Living Face Verification via Multi-CNNs

Peiqin Li*, Jianbin Xie, Wei Yan, Zhen Li, Gangyao Kuang

School of Electronic Science, National University of Defense Technology, Changsha, Hunan, 410073, P. R. China

ABSTRACT

In face verification applications, precision rate and identifying liveness are two key factors. Traditional methods usually recognize global faces and can not gain good enough results when the faces are captured from different ages, or there are some interference factors, such as facial shade, etc. Besides, the false face attack will pose a great security risk. To solve the above problems, this study examines how to achieve reliable living face verification based on Multi-CNNs (convolutional neural networks) and Bayes probability. Participants are required to make several expressions in random orders and contents, to ensure their liveness. Then, an effective component-based method is proposed for face recognition, and synthesized multiple CNNs can help reflecting intensities of different components. Eventually, the similarity between faces is calculated by integrating the results of each CNN, with the help of Bayes probability. Comparative experiments demonstrate that our algorithm outperforms traditional methods in face recognition accuracy. Moreover, our algorithm has unique preponderance in that it can verify the liveness of users, which can achieve higher security.

1. INTRODUCTION

With the rapid progress of face recognition technology, face authentication turns into an excellent way in security nowadays. In a traditional face authentication system, the camera captures face images of the people who need to be identified, then the features of the face are extracted and compared with enrolled ones. Finally the result is gained by calculating the similarity. The traditional system of simple face recognition has a shortage that simulating prosthetic targets can easily cheat it. In other words, if one person does not come in the front of the camera, instead his paper photograph, or a digital picture shown on a PAD is used by other people. They may potentially pass the identification. To avoid such problems, the authentication system requires that the image to be processed is captured from real faces, not other prostheses. Thus the living target identification has become one of the well-studied problems in computer vision [1].

Some effective face recognition algorithms have been studied. For face recognition, in [2, 3], an original face image is converted into a corresponding sketch image, after which recognition is conducted by sketches. Certain handcrafted descriptors, such as local binary pattern (LBP), scale invariant feature transform (SIFT), and histogram of oriented gradients (HOG) [4–6] has the effect of comparing faces. Various methods are applied to detect facial key points, as such methods used for recognition can accurately locate the face. However, such studies are employed for static face recognition, which may be easily attacked.

In order to verify that faces are captured from living persons, some methods have been generated. For example, 3D models are used to add stereo information of faces [7–9]. Although these methods may have reliable effects, they typically require additional and special imaging equipment.

Deep learning, a class of machine learning techniques mainly developed since 2006, can generate numerous stages of nonlinear information processing in hierarchical architectures, which are employed in feature learning and pattern classification [10]. Especially for face recognition, Convolutional Neural Network (CNN) is an excellent widely applied model [11–14]. In recent years, CNN is used by some famous companies and research teams for face detection or recognition, such as DeepID3 [15], NormFace [16], DeepFace [17], FaceNet [18], and so on. Generally speaking, deep learning methods turn a global face image as input data, and face analysis is accomplished internally. On one hand, this process shows the intelligent advantage of deep learning, on the other hand, feature extraction of a whole face increases the complexity of networks. Recognition accuracy may declines, especially when there are age differences between the enrollment and verification of human faces.

In this paper we propose a robust and useful algorithm, which takes advantage of CNN-Bayes probability jointed scheme for living person recognition. The rest of this paper is organized as follows: the framework of our algorithm introduced in Section 2, recognition of the face with constrained dynamic expression in Section 3, experimentation and comparison of the obtained results with competing methods in Section 4, and conclusions in Section 5.
2. FRAMEWORK OF DYNAMIC FACE RECOGNITION

We design a process for living identity verification. Firstly, participants are asked to make designated expressions. The expressions include closing left or right eyes, opening and closing the mouth, knitting and releasing the nose. Both the types and orders of expressions are random. Then, the faces with different expressions are recognized by our innovative algorithm. Concretely, we investigate the peculiarities of facial components as key targets to identify faces with different expressions. Based on such methods, only living persons can respond to the demands, and optimized methods can ensure the accuracy of identification. Meanwhile the whole algorithm is much easier to be achieved than traditional living identification. The framework is shown in Figure 1.

