Abstract — Faces represent complex multidimensional meaningful visual stimuli and developing a computational model for face recognition is difficult. We present a hybrid neural-network solution which compares favorably with other methods. The system combines local image sampling, a self-organizing map (SOM) neural network, and a convolutional neural network. The SOM provides a quantization of the image samples into a topological space where inputs that are nearby in the original space are also nearby in the output space, thereby providing dimensionality reduction and invariance to minor changes in the image sample, and the convolutional neural network provides for partial invariance to translation, rotation, scale, and deformation. The convolutional network extracts successively larger features in a hierarchical set of layers. We present results using the Karhunen–Loève (KL) transform in place of the SOM, and a multilayer perceptron (MLP) in place of the convolutional network. The KL transform performs almost as well (5.3% error versus 3.8%). The MLP performs very poorly (40% error versus 3.8%). The method is capable of rapid classification, requires only fast approximate normalization and preprocessing, and consistently exhibits better classification performance than the eigenfaces approach on the database considered as the number of images per person in the training database is varied from one to five. With five images per person the proposed method and eigenfaces result in 3.8% and 10.5% error, respectively. The recognizer provides a measure of confidence in its output and classification error approaches zero when rejecting as few as 10% of the examples. We use a database of 400 images of 40 individuals which contains quite a high degree of variability in expression, pose, and facial details. We analyze computational complexity and discuss how new classes could be added to the trained recognizer.


I. INTRODUCTION

The requirement for reliable personal identification in computerized access control has resulted in an increased interest in biometrics. Biometrics being investigated include fingerprints [4], speech [7], signature dynamics [36], and face recognition [8]. Sales of identity verification products exceed $100 million [29]. Face recognition has the benefit of being a passive, nonintrusive system for verifying personal identity. The techniques used in the best face recognition systems may depend on the application of the system. We can identify at least two broad categories of face recognition systems.

1) We want to find a person within a large database of faces (e.g., in a police database). These systems typically return a list of the most likely people in the database [34]. Often only one image is available per person. It is usually not necessary for recognition to be done in real-time.

2) We want to identify particular people in real-time (e.g., in a security monitoring system, location tracking system, etc.), or we want to allow access to a group of people and deny access to all others (e.g., access to a building, computer, etc.) [8]. Multiple images per person are often available for training and real-time recognition is required.

In this paper, we are primarily interested in the second case. We are interested in recognition with varying facial detail, expression, pose, etc. We do not consider invariance to high degrees of rotation or scaling—we assume that a minimal preprocessing stage is available if required. We are interested in rapid classification and hence we do not assume that time is available for extensive preprocessing and normalization. Good algorithms for locating faces in images can be found in [37], [40], and [43].

The remainder of this paper is organized as follows. The data we used is presented in Section II and related work with this and other databases is discussed in Section III. The components and details of our system are described in Sections IV and V, respectively. We present and discuss our results in Sections VI and VII. Computational complexity is considered in Section VIII. Section IX lists avenues for further research, and we draw conclusions in Section X.

II. DATA

We have used the ORL database, which contains a set of faces taken between April 1992 and April 1994 at the Olivetti
Research Laboratory in Cambridge, U.K.\textsuperscript{3} There are ten different images of 40 distinct subjects. For some of the subjects, the images were taken at different times. There are variations in facial expression (open/closed eyes, smiling/nonsmiling), and facial details (glasses/no glasses). All the images were taken against a dark homogeneous background with the subjects in an upright frontal position, with tolerance for some tilting and rotation of up to about 20 degrees. There is some variation in scale of up to about 10%. Thumbnails of all of the images are shown in Fig. 1 and a larger set of images for one subject is shown in Fig. 2. The images are greyscale with a resolution of 92 × 112.

\textsuperscript{3}The ORL database is available free of charge, see http://www.cam- orl.co.uk/facedatabase.html.

III. RELATED WORK

A. Geometrical Features

Many people have explored geometrical feature based methods for face recognition. Kanade [17] presented an automatic feature extraction method based on ratios of distances and reported a recognition rate of between 45–75% with a database of 20 people. Brunelli and Poggio [6] compute a set of geometrical features such as nose width and length, mouth position, and chin shape. They report a 90% recognition rate on a database of 47 people. However, they show that a simple template matching scheme provides 100% recognition for the same database. Cox \textit{et al.} [9] have recently introduced a \textit{mixture-distance} technique which achieves a recognition rate
of 95% using a query database of 95 images from a total of 685 individuals. Each face is represented by 30 manually extracted distances.

Systems which employ precisely measured distances between features may be most useful for finding possible matches in a large mugshot database.\(^4\) For other applications, automatic identification of these points would be required and the resulting system would be dependent on the accuracy of the feature location algorithm. Current algorithms for automatic location of feature points do not provide a high degree of accuracy and require considerable computational capacity [41].

B. Eigenfaces

High-level recognition tasks are typically modeled with many stages of processing as in the Marr paradigm of progressing from images to surfaces to three-dimensional (3-D) models to matched models [28]. However, Turk and Pentland [43] argue that it is likely that there is also a recognition process based on low-level two-dimensional (2-D) image processing. Their argument is based on the early development and extreme rapidity of face recognition in humans and on physiological experiments in a monkey cortex which claim to have isolated neurons that respond selectively to faces [35]. However, it is not clear that these experiments exclude the sole operation of the Marr paradigm.

Turk and Pentland [43] present a face recognition scheme in which face images are projected onto the principal components of the original set of training images. The resulting eigenfaces are classified by comparison with known individuals.

Turk and Pentland present results on a database of 16 subjects with various head orientation, scaling, and lighting. Their images appear identical otherwise with little variation in facial expression, facial details, pose, etc. For lighting, orientation, and scale variation their system achieves 96%, 85%, and 64% correct classification, respectively. Scale is renormalized to the eigenface size based on an estimate of the head size. The middle of the faces is accentuated, reducing any negative affect of changing hairstyle and backgrounds.

