Privacy Protection Performance of De-identified Face Images with and without Background

Zongji Sun, Li Meng* and Aladdin Ariyaeeinia
School of Engineering and Technology
University of Hertfordshire
Hatfield, AL10 9AB, UK
Email: {z.sun3, L.1.MENG*, a.m.ariyaeeinia}@herts.ac.uk

Xiaodong Duan, Zheng-Hua Tan
Department of Electronic Systems
Aalborg University, Denmark
Email: {xd, zt}@es.aau.dk

***Abstract*—This paper presents an approach to blending a de-identified face region with its original background, for the purpose of completing the process of face de-identification. The re-identification risk of the de-identified FERET face images has been evaluated for the *k*-Diff-furthest face de-identification method, using several face recognition benchmark methods including PCA, LBP, HOG and LPQ. The experimental results show that the *k*-Diff-furthest face de-identification delivers high privacy protection within the face region while blending the de-identified face region with its original background may significantly increases the re-identification risk, indicating that de-identification must also be applied to image areas beyond the face region.**

Keywords—face de-identification; privacy protection; face re-identification; seamless cloning

I. INTRODUCTION

With the advance of sensor technology and the reduced cost of data storage, a huge amount of personal data are being collected at an increasing pace due to their economic and social values. Face biometric, one of the easiest biometrics to collect, is widely used in various application scenarios. Its popularity has boosted due to the recent breakthrough in pattern recognition using deep learning. The latest benchmark results on the LFW (Labelled Faces in the Wild) dataset showed that with a massive training set the performance of face recognition based on a deep convolutional neural network (CNN) successfully achieved a pair-wise verification accuracy of 99.77% [1]. Zhang et al. [2] showed that the person recognition rate could achieve 83.05% on a photo album, where only half of the images in the album contain a frontal face.

However, such data often contain sensitive personal information, which has inevitably raised privacy concerns and been exploited in privacy attacks. The 1995 Data Protection Directive of the European Union (Directive 95/46/EC) [3] demands the deployment of appropriate technical and organizational measures to protect private information in the course of transferring or processing such data. This legal requirement along with ethical responsibilities has attracted intensive research effort in the field of de-identification [4], [5]. The goal of de-identification is twofold: privacy protection as well as data utility preservation. In such way, a de-identified dataset can be used as a replacement of its original dataset to facilitate further data analysis.

Masking, blurring and pixilation are the ad hoc face de-identification methods that were widely used in the past. However these methods do not achieve their goal of privacy protection as the blurring process is revisable while the identity in a pixelated or masked face image can be 100% recognised by parrot recognition [4]. Furthermore, all of these ad hoc methods are destructive and destroy data utility.

The *k*-Same-Pixel/Eigen face de-identification method was the first successful face de-identification method in terms of privacy protection. The *k*-Same methods guarantee a re-identification risk lower than 1/*k*. However, the original *k*-Same-Pixel/Eigen method has some limitations, including ghost artefacts in the de-identified image, *k*-dependant performance, loss of data utility and loss of data diversity, etc. Some of these limitations have been successfully addressed. For example, *k*-Same-M [5] face de-identification eliminated ghost artefacts by aligning faces in the Active Appearance Models. To further improve the privacy protection performance, *k*-Same-furthest [6] and *k*-Diff-furthest [7] face de-identification methods were proposed by the authors and their privacy protection performance with some moderate datasets were presented. This paper presents the work that has been carried out to close the loop of face de-identification, where the de-identified face region is blended back with the background of the original face image. Furthermore, the privacy protection performance of the previously proposed *k*-Diff-furthest methods has been evaluated with the benchmark dataset FERET, before and after background blending.

The rest of the paper is structured as follows. Section II explains the main techniques used in this work. Section III describes our work on closing the loop of face de-identification. Section IV evaluates the privacy protection performance of the proposed face de-identification methods. Finally, Section V summarises the key findings and proposes future work.

