Neural Systems for Complex Identification Tasks: The Access Control System ZN-Face and the Alarm Identification SENECA for Steel Casting Processes

M. Hormel, W. Konen, S. Fuhrmann and A. Flügel

ZN GmbH, Bochum
Germany
WWW: http://www.zn.ruhr-uni-bochum.de

Abstract. *Neural systems have become a widely used tool in many industrial and commercial applications. We report in this contribution on new applications of diagnosis and identification systems in two areas.*
Firstly, we present the access control system ZN-Face, a product developped at the ZN, which makes automated face recognition available for commercial access control systems. Neural systems have the necessary flexibility to analyse the visual information correctly, which we perceive so easily as a person's face. ZN-Face combines high recognition rates (99 %) with fast computation (3 sec) on standard hardware components (PC). The system is integrated into an easy-to-use GUI. ZN-Face is in daily operation at a large company since summer 1995. – Secondly, we report on a neural system for industrial process diagnosis, namely alarm identification in continuous steel casting, where a neural net in combination with a fuzzy system detects dangerous "hot spot"-process faults (breakouts) from the observation of high-dimensional temperature data. The system successfully detects previously undetected alarms and reduces the false alarm rate by a factor of 7. It is now (since spring 1995) installed at a major German steel manufacturing company.

1 Introduction

Technical diagnosis systems require reliable recognition or identification of complex patterns. Neural information processing has proven to be a very useful and robust technique in such pattern recognition tasks. The goal of a diagnosis is usually to identify certain critical states ("alarm states") of a process, and it can be broken down into two sub-goals: (i) reliable identification of true alarm states as early as possible and (ii) low probability of false alarms. In this contribution we describe two successful applications of this general scheme in different areas:

- Access control requires identification of persons from certain legitimation data. Here, we report on the access control product ZN-Face, which identifies persons from their facial images. An "alarm" is in this case the attempt of an imposter to gain access pretending to carry the face of an authorized person. "Low false alarm rates" means the reliable identification of authorized persons (better than 99% required).
- Continuous steel casting requires the identification of certain alarm states (breakouts). A hybrid neuro-fuzzy system SENECA has been developed and integrated into the steel casting process and has proven to perform better than the previous heuristic system.

2 Identification of faces

Face recognition is a remarkable example for the ability of humans to perform with great reliability a complex visual recognition task. We are able to recognize thousands of faces which we have learned during our lifetime. Our visual performance is very robust against a variety of factors like changes in facial expression, head posture or size, illumination, background, facial aging or partial occlusion of a face. It is one of the challenges of artificial information processing to achieve at least partially a similar performance on systems for automated visual recognition. The ease with which the problem is solved by the human brain, i. e. a biological neural system, may serve as a guideline in the sense that neural information processing paradigms are important also for the construction of automated face recognition systems.

Numerous approaches for solving the face recognition problem can be found in the literature; a comprehensive survey of the state of the art can be found in [1, 2, 3, 4].

In this contribution we will report on the development of the face recognition system ZN-Face which offers a turn-key solution for an access

control system.

2.1 Face recognition by graph matching

The basic recognition algorithm of ZN-Face is described in [4] and is an extension of the Elastic Graph Matching Algorithm [5]. Here, faces are stored as flexible graphs or grids (see Fig. 1) with characteristic visual features (Gabor features) attached to the nodes of the graph (*labeled graphs*).

A **B**

Fig. 1. **(A)** *Labeled graphs are the data representation in* ZN-Face. **(B)** *Such graphs can be shifted, scaled and deformed efficiently in the image domain.*

A data representation with labeled graphs has computational advantages:

robustness: Gabor features are invariant against intensity or contrast changes in the image. Furthermore, Gabor features are less affected by changes in head posture, size and facial expression than raw grey level features.

data compression: compared to the raw image which in our case has a size of 128×128 pixels, the size of the graph (about 1.6 kB) is smaller by a factor of 10.

scaling: a sparse graph can be readily adjusted to changes in the geometry (size, perspective, see Fig. 1B). Change in size in a pixel-based data representation, for example, would require a more complicated transformation.

distribution: Compared to a high-level feature description (e.g. 'eye', 'nose') the graph contains sufficient information distribution on simple, but numerous features. Even if the information at a single graph node is missing due to occlusion, recognition is usually still possible due to the information at the remaining nodes.

