Security of Biometric Systems

Dana Lodrová
Department of Intelligent Systems
Faculty of Information Technology
Brno University of Technology
Božetěchova 2, 612 66 Brno, Czech Republic
Dana.Brno@gmail.com

Abstract
The main contributions of the 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.

Categories and Subject Descriptors
J.3 [Life and Medical Sciences]: Biology and Genetics; K.6.5 [Management of Computing and Information Systems]: Security and Protection—authentication, unauthorised access; I.3.6 [Computer Graphics]: Methodology and Techniques—standards

Keywords
Biometrics, security, fingerprint, liveness detection, color and elasticity of finger, semantic conformance testing, finger minutiae data, interoperability, Ground Truth Database, standardization.

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, 8, 29, 30, 37, 42] 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 [44] or a successful attack of South Korean woman to Japanese immigration screening [40]).

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.

2. Security of biometric systems
At first it is necessary to analyze the possible vulnerabilities of biometric systems and describe the possible attacks and corresponding countermeasures/precautions.

2.1 Weak places and types of attack
The major weak places of a biometric system [3, 29] are marked in Fig. 1. As it can bee seen, there is neither component nor channel, which is impossible to attack.

Figure 1: A diagram of biometric system. Weak places are marked by numbers.
There are three basic types or goals of an attack: to obtain information/data, gain access or DoS (Denial of Service) attack [24, 29]. The simplest way to gain access is the spoofing of sensor, e.g., by the reactivation of latent fingerprint or using the fake finger. The possible precautions are the usage of liveness detection, fake finger detection or multi-modal biometric fusion. For gaining access, it is also possible to use, e.g., Replay attack or brute force attack.

The second possible goal of the 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 and subsequent creation of a fake finger. A possible precaution is the usage of cancelable/revocable biometrics.

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 invoke communication network by forged messages or by sabotage. It does not matter, which channel or component has been penetrated/invaded/compromised.

2.2 Spoofing of biometric sensor

In previous years, researches demonstrated several very successful methods for fooling of different types of fingerprint sensors. These methods can be divided into the following three categories [26]: reactivation of latent fingerprint, usage of artificial fake finger or dead/removed finger.

Activation of a latent fingerprint is the simplest and quickest way of spoofing of sensors. Thalheimer et al. [42] proposed a few ways how to fool capacitive fingerprint sensors. It is possible to breathe or put a thin-walled plastic bag filled with water on the sensor area. The combination of condensed water vapor from the breath or the water from the plastic bag with the grease from latent fingerprint causes the change of capacitance, which initiates the capturing process. 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.

The artificial fingers can be created most easily with assistance of enrollee. The enrollee presses his/her finger against prepared material and creates the mold, which is filled with appropriate material afterwards (e.g., free plastic mold and gelatin fingers [30]; wax mold and silicone fingers [42]; or dental impression material and play-doh fingers [36]). If the assistance of enrollee is not possible, the attacker has to obtain a latent fingerprint of the enrollee and create a mold using, e.g., photosensitive PCB (Printed Circuit Board) [26, 30]. On the other hand, it is also possible to slightly enhance the photograph of latent fingerprint and orders creation of a stamp in a common stationer’s shop (cost 4 EUR in 2007). The result can be seen in Fig. 2.

The most dangerous types of fake fingers are thin fingers glued on attackers own finger. It can be difficult to find this artificial finger by supervisor or a camera system. Moreover, some methods of liveness detection could penetrate through and test the liveness of a real finger behind it. This thin fake finger was successfully used, e.g., against Japanese fingerprint immigration screening in 2008 [40] and the possibilities of usage of fake fingers are also tested in the Life Finger project [8] using "BSI Fake-Tool-Box", which is able to spoof not only all 12 tested common sensors (5 different sensor technologies) but also all sensors with the liveness detection ability, which was possible to test [8].

The worst spoofing option is the usage of a human finger separated from a body. Prof. Schuckers et al. [37] tested this option by using of cadaver fingers 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.

2.3 Liveness detection and fake finger detection

The liveness detection (formerly called vitality detection) tries to detect whether the scanned sample belongs to the real live human finger and detects the presence of some property/properties typical for the live human sample. On the other hand, fake finger detection (spoof detection) tries to find whether the tested sample is a fake/artificial finger and detects 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.

In the last years, researches developed several methods, which are or can be used for the liveness detection purposes. The detailed comparison of these methods is given [26]. It can be seen that a lot of methods have been published without test results mainly because the princi-
ple was described in patent. As far as I know, there are only a few methods with published test results (e.g., odor analysis EER 7.48% [5], elasticity EER 4.78% [23], perspiration FAR 10% [36], impedance [39], color FAR 20% [48]) and the number of their tested subjects and used materials of fake fingers varies significantly (from 1 to 25 volunteers and maximally 3 different fake finger materials). 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) and detailed description of materials used for creation of fake fingers.

Nowadays, more and more fingerprint sensors on the market include some component/method for liveness detection (e.g., Lumidigm [28], Sagem Morpho [35], Sony [44], TST Biometrics [43]). 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 [8]). Some manufacturers even assume that the security of their solution will be higher, if they keep its principle hidden (so called "Security by obscurity" [26]).

Nowadays, the standard for liveness detection ISO/IEC 30107 (Anti-Spoofing and Liveness Detection Techniques) is under preparation [16]. This standardization project is in the 3rd Working Draft phase and it should contain (among others) necessary terms, concepts and error rate metrics [32].

