MIROSLAV BAČA, Ph.D.
E-mail: miroslav.baca@foi.hr
MIRKO ČUBRILO, Ph.D.
E-mail: mirko.cubrilo@foi.hr
KORNELIJE RABUZIN, Ph.D.
E-mail: kornelije.rabuzin@foi.hr
University of Zagreb,
Faculty of Organization and Informatics
Pavlinska 2, HR-42000 Varaždin, Republic of Croatia

Intelligent Transport Systems
Preliminary Communication
Accepted: Sep. 28, 2006
Approved: Oct. 5, 2007

USING BIOMETRIC CHARACTERISTICS TO INCREASE ITS SECURITY[1]

ABSTRACT

Terrorist attacks in New York City and Washington, District of Columbia on the morning of September 11, 2001 have changed our lives. The security problem became very important regarding all spheres of human activities. Tracking persons (employees, customers etc.) in ITS (Intelligent Transport System) is a huge problem. Biometrics offers a very good solution for this problem and is today maybe one of the most promising techniques for person's secure verification and authentication; biometric system also features some advantages when compared to other security systems. When using a biometric system one has to be careful because the functionality of a biometric application can be dramatically aggravated if inappropriate biometric features are selected. Classification of biometric features on contact and contactless, or distinction between "strong" and "soft" biometric features gives a framework for using biometric features, but it does not ensure that biometric features are implemented at a satisfactory level. The usage of multimodal or unimodal biometric system can significantly increase the system security but it also opens plenty of questions like privacy etc. This paper describes the implementation of biometric features which can be used in ITS, and delineates a new model of usage.

KEYWORDS

biometrics, security system, ITS

1. INTRODUCTION

Imagine the day when the door to a secured building can be opened by using an automated system for identification based on a person's physical presence, even though that person had left his or her ID or access card at home. Imagine ticketless airline travel, whereby a person can enter the aircraft based on a positive identification verified biometrically at the gateway. Imagine getting into a car, starting the engine by flipping down the driver's visor, and glancing into the mirror and driving away, secure in the knowledge that only authorized individuals can make the vehicle operate.

Human recognition process is very old and at the same time quite actual. This problem is solved by the application of biometrics. From the technical point of view, biometrics [1] is "the automated technique of measuring a physical characteristic or personal trait of an individual and comparing that characteristic to a comprehensive database for purposes of identification". Biometrics consists of [2]: Physical characteristics: eye features (iris, retina), facial features, hand geometry, ear shape, fingerprints, wrist/hand veins, DNA, chemical composition of body odour; Personal characteristics: handwritten signature, keystrokes/typing patterns, voiceprint. All these physical and personal characteristics are measured and integrated into a computer system for the person recognition purposes. Thus, biometrics is used for two major purposes [2]: identification and authentication. The Biometrics Glossary [1] says that the identification, the first main purpose of the biometrics, is "the one-to-many comparison of an individual human biometric sample against the entire database of biometric templates. It allows to determine whether a sample matches any of the templates and, if so, the identity of the enrolee whose template was matched." There are three main ways to authenticate an identity: (1) something you know; (2) something you have; and (3) something you are. These are often referred to as the three pillars of authentication [3].

Due to the development of biometrics and its machine-supported implementation, biometrics is nowadays widely used, whether applied by popular electronics or highly sophisticated devices and equipment [4], [5]. Insufficient, or rather inadequate knowledge of biometric features, which provide the basis of such systems, presents a major threat to all security systems, especially in ITS. When developing a secure ITS, it is necessary to observe the guidelines which are

intended to ensure development of a system secure enough to meet the requirements of the organization, place and time it pertains to [5]. This means that in such a system an ideal quality-price ratio will be implied. To accomplish this goal, the basics of biometric systems and biometric features need to be considered first. The first obstacle to be dealt with is an adequate selection of biometric features to constitute a system [7]. When merging the ideas of biometrics and ITS, we must consider two aspects: persons and transport vehicles. It means that we must insure effective transportation and increase the everyday life quality. When implementing biometrics in ITS, we must first consider the person and person's needs, and after that try to harmonize the person's needs with transport vehicles. In order to develop this, the paper depicted a new concept and a new model of a biometric system for ITS.