II. SUBJECT REVIEW

A. Face Modelling

Active Appearance Model (AAM) is a statistical approach to object modelling. In AAMs, each face image region is represented as a combination of a face shape model and a face texture model. The face shape is defined by the locations of a set of pre-defined facial landmarks and the shapeless texture is generated by warping the original face onto a common shape. An AAM is established through training, where Principal

Component Analysis (PCA) is applied to both the shapes and the textures of the faces in the training set for the purpose of dimensionality reduction. As a result, only the first n shape PCA eigenvectors $\{s_1, \dots, s_n\}$ and the first m texture PCA eigenvectors $\{A_1, \dots, A_m\}$ are used by the trained AAM to represent a given face image. For a given face image, the trained AAM generates its shape as $s = s_0 + \sum_{i=1}^{n} p_i s_i$, and its texture as $A = A_0 + \sum_{i=1}^{m} \lambda_i A_i$, where s_0 and A_0 are respectively the average shape and texture over the training set, shape parameters $\mathbf{p} \in \mathbb{R}^n$ and texture parameters $\boldsymbol{\lambda} \in \mathbb{R}^m$. Typically, when shape and texture parameters are combined together, a scaling factors is applied to one of the two parameter sets, e.g. in the format of $\{W_s p_1, \dots, W_s p_n, \lambda_1, \dots, \lambda_m\}$, to make sure they share a common range. AAMs have been used in face de-identification to not only extra shape and texture features from given face images but also to synthesise new face images. Some face features are not identity related and but will affect the visual quality of the de-identified images in forms of ghost artefacts (e.g. glasses, beard and moustache) or unnatural skin tone (e.g. illumination condition). To make sure good visual quality of the de-identified face images, some non-identity related factors are removed in this work by excluding face images with such non-identity features from the AAM training set. More details of this is given in Section III with example result images.

B. The k-Diff-furthest Face De-identification Method

The *k*-Same methods (*k*-Same-Pixel, *k*-Same-M, *k*-Same-furthest, etc.) all performs face de-identification by applying microaggregation to the original face images, where the set of original faces are divided into clusters of *k* and, for each cluster formed, all the original faces in the cluster are de-identified with the average of that cluster. As each de-identified face image appears in the de-identified image set *k* times and it can be matched, at best, with one of its *k* original faces, all *k*-Same method can guarantee a re-identification risk lower than 1/*k* for their de-identified faces.

To further reduce the re-identification risk, the *k*-Same-furthest method was proposed. It minimises the association between subjects and their face data by introducing data swapping after microaggragation. In each iteration of de-identification, *k*-Same-furthest forms two clusters, each of size *k*, among the remaining original faces and ensures the distance of the two formed clusters is maximised. Unlike *k*-Same-Pixel and *k*-Same-M, the *k*-Same-furthest method de-identifies the faces in one cluster using the average of the other cluster rather than its own. A similar clustering approach has been adopted in the MDAV-generic to form clusters of size *k* [8]. As stated in [8], optimal clustering is NP-hard. The clustering approach of [8] as well as the *k*-Same-furthest method is near-optimal. The main differences between the *k*-Same-furthest and the MDAV-generic method are: 1) MDAV-generic always uses the average of the remaining data to form the next pair of clusters while *k*-Same-furthest forms the next cluster pair based on a randomly selected face. As a result, any two runs of the *k*-Same-further method could hardly produce identical results. 2) Overlapping between each pair of clusters is prevented in *k*-Same-furthest to minimise re-identification risk (mathematical proof of this has been given in [7]). And 3) *k*-Same-furthest applies data swapping between each pair of clusters while MDAV-generic as a microaggregation method, it does not adopt data swapping.

In a set of *k*-Same de-identified face images, there are at least *k* subjects sharing the same de-identified face, making it impossible to distinguish let alone track individuals. In information theory, entropy of a data set is defined as the negative of the logarithm of its probability distribution. Repetition of data in *k*-Same face de-identification inevitably leads to entropy loss or information loss. Let $\mathbf{F}_{\text{orig}} = \{\Gamma_1, \dots, \Gamma_M\}$ be a set of *M* face images and be person-specific (i.e. one image per person). Let $\mathbf{F}_{deid}$ denote the de-identified version of $\mathbf{F}_{orig}$. The entropy of $\mathbf{F}_{orig}$ and $\mathbf{F}_{deid}$ is given in (1) and (2), respectively.