For face recognition, six kinds of components are chosen for the operation: left brow, right brow, left eye, right eye, nose, and mouth. They are detected and located with the help of facial landmarks. On faces of known categories, these components and entire faces are classified accordingly to train CNN models. The template face and unknown faces are handled separately, and the results are integrated to calculate the complete similarity of faces by Bayes probability.

The contributions of our study are summarized as follows:

- The dynamic faces with different expressions can efficiently ensure the target is living, thus the safety of identification system can be enhanced.
- Besides whole-face images, an effective component-based method is added for face recognition, and the peculiar features of components are distinct and stronger than those of single global face.
- Several ordered CNN models are used to extract features. This order can avoid limitations of normal CNN.
- Bayes probability is introduced to synthesize multiple CNNs. This method can effectively reflect the peculiar intensities of different components.

3. DYNAMICALLY FACE RECOGNITION

3.1. Facial Component Location

To strengthen the adaptability of global variations, pre-treatments such as adjustment and normalization of global brightness are needed. Then considering face usually has conformable local gray value, while other regions have diverse gray value, such as textures and graphic patterns on clothes, we should take advantage of the gray-similarity to detect possible face areas. Clustering analysis can achieve the pattern recognition based on the similarities to judge automatically [19]. Therefore, we make use of K-Means for clustering analysis, in order to reduce the object regions of face detection. The process is expounded as follows:

Algorithm 1: Clustering analysis based on K-Means

Input : Sample pixels x of image containing faces, the number of whole patterns k.
Output : The final clustering classes\( \{S_1, S_2, \cdots, S_k\} \).

1: **Initialization:** Randomly choose centers of clustering as \( C_{m1}^0, C_{m2}^0, C_{m3}^0, \cdots, C_{mk}^0 \), where \( m1, m2, m3, \cdots, mk \) separately means the number of iteration operation.

2: **while** \( C_{r+1}^i \neq C_i^r, (i = 1, 2, 3, \cdots, k) \) **do**
3: **for** \( i = 1: k \)
4: **if** \( d(x, C_i^j) = \min(d(x, C_j^f), f = 1, 2, 3, \cdots, k) \)
5: \( S_i^r' \leftarrow x \)
6: \( C_i^{r+1} = \frac{1}{n_i^r} \sum_{x_i^r \in C_j^f} x_i^r, (i = 1, 2, 3, \cdots, k) \)
7: \( n_i^r \) is the number of samples belonging to the \( S_i^r \).
8: **end if**
9: **end for**
10: **end while**
11: **end**
12: Cluster samples x from I into k patterns.

After these treatments, the searching range of Active Shape Model (ASM) [20] can be reduced, and the whole process can achieve higher speed. The location of facial component is annotated on training image set. Supposing that there are \( n \) face images in the training set and each face has \( m \) landmark points, the shapes can be represented as vectors

\[
X_i = (x_{i0}^0, x_{i1}^0, x_{i1}^1, \cdots, x_{i0}^m, y_{i0}^m)\quad i = 0, 1, \cdots, n - 1
\]  

Here \( x_i^j \) and \( y_i^j \) are the coordinates of the \( j \)th landmark in \( i \)th face image.
Aligning faces in set $X$, we can get the new set

$$\hat{x}^i = (x_0^i, y_0^i, x_1^i, y_1^i, \ldots, x_{m-1}^i, y_{m-1}^i)^T, \ i = 0, 1, ..., n - 1$$  (2)

And the average template of face is

$$X = \frac{1}{n} \sum_{i=0}^{n-1} \hat{x}^i$$  (3)

The deviation between samples and average template can be calculated as

$$dX^i = \hat{x}^i - X$$  (4)

And the covariance matrix is

$$S = \frac{1}{n} \sum_{i=0}^{n-1} (dX^i)(dX^i)^T$$  (5)

We assume the nonzero eigenvalue vector and eigenvector are $\lambda_i$ and $p_i$, then a face shape can be represented as

$$X = \overline{X} + p_i B_i$$  (6)