The biometric system looks on the prism unimodal and multimodal biometrics systems [8], and most quality choosing of biometrics characteristics. Once it became apparent that truly positive identification could only be based on the physical attributes of the person, two questions had to be answered. The first question: "What part of the body could be used?", and the second: "How could identification be accomplished with sufficient accuracy, reliability, and speed so as to be viable and acceptable?"

2. THE PROBLEM MODEL

It is obvious that selecting the right biometric feature (or several of them) is a challenge. Most of the currently known and applied biometric features contain a flaw which makes them impossible to be considered ideal. The question of adequate selection of biometric features, that is, characteristics that a feature is to consist of, therefore needs to be addressed. Most commonly, biometric features have to meet the following requirements: universality, uniqueness, permanence, collectability, accuracy, acceptability [9], as well as the likelihood of circumvention involved. The ideal biometric feature has to meet the following criteria: it has to be permanent and inalterable in terms of time; the procedure of gathering personal features has to be inconspicuous and conducted by means of devices involving minimum or no contact; it has to enable total automation of the system; the system has to be highly accurate and its operation speed such that it enables real-time operation [10]. None of the currently used biometric features meets all the criteria required in order to be considered ideal.

Although biometric devices rely on widely different technologies, much can be said about them in general. Figure 1 shows a modified generic biometric authentication system for ITS divided into five subsystems: data collection, transmission, signal processing, decision and data storage. The first subsystem (data collection) must be in the vehicle, whereas subsystems signal processing, decision making and data storage must be located at the ITS centre.

The issue of finding an ideal biometric feature to meet the demands of ITS should be raised. There are no easy solutions to this problem. First of all, there is no single feature appropriate enough to be considered ideal [12], [13]. The biometric feature to be used in ITS has to be absolutely reliable so that it can be determined with certainty whether in a particular situation a legitimate user is involved or not. Considering that none of the features mentioned so far are sufficiently reliable, combining single features in one of two possible ways – by means of unimodal or multimodal systems – arises as an immediate solution. Each of the two approaches has its advantages and disadvantages, so that they should be used in strict accordance with the policy of the system they are supposed to secure.

These are the important factors necessary for any effective biometric system in ITS: accuracy, speed and throughput rate, acceptability to users, uniqueness of the biometric organ and action, resistance to counterfeiting, reliability, data storage requirements, enrolment time, intrusiveness of data collection, and subject and system contact requirements. Accuracy is the critical characteristic of a biometric identifying verification system. If the system cannot accurately separate authentic persons from impostors, it should not even be termed as a biometric identification system. The speed and throughput rate are the most important biometric system characteristics. Speed is often related to the data processing capability of the system. It relates to the entire authentication procedure: stepping up to the system; inputting the card or PIN; input of the biometric data; processing and matching of data files; and annunciation of acceptation or reject decision. The biometric system acceptance occurs when those who must use the system agree that there are assets that need protection, the biometric system effectively controls access to these assets, system usage is not hazardous to the health of the users, system usage does not inordinately impede personnel movement and cause production delays, and the system does not enable management to collect personal or health information about the users. The ability to detect or reject counterfeit input data is vital to a biometric access control system meeting high security requirements. These include the use of rubber, plastic, or even hands or fingers of the deceased in hand or fingerprint systems, and mimicked or recorded input to voice systems. The system must allow authorized persons access while precluding others, without breakdown or deterioration in performance accuracy or speed.

When using biometrics systems in ITS, we must insure untroubled and unobtrusive surveillance of em-