2.4 Biometric fusion

Another approach to increase the security and reduce the chance of sensor deception is the usage of biometric fusion - multibiometrics. Generally, it is possible to distinguish six different approaches to multibiometrics [24]: multi-sensor, multi-modal, multi-instance, multi-sample, multi-algorithm, hybrid. From the security point of view, the best of above-described options is the application of multimodal 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.

In case of fingerprints, the additional biometric characteristic could be the finger veins, because it is difficult to obtain the vein pattern, and the finger vein sensor could be quite easily integrated in the optical fingerprint sensor, which reduces the price of final solution and time-consumption of the capturing.

In 2008, the pre-prototype of finger veins sensor (see Fig. 3 a) was created. The algorithm used in the pre-prototype consists of several phases: pre-processing (Median and Smooth filter), edge detection (convolution with special kernel), thresholding (binarization), post-processing (Median filter), thinning, and final post-processing (see Fig. 3 c). Separately the finger contour is detected and it is used as a filter to remove the artifacts outside of the finger area. The preliminary template consisted 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. The results look promising and this solution was registered as the Czech utility model No. 21548 [11], incrementally published, 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" [7] and this sensor became the first multi-modal sensor in the market.

2.5 Brute force attack

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 [29].

At first sight, this method (templates generating and waiting for results) 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 [29], e.g., fingerprint usually takes the oval area in the middle of the image, and the minutiae positions have usually a uniform distribution. Moreover, it is possible to improve this attack by using of so called Hill-climbing algorithm [3, 29]. Initially, 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 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 project [41] 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. 4). 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 algo-

Figure 3: Example of finger vein detection: a) pre-prototype of finger vein sensor, b) captured vein image, and c) captured vein image with extracted vein skeleton.
3. Liveness detection

Nowadays, the easiest way to successfully attack a biometric system is to attack (spoof) the sensor. Although, there are other possible precautions (e.g., cancelable/removable biometrics or multi-modal biometrics) the implementation of liveness/fake finger detection plays a crucial role in the sensor securing.

3.1 Analysis

After careful study of known methods and their problems, 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 based on the requirements for biometric characteristic: universality, distinctiveness, permanence, collectability, performance, acceptability, and security. Most of them is could be defined in the same way as in case of requirements for biometric characteristic. For example, distinctiveness does not mean to differentiate between individuals, but to differentiate among classes (e.g., live fingers, gelatin fake fingers), i.e., the property with a wide range of accepted values (e.g., temperature) cannot be used for liveness detection purposes.

According to 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.

The second group of requirements results from integration of this method into some fingerprint sensor [25]. It is necessary to measure the liveness of the same area at the same time as measuring of biometric characteristic. In case of testing of some process, 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. 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. Due to the usage of two concurrent measurements, it is also necessary to use such pair of sensor technology and liveness detection 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, or 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.

3.2 Principle of novel liveness detection approach

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. 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 turns to yellowish/whitish (see Fig. 5). 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. The rate of change is proportional to the force of finger pressing.

The color of finger can be detected using various color models. 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. On the other hand, the results 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* (axis from green to magenta) is significantly decreased and b* chromatic value (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, which I consider inappropriate.

The results of RGB color model are more definite and proper. The differences between average R values is 11, G 42 and B 20.

The 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 place 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 check 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 Section 4).

3. Liveness detection

Nowadays, the easiest way to successfully attack a biometric system is to attack (spoof) the sensor. Although, there are other possible precautions (e.g., cancelable/removable biometrics or multi-modal biometrics) the implementation of liveness/fake finger detection plays a crucial role in the sensor securing.

3.1 Analysis

After careful study of known methods and their problems, 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 based on the requirements for biometric characteristic: universality, distinctiveness, permanence, collectability, performance, acceptability, and security. Most of them is could be defined in the same way as in case of requirements for biometric characteristic. For example, distinctiveness does not mean to differentiate between individuals, but to differentiate among classes (e.g., live fingers, gelatin fake fingers), i.e., the property with a wide range of accepted values (e.g., temperature) cannot be used for liveness detection purposes.

According to 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.

The second group of requirements results from integration of this method into some fingerprint sensor [25]. It is necessary to measure the liveness of the same area at the same time as measuring of biometric characteristic. In case of testing of some process, 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. 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. Due to the usage of two concurrent measurements, it is also necessary to use such pair of sensor technology and liveness detection 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, or 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.

3.2 Principle of novel liveness detection approach

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. 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 turns to yellowish/whitish (see Fig. 5). 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. The rate of change is proportional to the force of finger pressing.

3.2 Principle of novel liveness detection approach

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. 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 turns to yellowish/whitish (see Fig. 5). 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. The rate of change is proportional to the force of finger pressing.

The color of finger can be detected using various color models. 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. On the other hand, the results 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* (axis from green to magenta) is significantly decreased and b* chromatic value (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, which I consider inappropriate.

The results of RGB color model are more definite and proper. The differences between average R values is 11, G 42 and B 20.

The color of finger can be detected using various color models. 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. On the other hand, the results 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* (axis from green to magenta) is significantly decreased and b* chromatic value (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, which I consider inappropriate.

The results of RGB color model are more definite and proper. The differences between average R values is 11, G 42 and B 20.
non-pressed finger, where \( X \) is particular component in RGB color model.

