Protecting the Privacy of Face by De-Identification Pipeline Based on Deep Learning

Anubha Parashar

Department of Computer Science and Engineering, Manipal University Jaipur, India

anubhaparashar1025@gmail.com

September 21, 2022

Overview

Introduction

- This paper proposes a reversible face de-identification pipeline that modifies face geometry and texture.
- Fourteen parameters for geometrical modification are used. For texture modification fixed face texture template is used.
- We have investigated the impact of various geometrical and surface alterations of face components like eyes, eyebrows, nose, and lips on the ability of humans and machines to recognize faces.
- The crowdsourcing and machine face recognition experiments were performed on images of famous people collected from the Internet.
- The obtained results in both types of experiments showed that face texture has a stronger impact on a level of privacy protection than face geometry (shape) modifications.

Contributions

1. Reversible face de-identification pipeline that combines the good properties of naive and complex de-identification methods;
2. Results of five psychological experiments that evaluate the impact of face texture and/or face geometry modifications to level of privacy protection;
3. Results of five experiments performed by automatic face recognition of de-identified faces,
4. Comparison of obtained results for both human and automatic face recognition.

Related works

1. In early systems original faces were replaced by an average of the face images of the K identities that were closest to the subject from a set of facial photographs that had been previously closed.
2. In [1], the variety of the de-IDed faces in order to prevent the generation of faces that are all same in appearance.
3. Deep neural networks have been utilised in recent years for the purpose of face de-identification. Deep neural networks are used to determine the K identities that are most similar to the subject.
4. GANs are used in the research presented in [2] to construct de-ID faces. Karla et al work's in [3] extends this methodology to full body synthesis. The GAN generated de-IDed faces, on the other hand, suffer from artefacts such as a discrepancy in skin colour between the de-IDed face and the surrounding area.

Methodology – Face de-identification pipeline

1. The proposed face de-identification pipeline has four stages: face detection, facial feature points localization, face region decomposition, and face de-identification with modification of face geometry and texture.
2. At the first stage (Face detection) we use of-the-shelf NPD face detector [4].
   It uses normalized pixel difference features (that are scale invariant, bounded, and able to reconstruct the original image) and deep quadratic trees to learn the optimal subset of features and their combinations, so manifolds
3. Facial feature points are localized by the fast method proposed in [5] at the second stage. It uses an ensemble of regression trees to estimate 68 facial landmark positions from a sparse subset of pixel intensities.