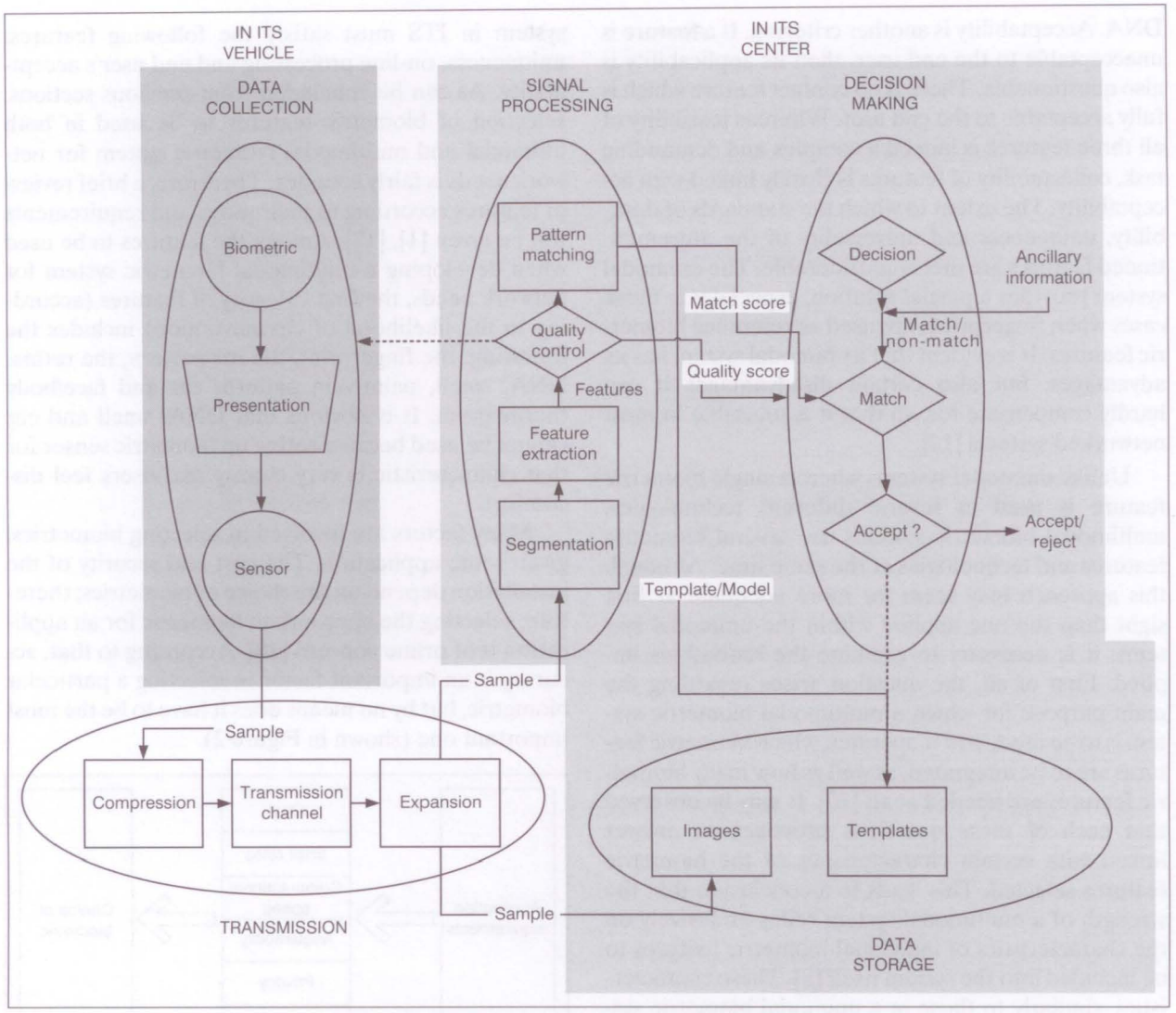

Figure 1 - Modified generic biometric model, according to [11]

ployees and customers, as well as vehicles in transports. Besides, biometrics must provide appropriate answers in the fields of payment and security.

3. THE SOLUTION MODEL

For solving the problem described in the previous part it is necessary to choose biometric characteristics which appease all the described enterprises. Since persons (and other parts of the system such as e. g. vehicles) in ITS can have many different functions (regardless of whether it is an employee or a customer) it is necessary to find proper biometric characteristics which enable that all parts of a system are interconnected at a satisfactory level. Some today's solution for vehicles in ITS (readers of plates and wireless smart cards) do not completely satisfy all the security aspects[2] required. Whereby biometric characteristic satisfies the ITS needs, it must be unique and it must be appropriate for quick on-line processing. The solution model can be observed separately for persons and for vehicles. If we observe a person, then the solution model can be developed with both unimodal and multimodal biometric system. The solution model for the vehicle can be developed only by means of a multimodal biometric system. Differences between unimodal and multimodal biometrics system can be observed only through price. There is no difference in quality when discussing these two types of systems.

