Privacy Protection for Social Media based on a Hierarchical Secret Image Sharing Scheme

September 23, 2019
ICIP 2019 – Taipei (Taiwan)

Sébastien BEUGNON\textsuperscript{1,2},
Pauline PUTEAUX\textsuperscript{1}
William PUECH\textsuperscript{1}

\textsuperscript{1}LIRMM, Univ. Montpellier, CNRS, France
\textsuperscript{2}STRATEGIES, Rungis, France
Multimedia content privacy issues

Social media
- 3.2 billion active users, i.e. 42% of global population
- 1,200 billion images taken per year
- 500 million images shared on Instagram and Facebook per day
Multiparty privacy conflict

Mainstream social media solutions

- Tagging/Untagging
- Report inappropriate content
- Ask the owner to remove content

Proposed solution

- Preserve privacy of users
- Negotiate collectively

Secret Sharing

For example, $k = 3$
Secret Sharing

For example, $k = 3$
Secret Sharing

- For example, $k = 3$
Secret Sharing

For example, $k = 3$
Secret Sharing

- For example, $k = 3$
Secret Sharing

\((k, n)\)-threshold scheme
(Shamir, 1979)

Based on polynomial interpolation:
\[ f(x) = \sum_{i=0}^{k-1} a_i \times x^i \]

- Finite field \( \mathbb{F}_p \) where \( p \) is prime
- \( a_0 = S \) with \( S \in \mathbb{F}_p \)
- Share \( s_j = (x_j, f(x_j)) \) where \( j \in \{1, \ldots, n\} \) and \( x_j \in \mathbb{F}_p^* \)

Secret Sharing applied on images

Secret Image Sharing (Thien and Lin, 2004)

- Sharing pixel values
- Shares are images


Outline

Multiparty privacy conflict issues in social media

Hierarchical secret image sharing scheme for privacy protection

Experimental results

Conclusion and future work
Sharing method overview

$k$-order polynomial generation

- Generation of a random sequence $a_0, a_1, \ldots, a_{k-1}$
- $a_k$ set to $s$
- $k$-order polynomial: $f(x) = \sum_{i=0}^{k} a_i \times x^i$
Sharing method

3 scenarios for sharing \(s\) values from \(R_j\)

- For the public share \(S_0\)
  - Threshold 2
  - 1-order polynomial
  - \(f^{(k+1-2)}(x_0) = f^{(k-1)}(x_0)\)

- For the user \(x_j\)
  - Threshold 2
  - 1-order polynomial
  - \(f^{(k+1-2)}(x_j) = f^{(k-1)}(x_j)\)

- For the user \(x_l\) (\(l \neq j\) and \(l \neq 0\))
  - Threshold \(k + 1\)
  - \(k\)-order polynomial
  - \(f^{(k+1-(k+1))}(x_l) = f(x_l)\)
Reconstruction method overview

- Public share $S_0$
- Users' shares $\{S_i\}$
- Trust level $k$

Diagram:

- $k'$ among $\frac{n}{k}$
- $k' \geq k$
- $k'$ Level 2 ROI reconstruction
- Level $(k + 1)$ ROI reconstruction
- Full reconstruction
- $k'$ ROI reconstructed image
- Original image $I$
Outline

Multiparty privacy conflict issues in social media

Hierarchical secret image sharing scheme for privacy protection

Experimental results

Conclusion and future work
Experimental results

Experimental setup

- Detection: social media tagging
- Parameters $k = 5$, $n = 8$ Majority consensus
Experimental results

Experimental setup

- Detection: social media tagging
- Parameters $k = 5$, $n = 8$ Majority consensus
- Public share $S_0$
Experimental results

Using the share $S_2$ of user $x_2$ and the public share $S_0$

Using the share $S_4$ of user $x_4$ and the public share $S_0$
Experimental results

► With user group \( \{x_1, x_2, x_4\} \) and the public share \( S_0 \) \((< k = 5)\)

► With user group \( \{x_1, x_3, x_5, x_7, x_8\} \) and the public share \( S_0 \) \((\geq k = 5)\)
Experimental results

Statistical analysis of shares

- High entropy (around 7.997 bits per pixel per channel)
- Low spatial correlation (around 0.0012)
Outline

Multiparty privacy conflict issues in social media

Hierarchical secret image sharing scheme for privacy protection

Experimental results

Conclusion and future work
Conclusion

▶ A new application case for Secret Image Sharing
▶ A new solution to resolve Multiparty Privacy Conflicts
Future work

Rendering improvement

- Pixel masking
- Face edges instead of a bounding box

Future work

Hierarchical Secret Image Sharing for multigroups

- Use advanced privacy configuration
- Hierarchy among users
- Visible only for friends, acquaintances, others
Thank you for your attention!

September 23, 2019
ICIP 2019 – Taipei (Taiwan)

Sébastien BEUGNON\textsuperscript{1,2}
Pauline PUTEAUX\textsuperscript{1}
William PUECH\textsuperscript{1}

\{firstname.name\}@lirmm.fr

\textsuperscript{1}LIRMM, Univ. Montpellier, CNRS, France
\textsuperscript{2}STRATEGIES, Rungis, France