Frankenstein: Learning Deep Face Representations using Small Data
Guosheng Hu, Xiaojiang Peng, Yongxin Yang, Timothy Hospedales, Jakob Verbeek

To cite this version:

HAL Id: hal-01306168
https://inria.hal.science/hal-01306168v2
Submitted on 25 Sep 2017

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L’archive ouverte pluridisciplinaire HAL, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d’enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.
Abstract.—Deep convolutional neural networks have recently proven extremely effective for difficult face recognition problems in uncontrolled settings. To train such networks, very large training sets are needed with millions of labeled images. For some applications, such as near-infrared (NIR) face recognition, such large training datasets are not publicly available and difficult to collect. In this work, we propose a method to generate very large training datasets of synthetic images by compositing real face images in a given dataset. We show that this method enables to learn models from as few as 10,000 training images, which perform on par with models trained from 500,000 images. Using our approach we also obtain state-of-the-art results on the CASIA NIR-VIS2.0 heterogeneous face recognition dataset.

Index Terms—face recognition, deep learning, small training data

I. INTRODUCTION

In recent years, deep learning methods, and in particular convolutional neural networks (CNNs), have achieved considerable success in a range of computer vision applications including object recognition [22], object detection [10], semantic segmentation [34], action recognition [44], and face recognition [40]. The recent success of CNNs stems from the following facts: (i) big annotated training datasets are currently available for a variety of recognition problems to learn rich models with millions of free parameters; (ii) massively parallel GPU implementations greatly improve the training efficiency of CNNs; and (iii) new effective CNN architectures are being proposed, such as the VGG-16/19 networks [45], inception networks [53], and deep residual networks [13].

Good features are essential for object recognition, including face recognition. Conventional features include linear functions of the raw pixel values, including Eigenface (Principal Component Analysis) [56], Fisherface (Linear Discriminant Analysis) [3], and Laplacianface (Locality Preserving Projection) [14]. Such linear features were later replaced by hand-crafted local non-linear features, such as Local Binary Patterns [1], Local Phase Quantisation (LPQ) [2], and Fisher vectors computed over dense SIFT descriptors [43]. Note that the latter is an example of a feature that also involves unsupervised learning. These traditional features achieve promising face recognition rates in constrained environments, as represented for example in the CMU PIE dataset [42]. However, using these features face recognition performance may degrade dramatically in uncontrolled environments, such as represented in the Labeled Faces in the Wild (LFW) benchmark [16]. To improve the performance in such challenging settings, metric learning can be used, see [5], [11], [58]. Metric learning methods learn a (linear) transformation of the features that pulls the objects that have the same label closer together, while pushing the objects that have different labels apart.

Although hand-crafted features and metric learning achieve promising performance for uncontrolled face recognition, it remains cumbersome to improve the design of hand-crafted local features (such as SIFT [25]) and their aggregation mechanisms (such as Fisher vectors [38]). This is because the experimental evaluation results of the features cannot be automatically fed back to improve the robustness to nuisance factors such as pose, illumination and expression. The major advantage of CNNs is that all processing layers, starting from the raw pixel-level input, have configurable parameters that can be learned from data. This obviates the need for manual feature design, and replaces it with supervised data-driven feature learning. Learning the large number of parameters in CNN models (millions of parameters are rather a rule than an exception) requires very large training datasets. For example, the CNNs which achieve state-of-the-art performance on the LFW benchmark are trained using datasets with millions of labeled faces: Facebook’s DeepFace [54] and Google’s FaceNet [40] were trained using 4 million and 200 million training samples, respectively.

For some recognition problems large supervised training datasets can be collected relatively easily. For example the CASIA Webface dataset of 500,000 face images was collected semi-automatically from IMDb [62]. However, in many other cases collecting large datasets may be costly, and possibly problematic due to privacy regulation. For example, thermal infrared imaging is ideal for low-light nighttime and covert face recognition applications [21], but it is not possible to collect millions of labeled training images from the internet for the thermal infrared domain. The lack of large training datasets is an important bottleneck that prevents the use of deep learning methods in such cases, as the models will overfit dramatically when using small training datasets [15].

To address this issue, the use of big synthetic training datasets has been explored by a number of authors [17], [30], [35], [36]. There are two important advantages of using synthetic data (i) one can generate as many training samples as desired, and (ii) it allows explicit control over the nuisance
factors. For instance, we can synthesize face images of all desired viewpoints, whereas data collected from the internet might be mostly limited to near frontal views. Data synthesis has successfully been applied to diverse recognition problems, including text recognition [17], scene understanding [30], and object detection [36]. Several recent works [66, 9, 27] proposed 3D-aided face synthesis techniques for facial landmark detection and face recognition in the wild.

Data augmentation is another technique that is commonly used to reduce the data scarcity problem [32, 45]. This is similar to data synthesis, but more limited in that existing training images are transformed without affecting the semantic class label, e.g. by applying cropping, rotation, scaling, etc.