According to my opinion, the choice of appropriate method for detection of width of papillary lines 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 3.1, the successful liveness detection mechanism should meet a lot of requirements. The requirement for concurrent measuring of the same area without interaction is met in the basis of the method proposal. 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, collectability, distinctiveness, and performance requirements. Nevertheless, I decide to verify these assumptions (at least partly) during the preliminary tests.

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. On the other hand, 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 parameters of elasticity similar to the live human skin. In principle, there are four well-known or theoretical ways of attack:

**Exchange two fake fingers.** The possible way to pretend the color change (and the change of elasticity) is to exchange two fake fingers, each of different color (and different width of papillary lines). I have tested exchange of two samples using the Nikon camera (30 fps) and the speed of exchange was only 0.07 sec [25]. Nevertheless, this situation cannot spoof the proposed liveness detection unit, if the continuous monitoring of the color change and the camera with high frame rate will be used.

**Usage of material with appropriate elasticity parameters.** 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 force 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.

**Usage of semi-transparent fake finger.** The creation and usage of functional fake finger of this type 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 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 semi-transparent) materials often contain significant amount of bubbles.

**Usage of dead/removed finger.** Rutty et al. [34] 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) [22, 38]. According to the study of Dr. Şäfer [38], the paleness of skin develops rapidly and it can be easily optically distinguished from the common live skin color. The following post-mortem change of skin color is turning dark purple (livor mortis) [22]. 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.

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, 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.

### 3.3 Hardware configuration

According to the previously described requirements and the software principle of new method, the hardware schema of the possible liveness detection unit was proposed. 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 [9], green light [14] or side illumination of finger [48]), the common white LED diodes or other ordinary light sources in various locations should be sufficient.

Our solution is patented (Czech utility model No. 19364 [27]) and there are basically two possible approaches to the hardware implementation. The first approach uses two different camera modules. The first camera module
3.4 Preliminary tests

I have conducted three consecutive preliminary tests. The first preliminary test was the proof-of-concept test for checking of the basic idea of this approach by the use of minimal hardware equipment. 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 (pressed and non-pressed images per each finger and session). Due to the high resolution (1200 × 1200 dpi) the capturing of one fingerprint takes approximately half a minute, which was very uncomfortable for the volunteers.

The colors (and the color change) of papillary lines in case of different volunteers appear to be sufficiently similar, see Fig. 8. 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 were determined using median, the papillary lines were visualized using Sobel operator and determined manually. The ranges of RGB components for non-pressed (R: 225-240, G: 155-175, B: 150-165) and pressed (R: 235-255, G: 200-220, B: 150-165) finger and the range of change of width of papillary lines (10 to 40%) were determined experimentally.

Nevertheless, the particular values of detected changes depend on the pressure force and also on the precision of the manual determining of papillary line width. 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.

The second preliminary test was performed on the large group of people to test mainly acceptability of this principle and functionality of the newly built pre-prototype and partly even security.

This test was conducted in winter semesters 2009/10 and 2010/11. The capture subjects were 320 students (304 men and 16 women). The optical bench was equipped with Sony XCD-SX910CR color camera, Computar MLH-10X macro zoom lens and my special robust end-piece, 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 altered by students.

Results of tests of acceptability requirements were excellent. 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.

The third preliminary test was focused on the possible improvements of pre-prototype and the basic overview of possible algorithms for automatic papillary line width detection. At first, it 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 [6] color camera module.

Ing. Homola (in his Master thesis under my supervision [13]) 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. He also tested and compared a large number of algorithms and 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 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.

3.5 Algorithm
The selection of appropriate algorithms and its parameters for the above described hardware configuration (see Section 3.3) 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:

Image capturing. The sequence of 75 BMP images was captured in every session (approx. 12 frames per second, i.e., one session takes approx. 6.25 s). The captured images are in the Bayer BG 8 file format [6]. It means that every pixel in each quadruple of neighboring 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 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). 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. In Fig. 9, the mean RGB values of 100px (in line) in the center of each image are shown during the slow pressing of finger. At first, the finger is approaching to the glass plate. Then the finger is close enough to not be so blurred and there are reflections of the light on the papillary ridges (see Fig. 9 a). Nevertheless, not all of the papillary lines are visible (and only few of them are focused) due to rounded shape of the finger.

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. Finally, the mean RGB colors of a new pixel are computed as the mean of both G values in the corresponding quadruple.

In the next phase (approx. from 39 to 47), the center of finger slightly touches the glass. In the area of slight touch (the center of image), the reflection of light is not visible, so the mean values of RGB colors decreased. The detection of this local minimum is used as the method to determine correct image of non-pressed finger.

The last phase is the pressing of finger against glass plate. 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. Finally, the image number 74 is considered to be an image of pressed 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: 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 for non-pressed and pressed fingers and computes their difference.
Optical merging. This step merges two black and white images (image of non-pressed finger and image of pressed finger) are converted into grayscale color range. Then the Gaussian adaptive threshold \( T = 128 \) for blocks \( 85 \times 85 \) is applied. Subsequently the Gaussian smooth filter (kernel \( 3 \times 3 \)) and threshold \( T = 128 \) are applied. The result of this phase could be seen in Fig. 10

Application of image filters. At first, both images (image of non-pressed finger and image of pressed finger) are converted into grayscale color range. Then the Gaussian adaptive threshold \( T = 128 \) for blocks \( 85 \times 85 \) is applied. The used image has been excluded after capturing due to the higher amount of textile fibers, which could influence the results.

