HADMÉRNÖK

XI. Évfolyam 2. szám – 2016. június

György Fialka - Tibor Kovács
gyorgyfialka@gmail.com - kovacs.tibor@bgk.uni-obuda.hu

THE CORRELATION AMONG TECHNICAL PARAMETERS, CONDITIONS OF APPLICATION AND BIOMETRICAL IDENTIFICATION

Abstract

The specifications indicated by the manufacturers in manuals can be different in the practice depending on the environment. Sometimes, if we want to install a biometric system, we just buy one reader, and we make tests for about six months to make sure the device is operating as it requested. Mostly we find problems about installations. An average sized system is very costly, for that raison it is indispensable to know how its elements work in a testing environment. We examined four biometrical devices and we are publishing the test results. We hope it can help to the companies to choose the adequate device.

A gyártók által kiadott felhasználói könyvekben megadott specifikációk a gyakorlatban - alkalmazási környezettől függően – eltérők lehetnek a leírtaktól. Számos esetben, ha installálni szeretnénk egy biometrikus rendszert, beszerzünk egy eszközt, és teszteljük fél évig csak azért, hogy meggyőződjünk róla: az akként működik, ahogy azt megadták. Gyakran gondokkal szembesülünk már az installáláskor is. Egy közepes méretű rendszer nagyon költséges tud lenni, ezért aztán fontos ismerni, hogy annak elemei tesztkörnyezetben miként viselkednek. Négy konkrét biometrikus eszközt teszteltünk és publikáljuk az eredményeket. Reméljük mindez segítségére lesz a felhasználóknak abban, hogy a számukra megfelelő eszközt ki tudják választani.

Keywords: *biometrics, fingerprint, hand geometry, iris recognition, palm vein, template, enrollment ~ biometria, ujjnyomat, kézgeometria, írisz-azonosítás, tenyérérhálózat, minta, felvétel*

INTRODUCTION

The man goal of the authors is do not sell any products but to test the biometric based devices and publish the test results.

The *Table 1* shows some important biometric devices' parameters (specifications) given by the manufacturer.

How are these devices working? First users should be registrated in the device. It means that some information will be stored in the device, like username, user ID or the fingerprint or other templates. When the user identifying her/himself the device compares his/her biometric data to the stored one. If these are origins from the same person, the identification - theoretically - will be successful. The device is "able" to find individual characteristics in the biometric pattern like points, intersections, crossings, characteristics, etc. All of these individual points have a relative coordinate. After each scanning the device can found several points but in the practice these points aren't sometimes the same. If the most of the typical points are the same the identification will be successful, otherwise denied.

			FINGERPRINT IDENTIFICATION				**OTHER BIOMETRICAL IDENTIFICATION**			
							Hand-geometry	Iris	Finger vein	Palm vein
	Model[1]		**Suprema BioEntry Plus**[2]	FingerKey DX	L1-4G V-flex	Bioscrypt V-Pass	**HandKey II**	**Panasonic BM-ET330**	L1-4G	**INTUS**
PARAMETERS[3]	**FAR**[4] [%]		n/a	n/a	n/a	0.2	0.1	1/1.200.000	n/a	1/12.000
	FRR[5] [%]		n/a	n/a	n/a	1	0.1	< 1	n/a	0.01
	Max User Number (N)		5.000	250	n/a	n/a	512	1.000	n/a	Unlimited
	Extended		n/a	500 – 2.000	n/a	n/a	1.000	5.025	n/a	n/a
	Template[6] **Storage Capacity**		10.000	2 per user	10.000 in 1:N 100.000 in 1:1	100 (max 200)	as user number	as user number	10.000 in 1:N 500.000 in 1:1	Unlimited
	Identification time		2.000 match in 1s	≤ 2s	< 1s for 100 user database	< 1s	< 1s	approx. 1s	Searches 6.000 templates ps	< 1s
	Ports	Ethernet	✓	✓	✓		✓	✓	✓	✓
		RS485	✓	2x	✓	✓	✓		✓	
		RS232		✓	✓	✓	✓			
		Wiegand				✓				✓
		Other			USB			Video Camera	WLAN	Lbus

Table 1: Specifications of biometrical identification devices (data from manufacturers)

