# Face Recognition as an Airport and Seaport Security Tool

JYRI RAJAMÄKI, TUOMAS TURUNEN, AKI HARJU,
MIIA HEIKKILÄ, MAARIT HILAKIVI & SAMI RUSANEN
Laurea Leppävaara
Laurea University of Applied Sciences
Vanha maantie 9,
FI 02650 Espoo, FINLAND
*Corresponding Author*: jyri.rajamaki@laurea.fi, www.laurea.fi

***Abstract:*** - The transportation industries have been subjected to unprecedented scrutiny and regulatory mandates in the post-9/11 era. On the other hand, the inner border inspections were closed down in Europe with the Schengen agreement. Freedom of movement has brought new challenges to the authorities and transportation companies. Effective camera surveillance with a facial recognition system (FRS) could be a realistic solution. FRS requires camera(s) and a control device; a computer with special software. The software processes the material, face images, collected by the cameras. FRS has been used as monitoring and controlling tool in major events and border crossings. The aim of FRS is to maintain and improve safety and security in a cost efficient way by saving manpower. However, FRS is an additional security tool and therefore not to be trusted only. FRS is being used mainly as a verification method where the human face functions as an access or pin code. Optimal operational environment for FRS is a dry environment with stable illumination; most likely indoor environment is needed to guarantee the operational ability. Images of the faces should be collected in close distance and the persons, who are to be identified, should cooperate. FRS is composition of technical elements and applications which are commonly used in everyday life. Profiling the environment and setting reasonable aims, FRS could be used in various places. Hence FRS is challenging the traditional methods as a sophisticated security tool for the sophisticated situations. So far, the only operational FRS in Finland started in summer 2008 at Helsinki-Vantaa airport. This paper examines and collects experiences from the airport pilot project, from literature and by interviewing experts of the security and facial recognition field. The aim of the paper is to specify the desired goal state, how FRS could be applied as a new seaport and maritime security tool.

***Key-Words: -*** Camera surveillance, Crime prevention, Face recognition, Facial recognition system, Maritime security, Port security.

## 1 Introduction

Administrating and processing information has been developing fast in the past decades. The human face as a digital image is much easier to produce and to treat compared to the situation in the last century. Digital cameras have replaced traditional photographic methods. The internet is expanding continuously, giving more possibilities to produce and to transmit information. The quality (text, voice, and image) of information is finding new paths and possibilities based on services provided by the network. E.g. webcams allow us rather easily to send live images and communicate currently. Cellular phones are taking over the market of the land line phones globally. Today, a cell phone with a build-in camera might be more common than the regular ones. We are able to use the GSM technology in image processing as well.

Besides the virtual reality, travelling in real world has increased. Transportation connections and the ways to travel are improving all the time. International agreements, such as the Schengen agreement, are extending the freedom of movement. The borders and the border procedures discontinued which has also given possibilities for the organized criminal activity and terrorism.

As a counter measure for this, the authorities all around the world are forced to improve the security procedures and the quality travelling documents, such as passports. One improvement has been the biometric identification method. The biometric

identifiers are stronger than the regular ones like the name, date of birth or the serial number of the passport. Most common biometric identifiers are the face, the finger prints and the irises. The human face as a digital image is in common use both in commercial and official procedures today.

When new EU members from the Eastern part of Europe joined the Schengen agreement in 2007, the inner border inspections were closed down. This meant that e.g. the Finnish Border Guard no longer observed and controlled the traffic at the seaports of Helsinki. Freedom of movement has brought new challenges both to the authorities and the privately owned companies (shipping companies, expeditors, passenger and cargo transportation etc.) in the port environment. Without regular border inspections, the criminals and the stolen goods are more easily moved from one country to another. Most likely, the level of active monitoring of public peace and security has decreased, and alternative monitoring and controlling methods are needed. Effective camera surveillance with a facial recognition could be a realistic solution. [1]

The authorities in Finland and Estonia are improving their cooperation against the organized crime groups' activities like smuggling of drugs and human beings. The Estonians have a very strong role especially in smuggling of amphetamine. Before Estonia joined the Schengen agreement, about 1500 persons were arrested and 200 deported at Helsinki and Tallinn seaports. Now when there are no border controls between Finland and Estonia, one of the key elements combating organized crime is criminal intelligence. [2]

Recently, a discussion among the Nordic countries about cooperation against international criminal activity has started. According to the Nordic Council enquiry, four out of five persons thought that crime prevention against border crossing criminality is one of the most important issues in the Nordic countries today. The secretary of the Nordic Council states that politicians should focus on this issue as well. [3]

Seaports are critical components of the global transportation infrastructure but before the terrorist attack of September 11 they have not been subject to comprehensive governmental regulation and security oversight [4]. The ports can be seen as "bottle necks" to other countries. E.g. containers after containers are being shipped and then forwarded to the inner parts of Finland or to the neighbouring countries. According to [8], crime against the transportations on the road is thought to increase in the future. This is just one example why we should focus on the security at the harbours. To keep the harbour safe is not only a local issue - it is also important at national and international levels. Today, the government of Finland has a productivity plan which means cutting down man power from the police, the border guard and other governmental agencies. However, we are getting more and more international which means new issues to be taken care of and new challenges how to maintain our security. New kinds of investments are needed in order to maintain the security. Facial recognition system (FRS) could be one solution.

This paper maps relevant the expertise on the scientific and technical issues related to facial recognition. Experiences are collected from FRS operating already today. With studying these facts, the paper provides the possibilities, how to adapt and implement FRS in a real environment. If and when a reliable and cost-effective FRS can be build, it could lead the way to launch the system as a common security tool at airports and seaports.

