MIROSLAV BAČA, D.Sc.
E-mail: miroslav.baca@foi.hr
ŽELJKO HUTINSKI, D.Sc.
E-mail: zeljko.hutinski@foi.hr
KORNELIJE RABUZIN, M.Sc.
E-mail: kornelije.rabuzin@foi.hr
University of Zagreb,
Faculty of Organization and Informatics
Pavlinska 2, HR-42000 Varaždin, Republic of Croatia

Invited Paper
Section: Traffic Safety and Security
Review
Accepted: Dec. 15, 2005
Approved: Feb. 21, 2006

USING FACE RECOGNITION SYSTEM IN SHIP PROTECTION PROCESS

ABSTRACT

The process of security improvement is a huge problem especially in large ships. Terrorist attacks and everyday threats against life and property destroy transport and tourist companies, especially large tourist ships. Every person on a ship can be recognized and identified using something that the person knows or by means of something the person possesses. The best results will be obtained by using a combination of the person's knowledge with one biometric characteristic. Analyzing the problem of biometrics in ITS security we can conclude that face recognition process supported by one or two traditional biometric characteristics can give very good results regarding ship security. In this paper we will describe a biometric system based on face recognition. Special focus will be given to crew member's biometric security in crisis situation like kidnapping, robbery or illness.

KEY WORDS

ITS, ship, biometrics, face recognition, security

1. INTRODUCTION

Every day we are witnessing terrorist attacks, kidnapping or some other crisis situations. Like other Mediterranean countries Croatia is a tourist-oriented country. This means that the tourism insures most of the income. Different crisis situations, especially in the tourist domain (like ships, aircraft or buses), may have negative influences. Tragic terrorist attack in Turkey is maybe the best example. Most of tragic terrorist attacks in the past occurred on the ground (England, Turkey, etc.), but it is very obvious that large cruisers are ideal "victims". To prevent most criminal activities, and other activities which are not normal, we have developed a Multimodal Biometric Model (MBM) for ship security. This model has several functions: the first function is crew supervision, the second one is passenger supervision and the third function is criminal prevention in a general system of international police (or security) organization. However, criminals are not the only subjects who are capable of violating ship security. The cause could also lie in unusual behaviour of crew (alcohol, drugs, sickness, etc.). To avoid all these violations we propose MBM in multimodal environment.

2. BIOMETRIC MODEL

It is obvious that selecting the right biometric feature (or several) is a challenge. Most of the currently known and applied biometric features contain a flaw which makes them impossible to be considered ideal. Therefore, the question of adequate selection of biometric features, that is, characteristics such a feature is to consist of, needs to be addressed. Most commonly, biometric features have to meet the following requirements: universality, uniqueness, permanence, collectibility, accuracy, acceptability [8], 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 [13]. None of the currenly used biometric features meets all the criteria required for it 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 placed within a vehicle, while

