TRANSPORT PROBLEMS 2009
PROBLEMY TRANSPORTU Volume 4 Issue 4

Miroslav BAČA*, Markus SCHATTEN, Jurica ŠEVA
Faculty of Organization and Informatics, University of Zagreb
Pavliska 2, 42000 Varazdin, Croatia
**Corresponding author.* E-mail: miroslav.baca@foi.hr

BEHAVIORAL AND PHYSICAL BIOMETRIC CHARACTERISTICS MODELING USED FOR ITS SECURITY IMPROVEMENT

Summary. Biometric technologies rely on specific biometric characteristics that are used for recognition. The particular characteristic for a given situation can be described through a serious of descriptive parameters including ease of collecting, permanence, measurably, acceptability, deceptiveness, universality, uniqueness, sample cost, system cost, database size, as well as environmental factors. By using our ontology-based framework for adequacy of biometric systems, we introduce a model for using biometric technologies in ITS. Such technologies increase security, safety and protection of ITS.

MODELOWANIE BEHAWIORALNYCH I FIZYKALNYCH CHARAKTERYSTYK BIOMETRYCZNYCH DLA POPRAWY BEZPIECZEŃSTWA SYSTEMÓW ITS

Streszczenie. Technologie biometryczne korzystają ze specyficznych cech charakterystycznych, używanych do rozpoznawania elementów wskazujących na specyficzne zachowanie kierowców. Te szczególne parametry są dobierane odpowiednio do potrzeb z uwagi na łatwość ich pomiaru, właściwości, mierzalność, możliwość akceptacji, uniwersalność, unikalność, koszt pomiaru, rozmiar bazy danych, jak również inne czynniki towarzyszące. Zastosowaniu do systemów sztucznej inteligencji poszukiwane są elementy adekwatne do założonych zadań. W tym kontekście przedstawiono model biometryczny, który zaimplementowano w projekcie ITS. Opracowane rozwiązania technologiczne pozwalają zwiększyć bezpieczeństwo systemów transportowych i niezawodność systemów wspomaganych inteligentnymi narzędziami ITS.

1. ITS SECURITY

Intelligent transportation systems' (ITS) security is a complex structure comprised of different kinds of security. In the first place there is the passengers' security, after that security of goods and finally data security. Some of these security related issues can be observed through the term safety, but this distinction must be clearly depicted. The word security comes from the Latin root *secura*, which means "free of concern." However, secure can also mean "firmly fixed" thus explaining why there is also an implication of control mechanism present in security. Safety comes from *salvus*, meaning "healthy," thus giving it a more personal meaning. Suppose we were to talk about car safety and car security. Car safety is about protecting people by making the car less likely to be involved in an

accident and including features that allow for people to be injured less likely in the case of an accident. Car security is about protecting the car and it's contents from criminal activity.

Thus to make the best results in ITS security more efforts have to be made to implement protection measures into all ITS security aspects. In order to make it possible we decided to use biometric technologies. Biometric technologies are automated methods for verifying or recognising the identity of a living person based on physical or behavioural characteristics. By using biometric technologies in all aspects of ITS security we can enhance security, but safety and protection as well.

Safety is one of the basic performance indicators of traffic systems and a major indicator of service quality [5]. Safety can be viewed through two different aspects, the first one dealing with passengers, and the second one dealing with goods and information. Passengers' safety is crucial for ITS security so it is usual to be more strict than security of goods and information. At this point let us observe the definition of safety through risk. We can say that security is achieved in a state in which risks of undesirable events are at an acceptable level. This definition implies the need for a definition of acceptable risk, and afterwards the set of undesirable events. All these definitions are very fuzzy and depend only on the people who estimate the risk or undesirability of events. Such a conceptualisation thus does not allow us to measure safety and the transparency of the approach is at least questionable. Fig. 1 shows the general model of ITS security.

