T 115 MEDICINOS TECHNOLOGIJA

A Human Classification System for Biometric Parameters

R. Volner

Department of Air Transport, Faculty of Transportation Sciences, Czech Technical University in Prague,
Horská 3,128 03 Prague 2, phone/fax: +420 2 2435 9183, e-mail: volner@fd.cvut.cz

P. Boreš

Department of Theory Circuit, Faculty of Electrical Engineering, Czech Technical University in Prague,
Technická 3,166 00 Prague 6, phone/fax: +420 2 2435 2098, e-mail: bores@feld.cvut.cz

Video-acoustic detection platform system architecture

The system is composed by the main module, the control and management module. This module uses the concept of task and event, establishing the task which are made by the rest of modules, the execution policies when events happen and the management of such events. The information of task, events, policies, logs and classification results are stored in a system database (Fig. 1).

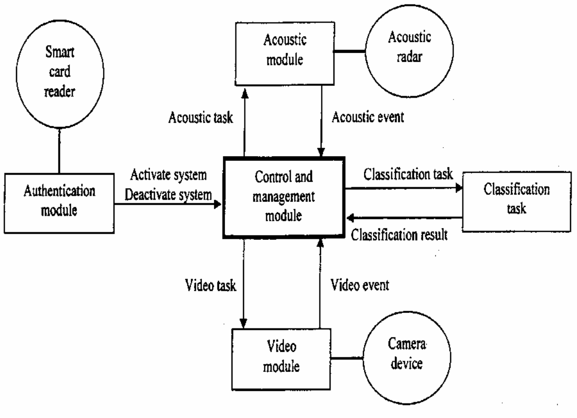

Fig. 1 System architecture

A task is the accomplishment of a sequence of action by device as a camera or an acoustic radar. An event is the answer to an incident during the accomplishment of a task. When a module generates an event, it is received by the control and management module, which decides, according to his policies, the actions to make (Fig. 2):

- to initiate a task in another module and to check the result,
- to initiate a task in another module,
- to send an event to another module,
- to ignore the event.

The system is compounded by another set of basic modules that accomplish different tasks:

- image module – it makes the capture of images through a camera device following the accomplishment of a task,

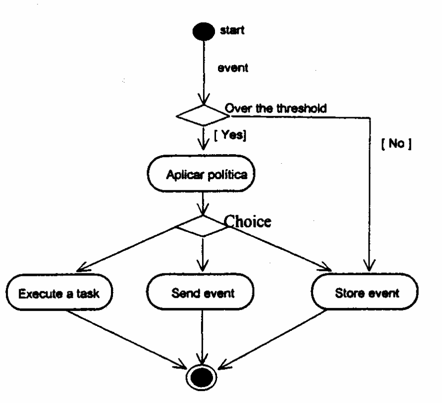

Fig. 2. Task management diagram

- acoustic module – it takes acoustic images following established tasks or activated by an event ones and detects the moving objects sending an event,
- authentication module – it controls the activation and the deactivation of the system using smart cards to identify the people that accede to the room,
- classification module – it allows classifying the results for the system training and the capture of information.

If we analyze the system architecture in layers or levels we found that it is divided in:

- centralized system database, where the whole information of the system is stored – tasks, events, logs, video and acoustic images, etc. (Fig. 3),

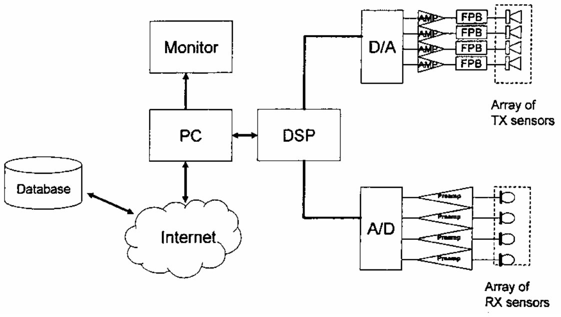

Fig.3. Acoustic module

- communication channel – channel used by the modules to intercommunicate,
- system module – each one of the elements that control the rest of devices used by the system,
- web server – that provides user interface service to the modules.

