Device.
TFT	Thin Film Transistor.
TURBINE	Trusted Revocable Biometric Identities.
USB	Universal Serial Bus.
UV	Ultra-Violet.
WD	Working Draft [process of standardization].
WG	Working Group [process of standardization].
WSQ	Wavelet Scalar Quantization [algorithm or file format].

Appendix A

Dactyloscopic card

The dactyloscopic (fingerprint) card has a slightly different appearance according to the state where it is used. The dactyloscopic card used in the Czech Republic can be found in Fig. A.1 and A.2. The left column and the top part of the card contain the personal data of the dactyloscoped (fingerprinted) person. The first row of fingerprints contains the rolled impressions of right hand fingers (from thumb to the little finger - right to left). In the second row, there are rolled impressions of left hand fingers - same type and order. The bottom part of dactyloscopic card contains the plain impression of each finger, which is used for the verification.



POLICIE ČESKÉ REPUBLIKY

DAKTYLOSKOPICKÁ
KARTA

Příjmení:		Datum narození:		R. č.: /
Jméno:		Rodné příjmení:		Místo narození:
Národnost:3)		Jméno otce:		Jméno matky (rodné příjmení):
Pohlaví: muž □ žena □	Výška v cm:	Barva2) očí:	Barva2) vlasů:	Barva2) obličeje:
P1	P2	P3	P4	P5
L1	L2	L3	L4	L5

Trvalý pobyt: __________

Číslo, datum a místo vydání dokladu totožnosti (OP, pas, aj.): __________

Daktyloskopován dne: __________

Kde: __________

Pro1): __________

Ev. číslo foto: __________

Podpis daktyloskopujícího:

Podpis daktyloskopovaného:

Poznámky:

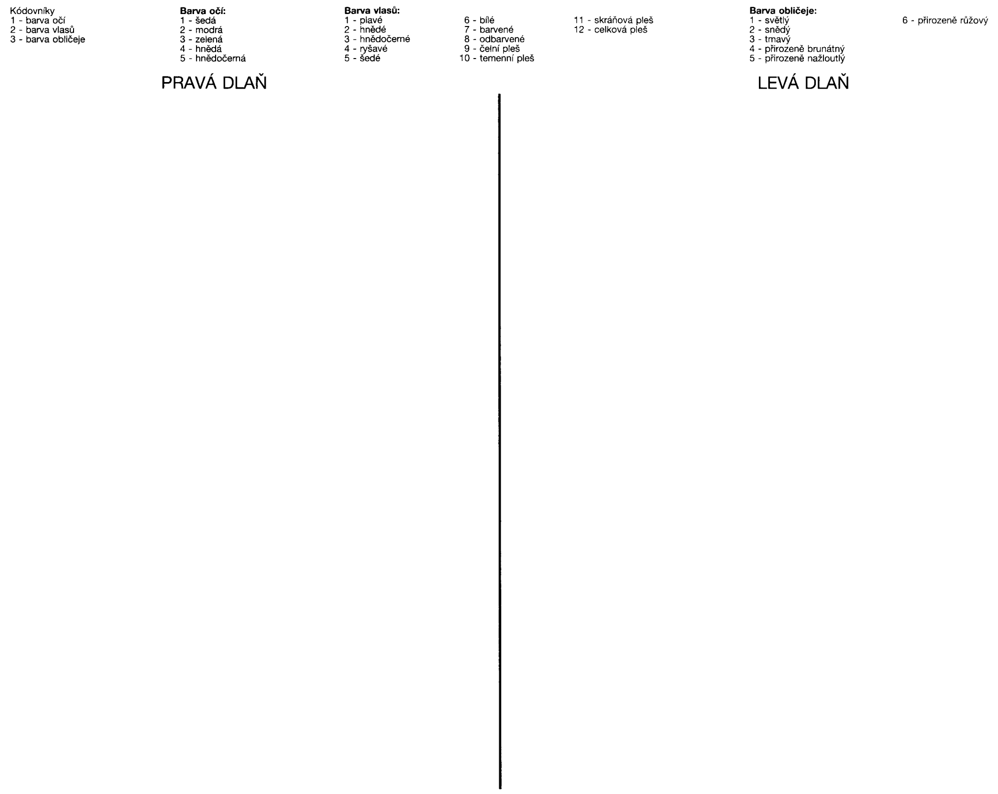
Levá ruka (kontrolní otisky čtyř prstů)	Kontrolní otisky palců		Pravá ruka (kontrolní otisky čtyř prstů)
	Levý	Pravý	

1) Uveďte důvod daktyloskopování osoby.
2) Viz kódovníky (druhá strana tiskopisu).
3) Uvádí se fakultativně, pokud se podaří zjistit národnost, u cizinců uvést státní příslušnost.

MV č. skl. 500

Figure A.1: Example of the dactyloscopic card used in the Czech Republic - front page.

The backside of the dactyloscopic card contains the code names for description of dactyloscoped person: the code names for color and amount of hair, color of eyes and description of face appearance.



Kódovníky
1 - barva očí
2 - barva vlasů
3 - barva obličeje

Barva očí:
1 - šedá
2 - modrá
3 - zelená
4 - hnědá
5 - hnědočerná

Barva vlasů:
1 - plavé
2 - hnědé
3 - hnědočerné
4 - ryšavé
5 - šedé
6 - bílé
7 - barvené
8 - odbarvené
9 - čelní pleš
10 - temenní pleš
11 - skráňová pleš
12 - celková pleš

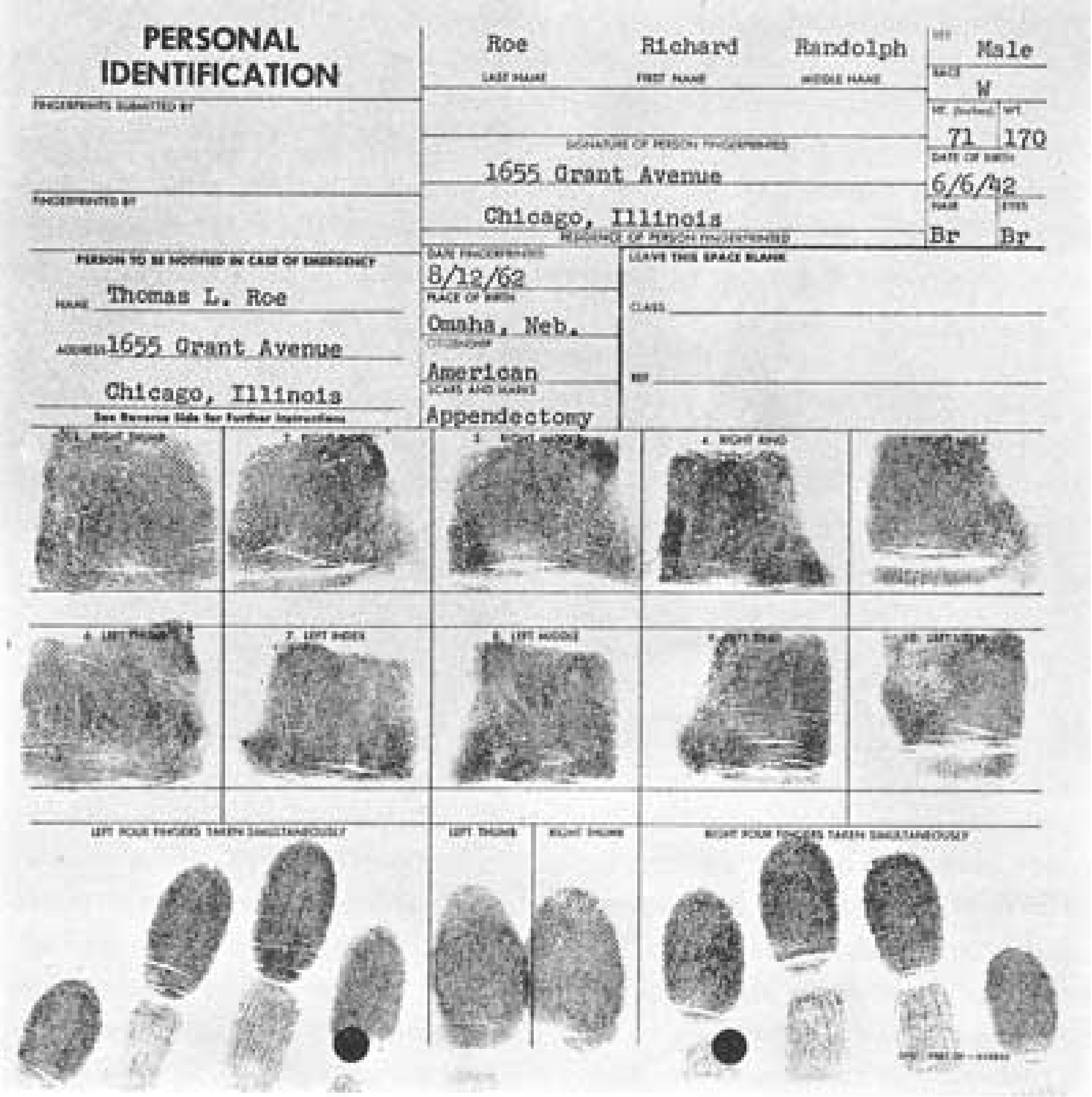
Barva obličeje:
1 - světlý
2 - snědý
3 - tmavý
4 - přirozeně brunátný
5 - přirozeně nažloutlý
6 - přirozeně růžový

PRAVÁ DLAŇ

LEVÁ DLAŇ

Figure A.2: Example of the dactyloscopic card used in the Czech Republic - back page.

The dactyloscopic card used by FBI in the United States of America has a different appearance (see Fig. A.3) [69]. In comparison with the Czech dactyloscopic card, the US card uses different types of personal information and does not contain codenames for description of dactyloscoped person. On the other hand, the appearance of the fingerprint part is almost the same. The first row of fingerprints contains the rolled impressions of right hand fingers, the second row contains rolled impressions of left hand fingers and the bottom part contains the plain impression of each finger for the verification purposes.



1. RIGHT THUMB
2. RIGHT INDEX
3. RIGHT MIDDLE
4. RIGHT RING
5. RIGHT LITTLE
6. LEFT THUMB
7. LEFT INDEX
8. LEFT MIDDLE
9. LEFT RING
10. LEFT LITTLE
LEFT FOUR FINGERS TAKEN SIMULTANEOUSLY
LEFT THUMB
RIGHT THUMB
RIGHT FOUR FINGERS TAKEN SIMULTANEOUSLY

PERSONAL IDENTIFICATION

FINGERPRINTS SUBMITTED BY

FINGERPRINTED BY

Roe Richard Randolph
LAST NAME FIRST NAME MIDDLE NAME

SIGNATURE OF PERSON FINGERPRINTED

1655 Grant Avenue
Chicago, Illinois
RESIDENCE OF PERSON FINGERPRINTED

SEX Male
RACE W
HT. (Inches) 71 WT. 170
DATE OF BIRTH 6/6/42
HAIR Br EYES Br

PERSON TO BE NOTIFIED IN CASE OF EMERGENCY
NAME Thomas L. Roe
ADDRESS 1655 Grant Avenue
Chicago, Illinois
See Reverse Side for Further Instructions

DATE FINGERPRINTED 8/12/62
PLACE OF BIRTH Omaha, Neb.
CITIZENSHIP American
SCARS AND MARKS Appendectomy

LEAVE THIS SPACE BLANK
CLASS.
REF.