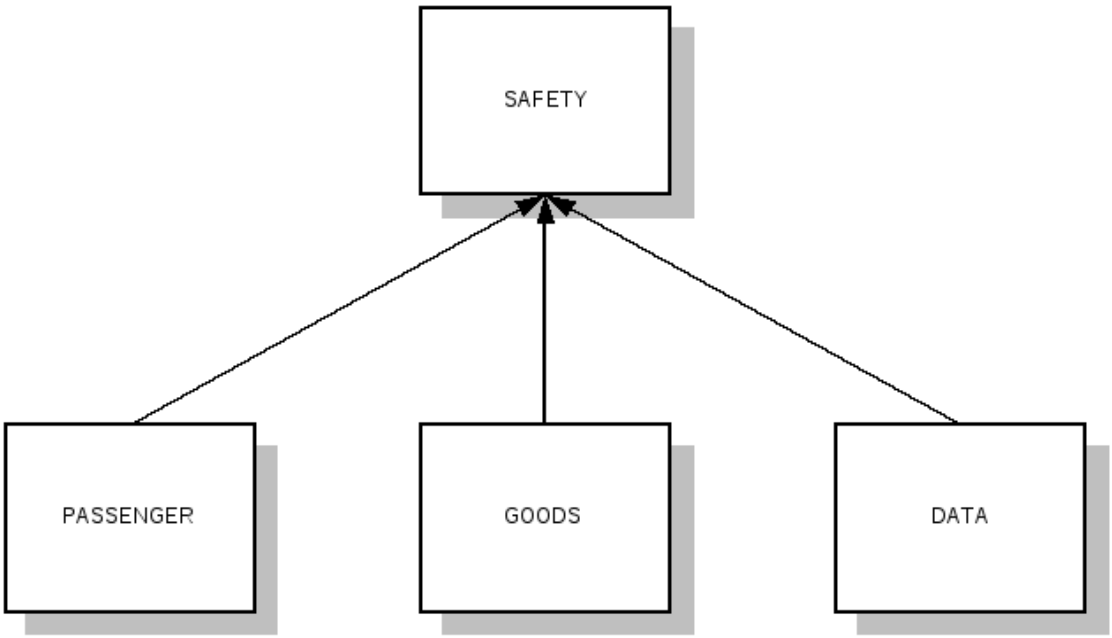

Fig. 1. General model of ITS safety
Rys. 1. Podstawowy schemat modelu ITS

The model, lets us conclude the first relation in which safety is a function as given in

$$S_A = f\{S_P, S_G, S_D\},$$

where: S_A is the overall safety, S_P the passengers' safety, and S_G the safety of goods and S_D the safety of data. Passenger safety is calculated as (according to [5]):

$$S_{PG} = \frac{K_{NS} \cdot 10^6}{Q \cdot l \cdot t}$$

where: S_{PG} represents the passengers' and goods' safety on a specific traffic roads' part; K_{NS} is the number of traffics accidents (shown on 100 million vehicle-km); Q vehicle day average (vehicle/day), l is road length (in km) and t is observing time in days. K_{NS} is calculated as:

$$K_{NS} = k_1 \cdot N_L \cdot k_2 \cdot N_T \cdot k_3 \cdot N_F$$

where: N_L represents the number of traffic accidents with low consequences, N_T represent the number of traffic accidents with high consequences and N_F the number of traffic accidents with human victims. Coefficient k_1, k_2, k_3 are previously determined and they have different values for different traffic media.

Good safety is the possibility of an adverse event during goods transportation. There are three types of potential risks: firstly basic transport risk (for example, traffic accidents, whether influence, fire and explosion, burglary, theft), second risk linked to goods conditions (breakage, humidity, leakage, wastage, corrosion, damage from fresh and sea water) and third war and political risk (capture, seizure, retention, operations of war, chaos, violence, civil unrest, strikes). So we can calculate risk like a simple possibility or like a complex combination of possibilities. Usually risk is observed as a function of possibilities that an (unwanted) event will happen p and the consequences of the particular event k.

$$Risk = f[(p_1, k_1), ..., (p_n, k_n))]$$

Data safety is observed through the so called CIA triad of information security. From that model information security is a function of confidentiality, integrity and availability $S_D = f\{C, I, A\}$. Every part of this function can be calculated separately. There is number of different ways to calculate confidentiality, integrity and availability but they not relevant to our discussion.

From this reasoning we find that there are several factors that can be influenced through the use of biometric technologies. For passengers' and goods' safety especially the K_{NS} parameter can be influenced by implementing adequate biometric measures. Basic transport risks (theft and burglary) can be lowered by using adequate authentication and security measures, as well as passengers' safety in the overall perspective. Data security has already been proved to be increased through biometric technologies [7].

Still the main problem remains: how to choose the appropriate biometric technology for a given ITS security system? Herein we introduce a framework that relies on an ontology-based system that calculates the adequacy level of a given biometric system depending on the particular situation.