The main contribution of this paper is a solution for training deep CNNs using small datasets. To achieve this, we propose a data synthesis technique to expand limited datasets to larger ones that are suitable to train powerful deep CNNs. Specifically, we synthesize images of a ‘virtual’ subject \( c \) by compositing automatically detected face parts (eyes, nose, mouth) of two existing subjects \( a \) and \( b \) in the dataset in a fixed pattern. Images for the new subject are generated by composing a nose from an image of subject \( a \) with a mouth of an image of subject \( b \). This is motivated by the observation that face recognition consists in finding the differences in the appearance and constellation of face parts among people. For a dataset with an equal number of faces per person, this method can increase a dataset of \( n \) images to one with \( n^2 \) images when using only 2 face parts (we use 5 parts in practice). A dataset like LFW can thus be expanded from a little over 10,000 images to a dataset of 100 million images.

Unlike existing face synthesis methods which use 3D models [66, 9, 27], our method is a pure 2D method which is much easier to implement. In addition, our method works on different tasks from [66, 9, 27]. Specifically, the methods [66, 9] are used for facial landmark detection, while ours for face recognition. The approach [27] assumes a relatively large training data (500,000 images) already exists, while we assume the training data is very small (10,000 images).

We experimentally demonstrate that the synthesized small training datasets indeed significantly improve the generalization capacity of CNNs. In our experiments, we generate a training set of 1.5 million images using an initial labeled dataset of only 10,000 images. Using the synthetic data we improve the face verification rate from 78.97% to 95.77% on LFW. In addition, the proposed face synthesis is also used for NIR-VIS heterogeneous face recognition [29] and improve the rank-1 face identification rate from 17.41% to 85.05%. With the synthetic data, we achieve state-of-the-art performance on both (1) LFW under the ‘unrestricted, label-free outside data’ protocol and (2) CASIA NIR-VIS 2.0 database under rank-1 face identification protocol.

II. RELATED WORK

Our work relates to three research areas that we briefly review below: face recognition using deep learning methods (Section II-A), face data collection (Section II-B), and data augmentation and synthesis methods (Section II-C).

A. Face recognition using deep learning

Since face recognition is a special case of object recognition, good architectures for general object recognition may carry over to face recognition. Schroff et al. [40] explored networks that are based on that of Zeiler & Fergus [64] and inception networks [53]. DeepID3 [49] uses aspects of both inception networks and the very deep VGG network [45]. Parkhi et al. [31] use the very deep VGG network, while Yi et al. [62] use 3 × 3 filters but fewer layers.

DeepFace [54] uses a 3D model for pose normalization, by which all the faces are rotated to the frontal pose. In this way, pose variations are removed from the faces. Then an 8-layer CNN is trained using four million pose-normalized images.

DeepID [51], DeepID2 [48], DeepID2+ [52] all train an ensemble of small CNNs. The input of one small CNN is an image patch cropped around a facial part (face, nose, mouth, etc.). The same idea is also used in [24]. DeepID uses only a classification-based loss to train the CNN, while DeepID2 includes an additional verification-based loss function. To further improve the performance, DeepID2+ adds losses to all the convolutional layers rather than the topmost layer only.

All the above methods train CNNs using large training datasets of 500,000 images or more. To the best of our knowledge, only [15] uses small datasets to train CNNs (only around 10,000 LFW images) and achieves significantly worse performance on the LFW benchmark: 87% vs 97% or higher in [40], [52], [54]. Clearly, sufficiently large training datasets are extremely important for learning deep face representations.

B. Face dataset collection

Since big data is important for learning a deep face representation, several research groups have collected large datasets with 90,000 up to 2.6 million labeled face images [5, 28], [31], [50], [62]. To achieve this, they collect face images from the internet, by querying for specific websites such as IMDb or general search engines for celebrity names. This data collection process is detailed in [31], [62].

Existing face data collection methods have, however, two main weaknesses. First, and most importantly, internet-based collection of large face datasets is limited to visible spectrum images, and is not applicable to collect e.g. infrared face images. Second, the existing collection methods are expensive and time-consuming. It results from the fact that automatically collected face images are noisy, and manual filtering has to be performed to remove incorrectly labeled images [31].

The difficulty of collecting large datasets in some domains, e.g. for infrared imaging, motivates the work presented in this paper. To address this issue we propose a data synthesis method that we describe in the next section.

C. Data augmentation and synthesis

The availability of large supervised datasets is the key for machine learning to succeed, and this is true in particular for very powerful deep CNN models with millions of parameters. To alleviate data scarcity in visual recognition tasks, data augmentation has been used to add more examples by applying
simple image transformations that do not affect the semantic-level image label, see e.g. [7]. Examples of such transformations are horizontal mirroring, cropping, small rotations, etc. Since it is not always clear in advance which (combinations of) transformations are the most effective to generate examples that improve the learning the most, Paulin et al. [32] proposed to learn which transformations to exploit.

Data augmentation, however, is limited to relatively simple image transformations. Out-of-plane rotations, for example, are hard to accomplish since they would require some degree of 3D scene understanding from a single image. Pose variations of articulated objects are another example of transformations that are non-trivial to obtain, and generally not used in data augmentation methods.