[1] http://www.thaiprintex.com/BioEntry.html
http://www.eyenetwatch.com/pdf/suprema/bioentry_plus.pdf
http://security.ingersollrand.com/Downloads/Literature/Documents/Fingerkey%20DX.pdf
www.l1id.com/files/428-L1VFlex4GDatasheet_%20032409_.pdf
http://emssa.net/source/content/L1/V-Flex/Bioscrypt%20-%20Flex.pdf
http://www.securitystoreusa.com/Honeywell-Access-NC-HG4II-HandKey-II-Standalone-Ha-p/481976.htm
http://www.panasonic.com/business/security/bm-et300_demo/iris.html
http://www.identix.com/pages/735-4g-finger-vein-reader
http://hk.search.yahoo.com/search;_ylt=Axt7wJ8Aiv5N1goAkKizygt.?p=fingervein+L1%2C+PDF&fr2=sb-top&fr=FP-tab-web-t&rd=r1
http://www.pcs.com/uploads/tx_nppcsproducts/INTUS_1600PS_presentation_P_en.pdf

[2] Models marked with bold letters are analyzed in detail

[3] Access control biometrics user guide – British security industry association, Form No.181, Issue 2, May 2010

[4] FAR: False Acceptance Rate, it shows how much non-user can enroll successfully out of 100 users

[5] FRR: False Rejection Rate, it shows how much user can not enroll successfully out of 100 users

[6] The code of the biometric pattern

Next we shortly present our experiences, tests and possible resolutions of a fingerprint, a handgeometry, an iris and a palmvein instrument.

SUPREMA BIOENTRY PLUS (FINGERPRINT IDENTIFICATION DEVICE)

According to the manufacturer data sheet the identification time is less than 1s, if the number of matches is not more than 2.000. The sensor resolution is 500 dpi and the device can store 10.000 templates (max user number is 5.000).

It can use two type of RF card: Proximity (125 kHz EM) and Mifare (13.56 MHz).

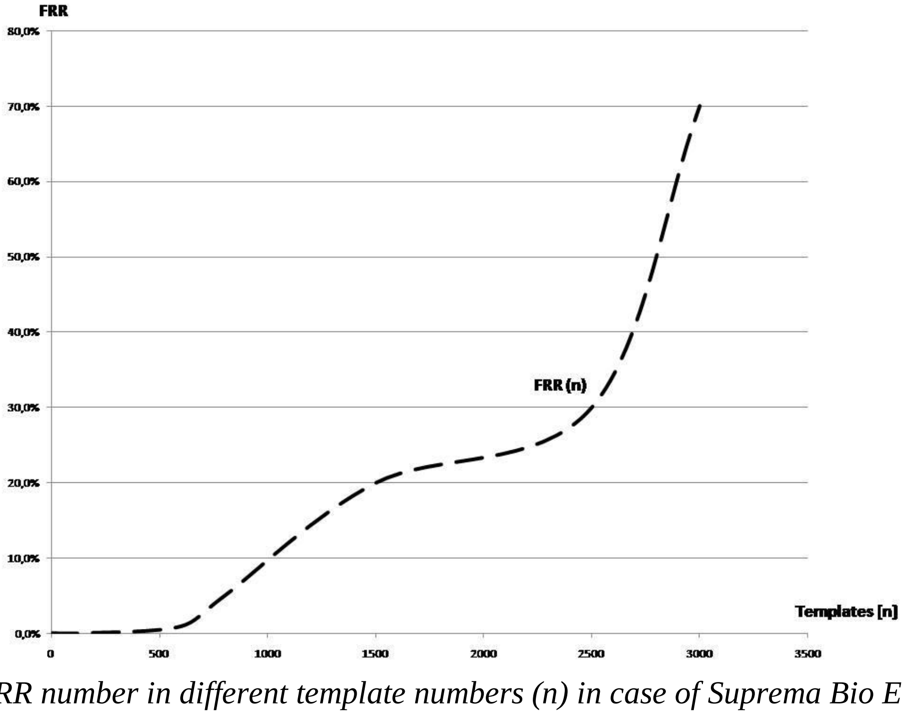
The three operation modes are Fingerprint, RF card, RF card + fingerprint.

The network interface is TCP/IP and RS485. The Wiegand output can be configurable up to 64 bits. [1]

In laboratory and when the users number was no more than 20 (approx. 150 templates) the device was fast and it had practically zero false rejection rate (FRR). The identification time was in accordance with the one given by the manufacturer.

Next we started use the instrument as a part of an access control system (the users could choose between biometric identification and well known chip-card). We registered 150-200 users a day.