The main functionalities of the system are (Fig. 4):

- monitoring of a closed enclosure – through the use of image and sound devices the system can monitor a room with permanent characteristics,
- capture of video-acoustic images allowing the correlation between both media,
- automatic intruder pre-detection thorough the processing of the video-acoustic images,
- user authentication thanks to use of smart cards and the visual and acoustic characteristics of the user,
- classification of the data obtained by the system,
- generation of statistical information for its later analysis.

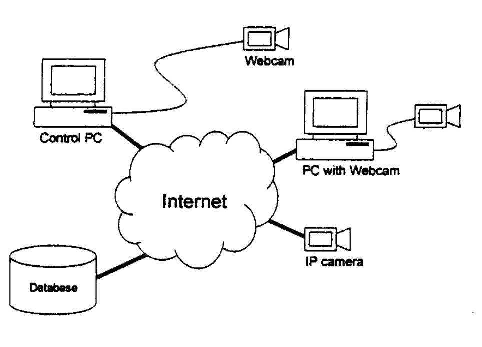

Fig. 4. Video module

Control and management module

The control and management module is the central and more significant element of the system. It is the responsible to control that the other modules accomplish every tasks, the management of the information and the events generated by the other modules and the definition of the policies to execute when the events arrive.

We have two types of tasks (Fig. 5):

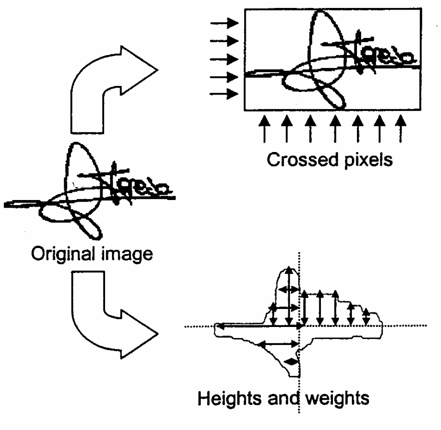

Fig. 5. Feature extraction by contour parameterization technique

- programmed tasks which are planned to be executed in a fixed moment, at a concrete date and time,
- not programmed tasks – those which are executed by the arrived of an event to the system.

The policies define the operation that the system must do after each event is produced. They are stored in the database, defining the thresholds that an event must surpass in order to be considered.

Handwritten signature verification system

In the last years, there have been many developments in the signature verification problem. It is in the off-line signature verification area where is centred this work. The control of forgeries by off-line systems has an important role in application areas as medicine (prescriptions, medical reports,…), commerce (cheques, contracts,..), government and law. In these cases the signature has been signed previously.

A new classification model, which has never been used for signature verification, is proposed in this system. This model is based on geometrical properties. These techniques are:

- contour measure – measure of widths and heights of the signature contour,
- contour following – signature contour measure in polar coordinates,
- region grouping – grouping the signature stroke in regions according a connection criterion,
- direct image – concatenation of all the rows of the matrix that represent the signature image.

Parameterization techniques

Parameterization is one of the critical points of the verification system. The choice of the parameterization system will be crucial and it will depend on several elements as vector size and classification system. Taking into account the classifier nature – based on geometric properties – and the good results of the use of direct images in other applications as facial recognition, four parameterization techniques has been proposed:

- contour measure – in this technique, the height of 60 points and the width of 40 points are measured in the signature contour,
- contour following – in this technique, the geometrical centre of the contour is calculated and it is followed in polar coordinates,
- region grouping – in this technique, the signature stroke is grouped according to a horizontal and vertical neighbor connection criterion, and after that, the geometrical centre – mass centre – is calculated for each region,
- direct image – in this technique, the rows of the matrix that represents the signature image are concatenated in order to obtain a vector.

Iris authentication biometric system

Identification is a difficult problem, with a complicated solution. The most secure way to solve it is by manual means – someone makes this process comparing a person with any data that reflects his/hers identity, such a policeman compares the person's face against his/hers passport photography. But not in all cases, a manual identification is viable – so the need of doing it by automatic means arises. In these situations, some feasible solutions can be used.

Biometrics tries to solve these problems , by using, instead of something the user's body, property that makes him/her different from others and represents his/herself in a univocally way. Biometrics uses something the user is, instead of something he/she has or knows.