A unimodal biometric system for identification and verification in ITS must ensure unique and fast on-line characteristic processing. It is very important that on stage of using biometrics in ITS we do not calculate price, because the prices of a system and services are small, while the price when a false biometric characteristic is selected is too high[3].

How to select the proper feature for a unimodal biometric system? One of the main criteria within unimodal biometric system in ITS should be uniqueness. Of all the currently used features, this criterion is met by the fingerprint, the iris pattern, the retina and

DNA. Acceptability is another criterion. If a feature is unacceptable to the end user, then its applicability is also questionable. There is no contact feature which is fully acceptable to the end user. Whereas feasibility of all three features is indeed a complex and demanding task, collectability of features is closely linked with acceptability. The extent to which the standards of durability, uniqueness and universality of the aforementioned features are met is considerable. The unimodal system provides a partial solution, especially in those cases when fingerprints are used as reference biometric features. It is evident that a unimodal system has its advantages, but also certain disadvantages it can hardly compensate for, so that it is unusable in most networked systems [14].

Unlike unimodal systems where a single biometric feature is used in several different technologies, multimodal biometric systems use several biometric features and technologies at the same time. Although this approach may seem far more adequate at first sight than the one applied within the unimodal systems, it is necessary to examine the limitations implied. First of all, the question arises regarding the main purpose for which a multimodal biometric system is to be used, how it operates, which biometric features are to be integrated, as well as how many biometric features are needed at all [10]. It may be observed that each of these questions provokes an answer linked with certain characteristics of the biometric features selected. This leads to a conclusion that the strength of a multimodal system relies exclusively on the characteristics of individual biometric features to be included into the system itself [8]. These characteristics, similarly to those in a unimodal biometric system, refer to uniqueness and speed. Uniqueness in a multimodal system tells us how big the credibility of a multimodal system is regarding discrimination between legal user and illegal user. The speed of a multimodal biometric system indicates the time needed by the system to perform personal identification. It is only through an appropriate and relatively fast integration of biometric features that the overall speed of a multimodal biometric system can be increased. Multimodal biometric system in ITS can be used only in authentication domain of vehicles, by using contact or contactless smart card with implemented biometric characteristics. Although this seems simple enough at first, the problem of feature selection is considerable indeed [15].

4. SELECTION OF BIOMETRIC CHARACTERISTICS

Selection of biometric characteristics for ITS can be very difficult. Unimodal and multimodal biometric system in ITS must satisfy the following features: uniqueness, on-line processing and end user's acceptability. As can be concluded from previous sections, selection of biometric features to be used in both unimodal and multimodal biometric system for network needs is fairly complex. Therefore, a brief review of features according to their usage and requirements will be given [1], [17]. Among the features to be used when developing a multimodal biometric system for network needs, the first category of features (according to the likelihood of circumvention) includes the following: the fingerprint, the iris pattern, the retina, DNA, smell, palm-vein pattern, ear and face/body thermogram. It is obvious that DNA, smell and ear cannot be used because seting up biometric sensor for that characteristic is very clumsy and users feel discomfort.

Many factors are involved in selecting biometrics, given some application. The cost and security of the installation depend on the choice of biometrics; therefore, selecting the appropriate biometric for an application is of prime concern [18]. According to that, accuracy is an important factor in selecting a particular biometric, but by no means does it have to be the most important one (shown in Figure 2).

