Bundeskriminalamt

Research project

Face recognition as a search tool

“Foto-Fahndung”

Final report

BKA

ZUSTELL- UND LIEFERANSCHRIFT: BKA, Thaerstraße 11, 65193 Wiesbaden
ÜBERWEISUNGSEMPFÄNGER: Bundeskasse Trier
BANKVERBINDUNG: Deutsche Bundesbank Filiale Trier (BBk Trier)
BLZ 585 000 00 Kto-Nr. 585 010 05

1 Management Summary 5
2 Introduction 7
3 Subject of testing 8
3.1 General prerequisites and structure 8
3.2 Data collection 10
3.2.1 Reference data 10
3.2.2 Participant data 10
3.2.3 Face finding 11
3.2.4 Face recognition 11
3.2.5 Data source 2 - transponder system 11
3.2.6 Data source 3 - analogue video camera 12
3.3 Companies involved (Face recognition systems) 12
3.4 Quality requisites of digital photographs 12
3.5 Legal bases 13
4 Field test 14
4.1 Results 15
4.2 Analysis software 16
4.3 Determination of the FER (False Enrolment Rate) 18
4.4 Genuine-Impostor Frequency 18
4.5 Results in accordance with time of day and location 20
4.6 System comparison 25
5 Summarised interpretation of the results and recommendations 26
6 Outlook 27

Appendix 1: Declaration of consent
Appendix 2: Incentives flyer
Appendix 3: Information flyer

Foreword

With the project "Gesichtserkennung als Fahndungshilfsmittel - Foto-Fahndung" (face recognition to assist with searches - photograph-based searches), the assessment of a possible, future police operational tool was carried out in public. Following a more than two-year preparatory phase, the BKA approached the Federal Ministry of the Interior (BMI) and applied for approval for this procedure with the involvement of the public. The objective was to achieve as much transparency as possible and the prerequisites for objective media reportage. On 16 February 2005, the BMI gave its approval for the research project.

Special thanks go to the Deutsche Bahn AG (German Rail), who made it possible for the BKA to utilise the locality at Mainz central station without which such an extensive project would not have been possible.

Our thanks also go to the Federal Police who supported the BKA at all times by making material and human resources available in a quick and unbureaucratic manner.

Last but not least mention should also be made at this stage of the 200 test participants who agreed to carry a transponder on their persons over a 4-month period and therefore to be available as "wanted persons". Thanks to the support of the Rhineland-Palatinate ministries and authorities in Mainz, it was also possible to acquire participants from this area.

Without the interaction of all the institutions and persons mentioned, it would not have been possible to carry out the field test successfully. Many thanks to all the participants.

February 2007, Wiesbaden

List of abbreviations

BDSG	Federal Data Protection Act
BFDI	Federal Commissioner for Data Protection and Freedom of Information
BKA	Federal Criminal Police Office
BKAG	Law on the Federal Criminal Police Office (BKA)
BMI	Federal Ministry of the Interior
BPOLG	Federal Police Act
DB AG	German Rail
FAR	False Acceptance Rate
FER	False Enrolment Rate
FRR	False Rejection Rate
GES	Face recognition system
ID	Identification
INPOL	Police Information system
JPEG	Joint Picture Expert Group
KI	Institute of Law Enforcement Studies and Training
NIST	National Institute of Standards and Technology
PIN	Personal Identification Number
RFID	Radio Frequency Identification

1 Management Summary

From October 2006 to the end of January 2007 under the working title "Foto-Fahndung", KI 16 - Research and Advisory Unit for Crime Prevention - tested biometric face recognition as a new search tool for the police. 200 commuters took part in the field test and contributed to the success of the project.
The outcome of the tests is that it is possible to automatically recognise wanted persons in crowds if the external conditions are right, in particular, the lighting.
The systems of three manufacturers were tested simultaneously in the entrance hall of Mainz central station.

Four different scenarios were analysed:

- Recognition performance on the escalator during daylight.
- Recognition performance on the escalator during night-time.
- Recognition performance on the stairs during daylight.
- Recognition performance on the stairs during night-time.

We have chosen the performance achieved by the highest performing face recognition system as a representative basis for the biometric systems.

An average of 22,673 persons passed through the monitored area every day. A false acceptance rate (frequency of false acceptances*)* of 0.1% is considered acceptable and manageable. The comparative tests were carried out under this premise of an average of 23 false acceptances daily.

The lighting had the highest impact on the recognition performance. While recognition probability of over 60% was achieved during daylight this figure sank to 10 - 20% during the night.

The impact on the recognition performance of the systems caused by the different movements of the participants on the stairs and escalator was less than expected. On average, the recognition probability in the case of the stairs - depending on the type of system - was 5 - 15 % lower than in the case of the escalators.

The analysis of and experience with the systems show that the surveillance of a specific area not only depends on the quality of the biometric algorithms used but essentially also on the potential offered by the camera technology utilised. The differences between the camera systems became particularly obvious at twilight. The differences in the resulting image quality impacted significantly on the recognition performance.

Since "Foto-Fahndung" was a technically-oriented research project which did not constitute a legal appraisal for a realistic situation, the following information can be deduced for the planner:

High recognition performance can be expected in indoor areas which have non-varying light conditions. Varying light conditions (darkness, back light, direct sunlight) cause a sharp

decrease in the recognition performance. A successful utilisation of biometric face recognition systems in outdoor areas does not seem to be very promising for search purposes at the moment.

Successful recognition using the 2D face recognition technology can only be achieved with frontal facial images. It can be deduced from this that a conscious or unconscious form of co-operative behaviour must be attained from the wanted person. This can be brought about by using eye catchers or controlled singling out of individuals. A possibility would be the usage of entry control systems which always involve splitting up crowds.

It has to be taken into consideration that for every identification response times have to be allowed for to enable the operational staff to take further action. The operational site should therefore be selected so that officers are already positioned at the control point or that it is ensured that the recognised person will still be in the monitored area for a certain period of time.

2 Introduction

The word biometrics derives from Greek: Bios (life) and Metron (the measure). Thus, the term has to do with measuring living things.

Identifying persons on the basis of their fingerprints is standard police procedure. Further biometric procedures which can be used for identifying persons have been available for some years now. We differentiate between static and dynamic and co-operative and non-co-operative procedures. Static procedures place the emphasis on the constancy of a trait; the property of permanency or only undergoing minimal change over a longer period of time. Examples of this include the finger, the hand and the face. Dynamic procedures focus on the recognition of changing traits such as pressure and movement. These can be a person's signature or gait, for example. Co-operative procedures require the involvement of the person who is to be identified: for instance, the placing of the finger on a sensor. Non-co-operative procedures can be used without the knowledge and assistance of the person who is to be identified. An example of this is face recognition which can also lead to identification without the conscious presentation of the trait.

As can be assumed from the definition "measurement of life", biometric traits are subject to a constant change process. The same is true of the requirements for trait capturing. The result is that different images of a trait always differ somewhat from one another. The identification of a person using biometrics works differently to identification using a PIN or password. A simple right or wrong is out of the question in biometric proceedings. Rather a match score is required between the stored reference template and the living trait in order to identify a person. This determinable measurement is called a threshold. If the similarity of the captured trait and the stored template exceeds this threshold, a person is regarded as identified, otherwise, the system assumes that two different persons are involved.

A large number of biometric procedures are utilised today for commercial purposes. Examples include fingerprint recognition, iris recognition, speech recognition, signature recognition etc. In the research project "Foto-Fahndung", the BKA exclusively tested face recognition systems.

Face recognition technology identifies people through facial traits which do not change easily and, to a large extent, remain constant over time. Before a biometric system can identify a person, this person's traits have to be captured. This initial recording is referred to as enrolment. The data used for the later comparison are stored in a special data format called the template.
Face recognition is often used for comparing a live image of a person with their reference image (e. g. in an entry check). This procedure which serves to confirm a specified identity is called a one-to-one verification (1:1). Face recognition systems are, however, also capable of comparing all persons stored in the system with an image of an as yet unidentified person. This is referred to as one-to-many (1:n) identification. Faces from the video stream of a camera can also be extracted and used as search images.
"Foto-Fahndung" exclusively describes the recognition of persons for the purpose of identification.

3 Subject of testing

The project "Face recognition as a search tool - Foto-Fahndung" was intended to achieve the following goals:

- utilisation and assessment of commercially available face recognition systems in respect of the possibilities of extracting faces out of a crowd
    - assessment of the recognition performance of algorithms with regard to their suitability for comparing live images with reference images in real time.

A quality enhancement is expected in the future in the development of both the algorithms and, in particular, the cameras. Whichever manufacturers then offer the best overall concept should be tested out again.

3.1 General prerequisites and structure

In order to be able to obtain classifiable results, it was necessary to get frontal images of the faces of the persons who were to be identified. This was possible in the area of the descending stairs in the entrance hall at Mainz central station. The cameras were mounted at a height of about 3.5 metres on a pillar opposite the stairs.
Figure 1 shows the schematic set-up of the test. The selected floor plan demonstrates the relationships in terms of size and distance. The area monitored by the cameras was restricted to the descending escalator and the adjacent half of the stairs as far as a permanently installed railing. The distance between the cameras and the monitored area was between 12.5 - 15 metres.