## 2 Research Methods

The subject of this study is a new innovation; the creation of FRS as a new seaport and maritime security tool. So, it is obvious to use the design-science research approach, described in [5]. In this study, the following sub-concepts of design-science research are applied; (1) evaluation of constructive results and (2) action research. Within the first sub-concept, the main goal is to evaluate, how FRS function as a border security tool at Helsinki-Vantaa Airport. Within the second sub-concept, the building and evaluation processes are combined in action research (Fig. 2) and a new seaport and maritime security tool is developed. Data is collected by using several methods; such as reviewing literature, by interviewing people and observing systems.

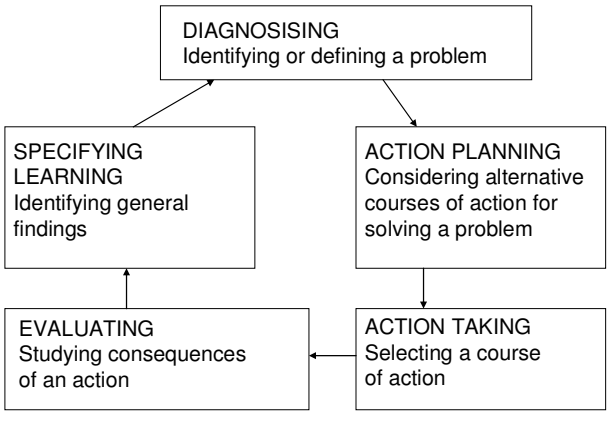


Fig. 1 Cyclical process of action research [5]

# 3 Facial Recognition Technology

Face recognition is something that human mind seems to achieve with ease. Achieving similar results with the computer based systems has proven to be difficult. Yet, nowadays more and more applications are marketed with different recognition capabilities. Machine learning systems are used for posture recognition with high recognition rate [22]. Manufacturers of digital cameras, camcorders, security surveillance products etc. claim that their products recognize for example faces and smiles and operate accordingly. How is it done and how can more sophisticated systems work with more crucial demands of accuracy of recognition? The potential for face recognition is considerable for example in the field of security and its different branches.

Development in today's technology is advancing fast. Many things were displayed in science-fiction films in the 70's are reality. Today, we are facing the situation, where people are being identified by their biometric features on several locations; e.g. in harbours, airports and government facilities. Face Recognition has advantages over other biometric technologies: it is unobtrusive and easy to use. [9]

The research of facial recognition is very popular all around the world. Although the facial recognition has been an interest of research from the 60's, the research work and the technical development have speeded up in 1990 – 2000. [10-11] Development has been so fast that the failures and errors in the systems have been decreased down to 10%. At the same time, capacity and performance have increased. Especially, collecting and processing the face expressions and features and categorizing the human faces have hugely developed. [11] In Finland, FRS has been researched for about five years and worldwide more than ten years. Facial recognition is a growing study field, because of the political pressure e.g. in the US and UK. [12]

Face recognition has a large number of different kinds of applications, mostly security related [9]. At the moment, face recognition is one of the primary biometric technologies, in development. This can be seen not only airports, but also in digital cameras, laptops and mobile devices. Human face plays an important role in our every day life and communication. A human can interpret facial impressions and determine rather quickly several factors of another person. Face can reveal gender, age, race, mood and several other factors to other person. For humans, interpreting them is natural.

Face can be considered as a unique class of objects. Facial anatomy contains structures that are always configured similarly. Even though the faces are formed in a similar way we can distinguish people from facial appearance alone. It is quite easy to identify a person from a static photograph. In a real life situation, we spend much more time evaluating the context and the surrounding environment. In real life, several other factors are also involved such as movement, illumination conditions, other objects and the pose of the face. The main object of artificial face recognition is to create such algorithms for dynamic vision and learning machine that they can operate efficiently in poorly controlled and changing environment [13].

FRS needs to identify automatically faces presented in pictures and videos. According to [9], FRS can operate in two modes: (1) Face verification (authentication): a query face is compared against a template; face whose identity is being claimed; or (2) Face identification (recognition): a query face image is compared against all the template images in the database. Variations of these two can be made e.g. a watch-list check, where a query face is matched to a list of suspects (one-to-few-match).

There is no formal definition for facial recognition. Facial recognition can be described as a system, which makes conclusions by detecting the human face from the camera footage and then comparing faces with a certain algorithm to the information from the database of faces. Generally, facial recognition can be divided to the facial recognition and verification. Face recognition aims to find out certain person from the image/material and the goal of the verification method is to confirm that the person is who s/he claims to be. [10-11] The scientific definition of FRS is not unambiguous. FRS can be divided in two different categories (recognition and verification), which are also the main areas of research. In the recognition method a chosen, e.g. wanted, person needs to be recognized from the crowd. Digital image of this person has to be stored in database in order to make comparison from the material. In the verification method, the human face works as a pass or pin –code. The right face allows the person to access the restricted area controlled by FRS. According to [12], most of the systems are based on the verification method.