$$H(\mathbf{F}_{\text{orig}}) = -\sum_{i=1}^{M} \mathrm{P}(\Gamma_i) \log_2 \mathrm{P}(\Gamma_i) = -\log_2 \frac{1}{M} \quad (1)$$

$$H(\mathbf{F}_{deid}) = -\sum_{i=1}^{\left|\frac{M}{k}\right|} P(\Gamma_{di}) \log_2 P(\Gamma_{di}) \leq -\log_2 \frac{k}{M}$$

$$= -\log_2 \frac{1}{M} - \log_2 k = H(\mathbf{F}_{orig}) - \log_2 k \quad (2)$$

It is easy to see that $H(\mathbf{F}_{orig}) > H(\mathbf{F}_{deid})$ as $k > 1$, meaning that information has been lost through the microaggreation process in *k*-Same face de-identification. This information loss is due to a decrease in data diversity but it is the mechanism adopted in all *k*-Same face de-identification methods for achieving a guaranteed re-identification risk lower than $1/k$.

To prevent information loss, we have maintained data diversity in the de-identified face set and proposed the *k*-Diff-furthest face de-identification method [7]. Like the *k*-Same-furthest method, *k*-Diff-furthest forms two non-overlapping clusters in each iteration. However, it swaps the cluster centres without aggregating the faces in each cluster. There are two contributions of *k*-Diff-furthest. Firstly, the entropy of the de-identified dataset is the same as that of the original dataset, which means each subject gets a unique de-identified face. The privacy protection performance of the proposed *k*-Diff-furthest method is evaluated in Section IV where the re-identification risk of the *k*-Diff-furthest de-identified faces is always near-zero.

C. Re-identification Risk of the De-identified Faces

Three types of re-identification attack can be used to test the protection performance of the de-identification results [4]. The first type of attack is termed naïve recognition, in which the original face images are used as the gallery and de-identified face images as the probes. The second type of attack is termed reverse recognition, in which the de-identified face images are used as the gallery and the original face images as the probes. The third type of attack is termed parrot recognition. The word 'parrot' means that the de-identification technique is duplicated by the attacker and the set of de-identified face images generated by the attacker is used as probes to match with the published version of the de-identified face image set. As mentioned in Section II.B, in each iteration of *k*-Same/Diff-furthest face de-identification two clusters are formed based on a randomly selected face. This means it is highly unlikely to repeat the same random selections and produce the same set of de-identified faces. In other words, parrot recognition does not work on either *k*-Same-furthest or *k*-Diff-furthest method.

TABLE I. KEY PARAMETERS OF THE FACE RECOGNITION METHODS USED IN THE EVELUATION EXPERIMENTS

Feature	*Parameter values*	*Distance measurement*
PCA	–	Euclidean distance
LBP	*radius* = 1, *neighbours* = 8	Chi-squared distance
HOG	*cell* = 10 × 10, *orientations* = 16	Cosine distance
LPQ	*cell* = 10 × 10	Cosine distance

In our work, AAM is used as the face descriptor. The proposed face de-identification methods form clusters based on Euclidean distance in the AAM feature space. Experimental results from our previous work [6], [9] showed that the re-identification risk is near zero if the attacker uses AAM face representation and matches faces based on Euclidean distance as well. To fully evaluate the privacy protection performance of our proposed methods, further evaluation experiments have been conducted which used various face representation models and distance measures, including Eigenface (PCA) [10], Local Binary Patterns (LBPs) [11], Histogram of Oriented Gradient (HOG) [12] and Local Phase Quantization (LPQ) features [13]. TABLE I summarises the key parameters of these face recognition benchmark methods. In addition, *k*-Nearest Neighbours method has been used to find the top match; and the dimension of both HOG features and LPQ features were reduced to 500 by applying PCA.

III. BLENDING THE DE-IDENTIFIED FACE WITH ITS ORIGINAL IMAGE BACKGROUND

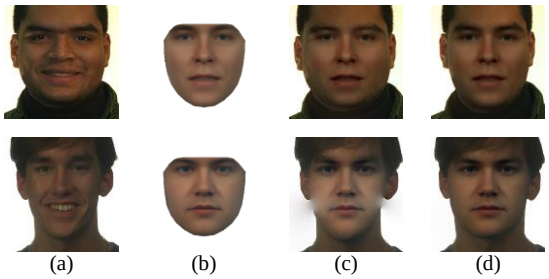
So far, all the published face de-identification methods focus on the isolated face region in the original images. The result images presented in the publications are composed of a de-identified face region and a blank background. The second column of Fig. 1 show the examples. As shown in the examples, the face region exclude hair, the ears, the forehead, the neck, the rest of the human body and the shooting environment. However, real life applications always prefer a face with a background. As stated, the background here means the rest of the human body and the shooting environment that are presented in the original image. In the case of face de-identification, this leads to the demand of blending the de-identified face region back onto its original image background.