Figure 2 shows the cameras on an assembly track at a height so about 3.5 metres. Each manufacturer came equipped with two high-resolution digital cameras; one was used for filming the escalator and the other the stairs. The 7th camera in the middle is the BKA control camera which filmed the monitored area non-stop over a 24-hour period. This was essential for the later analysis (determination of non-matches).

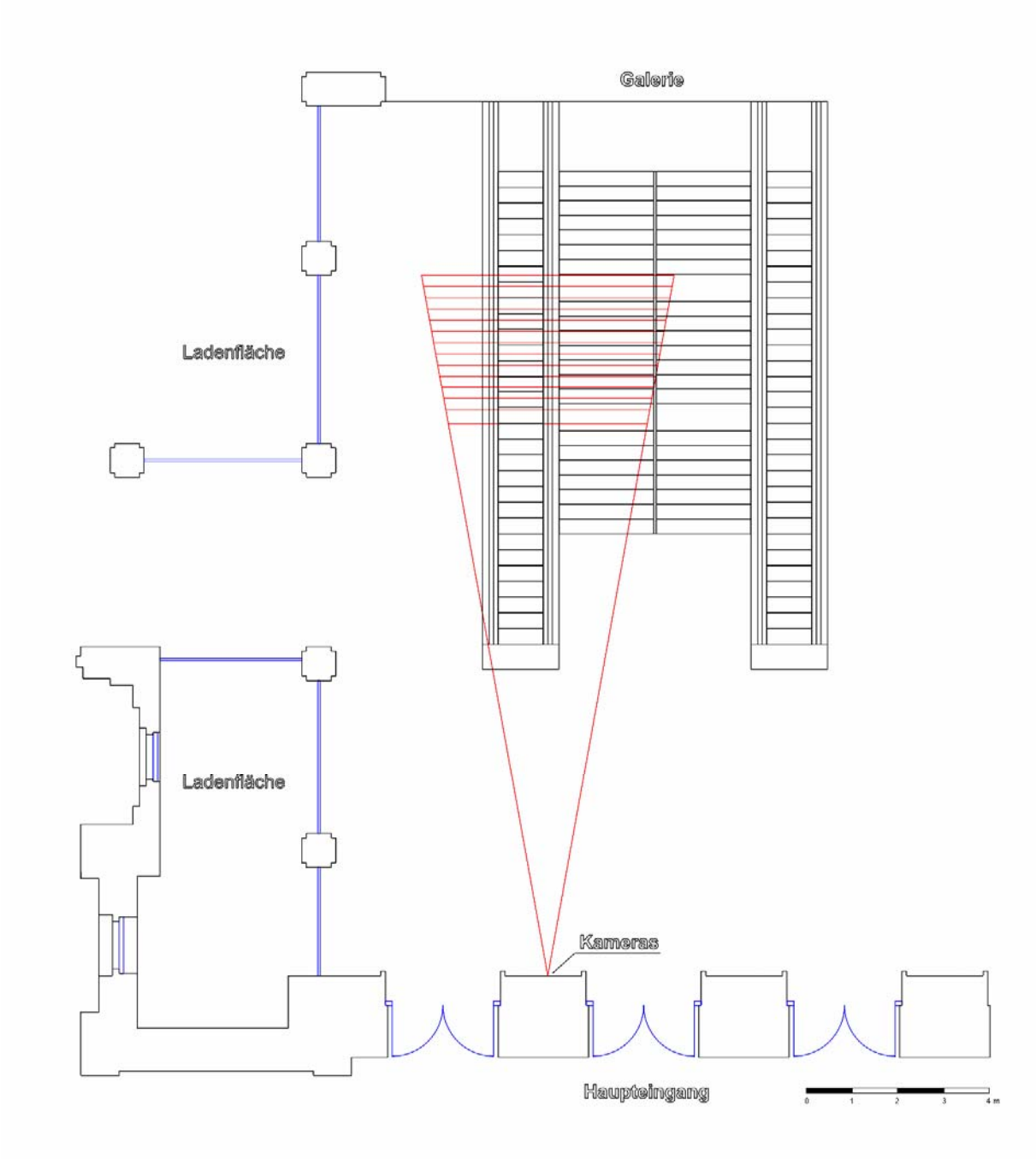


Figure 1 - Schematic presentation of the monitored area

Legend:

Galerie: gallery
Ladenfläche: shop area
Kameras: cameras
Haupteingang: main entrance

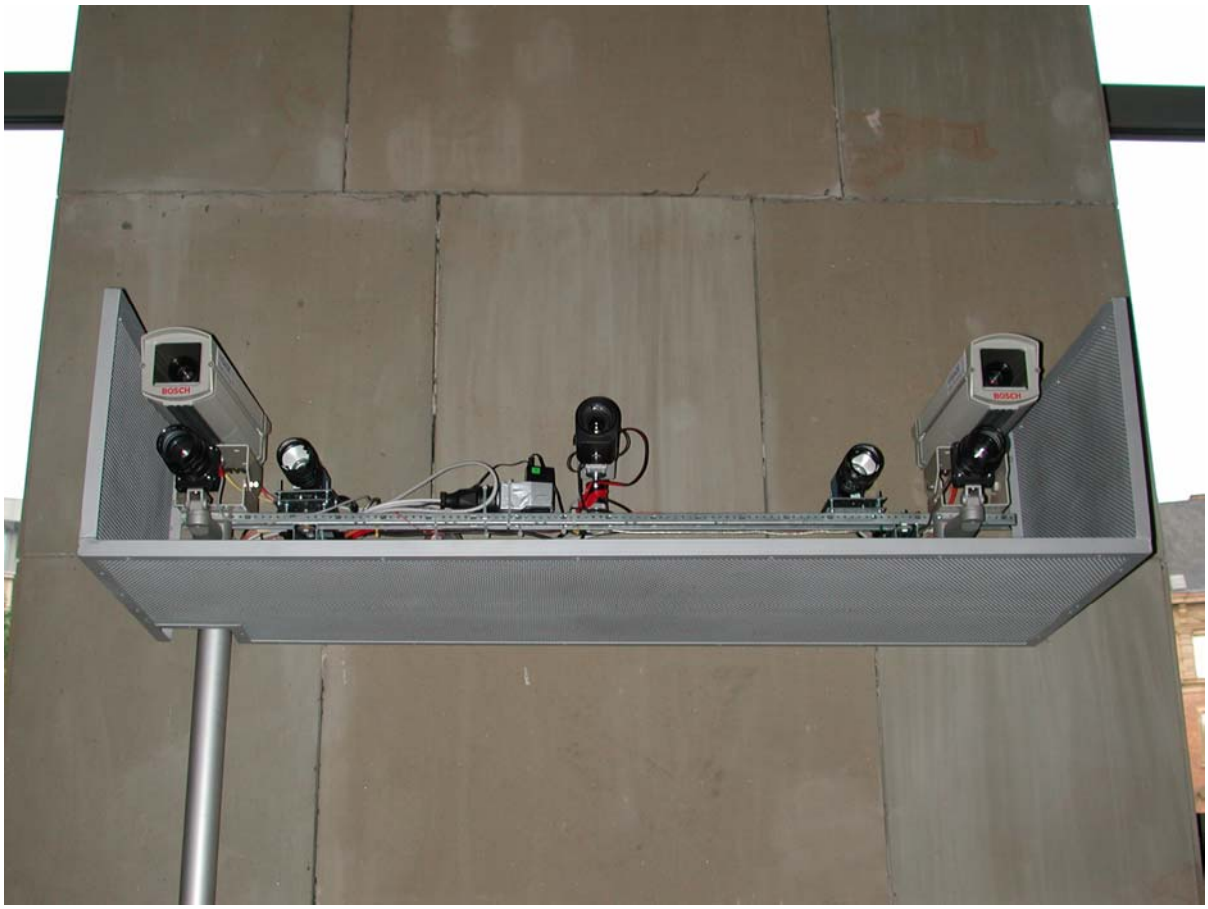


Figure 2 - Installation of cameras

3.2 Data collection

The following chapter describes the data sources which were required for the tests in the course of the project.

3.2.1 Reference data

A digital photograph of the face of each field test participant was taken in accordance with NIST standards (see point 3.4). The face recognition systems generated a template from these with which facial photographs were compared during the test.

3.2.2 Participant data

The data record of each field test participant contained his reference data and a user ID.
The assignment of the user ID to the transponder ID facilitated the coupling of the transponder and face recognition data in the analysis.

The internal data of the field test participants, i.e.

- Surname, first name
- Address
- Contact details (telephone number, email address)
- Gender
- Age

and their user ID were stored in a separate database at the BKA for assignment.

3.2.3 Face finding

The systems being tested were supposed to have a face-finding counter via which the total number of all the faces compared could be identified. The goal of reaching a conclusion about the quality of the face finding algorithms from the various number of comparisons carried out had to be abandoned. Some persons were filmed several times by the systems while passing through the monitored area so that it was not possible to make an inference with respect to the number of different persons.