Training models from synthetic data can overcome such difficulties, provided that sufficiently accurate object models are available. Recent examples where visual recognition systems have been trained from synthetic data include the following. Shotton et al. [41] train randomized decision forests for human pose estimation from synthesized 3D depth data. Jaderberg et al. [17] use synthetic data to train CNN models for natural scene text recognition. Su et al. [46] use synthetic images of objects to learn a CNN for viewpoint estimation. Papon and Schoeler [30] train a multi-output CNN that predicts class, pose, and location of objects from realistic cluttered room scenes that are synthesized on the fly. Weinmann et al. [59] synthesize material images under different viewing and lighting conditions based on detailed surface geometry measurements, and use these to train a recognition system using a SIFT-VLAD representation [18]. Ronzantsev et al. [37] use rough 3D models to synthesize new views of real object category instances. They show that this outperforms more basic data augmentation using crops, flips, rotations, etc.

Data synthesis techniques are also used for face analysis. To improve the accuracy of facial landmark detection in the presence of large pose variations [9], [66], a 3D morphable face models is used to synthesize face images in arbitrary poses. Similar data synthesis techniques are also used for pose-robust face recognition [27]. Unlike 3D solutions, we propose a 2D data synthesis method to solve the problem of training deep CNNs using very limited training data.

### III. Synthetic data engine

Human faces are well structured in the sense that they are composed of parts (eyes, nose, mouth, etc.) which are organized in a relatively rigid constellation. Face recognition relies on differences among people in the appearance of facial parts and their constellation. Motivated by this, our synthetic face images are generated by swapping one or more facial parts among existing “parent” images. In our work we use five face parts: right eye (RE), left eye (LE), nose (N), mouth (M) and the rest (R). See Figure 1 for an illustration. For simplicity, we only consider the synthesis using only two parent images in this work. Our synthesis method can easily be extended, however, to the scenario of more than two parent images.

![Fig. 1: Illustration of the face synthesis process using five parts: left-eye, right-eye, nose, mouth and the rest. Parent images P0 and P1 (top) are mixed by using the eyes of P1 and the other parts of P0 to form the synthetic image (bottom).](image)

**A. Compositing face images**

Suppose that we have an original dataset and let $S$ denote the set subjects in the dataset, and let $n_i$ denote the number of images of subject $i \in S$. To synthesize an image, we select a tuple $(i, j, c, s, t)$ where $i \in S, j \in S$ correspond to two subjects that will be mixed, and $s \in \{1, \ldots, n_i\}$ and $t \in \{1, \ldots, n_j\}$ are indices of images of $i$ and $j$ that will be used. The bitcode $c \in \{0, 1\}^5$ defines which parts will be taken from each subject. A zero at a certain position in $c$ means that the corresponding part will be taken from $i$, otherwise it will be taken from $j$. There are only $2^5 - 2 = 30$ valid options for $b$, since the codes 00000 and 11111 correspond to the original images of $s$ and $t$ respectively, instead of synthetic ones.

To synthesize a new image, we designate one of parent images as the “base” image from which we use the R (the rest) part, and the other as the “injection” image from which one or more parts will be pasted on the base image. Since the size of the facial parts in the two parent images are in general different, we re-size the facial parts of the injection image to that of the base image. The main challenge to implement the proposed synthesis method is to accurately locate the facial parts. Recently, many efficient and accurate landmark detectors have been proposed. We use four landmarks detected by the method of Zhang et al. [65] to define the rectangular region that corresponds to each face part.

We refer to each choice of $(i, j, c)$ with $i \neq j$ as a “virtual subject” which consists of a mix of two existing subjects in the dataset. In total we can generate $30|S|(|S| - 1) / 2$ different virtual subjects, and for each of these we can generate $n_i \times n_j$ samples. Note that if we set $i = j$ we can in the same manner synthesize $30n_i(n_i - 1) / 2$ new images for an existing subject.

Although some works [27], [55] empirically verified the
effectiveness of synthetic data, they did not give much insight into how. In our work, the synthetic data captures a dataset of richer intra-personal variations by generating a large number of images of the same identities, leading to a ‘deeper’ training set. Also, our engine can synthesize a large number of faces of new identities, generating a ‘wider’ training set. Thus the synthetic identities interpolate the whole space of pixel-identity mappings. Not surprisingly, a better CNN model can be trained using this deeper and wider training set. The methods of generating our deeper and wider training set are detailed in Section V-A.

B. Compositing artefacts

The synthetic faces present two types of artefacts: (I) hard boundary effects, and (II) inconsistent/unnatural intra-personal variations (lighting, pose, etc.) between facial patches. These are illustrated in Fig. 2. Note that the type I artefacts are generated by not only our method but also 3D synthesis methods such as [27], [55], [12]. As shown in the top-right side of Fig. 2, the artefacts created by 3D methods are due to inaccurate 3D model to 2D image fitting. The inaccurate fitting makes the synthetic faces extract the pixels from background rather than facial areas, leading to bad facial boundaries.