In Pentland et al. [33], [34] good results are reported on a large database (95% recognition of 200 people from a database of 3000). It is difficult to draw broad conclusions as many of the images of the same people look very similar, and the database has accurate registration and alignment [30]. In Moghaddam and Pentland [30], very good results are reported with the FERET database—only one mistake was made in classifying 150 frontal view images. The system used extensive preprocessing for head location, feature detection, and normalization for the geometry of the face, translation, lighting, contrast, rotation, and scale.

Swets and Weng [42] present a method of selecting discriminant eigenfeatures using multidimensional linear discriminant analysis. They present methods for determining the most expressive features (MEF) and the most discriminatory features (MDF). We are not currently aware of the availability of results which are comparable with those of eigenfaces (e.g., on the FERET database as in Moghaddam and Pentland [30]).

In summary, it appears that eigenfaces is a fast, simple, and practical algorithm. However, it may be limited because optimal performance requires a high degree of correlation between the pixel intensities of the training and test images. This limitation has been addressed by using extensive preprocessing to normalize the images.

C. Template Matching

Template matching methods such as [6] operate by performing direct correlation of image segments. Template matching is only effective when the query images have the same scale, orientation, and illumination as the training images [9].

D. Graph Matching

Another approach to face recognition is the well known method of graph matching. In [21], Lades et al. present a dynamic link architecture for distortion invariant object recognition which employs elastic graph matching to find the closest stored graph. Objects are represented with sparse graphs whose vertices are labeled with a multiresolution description in terms of a local power spectrum, and whose edges are labeled with geometrical distances. They present good results with a database of 87 people and test images composed of different expressions and faces turned 15\(^\circ\). The matching process is computationally expensive, taking roughly 25 s to compare an image with 87 stored objects when using

---

\(^4\) A mugshot database typically contains side views where the performance of feature point methods is known to improve [8].
Fig. 3. A depiction of the local image sampling process. A window is stepped over the image and a vector is created at each location.

a parallel machine with 23 transputers. Wiskott et al. [45] use an updated version of the technique and compare 300 faces against 300 different faces of the same people taken from the FERET database. They report a recognition rate of 97.3%. The recognition time for this system was not given.

E. Neural-Network Approaches

Much of the present literature on face recognition with neural networks presents results with only a small number of classes (often below 20). We briefly describe a couple of approaches.

In [10] the first 50 principal components of the images are extracted and reduced to five dimensions using an autoassociative neural network. The resulting representation is classified using a standard multilayer perceptron (MLP). Good results are reported but the database is quite simple: the pictures are manually aligned and there is no lighting variation, rotation, or tilting. There are 20 people in the database.

A hierarchical neural network which is grown automatically and not trained with gradient descent was used for face recognition by Weng and Huang [44]. They report good results for discrimination of ten distinctive subjects.

F. The ORL Database

In [39] a hidden Markov model (HMM)-based approach is used for classification of the ORL database images. The best model resulted in a 13% error rate. Samaria also performed extensive tests using the popular eigenfaces algorithm [43] on the ORL database and reported a best error rate of around 10% when the number of eigenfaces was between 175 and 199. We implemented the eigenfaces algorithm and also observed around 10% error. In [38] Samaria extends the top-down HMM of [39] with pseudo 2-D HMM’s. The error rate reduces to 5% at the expense of high computational complexity—a single classification takes 4 min on a Sun Spare II. Samaria notes that although an increased recognition rate was achieved the segmentation obtained with the pseudo 2-D HMM’s appeared quite erratic. Samaria uses the same training and test set sizes as we do (200 training images and 200 test images with no overlap between the two sets). The 5% error rate is the best error rate previously reported for the ORL database that we are aware of.

IV. SYSTEM COMPONENTS

A. Overview

In the following sections we introduce the techniques which form the components of our system and describe our motivation for using them. Briefly, we explore the use of local image sampling and a technique for partial lighting invariance, a self-organizing map (SOM) for projection of the image sample representation into a quantized lower dimensional space, the Karhunen-Loève (KL) transform for comparison with the SOM, a convolutional network (CN) for partial translation and deformation invariance, and an MLP for comparison with the convolutional network.

B. Local Image Sampling

We have evaluated two different methods of representing local image samples. In each method a window is scanned over the image as shown in Fig. 3.

1) The first method simply creates a vector from a local window on the image using the intensity values at each point in the window. Let \( x_{ij} \) be the intensity at the \( i \)th column and the \( j \)th row of the given image. If the local window is a square of sides \( W \) long, centered on \( x_{ij} \), then the vector associated with this window is simply \( [x_{i-W_j, i+j-W+1} : \ldots : x_{i+j, i+j+W-1} : x_{i+W_j, i+j+W}] \).

2) The second method creates a representation of the local sample by forming a vector out of 1) the intensity of the center pixel \( x_{ij} \), and 2) the difference in intensity between the center pixel and all other pixels within the square window. The vector is given by \( [x_{ij} - x_{i-W_j, i+j-W} : \ldots : x_{i-W_j, i+j+W-1} : \ldots : x_{i+j, i+j+W} : x_{i+W_j, i+j+W}] \). The resulting representation becomes partially invariant to variations in intensity of the complete sample. The degree of
invariance can be modified by adjusting the weight $w_{ij}$ connected to the central intensity component.