## 3.1 Verification method (authentication)

The verification method is more controlled system compared to the identification (recognition) method and therefore also more reliable. Under the verification, the person's picture is stored in the database and the comparison is made only between the person and the image in database. The

environment is controlled and semi-public (like airport); usually the verification is conducted indoors, where the illumination of the area can be controlled more easily. Facial recognition could also be used as a verification method between a person and a machine, like logging in to the computer and by this the PC would open just for the right person. FRS should be seen more like an additional asset for the security. [10-12]

### 3.2 Identification method (recognition)

Recognizing a person from the facial appearance alone presents several conflicting factors which make the task more difficult. Ref. [13] divides the changes of facial appearance in to two factors, namely intrinsic and extrinsic. Both are to be considered when implementing face recognition. Intrinsic factors in facial appearance include e.g. identity, facial expression, speech, sex and age. Extrinsic factors in facial appearance include viewing geometry, illumination, imaging process and other surrounding objects. Typically, the appearance of the face varies depending on the illumination and shadowing. Other objects which may be present in the image may cause occlusion and shadowing. The most significant factor still is posing. The other significant factors include motion and colour, detecting faces in cluttered scenes and tracking changes of the face. [13]

Although face recognition is extensively studies in the last decades, there are still unsolved problems for uncontrolled conditions, such as changes in illumination, pose, facial expression, facial texture (e.g. wrinkles) and shape (e.g. weight gain or loss), facial hair, presence of partial occlusions (e.g. glasses, scarf) and age progression [6, 7]. According to [10], today's most problematic issues in the facial recognition are the question of illumination and person's unwillingness to co-operate. The poor illumination is the most common problem, but also rapid changes on lightning conditions causes problems; illumination conditions ought to be stable [10]. Usually people do not want to be photographed and controlled, so the identification of one certain person from a crowded, uncontrolled area does not work properly today (the watch-list dilemma). Also, the cameras can still be fooled by using a makeup, growing a beard or changing the hairstyle. Because of these problems in identification, the research in Finland is more concentrated on the verification method. [12]

### 3.3 Face Recognition Processing

One key point to be perceived is to determine what the relevant information to the perception of face is and what form of representation enables such information to be extracted from faces needed to recognize. Such information needs to be represented in a form that can later be used for efficient matching of input. [13] Fig. 2 shows the face recognition processing flow.

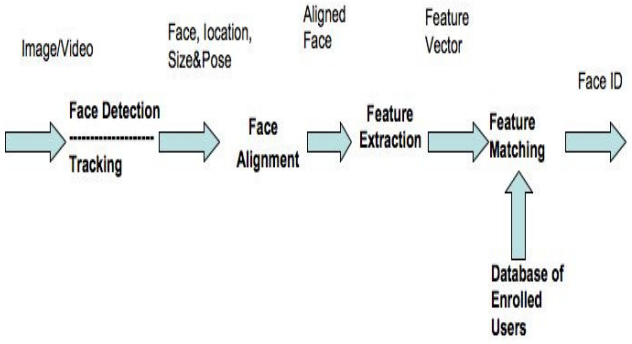


Fig. 2 Face recognition processing flow

Face is a three-dimensional object subject to varying in illumination, position, various expressions (such as sorrow or anger). Detecting the face itself from the background is called face detection. If the face is detected from a video, a face-tracking component is usually needed. [10]

The face needs to be aligned in most cases. The purpose of the alignment is to achieve the best possible circumstance for identifying the face. Eyes, nose, mouth and facial outline are called facial components. The face image is made from geometrical properties, such as the distance between eyes, size and pose, by using geometrical transforms or morphing. In addition, the image of the face is modified by the program so that the photometrical properties are best available for FRS. This means adjusting the illumination and grey scale of the image. [9]

The next phase in the face recognition processing is the feature extraction. This is done to provide the needed information to distinguish the different faces from each other. This is conducted by comparing geometrical and photometrical variations. Each face has its own feature vector or algorithm. This algorithm is compared with the faces in the database. The result is either a found match with a sufficient confidence or an unknown face. The result of FRS process depends drastically on the features that are extracted from the video or other surveillance-method. [9]

Some studies compare the recognition between a machine and a human. Artificial facial recognition is more reliable than human recognition when the face detected is unknown to the human detector. Vice versa, the human detector is much more reliable when the detected face is familiar. [14]

Naturally, we are able to recognize another person in disguise (but known to us) better than the computer. We could recognize the person even from a far, e.g. from the way s/he walks. On the other hand, the computer could be better in comparing and recognizing huge masses of faces which are totally unknown or strange to us, e.g. faces of African or Asian origin. [12] Compared to the human watcher, the computerized FRS is capable to cover wider areas. The machine guard is also tireless observer unlike its human counterpart. [11]

FRS can be conducted by using either two dimensional (2D) or three dimensional (3D) techniques. When the 2D system is used, the pixels in the picture are compared with the pixels from another picture taken by different cameras. The more stable the environment (e.g. illumination), the more reliably the recognition can be conducted. [10] In addition to photographs, also radiographs and craniometrists can be used as a template to build up 3D models. Multiple images are aligned using cranial characteristics as reference points from which the 3D model is being build by the computer modelling software. [15] Craniometrists is a technique where the skull bones are measured.

The best way of representation is a 2D appearance based model. The 2D coordinates of a point on a face at an arbitrary pose can be represented as a linear combination of coordinates of the corresponding point in a set of 2D images of the face at different poses provided that its shape remains rigid. These different views span the space of all the possible views and form a vector shape. The shape of the face can then be represented by selecting sufficient number of feature points on the face. Due to self-occlusion more views of the face are needed for effective representation. However, if sufficient 2D views are given, 3D image can be constructed. [13]

3D technologies are based on geometry; the human face is 3D. The illumination is the key element, because the 3D model of a human face is build up by the reflections of light from the human face. This sets demands to the operational environment of the cameras; illumination needs to be under control. The person has to cooperate also; otherwise the detection and saving the image of human face is very difficult. 3D modelling can be conducted with one or several cameras, which could help to gather the material for the model in case the person is not cooperative. 3D facial recognition is more accurate than 2D technologies, but also more expensive. The advantage of 3D is, however, that it could be adapted to the 2D environment. Some programs are able to use 2D material and build up 3D models. [10-11]