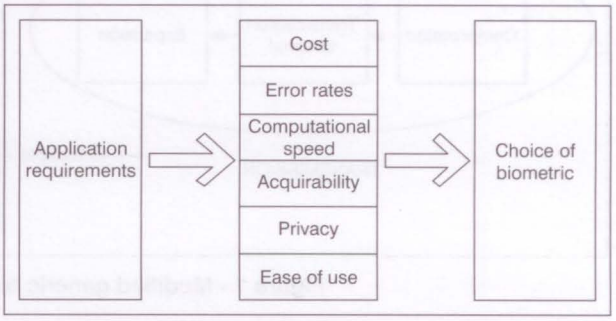

Figure 2 - Involving factors in the process of selecting the "right" biometric [18]

Among the characteristics to be used when developing a multimodal biometric system for network needs, the first category of features (according to the continuity) includes the characteristic used for unimodal biometrics system. As opposite to unimodal system, multimodal system possesses characteristics which are acceptable, fast, and easy for usage and implementation. Along with the features mentioned, several others should be analyzed. Therefore, the best way to display an overview of biometric features is by means of a chart, as can be seen in Table 1 (where L stands for "low", M for "medium" and H for "high").

Close inspection reveals that another table can be drawn from Table 1; this time according to the strength of individual biometric features. In order to do so, it is necessary to mark all the biometric characteristics denoted as H in the Implementation column. In this way, seven features will be obtained which are

Table 1 - An overview of biometric features

Characteristic	Universality	Permanence	Collectability	Acceptability	Features	Durability	Circumvention	Implementation
Fingerprint	M	H	M	M	H	H	M	H
DNA	H	H	L	L	H	H	L	L
Iris pattern	H	H	M	L	H	H	L	L
Retina	H	M	L	L	H	M	L	L
Ear	M	H	M	H	M	H	M	M
Face	H	L	H	H	L	M	H	H
Thermogram	H	H	H	H	M	L	L	M
Gait	M	L	H	H	L	L	M	M
Hand geometry	M	M	H	M	M	M	M	H
Palm-vein pattern	M	M	M	M	M	M	L	M
Keystroke dynamics	L	L	M	M	L	L	M	H
Smell	H	H	L	M	L	H	L	H
Signature	L	L	H	H	L	L	H	H
Voice	M	L	M	H	L	L	H	H

placed on the top of the list of features permanence. Consequently, it is necessary to single out those features which are denoted as H in all the other columns.

The analysis of biometric features according to their characteristics can significantly facilitate their selection. The transposition in the table and sorting in contents appliances in ITS system could make it possible to develop a biometric characteristics system which in appropriate way satisfies the required needs. As we can see, the most appropriate biometric characteristic for ITS is face. It can be concluded that apart from the face only fingerprints can alone or in combination with other characteristics insure a reasonable biometric system. General conclusion is that biometric characteristics used in ITS comply with biometric industry. This result can be compared with [19], according to which the employee-facing application gives very good results. Using biometric solution matrix for pc/network access authors get the following results: exclusivity (6/10), effectiveness (8/10), receptiveness (8/10), urgency (7/10) and scope (8/10).

5. SYSTEM FEASIBILITY

The feasibility of ITS biometric system may go in two ways; through person and through vehicle. If we merge person and vehicle, for model development purpose, with smart card, the biometric system can be very simplified. This simplified model is depicted in Figure 1.