Experiment setup and results

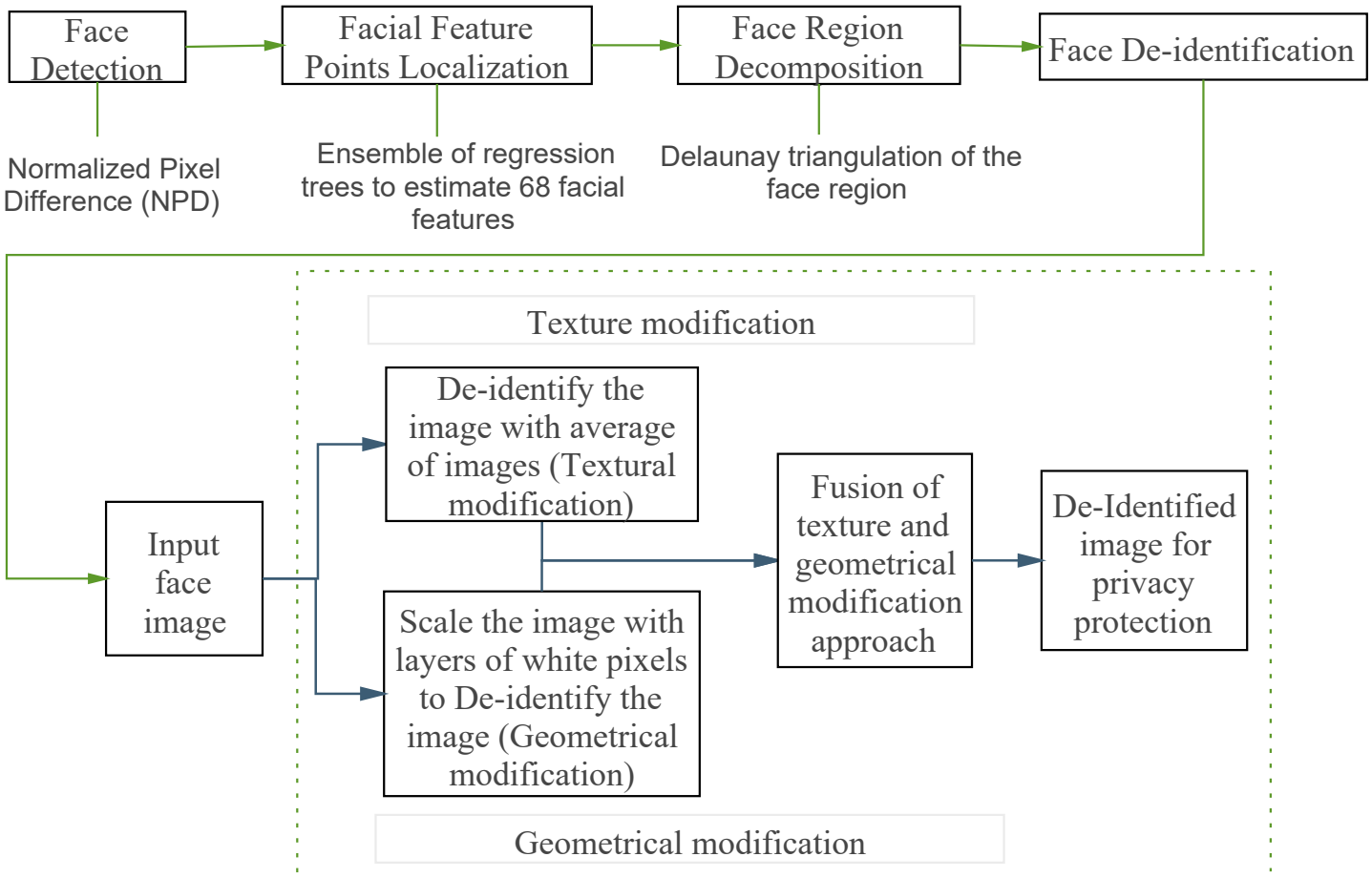

Figure: Methodology adopted

Methodology – Face de-identification pipeline

3. At the third stage the locations of the face feature points localized at the second stage are used to generate constrained Delaunay triangulation [6] that groups certain required segments into the triangulation.
4. The input in the fourth stage is constrained Delaunay triangulation of the face region. The following face components are subject to modification eyes, eyebrows, nose, and lips.

Face component modification parameters

1. For each face component a set of modifications is defined taking in consideration morphological characteristics of a human face is very difficult task to define what face components characteristics constitute the core concept that define face identity Face identity is subjective by nature for humans.
2. Only certain combinations of face components modifications can be performed, if we want to preserve naturalness of de-identified faces.
3. To preserve naturalness of a face, the very first step is to determine following global morphological characteristics of a face distance between eyes, head width and height, and nose tip position.

Face component modification parameters

1. Based on these global morphological characteristics, we introduced a range of allowable face modification parameters expressed in the interval from -1 to 1, of each face modification parameter is (pseudo) randomly where 0 defines original visual appearance, and -1 and 1 maximum allowed change in opposite directions. The value selected from the interval [-1,1].
2. For example, eye size modification parameter value from the interval [-1,1], is linearly mapped into the value $modified\_eye\_size$ from the eye size interval $[minsye\_size, max\_eye\_size]$ which is calculated as follows

$$[min/max_{(}eyesize)] = [\frac{eyes\_dist.}{K1} + \frac{head\_width}{K2}] \quad (1)$$

Face component modification parameters

1. A heuristic formula for defining range of allowed modification is determined for each face component modification parameter.
2. These formulas are determined based on face component characteristics obtained from distributions of their values in a database of near profile faces. The face component modifications with corresponding parameters are listed in Tab. 1.
   The symbols in Tab. 1 have the following meaning: $s_i^{x/y}$ - scale, $t_i^{x/y}$ - translation and α_i - rotation, and index i corresponds to the face component, while super index x or y denotes axis directions. For example, for an eye the typical values are $s_i^{x/y}$ $[0.85, 1.15]$, $t_i^{x/y}$ $[-15, 15]$ pixels, and $\alpha \in [-0.10, 0.15]$ radians.

Face component modification parameters

Table: Face component modifications

	Face components			
Modifications	**Eyes**	**Eyebrows**	**Nose**	**Lips**
Size horizontal	s_1^x	–	s_3^x	s_4^x
Size vertical	s_1^y	–	s_3^y	s_4^y
Position horizontal	t_1^x	t_2^x	–	–
Position vertical	t_1^y	t_2^y	t_3^y	t_4^y
Rotation	α_1	α_2	–	–

Face de-identification - affine transformations of face components

The affine transformation is then used on all Delaunay triangles belonging to corresponding face component. Note that the parameters of affine modification used for left and right eye, as well as for both eyebrows must preserve symmetrical appearance of a face. The following steps are performed in the process of transforming face components:

STEP 1: For each face component select a corresponding set of face feature points $FFP_i = \{(x_j, y_j)\}_i$, where $i \in (1, ..., 6)$ is index of a face component, and $j \in (1, ..., 68)$ is an index of face feature points, $\{\quad\}_i$ denotes a set of face feature points that belong to a face component i. Determine a center of face feature points for a face component i, denoted as (x_i^c, y_i^c). The (x_i^c, y_i^c) is used to define the displacement of the face component center from an image origin.