To build up a 3D image is a hot spot of research today. A problem is that the comparable pictures are usually taken only from the front, e.g. like passport photographs. However, the shape of the human face is 3D, so the features of the face could change radically in other positions. To build up a 3D image, images of face or head from different angles have to be collected. Also video material where the head is turning could be enough to build up a 3D image. Theoretically speaking, the quality of the video material does not have to be excellent if there is long enough footage available. 3D systems are much harder to pass or fool. [12]

# 4. FRS at Helsinki-Vantaa Airport

About 90% of Finland's international air traffic goes through Helsinki-Vantaa airport. Statistics in 2007: 13.1 million passengers, 180 000 takeoffs & landings, 30 airlines, 3 runways and 2 terminals. Finavia is a state-owned enterprise which maintains a network of 25 airports in Finland; Helsinki-Vantaa being the principal. Border crossing at the Helsinki-Vantaa is been monitored by the Finnish Border Guard. According to [16], the aim of the pilot FRS project in Helsinki-Vantaa is to test the system and ensure that it is able to reach its goals and fulfil the demands of the environment. The goals are mainly set by the Finnish Border Guard, while Finavia has concentrated to planning and building up the system. Finavia sees that FRS is a modern tool for modern environment. Besides as a security tool, FRS indicates that Helsinki-Vantaa wants to use improved and latest security methods to develop the airport environment. Based on the results of the pilot project, acquisitions are being made at the beginning of 2009. [16]

Lot of different FRS suppliers and technologies are available on the market. FRS is mainly used as an access control system in industrial branch and business world. The British police have probably the best systems today and police organisations are using FRS controlling huge public events and public places generally. Cameras are scanning the crowd and comparing the material to the database of wanted persons. However, only a few suppliers provide systems which meet the requirements of the Finnish Border Guard. A European supplier was

chosen, because they have already built up systems in several countries and their system seemed to best fulfil the needs of the Finnish Border Guard. [16]

With most FRS, a pre-registration is required, meaning that the system could be used only by the persons who have registered and probably paid a fee to use the system in their favour. When registered to the system, the person (a client) receives a pass card, based on e.g. smart card technology, and only the pass card holder can use the system. Trustedtravell program, used at Schiphol airport in Netherlands, is an example of this kind of a closed system. It is available for everybody, but the membership to the program is chargeable. The boarding and border control procedures are simpler to members; no queuing etc., compare to regular travellers. However, The Finnish Border Guard wanted an open system to Helsinki-Vantaa, where neither special fees nor registrations are needed. Also, the system should be based on a biometric passport, but that raises the issue that everybody does not have a biometric version of a passport. Biometric passports shown in Fig 3 are mainly used in Western countries, whose citizens are usually so-called low-risk passengers, and higher risk profiled passengers have to be inspected traditional way.


Fig. 3 Biometric passport

Assessing the risk, there are three requirements when entering Finland: (1) the person has to have a valid travel document; (2) the person has to be who he claims to be (verification), and (3) the person should not be a threat to a society, apprehended etc. With FRS, all these aspects could be covered. Automated border inspection checks the validity of the travel document and makes comparison between the images of passport holder and biometric data. Threat assessment is conducted by register check up.

The experiences from abroad shows that FRS based border inspection procedure is simple, fast and user friendly [16]. According to the experiences, persons who have used this procedure are willing to use it again. Based on the passenger interviews, automated procedure is mostly welcome, because they are able to conduct the inspection procedure by themselves independently. Within the Helsinki-Vantaa pilot project, nobody is forced to use FRS procedure; every passenger can choose whether to use the traditional procedure. Fig 4 shows the FRS gates which are in use at Helsinki-Vantaa Airport for the meantime.

FRS at an airport requires a certain level of illumination. The environment needs to be controlled, most likely by adjustable, artificial illumination and structural modifications in the environment.

Fig. 4 FRS gates at Helsinki-Vantaa Airport

The strength of FRS is that the system is very hard to fool with beard, getting/losing weight, changing hair style or using eye glasses. System is hard to bluff, because it measures certain unchangeable parameters from the human face. The parameters of nose, ears, upper lip or mouth are the same, unless the person has gone through a massive plastic surgery operation. On the other hand, some factors could always disturb the system, no matter what.

The reliability and functionality of FRS at Helsinki-Vantaa is in a good level, because the airport provides optimal environment for the system, such as proper illumination, dry indoor facilities and conduct facial recognition possibility to photograph persons in close distance. Still, some open questions should be answered: Could minors use the system alone or should they go through the procedure with their parents or other adult person? What could be a proper age limit to use the system? How to deal or maintain the control in case of a run-away or

kidnapped child? Also, low experiences about identical twins are available.

## 4.2 Border Inspection Procedure

FRS is been used as an automated border inspection system. The system is meant to be used by EU citizens who has biometric passport. Biometric information, like the face of the passport holder, is stored to a chip.

The border inspection is a two step procedure. The passenger sets the passport in to the chip reader as shown in Fig. 5. The reader collects the information from the chip in order to detect whether the passport is valid or forged. A register check is also conducted to discover possible apprehended persons. This detection stage takes about five seconds.

Fig. 5 Placing the passport to the reader

If everything is okay, the passenger enters to the second stage where the system conducts face inspection (facial recognition) of the passport holder. In the facial recognition stage the passenger has to look in to the mirror, as illustrated in Fig. 6. A camera that takes a photograph from the face is behind the mirror. The system conducts an image comparison between the taken photograph and the image from passport chip. The detection system calculates mathematically measured points from the human face. If the faces match each other and the register check is clear, the border inspection is conducted and the passenger is allowed to enter Finland.