One of the main challenges in this task is given by the noticeable differences between the original and the de-identified faces in terms of skin tone, illumination, direction of lighting, etc. Previous research in the field of face swapping and image editing has investigated similar problems and has provided several useful solutions to this challenge. The study on face swapping in [14] used one recolouring method followed by one relighting method to adjust the skin tone. Impett et al. [15] used histogram matching in the RGB space to allow real-time operation. As real-time operation is not a priority for our work at this stage, the more powerful but more time-consuming method of Poisson seamless cloning [16] has been used to achieve a better visual quality of the blended images.

As shown in Fig. 1, the face de-identification process changes not only the texture of a face but also the shape of the face. As a result, the shape of the new face might not fit within the original image background or the new shape may be too small to cover the area of the original face completely. This means a simple replacement would not generate satisfying results. One approach to this challenge could be warping the new face texture to the original face shape, where the shape of the original face would be recovered in the de-identified image and hence the face would fit perfectly with the original image background. However, the shape of a face contains rich personal identifiable information [17]. Bringing back the original face shape would significantly degrade the privacy protection performance of a face de-identification system. Therefore, the new shape of the de-identified face must be maintained after being blended with the original background.

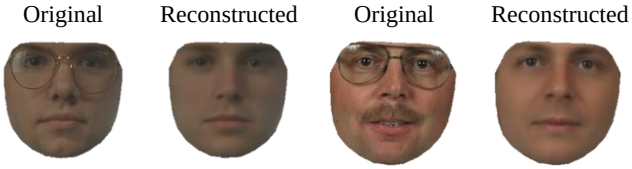
To maintain the new shape of the de-identified face region, a different approach has been taken in this work, where the background of the original face image is deformed to make just enough room to fit the new shape of the face region. The deformation of the background is achieved using Moving Least Squares [18] by solving the best affine transformation $l_v(x)$ that minimizes $\sum_i w_i |l_v(p_i) - q_i|^2$ where $\{p_i\}$ is a set of original points and $\{q_i\}$ is the target deformed positions of $\{p_i\}$. In our work, $\{p_i\}$ and $\{q_i\}$ each are the set of facial contour landmarks as defined in [19]. $\{p_i\}$ are the contour landmarks of the original face in the original image. $\{q_i\}$ are the aligned landmark positions of the de-identified face region. In this work, the de-identified face region is aligned to the original face region using inner corners of the eyes and tip of the nose.

The employment of background deformation has two contributions to a face de-identification system. The first contribution is a better visual quality of the de-identified face image. Fig. 1 shows the blending results of two de-identified faces without and with background deformation. As shown in the second image of Fig. 1 (c), unexpected white spots has appeared on the sides of the face as this de-identified face is wider than its original face. In Poisson blending, the new colours (or the new skin tone) of the de-identified face is calculated pixel by pixel based on the colours of the neighbourhood pixels in the destination image (i.e. the original face image in our case). When the de-identified face region is more narrow than its original face region (as in the first row of Fig. 1), for the pixels on either side of the de-identified face, their neighbourhood pixels from the destination (original) image are pixels within the original face region carrying the original skin tone. Therefore, after Poisson blending, the side of the de-identified face would be colour-matched to the skin tone of the original face and hence the rest of the body (e.g. the ears, the forehead and the neck). The same applies to the inner pixels of the de-identified face (e.g. the redness on the cheeks). In contrast, when a de-identified face is wider than its original face (as in the second row of Fig. 1), for the pixels on either side of the de-identified face, their neighbourhood pixels from the destination (original) image are pixels outside the original face region carrying colours from the original background. As the original face has a white background, without background deformation white spots has appeared on both sides of the de-identified face after Poisson blending (as shown in the second image of Fig. 1 (c)).



(a) (b) (c) (d)

Fig. 1. Blending results of de-identified face regions. (a) Original face images. (b) De-identified face region. (c) De-identified face image without background deformation. (d) De-identified face image with background deformation. Without background deformation, original face shape of (a) is restored in (c); while the shape of (b) is kept in (d) through background deformation.