3.2.4 Face recognition

The face recognition systems continuously extracted picture files of the faces of the persons who passed through the monitored area and compared these with the reference data. If the match found was insufficiently high, these picture files were discarded. They only existed for the short timeframe which was necessary for the comparison.
If a match with a reference data was identified, the following logged data were stored in addition to the picture files:

- Transaction-ID (individual name of a recognition process)
- User ID
- Date/time when the image was taken
- Match score
- Camera

Since reference data could also be erroneously assigned to persons not participating in the field test, these data were analysed within 48 hours in order to facilitate the deletion of facial images of uninvolved persons in due time.

3.2.5 Data source 2 - transponder system

Each test participant was equipped with a transponder which had been assigned an individual transponder ID. The transponder reader unit which was installed on site was equipped with two antennas, one in front of and one behind the video-monitored area. In this way, the time laps between data logging allowed to determine the direction. If a participant passed through the antenna field, his transponder ID was recorded by a reading device and the transponder ID, time stamp as well as a consistency check were logged.
This log made it possible to trace whether and when a test participant was in the logging area of the face recognition systems and should therefore have been identified.
In order to rule out problems occurring at a later stage through inaccurate internal clocks, the transponder system had a radio controlled clock module (so called DCF77).

3.2.6 Data source 3 - analogue video camera

The area to be captured by the face recognition systems was filmed at the same time by a video camera and stored digitally. In the cases of non-matches of registered persons who, pursuant to transponder logging, must have passed through the monitored area, conclusions regarding the cause and/or source of error for the non-match could be reached through a manual analysis of the video data.
In order to run synchronically with the transponder system, the time log of the video recorder was also controlled by a DCF77 - module. The analysis of the respective daily data also took place within 48 hours. It was not permissible to store the video data for a longer period of time.

3.3 Companies involved (Face recognition systems)

The face recognition systems were selected on the basis of a public tender. All bidders who applied were given the opportunity to participate in the field test.
The companies in question were:

a) Cognitec Systems GmbH
An der Flutrinne 12
01339 Dresden

b) Cross Match Technologies GmbH
Unstrutweg 4
07743 Jena

c) Bosch Sicherheitssysteme GmbH
Vertriebsniederlassung Frankfurt
Lahnstraße 34-40
60326 Frankfurt am Main

In this report the systems will be referred to as 1, 2 and 3. There is no connection to the designation a) - c) used above.

3.4 Quality requisites of digital photographs

The reference photographs taken in Mainz were based on the following criteria:

Depth of focus:
The facial image was to be focussed on the area from the nose to the ears. In order to avoid distortions, the focal distance should correspond to that of 85 - 135 mm lenses for a 35 mm camera. The camera was to be positioned at eye level.

Centering:
The middle points of the mouth and the bridge of the nose were to be horizontally centred. At least 50% of the width of the captured image was to be covered by the person's face. An imaginary horizontal line through the pupils was to lie at an approximate image height of between 55 - 60%.

Lighting:
Two photography lights were used for the illumination of the face. The light sources were angled in such a way that shadows and highlights were eliminated.

Background:
The person to be photographed was positioned in front of a smooth 18% grey backdrop. A backdrop reflection of 18% was guaranteed with the aid of a Kodak grey card, a neutral grey card or a densitometer.

The image, applied to a size of W 3.75 x H 5 cm, was taken with a resolution of 600 x 800 pixels and a colour depth of 24-bit RGB; approx. 50% of the width of the captured image was covered by the horizontal size of the head.

3.5 Legal bases

The research project was conducted on the basis of section 6 b (1) no. 1 of the Federal Data Protection Act in connection with section 2 (6) no. 3 of the BKA Law. The handling of the project data was regulated as follows:

Collection of data:
The legal basis for the collection of the personal data which was required for conducting the research project "Foto-Fahndung" results from

a) section 13 (1), (2) no. 2 of the Federal Data Protection Act for persons who volunteered to participate in the research project as well as
b) section 13 (1), (2) no. 8 of the Federal Data Protection Act for persons who did not voluntarily participate in the research project, however, were still captured on camera when they walked through the project area.

Data storage and data usage
The legal basis for the storage and analysis of the data collected results from

a) section 14 (1), (2) no. 2 of the Federal Data Protection Act for persons who volunteered to participate in the research project as well as
b) section 14 (1), (2) no. 9 of the Federal Data Protection Act for persons who did not voluntarily participate in the research project.

Deletion of the data
The personal data of the volunteer test participants were only stored as long as they were required for the purposes of the research project. All the data were irretrievably deleted at the latest on 16 March 2007, when the research project was concluded. If a test participant withdrew his participation in the research project, his data were immediately deleted.
The test participants agreed to this code of practice in a declaration of consent (see app. 1) coordinated with the Federal Data Protection Commissioner (BfDI). The personal data of the persons who did not voluntarily participate in the research project were deleted after 48 hours at the latest. This term analogously results from section 27 of the Law on the Federal Police.

4 Field test

Volunteers were recruited prior to the field test being conducted. This began in August 2006 at authorities and ministries in Mainz. The recruitment process continued at Mainz central station in September 2006. A stand was set up in this respect over a 3-week period in the entrance hall of the station. The volunteers were registered in order of their applications. No special criteria were used for the selection.

As compensation for the time and effort involved, the participants were offered a choice of 18 incentives, from which each participant could select one. They were handed out when the field test was concluded (selection of incentives: App. 2).

In addition to the recruitment of volunteers, the stand also served to inform passersby about the project. A flyer (App. 3) was created for this purpose and handed out by the organisers of the stand. At the same time, it was also possible to view the contents on the BKA homepage. The research project was officially launched on 09 October 2006 within the framework of a press conference at Mainz central station.

Frontal images of the head were taken of the 200 volunteer test participants. Each participant received a transponder which he was supposed to carry with him when passing through the entrance hall for the duration of the test.

The test participants were obliged to pass through the monitored area at least once a day. During the project period, the monitored area was passed through 141 times a day on average.

Figure 3 shows the area under camera surveillance. A receiver for the transponder signals was installed at the top and bottom of the escalator respectively.

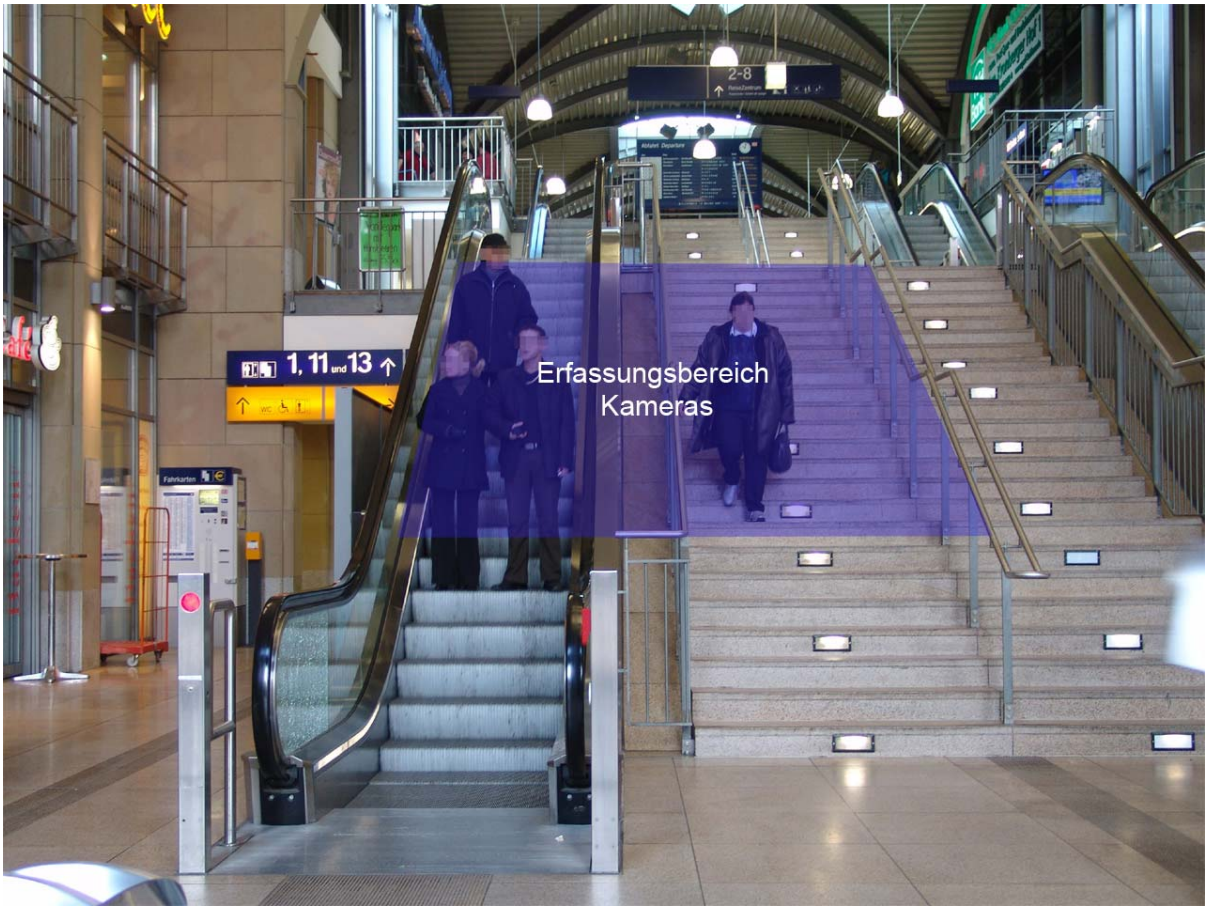


Figure 3 - Camera surveillance area (blue)

4.1 Results

The research project "Foto-Fahndung" deliberately forewent the creation of laboratory conditions. Attention was focussed more on testing the face recognition systems under real operational conditions such as the police encounter. Consequently, the installation of additional lighting did not come into question.