Here $P_i = (p_1, p_2, ..., p_i)$ is a matrix of the first $t$ eigenvectors of the covariance matrix, and $B_i = (b_1, b_2, ..., b_i)$ is a vector that indicates the variation from $X$ to $\overline{X}$ in the direction of $p_1, p_2, ..., p_i$. Across the training set, the variance of the $t$th parameter vector $p_i$ is given by the corresponding eigenvalue vector $\lambda_i$. To ensure the generated shape is similar to those in the training set, $b_i$ should meet the constraint condition as $|b_i| \leq 3 \sqrt{\lambda_i}$, which is a commonly-used configuration in the ASM domain.

Face shapes in videos and images can be searched and extracted, and then facial components can be located with the help of landmark points. Several examples are presented in Figure 2.

### 3.2. Face Recognition with CNN and Bayes Probability

Convolution network is a multilayer perceptron designed to identify 2D shapes. This network structure is highly invariant to translation, scaling, tilting or common deformation.

The layer of CNN can be divided into convolutional layers and sub sampling layers. The convolution layer is followed by a sub sampling layer to reduce computation time and establish spatial and structural invariance, whereas a convolutional filtering is carried out from $S$ to $C$. After a number of such layers, the final eigenvector is obtained.

In Figure 3, $f_x$ is a digital filter, $b_x$ is a bias parameter, $C_x$ is the feature map of convolutional layer, $W_{x+1}$ means the value of sub sampling, $b_{x+1}$ is the corresponding weight. This connection shows how to obtain the sub sampling layer $S_{x+1}$.

Alternating between the convolution layer and the sampling layer, CNN consists of forward propagation and backward propagation. Forward propagation is calculated and passed down layer by layer, thus the output of the current layer can be expressed as:

$$x' = f(W x' + b')$$  (7)

$l$ means the layers, $f$ is the activation function, such as tanh, sigmoid and relu, in this paper, relu is used.

Spread back propagation is used to calculate the error between results and given sample labels. Considering square variance loss function, for classification problem which contains $c$ categories and $N$ training samples, the error function is shown as:

$$E^N = \frac{1}{2} \sum_{n=1}^{N} \sum_{k=1}^{c} (y_{nk} - \hat{y}_{nk})^2$$  (8)
$x_k^n$ means $k$ dimensionality of the sample $n$, $y_k^n$ means the output $k$ of the sample $n$.

Back propagation will update convolution layer, and each output map may be associated with the convolution of several feature mappings on the previous layer. The general form of the convolution layer is:

$$x_j^l = f\left(\sum_{i \in M_j^l} x_i^{l-1} \times k_{ij}^l + b_j^l\right)$$

$l$ means the layers, $k$ is the convolutional kernel, $M_j^l$ is one of the input features, $b$ is the bias.

The sub sampling operation does not change the number of feature mappings, but only the size. If the size of the sampling operator is $n \times n$, then the size of the feature map becomes $1/n$ of the original feature after sampling. The general form of the sub sampling is:

$$x_j^l = f\left(\beta^l \downarrow \left(x_j^{l-1}\right) + b_j^l\right)$$

$\downarrow$ means a sub sampling function.

In sum total, CNN is a special kind of deep neural network model, its particularity embodies in two aspects, on the one hand, its connections between neurons are not all connected, on the other hand, some weights of connections between neurons in the same layer are shared. These specialties make it more similar to the biological neural networks, which can reduce the number of the weights and the complexity of the network model. It is very important because the deep structure is difficult to learn.

Convolutional Architecture for Fast Feature Embedding (Caffe) is a deep learning framework made with expression, speed, and modularity in mind. It is developed by Yangqing Jia in Berkeley AI Research (BAIR), and it is specially designed for realizing CNN model easily, and it has the characteristics of modularization, rapidity and openness. Therefore it is widely used to extract face features.

With the help of CNN and Caffe, significant results have been achieved in face recognition. However, there are some inherent shortages. For example, traditional CNN model extracts global features of a whole face, so it can’t map local differences accurately. Besides, for a CNN, the existence of facial component parts becomes a very powerful indicator of a face in the image. But the orienteering and relative spatial relationships between these components are not important for CNN [21] as shown in (Figure 4).