2. BIOMETRICS

In the field of biometrics there are few basic terms that should be defined: characteristic, method, model, sample and pattern.

A biometric characteristic or feature is a physical or behavioural (psychological) characteristic of a person that is used for the persons recognition. Physical characteristics are characteristics that are genetically implied and possibly influenced by the environment (e. g. face, iris, retina, finger, vascular structure etc.). Psychological characteristics are characteristics that are gathered or learned during time (e. g. signature, gait, typing dynamics, voice features etc.).

A biometric method is a set of procedures that are used to process biometric samples of a biometric characteristic in order to recognise the holder of the biometric characteristic.

A biometric model is a sample of a biometric person recognition system that facilitates the acquisition of information about biometric characteristics and the system itself. Such a model consists of methods for preprocessing and feature extraction, sample quality control as well as recognition.

A biometric sample is a measured quantity or set of quantities acquired by measuring some biological phenomena (in the broader sense of biometrics) or of some biometric characteristic (in the narrower sense) in space and/or time.

For every biometric characteristic particular patterns or structures exist that are used for the actual recognition process (e. g. minutiae structure and papillary lines for fingerprint, vascular structure on the edge of the eye for retina etc.). We shall call such structures patterns. There are also structures that are images of the actual patterns and are used in biometric methods to fulfill the actual recognition (e. g. elastic graphs of actual characteristics in elastic graph matching, eigenvectors in principal component analysis etc.). These structures should not be confused with biometric samples which are images of the actual biometric characteristic, while these structures are images of the actual pattern acquired through processing of a sample. Thus we shall call such structures extracted structures. There should also be a clear distinction between patterns and extracted structures. While the former exists as a fact the latter is obtained through an application of a biometric method on a biometric sample.

3. BIOMETRIC CHARACTERISTICS' ADEQUACY

To provide a framework for evaluation we used descriptive parameters of biometric characteristics [2] as well as corresponding evaluation criteriae shown in table 1. We developed an ontology-based computer model [8] in which every biometric characteristic was described through metainformation about its possible parameters.

Tab. 1

Descriptive parameters of biometric characteristics with corresponding evaluation criteriae

Parameter	Evaluation Criteria
Ease of collecting	If performance is important (especially time and cost)
Permanence	If the same users are going to use the system for a relatively long period of time
Measurability	If security and performance are important
Acceptability	If user's satisfaction is important (e.g. customers)
Deceptiveness	If security is important and there is a reasonable probability of eventual fraud attempts
Feasibility	If cost is important or if the organisation is very specific in terms of needs
Universality	If the system is to be used in lots of different situations (security, transactions etc.)
Uniqueness	If the number of possible users is potentially big and security is important
Sample cost	If the number of possible users is potentially big and cost is important
System cost	If the number of possible users is potentially small and cost is important
Database size	If the number of possible users is potentially big and performance is important
Environmental factors	If the system is to be used in lots of different situations (environmental, weather etc.)

These parameters are defined as fuzzy sets (high, medium, low). Its often the case that one cannot define these parameters exactly since they depend on different biometric methods that are used in a specific biometric system.

By evaluating a specific situation one has to have these criteriae in mind when analysing some situation's needs with regard to available biometric systems. Depending on the particular situation some of these criteriae will be more and some will be less important and so will the parameters in the evaluation query as argued further.

In order to perform evaluation one needs to establish an adequate metric to measure the adjustment of a biometric system with a certain situation. To do so we introduced the term ideal solution to be the set of possible biometric characteristics that fits best to the given constraints defined by a particular situation with regard to the knowledge that is implemented into the ontology. Since the

ontology is open this ideal solution is time dependent and dynamic with regard to current state of biometrics science. The distance of the ideal solution is the adequacy level of a given biometric model for a given situation and is denoted with the glagolitic letter ⱋ. The adequacy level is provided on a scale of 1 (ideal) to $C \times 3$ (worst case) where C is the cardinal number of the set descriptive biometric characteristic's parameters included in the ontology model. If this set remains constant than the scale has 36 levels of adequacy.

On the other hand biometric systems are usually evaluated using quality indicators including EER (Equal Error Rate), FAR (False Acceptance Rate), FIR (False Identification Rate), FMR (False Match Rate), FNMR (False Non Match Rate), FRR (False Rejection Rate), FTA (Failure to Acquire Rate), FTE (Failure to Enroll Rate), and ROC (Receiver Operating Characteristic). These indicators allow us to find an optimal model for a given situation in terms of security.