When the number of the templates has been crossed 600, the false rejection rate has been appeared and started to linearly increase. Above 800 templates, the FRR was more than 5 %. Over 1.500 templates, the devices practically became useless (the FRR was over 20 %, so we had to open the entrances without any controlling of the incoming crowd). We made statistics every day and we sometimes achieved 70 % false rejection rate (see Graph 2).



Graph 2: FRR number in different template numbers (n) in case of Suprema Bio Entry Plus in a real environment (made by the authors)

The method of enrollment a fingerprint template was the following: first we recorded a template to the device (during these tests, we scanned the left middle finger). It was the reference. Later we carried 4 enrollments a day by various conditions out (the measurements were completed in different time and seasons). We immediately recognized if the scanned finger is in a different position from the original position the result was even worst.

In laboratory we found the average enrolled individual points 19.9, consequently the device operated adequately (see Fig. 3, the numbers under each small image show the quantity of congruent point comparing the original template to the captured one).

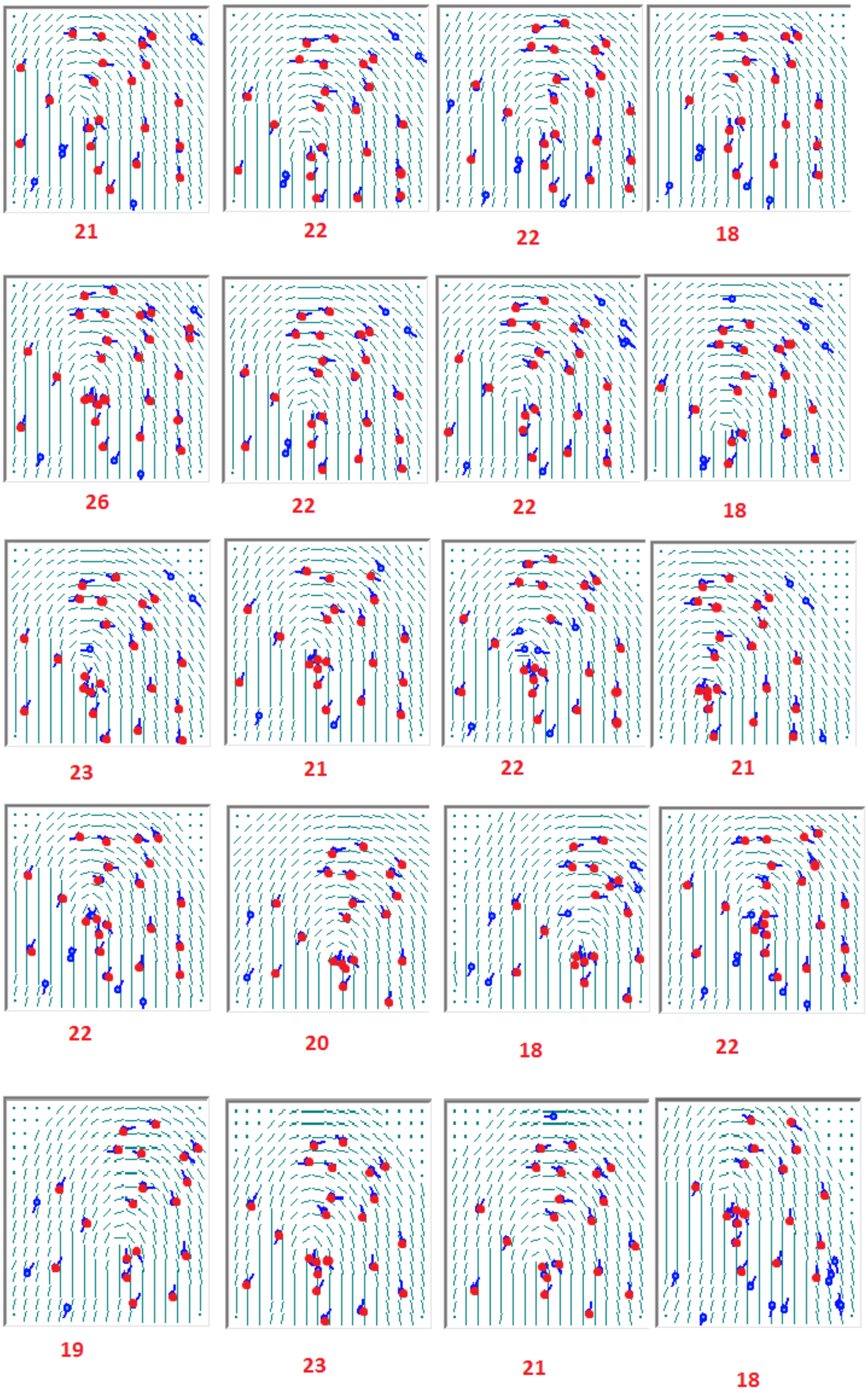


Fig. 3: Suprema BioEntry Plus test result (blue: reference points, red: enrolled points during identification; made by the authors)