Figure A.3: Example of the dactyloscopic card used by FBI in the United States of America [69].

Appendix B

Process of standardization

The process of creation of a standard takes several years and it is quite complicated. The text of future standard has to undergo seven phases [101]:

1. **Preliminary stage.** This stage is the first phase of the long standardization process. During this phase a preliminary work item (PWI) is created. Committee can also release a Call for Contribution (e.g., in case of absence of methodology, data, or experts opinion).

2. **Proposal stage.** During this phase the New Work Item Proposal (NWIP) is presented and the preliminary draft is created. The NWIP should be presented by its creator and she/he should also propose a project leader/editor and a date of publication.

3. **Preparatory stage.** The preliminary draft is modified into the Working Draft (WD). This draft is discussed in the group of experts.

4. **Committee stage.** During this phase, the text as a Committee Draft (CD) is discussed with National Bodies (NBs) to reach consensus.

5. **Enquiry stage.** During this stage, the Enquiry Draft (sometimes called Draft International Standard - DIS or Committee Draft for Vote - CDV) as a final version of text has to be approved (more or equal to 2/3 of experts have to agree and less or equal to 1/4 of experts have to disagree). The approved standard is called the Final Draft International Standard (FDIS).

6. **Approval stage.** This stage contains another vote of national bodies. Once the text is approved, the document enters the last stage.

7. **Publication stage.** This stage takes a few months. The minor mistakes, typos and inaccuracies are fixed during this phase and finally the text is published as an International Standard.

This process (with minor variations) is used not only for creation of the ISO standard, but also for creation of a new part of an existing standard, a revision/amendment of/to an existing standard or a part, a Technical Specification or a Publicly Available Specification [101].

Appendix C

ISO 19794-2:2005 file format

The tables C.1 – C.4 contain the clear summary of the mandatory data blocks/fields, their size, range of valid values and short explanation of individual values, if necessary.

Table C.1: The data blocks in ISO 19794-2:2005 file format [97].

Field	Size	Occurrence
Record header	24 B	1 per file
Fingerprint/view header	4 B	1 per fingerprint
Minutia data	6 B	1 per minutia
Extended data block length	2 B	1 per fingerprint
Extended data block	0 - ?	1 per fingerprint

Table C.2: The record header in ISO 19794-2:2005 file format [97].

Field	Size	Valid values	Notes
Format identifier	4 B	0x464D5200	'F', 'M', 'R', 0x0
Version of standard	4 B	0x20323000	' ', '2', '0', 0x0
Length of record	4 B	24 - 4 294 967 295	in bytes
Certification of sensor[1]	4 b		
Type ID of sensor[2]	12 b		0 = unknown ID
Image size X	2 B	0 - 65 535	in pixels
Image size Y	2 B	0 - 65 535	in pixels
Horizontal resolution X[3]	2 B	98 - 65 535	in pixels per cm
Vertical resolution Y[3]	2 B	98 - 65 535	in pixels per cm
Number of fingerprints	1 B	0 - 176[4]	
Reserved	1 B	0	for future use

[1] Certification of sensor: If the sensor was certified to be compliant with the US FBI's Image Quality Specifications, then the most significant bit is one, otherwise it is zero. The next two bits are reserved for the future image quality certifications and the least significant bit is reserved future ISO sensor certification.

[2] ID of sensor: This value is vendor specific. Nevertheless, the value zero (unknown/unreported ID) is acceptable.

[3] Resolution: Image resolution should not be less than 98.45 (rounded to 98 [100]) pixels per centimeter (250 pixels per inch).

[4] Number of fingerprints: It is possible to store 16 views/sessions per each of 11 fingers/finger positions (right thumb – left index finger plus unknown finger).

Table C.3: The fingerprint header in ISO 19794-2:2005 file format [97].

Field	Size	Valid values	Notes
Finger position	1 B	0 - 10	0 = unknown, 1–5 = right thumb – index 6–10 = left thumb – index
View (session) number	4 b	0 - 15	0 = first session
Impression number	4 b	0 - 3, 8	0 = live-scan plain 1 = live-scan rolled 2 = nonlive-scan plain 3 = nonlive-scan rolled 8 = swipe
Finger quality	1 B	0 - 100	0 = lowest quality
Number of minutiae	1 B	0 - 255	

Table C.4: The minutiae data block in ISO 19794-2:2005 file format [97].

Field	Size	Valid values	Notes
Minutiae type	2 b	0 - 2	0 = other 1 = ridge ending 2 = ridge bifurcation
Position X	14 b	0 - 16 383	in pixels from top-left corner
Reserved	2 b	0	for future use
Position Y	14 b	0 - 16 383	in pixels from top-left corner
Angle of minutia[5]	1 B	0 - 255	e.g.: 16 = 22.5 deg
Quality of minutia[6]	1 B	0 - 100	0 = unknown quality 1–100 = minimum – maximum

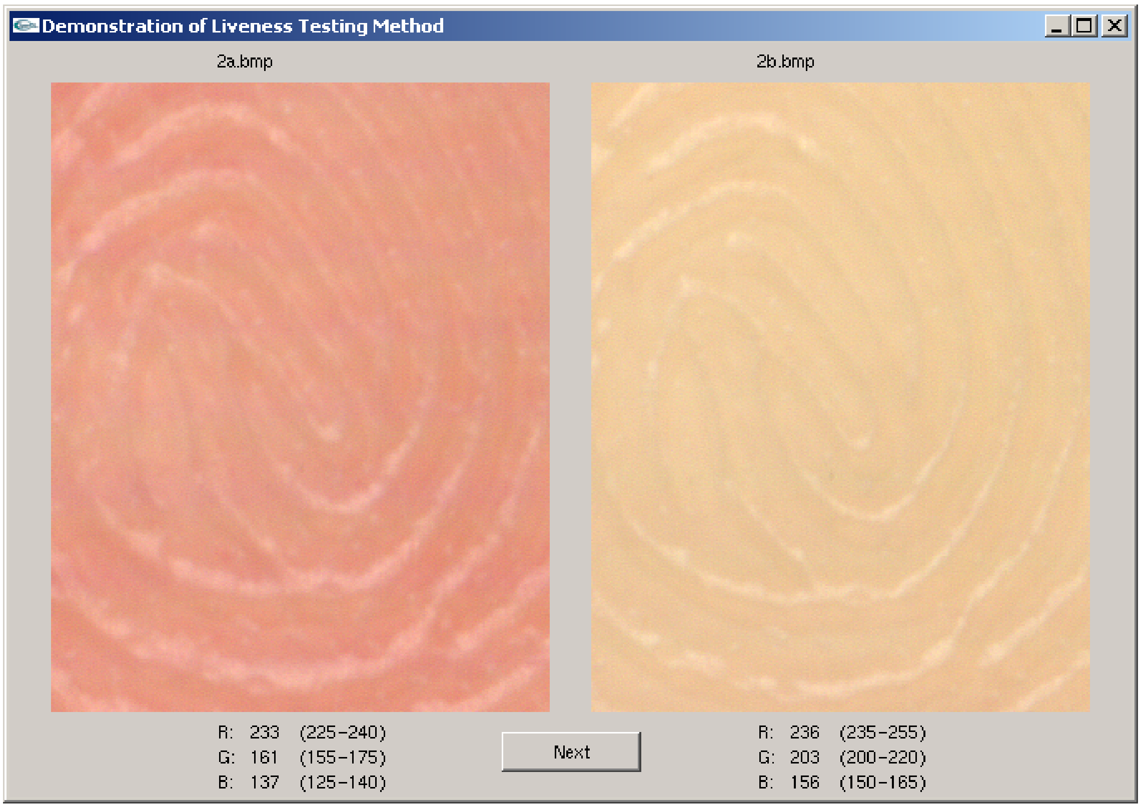
[5] Angle of minutia: The measured value (in degrees) is converted to the 0 – 255 range, e.g., the value of 180 deg means 128 and the value of 22.5 deg means 16.

[6] Quality of minutia: Any international standard describing the minutia quality determination methodology have not been published yet, so the ISO/IEC 19794-2:2005 standard does not ensure the comparability among minutiae quality values determined by different extractors or stored in different templates.

Appendix D

Application for first preliminary test of liveness detection method

Before creation of pre-prototype of liveness detection unit, the main idea was tested using a common office scanner. For these purposes, I developed an application called „Demonstration of Liveness Testing Method“ in C++ and OpenGL[1].



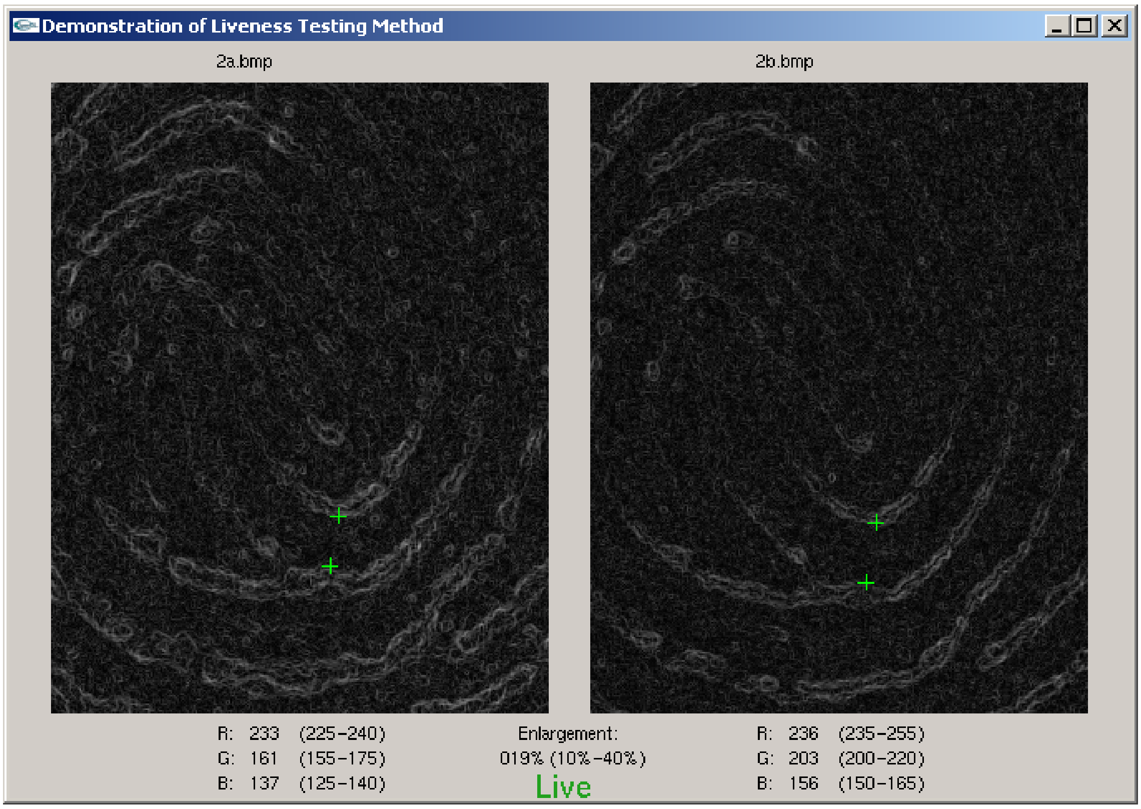
```
R:  233  (225-240)          R:  236  (235-255)
G:  161  (155-175)          G:  203  (200-220)
B:  137  (125-140)          B:  156  (150-165)
```

Figure D.1: Determining the color change: Loading two fingerprints (image before and after pressing) and determining the median of RGB components for each image.