It was possible to carry out exhaustive testing of four different scenarios under the conditions prevailing at the railway station. Decisive for the following classifications were the lighting and movements of the test persons. Although from a test scenario perspective, the central station in Mainz is an indoor area, it was remarkable that it became noticeably darker in the hall after sundown. This was expected to have a negative impact on the recognition performance.
The second decisive factor "movement" results from the fundamentally different behaviour of the test persons on the escalator and stairs. Whereas in general, the face of a person on an escalator moved uniformly through the captured area, descending the stairs led to jerky movements both in a horizontal as well as vertical direction. In addition, the line of vision of persons on the stairs is mostly directed downwards while, on the other hand, persons on the escalator look straight ahead. It was therefore anticipated that the systems would find it easier to detect persons on the escalator.

4.2 Analysis software

A special software was developed at the BKA for the simplification of the analysis. This software combined the data from the face recognition software with the data from the transponder system and in this way supported the manual analysis.

The analysis took place in two phases. Firstly, the signal from the transponder log served as a base. This analysis facilitated the determination of cases of non-matches and correct matches, separated according to stairs and escalator. Figure 4 shows the structure of this analysis. The examining case officer manually decided whether a test participant had in fact been in the monitored area and whether the face recognition systems had been able to identify the person or whether reasons were on hand for a non-match which were not attributable to the face recognition systems. The permanent video recording in the aforementioned 48-hour timeframe was on hand to assist with this.

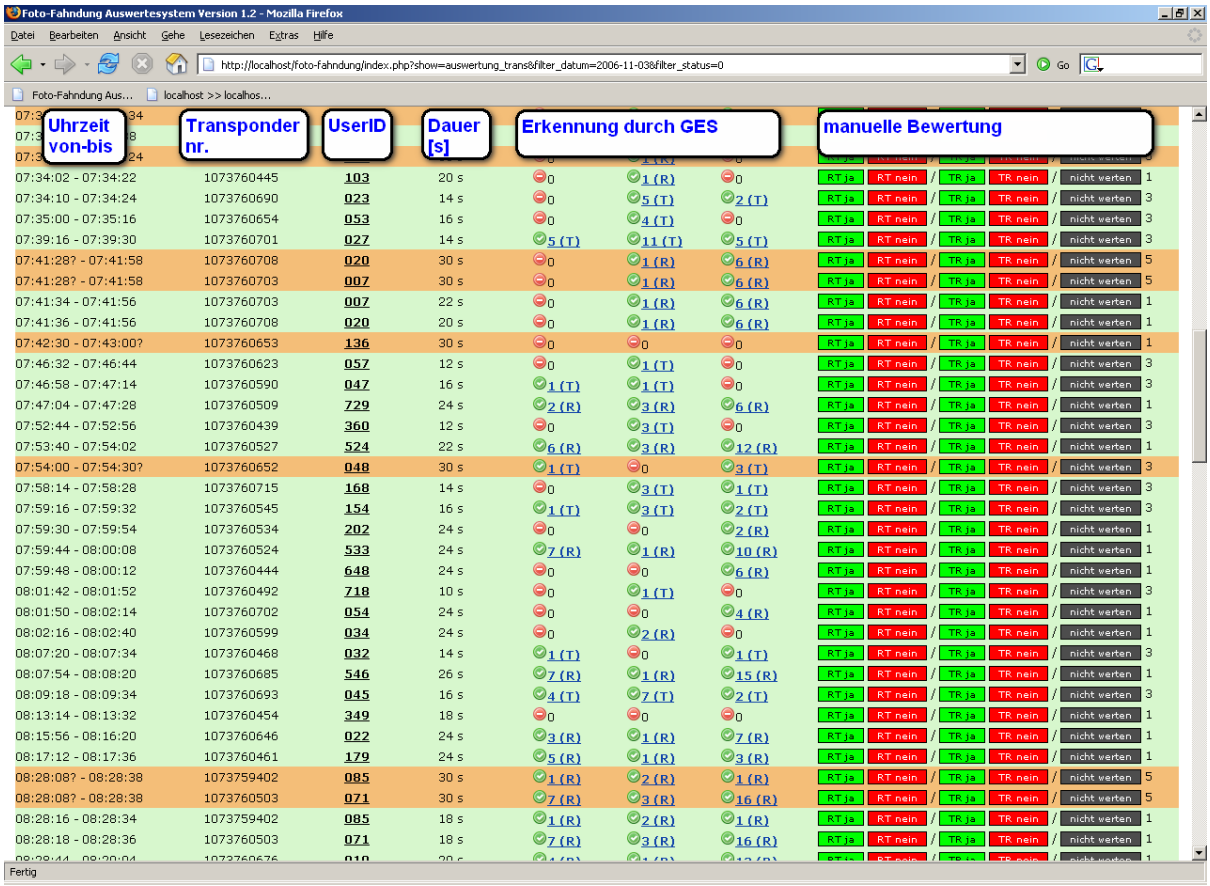


Figure 4 - Analysis according to the transponder log

Legend:
Uhrzeit von-bis: Time from-to
Transponder Nr.: transponder number
User Id: user ID
Dauer: duration
Erkennung durch GES: identification by face recognition system
Manuelle Bewertung: manual analysis.

In a second step the stored log files of the face recognition systems provided a basis for the analysis. In this way it was possible to identify false acceptances and the cases where the test participants did not have their transponders with them.

Figure 5 shows the pertinent screen surface which enabled the analyst to analyse the respective identifications. The display for the manual check is shown on figure 6.

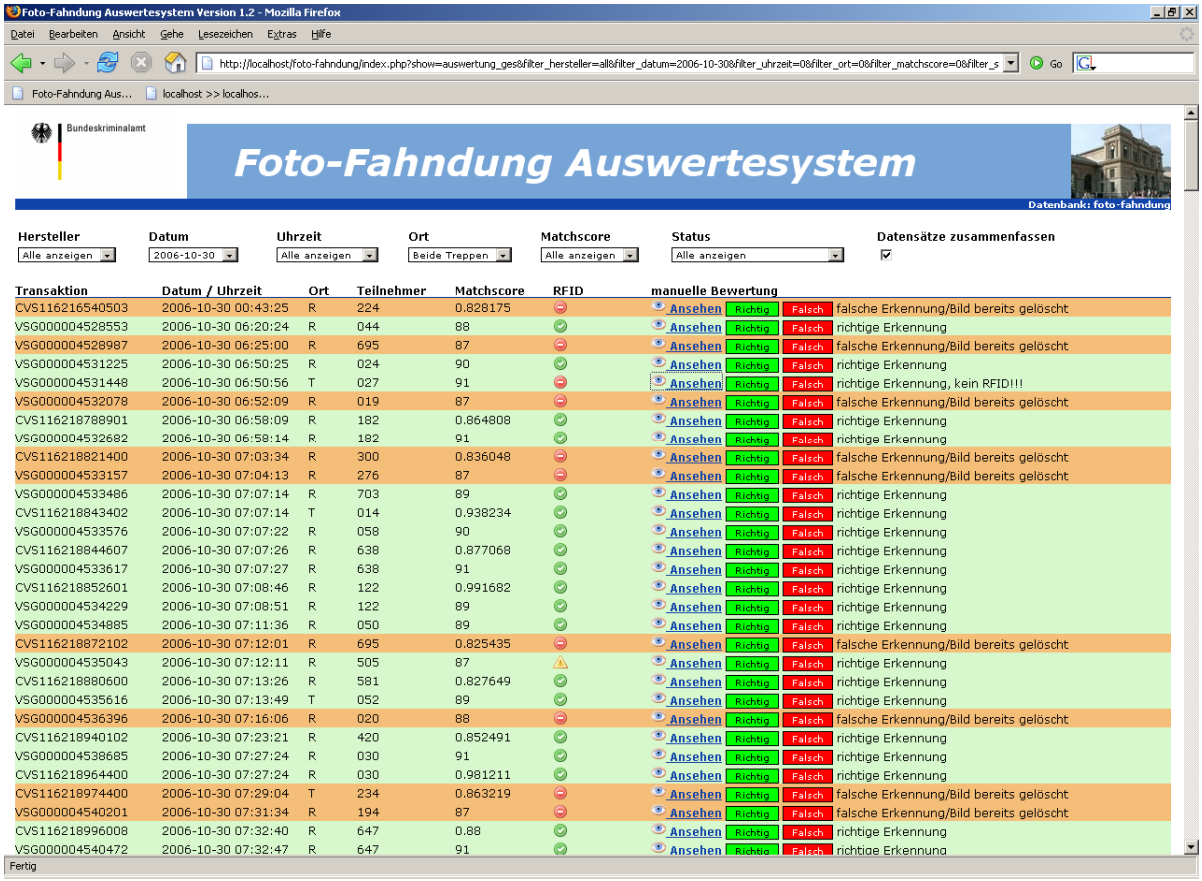


Figure 5 - Analysis according to log files of the face recognition systems

Legend:
Hersteller: manufacturer; Alle anzeigen: show all; Transaktion: transaction; Datum: date; Uhrzeit: time; Ort: location; Beide Treppen: both stairs; Matchscore: match score; manuelle Bewertung: manual analysis; ansehen: view; richtig: correct; falsch: false: falsche Erkennung/Bild bereits gelöscht: false identification/photograph already deleted; richtige Erkennung: match; Datensätze zusammenfassen: summarize data records
Teilnehmer: participant