STEP 2: Use all face modification parameters that correspond to face component i to determine parameters of the affine transformation: scale s_i^x and s_i^y, rotation α_i, and translations t_i^x and t_i^y.
STEP 3: Transform original vertices $\{FFP_i = (x_j, y_j)\}_i$, that overly face component i, by using affine transformation into new vertices of de-identified face component $FFP_i^* = \{(x_j^*, y_j^*)\}_i$.

$$\begin{bmatrix} x_j^* \\ y_j^* \\ 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & t_i^x \\ 0 & 1 & t_i^y \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} cos(\alpha_i) & sin(\alpha_i) & 0 \\ -sin(\alpha_i) & cos(\alpha_i) & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} s_i^x & 0 & 0 \\ 0 & s_i^y & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} x_j - x_i^c \\ y_j - y_i^c \\ 1 \end{bmatrix}$$

STEP 4: Backward mapping is performed as follows. For all face component pixels' coordinates $FCP_i^* = \{(x_l^*, y_l^*)\}_i$ that are inside the triangles defined with vertices $FFP_i^* = \{(x_j^*, y_j^*)\}_i$, use the inverse transformation for mapping pixels' coordinates $FCP_i^* = \{(x_l^*, y_l^*)\}_i$ into corresponding pixels' coordinates $FCP_i = \{(x_k, y_k)\}_i$ defined over the original face component image.

$$\begin{bmatrix} x_k^* \\ y_k^* \\ 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & x_i^c \\ 0 & 1 & t_i^c \\ 0 & 0 & 1 \end{bmatrix} \left(\begin{bmatrix} 1 & 0 & t_i^x \\ 0 & 1 & t_i^y \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} cos(\alpha_i) & sin(\alpha_i) & 0 \\ -sin(\alpha_i) & cos(\alpha_i) & 0 \\ 0 & 0 & 1 \end{bmatrix} \right.$$

$$\left. \begin{bmatrix} s_i^x & 0 & 0 \\ 0 & s_i^y & 0 \\ 0 & 0 & 1 \end{bmatrix} \right)^{-1} \begin{bmatrix} x_l^* \\ y_l^* \\ 1 \end{bmatrix}$$

STEP 5: Use spline interpolation to estimate RGB pixel values on transformed face component image on coordinates FCP_i^* $=\{(x_l^*, y_l^*)\}_i$ from RGB pixel values in the original face component image. Spline interpolation is necessary for pixel value mapping because pixel coordinates $FCP_i^* =\{(x_k, y_k)\}_i$ are real numbers while $FCP_i^* = \{(x_l^*, y_l^*)\}_i$ are all integer numbers.
Applying the above-described Steps 1-6 for all face components i $=1, 2, ..., 6$, a modified face is obtained, counted as a de-identified face.
The proposed face de-identification process is reversible. By applying a sequence of inverse transformations and using backward mapping and spline interpolation, the original appearance of the face can be restored.

Experiment setup and results

1. We compiled a set of 30 face images of famous people (7 females and 23 males with ages ranging from 30 to 75) from politics, sports, business and entertainment.
2. The evaluation is performed by means of crowdsourcing performed by 150 test subjects (20 females and 130 males). The test subjects were informed that faces in the tests are de-identified faces of famous people.
3. The background (ie context) and biometrical ques like hair and ears, that a user can use for face identification are removed in all tests. For example, some of them are shown in (Fig. 2. fifth row). We have performed five experiments.

Experiment setup and results

Figure: Examples of six faces used in experiment 1-5 are depicted consecutively in row 1-5. Each row corresponds to one experiment and each column to one face

Experiment setup and results

First experiment: The geometry of a face is left unchanged and texture of a face is replaced with the average texture obtained from 30 faces. All de-identified faces thus have the same texture and the original geometry (Fig. 2. first row). From the total of 4500 de-identified faces (30 faces x 150 test subjects) for only 60 de-identified faces original identity was revealed (ie. 1.33 % fail rate of de-identification).

Second experiment: The geometry of a face is changed as described in Section 3. A texture of a face is obtained by blending 50 % of an original texture and 50% of an average face texture (Fig. 2. second row). The following results are obtained: From the total of 4500 de-identified faces for 260 de-identified faces original identity was revealed (i.e. 5.78 % fail rate of de-identification),

Third experiment: The geometry of a face is changed as described in the Section 3. An original face texture was left unchanged (Fig. 2. third row).

Experiment setup and results

The following results are obtained: From the total of 4500 de-identified faces, original identities of 1410 de identified faces were revealed (i.e. 31.33 % fail rate of de-identification).