[1] Open Graphics Library [111].

The workflow of this program is simple. The program loads two BMP images (fingerprints in pressed and unpressed state), computes a median of each RGB component, transforms both images into grayscale, applies Sobel operator[2] and asks for manual determining of papillary lines width. At the end, the application evaluates whether the measured values (change of color and width of papillary lines) are within the predefined parameters and decides whether the images present a live or a fake finger.

The screenshots of the program workflow can be found on Fig. D.1 and D.2. The finger presented on these images is evaluated as live. The change of color is 3 for R component (236-233), 42 for G component (203-161) and 19 for B component (156-137) and the change of papillary line width is 19 %.



```
R:  233   (225-240)        Enlargement:          R:  236   (235-255)
G:  161   (155-175)      019% (10%-40%)          G:  203   (200-220)
B:  137   (125-140)          Live                B:  156   (150-165)
```

Figure D.2: Determining the change of papillary line width: Application of Sobel operator and manual determining the papillary line width. Program evaluated these images as corresponding to a live human finger.

[2] For detection of papillary lines in image captured by a common office scanner, a variety of methods (difference between Gaussian blurs, local thresholding, Sobel, Prewit and other operators, etc.) was tested, but the best results were achieved by using the Sobel operator.

Appendix E

Examples of fake fingers

For the purposes of final testing of my liveness detection approach, I used 10 fake fingers made of different materials. Some of these materials are commercially available (e.g., gelatin), other materials are used mostly by forensic experts (e.g., Durocast). The molds used for creation of all fake fingers (except the stamp) were made of wax from common tea candles with assistance of enrollees. The description of materials, photographs of fake fingers with corresponding captured fingerprints of pressed fake fingers and a few supplementary images are given below.

Stamp. For the purposes of these final tests, the sheet of rubber from a common office stamp was used. The production of the stamp with fingerprint relief is very cheap (it cost approx. 4 EUR in 2007) and the stamp can be made, e.g., in common stationer's shop in a few days [38].

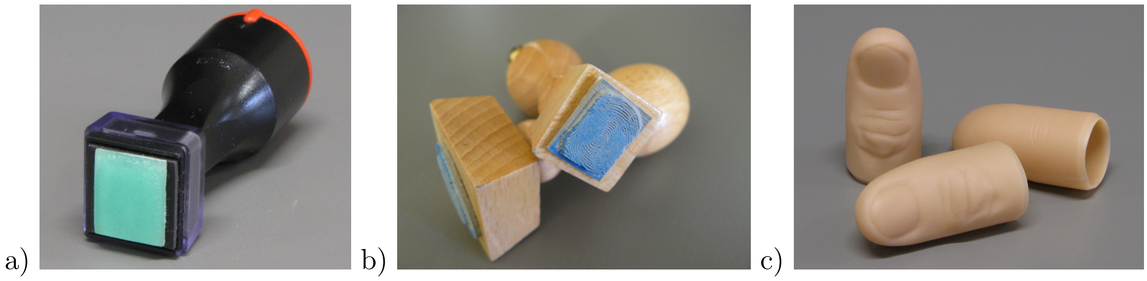


Figure E.1: Stamps and prosthetic fingers used for sensor spoofing.

Siloflex. The Siloflex is a silicone impression material used mostly by dentists. It is produced by SpofaDental, a.s. [120] and costs approx. 25 EUR per 260g (in 2010). The work with this material is quite simple (just mix base material with catalyst), but the resultant fake fingers are dark-blue (see Fig. E.2 a), which is a problem for one group of optical sensors (according to my experiences).

Siligum. It is the two-component silicone molding paste produced by Pebeo, SA and commercially available at shops with art supplies [113]. The material is quite cheap (approx. 22 EUR per 300g in 2010) and working with this material is simple (just mix both components). However, the resultant fake fingers are light-blue (see Fig. E.2 c), which can be a problem for some optical sensors (according to my experiences).

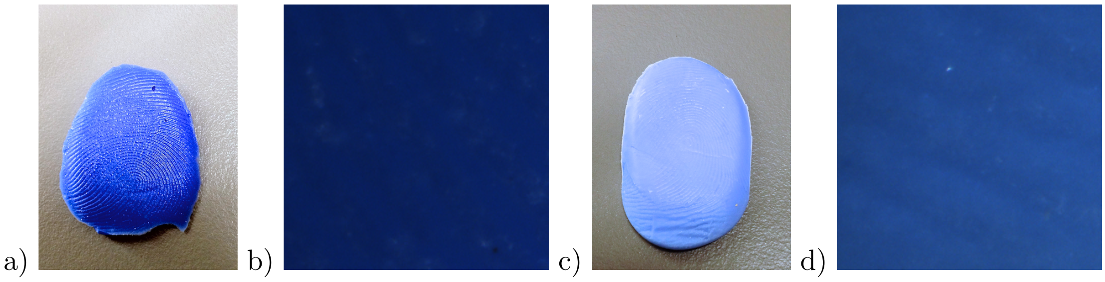


Figure E.2: Fake finger made of a) Siloflex with b) cut part of captured sample[1], and fake finger made of c) Siligum with d) cut part of captured sample[1].

Durocast. Durocast is a two-component impression compound used by forensic experts in various countries. This material is produced by Sirchie Fingerprint Laboratories [119] and the work with it is quite simple (just mix base material with catalyst). However, it is quite expensive (approx. 45 EUR per 330g in 2010) and it is not commercially available in the Czech Republic. The resultant fake fingers are about the magenta color (see Fig. E.3 a).

JaLatex. JaLatex is a latex-based material commercially available at shops with art supplies. For the purposes of fake fingers creation, I used two different color versions of JaLatex: transparent and skin-color (see Fig. E.3 c). The work with this material is simple but very unpleasant, because it contains significant amount of ammonia. The semi-transparent fake fingers are also colored similar to the color of human skin, which makes them ideal candidates for sensor spoofing attempts.

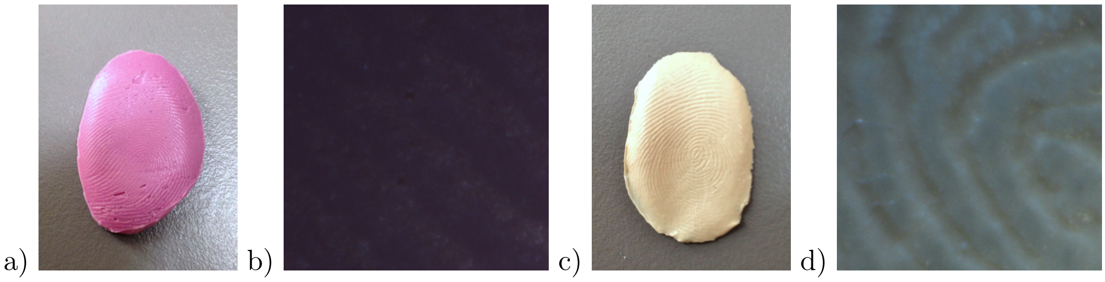


Figure E.3: Fake finger made of a) Durocast with b) cut part of captured sample[1], and fake finger made of c) skin color non-transparent JaLatex with d) cut part of captured sample.

Latex Gedeo. It is a molding material based on natural rubber produced by Pebeo, SA [113]. Latex Gedeo is cheap (approx. 6 EUR per 250ml in 2010) and commercially available at shops with art supplies. Unfortunately, the work with this material is same as in case of JaLatex: simple but very unpleasant due to the significant amount of ammonia. The fake fingers made of Latex Gedeo (see Fig. E.4 a) and transparent Jalatex are indistinguishable to the naked eye. Nevertheless, I decided to use both materials because they achieved different results during tests of various fingerprint sensors.

[1] The papillary lines in the catured samples may be little bit difficult to see with naked eye, especially in the printed version of this thesis. The electronic version of this thesis is attached on CD.

Gelatin. The usage of gelatin fake fingers was proposed by Prof. Matsumoto [45]. The used gelatin fake finger (see Fig. E.4 c) was made of edible gelatin commercially available in common groceries. Gelatin is naturally transparent and can be easily dyed, but the dyeing decreases the level of transparency and it is nontrivial task to obtain skin color or to obtain the exactly same color twice. The problem of this material is also the tiny bubbles formed during the cooking process, which causes impossibility of finding of papillary lines under high magnification and the used illumination (see Fig. E.4 d). Moreover, it is necessary to count with rapid degradation of such fake fingers due to drying out. The most of transparent gelatin fake fingers are of sufficient quality only for a few hours after creation and the optical parameters of colored gelatin fake fingers are changing even faster.

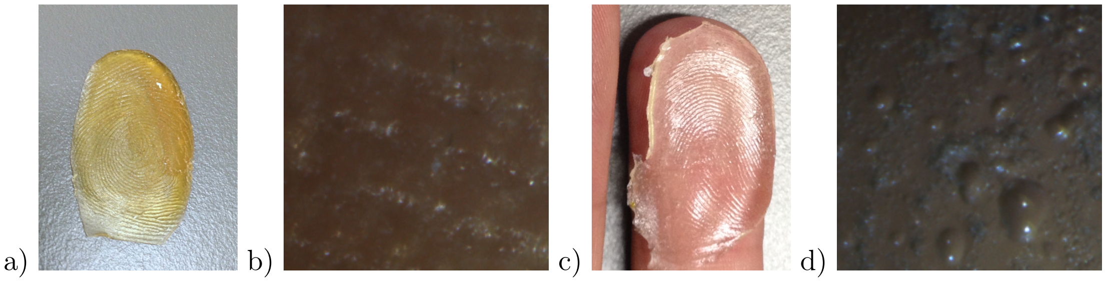


Figure E.4: Fake finger made of a) transparent Latex Gedeo with b) cut part of captured sample, and fake finger made of c) transparent gelatin with d) cut part of captured sample (see the presence of bubbles and absence of papillary lines).

It is important to use common edible gelatin (animal product) and do not use agar (so called Japanese gelatin, plant product), because it has completely different optical parameters: it is less transparent, slightly white colored and very sticky (it is almost impossible to avoid contamination by tiny textile fibers under normal circumstances).

Gummy bears. The „gummy bears" are commonly available candies made mostly of sugar, gelatin, and food coloring. Usage of „gummy bears" as a material for fake fingers is one variant of creation of gelatin fake fingers proposed by Prof. Matsumoto [45]. I used the gummy-bear fake fingers for tests of various sensors and (according to my experiences) the best quality gummy-bear fake fingers can be made of orange „jo-jo bears" from Nestlé Česko s. r. o. [107] (see Fig. E.5 a).