![Figure 4](image)

In contrast, Bayesian Program Learning (BPL) uses written parts and their order to identify characters, and this method has achieved excellent results [22]. Inspired from this, we use multiple CNNs to extract features of ordered facial components, and then calculate the ultimate similarity based on Bayesian probability. The process is presented in Figure 5.

Different CNN networks are used for face and various facial components in this study. Face labels are corresponding to each person, while the labels of components correspond to the types of components. For example, eyes are classified into triangular ones, narrow ones, big ones, and so on. Most kinds are difficult to describe, in fact digital label are directly used. More specifically, the network for global face has 64 layers, each network for other facial components has 20 layers, and the size of global face image is 128 × 128 pixels, the size of eye or brow is 32 × 32 pixels, the size of nose or mouth is 64 × 32 pixels.

After the establishment of two kinds of multiple CNN networks, the features of the template face and the face to be compared can be extracted, named as Feature$^{\text{comp}}$ and Feature$^{\text{target}}$. The probability of the similarity between the two as the same person is marked as $P_0$. Furthermore, the facial component $i$ is sent to its classification network, and output its classification type $S$, and corresponding probability $P_i, i = 1, 2, 3, ..., 7$. If the template face and the component parts to be compared with the face are used as input, the output is expressed as $(S_{p}, P_{0}), i = 1, 2, 3, ..., 7, j = 0, 1$. Here 0 represents a template face, and 1 represents a face to be compared.

Naïve Bayesian Model (NBM) is originated from classical mathematics theory. It has a solid mathematical foundation and a stable classification efficiency. It is one of the most widely used classification models. NBM needs few parameters to be estimated and is not very sensitive to missing data, and the algorithm is simple [23]. When a sample is given, $P(C_i | X)$ means the probability that it belongs to each category. $C_i$ represents the category, $X$ represents the test sample, and the maximum probability can be calculated as

$$P(C | x) = \frac{P(x | C) \cdot P(C)}{P(x)}$$

Similarly, if we get template face $X$ through CNN network, a series of probability values of target face $Y$, including the similarity of two faces, and the classification results and probability of each facial feature component. The problem can be summed up as: how to determine whether the two faces are the same person? In the form of reference [11], it can be expressed as:

$$P(C | (X, Y)) = \frac{P((X, Y) | c) \cdot P(c)}{P(X, Y)}$$

Here $c$ indicates that two faces are classified into the same class. To simplify the calculation, we define $P(C) = S_0$, then $P(S_0 | (X, Y))$ indicates that two faces are sorted into the same class, that is, facial components are classified to same pattern. At this time, the classification probability of all component parts is calculated as

$$P(S_0 | (X, Y)) = \sum_i (P_{0} \times P_{1} \times S) = \begin{cases} 0, & \text{if } (S_0 = S_1) \\ 1, & \text{if } (S_0 \neq S_1) \end{cases}$$

Here $P(S_0 | (X, Y))$ is calculated as final probability of whether two faces are treated as the same person. Thus, the face recognition
is achieved. Traditional methods usually use the global face as the input of convolutional neural networks. As people grow older, the face shape usually changes and affects the recognition results. Notice that even though the face become fat or thin, shapes of facial components are relatively stable, so this paper combines the global face and local facial components to extract features, thus it has better robustness in adapting to the changes of face age.

4. EXPERIMENTAL RESULTS AND ANALYSIS

We have tested the new algorithm on a personal computer that has an Intel Core CPU with 3.33 GHz and 8 GB DDR.

At large, the existing face recognition methods based on deep learning have achieved excellent results on ordinary image sets, such as the face database of AT&T Lab in Cambridge University [24], Extended Yale B database [25], the CMU pose, illumination and expression database [26], Pubfig [27], and so on. However, these algorithms do not work well on actual scenes, especially when one face is ID photo and the other is monitor image. So we build a face image set, in each group, it contains ID card photo and recent live images. There are 12 300 such groups in the image set, and they mainly contain these differences:

1. With glasses and without glasses.
2. Deformations caused by the change of the ages.

Some examples are shown in (Figure 6):

Comparatively, our experiments are operated with four deep learning methods: simple CNN for global face, optimized CNN including NormFace and DeepID3, and our multi-CNN with Bayes probability. In order to record their statistical results, we should introduce some definitions:

Similarity threshold: if two faces whose similarity is greater than the threshold, they will be judged as the same person.

