ANNALS of Faculty Engineering Hunedoara
– International Journal of Engineering
Tome XIV [2016] – Fascicule 3 [August]
ISSN: 1584-2665 [print; online]
ISSN: 1584-2673 [CD-Rom; online]
a free-access multidisciplinary publication
of the Faculty of Engineering Hunedoara

[1.]György FIALKA, [2.]Tibor KOVÁCS

THE VULNERABILITY OF BIOMETRIC METHODS AND DEVICES

[1.] Óbuda University, Budapest, HUNGARY

ABSTRACT: Biometric data or templates (fingerprint, hand-geometry, 2D or 3D face, palm or fingervein, iris, etc.) are always attached to a unique person. According to many experts, these data can not be delivered, copied, spied, or stolen unlike a secret code, password or access control card. We at Óbuda University (Budapest, Hungary) have established a system of criteria to determine the optimized use of biometric instruments (Mission Oriented Application). This article shows the scientific arrangement of this.
Keywords: vulnerability, biometric identification, fingerprint, handgeometry, vein

1. INTRODUCTION

The man goal of the authors is do not sell any products but to examine the vulnerability the biometric methods and devices and publish the test results. The *Table 1* shows some important biometric specifications given by the manufacturer.

First user's registrate in the device, so 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, typical points to the stored one. If the most of the typical points are the same the identification will be successful, otherwise denied.

In this article, we are going to review the most significant biometrical identification methods, and then we are going to summarize the most remarkable experiences and enumerate the basic criteria for the application of biometric identification methods (devices).

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

		FINGER-PRINT IDENTIFI-CATION[1]	OTHER BIOMETRICAL IDENTIFICATION			
			Hand-geometry[2]	Face[3]	Vein[4]	Iris[5]
PARAMETERS[6]	FAR[7] [%]	0.2	0.1	0.5	1/12.000	1/1.200.000
	FRR[8] [%]	1	0.1	0.5	0.01	< 1
	Max User Number (N)	250…5.000	512	500	Unlimited	1.000
	Extended Template[9] Storage Capacity		1.000	1.000	n/a	5.025
	Identification time	10.000 in 1:N 100.000 in 1:1	as user number	as user number	10.000 in 1:N 500.000 in 1:1	as user number
		< 1s	< 1s	approx. 1s	< 1s	approx. 1s

[1] Suprema BioEntry Plus, FingerKey DX, L1-4G V-flex and Bioscrypt V-pass (typical data)
[2] HandKey II
[3] FaceID (estimated data by many devices)
[4] L1-4G and INTUS
[5] Panasonic BM-ET330
[6] Access control biometrics user guide – British security industry association, Form No.181, Issue 2, May 2010
[7] FAR: False Acceptance Rate, it shows how much non-user can enroll successfully out of 100 users
[8] FRR: False Rejection Rate, it shows how much user can not enroll successfully out of 100 users
[9] The code of the biometric pattern

2. METHODS FOR BIOMETRIC IDENTIFICATION

At present the most widely used identification methods are fingerprint, handgeometry, 2D or 3D face, vein (hand or finger) and iris recognition. We are going to review these methods and their characteristics in brief below.

- Fingerprint: This is the most widespread method. The operation of the device is based on its capability to determine the most characterized patterns as points, intersections and crossings. It is possible every single point of a fingerprint to characterize by a coordinate, and every intersection and crossing and by vectors starting from the intersection or crossing point. Devices determine 15-30 points and/or vectors. [1]
- Handgeometry: The basics of the method are measuring the characteristics of a hand as length, width and thickness of the fingers and diameter of a circle drawn in the palm. The number of typical data is 14-30. [2]
- Face: In the case of 2D face recognition the most typical points of the face are selected (chin, nose, earlobes, eyebrow, etc.) and the distance between these preselected points creates a unit vector. This unit vector is the base of the other distances among typical points computed within the unit vector (e.g. the distance between chin and left earlobe of a specified person is 2 or 3 unit vectors). Instead of storing essential points or distances of these points, enrolling the proportions is more appropriate since the proportions are always permanent. The 3D face recognition methods take similar approach: a net is projected on to the face and the proportions of distances among the junctions of the net are stored. [3]
- Vein: The essence of the palm vein method is the illumination of the palm by infrared beam after which the blood rich in oxygen absorbs a considerable part of Infra Radiation. The received pattern is practically very similar to that of a fingerprint, which is generated by characterized lines. [4]
- Iris: The iris is a thin membrane on the interior of the eyeball. Iris patterns are extremely complex. Iris recognition uses individual differences in the complex patterns found in the iris of the human eye to authenticate individual identities. 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. Patterns are absolutely individual (even in fraternal or identical twins). Patterns are formed by six months after birth, stabilize after a year and they remain the same for life. Imitation is almost impossible. There are many solutions to record characteristics of an iris. One of them is when the pattern is similar to fingerprint (intersections, crossings). [5]

3. WEAK POINTS – VULNERABILITY

Hereby we are going to summarize the most remarkable experiences some of which showing surprising results.