Hats, scarves and sun glasses cannot be wore when facing the mirror to be photographed. All these detail are instructed during the procedure. In all the instructions for the facial detection are quite simple; the person has to face front. Indications are set onto the floor; how to position the feet and which direction to look. According to the supplier, it is much easier to face the mirror than the camera. Therefore a mirror is been used.

Fig. 6 Recognition compares the face with the image from the passport chip.

While the passenger is following the instructions, the procedure is been monitored by a border guard. All the information, both personal data and the photographs, are available also to border guard. This gives the possibility to conduct more detailed border inspection if needed and keeps the overall control of the procedure in human hands. According to [16], one border guard could monitor and control five FRS lines which give the possibility to relocate manpower. User experiences form Portugal e.g. shows that seven lines are too much for one person.

Previously the Finnish Border Guard has had a similar project concerning facial detection. In this project plan the cameras were located above each border inspection booth and the image comparison was conducted in the very same booth were the manual border inspection is been conducted today. By that time proper software was not available, so the detection could not be conducted. The cameras do exist already and in the future there a goal that FRS could be operational in a regular environment instead of a specially built line.

## 4.3 User Experiences

In first two months little bit more than 2000

passengers has used FRS. This is a rather small number compare to the overall amount of the passenger at the airport. FRS is still an optional way to go through the border procedures and the passengers are not aware of the existence of this system. Also the system is not located where the heavy crowd is moving. The Finnish Border Guard and Finavia will have an awareness campaign in autumn to boost the system among the passengers.

Failures have appeared because of several reasons. First, the passengers have not known that a biometric passport is needed in order to use FRS procedure. Old passport terminates the procedure from the beginning. The passport has been put up side down to the reader or then again the passenger has not been patient enough to wait the reader to scan the passport. Passengers have also misunderstood the facial detection part and they have tried to show the passport picture to the mirror (camera). In some cases, the passport has been in poor condition or the chip has been damaged, which means that FRS procedure has been impossible. The impostor method is one of the most common methods of illegal entry. In the impostor method the person is using a genuine and valid passport, but it does not belong to him. The person is relying on the resemblance of the real passport holder. FRS has detected one impostor case in two months period.

After two months, only one camera has required maintenance. The contract includes technical support in the first six months, where the supplier comes to repair all the defects if necessary. The average cost of one reader is 5k€. Also some modifications needed to be done in the environment which has incurred expenses.

The illumination has been a key factor in the functionality. The sun has caused problems in certain times a day; time to time there has been too much light. Curtains have been installed as a temporary solution against the influence of the sun.

### 4.4 Why Facial Recognition?

According to the ICAO standards, the basic biometric identifiers are the face, the fingerprint and the iris. Each member state can choose their method of identification; they can e.g. choose all three. Most of the member states have chosen the face as an identification method, because it is the easiest and the most convenient compare to the other methods. The development of the fingerprint method is however in progress as well. According to [16], the iris would be the best method because of its accuracy. The problem is, however, that it is not user friendly; the process of recognition is slow and also unpleasant to the customers.

Facial recognition is only one solution among various control and inspections methods. It should not be the one and only method when conducting inspection and control manoeuvres [16]. Passport holder's fingerprints are going to be stored to the chip as well in 2009. Because of this, The Finnish Border Guard is going to invest for the fingerprint scanners to the airport. In future the recognition will be based on both the face and the fingerprint. Today, 15 % of the Finns have new biometric passport. Within the next eight years everybody will have a biometric passport, because the last old version passports issued in 2006 will be expired. Quite soon, Europeans want to use the automated line instead of the traditional one [16]. One of the key issues for this is that it takes only approximately 15 seconds to go through the procedure.

Biometric identification seems to be the global recognition method in the future. This could mean that the technology will be developing, providing perhaps better tools to store and process information. The more common the system, the less expensive it could become. Current experiences indicates that the facial recognition is in deed probably the most discreet method today, not forgetting the possibilities of the fingerprint method. When considering biometric identifier to be stored to a travelling ticket, the facia recognition could be the better method compare to the fingerprint. If a person, a passenger, can provide the face image by him/her to the ticket by using e.g. own basic digital camera, to produce the ticket with proper data in it would be much easier and flexible because the fingerprint scanners are not every mans tool.

## 5. Port and Maritime Security Tool

### 5.1 Facial Recognition Technology

FRS is challenging traditional security tools. Common security tools and principles could be used. The question is where and how to use it. We do not have to build up the system from the scratch. We can use the experiences and technology of the existing system and modify them to another environment.

The structure of FRS is basically quite simple; several cameras and a database are needed. The cameras are monitoring the area of responsible. The database is controlling the cameras and it works as a detecting & alarming system in case of a disinformation fed by the cameras. Like the general camera surveillance system, FRS should be seen as an additional security & monitoring measure, not to

be trusted solely. With FRS, a large area can be covered and the monitoring & controlling can be conducted discreetly.

Generally, FRS can be divided to identification method and verification method. In identification method the human faces are "scanned" from the masses of people. Scanning is based on a database of faces (e.g. persons under warrant). The technology is still developing and there are no reliable experiences of this method today. Verification method is based on comparison of one person to the picture of database; the human face works as an access code. Hence the verification method can be seen as a simpler procedure to conduct compare to the identification method. In Finland, FRS is applied at Helsinki-Vantaa airport. The system uses the verification method and a chip card (smart card) technology which is commonly used in Finland.

Today, the main challenges are costs and reliability. Because of the sophisticated and unknown nature of FRS, equipment and software are still relatively expensive. The main obstacles for the reliability are poor illumination conditions and lack of collaboration of a person under detection. The verification method at Helsinki-Vantaa is operating with persons willing to co-operate (the passengers) and in indoor environment (the illumination can be controlled). Also, several universities in Finland are studying applications of facial recognition and having a research co-operation with other universities abroad. The experiences of the Helsinki-Vantaa pilot project and the domestic know-how should be seen as an asset when planning and building up FRS in Finland.