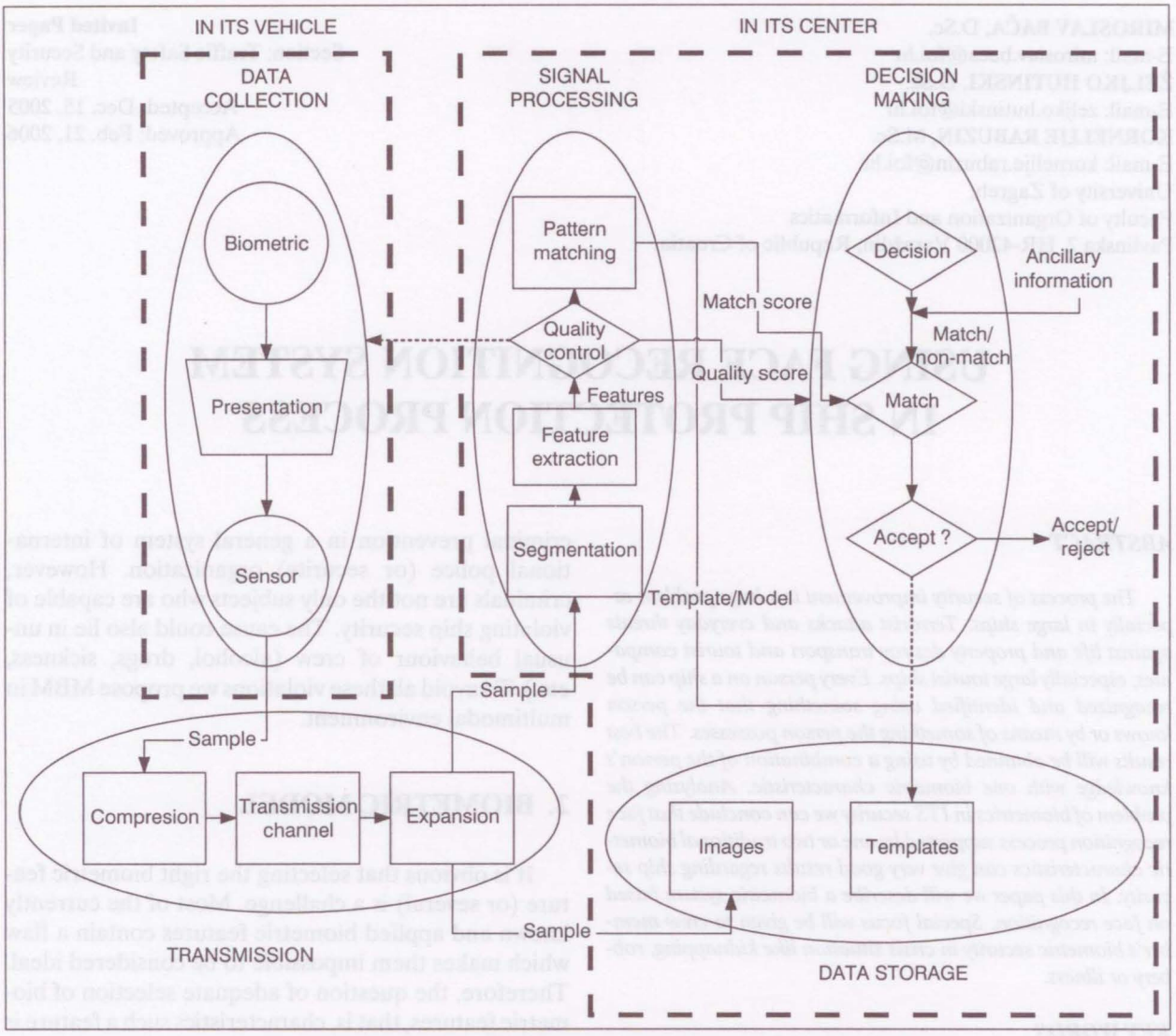

Figure 1 - Modified generic biometric model, according to [20]

other 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. This problem is not easy to solve. First of all, there is no single biometric feature appropriate enough to be considered ideal [10], [11]. 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 they should be used in strict accordance with the policy of a system they are supposed to secure [3].

When using biometric systems in ITS, we must insure untroubled and unobtrusive surveillance of employees and customers, as well as vehicles in transports. Besides, biometrics must provide appropriate answers in the fields of payment and security.

3. THE PROBLEM MODEL

The problem model must give directive for solving the ship security problem. There are three classes of problems which must be solved: the first one: Is a crew member really a member of the ship crew; the second: Is a passenger really a passenger of the ship and finally, the third one: Is anyone on the ship on the police (or security) wanted circular. The first two classes can be solved using some biometric method, and for that purpose we suggest face recognition method in combination with some soft biometric methods (only for the crew members). How can we choose the face recognition method? The answer is in Figure 2. Many factors are involved in selecting biometric, given some appli-

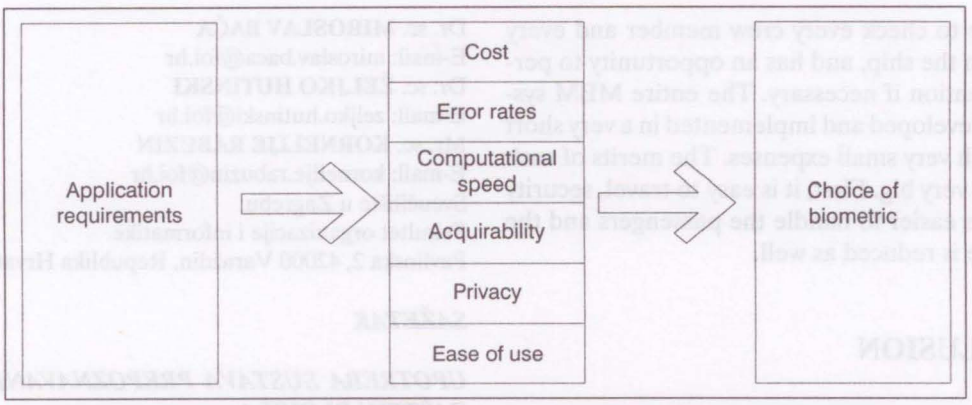

Figure 2 - Factors involved in the process of selecting the "right" biometric [5]

cation. The cost and security of the installation depend on the choice of biometric; therefore, selecting the appropriate biometric foe is of prime concern [5] for the application. Accordingly, accuracy is a very important factor in selecting a particular biometric, but it is not the most important one (shown in Figure 2).