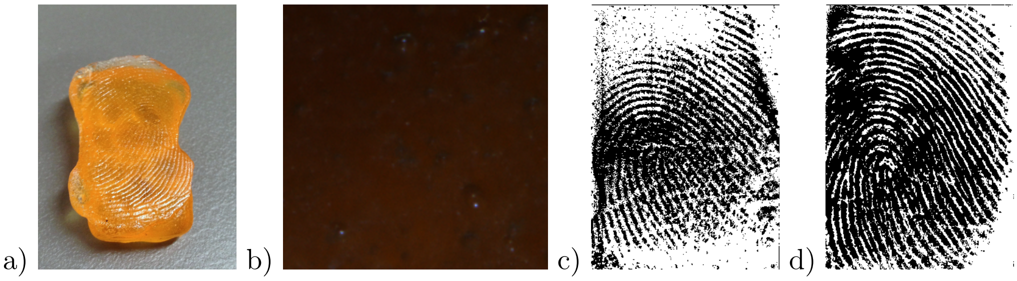


Figure E.5: The Fake finger made of a) orange gummy bears captured using b) my liveness detection approach (see the presence of bubbles and absence of papillary lines), c) Suprema SFM3050-TC1, and d) the corresponding live finger captured by the Suprema SFM3050-TC1.

The creation of these fake fingers is simple: the gummy bears are slightly melted using water bath, put into the wax mold and cooled down. Nevertheless, the problem can be the viscosity of the melted material and also the amount of tiny bubbles formed during the melting process (see Fig. E.5 b). Even if this material was not prone to form bubbles, these fakes would be easily detected, because (although this material has a memory effect) the re-narrowing (re-appearing) of the papillary lines usually takes a few tens of minutes.

Special compound. This compound is made from commercially available materials and allows enhancing the fake finger according to the skin color of particular person. This compound is primarily intended to spoof common optical touchless fingerprint sensors, but it was able to spoof even one of the existing sensors with the liveness detection capability (according to my experience). In case of fake fingers made of this special compound, it is necessary to count with a degradation of material. In most cases, these fake fingers can be used up to two days. In cases of very thin fake fingers, the borders of fake fingers can be dry and lighter in only ten minutes. The photograph of used fake finger made of special compound can be founf in Fig. E.6.

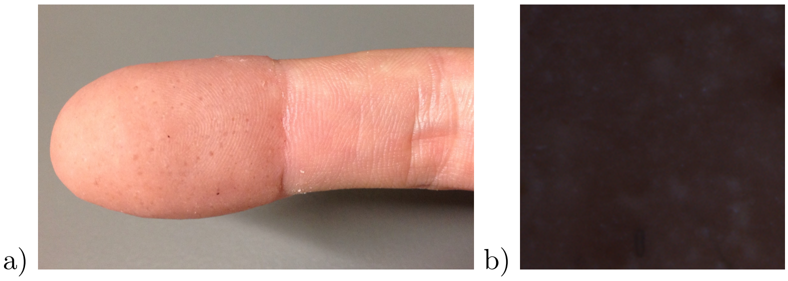


Figure E.6: Fake finger made of a) the special compound with b) cut part of captured sample (see the absence of papillary lines and presence of color areas corresponding to the various substances used for creation of this material).

Appendix F

Additional results of liveness detection

The following three figures (Fig. F.1 – F.3) show the detailed comparison of captured samples originating from live or fake fingers.

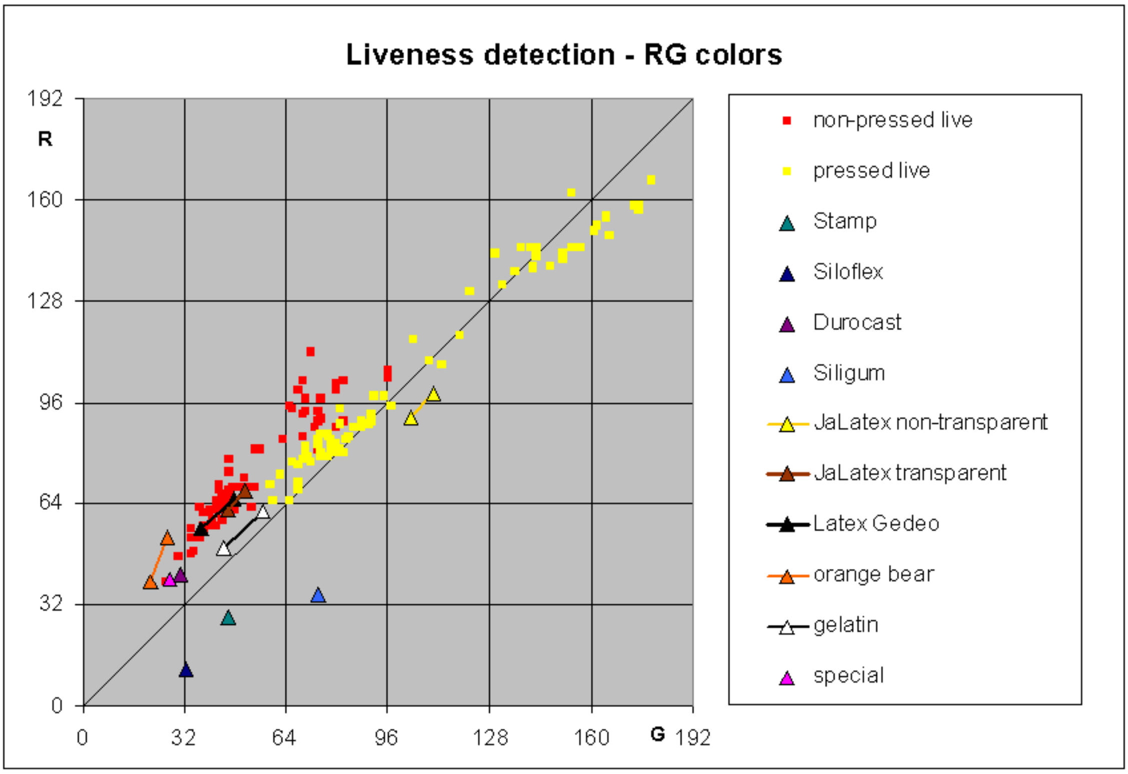


Figure F.1: The graph of mean R and G colors of non-pressed and pressed samples.

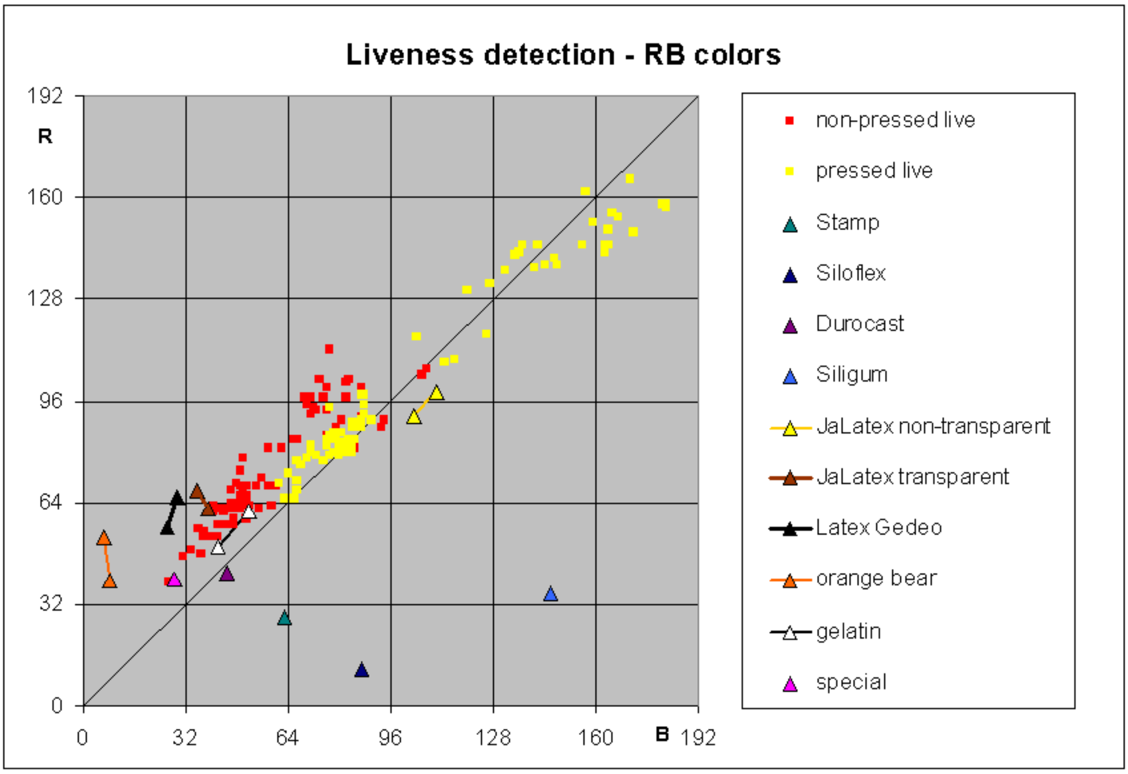


Figure F.2: The graph of mean R and B colors of non-pressed and pressed samples.

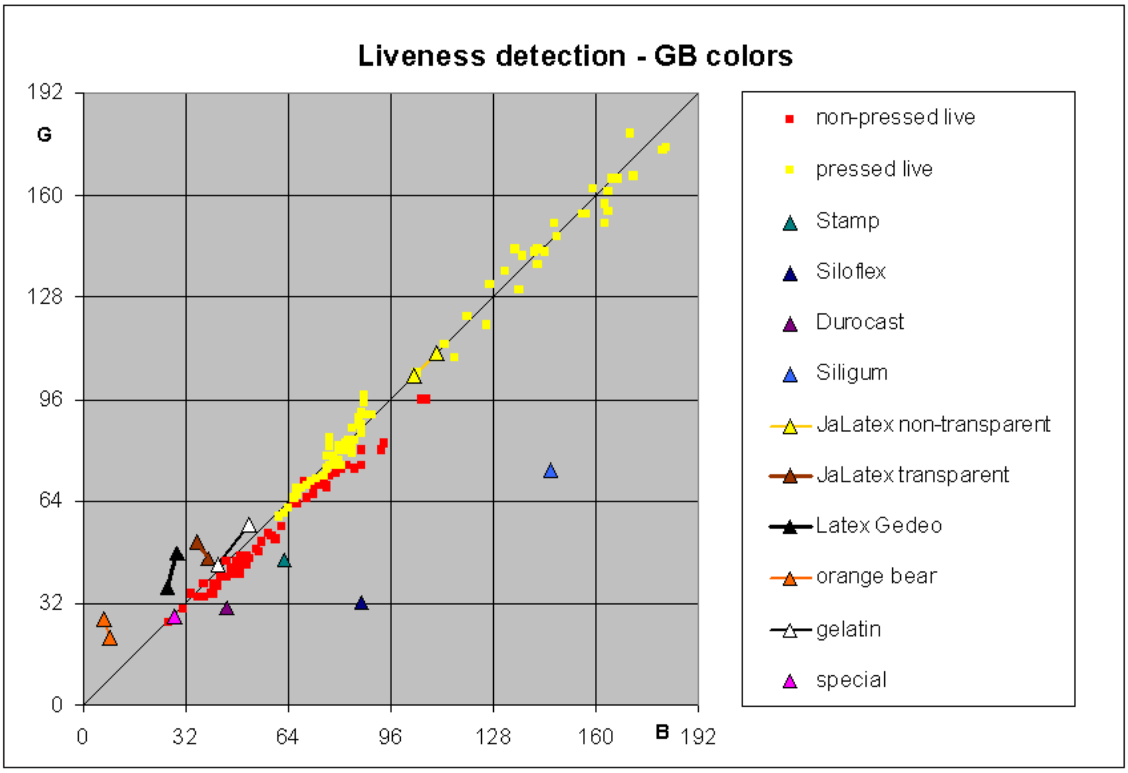


Figure F.3: The graph of mean G and B colors of non-pressed and pressed samples.