2.2 Access Control with ZN-Face

Fig. 2. *The access control system* ZN-Face *in a prototype realization, consisting of camera (behind semi-permeable mirror), LC-display and card reader.*

ZN-Face offers an automated access control system which performs a biometric identification of persons from their facial images. To achieve this, several extensions are necessary to transform the Elastic Graph Matching algorithm of Sec. 2.1 into a system which is easy to use in real-world security applications:

- *Fast computation on standard hardware:* In [5] the graph matching was performed on a transputer-based platform and required about 12 seconds for the identification. Now, the algorithm has been optimized and ported to a standard PC (Pentium PC/90 Mhz *without* special accelerator hardware). Computation time for a full identification is 3.5 seconds.
- *Semi-automated image acquisition:* No operator is available to adjust the camera (persons may differ in their height and their

distance to the camera) and to trigger the image acquisition. An appropriate semi-automated procedure is described below.
- *Easy-to-use system administration:* A Windows-based[1] GUI has been developed which allows simple control by an authorized system administrator (e.g. adding or deleting access rights, monitoring the access protocol).
- *Possibility to handle large databases (1000 persons and more).*

In order to achieve the last point without unacceptable increase in computation time, we perform with ZN-Face *identification* instead of recognition. Identification has the additional advantage of higher security because in addition to a standard personal identification via secret number (ID) or card, the face is used as independent control of the person's identity.

The basic identification procedure can be described as follows: The hardware setup of the system consists of a standard PC with framegrabber and a ZN-Face console (a prototype is shown in Fig. 2) containing camera, ID acquisition device (card reader or numeric pad) and LC-display. The camera is positioned behind a semi-permeable mirror which is tilted about $30 - 50^o$ against the vertical line. Camera and mirror are tilted in order to allow users of different height to view and position themselves centrally in front of the camera. (at the expense of some size variation in the acquired facial images). The user triggers the image acquisition and identifies himself. Now ZN-Face starts the identification whether the graph stored under the given ID in the database fits to the acquired image. This does not require to search the whole database, but only the stored graphs to the given ID and a fixed number of reference graphs have to be searched.

It has to be mentioned that even with the user's cooperation during image acquisition, there is considerable variation in the images with respect to head posture, size and position. This is due to the user-dependence of the automated image acquisition. Most of the variation can be handled successfully by the robustness of the elastic graph matching. Also, variations like different facial expressions or wearing glasses are handled very well by the algorithm. To cope with the remaining cases, the system offers the possibility to store more than one image for a given person ("teach-in", see below).

[1] Windows is a registered trademark of Microsoft

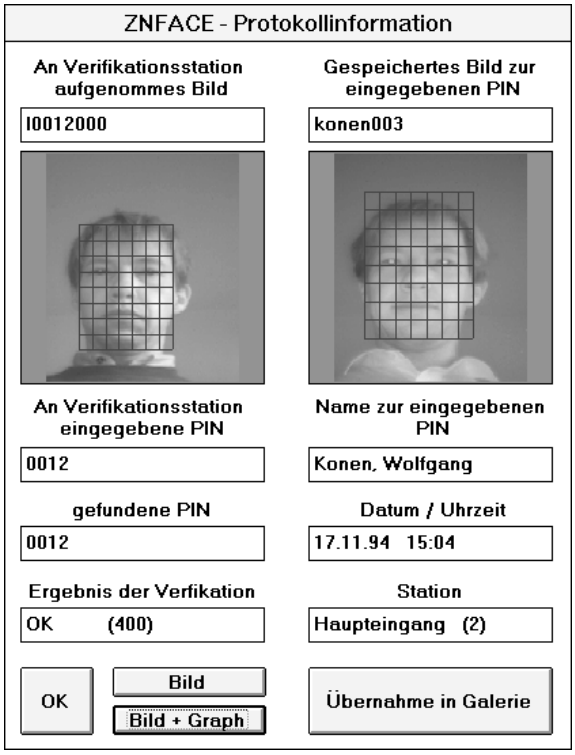

Fig. 3. *Protocol of the identification: On the left hand side the actually acquired image is shown, on the right hand side the best matching image from the database (to the given ID).*

Adding new persons to the database is made very simple for an authorized system administrator by using the graphical user interface (GUI) under Windows. In addition, the GUI offers a facility to browse through the identification protocol (Fig. 3). This control panel also offers the possibility of "teach-in": If an image acquired during identification is rejected although it shows the correct person (perhaps because stored and acquired image differ too strongly in head posture, thus leading to a low significance), the authorized system administrator has the option to add the picture into the person's record in the database. The system can handle an arbitrary number of images in a persons's record, although normally 1-3 images are sufficient for reliable identification.