Fourth experiment: The geometry of a face is changed to an average geometry obtained from 30 faces (i.e. average positions of 68 face feature points), while texture is left unchanged (Fig. 2. fourth row). The following results are obtained: From the total of 4500 de-identified faces, original identities of 1980 de-identified faces were revealed (i.e. 44.00 % fail rate of de-identification)

Fifth experiment: Original images of famous person are used (Fig. 2. fifth row). The following results are obtained: From the total of 4500 de-identified faces, total of 3020 true identities were known (ie 67.11 %).

The results of above first four experiments have shown that texture is even more important than face shape (face trigonometry).

Comparision with state-of-art

Identical test samples from 1-5 experiments are used to evaluate a level of privacy protection with [11] [12] [13] [14] [15].
When machine recognition approach is used for various datasets. We are comparing results obtained by machine. Tab. 2. depict results. From the results we can conclude that our method outperforms than the existing recognition of de identified faces (i.e., with altered visual appearances).

Table: Failed rate of de-identification (recognition rate) for machine

Comparision	**Machine/ Resnet**
[11]	0.8204
[12]	0.758
[13]	0.654
[14]	0.79
[15]	0.1173
Proposed model	**0.0667**

Conclusion

1. Proposed a hybrid reversible face de-identification pipeline that combines the good qualities of naive and complex face-de identification methods.
2. The texture of a face can be adaptively modified based on an original texture as in naive approaches. Geometrical modifications performed by affine transformation are pseudo reversible makes them compliant with security requirements.
3. Only fourteen parameters for geometrical modification are used, what makes them suitable for steganographic encoding into the de identified image. For texture modification fixed texture template is used.
4. The crowdsourcing and machine face recognition experiments have shown that modification of a face texture has stronger impact on a level of privacy protection then face geometry (shape) modifications and that the machine is superior to humans in the task of recognition of de-identified faces.

References

[1] Jain, Anil K., and Stan Z. Li. Handbook of face recognition. Vol. 1. New York: springer, 2011.

[2] Ribaric, Slobodan, and others. "De-identification for privacy protection in multimedia content: A survey." Signal Processing: Image Communication 47 (2016): 131-151.

[3] Chen, Renwang, and others. "Simswap: An efficient framework for high fidelity face swapping." In Proceedings of the 28th ACM International Conference on Multimedia, 2020.

[4] Liao, Shengcai, Anil K. Jain, and Stan Z. Li. "A fast and accurate unconstrained face detector." IEEE transactions on pattern analysis and machine intelligence 38, no. 2 (2015).

[5] Kazemi, and others. "One millisecond face alignment with an ensemble of regression trees." In Proceedings of the IEEE conference on computer vision and pattern recognition, 2014.

[6] Paul Chew, L. "Constrained delaunay triangulations." Algorithmica 4, no. 1 (1989): 97-108.

[7] He, Kaiming, and others. "Deep residual learning for image recognition." In Proceedings of the IEEE conference on computer vision and pattern recognition, pp. 770-778. 2016.

[8] Sinha, Pawan, and others. "Face recognition by humans: Nineteen results all computer vision researchers should know about." Proceedings of the IEEE 2006.

[9] King, Davis. "Dlib-ml: A machine learning toolkit." The Journal of ML Research 2009.

[10] Jiwen Lu, and others. Neighborhood Repulsed Metric Learning for Kinship Verification. IEEE Transactions on Pattern Analysis and Machine Intelligence (PAMI), 2014.

[11] Li, Tao, and Lei Lin. "Anonymousnet: Natural face de-identification with measurable privacy." Proceedings of the IEEE/CVF CVPR 2019.

[12] Wu, Y., Yang, F., Xu, Y. et al. Privacy-Protective-GAN for Privacy Preserving Face De-Identification. J. Comput. Sci. Technol. 34, 47-60 (2019).

[13] Zhu, Bingquan, et al. "Deepfakes for medical video de-identification: Privacy protection and diagnostic information preservation." Proceedings of the AAAI/ACM Conference on AI, 2020.

[14] Li, Yuezun, and Siwei Lyu. "De-identification without losing faces." Proceedings of the ACM Workshop on Information Hiding and Multimedia Security. 2019.

[15] Du, Liang, et al. "GARP-face: Balancing privacy protection and utility preservation in face de-identification." IEEE international joint conference on biometrics. IEEE, 2014.

[16] Ralph Gross, Edoardo Airoldi, Bradley Malin, and Latanya Sweeney. 2005. Integrating utility into face de-identification. In International Workshop on Privacy Enhancing Technologies.

[17] Ralph Gross, Latanya Sweeney, Fernando De La Torre, and Simon Baker. 2008. Semi-supervised learning of multi-factor models for face de-identification. In CVPR.

The End