Finding of maximal overlap. In an ideal case (absence of noise), the overlapping is indicated by an absence of red pixels and high amount of black pixels (surrounded by green pixels in case of live finger – see Fig. 11 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. 11 b) and absence of black pixels (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.

Measuring of change of papillary line width. The papillary line borders (in the used magnification) contain a lot of irregularities, e.g., small bays or protrusions. In case of very strong pressure of the finger, the values 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. Moreover, the shape of some minutia (e.g., minutia called "point") 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 particular papillary line.

These situations have been taken into account. Firstly, the algorithm tries to find a starting white pixel 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. Secondly, the algorithm does not try to find the nearest black pixel and then the second black pixel in the opposite direction, but it tries to find two opposing black pixels in 8 different directions. The shortest width is considered to be correct. This approach minimizes the problem with dashed papillary valleys caused by strong pressure of finger against glass. Using this procedure, 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 of pressed and non-pressed finger and width (four times) of papillary lines. 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 decided to slightly reduce the requirements given in Eq. 1 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.

According to the change of width, at least three of four width pairs (width of papillary line in pressed and non-pressed state) 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 minimal 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.

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.

3.6 Database

For the purposes of final tests, 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. 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. 12 (age from 20 to 68 years, average 29 years). The database also contain fingerprints in situa-
tions, which affect/may affect fingerprint color, elasticity or quality, i.e., diseases (e.g., atopic eczema, anemia, low blood pressure), manual work or hobby (e.g., judo, contrabass or hard work in the garden).

Due to usage of necessary protective housing and resulting lower user-friendliness (the difficult access to the glass plate) together with the nervousness of tested subjects, some images before and after pressing of finger against the glass were not corresponding. 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.

The fake fingers were made using the wax mold with assistance of user. 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). Some of the 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 fake finger attached to the live finger, which is different than the live finger, which was the model.

3.7 Final tests

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, but most of their papillary lines were easily distinguishable, so they also met this requirement.

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 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.

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. 13). The captured samples of these fake fingers contain a large amount of tiny bubbles. This problem was reported, e.g., by Wei-Yun [48]. I have created many samples of gelatin and gummy-bear fake fingers (several attempts per various colors and manufacturers) to choose the best (and the bubble-free) ones. All of them contain bubbles, so I chose the material (producer), which reached best results in the past. Unfortunately, the presence of amount of tiny bubbles and the characteristic properties of material caused that the papillary lines were not distinguishable.

Figure 12: Age distribution and gender of volunteers in the final test of my liveness detection approach.

Due to usage of necessary protective housing and resulting lower user-friendliness (the difficult access to the glass plate) together with the nervousness of tested subjects, some images before and after pressing of finger against the glass were not corresponding. 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.

The fake fingers were made using the wax mold with assistance of user. 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). Some of the 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 fake finger attached to the live finger, which is different than the live finger, which was the model.

3.7 Final tests

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, but most of their papillary lines were easily distinguishable, so they also met this requirement.

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 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.

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. 13). The captured samples of these fake fingers contain a large amount of tiny bubbles. This problem was reported, e.g., by Wei-Yun [48]. I have created many samples of gelatin and gummy-bear fake fingers (several attempts per various colors and manufacturers) to choose the best (and the bubble-free) ones. All of them contain bubbles, so I chose the material (producer), which reached best results in the past. Unfortunately, the presence of amount of tiny bubbles and the characteristic properties of material caused that the papillary lines were not distinguishable.

Figure 12: Age distribution and gender of volunteers in the final test of my liveness detection approach.

Due to usage of necessary protective housing and resulting lower user-friendliness (the difficult access to the glass plate) together with the nervousness of tested subjects, some images before and after pressing of finger against the glass were not corresponding. 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.

The fake fingers were made using the wax mold with assistance of user. 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). Some of the 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 fake finger attached to the live finger, which is different than the live finger, which was the model.

3.7 Final tests

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, but most of their papillary lines were easily distinguishable, so they also met this requirement.

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 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.

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. 13). The captured samples of these fake fingers contain a large amount of tiny bubbles. This problem was reported, e.g., by Wei-Yun [48]. I have created many samples of gelatin and gummy-bear fake fingers (several attempts per various colors and manufacturers) to choose the best (and the bubble-free) ones. All of them contain bubbles, so I chose the material (producer), which reached best results in the past. Unfortunately, the presence of amount of tiny bubbles and the characteristic properties of material caused that the papillary lines were not distinguishable.

Figure 13: The a) fake finger made of orange gummy bear b) captured using by Suprema SFM3050-TC1. c) The corresponding live finger captured by the Suprema SFM3050-TC1.

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). 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 were highlighted by combination of magnification and illumination (and used sequence of image filters).

All live sample series contain the correct color change and none of the tested fake fingers succeeded. (In case of usage of tighter conditions used in tests on scanner, there is FRR 10% and FAR 0%.) The graph of color changes of live and fake fingers (see Fig. 14) shows that the direction of color change of live finger samples is in accordance with the presented equation. Nevertheless, the consequences of the illumination instability are visible: both groups of live and fake fingers (see Fig. 14) shows that the direction of color change of live finger samples is in accordance with the presented equation. Nevertheless, the consequences of the illumination instability are visible: both groups of live and fake fingers (see Fig. 14) shows that the direction of color change of live finger samples is in accordance with

Figure 13: The a) fake finger made of orange gummy bear b) captured using by Suprema SFM3050-TC1. c) The corresponding live finger captured by the Suprema SFM3050-TC1.

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). 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 were highlighted by combination of magnification and illumination (and used sequence of image filters).