Figure 6 - Display for manual check of match

The bipartite analysis enabled each individual identification to be manually traced through the face recognition systems and the recording of those cases which would have been lost in an automated analysis (e. g. a participant does not have the transponder on his person). The images of uninvolved persons whose similarity to test participants exceeded the set threshold were always automatically deleted at the end of the respective analysis day.

4.3 Determination of the FER (False Enrolment Rate)

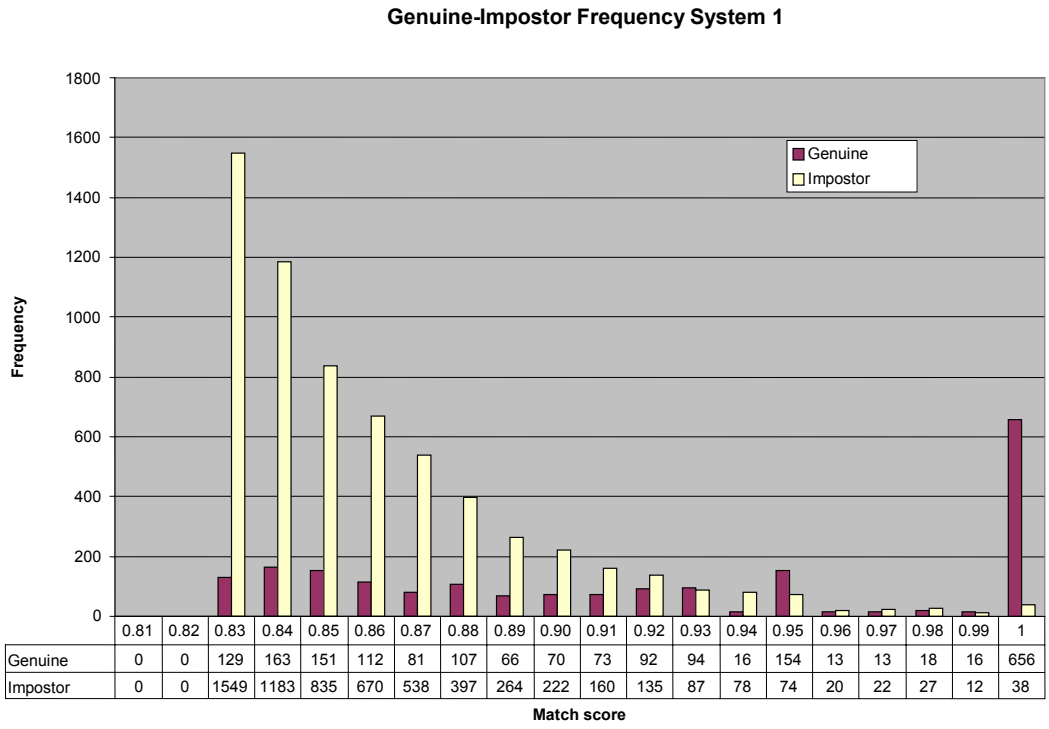
In this project the FER was 0% for all systems. It was possible to enrol all the images of the test participants.

4.4 Genuine-Impostor Frequency

The genuine-impostor frequency allows the frequency of occurrence of match scores for correct matches and false acceptances to be shown. In this way, if the threshold - the required match score between the reference image and the live image - is raised or lowered, the change in the proportion of false acceptances to correct matches can be deduced.

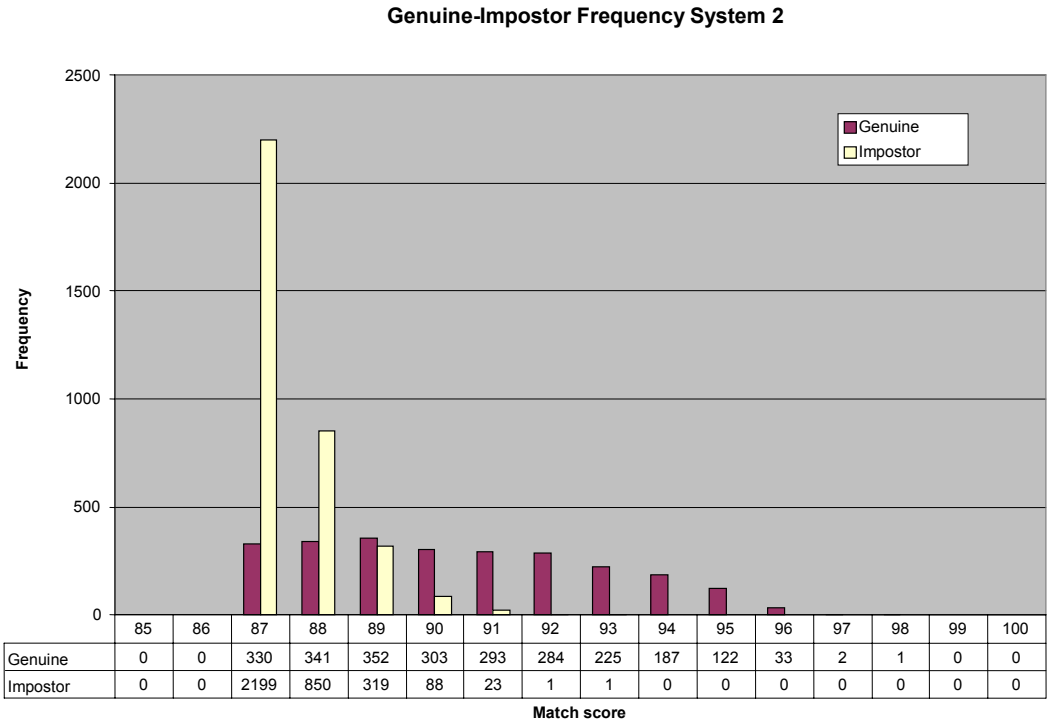
Depending on the required degree of security, (number of permissible false acceptances), the ideal working point of the systems can be determined in this way. As a rule, for comfortable application a higher false acceptance rate is acceptable since the main emphasis will be on identifying authorized users. The threshold setting can be lowered accordingly. In access control systems to sensitive areas, a high threshold will certainly be used and the fact that this will lead to a higher number of false rejections will be taken into account.

Figures 7 - 9 show the diagrams for threshold settings made by the manufacturers in accordance with BKA specifications. All the systems demonstrate that a raising of the respective threshold would prevent a high proportion of false acceptances. The proportion of correct matches which would be lost in the process can also be seen from the diagram. The threshold setting was kept deliberately low for this research project so that from the outset data would not be lost which would then no longer have been available for analysis.