(a) (b)

Fig. 2. Examples of reconstructed faces from face features

IV. Evaluation of Re-identification Risk

This section evaluates the re-identification risk of the de-identified face images generated by the *k*-Diff-furthest method.

A. Dataset

A subset of the FERET face dataset [20] containing 963 subjects has been used in the experiments. This subset was chosen from the available images of 994 subjects to ensure that each subject has two colour frontal face images ('fa' and 'fb'). All the 'fa' faces were used as the gallery in the re-identification tests to match against either the original version or the de-identified version of the 'fb' faces. Fig. 5 shows the original 'fa' (the first row), the original 'fb' (the second row) and the de-identified 'fb' (the last row) images for five subjects from the chosen FERET subset. As each pair of 'fa' and 'fb' images were taken at the same shooting session, they present a high degree of similarity and hence a challenge to our *k*-Diff-furthest face de-identification method.

B. Training of the AAM Face Representation Model

In this study, all the *k*-Diff-furthest de-identified faces were generated with the same AAM, which was trained on a subset of the FERET dataset. The AAM training set contains 1952 colour images of frontal faces taken from the FERET dataset and all of them are without glasses, beard or moustache. The exclusion of such features has enabled the automatic removal of such non-identity related features through AAM representation, as shown by the examples in Fig. 2. As a result, no faded (or averaged out) glasses frame, beard or moustache would appear on the resulting de-identified face images to degrade the visual quality of the image. In addition, it was observed that the most significant texture feature in our trained AAM describes merely the lighting condition of the images. To calibrate the lighting condition, the most significant texture feature is always set to its mean value (over the training set) for all the images represented in our face model.

C. Re-identification Tests

Before calculating face features with its face representation model, all face recognition systems isolate the face region from the background through cropping. Some systems crop the face region with a rectangular box while some systems define the face region with some facial landmarks (e.g. those on the eyebrows and the jawline as in our *k*-Diff-furthest method). In our re-identification tests, the face images were first aligned to the mean shape of the training set (approximately 200 × 200 pixels) and then cropped by a rectangular box co-centred with the mean shape. The size of the cropping box is either 200 × 200 or 300 × 300 pixels. The cropped images can be with or without a background. Fig. 3 shows the face images used in these re-identification tests for an example subject.

TABLE III presents the re-identification risk of the *k*-Diff-furthest method measured in naïve recognition attacks against four face recognition methods. All the recognition rates in TABLE III are averages over 10 runs and are presented in the format of accuracy ± standard deviation. TABLE III (a) shows that without merging with the original background the de-identified face regions generated by our *k*-diff-furthest method always present a near zero re-identification risk for all the benchmark face recognition methods tested.

TABLAE III (b) shows the re-identification risk increases when the de-identified face region is blended with its original background. This is mainly due to the fact that the Passion blending process has brought the skin-tone and illumination of the original face image back to the de-identified face image. Furthermore, the more the original background in a cropped face image, the higher the re-identification risk will be. The results are under 7% and still acceptable when the face images were cropped with a 200 × 200 square. However, the level of re-identification risk became unacceptably high when the face images were cropped with a 300 × 300 square, indicating that background areas around the face region may also contain personal identifiable information and de-identification must also be applied to these image areas to achieve complete privacy protection. Further experiments have been conducted to evaluate the re-identification risk presented by the background area alone. Results of these experiments are presented and discussed in the next sub-section.

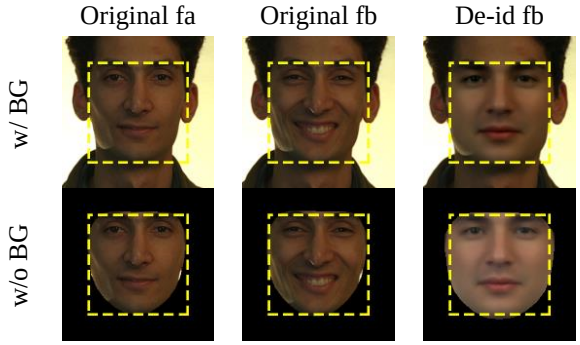


Fig. 3. Example of faces of one person with 200 pixels square (inside yellow boxes) and 300 pixels square cropping

TABLE IV shows the results of reverse recognition attacks, which are similar to those of naïve recognition attacks. All the de-identified face images yield a near zero re-identification risk when the background is excluded from the image but a much higher risk when the background is included.