Despite the existence of these artefacts, this synthetic data is still useful for training strong face recognition models. This can be understood from several perspectives: (1) Type I artefacts are common to all the synthetic faces in the training set, therefore the CNN does not learn to rely on artefacts as discriminative features coding for identity, i.e., it learns artefact invariance. This means its performance is not compromised when subsequently presented with artefact-free images at testing-time. Other studies have also shown that synthetic data still improves recognition performance, despite the presence of type I artefacts [27]. (2) The artefacts can be regarded as noise, which has been shown to improve model generalisation in a variety of settings by increasing robustness and reducing overfitting. For example in the case of CNNs, training with data augmentation in the form of specifically designed deformed noise is important to obtain good recognition performance [63]; and in the case of de-noising auto encoders, training on images with noise, corruption and artefacts has been shown to improve face classification performance [57]. (3) As a concrete example to understand how type II artefacts can improve performance, consider two synthetic images with the same identity label, but one a type II artefact on the mouth caused by illumination, e.g., in Fig. 2 (bottom left). Training to predict these images as having the same identity means that the CNN learns an illumination-invariant feature for the mouth. And similarly for other intra-personal variations (such as pose, expression). Thus while some artefact images look strange, they are actually a powerful form of data augmentation that helps the CNN to learn robustness to all these nuisance factors.

IV. FACE RECOGNITION PIPELINE

In this section we describe the different elements of our pipeline for face identification and verification in detail.

<table>
<thead>
<tr>
<th>TABLE I: Our two CNN architectures</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CNN-L</strong></td>
</tr>
<tr>
<td>conv1</td>
</tr>
<tr>
<td>32 x 3 x 3, st.1; 64 x 3 x 3, st.1</td>
</tr>
<tr>
<td>x2 maxpool, st.2</td>
</tr>
<tr>
<td>conv2</td>
</tr>
<tr>
<td>64 x 3 x 3, st.1; 128 x 3 x 3, st.1</td>
</tr>
<tr>
<td>x2 maxpool, st.2</td>
</tr>
<tr>
<td>conv3</td>
</tr>
<tr>
<td>96 x 3 x 3, st.1; 192 x 3 x 3, st.1</td>
</tr>
<tr>
<td>x2 maxpool, st.2</td>
</tr>
<tr>
<td>conv4</td>
</tr>
<tr>
<td>128 x 3 x 3, st.1; 256 x 3 x 3, st.1</td>
</tr>
<tr>
<td>x2 maxpool, st.2</td>
</tr>
<tr>
<td>conv5</td>
</tr>
<tr>
<td>160 x 3 x 3, st.1; 320 x 3 x 3, st.1</td>
</tr>
<tr>
<td>x7 avgpool, st.1</td>
</tr>
<tr>
<td>Fully connected</td>
</tr>
<tr>
<td>Softmax-5000</td>
</tr>
</tbody>
</table>

A. CNN architectures

Face recognition in the wild is a challenging task. As described in Section II-A, the existing deep learning methods highly depend on big training data. Very little research investigates training CNNs using small data. Recently, Hu et al. [15] evaluated CNNs trained using small datasets. Due to the limited training samples, they found the performance of CNNs to be worse than handcrafted features such as high-dimensional features [6] (0.8763 vs 0.9318). In this work, we use a limited training set of around 10,000 images to synthesize a much larger one of around 1.5 million images for CNN training. The synthesized training data captures various deformable facial patterns that are important to improve the generalization capacity of CNNs.

We use two CNN architectures. The first one, from [15] has fewer filters and is referred as CNN-S. The second, from [62], is much larger and referred as CNN-L. These two architectures are detailed in Table I. Using the CNN-L model we achieve state-of-the-art performance on the LFW dataset [16] under ‘unrestricted, label-free outside data’ protocol.
B. NIR-VIS heterogeneous face recognition

NIR-VIS (near-infrared to visual) face recognition is important in applications where probe images are captured by NIR cameras that use active lighting which is invisible to the human eye [29]. Gallery images are, however, generally only available in the visible spectrum. The existing methods for NIR-VIS face recognition include three steps: (i) illumination pre-processing, (ii) feature extraction, and (iii) metric learning. First, the NIR-VIS illumination differences cause the main difficulty of NIR-VIS face recognition. Therefore, illumination normalization methods are usually used to reduce these differences. Second, to reduce the heterogeneities of NIR and VIS images, illumination-robust features such as LBP are usually extracted. Third, metric learning is widely utilized, aiming at removing the differences of modalities and meanwhile keeping the discriminative information of the extracted features.

In this work, we also follow these three steps that are detailed in Section V-D. Unlike the existing work that extracts handcrafted features, we learn face representations using two CNN architectures described above. To our knowledge, we are the first to use deep CNNs for NIR-VIS face recognition. The main difficulty of training CNNs results from the lack of NIR training images, which we address via data synthesis.