TP_num: the number of true positive.
TN_num: the number of true negative.
FP_num: the number of false positive.
FN_num: the number of false negative.

True positive rate (TPR):
\[ TPR = \frac{TP\_Num}{TP\_Num + FN\_Num} \]

False positive rate (FPR):
\[ FPR = \frac{FP\_Num}{TN\_Num + FP\_Num} \]

False negative rate (FNR):
\[ FNR = \frac{FN\_Num}{TP\_Num + FN\_Num} \]

Error rate curve (ERC):

The similarity threshold is the x-axis, then curves are drawn with TPR, FPR and FNR as the ordinate respectively. The intersection of FPR and FNR curves is equal error rate (EER) point, the corresponding abscissa of which is the optimal threshold.

Receiver operating characteristic (ROC):

Take FPR as the abscissa and TPR as the ordinate to draw the curve. The larger area under the curve indicates better effect of classifier.

In this paper, corresponding performances are shown in Figures 7 and 8.

(a) Simple CNN, the best threshold of EER point is 0.49, the FPR value is 0.42, and the TPR value is 0.58 at this point.

(b) NormFace, the best threshold of EER point is 0.63, the FPR value is 0.14, and the TPR value is 0.86 at this point.

(c) DeepID3, the best threshold of EER point is 0.48, the FPR value is 0.12, and the TPR value is 0.88 at this point.

(d) Our new algorithm, the best threshold of EER point is 0.51, the FPR value is 0.08, and the TPR value is 0.92 at this point.

![Figure 7](image1)

![Figure 8](image2)

Table 1 | Average test time.

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Time cost per face</th>
</tr>
</thead>
<tbody>
<tr>
<td>Simple CNN</td>
<td>0.08 second</td>
</tr>
<tr>
<td>NormFace</td>
<td>0.09 second</td>
</tr>
<tr>
<td>DeepID3</td>
<td>0.08 second</td>
</tr>
<tr>
<td>Our new algorithm</td>
<td>0.09 second</td>
</tr>
</tbody>
</table>

The smaller FPR value of EER point in the ERC map, and the bigger area of TPR in the ROC map represent better performance. In this experiment, the new algorithm achieves the highest TPR whereas its FPR is lower than that of other algorithms. The experimental results demonstrate the previous theoretical analysis. The new algorithm in this paper is indeed more adaptable to illumination changes, age changes, wearing glasses and other aspects. The face recognition effect is better than the contrast method.

From a computational cost perspective, the overall calculation is related to the number of layers because of the convolution operations. Based on the hardware and test mentioned above, the average test time (but not training time) by CPU is shown in Table 1.

The new algorithm is at the same level as other methods. Since these CNNs are parallel processing, that means the new method does not increase the time complexity.

After aggregating and analyzing the experiment results, the new algorithm has a significant advantage: it can spend the same time to achieve better treatment effect.

5. CONCLUSION AND FUTURE WORK

Traditional CNN face recognition methods extract global features of faces, but they are easily affected in practical applications, because of the following factors:

1. Although the complete face is pre-processed by correction and normalization, it is unavoidable that the face is skewed and affects the global feature.

2. There is partial occlusions in the face area, such as wearing glasses.

3. As age goes on, face may increasingly change.
In this study, face images are captured with randomly changed expressions, and facial components are obtained via optimized pre-treatment. Then various CNN models are designed for the different facial components such as: global face, left brow, right brow, left eye, right eye, nose, and mouth. The CNN models are trained to extract different features. Finally Bayes probability is used to combine global features and local features. The new method can preferably adapt to the above three kinds of effects, and improve the accuracy of personal identification. It can verify the liveness of targets in particular. Therefore, this study has achieved the goal of enhancing accuracy and safety through the new method.

REFERENCES