## 5.2 Access Controls in Port Security Management

Port security management provides authorities and maritime industry professionals; such as port operators, employees, users and stakeholders, with a basic awareness and understanding of security management in the port facility environment. Port security is a risk management activity and in the business of security, the risk management process begins with understanding the target environment as being fraught with risks that must be identified, assessed and managed. E.g., ports are an attractive target for terrorists and criminal conspiracies due to their high role in national and local economies. Therefore, developing of comprehensive port access control systems and protocols is important. The two major components essential to comprehensive port access control are: (1) identification and credentialing, and (2) restricted-area access controls. The first one provides seaports with a systemic way to identify and control who has authorization to enter a seaport; the second one comprise physical infrastructure physical infrastructure, procedures, systems and guidance for screening, monitoring and controlling access into the facility. The primary methods for restricting access are to identify unauthorized persons before access is granted and to conduct screening activities during access. [4]

## 5.3 Biometrics and Chip Card Technology

Biometrics refers to methods for recognizing a person's identity. Identity can be established e.g. by means of face recognition, fingerprints, voiceprint identification and/or a scan of the iris of the eye. The aim of biometric passports is to make travelling safer and smoother. They will improve international security and contribute to fighting terrorism and illegal immigration. However, the aim is not to raise the general level of control but rather to focus control more carefully than before. [17]

The chip card (smart card) technology is in common use today. FRS in Helsinki-Vantaa airport uses the chip card technology. Persons under detection provide their passport (including chip card) to the inspection. The digital image of face in the chip card is been compared to the real person at FRS gate. Why do not use similar technology also in port and maritime security?

For port and maritime security professionals, adapting existing access control systems to biometric chip card readers able to read individual biometrics and media across a spectrum of port environments requires considerable analysis by port security. Chip card readers must be installed at all locations where all employees and passengers (pedestrians and vehicle occupants) have ready access to biometric reading devices. Access control system may enable pedestrians and vehicle occupants to present their biometrics (e.g. faces, fingerprints) and chip cards without interacting directly with a human gate operator. Access-point architecture and system design must balance cost, efficiency and gate throughput time against risk assessments and security concerns. Also, portable or handheld reader devices may be used in different locations or for vehicles with multiple occupants. The placement of computers and cabling within existing or planned security gatehouses should be based on available space and competition with electronic routing requirements. Gatehouse space constraints and current operational requirements are key factors in considering the purchase and installation of new access control systems. Outlying

or temporary port access gates may have no power or connectivity between chip card readers and servers. [4]

## 5.4 Case Viking Line

Viking Line Ltd, owning seven vessels sailing at Baltic Sea, has 5.7 million passengers per year which means about 16,000 passenger and 1,500 vehicles per day. On board, the security staff consists of 3-5 persons and the surveillance camera system of approximately 60 cameras. The purpose of the cameras is to support the crime investigations (thefts, sabotages etc.) and to monitor the public safety. [18]

Tickets could be bought without any recognition of identity and passengers can enter the ship without verification. According to [19], there are no legislations concerning personal control, luggage inspections and identity card requirement prior boarding in the Baltic Sea region today.

Although there are no clear guidelines from the authorities, the captain however should know all the persons who are on board [20]. In this kind of situation, an organized and reliable verification system should be build up. FRS could be a monitoring and analyze tool both for the ships security and the captain. In the next two sub-subsections, the suitability of FRS is demonstrated by reviewing the terminal and ship environments. However, applying of FRS at vehicle entrance situations is not studies.

### 5.4.1 Terminal Environment

Fig. 7 Current Magnetic Card Gates at Viking Line Terminal.

Today, pedestrian passengers are using magnetic card application (see Fig. 7) and the employees like cleaners regular, credit card size plastic access cards with a photograph in it. There is no guarantee, that the holder of the card, who is entering the ship, is the person who he or she claims to be. Comparing e.g. to the access card (with a photograph) system, FRS has several usable and safer possibilities. With regard to access cards, all employees must carried a card, but it could be lost and used by another person, or be forged; the holder of the card could only be recognized in close distance; the security system for the cards has to built and maintained (like FRS as well); and when the person no longer has rights to use the card, there is no guarantee that the card is returned safely. When looking at FRS, extra gadgets, items or issues (access cards, tags etc.) are not needed; minimize the lost, misuse and forgery of the identification item; the person can be identified discreetly, safely and probably from the far distances; by identifying from the far distances, larger areas can be monitored and controlled; the human face can be a flexible identification method in huge organizations including different buildings, cities, countries, continents etc.

The current gates could easily be replaced by facial recognition gates and a similar FRS to at Helsinki-Vantaa airport could be applied. Passengers would need to identify themselves with a proper document with a chip. They are cooperative because they want to travel. Also, employees should use access procedures and FRS gates before entering restricted-areas and on board. There must be zero tolerance for violators. Passengers and employees who refuse to follow established identification procedures should be prohibited from working or entering port facilities and on board.

The terminal area is controlled. Only the authorized persons can enter the boat, one by one. Terminal environment is indoor environment, where illumination can be manipulated. The area supports the adoption of FRS, the surrounding and its possibilities are optimal.

The following tasks for FRS could be set: (1) General control system for monitoring the passengers, the crew, the maintenance, the suppliers etc., because the captain must know, who is on board. (2) An early warning system for detecting a person who's face is not in the database and who does not have right to enter the boat.

### 5.4.2 On Board

An additional FRS could be located at the pedestrian entrance to the ship shown in Fig. 8.