C. Network Fusion

Fusion of multiple networks is a widely used strategy to improve the performance of deep CNN models. For example, in [45] an ensemble of seven networks is used to improve the object recognition performance due to complementarity of the models trained at different scales. Network fusion is also successfully applied to learn face representations. DeepID and its variants [48], [51], [52] train multiple CNNs using image patches extracted from different facial parts.

The heterogeneity of NIR and VIS images is intrinsically caused by the different spectral bands from which they are acquired. The images in both modalities, however, are reflective in nature and affected by illumination variations. Illumination normalization can be used to reduce such variability, at the risk of losing identity-specific characteristics. In this work, we fuse two networks that are trained using the original and illumination-normalized images respectively. This network fusion significantly boosts the recognition rate.

D. Metric Learning

The goal of metric learning is to make different classes more separated, and instances in the same class closer. Most approaches learn a Mahalanobis metric

\[ d_A^2(x_i, x_j) = (x_i - x_j)^T A (x_i - x_j), \]

which maximizes inter-class discrepancy, while minimizing intra-class discrepancy. Other methods, instead learn a generalized dot-product of the form

\[ d_B^2(x_i, x_j) = x_i^T B x_j. \]

Metric learning methods are widely used for face identification and verification. Because identification and verification are two different tasks, different loss functions should be optimized to learn the metric. Joint Bayesian metric learning (JB) [5] and Fisher linear discriminant analysis (LDA) are probably the two most widely used metric learning methods for face verification and identification respectively. In particular, LDA can be seen as a method to learn a metric of the form of Eq. (1), while JB learns a verification function that can be written as a weighted sum of Eq. (1) and (2). In our work we use JB and LDA to improve the performance of face verification and identification respectively.

V. Experiments

A. Data synthesis methods

Given a set of face images and their IDs, we define three strategies for synthesis: Inter-Synthesis, Intra-Synthesis, and Self-Synthesis. Inter-Synthesis synthesizes a new image using two parents from different IDs as shown in Fig. 1. The facial components of an Intra-Synthesized face are from different images with the same ID. Self-Synthesis is a special case of Intra-Synthesis. Specifically, one given image synthesizes new images by swapping facial components of itself and its mirrored version. By virtue of Self-Synthesis, one input image can become maximum 32 images which have complementary information. In the view of NIR-VIS cross-modality, we also define ‘cross-modality synthesis’ which uses images from different modalities to synthesize a new one. Some synthetic images from the CASIA NIR-VIS 2.0 dataset with LSSF [60] illumination normalization are shown in Fig. 3. The reasons of using LSSF illumination normalization are detailed in Section V-D. As shown in Fig. 3, the results of Intra-Synthesis method are usually more natural than Inter-Synthesis method since the Intra-Synthesis method uses the same ID. However, as shown in the right of Fig. 3, Intra-Synthesis can also create artefacts due to large pose variations.

B. Implementation details

Before face synthesis, all the raw images are aligned and cropped to size 100 × 100 as in [62] on both datasets. We train our models using images only from LFW and CASIA NIR-VIS2.0 databases. For the CNN-S model on both datasets, we set the learning rate as 0.001, and decrease it by 10 times every 4000 iterations, and stop training after 10K iterations. We find that dropout is not helpful for the small network, and report results obtained without it. For the CNN-L model on the NIR-VIS dataset, we set the learning rate as 0.01, and decrease it by 10 times every 8000 iterations, and stop training after 20K iterations. For the CNN-L model on the LFW dataset, we set the learning rate as 0.01, and decrease it by 10 times every 120K iterations, and stop training after 200K iterations. We set dropout rate as 0.4 for the pool5 layer of the CNN-L model. For both CNN-S and CNN-L models, the batch size is 128, momentum is 0.9, and decay is 0.0005. Softmax loss function is used to guide CNN training. The features used in our recognition experiments with CNN-S and CNN-L are FC-160 (160D) and Pool5 (320D), respectively.
TABLE II: Training data synthesized from LFW

<table>
<thead>
<tr>
<th></th>
<th>IDs</th>
<th>Images</th>
<th>Images/ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Synthetic</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Intra-Syn</td>
<td>5K</td>
<td>500K</td>
<td>100</td>
</tr>
<tr>
<td>Inter-Syn</td>
<td>5K</td>
<td>1M</td>
<td>200</td>
</tr>
<tr>
<td>Total</td>
<td>10K</td>
<td>1.5M</td>
<td>150</td>
</tr>
<tr>
<td>Raw</td>
<td>5K</td>
<td>10K</td>
<td>2</td>
</tr>
</tbody>
</table>

C. Face recognition in the wild

1) Database and protocol: Labeled Faces in the Wild (LFW) [16] is a public dataset for unconstrained face recognition study. It contains 5,749 unique identities and 13,233 face photographs. The training and test sets are pre-defined in [16]. For evaluation, the full dataset is divided into ten splits, and each time nine of them are used for training and the left one for testing. Our work falls in the protocol of ‘Unrestricted, Label-Free Outside Data’ as we use the identity information to train the neural network (softmax loss). Meanwhile, all face images are aligned using a model trained on unlabeled outside data. As a benchmark for comparison, we report the mean and standard deviation of classification accuracy.