C. The Self-Organizing Map

1) Introduction: Maps are an important part of both natural and artificial neural information processing systems [2]. Examples of maps in the nervous system are retinotopic maps in the visual cortex [31], tonotopic maps in the auditory cortex [18], and maps from the skin onto the somatosensory cortex [32]. The SOM, introduced by Kohonen [19], [20], is an unsupervised learning process which learns the distribution of a set of patterns without any class information. A pattern is projected from an input space to a position in the map—information is coded as the location of an activated node. The SOM is unlike most classification or clustering techniques in that it provides a topological ordering of the classes. Similarity in input patterns is preserved in the output of the process. The topological preservation of the SOM process makes it especially useful in the classification of data which includes a large number of classes. In the local image sample classification, for example, there may be a very large number of classes in which the transition from one class to the next is practically continuous (making it difficult to define hard class boundaries).

2) Algorithm: We give a brief description of the SOM algorithm, for more details see [20]. The SOM defines a mapping from an input space $\mathbb{R}^n$ onto a topologically ordered set of nodes, usually in a lower dimensional space. An example of a 2-D SOM is shown in Fig. 4. A reference vector in the input space, $\mathbf{m}_i = [\mu_{i1}, \mu_{i2}, \cdots, \mu_{in}]^T \in \mathbb{R}^n$, is assigned to each node in the SOM. During training, each input vector, $\mathbf{x}$, is compared to all of the $\mathbf{m}_i$, obtaining the location of the closest match $\mathbf{m}_c$ (given by $||\mathbf{x} - \mathbf{m}_c|| = \min_i ||\mathbf{x} - \mathbf{m}_i||$) where $||\cdot||$ denotes the norm of vector $\mathbf{a}$. The input point is mapped to this location in the SOM. Nodes in the SOM are updated according to

$$m_c(t + 1) = m_c(t) + h_{ci}(t)[x(t) - m_c(t)] \tag{1}$$

where $t$ is the time during learning and $h_{ci}(t)$ is the neighborhood function, a smoothing kernel which is maximum at $m_c$. Usually, $h_{ci}(t) = h(|r_c - r_i|, t)$, where $r_c$ and $r_i$ represent the location of the nodes in the SOM output space. $r_c$ is the node with the closest weight vector to the input sample and $r_i$ ranges over all nodes. $h_{ci}(t)$ approaches 0 as $|r_c - r_i|$ increases and also as $t$ approaches $\infty$. A widely applied neighborhood function is

$$h_{ci} = \alpha(t) \exp\left(-\frac{|r_c - r_i|^2}{2\sigma^2(t)}\right) \tag{2}$$

where $\alpha(t)$ is a scalar valued learning rate and $\sigma(t)$ defines the width of the kernel. They are generally both monotonically decreasing with time [20]. The use of the neighborhood function means that nodes which are topographically close in the SOM structure are moved toward the input pattern along with the winning node. This creates a smoothing effect which leads to a global ordering of the map. Note that $\sigma(t)$ should not be reduced too far as the map will lose its topographical order if neighboring nodes are not updated along with the closest node. The SOM can be considered a nonlinear projection of the probability density, $p(\mathbf{x})$ [20].

3) Improving the Basic SOM: The original SOM is computationally expensive due to the following.

1) In the early stages of learning, many nodes are adjusted in a correlated manner. Luttrel [27] proposed a method, which is used here, that starts by learning in a small network, and doubles the size of the network periodically during training. When doubling, new nodes are inserted between the current nodes. The weights of the new nodes are set equal to the average of the weights of the immediately neighboring nodes.

2) Each learning pass requires computation of the distance of the current sample to all nodes in the network, which is $O(N)$. However, this may be reduced to $O(\log N)$ using a hierarchy of networks which is created from the above node doubling strategy.\footnote{This assumes that the topological order is optimal prior to each doubling step.}

D. KL Transform

The optimal linear method\footnote{In the least mean squared error sense.} for reducing redundancy in a dataset is the KL transform or eigenvector expansion via principle components analysis (PCA) [12]. PCA generates a set of orthogonal axes of projections known as the principal components, or the eigenvectors, of the input data distribution in the order of decreasing variance. The KL transform is a well-known statistical method for feature extraction and multivariate data projection and has been used widely in pattern recognition, signal processing, image processing, and data analysis. Points in an $n$-dimensional input space are projected into an $m$-dimensional space, $m \leq n$. The KL transform is used here for comparison with the SOM in the dimensionality reduction of the local image samples. The KL transform is also used in eigenfaces, however in that case it
is used on the entire images, whereas it is only used on small local image samples in this work.

**E. Convolutional Networks**

The problem of face recognition from 2-D images is typically very ill-posed, i.e., there are many models which fit the training points well but do not generalize well to unseen images. In other words, there are not enough training points in the space created by the input images in order to allow accurate estimation of class probabilities throughout the input space. Additionally, for MLP networks with 2-D images as input, there is no invariance to translation or local deformation of the images [23].

Convolutional networks (CN) incorporate constraints and achieve some degree of shift and deformation invariance using three ideas: local receptive fields, shared weights, and spatial subsampling. The use of shared weights also reduces the number of parameters in the system aiding generalization. Convolutional networks have been successfully applied to character recognition [3], [5], [22]–[24].

A typical convolutional network is shown in Fig. 5 [24]. The network consists of a set of layers each of which contains one or more planes. Approximately centered and normalized images enter at the input layer. Each unit in a plane receives input from a small neighborhood in the planes of the previous layer. The idea of connecting units to local receptive fields dates back to the 1960’s with the perceptron and Hubel and Wiesel’s [15] discovery of locally sensitive orientation-selective neurons in the cat’s visual system [23]. The weights forming the receptive field for a plane are forced to be equal at all points in the plane. Each plane can be considered as a feature map which has a fixed feature detector that is convolved with a local window which is scanned over the planes in the previous layer. Multiple planes are usually used in each layer so that multiple features can be detected. These layers are called convolutional layers. Once a feature has been detected, its exact location is less important. Hence, the convolutional layers are typically followed by another layer which does a local averaging and subsampling operation (e.g., for a subsampling factor of two: \( y_{ij} = \frac{1}{4} (x_{2i,j} + x_{2i+1,j} + x_{2i,j+1} + x_{2i+1,j+1}) \) where \( y_{ij} \) is the output of a subsampling plane at position \( i,j \) and \( x_{ij} \) is the output of the same plane in the previous layer). The network is trained with the usual backpropagation gradient-descent procedure [13]. A connection strategy can be used to reduce the number of weights in the network. For example, with reference to Fig. 5, Le Cun et al. [24] connect the feature maps in the second convolutional layer only to one or two of the maps in the first subsampling layer (the connection strategy was chosen manually).