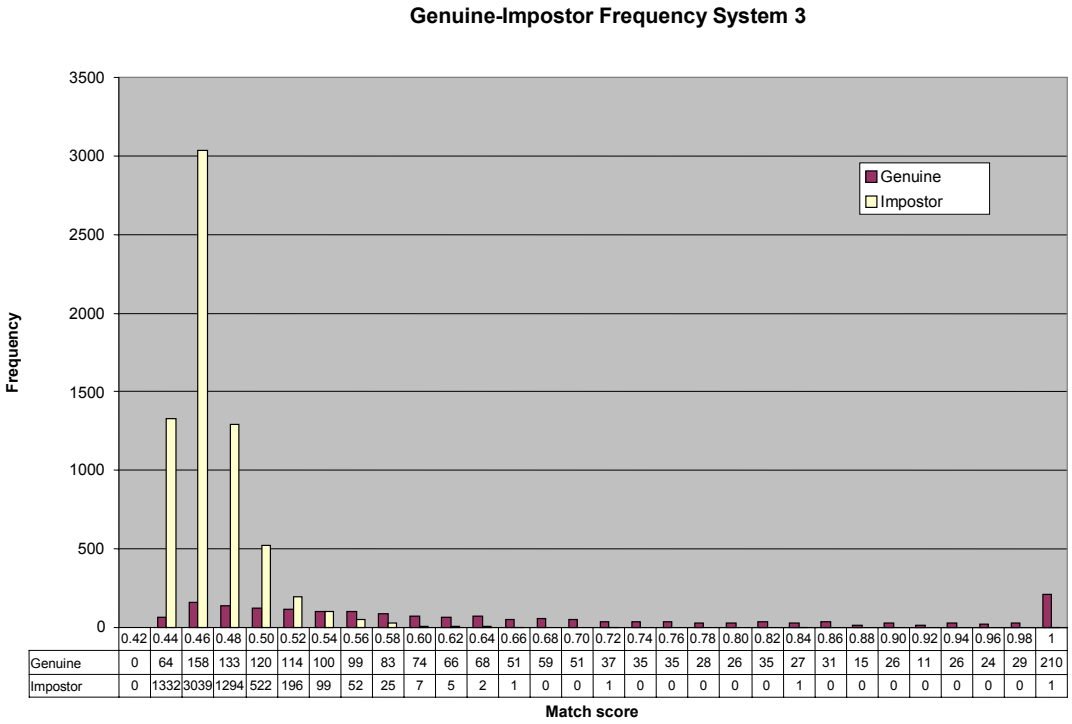
	0.81	0.82	0.83	0.84	0.85	0.86	0.87	0.88	0.89	0.90	0.91	0.92	0.93	0.94	0.95	0.96	0.97	0.98	0.99	1
Genuine	0	0	129	163	151	112	81	107	66	70	73	92	94	16	154	13	13	18	16	656
Impostor	0	0	1549	1183	835	670	538	397	264	222	160	135	87	78	74	20	22	27	12	38

Figure 7



	85	86	87	88	89	90	91	92	93	94	95	96	97	98	99	100
Genuine	0	0	330	341	352	303	293	284	225	187	122	33	2	1	0	0
Impostor	0	0	2199	850	319	88	23	1	1	0	0	0	0	0	0	0

Figure 8



	0.42	0.44	0.46	0.48	0.50	0.52	0.54	0.56	0.58	0.60	0.62	0.64	0.66	0.68	0.70	0.72	0.74	0.76	0.78	0.80	0.82	0.84	0.86	0.88	0.90	0.92	0.94	0.96	0.98	1
Genuine	0	64	158	133	120	114	100	99	83	74	66	68	51	59	51	37	35	35	28	26	35	27	31	15	26	11	26	24	29	210
Impostor	0	1332	3039	1294	522	196	99	52	25	7	5	2	1	0	0	1	0	0	0	0	0	1	0	0	0	0	0	0	0	1

Figure 9

The threshold parameters relevant for the analysis differ from manufacturer to manufacturer. Furthermore, the functions on which the comparisons are based are not linear. Therefore, assumed larger steps in the parameters do not also automatically mean that the system's selectivity in respect of correct matches and false acceptances is higher.

Comparability is established under item 4.6 by means of converting the results into a false acceptance rate (specifically the number of false acceptances) of 0.1%.

4.5 Results in accordance with time of day and location

The results of biometric face recognition depend heavily on external factors. The scenario at Mainz central station made it possible to differentiate between various scenarios. It was thus possible to examine the influence of lighting (day/night) and that of human behaviour more closely. The test participants' behaviour on the escalator varied significantly from that on the stairs. People using the escalator remain relatively immobile for the most part and let their gaze wander. People on the stairs perform hefty, quick horizontal and vertical movements. This can be explained by the nature of a stairs per se. The acceleration of gravity affects the person with each step he takes. When climbing stairs a person also automatically swings the upper body. It was therefore to be expected that there would be a marked difference between the results from the stairs and the results from the escalator.

The influence of the various lighting conditions during daytime and night-time became clear at the beginning of the adaptation phase. For this reason, the analysis of the recognition performance of the systems was carried out on an hourly basis. The percentage given results from the quotient of identifications and times the test participants passed through in a one-hour analysis timeframe. If, at specific times, fewer than ten test persons passed through the monitored area, this value was discarded.

The following diagrams show the system identifications separated according to stairs and escalator. Not always did the face recognition systems have a chance to actually identify the test participants. Some of the participants did not look frontally to the camera, but in another direction. The reasons for this may have been conversations or distractions. Also on the stairs one tends to look down so as not to stumble. Each time a person passed through the monitored area he was tracked in the video stream by the analysts. It was thus possible to ascertain whether a person was in fact identifiable for the systems. Consequently, there are two different curves in each of the following diagrams. One curve illustrates the relative number of identifications in proportion to the total number of times the persons passed through the monitored area and the second curve shows the number of identifications for persons who fulfilled the prerequisites for a successful identification (frontal image).

Figures 10 - 12 represent the respective results which were obtained from the escalator; figures 13 - 15 the results from the stairs.