Under LFW protocol, the training set in each fold is different. Therefore, the size of synthetic data and the original raw LFW data in Table II is averaged over 10 folds. We generate 1.5 million training images, including 1 million ‘Inter-Syn’ ones and 0.5 million ‘Intra-Syn’ ones, as defined in Section V-A.

2) Analysis of CNN model and synthetic data: We here analyse the trained model by visualising the synthetic images in feature space. We choose the images of two subjects (George W. Bush and Colin Powell), which have the largest number of images in LFW, and the synthetic images derived from the two subjects for analysis. To analyse the effects of replacing different facial components (eyes, nose, mouth), we only replace one patches of a particular facial component of Bush with ones from himself (Intra-Synthesis) or from Powell (Inter-Synthesis), as shown in Fig. 4. For each case, 100 images are synthesised. Therefore, there are 8 groups of images: 2 groups of original images (Bush and Powell), 3 Intra-Synthesis (one of three components is replaced by images of Bush) and 3 Inter-Synthesis (by images of Powell). These images are fed into one CNN-L to extract features, which are then projected to a PCA space. The first two PCA components of each feature are shown in Fig. 5.

Fig. 5(a)-(c) show the face distributions if one particular facial component is replaced. In Fig. 5(a), 3 identities, ‘GeorgeWBush+intra-Eyes’, ‘ColinPowell’ and ‘inter-Eyes’ are well separated. It means that the identity information is kept if Bush’s eyes are replaced by those from himself. In contrast, a new identity space is generated by the synthetic images that replace Bush’s eyes with Powell’s. The same conclusion can be drawn from nose in Fig. 5(b). In Fig. 5(c), however, ‘intra-Mouth’ and ‘inter-Mouth’ are not well separated. It means that the mouth component is not very discriminative between people. Fig. 5(d) and (e) contrast the results when training with original and synthetic (Fig. 5(d)) versus original data only (Fig. 5(e)). Fig. 5(d) is relatively more discriminative for identity, particularly the synthetic identities. Thus we can see that training with synthetic data is important to interpolate the identity space, and thus achieve good results for unseen identities – as required at testing time.

3) Impact of synthetic data: Table III analyzes the importance of using the synthetic data. First, CNN-S trained using synthetic data (‘Intra-Syn’ and ‘Inter-Syn’) outperforms greatly the model trained using just the original LFW images, showing the importance of data synthesis. Second, ‘Inter-
Syn’ works slightly better than ‘Intra-Syn’, since ‘Inter-Syn’ can capture richer facial variations. Third, combining ‘Inter-Syn’ and ‘Intra-Syn’ works better than either of them because they capture complementary variations. Fourth, averaging the features of 32 ‘Self-Syn’ (‘32-Avg’ in Table III and defined in Section V-A) images works consistently better than that of one single test image (‘single’ in Table III). Fifth, CNN-L works consistently better than CNN-S using either original LFW or synthetic images because deeper architecture has stronger generalization capacity. Finally, metric learning further enhances the face recognition performance.

4) Impact of Image Blending: In Section III, we speculated the existence of artifacts (‘hard boundaries’) can improve the robustness of the model. We now experimentally investigate this by reducing such ‘hard boundaries’ using image blending. In particular, we implemented Poisson image editing [33] to smooth these boundaries. In Fig. 6, we show some results of Poisson image blending. From Fig. 6, as expected, Poisson blending does make the boundaries much smoother compared with our synthesis method. In Table III, we compare the results with and without Poisson image editing. We can see that recognition accuracy based on training data synthesised with ‘hard’ boundaries is, somewhat, higher than with Poisson blending. This supports the idea that ‘hard’ boundaries provide a source of noise that is beneficial in making network training more robust detailed in Section III.

5) Comparison with the state-of-the-art: Table IV compares our method with state-of-the-art methods. All methods listed in Table IV except ours use hand-crafted features, again underlining the difficulty of training deep CNNs with small data. The best deep learning solution [47] recorded in official benchmark achieves 91.75%, and ours is 4% better. In addi-
TABLE III: Comparison of synthetic data methods on LFW

<table>
<thead>
<tr>
<th>Architecture</th>
<th>Metric learning</th>
<th>Training data</th>
<th>single (%)</th>
<th>32-Avg (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Original</td>
<td>78.97 ± 0.78</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Intra-Syn+Original</td>
<td>83.03 ± 0.56</td>
<td>83.93 ± 0.49</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Inter-Syn+Original</td>
<td>83.18 ± 0.74</td>
<td>84.35 ± 0.65</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Intra-Syn+Inter-Syn+Original</td>
<td>80.61 ± 0.71</td>
<td>80.98 ± 0.57</td>
</tr>
</tbody>
</table>