**V. System Details**

The system we have used for face recognition is a combination of the preceding parts—a high-level block diagram is shown in Figs. 6 and 7 shows a breakdown of the various subsystems that we experimented with or discuss.

Our system works as follows (we give complete details of dimensions etc. later).

1) For the images in the training set, a fixed size window (e.g., \( 5 \times 5 \)) is stepped over the entire image as shown in Fig. 3 and local image samples are extracted at each step. At each step the window is moved by four pixels.

2) An SOM (e.g., with three dimensions and five nodes per dimension, \( 5^3 = 125 \) total nodes) is trained on the vectors from the previous stage. The SOM quantizes the 25-dimensional input vectors into 125 topologically
ordered values. The three dimensions of the SOM can be thought of as three features. We also experimented with replacing the SOM with the KL transform. In this case, the KL transform projects the vectors in the 25-dimensional space into a 3-D space.

3) The same window as in the first step is stepped over all of the images in the training and test sets. The local image samples are passed through the SOM at each step, thereby creating new training and test sets in the output space created by the SOM. (Each input image is now represented by three maps, each of which corresponds to a dimension in the SOM. The size of these maps is equal to the size of the input image (92 × 112) divided by the step size (for a step size of four, the maps are 23 × 28).

4) A convolutional neural network is trained on the newly created training set. We also experimented with training a standard MLP for comparison.

A. Simulation Details

In this section we give the details of one of the best performing systems. For the SOM, training is split into two phases as recommended by Kohonen [20]—an ordering phase and a fine-adjustment phase. In the first phase 100,000 updates are performed, and in the second 50,000 are performed. In the first phase, the neighborhood radius starts at two-thirds of the size of the map and reduces linearly to one. The learning rate during this phase is \( \alpha \times \left(1 - n/N\right)\)

The convolutional network contained five layers excluding the input layer. A confidence measure was calculated for each classification:

\[
y_i = \frac{\exp(u_i)}{\sum_{j=1}^{k} \exp(u_j)}
\]

where \(u_i\) are the original outputs, \(y_i\) are the transformed outputs, and \(k\) is the number of outputs. The number of planes in each layer, the dimensions of the planes, and the dimensions of the receptive fields are shown in Table I. The network was trained with backpropagation [13] for a total of 20,000 updates. Weights in the network were updated after each pattern presentation, as opposed to batch update where weights are only updated once per pass through the training set. All inputs were normalized to lie in the range \([-1, 1]\). All nodes included a bias input which was part of the optimization process. The best of ten random weight sets was chosen for the initial parameters of the network by evaluating the performance on the training set. Weights were initialized on a node by node basis as uniformly distributed random numbers in the range \([-\text{fan-in}, \text{fan-in}]\) where \(\text{fan-in}\) is the fan-in of neuron \(j\) [13]. Target outputs were 0.8 and 0.8 using the \(\tanh\) output activation function.\(^7\) The quadratic cost function

\(^7\)This helps avoid saturating the sigmoid function. If targets were set to the asymptotes of the sigmoid this would tend to: 1) drive the weights to infinity; 2) cause outlier data to produce very large gradients due to the large weights; and 3) produce binary outputs even when incorrect—leading to decreased reliability of the confidence measure.
TABLE I

<table>
<thead>
<tr>
<th>Layer</th>
<th>Type</th>
<th>Units</th>
<th>x</th>
<th>y</th>
<th>Receptive field x</th>
<th>Receptive field y</th>
<th>Connection Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Convolutional</td>
<td>20</td>
<td>21</td>
<td>26</td>
<td>3</td>
<td>3</td>
<td>100</td>
</tr>
<tr>
<td>2</td>
<td>Subsampling</td>
<td>20</td>
<td>11</td>
<td>13</td>
<td>2</td>
<td>2</td>
<td>-</td>
</tr>
<tr>
<td>3</td>
<td>Convolutional</td>
<td>25</td>
<td>9</td>
<td>11</td>
<td>3</td>
<td>3</td>
<td>30</td>
</tr>
<tr>
<td>4</td>
<td>Subsampling</td>
<td>25</td>
<td>5</td>
<td>6</td>
<td>2</td>
<td>2</td>
<td>-</td>
</tr>
<tr>
<td>5</td>
<td>Fully connected</td>
<td>40</td>
<td>1</td>
<td>5</td>
<td>6</td>
<td>6</td>
<td>100</td>
</tr>
</tbody>
</table>

was used. A search then converge learning rate schedule was used8

$$\eta = \eta_0 \frac{n}{N/2} + \frac{c_1}{\max(1, c_2(n - c_2 N))}$$

where $\eta = \text{learning rate}$, $\eta_0 = \text{initial learning rate} = 0.1$, $N = \text{total training epochs}$, $n = \text{current training epoch}$, $c_1 = 50$, and $c_2 = 0.65$. The schedule is shown in Fig. 8. Total training time was around four hours on an SGI Indy 100Mhz MIPS R4400 system.

