Fingerprinting Relational Data


**Agenda**

- Background on fingerprinting relational data sets
  - Motivation
  - Requirements & workflow
- Current research directions
  - Fingerprinting categorical data
  - Evaluating fingerprinting schemes
- Challenges and future research
Fingerprinting Relational Data

Background
Fingerprinting - motivation

• Why protecting the shared data?
  o Data owner used a lot of resources to collect/create the data (money, human experts, time...)
  o Sensitive data (e.g. medical data)
    – Privacy implications: only the trusted parties get the data and should not share it further

- Anonymising data? Reduces utility!
✓ Controlled data sharing → the goal
  o Share full data
  o Trace the unauthorised data re-distribution

SBA Research, 2021
Controlled data sharing via fingerprinting

- Embedding owner’s signature and recipient’s identification into the data

<table>
<thead>
<tr>
<th>Age</th>
<th>Blood Pressure</th>
<th>Diabetes</th>
</tr>
</thead>
<tbody>
<tr>
<td>32</td>
<td>64</td>
<td>1</td>
</tr>
<tr>
<td>31</td>
<td>66</td>
<td>0</td>
</tr>
<tr>
<td>50</td>
<td>72</td>
<td>1</td>
</tr>
<tr>
<td>48</td>
<td>70</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Age</th>
<th>Blood Pressure</th>
<th>Diabetes</th>
</tr>
</thead>
<tbody>
<tr>
<td>33</td>
<td>64</td>
<td>1</td>
</tr>
<tr>
<td>31</td>
<td>68</td>
<td>0</td>
</tr>
<tr>
<td>50</td>
<td>72</td>
<td>1</td>
</tr>
<tr>
<td>47</td>
<td>70</td>
<td>0</td>
</tr>
</tbody>
</table>
**Fingerprinting: requirements & workflow**

**Requirements:**

1. Recognisable by the owner
2. Not detectable and consequently removable by the recipients
3. Robust to the attacks
4. Does not change the utility of the data too much
Current research directions

Fingerprinting categorical data &
Evaluation of fingerprinting schemes
Challenge: categorical data

- *Minor* alterations in categorical data?

<table>
<thead>
<tr>
<th>age</th>
<th>sex</th>
<th>employed</th>
<th>Alzheimers stage</th>
</tr>
</thead>
<tbody>
<tr>
<td>59</td>
<td>Male</td>
<td>No</td>
<td>late</td>
</tr>
<tr>
<td>67</td>
<td>Male</td>
<td>No</td>
<td>late</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
</tbody>
</table>

- kNN-based fingerprinting: "*modify the value to something that is likely to occur in the original dataset*" [1]

Quality estimation

• Robustness against attacks
  o Attacker model: *white-box naive attacker*
  o Attacks: horizontal & vertical subset attack, flipping attack, ...

• Utility of fingerprinted data
  o Statistical properties (mean, var, distribution, ...)
  o **ML performance (accuracy, ...) [2]**

Quality estimation

- Robustness against attacks → **maximise** modifications
- Preserve data utility → **minimise** modifications
Quality estimation

- **Data properties** affect the robustness and utility of fingerprinted data, e.g. data size, type of attributes, entropy, etc.

Table Experimental results of horizontal subset attack success ($f_m$) on the Forest Cover Type dataset (left; size: 581012 x 54) and Adult (right; size: 48842 x 14), where $p'$ denotes the strength of the attack.

<table>
<thead>
<tr>
<th>%_marks</th>
<th>$p' = 80%$</th>
<th>$p' = 95%$</th>
<th>$p' = 99%$</th>
</tr>
</thead>
<tbody>
<tr>
<td>17%</td>
<td>0</td>
<td>0</td>
<td>0.01</td>
</tr>
<tr>
<td>4%</td>
<td>0</td>
<td>0</td>
<td>1.0</td>
</tr>
<tr>
<td>2%</td>
<td>0</td>
<td>0.19</td>
<td>1.0</td>
</tr>
<tr>
<td>1%</td>
<td>0</td>
<td>0.99</td>
<td>1.0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$p' = 80%$</th>
<th>$p' = 95%$</th>
<th>$p' = 99%$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.20</td>
<td>0.95</td>
<td>1.0</td>
</tr>
<tr>
<td>0.99</td>
<td>1.0</td>
<td>1.0</td>
</tr>
<tr>
<td>1.0</td>
<td>1.0</td>
<td>1.0</td>
</tr>
<tr>
<td>1.0</td>
<td>1.0</td>
<td>1.0</td>
</tr>
</tbody>
</table>

Summary & Future Challenges
Summary

• Fingerprinting wider range of attribute types – categorical data

• Effects of fingerprinting parameters on robustness and data utility

• Novel utility measurement – effects on a machine learning task
Future challenges

1. Designing tools for fingerprinting relational data in practice
   o Unifying fingerprinting scheme for relational data sets
   o Open-source implementation
   o OSSDIP – controlled data visiting infrastructure for sensitive data

2. Aiding the fingerprint parameter choice for the data holder
   o Bigger-scale analysis to capture pattern and trends in robustness and data utility depending on fingerprinting parameters
   o Analysis of effects of data properties on the quality of fingerprint
   o Parameter choice guidelines tailored for a data set and its intended usage scenario; (semi-)automated process
Tanja Šarčević
SBA Research
Floragasse 7, 1040 Vienna
tsarcevic@sba-research.org