All live sample series contain the correct color change and none of the tested fake fingers succeeded. (In case of usage of tighter conditions used in tests on scanner, there is FRR 10% and FAR 0%.) The graph of color changes of live and fake fingers (see Fig. 14) shows that the direction of color change of live finger samples is in accordance with the presented equation. Nevertheless, the consequences of the illumination instability are visible: both groups of live and fake fingers (see Fig. 14) shows that the direction of color change of live finger samples is in accordance with
color change. Another material (non-transparent JaLatex) shows the small color change, which looks alright at first glance (see Fig. 14), but it has the opposite direction. This could be caused probably by higher amount of reflections of light in image of non-pressed sample. In case of remaining four semi-transparent materials, 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 one.

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 percentage points in case of fake finger samples, but about a few tens percentage 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 live finger samples were classified as originating from the live human fingers (contained at least three correct width changes of four). The boxplot of correct widths of non-pressed/pressed papillary lines of men (mean 26.7/34.9 px) and women (mean 24.2/32.1 px) can be found in Fig. 15. The mean value of change is 24.9%. The outliers (in Fig. 15) are also 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 (in case of usage of tighter conditions used in tests on scanner, there is FRR 11.6%).

As it was mentioned earlier, three materials (special compound, gelatin and gummy bear) had to be excluded due to the impossibility to detect papillary lines and only fake fingers made of seven materials were 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 unable to find non-pressed sample. 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, the material was pressure resistant as it was expected. 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 (from the spoofing point of view). 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.

The last material (JaLatex transparent) was also unsuccessful, but the image analysis showed one interesting result. As you can see in Fig. 16, this material was transparent enough to cause an interference of papillary lines on fake finger and on live finger behind. Nevertheless, this material was not transparent enough for the sufficient amount of light and thus does not 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

\[ \text{The outliers are defined as values lower than } Q_1 - 1.5 \times (Q_3 - Q_1) \text{ or higher than } Q_3 + 1.5 \times (Q_3 - Q_1) \, [49]. \]
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 behavior of captured subject.

4. Semantic conformance testing
As it is mentioned earlier (see Section 2.5), the development of semantic conformance testing is a consequence of results of MINEX [41] and similar projects, which have confirmed that some automatic minutiae extractors have not followed the intentions of the ISO/IEC 19794-2:2005 standard [18] and have placed the minutiae in some kind of grid instead of placing them at the faithful location. 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 [19]. The first two levels (syntactic tests) were quite easily created and implemented, 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).

4.1 Analysis
This analysis was based on my experience with the fingerprint minutiae extraction algorithms and the results of proof-of-concept tests conducted on images from my private fingerprint database (e.g., fingerprint with skin diseases, scars, or dirt) and several images from the NIST SD14\textsuperscript{5} database [45]. The results of tests confirmed that there are basically three different types of problems:

- **Minutiae outside the appropriate area.** The minutia outside of the fingerprint area or at the border (see Fig. 17 a) occurred very frequently. The reason of this failure can be problems with foreground/background masking caused by noise, dirt, drawing or written characters in the background of an image or some specific problems of a particular algorithm.

- **Imprecisely placed minutiae.** According to the description of minutiae data given in the ISO/IEC 19794-2:2005 standard [18], 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, e.g., if the minutia type is wrongly determined, then there is a strong likelihood that the position of minutia will be imprecise too (see Fig. 17 b).

- Three 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.

- **Problematic areas.** These areas are created by specialties distorting the standard flow of papillary lines in image. These distortions can interrupt the regular ridge flow, e.g., by bended skin, scar, or dry finger (where the papillary lines may appear as the series of papillary dots) and create fake ridge endings. Moreover, the wet fingers or the very hard pressing of finger against the sensor surface cause, that the papillary lines may optically join and create fake ridge bifurcations.

In more complicated cases, the affected part of the fingerprint can contain the completely new (fake) ridge pattern (see Fig. 17 c). This situation may occur mostly in case of some skin diseases. The correct minutiae detection in such areas is very difficult. Even the human dactyloscopic/fingerprint experts can have problems because it cannot be easily determined whether the ridge ending or bifurcation is caused by a disease or it is natural.

The problematic areas 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.

4.2 Ground Truth Database
For the purposes of computation of semantic conformance rates, it is essential to have the reference set (so called the Ground Truth Minutiae, GTMs) based on a large scale and carefully selected database of fingerprint evaluated by the independent institution. It is not possible to choose one (or more) vendor(s)/fingerprint extraction algorithm(s) to generate ground truth minutiae, because it would create monopoly on the market and disadvantage the other vendors/algorithms. The ground truth

\begin{figure}[h]
\centering
\includegraphics[width=\textwidth]{figure16.png}
\caption{Example crossing of papillary lines of live and fake finger: a) captured image, b) image processed by series of image filters.}
\end{figure}

\begin{figure}[h]
\centering
\includegraphics[width=\textwidth]{figure17.png}
\caption{a) Minutiae detected at the border of the fingerprint area. b) The ridge bifurcation detected as the ridge ending. c) Fake minutiae found in the area of wart. The ridge endings are drawn as squares and ridge bifurcations are drawn as crosses.}
\end{figure}

\textsuperscript{5}National Institute of Standards and Technology, Special Database 14.
minutiae also could not be set by an inexperienced person/institution, so the only one solution was to ask 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.