TABLE IV: Comparison with state-of-the-art methods on LFW

<table>
<thead>
<tr>
<th>Methods</th>
<th>Accuracy (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fisher vector faces [43]</td>
<td>93.03 ± 1.05</td>
</tr>
<tr>
<td>HPEN [67]</td>
<td>95.25 ± 0.36</td>
</tr>
<tr>
<td>MDMC-DCPs [8]</td>
<td>95.38 ± 0.34</td>
</tr>
<tr>
<td>The proposed</td>
<td>95.77 ± 0.38</td>
</tr>
</tbody>
</table>

TABLE V: Hand-crafted features on LFW

<table>
<thead>
<tr>
<th>Methods</th>
<th>Accuracy (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>HD-LBP</td>
<td>84.13 ± 1.76</td>
</tr>
<tr>
<td>HD-LBP+JB (original)</td>
<td>89.02 ± 1.11</td>
</tr>
<tr>
<td>HD-LBP+JB (original + synthetic)</td>
<td>91.03 ± 1.06</td>
</tr>
</tbody>
</table>

Fig. 6: Comparison of synthesis with/without blending. Row 1-2: Input image pairs, Row 3: Our synthesis with ‘hard boundaries’, Row 4: Poisson blending

Fig. 7: Recognition rate (%) on LFW using the original CASIA WEBFACE training data (0.5M) and synthetic data (0-3M).

7) Impact of synthetic images on larger training sets: Our original motivation was to learn effective face representations from small datasets. We demonstrated the effectiveness of generating synthetic data to expand a small training set (LFW, 5K identities and 10K images) in Table III. Recently, some bigger training sets of face images in the wild have been released, such as CASIA WEBFACE [62] (10K identities and 0.5M images). We conduct experiments using the latter dataset to assess whether our data synthesis strategy is also useful for such larger datasets. As before, we keep the ratio 2:1 of ‘Inter-Syn’ and ‘Intra-Syn’ synthetic images. To investigate the effects of the size of synthetic data, we generate six sets of synthetic images: {0.5M, 1M, 1.5M, 2M, 2.5M, 3M} images. We trained the CNN-L network using the original CASIA WEBFACE images, plus a variable amount of synthetic data. From Fig 7, we can see that the recognition rate on LFW increases with the amount of synthetic data. This demonstrates that our data synthesis strategy is still very effective even with relatively large datasets.
D. NIR-VIS face recognition

1) Database and protocol: The largest face database across NIR and VIS spectrum so far is the CASIA NIR-VIS 2.0 face database [23]. It contains 17,580 images of 725 subjects which exhibit intra-personal variations such as pose and expression. This database includes two views: view 1 for parameter tuning and view 2 including 10 folds for performance evaluation. During test, the gallery and probe images are VIS and NIR images respectively, simulating the scenario of face recognition in the dark environment. The rank 1 identification rate including the mean accuracy and standard deviation of 10 folds are reported.

Because the images of CASIA NIR-VIS2.0 are from two modalities (NIR and VIS), we applied ‘cross-modality synthesis’ to synthesize new images. The size of synthesized data is detailed in Table VI.

2) Illumination normalization and feature extraction: Illumination Normalization (IN) methods are usually used to narrow the gap between NIR and VIS images. To investigate the impact of IN, we preprocessed images using three popular IN methods: illumination normalization based on large- and small-scale features (LSSF) [60], Diffence-of-Gaussian filtering-based normalization (DOG), and single-scale retinex (SSR) [19]. We train CNN-S and CNN-L using illumination normalized and non-normalized images. For simplicity, only the images from CASIA NIR-VIS2.0 excluding synthetic ones are used. Fig. 8 shows the face recognition rates at different training iterations using different input images for the CNN-S and CNN-L networks. The results show the effectiveness of IN, and LSSF achieves the best performance due to its strong capacity of removing illumination effects without affecting identity information. As for the LFW experiments in Section V-C, CNN-L works better than CNN-S.

We also extracted LBP features from the LSSF-normalized images, and achieve 12.48 ± 3.1 in comparison with 17.41 ± 3.76 obtained with features from the CNN-L network. Showing again the superior performance of CNN learned features.

3) Effects of synthetic data: In practice, we find two problems with the synthetic data generated from the CASIA NIR-VIS2.0 dataset: (1) It cannot capture enough facial variations because it only has 357 subjects as shown in Table VI. (2) There are much fewer VIS images than NIR ones. To solve these two problems, we also use the synthetic data generated from LFW images defined in Table II.

Table VII compares the results achieved by these two sources of synthetic data. First, the accuracy achieved by using the synthetic data generated from CASIA NIR-VIS2.0 database is 34.13 ± 2.13, in comparison with 17.41 ± 3.76 without synthetic data. The significant improvement shows the effectiveness of data synthesis. Second, the model trained using raw and synthetic LSSF-normalized LFW images greatly outperforms those synthetic CASIA NIR-VIS2.0 images: 66.37 ± 1.45 vs. 38.45 ± 2.08, although NIR images are completely unseen during training. The reasons are 2-fold: (1) LFW images contains more subjects which can capture more facial variations as analyzed above. (2) LSSF can greatly reduce the gap between NIR and VIS, therefore, LSSF-normalized LFW synthetic images can generalize well to LSSF-normalized NIR images. To further improve the face recognition performance, we trained the network using both raw and synthetic data from both sources (LFW+CASIA NIR-VIS). The face recognition rate is improved from 66.37 ± 1.45 to 68.97 ± 1.24, showing the value provided by our of bigger synthetic dataset.