VI. EXPERIMENTAL RESULTS

We performed various experiments and present the results here. Except when stated otherwise, all experiments were performed with five training images and five test images per person for a total of 200 training images and 200 test images. There was no overlap between the training and test sets. We note that a system which guesses the correct answer would be right one out of 40 times, giving an error rate of 97.5%. For the following sets of experiments, we vary only one parameter in each case. The error bars shown in the graphs represent plus or minus one standard deviation of the distribution of results from a number of simulations.9 We note that ideally we would like to have performed more simulations per reported result, however, we were limited in terms of computational capacity available to us. The constants used in each set of experiments were: number of classes: 40, dimensionality reduction method: SOM, dimensions in the SOM: three, number of nodes per SOM dimension: five, image sample extraction: original intensity values, training images per class: five. Note that the constants in each set of experiments may not give the best possible performance as the current best performing system was only obtained as a result of these experiments. The experiments are as follows.

1) Variation of the number of output classes—Table II and Fig. 9 show the error rate of the system as the number of classes is varied from ten to 20 to 40. We made no attempt to optimize the system for the smaller numbers of classes. As we expect, performance improves with fewer classes to discriminate between.

2) Variation of the dimensionality of the SOM—Table III and Fig. 10 show the error rate of the system as the dimension of the SOM is varied from one to four. The best performing value is three dimensions.

3) Variation of the quantization level of the SOM—Table IV and Fig. 11 show the error rate of the system as the size of the SOM is varied from four to ten nodes per dimension. The SOM has three dimensions in each case. The best average error rate occurs for eight or nine nodes per dimension. This is also the best average error rate of all experiments.

4) Variation of the image sample extraction algorithm—Table V shows the result of using the two local image sample representations described earlier. We found that using the original intensity values gave the best performance. We investigated altering the weight assigned to the central intensity value in the alternative representation but were unable to improve the results.

5) Substituting the SOM with the KL transform—Table VI shows the results of replacing the SOM with the KL transform.

---

8Relatively high learning rates are typically used in order to help avoid slow convergence and local minima. However, a constant learning rate results in significant parameter and performance fluctuation during the entire training cycle such that the performance of the network can alter significantly from the beginning to the end of the final epoch. Moody and Darkin have proposed “search then converge” learning rate schedules. We have found that these schedules still result in considerable parameter fluctuation and hence we have added another term to further reduce the learning rate over the final epochs (a simpler linear schedule also works well). We have found the use of learning rate schedules to improve performance considerably.

9We ran multiple simulations in each experiment where we varied the selection of the training and test images (out of a total of $10 \times 5! = 30,240$ possibilities) and the random seed used to initialize the weights in the convolutional neural network.
transform. We investigated using the first one, two, or three eigenvectors for projection. Surprisingly, the system performed best with only one eigenvector. The best SOM parameters we tried produced slightly better performance. The quantization inherent in the SOM could provide a degree of invariance to minor image sample differences and quantization of the PCA projections may improve performance.

6) Replacing the CN with an MLP—Table VII shows the results of replacing the convolutional network with an MLP. Performance is very poor. This result was expected because the MLP does not have the inbuilt invariance to minor translation and local deformation which is created in the convolutional network using the local receptive fields, shared weights, and spatial subsampling. As an example, consider when a feature is shifted in a test image in comparison with the training image(s) for the individual. We expect the MLP to have difficulty recognizing a feature which has been shifted in comparison to the training images because the weights connected to the new location were not trained for the feature.

The MLP contained one hidden layer. We investigated the following hidden layer sizes for the MLP: 20, 50, 100, 200, and 500. The best performance was obtained with 200 hidden nodes and a training time of two days. The learning rate schedule and initial learning rate were the same as for the original network. Note that the best performing KL parameters were used while the best performing SOM parameters were not. We note that it may be considered fairer to compare against an MLP with multiple hidden layers [14], however selection of the appropriate number of nodes in each layer is difficult (e.g., we have tried a network with two hidden layers containing 100 and 50 nodes, respectively, which resulted in an error rate of 90%).

7) The tradeoff between rejection threshold and recognition accuracy—Fig. 12 shows a histogram of the recognizer's confidence for the cases when the classifier is correct and when it is wrong for one of the best performing systems. From this graph we expect that classification performance will increase significantly if we reject cases below a certain confidence threshold.

Fig. 13 shows the system performance as the rejection threshold is increased. We can see that by rejecting examples with low confidence we can significantly increase the classification performance of the system. If we consider a system which used a video camera to take a number of pictures over a short period, we could expect that a high performance would be attainable with an appropriate rejection threshold.

8) Comparison with other known results on the same database—Table VIII shows a summary of the performance of the systems for which we have results using the ORL database. In this case, we used a SOM quantization level of eight. Our system is the best performing system and performs recognition roughly 500 times faster than the second best performing system—the pseudo 2-D HMM's of Samaria. Fig. 14 shows the images which were incorrectly classified for one of the best performing systems.

9) Variation of the number of training images per person. Table IX shows the results of varying the number of images per class used in the training set from one to five for PCA+CN, SOM+CN and also for the eigenfaces algorithm. We implemented two versions of the eigenfaces algorithm—the first version creates vectors for each class in the training set by averaging the results of the eigenface representation over all images for the same person. This corresponds to the algorithm as described by Turk and Pentland [43]. However, we found that using separate training vectors for each training image resulted in better performance. We found that using between 40 to 100 eigenfaces resulted in similar performance. We can see that the PCA+CN and SOM+CN methods are both superior to the eigenfaces technique even when there is only one training image per person. The SOM+CN method consistently performs better than the PCA+CN method.

VII. DISCUSSION

The results indicate that a convolutional network can be more suitable in the given situation when compared with a
standard MLP. This correlates with the common belief that the incorporation of prior knowledge is desirable for MLP style networks (the CN incorporates domain knowledge regarding the relationship of the pixels and desired invariance to a degree of translation, scaling, and local deformation).