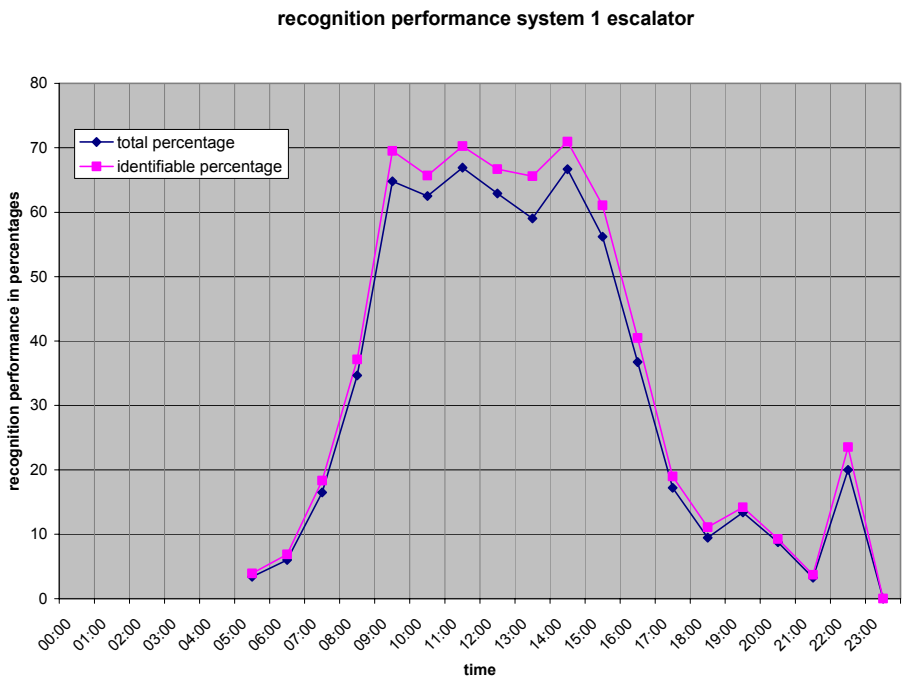


Figure 10

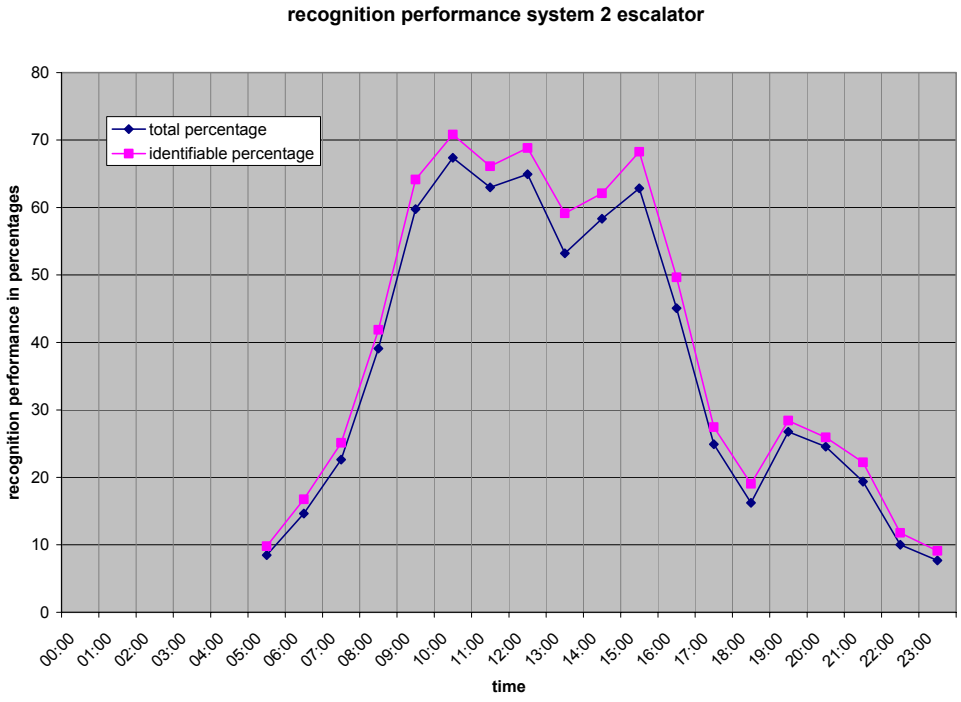


Figure 11

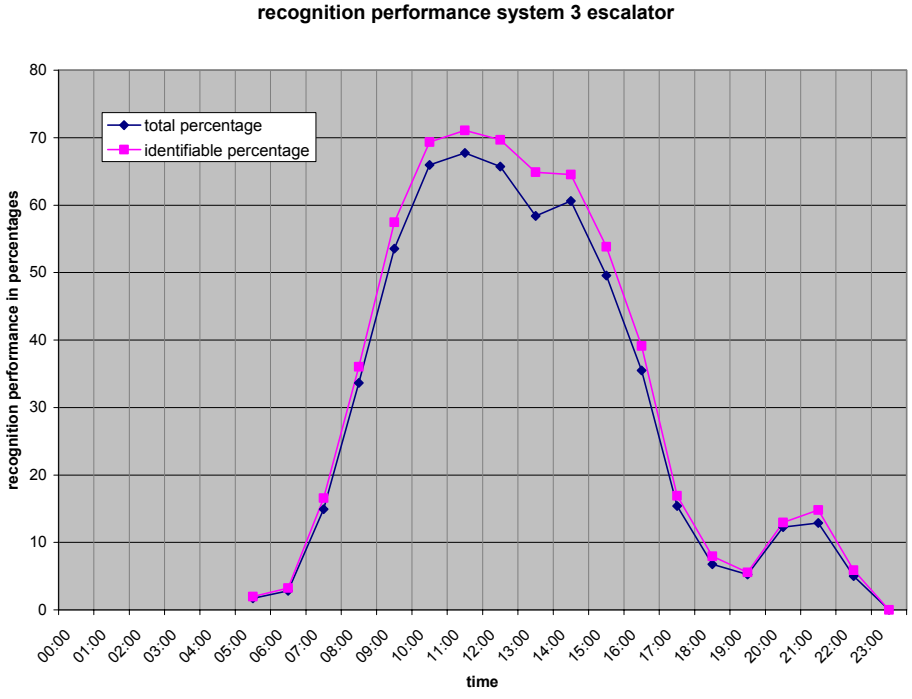


Figure 12

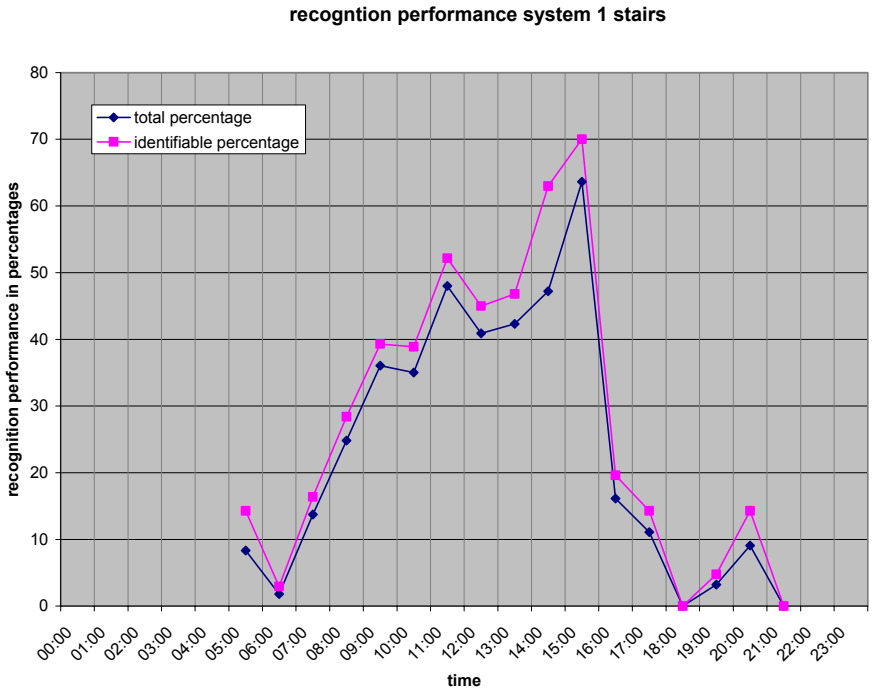


Figure 13

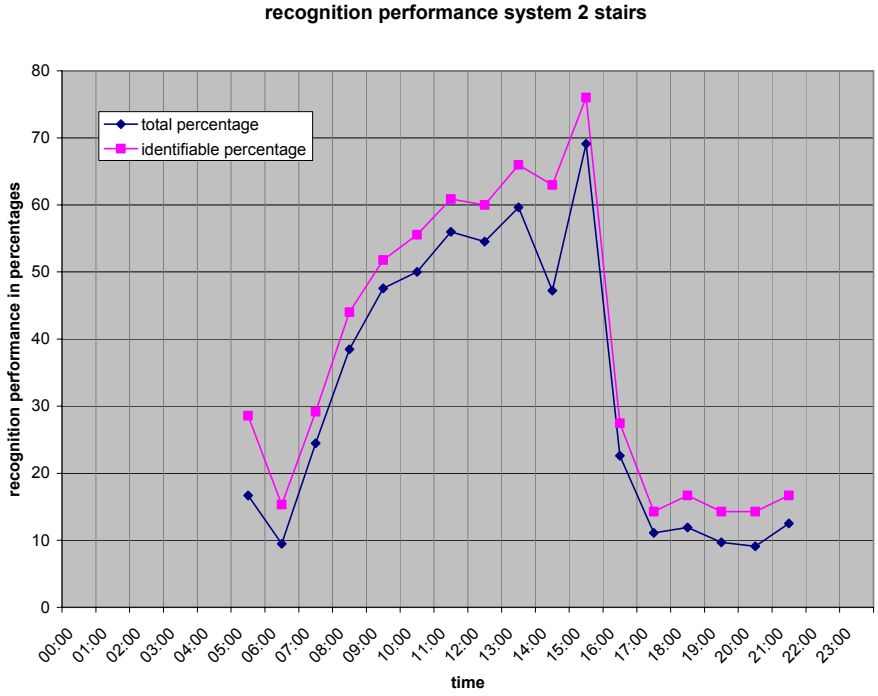


Figure 14

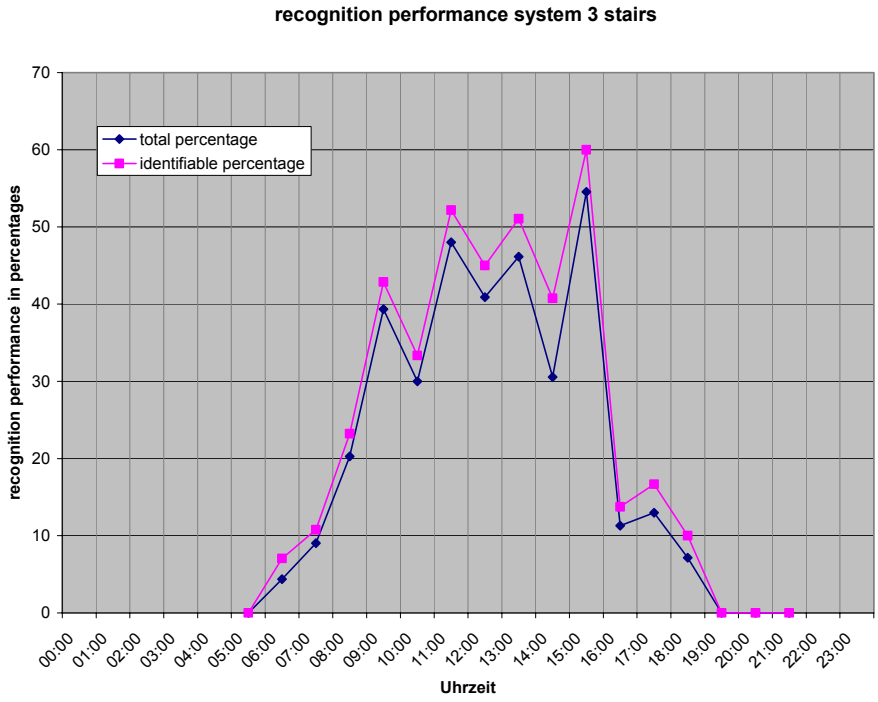


Figure 15

The diagrams allow us to make some interpretations. We can clearly see that considerably higher recognition performances are achieved on the escalator when the systems were able to get a frontal image for the biometric comparison.

While the recognition performances of all the systems drop significantly during the darkness, recognition performances of over 70% are realistically achievable during daylight. These marked differences between daylight and darkness are explained by the fact that only half of the artificial lighting is active in the station hall and for this reason it is noticeably darker there at night. The consequence of this is that the digital cameras have to work with longer exposure times and wider apertures. This results in images with blurred movement which are of little use.

As anticipated, in the comparison of the recognition performances between the escalator and the stairs, a higher number of identifications was achieved from the escalator. This resulted from the blurred movements which are caused by the movements on the stairs.

4.6 System comparison

A direct comparison of the systems is possible by defining a specific working point. This working point should arise from the practical application of the system requirements.
In the case on hand, this means finding a manageable value which, in a real situation, produces a justifiable number of false alarms.
On average, 22,673 persons passed through the monitored area daily. These data were acquired from counts repeated every 24 hours. In practice, a manageable number of false acceptances is produced with a FAR of 0.1%. In this case, an average of 23 false acceptances are tolerable over a 24-hour period.
The threshold, with a false acceptance rate of 0.1%, was then calculated for each system from the recorded data.