When designing an authentication system, if on-line connection to central databases wants to be avoided, the user's template can be distributed to the user, so that he/she carriers always his/her biometric information with him/her. These data can be stored in a token with high security mechanisms, such as a smart card. But then, security can be compromised when transferring biometric data to the system in charge to perform the biometric verification.

Iris recognition

All biometric systems relay on measuring a human characteristic, which can be physical or behavioral. The characteristic chosen depends on the system requirements, so, as an example, for low security systems, where the user comfort is an important requirement, hand geometry could be a good choice, while for high security environments one of the most promising techniques relays on human iris.

The human iris has some characteristics that make it suitable to be use in biometrics applications:

- the possibility of finding an iris equal to another one is considered to be null, even the two iris of the same individual are different,
- the iris pattern does not change through the user's whole life,
- it is naturally isolated by the cornea,
- modifying it surgically without any risk for the vision is nearly impossible,
- the physically response to light provides it a suitable way to test the aliveness of it.

Iris recognition systems relays on a very similar architecture (Fig. 6).

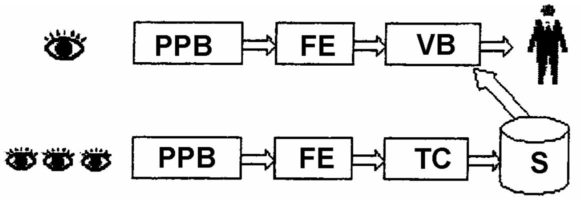

Fig. 6. Iris recognition system: PPB – pre-processing block, FE – feature extraction, VB – measure verification block, TC – Template calculation, S – storage

The firs block presents the image acquisition. This block is used to obtain from the real world the necessary data to process the biometric algorithm. These data can be just a digital image or something more sophisticated . In an iris recognition system, the image acquisition is done by a camera, it can be a high resolution photography camera or an infrared one.

After that, preprocessing block takes these data and prepare it for the following block, improving the characteristics of the initial image, equalizating, taking out the useless information from the rest or emphasizing the parts of the image that contents more information.

The feature extraction block is in charge of converting the data in a feature vector which makes it suitable to be measure, to be compared. The feature data should be univocal of each user. The data obtained before is used in different ways depending of the aim of the system at the moment. If the data want to be stored, the feature data is treated to create a template of the user and it is storaged with the rest of the user data. On the other hand, if the user belongs to the database of the system a verification block should determine if the physical characteristic belongs to the user he/she says to be, comparing the sample feature vector with the template stored. This block depends on the algorithms used before, as for the Gabor filters and wavelet transform, the Hamming distance, the Euclidean one and the zero-crossing distance have been studied.

Based system in the feature of hand palm

Biomedical systems are a field increasingly more important in the environment of the research and the industrial field. In this sense, the biometric is easy to use, nothing that to remember, nothing that to change and nothing that to lose. Besides, it provides a higher level of security, with a human characteristic that easily cannot be guessed or deciphered.

The majority of the biometric systems work with very similar ways and can be summarized in two steps:

- the first step consists of the registration of the person in the system. During the process of registration, the system captures the characteristic of the person, it processes it to create an electronic representation,
- according to the traditional theory in biometric, the second step depends on if the function of the biometric system consists of verifying the identity of the person or to identify the person.

In the case of verification, the people show their hands to system which are their identity, presenting identification card or introducing some special key. The system captures the characteristic of the person and it processes it to create an electronic representation called – model in alive. Finally, the system compares the model in alive with the model of reference of the person. If both models coincide the verification was carried out with success. In opposite case, the verification is failed. In the case that the function of the biometric system is identification, the person does not report to biometric system which is him identity. The system only captures the characteristic of the person and it processes it to create the model in alive. Then, the system proceeds to compare the model in alive with the set of reference models, to determine the identity of the person.

The use of the palm of the hand as measure of authentication has turned out to be an ideal solution for applications of middle security, where the convenience is an option lot more important than the security or the precision. In the same way, this technique offers a good balance between performance and facility of use. The fast and easy integration in other systems of security do that the use of the hand is an obvious first step in many biometric projects. Even, the geometry of the hand has a privileged position in the market of sales.