4) Comparison with the state-of-the-art: The CNN-L models in Table VIII are all trained using synthetic data. First, LSSF-normalized and Original LFW synthetic data achieve very comparable performance: 68.97% vs. 69.11%. However, the fusion (averaging) of these two features can significantly improve the face recognition rates. It shows the

**TABLE VI: Synthetic data using CASIA NIR-VIS2.0 database**

<table>
<thead>
<tr>
<th></th>
<th>IDs</th>
<th>Images</th>
<th>Images/ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Synthetic</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Intra-Syn</td>
<td>357</td>
<td>90K</td>
<td>250</td>
</tr>
<tr>
<td>Inter-Syn</td>
<td>1K</td>
<td>150K</td>
<td>150</td>
</tr>
<tr>
<td>Total</td>
<td>1.4K</td>
<td>240K</td>
<td>170</td>
</tr>
<tr>
<td>Original</td>
<td>357</td>
<td>8.5K</td>
<td>23</td>
</tr>
</tbody>
</table>

**TABLE VII: Evaluation of the impact of synthetic data**

<table>
<thead>
<tr>
<th>Training Data</th>
<th>CASIA NIR-VIS2.0</th>
<th>LFW</th>
<th>Accuracy(%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Baseline</td>
<td>Raw</td>
<td>-</td>
<td>17.41 ± 3.76</td>
</tr>
<tr>
<td>Synthetic Data</td>
<td>Raw+Syn</td>
<td>-</td>
<td>34.13 ± 2.13</td>
</tr>
<tr>
<td></td>
<td>Raw+Syn</td>
<td>Raw</td>
<td>38.45 ± 2.08</td>
</tr>
<tr>
<td></td>
<td>Raw+Syn</td>
<td>Raw+Syn</td>
<td>68.97 ± 1.24</td>
</tr>
</tbody>
</table>

![Fig. 8: Effect of illumination normalization methods using the CNN-S (top) and CNN-L networks.](image-url)
fusion can keep the discriminative facial information but remove the illumination effects. Second, not surprisingly, metric learning can further improve the performance. The metric learning method used here is LDA, which is the most widely used one for face identification. Finally, Table VIII compares the proposed method against the state-of-the-art solutions [26], [20]. [26] uses a designed descriptor that performs better in this dataset compared with other generic hand-crafted features, and LDA can further improve the accuracy. Our method significantly outperforms [26] when metric learning is not used (79.96% vs. 56.6%), and maintains superior performance when metric learning is used (85.05% vs. 81.8%). [20] tries to solve the domain shift between two data sources (NIR and VIS) by a cross-modal metric learning: it assumes that a pair of NIR and VIS images shares the same sparse representation under two jointly learned dictionaries. Our method improves over [20] with a 7% margin without such an extra step of dictionary learning. Concurrently to our work, Saxena & Verbeek [39] obtained a comparable performance of 85.9% using a cross-modal version of LDML metric learning [11], albeit using CNN features learned from the 500,000 face images of the CASIA WEBFACE dataset. Finally, Yi et al. [61] obtained the best performance of 86.1% using an approach that extracts 40 dim. Gabor features at 176 local face regions, and uses these to train 176 different restricted Boltzmann machines (RBMs) specialized to model the modality shift at each face region. Note that unlike our approach based on feed-forward CNNs, their approach requires Gibbs sampling at test-time to infer the face representations.

VI. CONCLUSIONS AND FUTURE WORK
Recently, convolutional neural networks have attracted a lot of attention in the field of face recognition. However, deep learning methods heavily depend on big training data, which is not always available. To solve this problem in the field of face recognition, we propose a new face synthesis method which swaps the facial components of different face images to generate a new face. With this technique, we achieve state-of-the-art face recognition performance on LFW and CASIA NIR-VIS2.0 face databases.

In the future, we will apply this technique to more applications of face analysis. For example, the proposed data synthesis method can easily be used in training CNN-based face detection, facial attribute recognition, etc. More generally, the method applies to any objects which are well structured. For example, the human body is well structured and human images can be synthesised using this method. The synthetic images can be used to train deep models for pose estimation, pedestrian detection, and person re-identification.

ACKNOWLEDGMENT
This work is supported by European Unions Horizon 2020 research and innovation program under grant No 640891, the Science and Technology Plan Project of Hunan Province (2016TP1020), the Natural Science Foundation of China (No. 61502152), and the French research agency contracts ANR-16-CE23-0006 and ANR-11-LABX-0025-01. We gratefully acknowledge NVIDIA for the donation of the GPUs for this research.

REFERENCES