For this purposes, the Ground Truth Database (GTD) has been created. The images came from the NIST SD14 [45] and SD29 [46] fingerprint databases (i.e., GTD-SD14 and GTD-SD29) and they were carefully selected by Ms. Elham Tabassi (NIST) to represent the variability of fingers, fingerprint types, quality (NFIQ, i.e., NIST Fingerprint Image Quality [47]), position and consist of the approximately same amount of male and female fingerprints.

For the purpose of collection of minutiae set by experts, I have prepared the program “GUI for dactyloscopy” (see Fig. 18). The GUI can load fingerprints in BMP or WSQ file formats. It supports the setting of fingerprint type, quality and completeness and inserting minutiae, cores and deltas. It is possible to zoom in/out fingerprint in the interval from 10 % to 500% and select each of the inserted objects to see its properties. It is also possible to remove or add one angle of delta but delta can have only two or three angles in total and the missing angle value is filled by one of the rest values (according to the ISO/IEC 19794-2:2005 [18]).

Although, the used colors (neon green for selected minutiae, cyan for non-selected minutiae, neon yellow for selected core/delta, and red for non-selected cores/deltas) 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. Moreover, the setting of the quality was restricted to the five possibilities: excellent (90), very good (70), good (50), fair (30), poor (10), and value "not set" (0) to reduce the time-consumption.

The resultant minutiae, core and delta record is stored in the *.gtm file format. 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 [18], but they are placed so, that it is easy to apply batch processing and the result is easily human-readable in a common text editor.

For the purposes of international cooperation, the harmonized dactyloscopic specification/knowledge base was created (by Ms. Bernhardt from German Federal Criminal Office). This document has been reviewed by various dactyloscopic experts and academic researchers. This dictionary was also enhanced after the analysis of the preliminary tests.

### 4.3 Conformance rates

I have proposed three conformance rates. 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 (Ground Truth Minutiae) set and AGM (Automatically Generated Minutiae) set.

The first conformance rate is marked as \(c_{gtm}\) and indicates the preciseness of placement and assessment of parameters of AGMs according to the GTMs. 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 the tolerated distance \(tol_d\), the minutia is further processed, otherwise it is rejected and the algorithm considers this AGM as missing:

\[
c_{gtm} = \frac{n_{gtm}}{n_{agm}}
\]

\[
m_{c_{gtm}} = \begin{cases} 
0 & \text{if } d \leq tol_d \\
1 - p & \text{otherwise}
\end{cases}
\]

\[
tol_d = \frac{W}{4}
\]

where \(n_{gtm}\) is the number of GTMs, \(d\) is the Euclidean distance 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 \(m_{cs}\) 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:

\[
p = p_{\Delta \theta} + p_{\Delta \tau}
\]

\[
p_{\Delta \theta} = \frac{|\theta_{gtm} - \theta_{agm}| \times 0.5}{\pi}
\]

\[
p_{\Delta \tau} = \begin{cases} 
0.25 & \text{if } t_{gtm} \neq t_{agm} \\
0 & \text{otherwise}
\end{cases}
\]

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

The different maximal value of punishment for different deficiencies (see Equations 6 and 7) 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.

The second conformance rate $cr_{agm}$ describes the proportion of false minutiae placed outside or at the border of fingerprint area. It expresses 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, but the false minutiae outside the fingerprint area can point to a more severe problem:

$$cr_{agm} = \frac{\sum_{i} mps_i}{n_{agm}}$$  \hspace{1cm} (8)

$$mps_i = \begin{cases} 
0 & \text{if } agm \text{ is outside the fingerprint area} \\
0.5 & \text{if } agm \text{ is at the borderline} \\
1 & \text{otherwise}
\end{cases}$$  \hspace{1cm} (9)

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

The third conformance rate $cr_{amf}$ gives us an overview, how many unpaired AGMs are inside the fingerprint area. It is a 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.

$$cr_{amf} = 1 - \frac{n_{iaagm}}{n_{agm}}$$  \hspace{1cm} (10)

where $n_{iaagm}$ 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.

The workflow of computation of these conformance rates is as follows. The input data is the image containing fingerprint and data collected from experts in *.gtm file format. The image is processed by tested automatic minutiae extractor and the generated set of minutia (AGMs) is converted and saved also in the *.gtm file format. The fingerprint image is also an input to the fingerprint area extraction algorithm (see Section 4.4).

For the purposes of computation of first and second conformance rate and clustering of data from experts, it is necessary to know the space between two thinned parallel papillary lines (labeled as $W$). 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. The measured values were so similar, that we decided to set (to round) the value of papillary line width as a constant value $W = 12\, \text{px} \Rightarrow W/4 = 3\, \text{px}$.

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.

4.4 Fingerprint area detection

The fingerprint area detection pipeline was designed by Mr. Doležel under my leadership and in my cooperation [10]. The final pipeline consists of 6 phases:

1. Fingerprint pre-processing. 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]. Nevertheless, our approach contains several improvements to achieve smoother and more precise fingerprint segmentation, e.g., usage of smaller blocks (6 × 6 px), maximal overlapping (5px) in both directions, and computation of average magnitude Gabor features for every pixel.

3. Erosion. The segmented area is slightly larger than the original fingerprint, so the omnidirectional morphological erosion $12 \times 6px$ is used.

4. Artifacts removal. It is necessary to remove artifacts (e.g., 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 [12] 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.