4. MODELING BIOMETRIC CHARACTERISTICS FOR ITS SECURITY

Due to the development of biometrics and its machine-supported implementation, biometrics is nowadays widely used, whether applied by popular or highly sophisticated electronics devices and equipment [4, 6]. Insufficient, or rather inadequate knowledge of biometric features or characteristics, which provide the basis of such systems, presents a major threat to all security systems, especially in ITS [3]. When developing a secure ITS it is necessary to observe guidelines which are intended to ensure development of a system secure enough to meet the requirements of the organisation, as well as the place and time it pertains to. This means that in such a system an ideal quality-price ratio will be implemented but there are other issues to consider as well. To accomplish a secure ITS, 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. Herein we introduce a new model of biometric systems for ITS that will allow for the choosing of the most adequate physical or behavioural biometric characteristic.

Although biometric devices rely on widely different technologies, much can be said about them in general. Fig. 2 [9] shows a modified general 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 inside the vehicle, while the subsystems signal processing, decision making and data storage must be located in an ITS centre.

As argued previously a major problem in this part is choosing the right biometric characteristics. Among characteristics to be used when developing a multimodal biometric system for a networked environment, the first category of features (according to the continuity) includes the characteristics used for uni-modal biometrics systems. In opposite to uni-modal systems multimodal systems possesses characteristics which are acceptable, fast, and easy for usage and implementation. Along with the features mentioned, several other should be analysed. Therefore the best way to display and overview of biometric features is by means of fuzzy sets. In a research we identified over 30 existing biometric characteristics having corresponding biometric methods whereby the set is very likely to be expanded in future research. Please refer to [1, 8] for an throughout discussion on descriptive parameters of biometric characteristics. The previously defined descriptive parameters are specified for each biometric characteristic using fuzzy variables high, medium and low.

The analysis of biometric features according to their characteristics can significantly facilitate the selection of biometric features. 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.