D. Background Attack to Face De-identification System

As shown by TABLE III and TABLE IV the background area of an original face image presents personal identifiable information and can increase the re-identification risk when being blended with the de-identified face region. Here the background area may contain not only the background environment of the original image but also the hairstyle, the ear, the neck and the dressing style presented in the original image.

This experiment aimed to investigate the possibility of using merely the background area of the original face image to attack the face de-identification system. Fig. 4 shows some example images used in this experiment. Background attack is a generic attack to any face de-identification method that modifies the face region only. The idea and implementation of this attack is basic. All the face images were applied with an inverse crop based on their facial landmarks, so that only the image area outside the face region was kept. Inverse crop has been used in face recognition to compare the recognition performance between human and computer [21], [22]. After inverse crop, the images were cropped into the size of 300 × 300 for face recognition. The experimental results are shown in TABLE II Comparing with the results shown in TABLE III, it is clear that the background area of the original image was the main contributor to the increase in the re-identification risk.

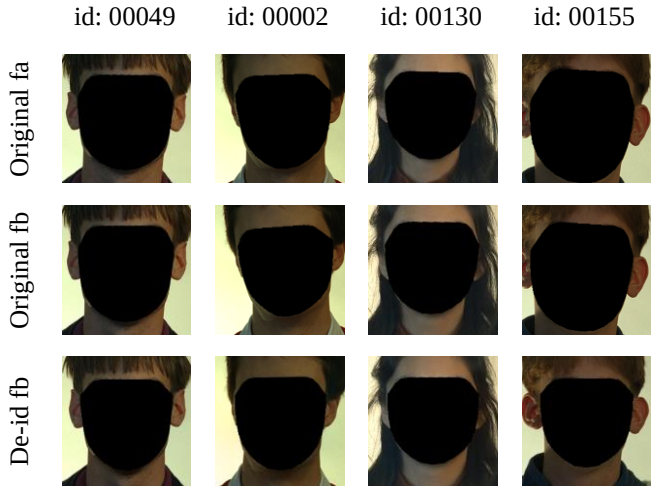


Fig. 4. Examples of inverse crop face images used in background attack experiment

TABLE II. RE-IDENTIFICATION RISK (%) OF INVERSE CROPPED FACE IMAGES

Method	*300 × 300 inverse crop*	
	Original	*De-id*
PCA	56.39	31.82 ± 0.89
LBP	**78.19**	**55.62 ± 0.68**
HOG	53.27	27.07 ± 1.09
LPQ	60.44	32.88 ± 1.06

V. CONCLUSIONS

The experiment results show that the *k*-Diff-furthest face de-identification method provides high privacy protection within the face region. However, blending the de-identified face to its original background increases the re-identification risk. Although a face recognition software focuses on the cropped face region, but information contained in the background area around the face region (e.g. hair colour, hairstyle, and dressing style) can also be used to identify a person. Our experiment of a background attack confirmed that face region is sufficient but not necessary for identifying a person. To protect privacy of the individuals captured in an image/video, de-identification must be applied to not only the face region but also all the image regions that contain personal identifiable information.

REFERENCES

[1] J. Liu, Y. Deng, T. Bai, Z. Wei, and C. Huang, "Targeting Ultimate Accuracy: Face Recognition via Deep Embedding," Jun. 2015.

[2] N. Zhang, M. Paluri, Y. Taigman, R. Fergus, and L. Bourdev, "Beyond Frontal Faces : Improving Person Recognition Using Multiple Cues," in Computer Vision and Pattern Recognition (CVPR), 2015.

[3] European Parliament, "Directive 95/46/EC," Off. J. Eur. Communities, vol. L281, p. 31, 1995.

[4] E. M. Newton, L. Sweeney, and B. Malin, "Preserving privacy by de-identifying face images," IEEE Trans. Knowl. Data Eng., vol. 17, no. 2, pp. 232–243, Feb. 2005.

[5] R. Gross, L. Sweeney, F. de la Torre, and S. Baker, "Model-Based Face De-Identification," in 2006 Conference on Computer Vision and Pattern Recognition Workshop (CVPRW'06), 2006, pp. 161–161.