Communication requirements

Another constraint comes with the fact that biometric data should be transferred to the biometric token. In that sense, two situations should be considered:

- the transmission of the template,
- the communication of the current biometric sample.

The first one, in a match-on-token system, is not really constraint, because that communication will only take place once or twice in the token life, i.e. the template will only be transferred in the personalization phase and never will go out of the token during its us-age.

Sending the current biometric sample from the terminal to the token is a completely different issue. Depending on the technique and method used, it could be as simple as just transferring the feature vector – once it has been extracted from the image or signal captured – to the token. In these cases this will mean to send as many bytes as the template. The way data is transferred to the token will limit the viable length of the vector, which will also depend on the application restrictions. Usually applications need that the biometric verification could be done in less that 1 s, for not giving users the feeling of a slow identification. Considering a serial communication – which is a real restriction to reduce connection pins, there is a direct relation between the speed of the communication and the size of the vector to be transferred. As an example, considering the matching time as null – which is not at all realistic, and the lack of communication overheads – parity, ciphering, handshake, packet handling, etc., a communication at 9600 b/s will restrict the size of the vector to 1200 bytes, while to be able to send 7kB, communication speed should increase to 56kb/s.

Once again some biometric algorithms could require that the amount of biometric data to be transferred to the matching algorithm makes unviable to use conventional serial communication, needing other protocols as the ones used for multimedia applications – USB 2.0 or IEEE 1394. This is the case of those situations where the matching is performed at the same time that the sample processing – for the feature extraction, because it is done by modeling solution – such as neural networks, or when the verification is made using a large set of feature vectors coming from continuous utterances of the biometric parameter of the user.

The serial communication has been chosen, instead of parallel one, in order to reduce cable connection. This decision has the inconvenience of reducing also communication speed, but considering current protocols and interfaces – USB, fire-wire, etc., this is not longer a hard restriction.

To be able to cope with both, standard smart card technology and the set of new interfaces, the UART – universal asynchronous receiver transmitter – should be designed with different configurations. Regarding speed, the lowest baud rate accepted should be the one obtained by having a time bit of 372 cycles of the clock supplied to the card – which should be lower than 5 MHz, as it is considered in ISO 7816 standard, related to smart cards. For non smart cards implementation, then speed will depend on the clock frequency and speeds higher than 1 Mb/s are recommended.

The general implementation will adopt communication with TTL levels in a single bi-directional line – allowing only half-duplex communication. Then, other implementations can adept those levels to USB, RS-232, RS-488, et.

Voice biometrics

It is possible today to automate a growing number of speaker-recognition tasks with such technologies as speaker verification and speaker identification. Like human listeners, voice biometrics use the features of a person's voice to ascertain the speaker's identity. Systems performing this function have been applied to real-world security applications for more than a decade. Their use is increasing rapidly in a broad spectrum of industries, including financial services, retail, corrections, even entertainment. Here, I provide an overview of speaker verification and speaker identification, focusing on deployed, real-world technologies and the types of applications being used today.

Types of voice Biometrics

Voice-biometrics systems can be categorized as belonging two industries (Fig. 7):

- speech processing,
- biometric security.

The following section outline the best-known commercialized forms of voice biometrics:

- speaker verification (Fig. 8),
- speaker identification (Fig. 9).

This dual parentage has strongly influenced how voice-biometrics tools operate in the real world.

Applications of voice biometrics provide security, fraud prevention or monitoring (Table 1).

Current research and market trends indicate that future applications of voice-biometrics will be text-independent and incorporate other speech-processing and biometric technologies. Such applications are already in demand in several markets. For example, health-care, financial services and other industries that handle large numbers of sensitive documents have begun to incorporate multiple biometrics into their security strategies. The use of products for multiple and layered biometrics is further supported by declining prices biometrics sensors and development of standards, facilitating the development of multi-biometric applications.

The wireless industry, Internet security providers and telecom services providers all support development of on obtrusive, text-independent speaker verification and identification to secure the communications environments of the future.