The face recognition method is the most appropriate because we can use cameras and provide observation of the entire ship. It also means that we can use face recognition in the process of using of ship facilities (like saunas, rooms, pools etc.). In that way passengers can use all facilities without tickets, keys, smart cards and so on.

4. THE SOLUTION MODEL

The solution model depicted in Figure 3 uses biometric templates of all the crew members and passengers for the authentication/identification process. The solution model is split into three basic subsystems. The first subsystem is the ship biometric system. The ship biometric system must compare all the photos of the crew members and passengers with their template photos. This subsystem must classify persons in one of the three classes: crew, passenger and intruder. In the class crew the system uses some of the soft biometric measures (like blood pressures, height or weight). Using soft biometric methods is necessary because in the crisis situation an intruder can very easily replace the face, but if the system detects high (not normal) blood pressure, it can stop the ship. The ship biometric subsystem works in combination with port biometric subsystem. Port biometric subsystem inputs are all templates from crew, passengers from MBM (in the port of origin) and it performs checking at the end point to determine whether all the crew and passengers have arrived in the destination port.

The third component of the MBM system is police/security biometric subsystem. This subsystem coordinates the start and end port subsystems with the ship subsystem. The police/security subsystem has

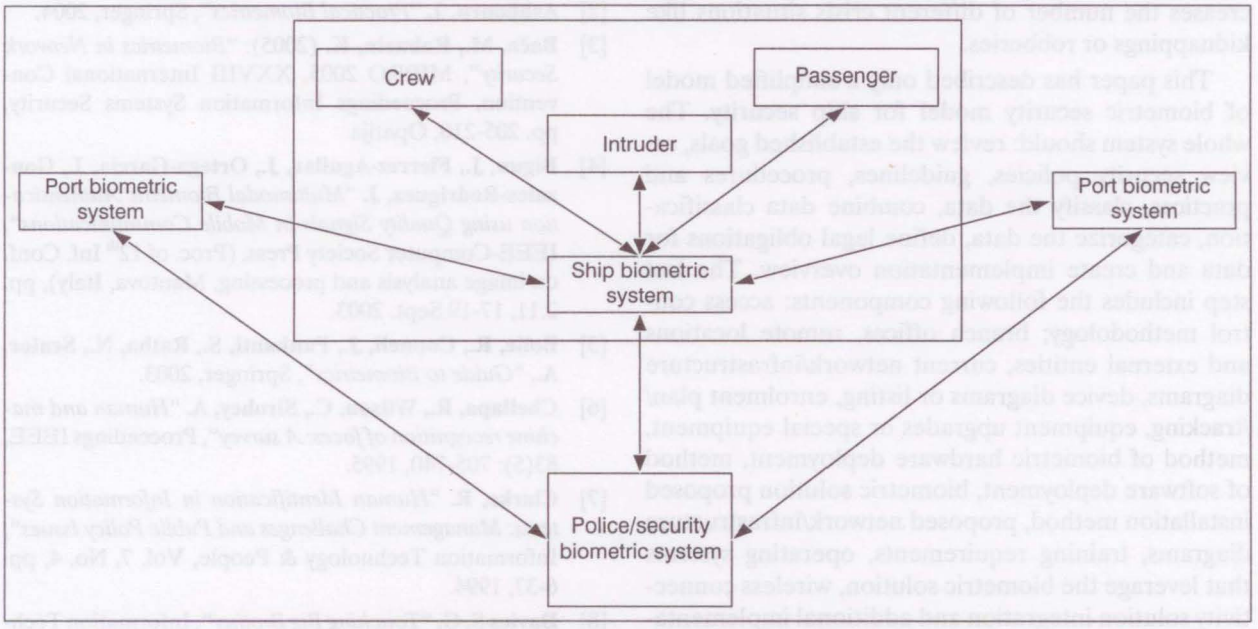

Figure 3 - Generic solution model for biometric ship security

enough time to check every crew member and every passenger on the ship, and has an opportunity to perform intervention if necessary. The entire MBM system can be developed and implemented in a very short time and with very small expenses. The merits of such a system are very big. First, it is easy to travel, security is better, it is easier to handle the passengers and the criminal rate is reduced as well.