2.3 Results

Nearly all papers on face recognition algorithms – with the exception of [5] – usually report only on the recognition rate achieved by the algorithm, i. e. how successfully a person is accepted whose image is in the database. But this is only one side

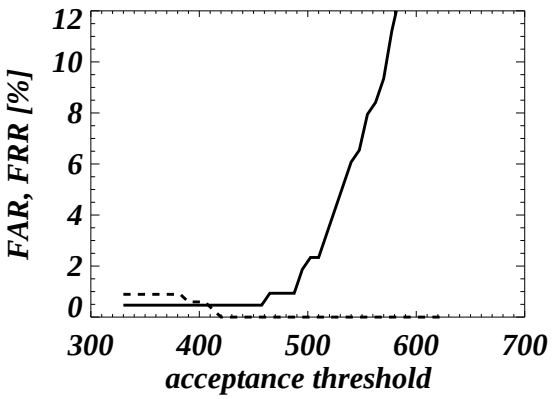

Fig. 4. *False rejection rate (FRR, solid line) and false acceptance rate (FAR, dashed line) from 800 identification trials as a function of the adjustable acceptance threshold.*

of the coin: Often even more important for biometric devices is the question, how successfully persons are rejected whose image is *not* in the database. Biometric research names errors of the former kind as *False Rejection Rate (FRR)* while errors of the latter kind contribute to the *False Acceptance Rate (FAR)*. Of course, there is a trade-off between both types of errors and consequently it is much more difficult to build a system with a high recognition rate *and* a low FAR than a system with a high recognition rate alone.

Fig. 4 shows the results of 800 face identifications (400 authentics, 400 imposters) as a function of the acceptance threshold. Unsuccessful identifications of authentics (acceptance value too low) contribute to the FRR and false acceptances of imposters contribute to the FAR. As can be seen from Fig. 4, the combined minimum of FAR and FRR is achieved at a level of 0.5%. Setting the threshold to the 'safe' value 470 still produces a identification rate of better than 99% ($FRR < 1\%$).

The system has also been shown recently 'live' on several exhibitions (SECURITY'94 and CeBit'95 and '96) where it operated successfully under real-world conditions with 'untrained' visitors. Since summer 1995 ZN-Face is in daily operation at a large company and it is very well accepted by the users, because face identification is one of the least "intrusive" biometric techniques.

3 Alarm identification with SENECA

In a continuous casting facility molten steel is poured from a melting pot into a tundish and from there into a watercooled mold where it solidifies (Fig. 5). The solid steel is then cut into pieces of a fixed length for further treatment in a rolling mill. Due to the cooling within the mold the steel develops a solid shell which surrounds a still molten core when it is withdrawn from the mold. From time to time the the formation of the solid shell is disturbed so that a rupture of the shell, a so called "breakout", occurs once the rupture leaves the mold and liquid steel leaks into the facilities. This causes long shutdown times and enormous costs.

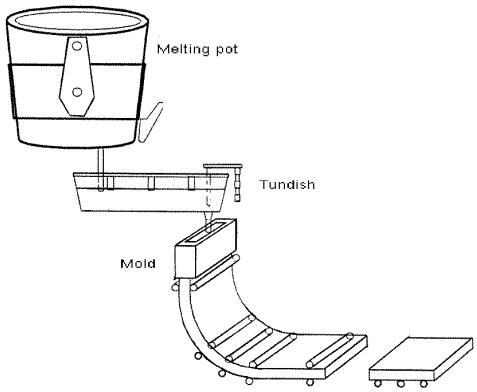

Fig. 5. *Continous Steel Casting*

One reason for breakouts is the effect of molten steel sticking to the walls of the mold which has been investigated eg. in [6]. When the steel is withdrawn from the mold a rupture of the solidifying shell at the lower end of sticking point occurs. Due to the movement of the steel and new material filling the gap the sticker grows. The rupture therefore travels downwards and can be detected by a sudden temperature increase measured at the wall of the mold (Fig. 6).

Today most casting facilities are equipped with a system which monitors many parameters of the casting process including several temperatures measured at the mold. These systems can be used to implement a mechanism for detection and prevention of breakouts but there exist at least two problems with conventional breakout-detection mechanisms.

