APDM2017 (IJCAI2017 workshop36)

Privacy Preserving Face Retrieval in the Cloud for Mobile Users

Xin Jin[1], Chenggen Song[1], Shiming Ge[2,*]

[1]Beijing Electronic Science and Technology Institute
GOCPCCC Key Laboratory of Information Security
[2]Institute of Information Engineering, Chinese Academy of Sciences
*Corresponding author: geshiming@iie.ac.cn

http://kislab.besti.edu.cn/victory/

Homepage

北京電子科技学院 Beijing Electronic Science and Technology Institute

VICTORY besti

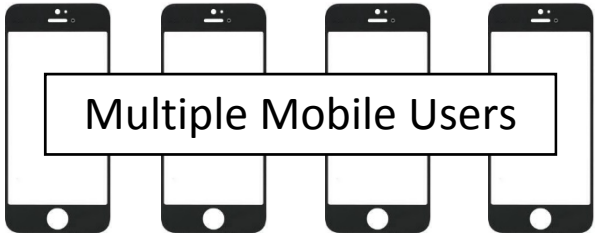
中国科学院信息工程研究所 INSTITUTE OF INFORMATION ENGINEERING,CAS

Official WeChat
官方微信

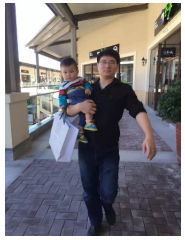
Outline

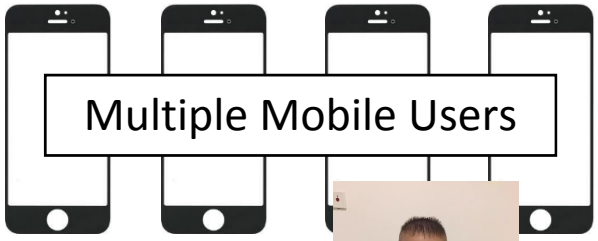
1. **Motivation**
2. **Related Work**
3. **Privacy Preserving Face Retrieval**
4. **Experimental Results**
5. **Conclusion and Discussion**