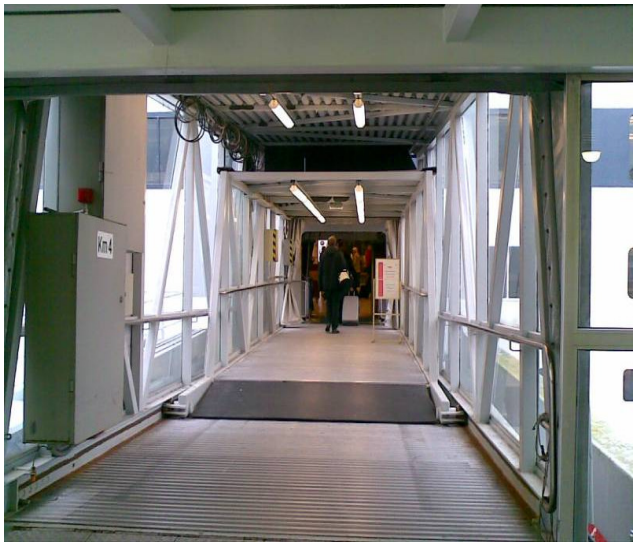

Fig. 8 Entrance to the ship

Special software is able to build up 3D models from 2D images, and so called "super resolution" software used in UK could improve the quality of 2D images and video footage [10-12]. FRS in the terminal could be linked to the existing surveillance systems and databases of the ship. The ship environment is complex and challenging to monitor, as illustrated in Fig. 9 and Fig. 10. With a database of images and a monitoring system based on facial recognition, persons could be monitored automatically. There are already running systems which could be applied: Most employees, e.g. cabin cleaners, have access cards with a photo - this database of pictures could be utilized. Also, the ships have dozens of surveillance cameras and the existing camera network could be exploited. If the video material could be used to build up comparable images ("super resolution"), there is a structure for 24 hours monitoring system.

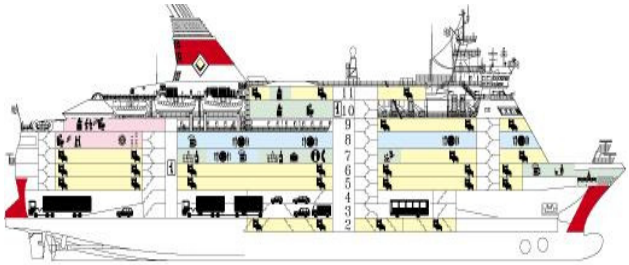

Fig. 9 MS Viking Gabriella – 10 decks, cargo & vehicle area and the sun deck & helicopter pad.

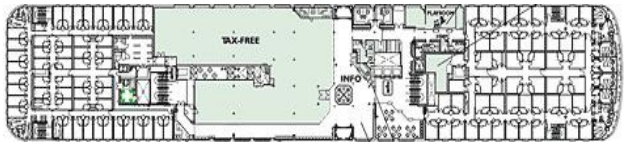


Fig. 10 Decks include different areas, such as shops, restaurants, corridors, cabins, restricted areas.

FRS at sea could be seen as an additional and automated "eyes" at sea. It detects person whose face is not in the database and who does not have a right to exist on board. It could also be an excellent support tool to the investigations of accidents and crimes.

## 6. Experimental Evaluation and Conclusions

Using FRS in environments such as airports and seaports shows that the large areas can be covered. FRS in governmental facilities indicates not only the level of the usage but also the reliability of the current systems. FRS used in common technological applications indicates that it is becoming "an everyman's tool". Why the authorities and organizations in Finland are not using it already on daily basis?

For the public, externally, FRS could look like a normal surveillance camera system. When planning and building up FRS, it is crucial to know the basic process of FRS. There are high standards for the environment where FRS is used and to the quality of equipment used. The location of the facility where FRS is being used should have standard illumination. The facilities should be arranged so that the individuals are videoed from the same direction. Existing camera systems, if available, and common principles for the camera surveillance, like proper planning including evaluation of the environment and cooperation with the authorities [21], can be used when planning and building up FRS.

Although FRS is extensively studies in the last decades, there are many unsolved problems for uncontrolled conditions, such as changes in illumination, pose, facial expression, facial texture (e.g. wrinkles) and shape (e.g. weight gain or loss), facial hair, presence of partial occlusions (e.g. glasses, scarf) and age progression. However, FRS seems to be a suitable control tool when there are masses of people, but the means of control are limited. This kind of environments can be found everywhere; airports, seaports, railway stations, big events & happenings, shopping malls etc. Especially

at the border crossings, there are zillions of unfamiliar face characters to be monitored and at the border it is crucial to detect the person who s/he claims to be. Of the artificial recognition applications, FRS is probably the best solution for a discreet monitoring of a public area.

In Finland, the facial recognition system has been used at the Helsinki-Vantaa airport. FRS has been used since the beginning of June 2008. In Finland, there are surveillance camera systems (computer with database controlling several cameras) e.g. in shopping malls, department stores, railway stations and ferries. Maybe these existing camera systems could be modified and upgraded for them to work as a facial recognition system. Noteworthily, also video material can be used which gives the possibility to utilise data taken from e.g. staircases and elevators where people are moving. Using existing camera systems can be seen as a cost effective way.

Fig. 11 shows the main routes and ports in the Baltic Sea area. Proper passenger control in the ships sailing at the Baltic Sea could be a perfect crime prevention tool against international criminal activity in the Nordic terrain. FRS in ships could be seen not only as an excellent monitoring tool for the maritime security on board, but in the wider perspective as a counter measure or an investment against the international organized crime activities which are taking advantage of extended freedom of movement in EU. Crime prevention is a common goal for authorities and private enterprises across the borderline.