The following diagram shows the average recognition performances of the three systems throughout the entire project period. A differentiation between daylight and darkness, stairs and escalator was not made for this diagram.

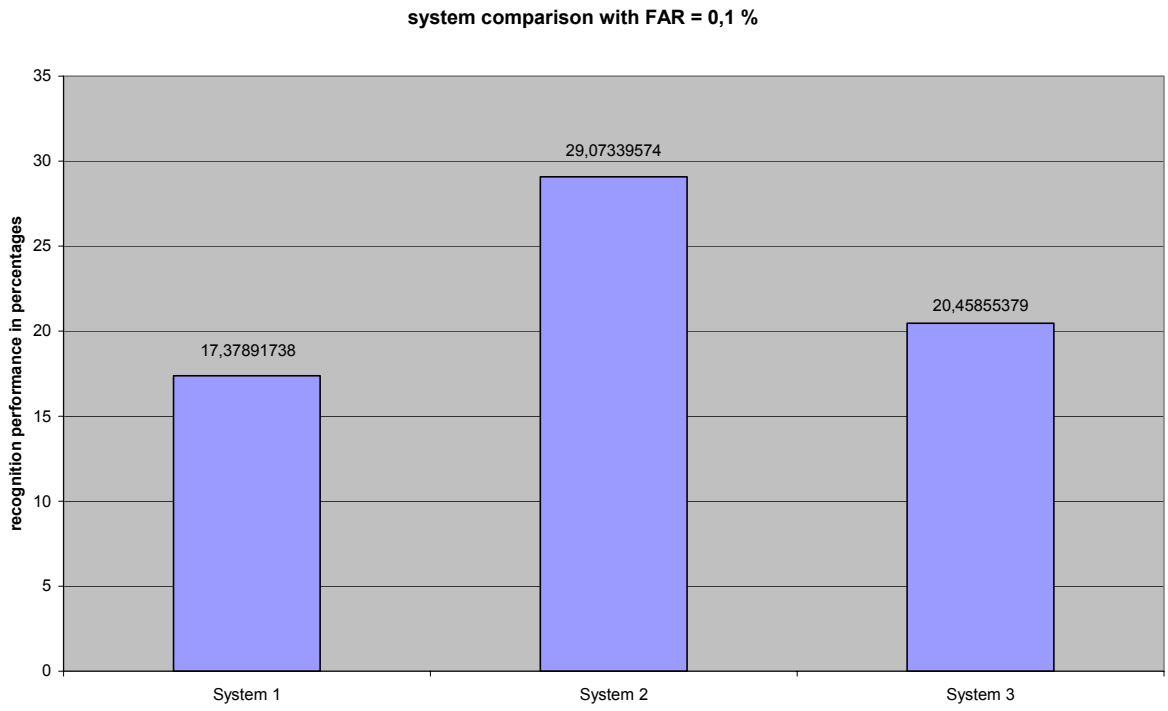


Figure 16

- System 1 achieves an overall recognition performance of 17.38%.
- System 2 achieves an overall recognition performance of 29.07%.
- System 3 achieves an overall recognition rate of 20.46% under the assumption of a FAR of 0.1%.

What appears at first glance to be low identification rates can be explained by the fact that most of the test persons passed through the monitored area at times when the lighting conditions were not ideal.

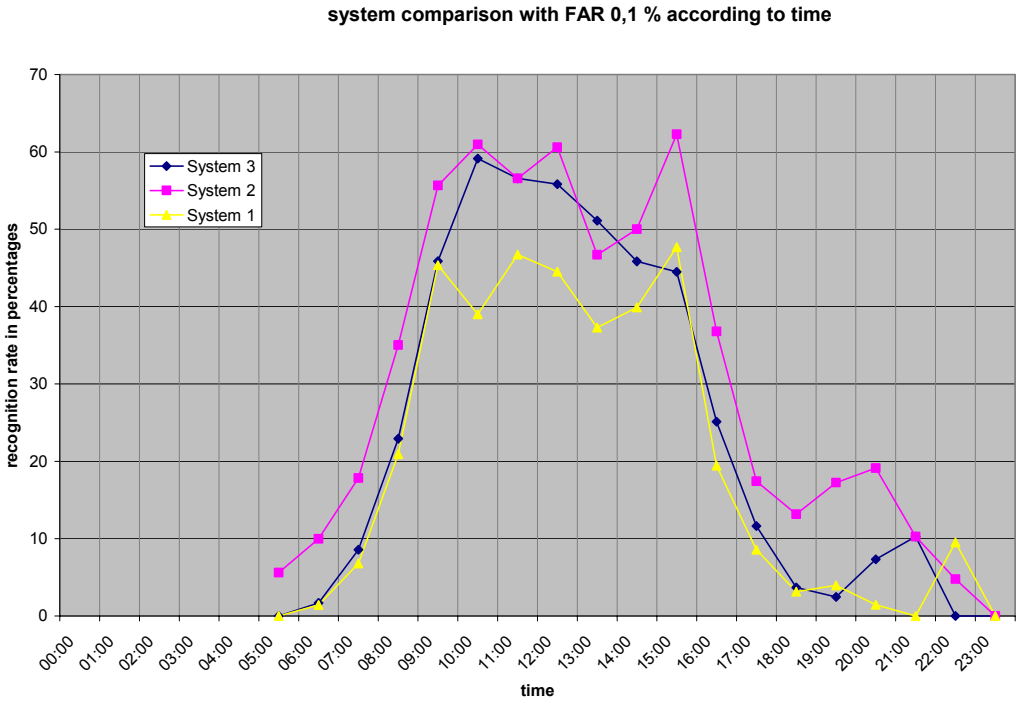


Figure 17

In order to do justice to the face recognition systems, closer inspection is also required here. Figure 16 does not take the environmental conditions into account. Figure 17 illustrates the recognition performances of the systems dependent on time and in this way enables a comparison under changing lighting conditions. Times when the monitored area was crossed less than ten times by test persons were not included in the diagram. A differentiation between escalator and stairs was dispensed with at this point.

5 Summarised interpretation of the results and recommendations

The "Foto-Fahndung" project confirmed that it is possible from a technical point of view to use face recognition systems in search scenarios. The tests were not confined exclusively to the algorithms of the manufacturers but encompassed complete systems to which the camera technology which was used in the monitoring of the area also belongs.

If we take the complete systems into consideration, one system emerges a clear winner. This is system 2, which made the best overall impression. This system offered the best coordinated biometrics and camera technology package.

The field test showed that environmental conditions such as lighting and quick movements exert considerable influence on the recognition performances of the systems. Under real operational conditions, recognition performances of over 60% with a false acceptance rate of 0.1% can be achieved without any great time and effort being involved.

By employing simple measures it should be possible to minimise the influences which still impacted negatively on the recognition performances in our field test. Through measures which steer the test persons' line of vision towards the cameras (e. g. a marquee in the

proximity of the cameras), it would easily have been possible to again obtain better comparison images from the video stream. A higher number of frontal images would undoubtedly have brought about an increase in the number of correct matches and a decrease in the number of false acceptances.

If the possibility exists to split up the crowds and foster a co-operative form of behaviour, for example, during entry checks, it can be expected that the large majority of wanted persons will be reliably identified by a biometric face recognition system.

Depending on the operational situation, response times have to be planned for the operational forces who, in the case of an identification, will implement further measures. It has to be borne in mind that in a public place a person can already gain such distance from the surveillance area within one minute that it is difficult or impossible to find him again.

A realistically tolerable false acceptance rate of 0.1% is a manageable value. However, it also shows that the final decision on whether identification can be authenticated is always in the hands of a person who already adjudicates the on-screen identification. Otherwise, at Mainz central station about 23 citizens a day would have been subjected to further measures due to false acceptances.

6 Outlook

As can be deduced from the results achieved, recognition probability and recognition precision depend greatly on external influences. Thus, besides the lighting, different postures and inclinations of the head exert considerable influence on the recognition performances of the systems.
Three-dimensional (3D) face recognition technology is a solution which can bring about improvements to this situation. A European project aimed at developing a 3D face recognition algorithm is currently being conducted under the working title 3D-Face. Although the objective of 3D face recognition is completely different, namely for the purpose of verification of personal ID documents, it will also be possible to use the results for identification purposes. In accordance with current planning, a field test is scheduled to be conducted in April 2009 to test the performance capacity of the algorithm which is to be developed.

In this connection, it is conceivable that in future when an offender is being photographed and fingerprinted, a three-dimensional image can be created. In later identifications, inclinations and turnings of the head could be corrected to a certain extent by aligning the stored 3D model with the angle from which the 2D live image was taken.

It is assumed that further potential for enhancing the total systems lies in the digital imaging technology. Analogue surveillance cameras are currently being replaced by digital ones. This changeover is still at an early stage. Improved quality in imaging technology and camera controls is to be expected and this will contribute towards making better image material for biometric comparisons.

By order

signed.
Pretzel, KOK

signed.
Lotz, TB