Convolutional networks have traditionally been used on raw images without any preprocessing. Without the preprocessing we have used, the resulting convolutional networks are larger, more computationally intensive, and have not performed as well in our experiments [e.g., using no preprocessing and the
Fig. 13. The test set classification performance as a function of the percentage of samples rejected. Classification performance can be improved significantly by rejecting cases with low confidence.

![Classification Performance Graph](image)

Fig. 14. Test images. The images with a thick white border were incorrectly classified by one of the best performing systems.

![Test Images](image)

<table>
<thead>
<tr>
<th>TABLE IV</th>
<th>ERROR RATE OF THE FACE RECOGNITION SYSTEM WITH VARYING NUMBER OF NODES PER DIMENSION IN THE SOM. EACH RESULT GIVEN IS THE AVERAGE OF THREE SIMULATIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>SOM Size</td>
<td>4</td>
</tr>
<tr>
<td>Error rate</td>
<td>8.5%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>TABLE V</th>
<th>ERROR RATE OF THE FACE RECOGNITION SYSTEM WITH VARYING IMAGE SAMPLE REPRESENTATION. EACH RESULT IS THE AVERAGE OF THREE SIMULATIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Input type</td>
<td>Pixel intensities</td>
</tr>
<tr>
<td>Error rate</td>
<td>5.75%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>TABLE VI</th>
<th>ERROR RATE OF THE FACE RECOGNITION SYSTEM WITH LINEAR PCA AND SOM FEATURE EXTRACTION MECHANISMS. EACH RESULT IS THE AVERAGE OF THREE SIMULATIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dimensionality reduction</td>
<td>Linear PCA</td>
</tr>
<tr>
<td>Error rate</td>
<td>5.33%</td>
</tr>
</tbody>
</table>

same CN architecture except initial receptive fields of $8 \times 8$ resulted in approximately two times greater error (for the case of five images per person)].

Fig. 15 shows the randomly chosen initial local image samples corresponding to each node in a 2-D SOM, and the final samples to which the SOM converges. Scanning across the rows and columns we can see that the quantized samples represent smoothly changing shading patterns. This is the initial representation from which successively higher level features are extracted using the convolutional network. Fig. 16 shows the activation of the nodes in a sample convolutional network for a particular test image.
TABLE VIII

<table>
<thead>
<tr>
<th>System</th>
<th>Error rate</th>
<th>Classification time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top-down HMM</td>
<td>13%</td>
<td>n/a</td>
</tr>
<tr>
<td>Eigenfaces</td>
<td>10.5%</td>
<td>n/a</td>
</tr>
<tr>
<td>Pseudo 2D-HMM</td>
<td>5%</td>
<td>240 seconds $^1$</td>
</tr>
<tr>
<td>SOM+CN</td>
<td>3.8%</td>
<td>&lt; 0.5 seconds $^2$</td>
</tr>
</tbody>
</table>

TABLE IX

<table>
<thead>
<tr>
<th>Images/person</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Eigenfaces -- average per class</td>
<td>38.6</td>
<td>28.8</td>
<td>28.9</td>
<td>27.1</td>
<td>26</td>
</tr>
<tr>
<td>Eigenfaces -- one per image</td>
<td>38.6</td>
<td>20.9</td>
<td>18.2</td>
<td>15.4</td>
<td>10.5</td>
</tr>
<tr>
<td>PCA+CN</td>
<td>34.2</td>
<td>17.2</td>
<td>13.2</td>
<td>12.1</td>
<td>7.5</td>
</tr>
<tr>
<td>SOM+CN</td>
<td>30.0</td>
<td>17.0</td>
<td>11.8</td>
<td>7.4</td>
<td>3.8</td>
</tr>
</tbody>
</table>

Fig. 15. SOM image samples before training (a random set of image samples) and after training.

VIII. COMPUTATIONAL COMPLEXITY

The SOM takes considerable time to train. This is not a drawback of the approach however, as the system can be extended to cover new classes without retraining the SOM. All that is required is that the image samples originally used to train the SOM are sufficiently representative of the image samples used in new images. For the experiments we have reported here, the quantized output of the SOM is very similar if we train it with only 20 classes instead of 40. In addition, the KL transform can be used in place of the SOM with a minimal impact on system performance.

It also takes a considerable amount of time to train a convolutional network; how significant is this? The convolutional network extracts features from the image. It is possible to use fixed feature extraction. Consider if we separate the convolutional network into two parts: the initial feature extraction layers and the final feature extraction and classification layers. Given a well-chosen sample of the complete distribution of faces which we want to recognize, the features extracted from the first section could be expected to also be useful for the classification of new classes. These features could then be considered fixed features and the first part of the network may not need to be retrained when adding new classes. The point at which the convolutional network is broken into two would depend on how well the features at each stage are useful for the classification of new classes (the larger features in the final layers are less likely to be a good basis for classification of new examples). We note that it may be possible to replace the second part with another type of classifier—e.g., a nearest-neighbors classifier. In this case the time required for retraining the system when adding new classes is minimal (the extracted feature vectors are simply stored for the training images).

To give an idea of the computational complexity of each part of the system we define:

$N_c$ the number of classes;

$N_n$ the number of nodes in the SOM;

$N_{w1}$ the number of weights in the convolutional network;

$N_{w2}$ the number of weights in the classifier;

$N_{tr}$ the number of training examples;

$N_n$ the number of nodes in the neighborhood function;

$N_{nm1}$ the total number of next nodes used to backpropagate the error in the CN;

$N_{nm2}$ the total number of next nodes used to backpropagate the error in the MLP classifier;

$N_{od}$ the output dimension of the KL projection;

$N_{id}$ the input dimension of the KL projection;

$N_{samples}$ the number of training samples for the SOM or the KL projection;

$N_{samples_{local}}$ the number of local image samples per image.