Table 1. Example deployed application

Function	Application type	Example
	Data and data networks	**Password reset (over the telephone) using virtual help desk**
		Off-site access to secure data networks
Security		**Internal wire transfers**
	Physical/site access	Immigration and naturalization service
		Door access control system and located box for children
		Evening and weekend access to the city buildings
	Telephone network security (tool fraud)	Tool-free long-distance lines for buildings and staff
		Integration of speaker verification into wireless security package offered to carriers
	Transaction security	**Automated product-ordering over the telephone**
Fraud prevention		Transfer of money between accounts of a bank customer
		Time and attendance of part-time employees
	Time and attendance monitoring	Time and attendance of workers
		Tracking of juvenile and adult probationers
Monitoring	Corrections monitoring	**Monitoring of home-incarcerated offenders**

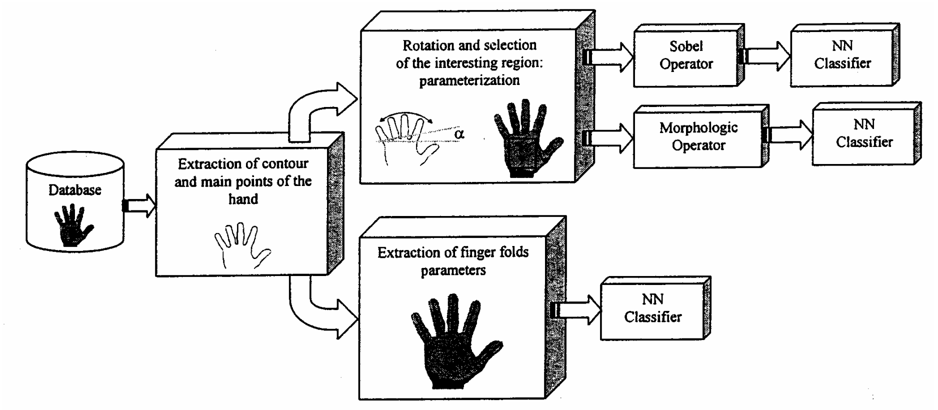
Database
Extraction of contour and main points of the hand
Rotation and selection of the interesting region: parameterization
α
Sobel Operator
NN Classifier
Morphologic Operator
NN Classifier
Extraction of finger folds parameters
NN Classifier

Fig. 7. Steps in the verification/identification of hands in our database

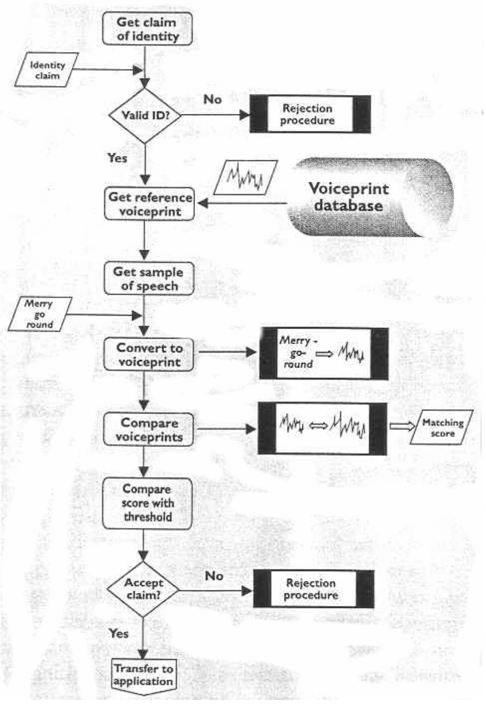

Fig. 8. Speaker verification

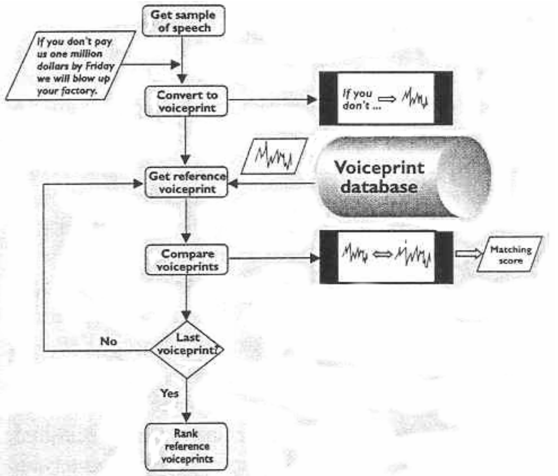

Fig. 9. Speaker identification

Conclusion

Current research and market trends indicate that future applications of voice-biometrics will be text-indenpendent and incorporate other speech-processing and biometric technologies. Such applications are already in demand in several markets. For example, health-care, financial services and other industries that handle large numbers of sensitive documents have begun to incorporate multiple biometrics into their security strategies. The use of products for multiple and layered biometrics is further supported by declining prices.