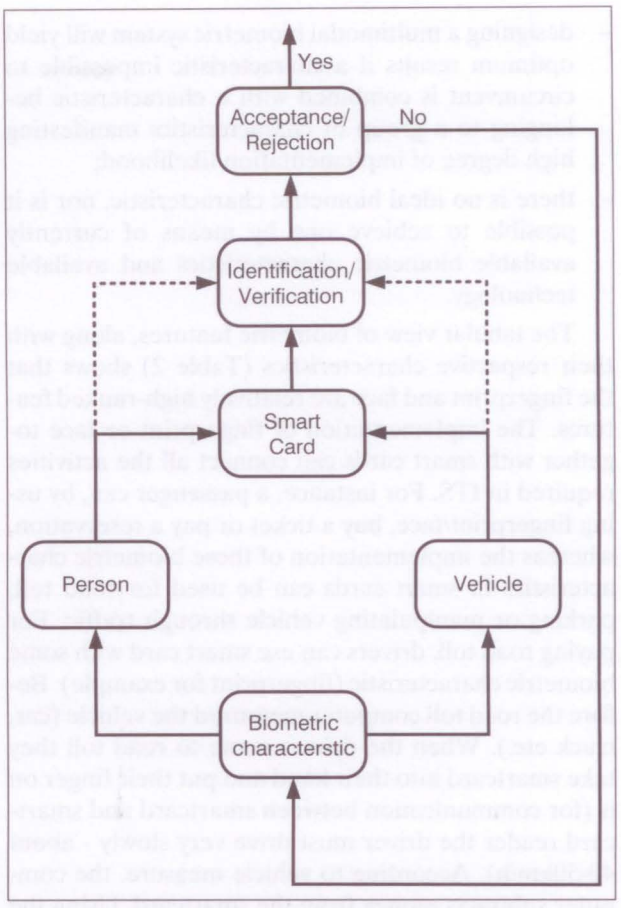

Figure 3 - New biometric model for ITS

As we can see in Figure 3 this new model has three different approaches. The first approach is through person. If we want to use only persons in ITS we follow this approach. If we want to use a biometric system for vehicles we follow the second approach, but if we want to merge persons and vehicles we use the latter approach (merged through smart card). Every part of this model can be used separately but they all can be used at the same time. For the best results this new model we must follow the following implementation factors: training operational personnel; training users; the enrolment process; the environment and installation and commissioning [17].

6. CONCLUSION

Selecting a biometric system to be used in ITS is a demoralizing task. Throughout the paper, a number of conditions have been discussed that need to be satisfied in the course of designing such a system. The conclusions are as follows:

- designing a unimodal biometric system for ITS is only possible by means of a characteristic which is easy to be implemented and has high permanence;

- designing a multimodal biometric system will yield optimum results if a characteristic impossible to circumvent is combined with a characteristic belonging to a group of characteristics manifesting high degree of implementation likelihood;
- there is no ideal biometric characteristic, nor is it possible to achieve one by means of currently available biometric characteristics and available technology.

The tabular view of biometric features, along with their respective characteristics (Table 2) shows that the fingerprint and face are relatively high-ranked features. The implementation of fingerprint or face together with smart cards can connect all the activities required in ITS. For instance, a passenger can, by using fingerprint/face, buy a ticket or pay a reservation, whereas the implementation of these biometric characteristics in smart cards can be used for road toll, parking or manipulating vehicle through traffic. For paying road toll, drivers can use smart card with some biometric characteristic (fingerprint for example). Before the road toll computer measured the vehicle (car, truck etc.). When the drivers come to road toll they take smartcard into their hand and put their finger on it (for communication between smartcard and smartcard reader the driver must drive very slowly - about 40-50km/h). According to vehicle measure, the computer subtracts money from the smartcard. Using the combination of fingerprint and smart card is very acceptable because it is impossible to make a forgery and all the data in the smart card are secure according to all EU privacy protection acts.

Dr. sc. **MIROSLAV BAČA**
E-mail: miroslav.baca@foi.hr
Dr. sc. **MIRKO ČUBRILO**
E-mail: mirko.cubrilo@foi.hr
Dr. sc. **KORNELIJE RABUZIN**
E-mail: kornelije.rabuzin@foi.hr
Sveučilište u zagrebu, Fakultet organizacije i informatike
Pavlinska 2, 42000 Varaždin, Republika Hrvatska

SAŽETAK

KORIŠTENJE BIOMETRIJSKIH KARAKTERSTIKA ZA POVEĆANJE SIGURNOSTI ITS-A

Teroristički napad na New York i Washington u jutarnjim satima 11 rujna 2001. godine u potpunosti je promijenio naše živote. Problemi sigurnosti postali su vrlo važan segment svakodnevnih ljudskih aktivnosti. Praćenje aktivnosti osoba (zaposlenika, klijenata, itd.) u domeni ITS-a(Inteligentni Transportni Sustav) predstavlja vrlo veliki izazov i problem. Biometrija nudi vrlo dobre solucije za rješavanje tih problema i danas možda predstavlja tehniku koja najviše obećava za autentikaciju i verifikaciju osoba. Biometrijski sustavi također posjeduju određene prednosti u odnosu na druge sigurnosne sustave. Prilikom korištenja biometrijskih sustava treba voditi računa jer funkcionalnost biometrijskih sustava može biti drastično smanjena neprimjerenim odabirom biometrijskih karakteristika. Klasifikacija biometrijskih karakteristika na kontaktne i nekontaktne, ili razlika između takozvanih jakih i slabih biometrijskih karakteristika daje jasan okvir za korištenje biometrijskih karakteristika ali ne osigurava primjerenost same karakteristike. Korištenje multimodalnog ili unimodalnog biometrijskog sustava može značajno povećati sigurnost sustava ali također i otvoriti neka nova pitanja vezana za privatnost. Rad opisuje primjenu biometrijskih karakteristika u ITS sustavima te daje prijedlog modela korištenja.