Tables X and XI show the approximate complexity of the various parts of the system during training and classification. We show the complexity for both the SOM and KL alternatives for dimensionality reduction and for both the neural network (MLP) and a nearest-neighbors classifier (as the last part of the convolutional network—not as a complete replacement, i.e., this is not the same as the earlier MLP experiments). We note

The SOM takes considerable time to train. This is not a drawback of the approach however, as the system can be extended to cover new classes without retraining the SOM. All that is required is that the image samples originally used to train the SOM are sufficiently representative of the image samples used in new images. For the experiments we have reported here, the quantized output of the SOM is very similar if we train it with only 20 classes instead of 40. In addition, the KL transform can be used in place of the SOM with a minimal impact on system performance.

It also takes a considerable amount of time to train a convolutional network; how significant is this? The convolutional network extracts features from the image. It is possible to use fixed feature extraction. Consider if we separate the convolutional network into two parts: the initial feature extraction layers and the final feature extraction and classification layers. Given a well-chosen sample of the complete distribution of faces which we want to recognize, the features extracted from the first section could be expected to also be useful for the classification of new classes. These features could then be considered fixed features and the first part of the network may not need to be retrained when adding new classes. The point at which the convolutional network is broken into two would depend on how well the features at each stage are useful for the classification of new classes (the larger features in the final layers are less likely to be a good basis for classification of new examples). We note that it may be possible to replace the second part with another type of classifier—e.g., a nearest-neighbors classifier. In this case the time required for retraining the system when adding new classes is minimal (the extracted feature vectors are simply stored for the training images).

To give an idea of the computational complexity of each part of the system we define:

$N_c$ the number of classes;

$N_n$ the number of nodes in the SOM;

$N_{w1}$ the number of weights in the convolutional network;

$N_{w2}$ the number of weights in the classifier;

$N_{tr}$ the number of training examples;

$N_n$ the number of nodes in the neighborhood function;

$N_{nm1}$ the total number of next nodes used to backpropagate the error in the CN;

$N_{nm2}$ the total number of next nodes used to backpropagate the error in the MLP classifier;

$N_{od}$ the output dimension of the KL projection;

$N_{id}$ the input dimension of the KL projection;

$N_{samples}$ the number of training samples for the SOM or the KL projection;

$N_{samples_{local}}$ the number of local image samples per image.

Tables X and XI show the approximate complexity of the various parts of the system during training and classification. We show the complexity for both the SOM and KL alternatives for dimensionality reduction and for both the neural network (MLP) and a nearest-neighbors classifier (as the last part of the convolutional network—not as a complete replacement, i.e., this is not the same as the earlier MLP experiments). We note
Fig. 16. A depiction of the node maps in a sample convolutional network showing the activation values for a particular test image. The input image is shown on the left. In this case the image is correctly classified with only one activated output node (the top node). From left to right after the input image, the layers are: the input layer, convolutional layer 1, subsampling layer 1, convolutional layer 2, subsampling layer 2, and the output layer. The three planes in the input layer correspond to the three dimensions of the SOM.

Fig. 17. Sensitivity to various parts of the input image. It can be observed that the eyes, mouth, nose, chin, and hair regions are all important for the classification. The z axis corresponds to the mean squared error rather than the classification error (the mean squared error is preferable because it varies in a smoother fashion as the input images are perturbed). The image orientation corresponds to upright face images.

that the constant associated with the log factors may increase exponentially in the worst case (cf. neighbor searching in high-dimensional spaces [1]). We have aimed to show how the computational complexity scales according to the number of classes, e.g., for the training complexity of the MLP classifier: although $N_{w2} + N_{mv2}$ may be larger than $N_c$, both $N_{w2}$ and $N_{mv2}$ scale roughly according to $N_c$.

With reference to Table XI, consider, for example, the main SOM+CN architecture in recognition mode. The complexity of the SOM module is independent of the number of classes. The complexity of the CN scales according to the number of weights in the network. When the number of feature maps in the internal layers is constant, the number of weights scales roughly according to the number of output classes (the number

<table>
<thead>
<tr>
<th>Section</th>
<th>Training complexity</th>
</tr>
</thead>
<tbody>
<tr>
<td>KL</td>
<td>$O((2 + N_{w1})N_{samples} + 3N_{mv2}) \approx O(N_{w1}^2 + N_{mv2})$</td>
</tr>
<tr>
<td>SOM</td>
<td>$O(k_3N_{samples}N_wk_2\log N_z) \approx O(N_{samples}N_2\log N_z)$ (for $N_z$ varies)</td>
</tr>
<tr>
<td>CN</td>
<td>$O(k_2N_{w1}(N_{w2} + N_{mv2})) \approx O(N_{w1}N_{w2})$</td>
</tr>
<tr>
<td>MLP Classifier</td>
<td>$O(k_2N_{w1}(N_{w2} + N_{mv2})) \approx O(N_{w1}N_{w2})$</td>
</tr>
<tr>
<td>NN Classifier</td>
<td>$O(N_{w1})$</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Section</th>
<th>Classification complexity</th>
</tr>
</thead>
<tbody>
<tr>
<td>KL</td>
<td>$O(N_{window}N_{w1}N_{out})$</td>
</tr>
<tr>
<td>SOM</td>
<td>$O(N_{window}k_1\log N_z) \approx O(N_{window}N_2)$</td>
</tr>
<tr>
<td>CN</td>
<td>$O(k_2N_{w1}) \approx O(N_{w1})$</td>
</tr>
<tr>
<td>MLP Classifier</td>
<td>$O(N_{w2}) \approx O(L_N)$</td>
</tr>
<tr>
<td>NN Classifier</td>
<td>$O(k_4\log N_{w2}) \approx O(\log N_c)$</td>
</tr>
</tbody>
</table>
of weights in the output layer dominates the weights in the initial layers).

