Distinguishable De-identified Faces

Zongji Sun, Dr Lily Meng and Prof Aladdin Ariyaeininia,
School of Engineering and Technology,
University of Hertfordshire, Hatfield, UK, AL10 9AB
Outline

• Previous work of face de-identification
• $k$-Same family of face de-identification methods
• Motivation of this work
• Overview of the proposed method
• Experimental results
• Conclusions
Previous (related) work

• Ad hoc methods: blurring, pixelation, censor bars

• These ad hoc methods cannot protect their de-identified faces from face recognition software.
The $k$-Same family of face de-id methods

Face features in a simplified 2D illustration
The $k$-Same family of face de-id methods

Face features in a simplified 2D illustration
The $k$-Same family of face de-id methods

Face features in a simplified 2D illustration
The $k$-Same family of face de-id methods

Face features in a simplified 2D illustration
The $k$-Same family of face de-id methods

Face features in a simplified 2D illustration
The $k$-Same family of face de-id methods

Face features in a simplified 2D illustration
The $k$-Same family of face de-id methods

Face features in a simplified 2D illustration
The *k*-Same family of face de-id methods

- The first member: *k*-Same-Eigen, 2005 [4]

<table>
<thead>
<tr>
<th>Limitations</th>
<th>Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preservation of data utility</td>
<td><em>k</em>-Same-Select, 2005 [5]</td>
</tr>
<tr>
<td>Ghost artefacts</td>
<td><em>k</em>-Same-M, 2006 [6]</td>
</tr>
<tr>
<td>Limited privacy protection</td>
<td><em>k</em>-Same-furthest, 2014 [7]</td>
</tr>
</tbody>
</table>

Original

\[
k = 5
\]

\[
k = 2 \quad k = 4 \quad k = 8 \quad k = 10
\]

[5]  
[6]
Our previous work – $k$-Same-furthest

De-identification Level $k$

Rank 1 Accuracy

- $1/k$
- $k$-Same-M by AAM
- $k$-Same-M by PCA
- $k$-Same-furthest by AAM
- $k$-Same-furthest by PCA
A problem of $k$-Same faces in real-life applications

- People share the same de-identified face
A problem of $k$-Same faces in real-life applications

• People share the same de-identified face

Hi, I’m Jack
A problem of $k$-Same faces in real-life applications

- People share the same de-identified face

Hi, I’m Jack

Hi, I’m Oliver
A problem of $k$-Same faces in real-life applications

- People share the same de-identified face

Hi, I’m Jack

Hi, I’m Oliver

Hi, I’m Harry
A problem of $k$-Same faces in real-life applications

- People share the same de-identified face
A problem of $k$-Same faces in real-life applications

- People share the same de-identified face

Guess who we are?
A problem of \( k \)-Same faces in real-life applications

- People share the same de-identified face

- Impossible to track/distinguish individuals in a de-identified video.
Our $k$-Diff-furthest method

Face features in a simplified 2D illustration
Our $k$-Diff-furthest method

Face features in a simplified 2D illustration
Our $k$-Diff-furthest method

Face features in a simplified 2D illustration
Our $k$-Diff-furthest method

Face features in a simplified 2D illustration
Our $k$-Diff-furthest method

Face features in a simplified 2D illustration
Our $k$-Diff-furthest method

Face features in a simplified 2D illustration
Our $k$-Diff-furthest method

Face features in a simplified 2D illustration
*k*-Diff-furthest de-identified faces

- Original faces
- De-identified faces
Protection of original identities

Processing of $k$-Diff-furthest illustrated with a simplified example in 2D space
Recognition rates for de-identified faces against their original faces

![Graph showing recognition rates against de-identification level and k. The graph displays different accuracy rates for different de-identification levels and values of k.](image-url)
Diversity of face datasets

- Histogram of feature distances of original faces and various sets of de-identified faces when $k=5$
- Distribution of $k$-Diff-furthest de-identified face set have the similar outline with the original face data set
Experimental results by $k$-Diff-furthest

Original faces

De-identified faces ($k=5$)
Experimental results by $k$-Diff-furthest

Original faces

De-identified faces ($k=5$)
Conclusions

• Main contribution: distinguishable de-identified faces.

• Diversity of the original face set is maintained in the de-identified face set.

• Perfect privacy protection performance is achieved.
References

[1] Blurring example image [available on: http://cnet2.cbsistatic.com/hub/i/r/2008/05/13/e0ceb6e1-f8fb-11e2-8c7c-d4ae52e62bcc/thumbnail/770x433/a4637468a88162ae78615867cbd89d48/face_blurring_street_view_5.13.2008.png]


References


Thank you
Questions?