[6] L. Meng and Z. Sun, "Face De-identification with perfect privacy protection," in 2014 37th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), 2014, pp. 1234–1239.

[7] Z. Sun, L. Meng, and A. Ariyaeeinia, "Distinguishable de-identified faces," in 2015 11th IEEE International Conference and Workshops on Automatic Face and Gesture Recognition (FG), 2015, vol. 04, pp. 1–6.

[8] J. Domingo-Ferrer and V. Torra, "Ordinal, Continuous and Heterogeneous k-Anonymity Through Microaggregation," Data Min. Knowl. Discov., vol. 11, no. 2, pp. 195–212, Sep. 2005.

[9] L. Meng, Z. Sun, A. Ariyaeeinia, and K. L. Bennett, "Retaining expressions on de-identified faces," in 2014 37th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), 2014, pp. 1252–1257.

[10] M. Turk and A. Pentland, "Eigenfaces for Recognition," J. Cogn. Neurosci., vol. 3, pp. 71–86, 1991.

[11] T. Ahonen, A. Hadid, and M. Pietikainen, "Face Description with Local Binary Patterns: Application to Face Recognition," IEEE Trans. Pattern Anal. Mach. Intell., vol. 28, no. 12, pp. 2037–2041, Dec. 2006.

[12] N. Dalal and B. Triggs, "Histograms of Oriented Gradients for Human Detection," in 2005 IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR'05), 2005, vol. 1, pp. 886–893.

[13] V. Ojansivu and J. Heikkilä, "Blur Insensitive Texture Classification Using Local Phase Quantization," in Image and Signal Processing, vol. 5099, A. Elmoataz, O. Lezoray, F. Nouboud, and D. Mammass, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2008, pp. 236–243.

[14] D. Bitouk, N. Kumar, S. Dhillon, P. Belhumeur, and S. K. Nayar, "Face swapping: automatically replacing faces in photographs," ACM Trans. Graph., vol. 27, no. 3, pp. 39:1–39:8, Aug. 2008.

[15] L. Impett, P. Robinson, and T. Baltrusaitis, "A facial affect mapping engine," in Proceedings of the companion publication of the 19th international conference on Intelligent User Interfaces - IUI Companion '14, 2014, pp. 33–36.

[16] P. Pérez, M. Gangnet, and A. Blake, "Poisson image editing," ACM Trans. Graph., vol. 22, no. 3, p. 313, Jul. 2003.

[17] M. Smiatacz, "Face Recognition: Shape versus Texture," in Advances in Intelligent Systems and Computing, vol. 313, R. S. Choraś, Ed. Cham: Springer International Publishing, 2015, pp. 211–218.

[18] S. Schaefer, T. McPhail, and J. Warren, "Image deformation using moving least squares," ACM Trans. Graph., vol. 25, no. 3, p. 533, Jul. 2006.

[19] C. Sagonas, G. Tzimiropoulos, S. Zafeiriou, and M. Pantic, "300 Faces in-the-Wild Challenge: The First Facial Landmark Localization Challenge," in 2013 IEEE International Conference on Computer Vision Workshops, 2013, pp. 397–403.

[20] P. J. Phillips, S. A. Rizvi, and P. J. Rauss, "The FERET evaluation methodology for face-recognition algorithms," IEEE Trans. Pattern Anal. Mach. Intell., vol. 22, no. 10, pp. 1090–1104, 2000.

[21] P. J. Phillips and A. J. O'Toole, "Comparison of human and computer performance across face recognition experiments," Image Vis. Comput., vol. 32, no. 1, pp. 74–85, Jan. 2014.

[22] N. Kumar, A. Berg, P. N. Belhumeur, and S. Nayar, "Describable Visual Attributes for Face Verification and Image Search.," IEEE Trans. Pattern Anal. Mach. Intell., vol. 33, no. 10, pp. 1962–77, Oct. 2011.