5. Removal of holes and insignificant areas. The image may contain several holes inside the fingerprint area and also several insignificant areas/noise identified as small foreground areas. At first all white areas (background areas) are identified and their size in pixels is computed. Then the largest area(s) is (are) marked as background and other areas are filled with black color. The removal of insignificant foreground areas is done similarly.

6. Fingerprint border detection. At the end, a gray line is drawn around the detected fingerprint area. 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. 19 c).

Although our fingerprint area extraction pipeline of algorithms proved to be much better than the competing algorithms (see Fig. 19), we decided to use manually extracted fingerprint areas to increase preciseness.
4.5 Clustering of data from experts

The creation of GTMs consists of three phases. 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 non-trivial task, because the number of clusters is not known. To solve this problem, an approach inspired by the Apriori algorithm [49] and general principle of hierarchical clustering [49] is used. 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 $W/4$).\(^7\)

The clustering procedure is based on creation of the auxiliary sets of $n$-set. 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.

\[
A_1 = \left\{ a \mid a \subseteq \bigcup_{u=1}^{n_{exp}} T_u, |a| = 1 \right\}
\]

\[
A_2 = \left\{ a \mid a \subseteq \bigcup_{u=1}^{n_{exp}} T_u, |a| = 2, \forall r \in \{1, 2, 3, \ldots, n_{exp}\} : a \not\subseteq T_r, d(a) \leq \frac{W}{2} \right\}
\]

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

The other auxiliary sets are constructed in the same way (see Equation 14). 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.

\[
\forall i \in \{1, \ldots, n_{exp}\} : \\
A_i = \left\{ a \mid a \subseteq \bigcup_{u=1}^{n_{exp}} T_u, |a| = i, \left( \begin{array}{c} a \\ i-1 \end{array} \right) \subseteq A_{i-1} \right\}
\]

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:

\[
C = \{ c \mid c \in A_r, \forall b \in A_{r+1} : c \not\subseteq b \} \cup A_{n_{exp}}
\]

The implementation of the clustering algorithm described in Equations 11–15 is adjusted to achieve higher robustness and speed. 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 $n = 11$, there is eleven possible combinations of the elements from 11-set in 10-set). 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 determination of the cluster center and its characteristic (position, type, angle and quality) is a non-trivial task. Firstly, the position of cluster center is computed as the average value of $x$-coordinates (and the $y$-coordinates) of all minutiae in this cluster.

Secondly, it is needed to determine the type of the cluster center. The determination is based on the ISO directives [21]: 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. In case of computation of $cr_{gt}$, conformance rate, the punishment for wrong minutia type is not applied.

Then it is necessary to compute the angle of cluster center, which is a non-trivial task. Let’s assume that there are two different angles $\theta_1 = 0^\circ$ and $\theta_1 = 180^\circ$, or three angles $\theta_1 = 0^\circ$, $\theta_2 = 120^\circ$ and $\theta_3 = 240^\circ$. It follows that it
is not possible to use the common average. Moreover, the computation of the angle has to be robust and has to allow to determine, whether the consensus (in accordance with ISO directives [21], i.e., 2/3 majority) 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 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:

\[
\begin{align*}
x_\theta &= \frac{\sum_{u=1}^{n_cl} \cos \theta_u}{n_{cl}}, \\
y_\theta &= \frac{\sum_{u=1}^{n_cl} \sin \theta_u}{n_{cl}} \tag{16}
\end{align*}
\]

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

3. The coordinates \((x_\theta, y_\theta)\) can be imagined as the end-point 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.

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 \(\theta_1 = 0^\circ, \theta_2 = 180^\circ, \theta_3 = 0^\circ\). 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.

The computation of the quality of cluster is the final phase of GTMs creation. 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):

\[
q_{cl} = \frac{\sum_{u=1}^{n_cl} q_u}{n_{exp}} \tag{17}
\]

where \(q_u\) is the quality of cluster and \(q_u\) is the quality of the \(u\)-th minutia in this cluster.

The influence of determination of cluster quality threshold is illustrated in Fig. 20. It can be seen that the minutiae in the bottom-right corner of the image create a nice cluster with the almost perfect consensus (7 of 8 contributing experts, \(q_{cl} = 64\)). In the upper-left corner of image, there are two minutiae of "other" type (\(q_{cl} = 6\) in both cases). After the clustering, there are three cluster centers, because two minutiae located in the upper-left image corner were too distant from each other to create one minutia cluster. The application of the quality of cluster threshold \((T = 37)\) removes the upper two cluster centers with the insufficient quality and only the cluster center in the bottom-right image corner is considered to be a ground-truth-minutia.

The detailed influence of application of the cluster quality threshold can be seen in Fig. 21 (the data used for this test is described in Section 4.2). 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.

4.6 Final tests

The database for tests consists of 733 fingerprints (486 images from GTD-SD14 and 247 images from GTD-SD29). Every image was evaluated by three dactyloscopic experts. Using this dataset, three different minutiae extraction algorithms were tested: mindtct from NIST NBIS (NIST Biometric Image Software) package (Rel 1.1.0)\(^8\), Innovatrics ANSI and ISO SDK v 1.52\(^{17}\) [15], VeriFinger 6.1 SDK from NeuroTechnology\(^7\) [31]. In many cases, the results computed for GTD-SD14 and GTD-SD29 are so different that it was necessary to display the results separately.

\(^8\)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.
The graph in Fig. 22 shows the results of first semantic conformance rate $c_{r_{gtm}}$, for all used algorithms on GTD-SD14 database depending on threshold of quality of cluster. 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 (inconsistency of experts opinion - minutiae form separate clusters) are included. This situation increases the number of ground truth minutiae and thus decreases the $c_{r_{gtm}}$. The maximum value of $c_{r_{gtm}}$ 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. 21).