Appendix G

The structure of the Ground Truth Database

The images in the Ground Truth were carefully selected by Ms. Elham Tabassi (NIST). The final GTD database consists of 9 638 fingerprints (6 800 from NIST SD14 database [71] and 2 838 images from NIST SD29 database [72]). Unfortunately, it is not possible to create the absolutely balanced database due to the limited sources and the non-uniform representation of patterns in the population. The characteristic of the final image selection can be found in Tab. G.1 and G.2.

Table G.1: The structure of the GTD database [65]. Finger position denotes the fingers from the right thumb (1) to the left index finger (10). Some information about fingerprints in SD29 database was unavailable.

	Sex		**Finger position**									
	Male	**Female**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
SD14	3 400	3 400	666	788	690	598	592	720	808	706	618	614
SD29	-	-	273	288	300	281	286	298	275	289	281	267
Total	-	-	939	1076	990	879	878	1018	983	995	899	881

Table G.2: The structure of the GTD database [65]. The fingerprint types are: arch (A), tented arch (TA), ulnar loop (UL), radial loop (RL), and whorl (W). Some information about fingerprints in SD29 database was unavailable.

	Fingerprint quality (NFIQ)					**Fingerprint type**					**Total**
	1	**2**	**3**	**4**	**5**	**A**	**TA**	**UL**	**RL**	**W**	
SD14	1 885	566	2 624	702	1 023	833	666	1 878	1 862	1 556	6 800
SD29	831	822	802	239	144	-	-	-	-	-	2 838
Total	2 716	1388	3 426	941	1 167	-	-	-	-	-	9 638

Appendix H

Additional results of semantic conformance testing

The following three figures (Fig. H.1 – H.3) show the detailed comparison of individual algorithms based on their conformance rate. The used algorithms are: mindtct.exe algorithm from NIST NBIS package (Rel 1.1.0) [106], Innovatrics ANSI and ISO SDK v 1.52 [93] and VeriFinger 6.1 SDK from NeuroTechnology [108].

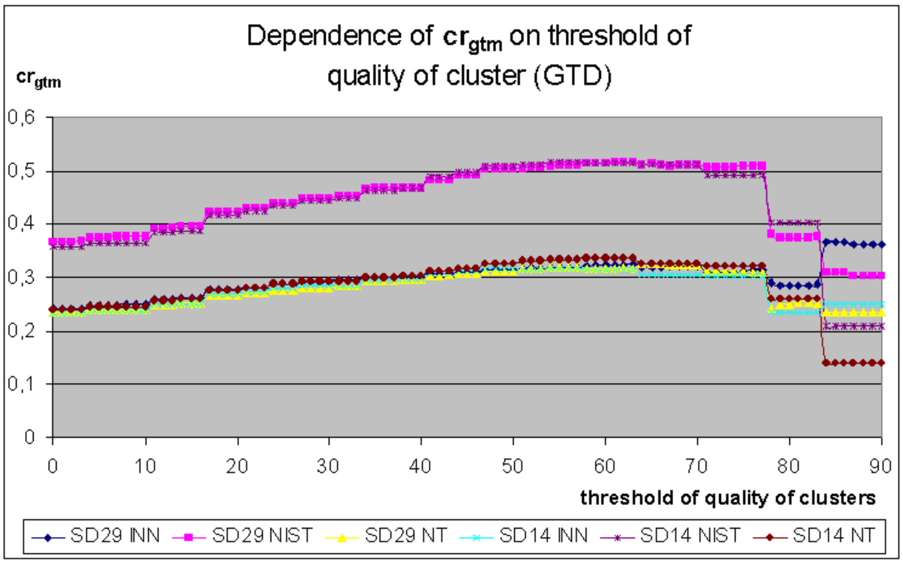


Figure H.1: Dependence of cr_{gtm} on quality of cluster threshold for both parts of GTD database. The algorithms from NIST, Innovatrics and NeuroTechnology are marked as NIST, INN and NT, respectively.

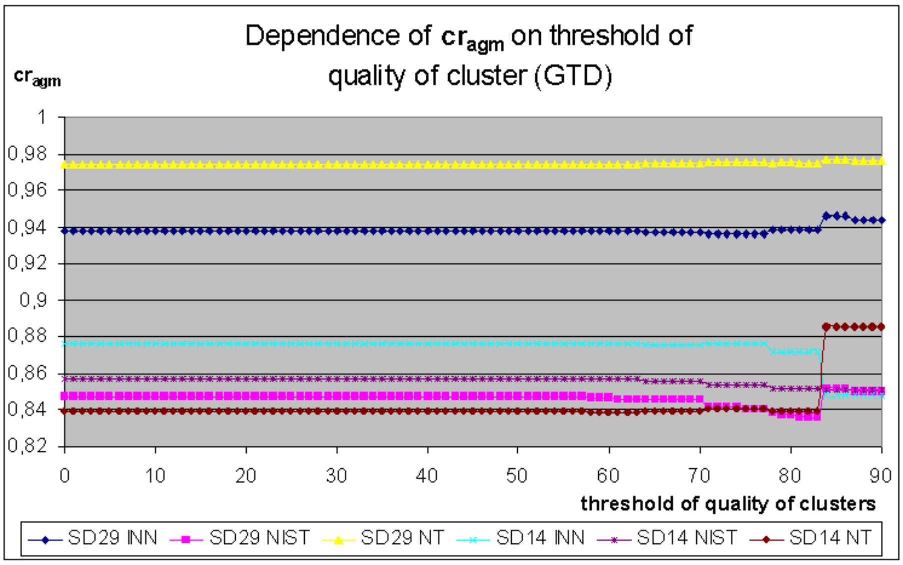


Figure H.2: Dependence of cr_{agm} on quality of cluster threshold for both parts of GTD database. The algorithms from NIST, Innovatrics and NeuroTechnology are marked as NIST, INN and NT, respectively.

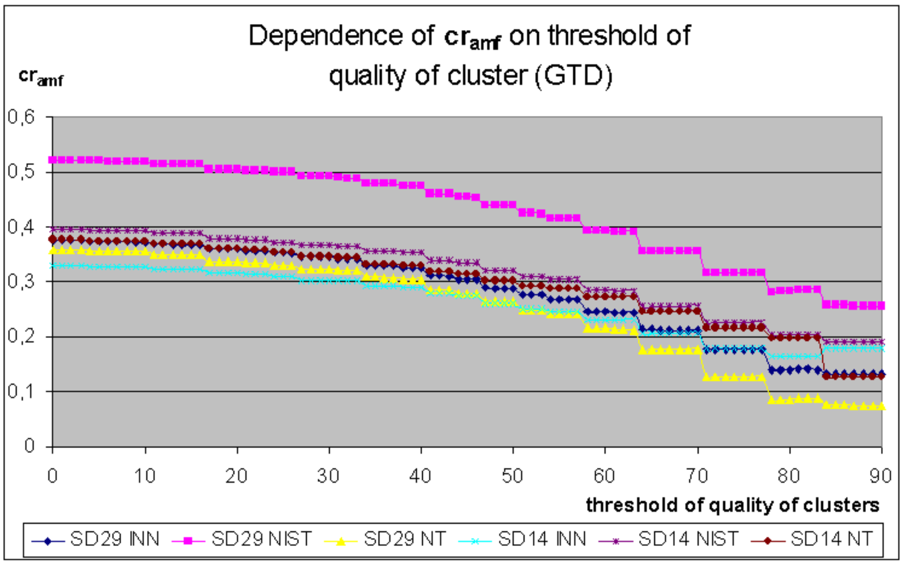


Figure H.3: Dependence of cr_{amf} on quality of cluster threshold for both parts of GTD database. The algorithms from NIST, Innovatrics and NeuroTechnology are marked as NIST, INN and NT, respectively.

The following six figures (Fig. H.4 – H.9) show the detailed comparison of three conformance rates of the same algorithm. The used algorithms are: mindtct.exe algorithm from NIST NBIS package (Rel 1.1.0) [106], Innovatrics ANSI and ISO SDK v 1.52 [93] and VeriFinger 6.1 SDK from NeuroTechnology [108].

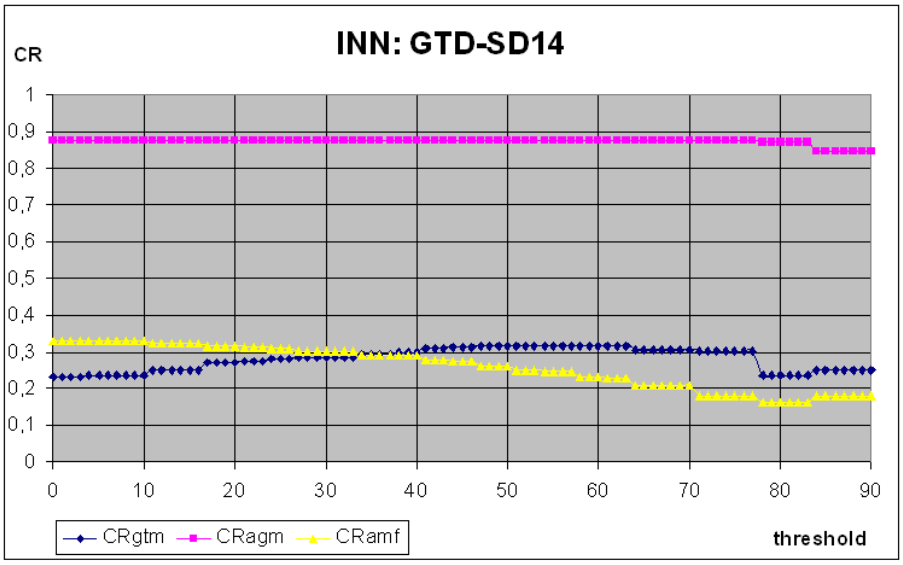


Figure H.4: Dependence of conformance rates on quality of cluster threshold for GTD-SD14 database and algorithm from Innovatrics.