In terms of computation time, the requirements of real-time tasks varies. The system we have presented should be suitable for a number of real-time applications. The system is capable of performing a classification in less than half a second for 40 classes. This speed is sufficient for tasks such as access control and room monitoring when using 40 classes. It is expected that an optimized version could be significantly faster.

IX. FURTHER RESEARCH

We can identify the following avenues for improving performance.


2) More precise normalization of the images to account for translation, rotation, and scale changes. Any normalization would be limited by the desired recognition speed.

3) The various facial features could be ranked according to their importance in recognizing faces and separate modules could be introduced for various parts of the face, e.g., the eye region, the nose region, and the mouth region (Brunelli and Poggio [6] obtain very good performance using a simple template matching strategy on precisely these regions).

4) An ensemble of recognizers could be used. These could be combined via simple methods such as a linear combination based on the performance of each network, or via a gating network and the expectation-maximization algorithm [11], [16]. Examination of the errors made by networks trained with different random seeds and by networks trained with the SOM data versus networks trained with the KL data shows that a combination of networks should improve performance (the set of common errors between the recognizers is often much smaller than the total number of errors).

5) Invariance to a group of desired transformations could be enhanced with the addition of pseudo-data to the training database—i.e., the addition of new examples created from the current examples using translation, etc. Leen [26] shows that adding pseudodata can be equivalent to adding a regularizer to the cost function where the regularizer penalizes changes in the output when the input goes under a transformation for which invariance is desired.

X. CONCLUSIONS

We have presented a fast, automatic system for face recognition which is a combination of a local image sample representation, an SOM network, and a convolutional network for face recognition. The SOM provides a quantization of the image samples into a topological space where inputs that are nearby in the original space are also nearly in the output space, which results in invariance to minor changes in the image samples, and the convolutional neural network provides for partial invariance to translation, rotation, scale, and deformation. Substitution of the KL transform for the SOM produced similar but slightly worse results. The method is capable of rapid classification, requires only fast approximate normalization and preprocessing, and consistently exhibits better classification performance than the eigenfaces approach [43] on the database considered as the number of images per person in the training database is varied from one to five. With five images per person the proposed method and eigenfaces result in 3.8% and 10.5% error, respectively. The recognizer provides a measure of confidence in its output and classification error approaches zero when rejecting as few as 10% of the examples. We have presented avenues for further improvement.

There are no explicit 3-D models in our system, however we have found that the quantized local image samples used as input to the convolutional network represent smoothly changing shading patterns. Higher level features are constructed from these building blocks in successive layers of the convolutional network. In comparison with the eigenfaces approach, we believe that the system presented here is able to learn more appropriate features in order to provide improved generalization. The system is partially invariant to changes in the local image samples, scaling, translation and deformation by design.

ACKNOWLEDGMENT

The authors would like to thank I. Cox, S. Haykin, and the anonymous reviewers for helpful comments, and the Olivetti Research Laboratory and Ferdinando Samaria for compiling and maintaining the ORL database.

REFERENCES


Ah Chung Tsoi (S’70–M’72–M’84–SM’90), was born in Hong Kong. He received the Higher Diploma in electronic engineering, Hong Kong Technical College, in 1969, and the M.Sc. degree in electronic control engineering and the Ph.D. degree in control engineering from the University of Salford in 1970 and 1972, respectively.

From 1972 to 1974 he worked as Senior Research Fellow at the Inter-University Institute of Engineering Control, University College of North Wales, Bangor, Wales. From 1974 to 1977, he worked as a Lecturer at the Paisley College of Technology, Renfrewshire, Scotland. From 1977 to 1984, he worked as a Senior Lecturer at the University of Auckland, New Zealand. From 1985 to 1990, he worked as a Senior Lecturer at the University College, University of New South Wales. He is presently a Professor in Electrical Engineering at the University of Queensland, Australia. His research interests include aspects of neural networks and their application to practical problems, adaptive signal processing, and adaptive control.

Andrew D. Back (M’96) received the B.Eng. degree with distinction from Darling Downs Institute of Advanced Education (now the University of Southern Queensland), Australia, in 1985, and the Ph.D. degree from the University of Queensland, Australia, in 1992.

He was a Research Fellow with the Defence Science and Technology Organization (DSTO) from 1988 to 1992, and a Research Scientist with the DSTO in 1993. In 1995 he was a Visiting Scientist at the NEC Research Institute, Princeton, NJ. He is currently a Frontier Researcher with the Brain Information Processing Group in the Frontier Research Program at the Institute of Physical and Chemical Research (RIKEN) in Japan. He has published about 30 papers. His research interests include nonlinear models for system identification, time series prediction, and blind source separation.

Dr. Back was awarded an Australian Research Council (ARC) Postdoctoral Research Fellowship in the Department of Electrical and Computer Engineering at the University of Queensland for the period from 1993–1996. He has organized workshops for the Neural Information Processing Systems Conference in 1994, 1995, and 1996 in area of neural networks for signal processing.
for face recognition task by Sankaranarayanan et al. [41]. We argue that a network pre-trained on face recognition task possesses ne-
grained information of a face which can be used to train other face-related tasks efficiently. Task-specific sub-networks are branched out from different layers of this network depending on whether they rely on local or global information of the face. The complete network, when trained end-to-end, significantly improves the face recognition performance as well as other face analysis tasks. This paper makes the following contributions. 1) We propose a novel CNN architecture. The convolutional network extracts successively larger features in a hierarchical set of layers. We present results using the Karhunen-Loeve transform in place of the SOM, and a multilayer perceptron (MLP) in place of the convolutional network for comparison. We use a database of 400 images of 40 individuals which contains quite a high degree of variability in expression, pose, and facial details.