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. 23. It can be seen the almost constant value of the second conformance rate $c_{r_{agm}}$. 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 9). 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 third conformance rate $c_{r_{amf}}$ is slowly decreasing during the increase of the threshold of cluster quality (see Fig. 23) 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 10).

The short summary of results can be found in Table 1. In case of first conformance rate $c_{r_{gtm}}$, the NIST algorithm achieves much better results than the others. The results of other two algorithms are balanced, and the difference is almost negligible.

The results for second conformance rate $c_{r_{agm}}$ are more surprising. In case of GTD-SD14 dataset, 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 Innovatics 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.

In case of the third conformance rate $c_{r_{amf}}$, the results of all three algorithms on both parts of dataset are very similar except one. The value of conformance rate $c_{r_{amf}}$ 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 part of test - it extracts the minimal number of "false minutiae" in proportion to the number of all extracted minutiae.

5. Conclusion and future work

These objectives were met and I have presented two new securing of biometric systems. My first contribution is within liveness detection. I created a novel method for the liveness detection, which can be integrated into a common optical fingerprint sensor. This method was patented (Czech utility model No. 19364), widely tested (374 volunteers and a lot of fake fingers made of various materials), and it shows better results than others. 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).

There are also possibilities for the future research. The first possibility could be the creation of an algorithm, which will be capable correctly deform papillary lines to reduce the unwanted effect of finger elasticity and enable the measuring of papillary lines in all image areas. 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., 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).

The second contribution is within standardization. I analyzed the common problems of minutiae extraction algorithms and subsequently I proposed and tested method-
ology to determine semantic conformance rates of minutiae extractors to increase security and interoperability of minutiae extraction and comparison process. 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.

This semantic conformance testing methodology was created as a contribution in response to the ISO/IEC SC37 N3058 [17] (Call for Contributions on Metric for Measuring Accuracy of Minutiae Placement). My contribution was accepted well and I am working as a co-editor since January 2010. Nowadays (May 2012), these equations are included into ISO/IEC 29109-2 [20] Amd. 2, which is in the preparatory stage as Fourth Working Draft and there is still much work to do before it will be published.

In this extended abstract, I have also shortly presented my other smaller contributions, i.e., the patented unit for the finger vein detection (Czech utility model No. 21548), which was intended to use separately or integrated into a common optical fingerprint sensor.

All these topics were incrementally published, cited several times and my work on semantic conformance testing is followed by Mr. Abt in his research [1, 2].

Acknowledgements. This work was partially supported by the grants “Information Technology in Biomedical Engineering”, GA102/09/H083 and “Education of liveness testing in subject Biometric systems”, FR2525/2009/G1, the research plan “Security-Oriented Research in Information Technology”, MSM0021630528, and the “IT4Innovations Centre of Excellence”, ED1.1.00/02.0070.

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 the finger vein detection (Czech utility model No. 21548), which was intended to use separately or integrated into a common optical fingerprint sensor.

All these topics were incrementally published, cited several times and my work on semantic conformance testing is followed by Mr. Abt in his research [1, 2].

References


Table 1: The results of tests of semantic conformance testing methodology for miniature from NIST, SDK from Innovatrics and Verifinger from NeuroTechnology. The threshold of cluster quality is marked as T.

<table>
<thead>
<tr>
<th>Vendor</th>
<th>DB</th>
<th>T</th>
<th>(c_{Tgm} )</th>
<th>(c_{Tgm} )</th>
<th>(c_{Tgm} )</th>
<th>(\eta_{Tgm} )</th>
<th>(\eta_{Tgm} )</th>
</tr>
</thead>
<tbody>
<tr>
<td>NIST</td>
<td>14</td>
<td>60</td>
<td>0.514 (0.130)</td>
<td>0.857 (0.063)</td>
<td>0.286 (0.112)</td>
<td>41 (22)</td>
<td>202 (49)</td>
</tr>
<tr>
<td>INN</td>
<td>14</td>
<td>60</td>
<td>0.316 (0.106)</td>
<td>0.876 (0.078)</td>
<td>0.231 (0.095)</td>
<td>41 (22)</td>
<td>160 (39)</td>
</tr>
<tr>
<td>NT</td>
<td>14</td>
<td>60</td>
<td>0.333 (0.133)</td>
<td>0.883 (0.103)</td>
<td>0.273 (0.119)</td>
<td>41 (22)</td>
<td>147 (36)</td>
</tr>
<tr>
<td>NIST</td>
<td>29</td>
<td>60</td>
<td>0.514 (0.156)</td>
<td>0.847 (0.085)</td>
<td>0.393 (0.150)</td>
<td>28 (16)</td>
<td>89 (32)</td>
</tr>
<tr>
<td>INN</td>
<td>29</td>
<td>60</td>
<td>0.325 (0.138)</td>
<td>0.938 (0.055)</td>
<td>0.246 (0.111)</td>
<td>28 (16)</td>
<td>64 (24)</td>
</tr>
<tr>
<td>NT</td>
<td>29</td>
<td>60</td>
<td>0.317 (0.151)</td>
<td>0.974 (0.040)</td>
<td>0.215 (0.125)</td>
<td>28 (16)</td>
<td>54 (22)</td>
</tr>
</tbody>
</table>