State that generally it is possible to improve the efficiency of identification if we use 1:1 method instead of 1:N (in the case of 1:1 identification we compare one template to a enrolled one, e. g. passport with biometrical data, while in the case of 1:N the comparison method is one template to all saved users). However, supplementary data (a code, a card or a memory chip) is necessary, but the total identification time does not increase. If the number of comparing templates is too high, the false rejection and/or false acceptance show an extreme increase.

The aforementioned the fingerprint identification is the mostly applied technology on the biometric devices market at present. We may find it on our laptops, in passports, access control systems, bank offices and in numerous areas of our everyday lives. This technology has an enormous significance despite the fact that it is one of the most vulnerable. There are many occupations where fingerprint can often be damaged (mason, gardener, butcher, etc.). Not to mention 5 % of population who do not have any available fingerprint.

Fingerprint is an external biometric data, which is the main source of its vulnerability. Manufacturers, offices require, prescribe or propose users enroll their index or thumb primarily, although the likelihood of injury and contamination adversely affecting the identification is self-evident. The index and thumb are the most used, because they are essential for the grip. Object touched are contaminated and/or small particles peel from the surface. These fine particles fill out gaps of fingerprint. Due to this, the characteristics, which are the basic of identification, will be disappeared.

In many cases, the use of the little finger to enroll a fingerprint is a possible solution. Majority of people does not use it in fact, for that reason the probability of vulnerability is far less.

Unfortunately acquire fingerprint, it is not necessary to be an expert. Whoever is cable to pick it from an everyday glass off by a 20 USD-007 agent-kit available in a department store and a moderately skillful stamp maker prepares a thin rubber print within twenty minutes. Putting it on anybody's fingertip, the fingerprint identification device recognizes it as a live template. In this case we can't mislead the instrument if its principle of operation is based on polarized illumination detection.

Some years ago, we installed a hybrid access control system controlled by cards and fingerprints. The number of users was about 4.000. According to data sheet of biometric device the memory storages 10.000 templates and the identification time is no more than two seconds. Our experience was over 500 templates the number of false rejections has been started to increase exponentially and reaching 1.200 templates the system has been collapsed. From this moment our institute tests the biometric devices 10%, 20%, full charged state of memory capacity, too. During the test, we enroll 20-50 real templates and the remaining is refilled by automatically generated ones. The device is well applicable if the function of false rejection rate depending on number of templates is low constant (e.g. $\leq 0.1\%$).

Handgeometry devices were testing in laboratory environment and industrial places more than 10 years. The maximum user number was 1.500, and they were using devices daily.

0.3% of users are afraid from this technology because they never seen before similar or afraid from infections' spreading, but installing sanitizers close to device nobody takes advantage of this possibility. Sometimes the extreme hand sizes (small or big) and too long artificial nails increase false rejections. Some user finds so extraordinary this technology and too often, unnecessarily used it.

In numerous cases face recognition devices store in their memory infra images prepared from faces. Obtaining these photos from memory and showing them to the instrument's detector it recognizes them as real templates.

Sometimes devices mentioned before detect drawing faces as a real one, however during identification it means a difficulty if a cap or glasses cover eyes, a sweater or pullover is high-necked and they reach chin and lips. Locks of hair covering partially the face do not cause any inconvenience.

At present vein recognition systems are one of the safest biometric identification devices, because they measures inner features. Unfortunately, in this case sometimes the method itself prevents the identification. If there is a significant temperature difference between the sites where the device has been installed and neighbouring place (space) this phenomenon may obstruct the successful detection. When the device is operating in a foyer or lobby controlling an access control system where the temperature is considerably lower than on the street, then the thin film moisture condenses on the surface of the hand. This humidity absorbs the infrared beams, there is not any reflection consequently the detection is impossible.

Another case we (at Applied Biometrics Institute) were drawing a pattern (lines) on medical gloves with black felt pen and tried to enrol the "gloves" and gloves on the hand. We had successful registrations and thereafter identifications in both cases. As we stored handvein, too, we could determine the device has been identified the "gloves". Conclusion is the instrument cannot distinguish the live sample.