Biometrics security system enabled air transport have opened up a new set of service opportunities. At the same time, they have also introduced several security threats that need to be addressed. These security threats can originate from outside the airplane or from within the plane.

Note. This paper and research has been supported by MSMT grant N^o. CEZ: 6840770014.

References

1. **Volner R.** CATV – Interactive Security and Communication System // 34th Annual 2000 International Carnahan Conference on Security Technology. – October 2000 Ottawa, Canada. – IEEE Catalog Number 00CH37083. ISBN 0-7803-5965-8. – P. 124–136.
2. **Volner R.** Home security system and CATV // 35th Annual 2001 International Carnahan Conference on Security Technology. – October 2001 London, England. – IEEE Catalog Number 01CH37186. ISBN 0-7803-6636-0. – P.293–306.
3. **Volner R.** CATV Architecture for Security // 36th Annual 2002 International Carnahan Conference on Security Technology. – October 2002, Atlantic City, New Jersey, USA.- IEEE Catalog Number 02CH37348. ISBN 0-7803-7436-3. – P. 209–215.
4. **Volner R., Poušek L.** Wireless Biomedical Home Security Network – architecture and modeling Network // 38th Annual 2004 International Carnahan Conference on Security Technology. – October 2004 Albuquerque, New Mexico, USAIEEE Catalog Number 04CH37572. ISBN 0-7803-8506 – 3. – P. 69–76,

Pateikta spaudai 2005 04 25

R. Volner. P. Boreš. Žmogaus biometrinių parametrų klasifikavimo sistema // Elektronika ir elektrotechnika. – Kaunas: Technologija, 2005. – Nr. 6(62). – P. 16–21.

Užduoties ir pagrindinio modulio suvokimas leidžia pritaikyti sistemą analizuojant, kokie pokyčiai įvyksta ir kaip sistema veikia įvedus naujus modulius. Naudojant klasifikavimo modulį galima atlikti patikimesnius tyrimus. Biometrijos svarba nuolat didėja. Biometrinių sistemų paskirtis – atpažinti tiriamąjį, lyginant jo biometrinius duomenis su jau turimais. Siūloma nauja autentifikavimo sistemos struktūra. Ji remiasi delno linijų analize. Il. 9, bibl. 4 (anglų kalba; santraukos lietuvių, anglų ir rusų k.).

R. Volner. P. Boreš. A Human Classification System for Biometric Parameters // Electronics and Electrical Engineering. – Kaunas: Technologija, 2005. – No. 6(62). – P. 16–21.

The definition of task and events managed by the core module allows that the system can be adapted, changing the how the system works or adding new modules. The use of a classification module allows the human supervision contributing with greater reliability. Use of biometrics in increasing everyday, as security concerns do. The purpose of biometric systems is finding the identity of the user comparing his biometric data with the one previously stored. The author proposes in this paper a new architecture for an authentication system. In this paper we are going to use the drawings that form the characteristics of the hand palm, as are fold – commonly called lines of the hand, cracks, scars and even fold of the fingers for verify and identify to person. Ill. 9, bibl. 4 (in English; summaries in Lithuanian, English and Russian).

Р. Волнер, П. Бореш. Система классификации биометрических параметров человека // Электроника и электротехника.– Каунас: Технология, 2005. – № 6(62). – С. 16–21.

Понимание задачи и основного модуля системы классификации биометрических параметров человека позволяет понять, какие изменения происходят и как система действует при введении новых модулей. Применение модуля классификации позволяет производить более надежные исследования. Значимость биометрии постоянно растет. Цель биометрических исследований – узнать исследуемого при помощи сравнивания биометрических данных с уже имеющимися. Предлагается новая структура системы аутентификации. Она основана на анализе линий ладони человека. Ил. 9, библ. 4 (на английском языке; рефераты на литовском, английском и русском яз.).