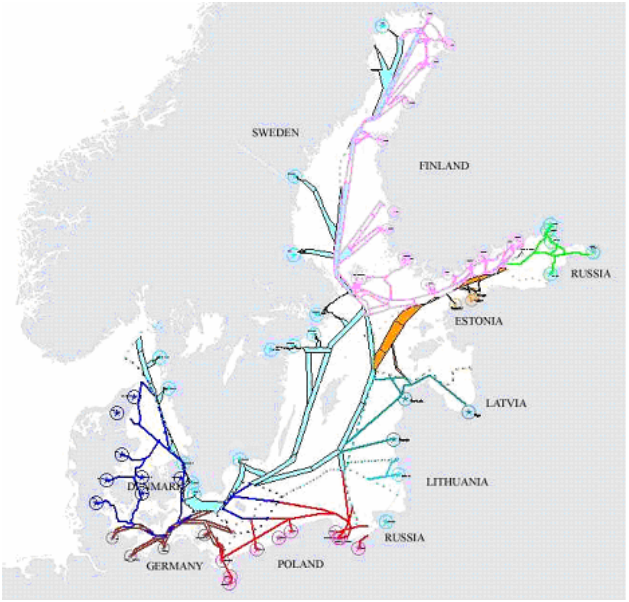


Fig. 11 Main routes and ports in the Baltic Sea area

*References:*

[1] Rajamäki, J., Turunen, T., Harju, A., Heikkilä, M., Hilakivi, M. and Rusanen, S., "Facial Recognition System as a Maritime Security Tool", in *Proceedings of the 8th WSEAS International Conference on Signal Processing (SIP '09)*, Istanbul, Turkey, May 30 - June 1, 2009, pp. 115-121.

[2] "Finnish and Estonian Police Agree to Closer Cooperation in Fighting organised crime", *Helsingin Sanomat, International Edition – Foreign*, 29.1.2008. Available: http://www.hs.fi/english/article/Finnish+and+Estonian+police+agree+to+closer+cooperation+in+fighting+organised+crime/1135233644885

[3] "Rikollisuudentorjunta halutaan osaksi pohjoismaista yhteistyötä", *YLE News,* 22.10.2008. (In Finnish) Available: http://www.yle.fi/uutiset/ulkomaat/2008/10/rikollisuudentorjunta_halutaan_osaksi_pohjoismaista_yhteistyota_357018.html

[4] Christopher, K., *Port Security Management*, Taylor & Francis Group, FL, 2009.

[5] Järvinen, P., *On Research Methods,* Juvenes-Print, Tampere, 2004.

[6] Sertbay, H. and Toygar, Ö, "Face Recognition in the Presence of Age Differences using Holistic and Subpattern-based Approache", in *Proceedings of the 8th WSEAS International Conference on Signal Processing (SIP '09)*, Istanbul, Turkey, May 30 - June 1, 2009, pp. 94-98.

[7] Ramanathan, N., Chellappa, R. and Biswas, S., "Computational Methods for Modeling Facial Aging: A Survey", *Journal of Visual Languages and Computing*, Volume 20, Issue 3, 2009.

[8] Saxholm, N., *Tilanneselvitys lastiyksikköön kohdistuvasta rikollisuudesta*, BBA Thesis, Laurea University of Applied Sciences, 2007. (In Finnish)

[9] Li, S. & Jain, A., *Handbook of Face Recognition*, Springer Science + Business Media, Inc. USA, 2005.

[10] Ahonen, T., The interview of research scientist on 13.5.2008, University of Oulu.

[11] Lehmussola, A., The interview of forensic engineer on 12.5.2008, National Bureau of Investigations, Finland.

[12] Kämäräinen, J., The interview of professor on 9.6.2008, Lappeenranta University of Technology.

[13] Gong, S., McKenna, S., Psarrou, A.. Dynamic Vision, *From Images to Face Recognition*, Imperial College Press, Singapore, 2000.

[14] O'Toole, A., Phillips, P., Jiang, F., Ayyad, J., Penard, N. and Abdi, H., "Face Recognition Algorithms Surpass Humans Matching Faces Over Changes in Illumination", *IEEE Transactions on Pattern Analysis and Machine Intelligence*, Volume 29, Issue 9, 2007, pp. 1642 – 1646.

[15] Thompson, T. and Black, S., *Forensic Human Identificatio: An Introduction*, Taylor & Francis Group, FL, 2007.

[16] Herranen, I., The interview of Major on 19.5.2008, Finnish Border Guard.

[17] Biometrics project, Ministry of the Interior, Finland, 2004. Available: http://www.intermin.fi/intermin/hankkeet/biometria/home.nsf/pages/indexeng

[18] Granell, K., The interview of the Fleet Safety Officer on 14.10.2008. Viking Line Ltd.

[19] Nicander, L., Maritime security presentation in Viking Gabriella on 14.10.2008, Center For Asymmetric Threat Studies (CATS), Sweden.

[20] Sundell, R., The interview of the Captain of MS Gabriella on 15.10.2008, Viking Line Ltd.

[21] Harju, A., *Kameravalvonnan merkitys liikeyritysten rikostorjunnassa: mitä se edellyttää yritysten kameravalvonnalta (The Significance of Camera Surveillance in Conducting Crime Precluding in Business)*, BBA Thesis, Laurea University of Applied Sciences, 2007. (In Finnish)

[22] Tahir, N., Hussain, A., Samad, S. and Husain, H., "A Machine Learning Approach for Posture Recognition Based on Simplified Shock Graph", in *Proceedings of the 8th WSEAS International Conference on Signal Processing (SIP '09)*, Istanbul, Turkey, May 30 - June 1, 2009, pp. 27 - 32.