HANDKEY II (HANDGEOMETRY IDENTIFICATION DEVICE)

The HandKey II is a fourth generation biometric access controller of recognition systems. The HandReader records and stores the three-dimensional shape of the hand for comparison and identity verification. Upon verification, the HandReader produces an output that can unlock a door, send card format data to an access control panel, or communicate with a host computer. The HandReader also has auxiliary inputs and outputs that can be used to control other systems such as CCTV cameras and alarms.

The device is easy to use and has the minimal identification problems. The device has positioning pins which helps to keep the fingers in the correct position. This is the main point that makes the hand geometry successful. The hand and the fingers are in the same position in each scanning, and it makes the identification process successful.

The HandReader is an intelligent access control system that can operate as a stand-alone unit, in a network with other HandReaders, or in a network with a host computer. The maximum number of users depends on the license in the device (the typical user number is 256, 512, 9.728, 27.904 or 32.512).

We tested the Handkey II in 10 different industrial places and also in laboratory environment. The maximum user number was 1.500 (Transelectro Inc., Budapest, Hungary). The tests in real environment had 6.000 users who used the devices daily.

Some details given by the manufacturer:

- Network benefits without network wiring,
- Fits seamlessly into existing,
- Audit trails,
- Access profiles,
- Time zones,
- Alarm outputs.

The following problems were revealed:

- a couple of first time user is afraid to use the device,
- extreme hand size,
- identical twins,
- artificial nails,
- spreading infections.

In details:

We found 0.3 % of the users are afraid to use the device, because it has a brand new method never seen before. So they get used to it during a relatively long period of operation time.

The extreme hand size can be a challenge for this device. We experienced that extremely big or small hand size can lead to high false rejection rate. This problem can be resolved easily as we can set reject threshold to a less secure level for these samples, so the user can enter without any problem.

In case of twins the Handkey II accepts the other twin on the default reject threshold. We set the security level higher, so the device can distinguish twin-samples (this change is necessary only for the identical twin users, for other users, the default threshold level is used).

There is a serious problem as well, when a female user has extremely long artificial nails.

We heard of new virus types in the last years. We think the users are afraid to use the devices because it has hot points to spread the infections. We installed sanitizers close to the hand geometry reader and we informed the users how to use it. Nobody practically used them. Some users tried to enroll the sample without touching the surface (it is possible in case of this device, but it causes a longer identification time).

Some of the users found this device so fantastic they used more frequently it than it was necessary. This may cause huge logs, and incomprehensible statistics: if there is a time and attendance system controlled by the Handkey II, it will be hard to get the information from the mass of data.

The Handkey II resolves the problems of high amount of user by using the 1:N method. It means, that the user types his/her user ID number on the num pad of the device before matching. The device compares whether the template belongs to the given ID number (one comparison). This method has several advantages such as short matching time and good FAR and FFR values.

People may think that typing the user number can highly increase the time of the enrollment. Our experiences show the time of typing the user ID is negligible, so it does not mean a longer enrollment process.

PANASONIC IRIS READER (IRIS IDENTIFICATION)

When both eyes are reflected in the mirror the system automatically captures the iris images and completes recognition in 1 s (or less). The quick identification process prevents waiting in line.

The device is characterized by high security with false acceptance ratio as 1 in 1.2 million.

Iris recognition uses individual differences in the complex patterns found in the iris of the human eye to authenticate individual identities and it is the most precise of all biometric identification systems. The false acceptance ratio is so low that the probability of falsely identifying one individual as another is virtually zero.