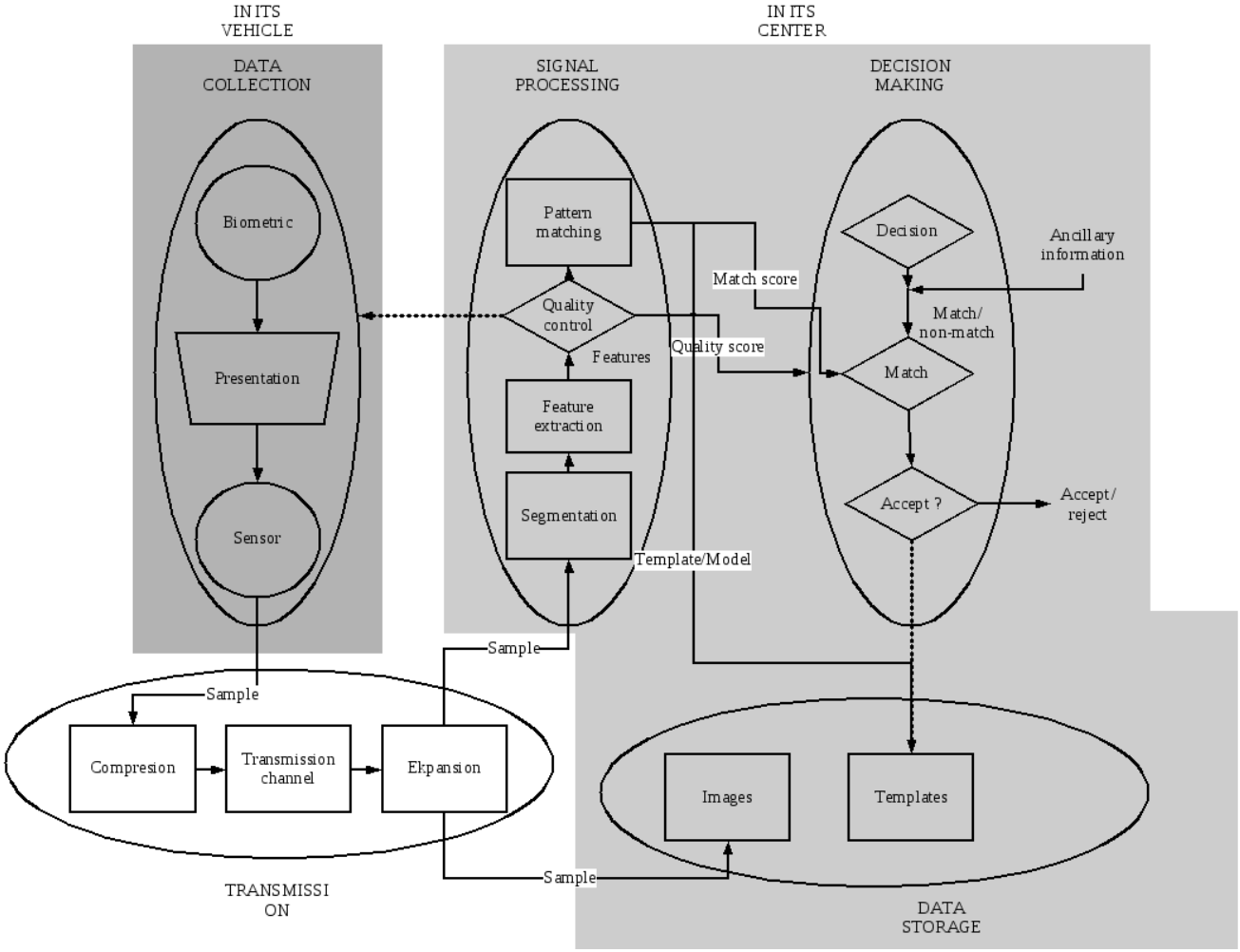

Fig. 2. Modified generalised biometric system model
Rys. 2. Zmodyfikowany model ogólny systemu biometrycznego

4.1. Goods' Safety

To acquire the best possible solutions for goods' safety in ITS (adequacy level as close as possible to $h = 1$) we need to provide a descriptor of requirements for a particular situation. These requirements have to be ordered by priority in order to identify an optimal solution. As seen from table \ref{tab-desc-char most important parameters for goods safety by priority include:

1. **Environmental factors** (low to medium) - since the system will probably be used in a wide range of different situations.
2. **Feasibility** (high) - since costs are important and the situation is special.
3. **Ease of collecting** (high) - since performance is important and the system will be used very often.
4. **Sample cost** (low) - since costs are important and the number of potential users is big.
5. **Deceptiveness** (medium to high) - since we want to prevent fraud and burglary.
6. **Universality** (medium) - since the number of possible uses is relatively big.
7. **Uniqueness** (medium) - since we want to increase security and the number of possible users is relatively big.

After evaluating these constraints in the ontology-based computer model we got the following results shown in tab. 2.

Tab. 2

Adequacy levels of characteristics for goods' protection

h	Characteristic
1	Finger
2	Handgrip
3	Palm
5	Keystroke dynamics
6	Face
8	Iris

As we can see the characteristics with the highest adequacy level are finger (h = 1), handgrip (h = 2) and palm (h = 3) which is expected. In protecting goods in an ITS we could thus use simple fingerprint and palm geometry scanners on the vehicles to provide a secure environment for goods. Especially the handgrip solution seems interesting since vehicles often have to be opened manually by hand. Thus, by establishing a hand grip sensor on the door handles, goods could be adequately protected.

4.2. Passengers' Safety

To establish a secure environment for the safety of passengers one needs to consider the following requirements ordered by priority:

1. **Acceptability** (high) - since we are dealing with customers.
2. **Uniqueness** (high) - since we want to increase security and the number of possible users is very big.
3. **Environmental factors** (low to medium) - since the system will probably be used in a wide range of different situations.
4. **Ease of collecting** (high) - since performance is important and the system will be used very often.
5. **Feasibility** (high) - since costs are important and the situation is special.

After evaluating these constraints in the ontology-based computer model we got the following results shown in tab. 3.

Tab. 3

Adequacy levels of characteristics for passengers' protection

h	Characteristic
1	Palm
1	Face
6	Thermogram
7	Gait
7	Head
7	Voice

As one can see the biometric characteristics palm and face have the most suitable adequacy level (h = 1), but the other obtained results should also be considered. These results imply that customers would be most adequately protected by using face or palm geometry scanners. Thermograms, human gait, 3D head geometry as well as voice seem promising, but are the current state a bit expensive technologies.