Regarding to the iris recognition systems the principal problem was 7-8 years ago, that more than 20 % of users refused this kind of biometric detection. This percentage was surprising because the respondents were students. The main raison was they feared eyes from IR radiation. At present due to the development of photo technology an image sensor of an iris detector is capable to enrol the iris from five meters if the speed of the user is no more than 1 m/s (it's true the illumination has a key role). It means the iris - despite of its complexity - become a real external biometric data, it can be relatively simply acquired.

4. BASIC CRITERIA FOR APPLICATION

Next, we will enumerate the basic criteria for the application of biometric identification methods (devices). With assistance of these, it is generally possible to determine the definite place of use of a device. In certain cases, the task of applier of a technology is simple: he or she may make a decision by the principle of operation, but sometimes it is inevitable to conduct complex measurements.

- External or internal data: Is the origin of the biometric data external or internal? The external data are directly visible and generally more vulnerable, it is easier to acquire (i. e. appropriate,

copy) them. In this sense the fingerprint, handgeometry, face and iris recognition methods (devices) provide external data whereas vein identification is an internal one.

- Touch or non-touch technology: During the enrollment of biometric data one must either touch the surface of the detector or any part of the device or not. The touching technology bears infection hazard, so users aver from it.
- Live sample: Is the device suitable to recognize live samples? If not, so the acquired (copied) sample is available without any difficulty.
- Total identification time: If the biometric device manages, an access control system the total identification time is the most substantial data. According to definition it takes from the moment of the person arriving to the device closer as one meter and finishes when he or she makes away more than one meter (after a successful identification). These data changes from situation to situation, so it is unavoidable to measure physically them. Data sheet contains electronic identification time only, from the start of capture of biometric enrollment to a response signal sending. This is shorter considerably than the total identification time.
- Clone recognition: According to our definition clone is a copied live sample (e.g. a thin rubber fingerprint will be prepared from a real sample and will be put on a fingertip. The device recognizes it as a live sample except if the method - e.g. identification by polarized light - is capable to filter this fake).
- Constancy of False Rejection Rate (FRR): At present, the majority of biometric identification devices manage thousands of users' templates. Our experience is the FRR's dependence by number of templates is much more exponential as constant in many cases. Effects of temperature, humidity, illumination or contamination may a determinative impact for FRR, too.

5. CONCLUSION

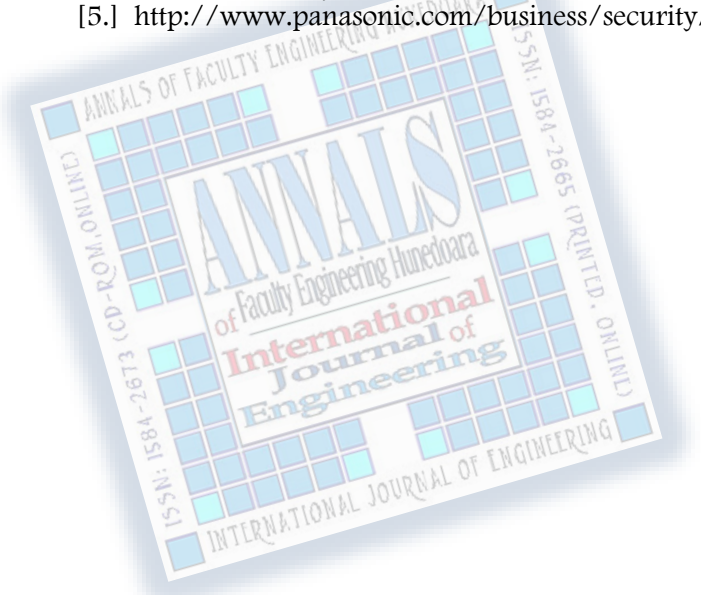
Methods and devices such as fingerprint, face and iris detection are used at high priority or sensitive places (e.g. at airports or during bank transactions) for security control and their proliferation are expected in the field of e-commerce. For that reason, the examination of vulnerability (i.e. finding week points) of biometric methods and devices is fundamental.

We found the basic problem of the biometric identification is to positioning the members (of body) to the same position where the user placed during registration. Most of the devices cannot handle this problem.

We will enumerate the basic criteria for the application of biometric identification methods (devices), namely external or internal data, touch or non-touch technology, live sample, total identification time, clone recognition and constancy of FRR. With assistance of these, it is generally possible to determine the definite place of use of a device.

Bibliography

[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.pcs.com/uploads/tx_nppcsproducts/INTUS_1600PS_B_en.pdf
[4.] http://product.yktworld.com/article/201008/20100816154200515.html
[5.] http://www.panasonic.com/business/security/bm-et300_demo/iris.html



ANNALS of Faculty Engineering Hunedoara
– International Journal of Engineering