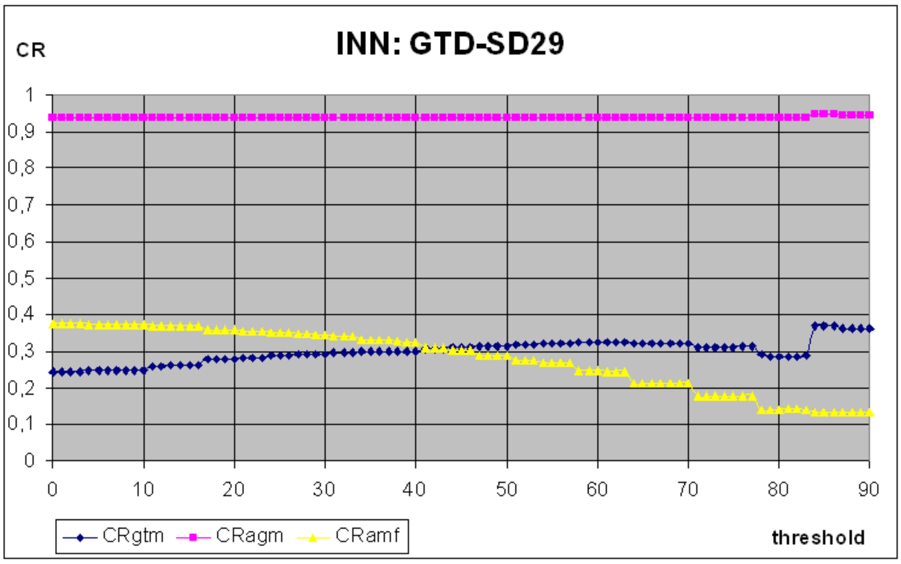


Figure H.5: Dependence of conformance rates on quality of cluster threshold for GTD-SD29 database and algorithm from Innovatrics.

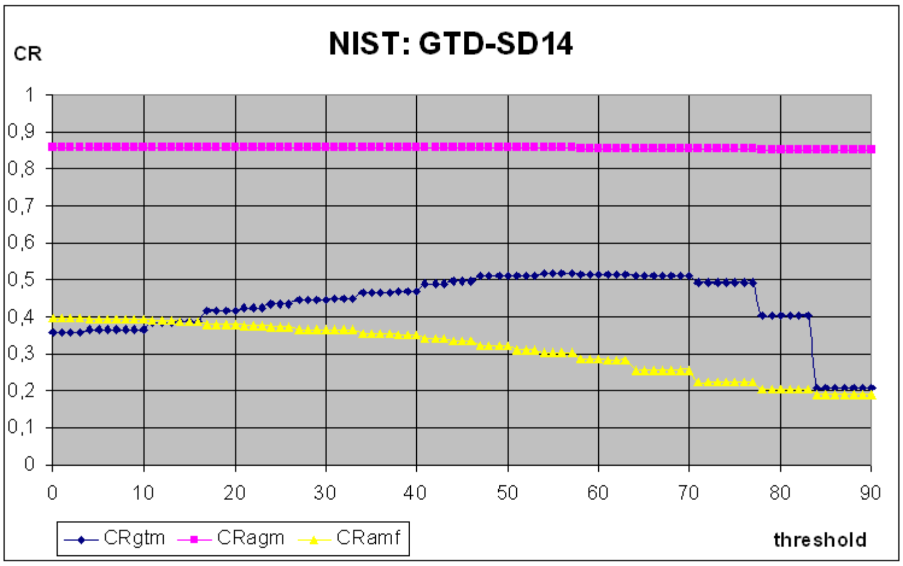


Figure H.6: Dependence of conformance rates on quality of cluster threshold for GTD-SD14 database and algorithm from NIST.

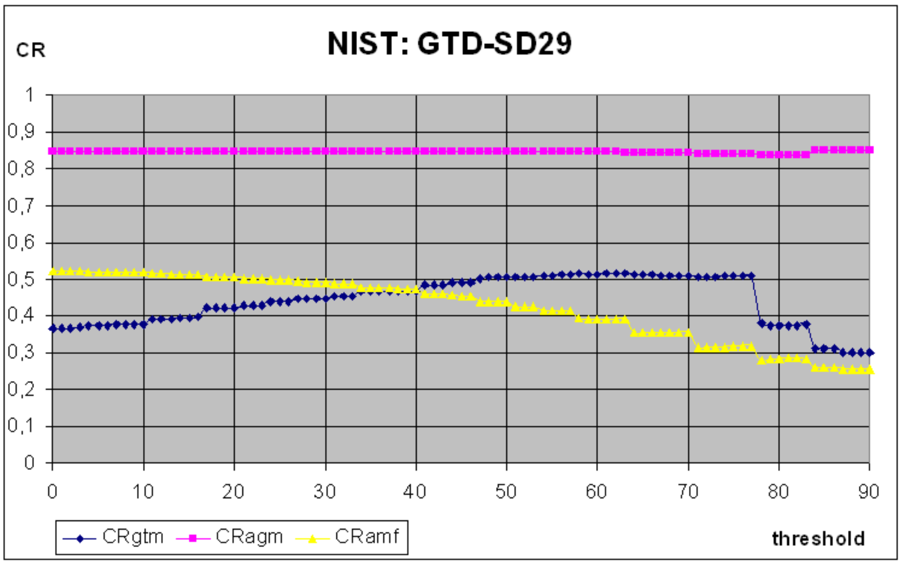


Figure H.7: Dependence of conformance rates on quality of cluster threshold for GTD-SD29 database and algorithm from NIST.

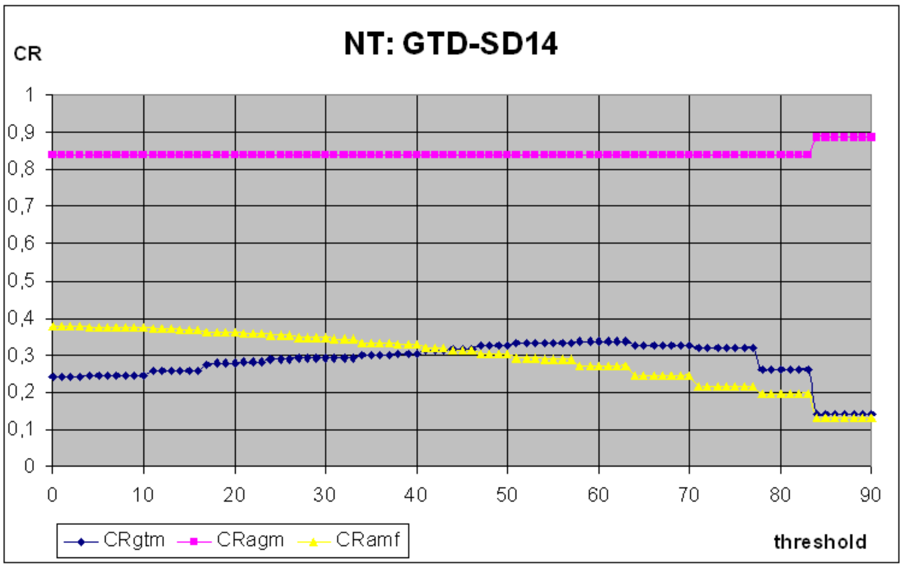


Figure H.8: Dependence of conformance rates on quality of cluster threshold for GTD-SD14 database and algorithm from NeuroTechnology.

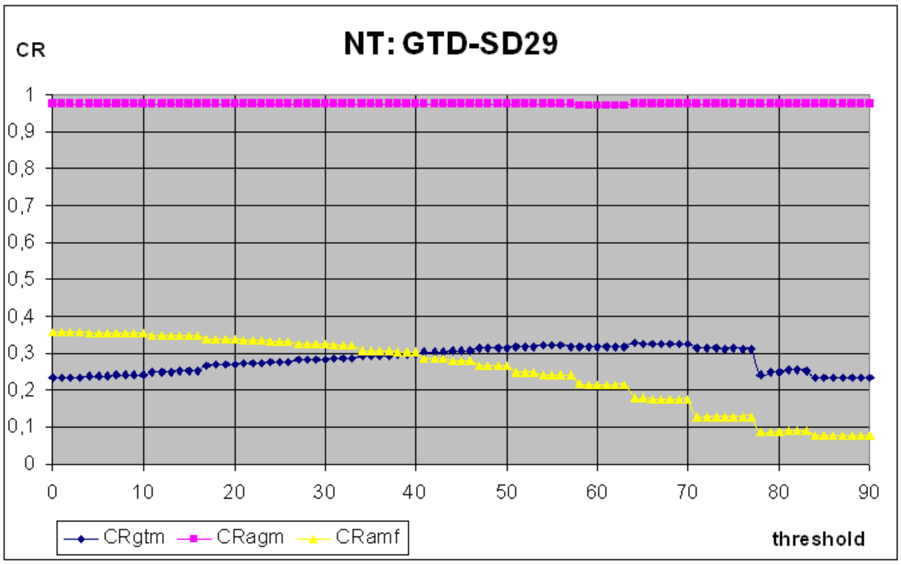


Figure H.9: Dependence of conformance rates on quality of cluster threshold for GTD-SD29 database and algorithm from NeuroTechnology.

Lists of author's publications, research and teaching activities

All lists are ordered alphabetically by primary author's surname.

Patents and utility models

1. DRAHANSKÝ, M., HEJTMÁNKOVÁ, D., DVOŘÁK, R., KRAJÍČEK, J., NEZHYBA, O.: *Biometric security device for acquirement and recognition of finger veins of a human hand.* Proposal for Czech Patent.
2. DRAHANSKÝ, M., HEJTMÁNKOVÁ, D., DVOŘÁK, R., KRAJÍČEK, J., NEZHYBA, O.: *Biometric security device for acquirement and recognition of finger veins of a human hand.* Czech utility model No. 21548. 2010.
3. LODROVÁ, D., DRAHANSKÝ, M.: *Liveness Detection on Fingers by Causation of Optical Changes.* Czech utility model No. 19364. 2009.

Books and book chapters

1. DRAHANSKÝ, M., ORSÁG, F., DOLEŽEL, M., DVOŘÁK, R., HÁJEK, J., HANÁČEK, P., HEJTMÁNKOVÁ, D., HERMAN, D., KNĚŽÍK, J., MARVAN, A., MRÁČEK, Š., STRUŽKA, J., VÁŇA, J.: *Biometrie* [Biometrics]. Brno (Czech Republic): Computer Press, 2011. ISBN 978-80-254-8979-6.

   cited in:

   - MALČÍK, D., DRAHANSKÝ, M.: Anatomy of Biometric Passports. *Journal of Biomedicine and Biotechnology* [JBB], Vol. 2012, No. 1. New York (USA): Hindawi Publishing Corporation, 2012. p. 8. ISSN 1110-7243.
   - MALČÍK, D., DRAHANSKÝ, M.: Anatomy of Biometric Passports. *Advanced Science and Technology Letters: Information Science and Industrial Applications* [ASTL], Vol. 2012, No. 4. Cebu (Philippines): SERSC, 2012. pp. 258–263. ISSN 2287-1233.