Benefits of using Iris Technology are the following:

- The iris is a thin membrane on the interior of the eyeball. Iris patterns are extremely complex.
- Patterns are individual (even in fraternal or identical twins).
- Patterns are formed by six months after birth, stable after a year. They remain the same for life.
- Imitation is practically impossible.
- Patterns are easy to capture and encode. [3]

The most significant device features are:

- Iris recognition time: approx. 1.0 s (after iris image capturing until the recognition result is output).
- Eye image capturing range: approx. 30 cm to 40 cm (between the eyes and the mirror).
- Total number of users enrolled BM-ET330: 1.000 users max.
- Iris server: 5.025 users max.
- Angular field view horizontal: 115°, Vertical: 85° (fixed, video surveillance camera).
- False rejection rate: <1%. [4]

We had 150 users to test the device and 66 persons were using it daily. Only 10% of the users found, that device is hard to use (userfriendly device) and 86% of them that the device is sophistic and they like to use it. 20% of the users are mistrustful about this technology. [5]

The most serious problem is the lack of support. We found that sometimes the iris reader becomes unable to finish the booting process. That means the booting process started after we connect the device to the power but it never stop (even after hours). We successfully resolved the problems about the iris reader, however there was no support available anywhere (we tried to contact the Panasonic several times by email and by phone, but we could not find the adequate contact person for this device).

Another problem is to take the correct position in front of the camera for the new users. Our experiences show that it took about a half minute at least during the first week. Once the users had experience in this field and time of the identification has been reduced to 1-5 s (practically the users know where the eyes should be located in front of the reader, namely eyes should be right in the opposite of the camera). The device can help to the user to get the correct position, arrows will be showed to the user which way should he/she move and the device gives verbal instructions.

We made tests in our Laboratory if the iris reader allows users to wear glasses or contact lenses. The environment was real, we tested the devices with 60 persons with different glasses and contact lenses. We found the glasses and the contact lenses will not make any negative effects in the process of identification. The users can wear these things during the identification.

People have different heights and therefore the device should be able to capture useful iris pictures for all kind of people. This device mechanically solves this problem, because there is a viewing angle of the camera that can be set easily by the user before identification.

The conclusion is easy to use this device, which can guarantee a low false acceptation rate. The first time it may be hard to found the correct position, so the time of the identification can be long at the first few weeks. When the user has a little practice by using the device, the identification is fast.

INTUS (PALM VEIN READER)

False acceptance rate is of this device no more than 0.00008%. An impressive level of security comparable to that of iris recognition is based on the highly complex vein pattern in the palm of the hand. Excellently suited for the unique identification of persons, this internal biometric feature provides optimum protection against tampering.

Palm vein authentication is based on the absorption of infrared radiation (heat radiation) in venous blood. A sensor illuminates the palm with infrared light and the oxygen-reduced blood in the veins absorbs the infrared rays. The sensor camera captures an image of the individual’s vein pattern and converts it to a template.

The template is encrypted by the sensor and then saved to a database (for identification) or to a card or tag (for verification using “template on card”). [6]

The device requires a fast computer, otherwise the system produces a relative high false rejection rate. When we ordered the device, we found the hardware looks good at the first time because it is noiseless, it has no moving parts like hard-drive or fan (with the original hardware the device was slow and it had relative high false rejection rate).

The reader must be connected to the server with USB-cable. It can cause problems, because the maximum length of the USB cable is relatively short.

In case of wet or sweaty hands, the false rejection rate is relative high.

We tried the software with a more powerful computer with success. The card reader and the num pad become unfortunately useless. To have a better FRR and faster identification have to change the computer (but the num pad and the card reader will be lose).

We was trying to change the USB cable to a longer one and convert the data format to another twisted pair connection – without any success.

Conclusion the original server computer is extremely slow for this task even in case of small amount of users. A faster computer accomplishes without any problem the mission.

CONCLUSIONS

We found the basic, general and serious problem of the biometric identification is to positioning the members (of body) to the same position where the user placed during registration. The first template should be recorded in a well-positioned anyway and all the following scanning should be perfectly in the same way positioned. Most of the devices cannot handle this problem, some of them can give signals to the user about where should he/she move to achieve better results. The best solution is that the device has a fix position we can stay in the same stable position.

Surprisingly the original server computer is slow for biometrical identification tasks. A faster computer accomplishes without any problem the mission.

References

[1] http://www.eyenetwatch.com/pdf/suprema/bioentry_plus.pdf

[2] http://www.securitystoreusa.com/Honeywell-Access-NC-HG4II-HandKey-II-Standalone-Ha-p/481976.htm

[3] http://www.panasonic.com/business/security/bm-et300_demo/iris.html

[4] http://product.yktworld.com/article/201008/201008161542000515.html

[5] Suplicz, S. – Fűzi, B.: Essay on access control systems managed by an iris identification device (aversiv reactions and attitudes of the users), Budapest Tech, 2007

[6] http://www.pcs.com/uploads/tx_nppcsproducts/INTUS_1600PS_B_en.pdf