TABLE III. NAIVE RECOGNITION RATES (%) OF ORIGINAL 'FB' FACES AND DE-IDENTIFIED 'FB' FACES AGAINST ORIGINAL 'FA'

Method	*Without background*				*With background*			
	200 × 200		*300 × 300*		*200 × 200*		*300 × 300*	
	Original	*De-id*	*Original*	*De-id*	*Original*	*De-id*	*Original*	*De-id*
PCA	47.25	0.13 ± 0.16	42.37	0.07 ± 0.09	54.83	4.10 ± 0.58	61.27	39.13 ± 0.55
LBP	**74.25**	0.11 ± 0.10	**63.03**	0.13 ± 0.11	**83.39**	1.30 ± 0.24	**87.23**	55.12 ± 0.56
HOG	47.14	0.21 ± 0.14	18.38	0.17 ± 0.20	74.87	**6.09 ± 0.48**	78.09	56.93 ± 0.70
LPQ	53.27	**0.25 ± 0.18**	47.04	**0.25 ± 0.11**	80.48	4.42 ± 0.61	82.66	**59.14 ± 0.81**
	(a)				(b)			

TABLE IV. REVERSE RECOGNITION RATES (%) OF ORIGINAL 'FB' FACES AND DE-IDENTIFIED 'FB' FACES AGAINST ORIGINAL 'FA'

Method	*Without background*				*With background*			
	200 × 200		*300 × 300*		*200 × 200*		*300 × 300*	
	Original	*De-id*	*Original*	*De-id*	*Original*	*De-id*	*Original*	*De-id*
PCA	45.38	**0.33 ± 0.19**	41.53	**0.30 ± 0.21**	53.48	**9.41 ± 0.53**	61.37	49.06 ± 0.61
LBP	**72.59**	0.23 ± 0.14	**63.14**	0.21 ± 0.11	**80.48**	1.59 ± 0.41	**86.60**	59.28 ± 1.63
HOG	46.52	0.24 ± 0.16	17.03	0.07 ± 0.09	74.77	5.92 ± 0.70	76.95	**59.81 ± 0.68**
LPQ	50.88	0.23 ± 0.15	46.31	0.20 ± 0.14	80.06	4.35 ± 0.58	82.87	58.36 ± 0.48
	(a)				(b)			

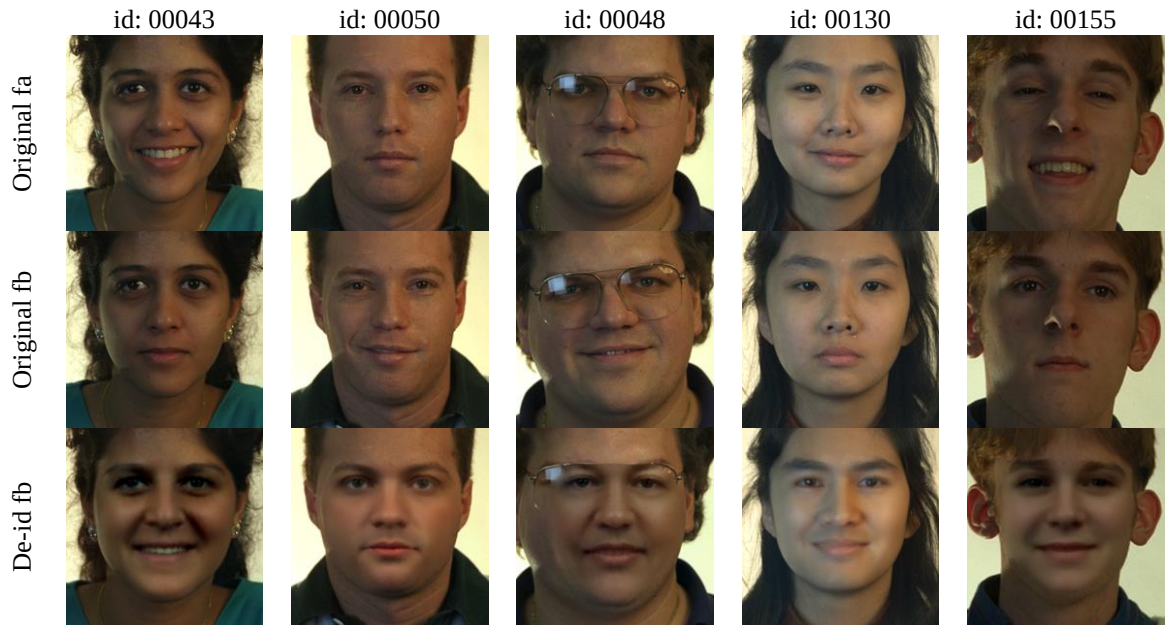


Fig. 5. Examples of the FERET face images used in the re-identification tests