Journal articles

1. DOLEŽEL, M., HEJTMÁNKOVÁ, D., BUSCH, C., DRAHANSKÝ, M.: Segmentation Procedure for Fingerprint Area Detection in Image Based on Enhanced Gabor

Filtering. *International Journal of Bio-Science and Bio-Technology* [IJBSBT], Vol. 2, No. 4. Korea: SERCS, 2010. pp. 39–50. ISSN 1976-118X.

cited in:

- HOANG, F. N., SPITSYN, V. G.: Алгоритмы для Классификации Отпечатков Пальцев на Основе Применения Фильтра Габора, Вейвлет/Преобразования и Многослойной Нейронной Сети [Algorithm for Fingerprint Classification Based on the Application of Gabor Filters, Wavelet Transformations and Multi-layer Neural Network]. *Bulletin of the Tomsk Polytechnic University*, Vol. 320, No. 5. Tomsk (Russia): TPU, 2012. pp. 60–64. ISSN 1684-8519.

2. DRAHANSKÝ, M., BŘEZINOVÁ, E., HEJTMÁNKOVÁ, D., ORSÁG, F.: Fingerprint Recognition Influenced by Skin Diseases. *International Journal of Bio-Science and Bio-Technology* [IJBSBT], Vol. 2, No. 4. Korea: SERCS, 2010. pp. 11–22. ISSN 1976-118X.

   cited in:

   - BÖHM, C., FÄRBER, I., FRIES, S., KORTE, U., MERKLE, J., OSWALD, A., SEIDL, T., WACKERSREUTHER, B., WACKERSREUTHER, P.: Efficient Database Techniques for Identification with Fuzzy Vault Templates. In: *Proceedings of the Special Interest Group on Biometrics and Electronic Signatures* [BIOSIG2011]. Darmstadt (Germany): GI, 2011. pp. 115–126. LNI 191, ISBN 978-3-88579-285-7.
   - COZZELLA, L., SIMONETTI, C., SPAGNOLO, G. S.: Is it possible to use biometric techniques as authentication solution for objects? Biometry vs. hylemetry. In: *Proceedings of the 5th International Symposium on Communications, Control and Signal Processing* [ISCCSP 2012]. Rome (Italy): IEEE, 2012. pp. 1–6. ISBN 978-1-4673-0274-6.
   - DRAHANSKÝ, M., DOLEŽEL, M., URBÁNEK, J., BŘEZINOVÁ, E., KIM, T-H.: Influence of Skin Diseases on Fingerprint Recognition. *Journal of Biomedicine and Biotechnology*, Vol. 2012, No. 4. New York (USA): Hindawi Publishing Corporation, 2012. p. 14. ISSN 1110-7251.
   - MNGENGE, N. A., NELWAMONDO, F. V., MALUMEDZHA, T., MSIMANG, N.: Quality-Based Fingerprint Segmentation. In: CAMPILHO, A., KAMEL, M. (Eds.): *Image Analysis and Recognition.* Berlin (Germany): Springer, 2012. pp. 54–63. LNCS 7325/2012. ISBN 978-3-642-31297-7.
   - XIE, S. J., YANG, J. C., PARK, D. S., YOON, S., SHIN, J.: Fingerprint Quality Analysis and Estimation for Fingerprint Matching. In: YANG, J., NANNI, L. (Eds.): *State of the art in Biometrics.* Rijeka (Croatia): InTech, 2011. pp. 3–24. ISBN 978-953-307-489-4.

3. DRAHANSKÝ, M., BŘEZINOVÁ, E., ORSÁG, F., HEJTMÁNKOVÁ, D.: Dermatologické faktory ovlivňující snímání otisků prstů pro biometrické účely [Dermatologic Factors Influencing Capturing of Fingerprints for Biometric Purposes]. *Kriminalistika*, Vol. 42, No. 3. Praha (Czech Republic): MVČR, 2010. pp. 196–206. ISSN 1210-9150.

4. DRAHANSKÝ, M., HEJTMÁNKOVÁ, D.: New Experiments with Optical Liveness Testing Methods. *Journal of Information Hiding and Multimedia Signal Processing*

[JIHMSP], Vol. 1, No. 4. Taiwan: Ubiquitous International USA, 2010. pp. 301–309. ISSN 2073-4212.

cited in:

- YAMBAY, D., GHIANI, L., DENTI, P., MARCIALIS, G. L., ROLI, F., SCHUCKERS, S.: LivDet 2011 - Fingerprint Liveness Detection Competition 2011. In: *Proceedings 2012 5th IAPR International Conference on Biometrics* [ICB2012]. New Delhi (India): IEEE, 2012. pp. 208–215. ISBN 978-1-4673-0396-5.

5. DRAHANSKÝ, M., LODROVÁ, D.: Liveness Detection for Biometric Systems Based on Papillary Lines. *International Journal of Security and Its Applications* [IJSIA], Vol. 2, No. 4. Korea: SERSC, 2008. pp. 29–37. ISSN 1738-9976.

   cited in:

   - MALČÍK, D., DRAHANSKÝ, M.: Anatomy of Biometric Passports. *Journal of Biomedicine and Biotechnology* [JBB], Vol. 2012, No. 1. New York (USA): Hindawi Publishing Corporation, 2012. p. 8. ISSN 1110-7243.
   - SINGH, A., TIWARI, S., SINGH, S. K.: Vitality Detection in Face Images using Second Order Gradient. *International Journal of Computer Applications & Information Technology* [IJCAIT], Vol. 1, No. 2. India: Mahadev Educational Society, 2012. pp. 96–101. ISSN 2278-7720.
   - SU, F., XIA, L., CAI, A., MA, J.: A Dual-Biometric-Modality Identification System Based on Fingerprint and EEG. In: *IEEE International Conference on Biometrics: Theory Applications and Systems* [BTAS2010]. Washington (USA): IEEE, 2010. pp. 1–6. ISBN 978-1-4244-7581-0.
   - SU, F., XIA, L., CAI, A., MA, J.: Evaluation of Recording Factors in EEG-based Personal Identification: a Vital Step in Real Implementations. In: *Proceedings of International Conference on Systems Man and Cybernetics* [SMC2010]. Istanbul (Turkey): IEEE, 2010. pp. 3861–3866. ISBN 978-1-4244-6586-6.
   - SURESH, M., KRISHNAMOHAN, P. G., MALLIKARJUN, S. H.: Electromyography Analysis for Person Identification. *International Journal of Biometrics and Bioinformatics* [IJBB], Vol. 2, No. 3. Malaysia: Computer Science Journals, 2011. pp. 172–179. ISSN 1985-2347.

6. DRAHANSKÝ, M., LODROVÁ, D., ORSÁG, F., BŘEZINOVÁ, E.: Detekce živosti prstů [Liveness Detection of Fingerprints]. *Data Security Management* [DSM], Vol. 13, No. 2. Praha (Czech Republic): TATE International, 2009. pp. 22–26. ISSN 1211-8737.

7. HEJTMÁNKOVÁ, D., DVOŘÁK, R., DRAHANSKÝ, M., ORSÁG, F.: A New Method of Finger Veins Detection. *International Journal of Bio-Science and Bio-Technology* [IJBSBT], Vol. 1, No. 1. Korea: SERSC, 2009. pp. 11–15. ISSN 1976-118X.

   cited in:

   - JUAN, C.-C.: *Segmentation of Finger Vein Image using Level Set Method with Image Inhomogeneity Correction.* Jhongli City (Taiwan), 2011. Master thesis, National Central University, Department of Electrical Engineering.

- LISÁK, P.: Human Recognition by Finger Veins. In: *Proceedings of the 17th Conference STUDENT EEICT 2011*, Vol. 2. Brno (Czech Republic): NOVPRESS, 2011. p. 3. ISBN 978-80-214-4273-3.
- LISÁK, P.: *Rozpoznávanie človeka podla žíl v prste* (Human Recognition by Finger Veins). Brno (Czech Republic), 2011. Master thesis, Brno University of Technology, Faculty of Information Technology.

Conference papers

1. BUSCH, C., HEJTMÁNKOVÁ, D., TABASI, E., GROTHER, P., KRODEL, W., NEUMANN, L., RUHLAND, T., DOLEŽEL, M., KORTE, U.: Semantic Conformance Testing Methodology and Initial Results for Fingerprint Minutia Encoding, In: *Proceedings of the International Biometric Performance Conference* [IBPC2010]. Gaithersburg (USA): NIST, 2010. p. 23.
2. BUSCH, C., LODROVÁ, D., TABASSI, E., KRODEL, W.: Semantic Conformance Testing for Finger Minutiae Data. In: *Proceedings of IWSCN2009.* Trondheim (Norway): IEEE, 2009. pp. 17–24. ISBN 978-82-997105-1-0.

   cited in:

   - ABT, S.: *Assessing Semantic Conformance of Minutiae-based Feature Extractors.* Darmstadt (Germany), 2011. Master thesis, Darmstadt University of Applied Sciences, Department of Computer Science.
   - ABT, S., BUSCH, C., BAIER, H.: A quality score honoring approach to semantic conformance assessment of minutiae-based feature extractors. In: *Proceedings of the Special Interest Group on Biometrics and Electronic Signatures* [BIOSIG2011]. Darmstadt (Germany): GI, 2011. pp. 21–32. LNI 191, ISBN 978-3-88579-285-7.
   - ABT, S., BUSCH, C., NICKEL, C.: Applikation des DBSCAN Clustering-Verfahrens zur Generierung von Ground-Truth Fingerabdruck-Minutien [Application of DBSCAN Clustering Method to Generate Ground-Truth Fingerprint Minutiae]. In: *Proceedings of the Special Interest Group on Biometrics and Electronic Signatures* [BIOSIG2010]. Darmstadt (Germany): GI, 2010. pp. 95–106. LNI 164, ISBN 978-3-88579-258-1.
   - RIOPKA, T. P., MA, L.: Characterizing minutia extractors for semantic conformance testing. In: *Fourth IEEE International Conference on Biometrics: Theory Applications and Systems* [BTAS2010]. Washington (USA): IEEE, 2010. pp. 431–436. ISBN 978-1-4244-7581-0.
3. DOLEŽEL, M., HEJTMÁNKOVÁ, D., BUSCH, C., DRAHANSKÝ, M.: Fingerprint Area Detection in Fingerprint Images Based on Enhanced Gabor Filtering. In: *Database Theory and Application, Bio-Science and Bio-Technology* [BSBT2010]. Berlin (Germany): Springer, 2010. pp. 234–240. ISBN 978-3-642-17622-7.
4. DRAHANSKÝ, M., BŘEZINOVÁ, E., ORSÁG, F., LODROVÁ, D.: Classification of Skin Diseases and Their Impact on Fingerprint Recognition. In: *Proceedings of the Special Interest Group on Biometrics and Electronic Signatures* [BIOSIG2009]. Darmstadt (Germany): GI, 2009. pp. 173–176. LNI 155, ISBN 978-3-88579-249-9.

cited in:

- MALČÍK, D., DRAHANSKÝ, M.: Anatomy of Biometric Passports. *Journal of Biomedicine and Biotechnology* [JBB], Vol. 2012, No. 1. New York (USA): Hindawi Publishing Corporation, 2012. p. 8. ISSN 1110-7243.

5. DRAHANSKÝ, M., LODROVÁ, D.: Experiments with Optical Liveness Testing Method. In: *Proceedings of the 2009 Fifth International Conference on Intelligent Information Hiding and Multimedia Signal Processing* [IIH-MSP 2009]. Kyoto (Japan): IEEE, 2009. p. 123–128. ISBN 978-0-7695-3762-7.