4.3. Data Safety

ITS data safety, the last but not least important factor of IT safety has to be considered through the following parameters:

1. **Measurability** (high) - data security is very important as well as performance.
2. **Deceptiveness** (low) - the goal is to reduce the risk of eventual fraud.
3. **Permanence** (medium) - there is a relative possibility that the same users will use the system for a longer period of time.
4. **Feasibility** (high) - cost is an important factor and biometrics in ITS security is a specific situation.

By issuing a series of queries we obtained the following results (tab. 4) from the ontology reasoning system.

Tab. 4

Adequacy levels of characteristics for passangers' protection

	Characteristic
1	Iris
2	Retina
2	Thermogram
2	Gait
2	Vascular structure

As one can see from these results the most secure biometric characteristics were chosen since we didn't specify the acceptability parameter and insisted on data security. This results implicate that iris and retina scanners, thermal cameras as well as gait and vascular structure imaging could be used for data protection in ITS systems.

5. CONCLUSION

In this paper we analysed a few aspects of using biometric systems in ITS to increase security. By using an ontology-based computer model we were able to obtain adequacy levels of possible biometric characteristics for such systems. These adequacy levels showed that the most adequate systems for goods' safety should rely on finger, handgrip and palm characteristics; passengers safety on palm and face characteristics; whilst data safety on iris, retina, thermogram, gait and vascular structure characteristics. Most of these features are physical, which was in a way expected since the improvement of security was sought. Only hand grip and gait characteristics are behavioral but they have special parameters that make them usable in ITS security.

As previous results shows, the decision about biometric characteristics depends on the particular situation. In three aspects of ITS safety we found various possible solutions. Maybe a good decision would be to combine various solutions into multimodal biometric systems in order to increase security (which is why additional solutions were presented).

These characteristics are only the first step towards biometric system implementation for ITS security, since other factors have to be considered as well. If we combine these results with existing quality indicators of concrete biometric systems we can ease this decision.

By using biometric technologies we can reduce the number of traffics accidents (K_{NS}) and thereby implicitly increase the passengers' (S_P) and goods' (S_G) safety. On the other hand the risk of unwanted event like fraud and burglary ($Risk$) is also reduced which implies goods' safety improvement. Biometric technologies increase data safety (S_D) on all three levels including confidentiality (C), integrity (I) and availability (A).

References

1. Bača M., Schatten M., Rabuzin K.: *A framework for systematization and categorization of biometrics methods.* In M. Bača and B. Aurer, editors, International Conference on Information and Intelligent Systems – IIS2006 Conference Proceedings, Faculty of Organization and Informatics, September, 2006, pp. 271–278.
2. Bača M., Schatten M., Tonimir K.: *Biometric characteristic's metrics in security systems.* In 1. Znanstveno-struna konferencija s međunarodnim sudjelovanjem, Menadžment i sigurnost, M&S. Hrvatsko drutvo inženjera sigurnosti, 2006.
3. Bača M., Čubrilo M., Rabuzin K.: *Using biometric characteristics to increase its security*. Traffic &Transportation Scientific Journal on Traffic and Transportation Research, 19(6), 2007, pp. 353–359.
4. Bigun J., Fierrez-Aguilar J., Ortega-Garcia J.: *Multimodal biometric authentication using quality signals in mobile communications*. In Proceedings of the 12th International Conference on Image Analysis and Processing, IEEE Computer Society Press, September, 2003, pp. 2–11.
5. Bošnjak I.: *Osnove prometnog inenjerstva*. Fakultet prometnih znanosti, Zagreb, Croatia, 2005.
6. Dieckmann U., Plankensteiner P., Wagner T.: Sesam: *A biometric person identification system using sensor fusion*. Pattern Recognition Letters, 18(9), 1997, pp. 827–833.
7. Kišasondi T., Bača M., Schatten M.: I*mproving computer authentification systems with biometric technologies*. In R. Sandri, M. Baranović, Željko Hutinski, and D. Čišić, editors, Proceedings of the 29th International Convention: Information Systems Security: MIPRO 2006, Croatian Society for Information and Communication Tachnology, 2006, pp. 166–171.
8. Schatten M.: *Zasnivanje otvorene ontologije odabranih segmenata biometrijske znanosti*. M.sc. diss., Faculty of Organization and Informatics, Varaždin, January, 2008.
9. Wayman J.L.: *Generalized biometric identification system model*. In Collected Works 1997 - 2000, San Jose State University, 2000, pp. 25–31.

Received 04.05.2009; accepted in revised form 13.12.2009