1. The detection-system has to be robust

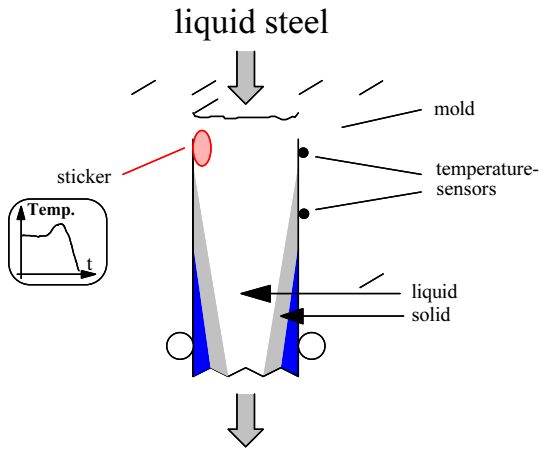

Fig. 6. *Sticker formation in the mold*

against variations in measured temperatures which depend on variations eg. in casting speed and other parameters.

2. The system should generate as few false alarms as possible, since the area where a false alarm occured is cut out. This leads to shorter steel bars and affects all successive processing steps.

3.1 Neural network approach to breakout detection

To detect the temperature signal pattern which is characteristic for a rupture the neural-network based system SENECA has been developed. It consists of individual multi-layer-perceptron networks for each sensor which share their weights among each other and generate a response whether the network detected a rupture or not.

Special care must be taken of temperature-sensors which are near the edges of the mold. The signals measured here show a much greater variation than the signals near the middle. To cope with this effect a fuzzy-logic based system performs a weigthing of the output of the neural networks, depending on the temperature differences to sensors in the neighbourhood.

The system was trained with data collected from 262 casting processes which have occurred during the operation of the casting facility. Within this data were 86 real and 171 false alarms detected by a conventional algorithm. A selected training set of real and false alarms has been used to train to the neural network.

3.2 Performance of the system

Offline evaluation of the system performance based on the available data has shown that SENECA was able to correctly detect all real alarms. Moreover, it was able to identify five ruptures which have not been found by the conventional system and led to a real breakout. The rate of false alarms generated by the detection mechanism could be lowered to about 20% of the conventional algorithm.

Over a period of several months the system has been tested in parallel to the conventional algorithm. The results of the offline-evaluation have been fully confirmed. All real alarms have been detected by both systems. However, the alarms from the neural detection system SENECA came up to 14 seconds earlier than those of the conventional system. In online operation, SENECA's false alarm rate is about 25% compared to the conventional system. This can be improved further by using the collected data for additional training.

4 Conclusion and outlook

Elastic Graph Matching has proven to be a powerful algorithm for the identification of human faces. This makes it an appropriate tool for a biometric access control device which has been presented in this work. The fast identification of faces on standard hardware opens new application possibilities on the biometry market. Further developments will be made in the direction of fully automated acquisition of facial images and face localization in more complex scenes.

The ability of neural networks to detect complex patterns in noisy signals makes them a valuable tool in almost any fault detection system and helps in increasing the production's quality standards. SENECA is one example for a neural-network based system which has been trained using historical data and which can improve continously by learning from experiences gathered during online operation.

References

1. V. Bruce and M. Burton. *Processing Images of Faces.* ABLEX Publishing-Corporation, Norwood, NJ, 1992.
2. M. Turk and A. Pentland. Face recognition using eigenfaces. In *IEEE Proc. of CVPR*, pages 586–591, Maui, Hawaii, June 1991.

3. M. Bichsel, editor. *Proceedings of the International workshop on automatic face- and gesture-recognition (IWAFGR)*, MultiMedia Laboratory, University of Zurich, Switzerland, 1995.
4. W. Konen and E. Schulze-Krüger. ZN-Face: A system for access control using automated face recognition. In M. Bichsel, editor, *Int. Workshop on Face and Gesture Recognition*, 1995.
5. M. Lades, J. Vorbrüggen, J. Buhmann, J. Lange, C.v.d. Malsburg, R.P. Würtz, and W. Konen. Distortion invariant object recognition in the dynamic link architecture. *IEEE Transaction on Computers*, 42:300–311, 1993.
6. Kenneth E. Blazek and Ismael G. Saucedo. Characterization of the formation, propagation and recovery of sticker/hanger type breakouts. *ISIJ International*, 30(6):435–443, 1990.