KLJUČNE RIJEČI

biometrija, sustav sigurnosti, ITS

REFERENCES

1. the presented results originated from the scientific project (Methodology of biometrics characteristics evaluation 016-0161199-1721), supported by the Ministry of Science, Education and Sport of the Republic of Croatia
2. Because they can be stolen for example very easily.
3. Falsification of characteristic is not repaid.

LITERATURE

[1] *** The Biometrics Glossary Page, http://www.eyenetwach.com/biometrics-glossary/biometric-terms.html (29.10.2003.)

[2] *** International Security Homepage, http://www.security-int.com (27.10.2003.)

[3] **P. Reid**: *Biometrics for Network Security*, Prentice Hall, Upper Saddle River, NJ, 2004.

[4] **U. Dieckmann, P. Plankensteiner, T. Wagner**: *Sesam: A biometric person identification system using sensor fusion*, Pattern Recognition Letters, 1997. 18(9): 827-833

[5] **J. Bigun, J. Fierrez-Aguilar, J. Ortega-Garcia, J. Gonzales-Rodriguez**: *Multimodal Biometric Authentication using Quality Signals in Mobile Communications*, IEEE--Computer Society Press, (Proc. of 12'th Inf. Conf. on image analysis and processing, Mantova, Italy), 2003. pp. 2.11,

[6] **A. Jain, A. Ross, S. Prabhakar**: *An introduction to biometric recognition*, Michigan State University, 2004

[7] **S. Panikanti, R. Bolle, A. Jain**: *Biometrics: The Future of Identification*, IEEE Computer, Vol. 33, 2000.

[8] **M. Bača, K. Rabuzin**: *Biometrics in Network Security*, MIPRO 2005, XXVIII International Convention, Proceedings Information Systems Security, Opatija, 2005. pp. 205-210

[9] **S. G. Davies**: *Touching Big Brother*, Information Technology & People, Vol. 7, No. 4, 1994

[10] **A. Jain, R. Bolle, S. Pankanti: Biometrics**: *Personal Identification in Networked Society*, Kluwer, 1999.

[11] **J. Wayman, A. Jain, D. Maltoni, D. Maio**: *Biometric Systems*, Springer, 2005.

[12] **K. V. Diegert**: *Estimationg performance characteristics of biometric identifiers*, Proceedings of Biometrics Consortium Conference, San Jose, CA, 1996.

[13] **L. Hong, A. Jain, S. Pankanti**: *Can multibiometrics improve performance?* Proceedings AutoID, NJ, 1999.

[14] **R. Clarke**: *Human Identification in Information Systems: Management Challenges and Public Policy Issues*, Information Technology & People, Vol. 7., No. 4., 1994. pp. 6-37.

[15] **J. Kittler, Y. Li, K. Matas, M. U. Sanchez**: *Combining evidence in multimodal personal Identity recognition systems*, Proc. 1st. Int. Conf. on Audio Video-Based Personal Authentication, 1997. pp 327-334

[16] **J. Ashbourn**: *Biometrics: Advanced Identity Verification: The Complete Guide*, Springer-Verlag, 2000.

[17] **R. Chellapa, C. Wilson, A. Sirohey**: *Human and machine recognition of faces: A survey*, Proceedings IEEE, 1995. 83(5): 705-740

[18] **R. Bolle, J. Connell, S. Pankanti, N. Ratha, A. Senior**: *Guide to Biometrics*, Springer, 2003.

[19] **S. Nanavati, M. Thieme, R. Nanavati**: *Biometrics*, Wiley, 2002.

[20] **J. Ashbourn**: *Practical Biometrics*, Springer, 2004.