5. CONCLUSION

Great fear of terrorism, kidnapping and other criminal activities has also big influence on everyday lives. Many tourists do not want to visit a country which is under terrorist attacks, and tries to find some peaceful location for vacation. To insure such a vacation, we propose a multimodal biometric system based on face recognition method which could be used on ships. Using this simplified model it is possible to insure the following goals:

- increase of general security on ships,
- increase of tourist comfort,
- decrease in the number of crisis situations.

The first goal is reached by connecting the subsystems. Every part of the entire system provides a certain security mechanism. In this way all the parts are connected into one system and security is rapidly increased. The tourist comfort like using rooms, pool, sauna and other tourist facilities is easier with biometric method (face) because passengers cannot "lose" their faces (but they could lose a ticket or a key). Implementing biometric features (face) in combination with some soft biometric features (blood pressure) decreases the number of different crisis situations like kidnappings or robberies.

This paper has described only a simplified model of biometric security model for ship security. The whole system should: review the established goals, review security policies, guidelines, procedures and practices, classify the data, combine data classification, categorize the data, define legal obligations for data and create implementation overview. The last step includes the following components: access control methodology; branch offices, remote locations and external entities, current network/infrastructure diagrams, device diagrams or listing, enrolment plan/ /tracking, equipment upgrades or special equipment, method of biometric hardware deployment, method of software deployment, biometric solution proposed installation method, proposed network/infrastructure diagrams, training requirements, operating systems that leverage the biometric solution, wireless connectivity solution integration and additional implementation plan considerations.

Dr. sc. **MIROSLAV BAČA**
E-mail: miroslav.baca@foi.hr
Dr. sc. **ŽELJKO HUTINSKI**
E-mail: zeljko.hutinski@foi.hr
Mr. sc. **KORNELIJE RABUZIN**
E-mail: kornelije.rabuzin@foi.hr
Sveučilište u Zagrebu,
Fakultet organizacije i informatike
Pavlinska 2, 42000 Varaždin, Republika Hrvatska

SAŽETAK

UPOTREBA SUSTAVA PREPOZNAVANJA LICA ZA ZAŠTITU PLOVILA

Proces osiguravanja sigurnosti vrlo je veliki problem, posebice kod velikih brodova. Teroristički napadi i svakodnevni napadi na život i imovinu uništavaju prijevozničke i turističke organizacije a samim tim i ekonomski napredak. Posebice se stoga to odnosi na velike turističke brodove. Svaka osoba na brodu može se prepoznati i identificirati prema nečemu što zna ili prema nečemu što posjeduje. Najbolji se rezultati dobivaju povezivanjem onoga što osoba zna sa onim što osoba posjeduje. Analizirajući problem biometrije u ITS sigurnosti zaključili smo da proces prepoznavanja lica potpomognut sa jednom ili dvije tradicionalne biometrijske karakteristike može dati vrlo dobre rezultate u osiguranju broda. Posebnu pozornost u ovom radu obratili smo spram ponašanja posade u kriznim situacijama poput otmice, pljačke ili bolesti.

KLJUČNE RIJEČI

ITS, brod, biometrija, prepoznavanje lica, sigurnost

LITERATURE

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

[2] **Ashbourn, J.** "*Practical Biometrics*", Springer, 2004.

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

[4] **Bigun, J., Fierrez-Aguilar, J., Ortega-Garcia, J., Gonzales-Rodriguez, J.** "*Multimodal Biometric Authentication using Quality Signals in Mobile Communications*", IEEE-Computer Society Press, (Proc. of 12th Inf. Conf. on image analysis and processing, Mantova, Italy), pp. 2.11, 17-19 Sept. 2003.

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

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

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

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

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

[10] **Diegert K. V.** "*Estimating performance characteristics of biometric identifiers*", Proceedings of Biometrics Consortium Conference, San Jose, CA, 1996.

[11] **Hong, L., Jain, A., Pankianti, S.** "*Can multibiometrics improve performance?*", Proceedings AutoID, NJ, 1999.

[12] International Security Homepage, http://www.security-int.com (27 Oct. 2003)

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

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

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

[16] **Nanavati S., Thieme, M., Nanavati, R.** "*Biometrics*", Wiley, 2002.

[17] **Panikanti, S., Bolle, R., Jain, A.** "*Biometrics: The Future of Identification*", IEEE Computer, Vol. 33, No. 2000.

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

[19] The Biometrics Glossary Page, http://www.eyenetwach.com/biometrics-glossary/biometric-terms.html (29 Oct. 2003)

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