6. DRAHANSKÝ, M., LODROVÁ, D.: Liveness Detection for Biometric Systems Based on Papillary Lines. In: *Proceedings of Information Security and Assurance* [ISA2008]. Busan (Korea): IEEE, 2008. pp. 439–444. ISBN 978-0-7695-3126-7.

   cited in:

   - DRAHANSKÝ, M.: Liveness Detection in Biometrics. In: CHETTY, C., YANG, J. (Eds.): *Advanced Biometric Technologies.* Rijeka (Croatia): InTech, 2011. pp. 179-198. ISBN 978-953-307-487-0.
   - DUNSTONE, T., YAGER, N.: Vulnerabilities. In: *Biometric System and Data Analysis: Design, Evaluation, and Data Mining.* Eveleigh (Australia): Springer, 2009. pp. 247–262. ISBN 978-0-387-77625-5.

7. DVOŘÁK, R., HEJTMÁNKOVÁ, D., DITTRICH, P., VÁŇA, J., DRAHANSKÝ, M.: Research in the area of biometric systems - liveness detection; recognition of 3D hand, finger veins and thermofaces. In: *World and homeland security.* Brno (Czech Republic): UNOB, 2010. pp. 143–152. ISBN 978-80-7231-728-8.

8. HEJTMÁNKOVÁ, D., DVOŘÁK, R., DRAHANSKÝ, M., ORSÁG, F.: Method for Finger Veins Detection. In: *Analysis of Biomedical Signals and Images* [BIOSIGNAL2010]. Brno (Czech Republic): VUTIUM, 2010. pp. 240–243. ISBN 978-80-214-4105-7.

9. HEJTMÁNKOVÁ, D., DVOŘÁK, R., DRAHANSKÝ, M., ORSÁG, F.: A New Approach for Veins Detection. In: *Proceedings of International Conference BSBT 2009.* Berlin (Germany): Springer, 2009. pp. 76–80. ISBN 978-3-642-10615-6.

10. LODROVÁ, D.: Rozpoznávání živosti otisků prstů [Liveness testing by fingers]. In: *Proceedings of the 13th Conference STUDENT EEICT 2007.* Brno (Czech Republic): VUTIUM, 2007. pp. 260–262. ISBN 978-80-214-3408-0.

11. LODROVÁ, D., BUSCH, C., TABASSI, E., KRODEL, W., DRAHANSKÝ, M.: Semantic Conformance Testing Methodology for Finger Minutiae Data. In: *Proceedings of the Special Interest Group on Biometrics and Electronic Signatures* [BIOSIG2009]. Darmstadt (Germany): GI, 2009. pp. 31–42. LNI 155, ISBN 978-3-88579-249-9.

    cited in:

    - ABT, S.: *Assessing Semantic Conformance of Minutiae-based Feature Extractors.* Darmstadt (Germany), 2011. Master thesis, Darmstadt University of Applied Sciences, Department of Computer Science.

- ABT, S., BUSCH, C., BAIER, H.: A quality score honoring approach to semantic conformance assessment of minutiae-based feature extractors. In: *Proceedings of the Special Interest Group on Biometrics and Electronic Signatures* [BIOSIG2011]. Darmstadt (Germany): GI, 2011. pp. 21–32. LNI 191, ISBN 978-3-88579-285-7.
- ABT, S., BUSCH, C., NICKEL, C.: Applikation des DBSCAN Clustering-Verfahrens zur Generierung von Ground-Truth Fingerabdruck-Minutien [Application of DBSCAN Clustering Method to Generate Ground-Truth Fingerprint Minutiae]. In: *Proceedings of the Special Interest Group on Biometrics and Electronic Signatures* [BIOSIG2010]. Darmstadt (Germany): GI, 2010. pp. 95–106. LNI 164, ISBN 978-3-88579-258-1.

12. LODROVÁ, D., DRAHANSKÝ, M.: Methods of Liveness Testing By Fingers. In: *Analysis of Biomedical Signals and Images* [BIOSIGNAL2008]. Brno (Czech Republic): VUTIUM, 2008. pp. 1–7. ISBN 978-80-214-3612-1.

    cited in:

    - DRAHANSKÝ, M.: Liveness Detection in Biometrics. In: CHETTY, C., YANG, J. (Eds.): *Advanced Biometric Technologies.* Rijeka (Croatia): InTech, 2011. pp. 179-198. ISBN 978-953-307-487-0.

13. LODROVÁ, D., DRAHANSKÝ, M.: New Liveness Detection Method Based on Causation of Optical Changes. In: *Proceedings of IWSCN2009.* Trondheim (Norway): IEEE, 2009. pp. 25–29. ISBN 978-82-997105-1-0.

Other publications

1. DRAHANSKÝ, M., LODROVÁ, D.: *Optical Principle for Liveness Detection.* Alghero (Italy): 2008. p. 10. [presentation].
2. DRAHANSKÝ, M., ORSÁG, F., LODROVÁ, D.: *Technické hodnocení biometrických systémů* [Technical Evaluation of Biometric Systems]. Praha (Czech Republic): NBU, 2008. p. 108. [research report with classified information].
3. LODROVÁ, D.: *Spoofing and anti-spoofing methods for fingerprint sensors.* Oslo-Fornebu (Norway): IDEX ASA, 2008. p. 16. [technical report].
4. LODROVÁ, D.: *Testing of abnormal behavior of users on IDEX fingerprint sensor.* Gjøvik (Norway): IDEX, 2009. p. 21. [technical report with classified information].

Solicited lectures

1. HEJTMÁNKOVÁ, D.: *Level 3 Conformance Testing for Finger Minutiae Data.* Canberra (Australia): CrimTrac, 2009. p. 27. [presentation].
2. HEJTMÁNKOVÁ, D., DITTRICH, P.:*Liveness detection for TBS touchless sensor.* Pfaeffikon SZ (Switzerland): Touchless Biometric Systems AG, 2010. p. 26. [presentation].

3. LODROVÁ, D.: *Level 3 Conformance Testing for Finger Minutiae Data.* Moscow (Russia): ISO/IEC JTC 1/SC 37 WG3, 2009. p. 13. [presentation].

4. LODROVÁ, D.: *Semantic Conformance Testing for Finger Minutiae Data.* Darmstadt (Germany): Fraunhofer Gesellschaft, 2009. p. 21. [presentation].

5. LODROVÁ, D.: *Spoofing and anti-spoofing methods for fingerprint sensors.* Oslo-Fornebu (Norway): IDEX ASA, 2008. p. 33. [presentation].

Reviews

1. ACN 2011, review of 3 paper.
2. BSBT 2009, review of 2 papers.
3. EEICT 2010, review of 1 paper.
4. EEICT 2011, review of 1 paper.
5. IIH-MSP 2009, review of 2 papers.
6. ISA 2011, review of 3 papers.
7. ISO/IEC JTC1/SC37 WG3 2010, review and comments to 2nd WD ISO/IEC 29109-2 Amd.2.

Software

1. DLUHOŠ, O., DOLEŽEL, M., HEJTMÁNKOVÁ, D.: *GUI for fast fingerprinting.* 2010.
2. LODROVÁ, D.: *GUI for dactyloscopy.* 2010.

Projects

1. *Adjustment of algorithms for 3D fingerprints*, TBS, TBS-BL-2009, 2009-2010. [team leader].
2. *Advanced secured, reliable and adaptive IT*, FIT-S-11-1, 2011-2013. [team member].
3. *Biometric Authentication Systems based on Biometric Template Protection Schemes*, BioKeyS-Pilot-DB, BSI, 2010-2011. [team member].
4. *Education of liveness testing in subject Biometric systems*, FRVŠ MŠMT,FR2525/2009/G1, 2009. [research leader].
5. *Finger veins recognition*, Digitus, VEPA20092010, 2009-2010. [team leader].
6. *Ground Truth Database for Finger Minutiae Data*, BKA, GTD, 2008-2013. [team leader].
7. *Idex project*, IDEX, IDEX, 2008-2009. [team member].

8. *Information Technology in Biomedical Engineering*, GAČR, GD102/09/H083, 2009-2012. [team member].
9. *Student Scientific Activity*, JCMM, SOČ, 2010. [team leader].
10. *TeamIT - Building Competitive Research Teams in IT*, MŠMT, CZ.1.07/2.3.00/ 09.0067, 2009-2012. [team member].
11. *Technical evaluation of biometric systems*, NBU, ST20072007006, 2007. [team member].
12. *Testing of the sensor TST-Biometrics BiRD 3*, TST, TST-2009-FIT, 2009. [team leader].
13. *Trusted Revocable Biometric Identities*, EU-7FP-ICT, TURBINE, 2008-2011. [team member].

Memberships

2012 Bio-Science and Bio-Technology BSBT2012 [Program committee].
ISO/IEC JTC 1/SC 37 WG3 [co-editor].
SERSC - Czech section [Secretary].

2011 Advanced Communication and Networking ACN2011 [Program committee].
Bio-Science and Bio-Technology BSBT2011 [Program committee].
Information Security and Assurance ISA2011 [Program committee].
ISO/IEC JTC 1/SC 37 WG3 [co-editor].
SERSC - Czech section [Secretary].

2010 Bio-Science and Bio-Technology BSBT2010 [Program committee].
ISO/IEC JTC 1/SC 37 WG3 [co-editor].
SERSC - Czech section [Secretary].

2009 Bio-Science and Bio-Technology BSBT2009 [Program committee].
SERSC - Czech section [Secretary].

2008 Bio-Science and Bio-Technology BSBT2008 [Steering committee].

Abroad residences

2010/04/26 TOUCHLESS BIOMETRIC SYSTEMS AG, Pfäffikon SZ (Switzerland).
- 2010/05/07 Liveness detection for a fingerprint sensor.

2008/08/12 GJØVIK UNIVERSITY COLLEGE, NISlab, Gjøvik (Norway).
- 2009/02/11 Semantic conformance testing for finger minutiae data.

2008/08/12 IDEX ASA, Oslo-Fornebu (Norway).
- 2009/02/11 Liveness detection, testing of quality of fingerprint sensors.

Teaching activities

Lectures

2009/10	Biometric systems	1 lecture (Fingerprints)
2010/11	Biometric systems	1 lecture (Fingerprints)

Laboratory exercises

2007/08	Assembly Languages	7× 5 groups of 20 students
	Biometric systems	2× 13 groups of 10 students
	Robotics	1× 1 group of 10 students
2009/10	Biometric systems	2× 18 groups of 10 students
2010/11	Biometric systems	2× 10 groups of 10 students

Individial projects

2009/10	Biometric systems	39 projects
2010/11	Biometric systems	20 projects

Midterm exam

2008/09	Fundamentals of Artificial Intelligence	503 students

Theses

2008/09	Reviewing of Bachelor thesis	1×
2009/10	Supervising of Bachelor thesis	2×
	Supervising of Master thesis	1×
	Reviewing of Master thesis	2×
2010/11	Supervising of Master thesis	1×
	Reviewing of Bachelor thesis	5×

The requirements for the amount of teaching activities have been met.