Motivation

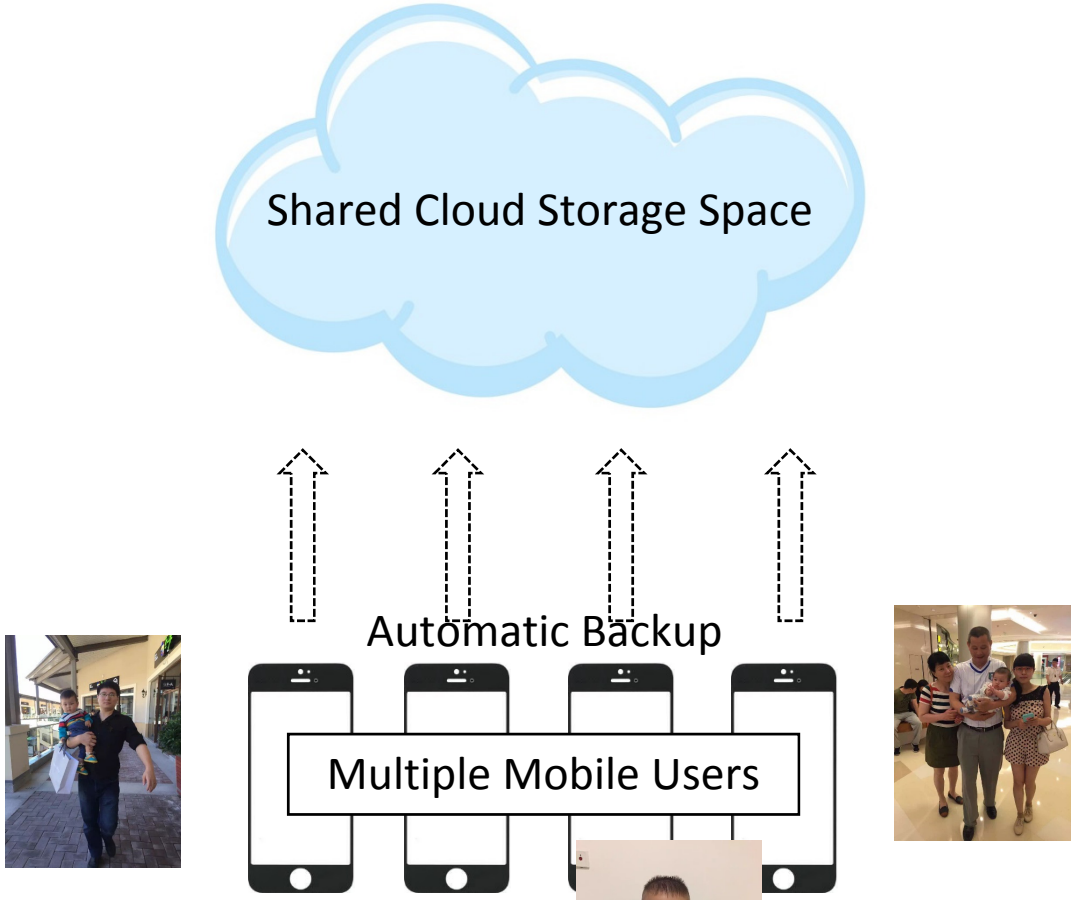


Motivation

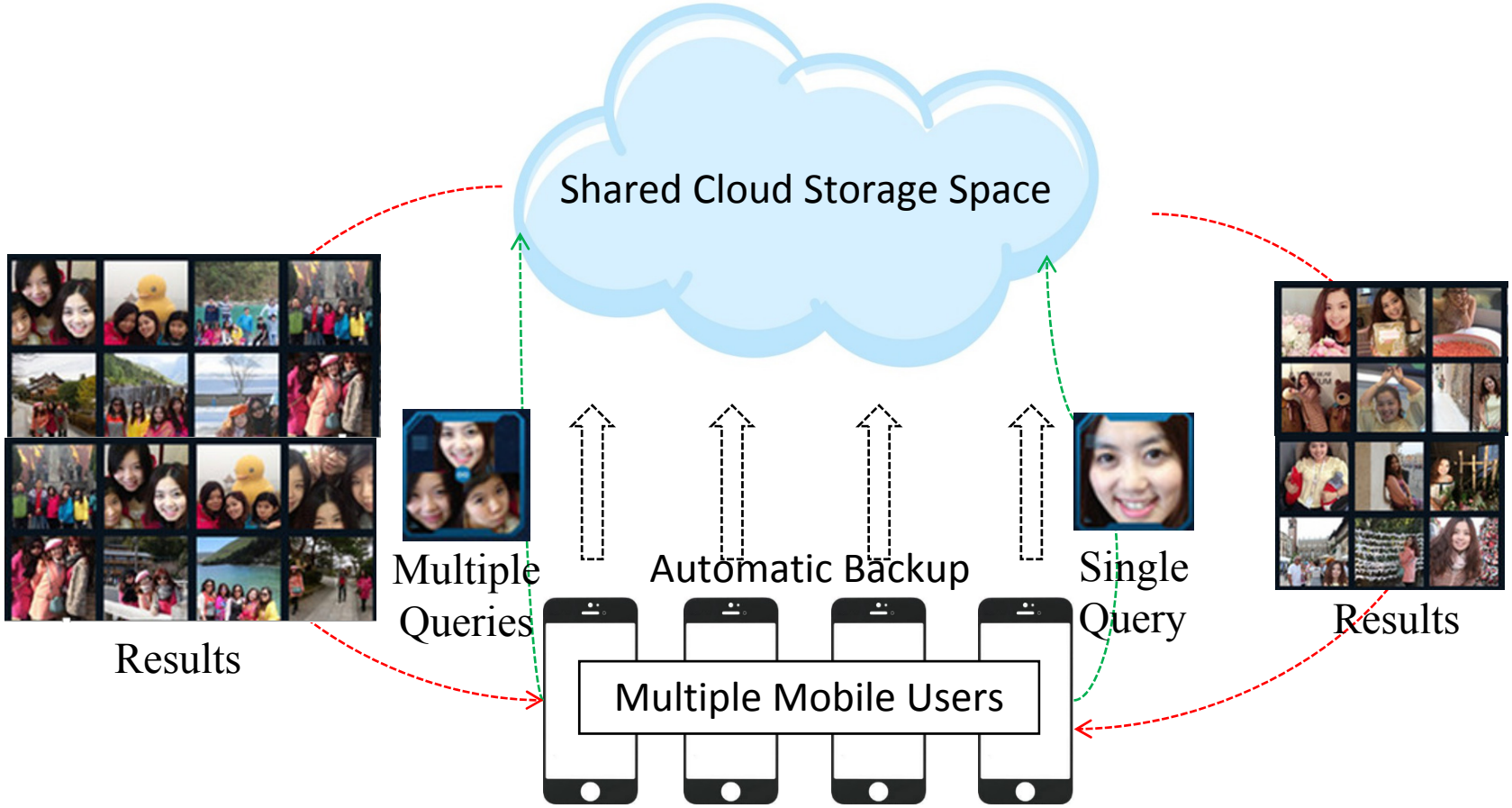




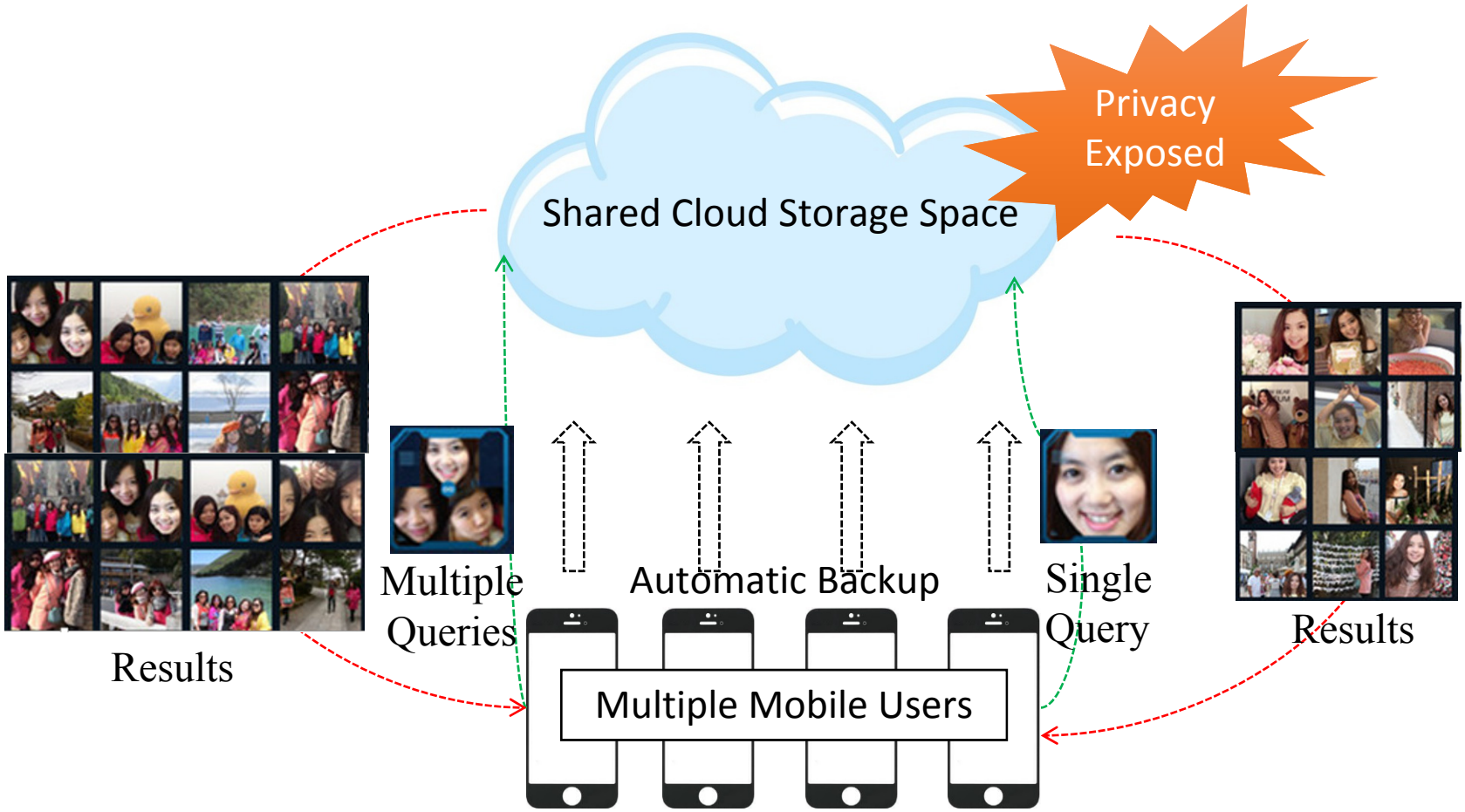
Motivation


Shared Cloud Storage Space
Automatic Backup
Multiple Mobile Users

Motivation


Shared Cloud Storage Space
Multiple Queries
Automatic Backup
Single Query
Results
Results
Multiple Mobile Users

Motivation


Privacy
Exposed
Shared Cloud Storage Space
Multiple
Queries
Automatic Backup
Single
Query
Results
Results
Multiple Mobile Users

Outline

1. Motivation
2. Related Work
3. Privacy Preserving Face Retrieval
4. Experimental Results
5. Conclusion and Discussion

Related Work

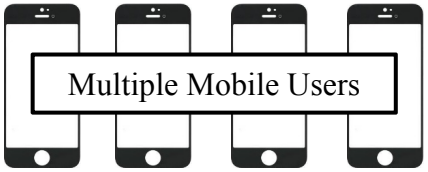
- **First Blind Vison: Secure Face Detection** [Avidan and Butman, 2006] [Jin et al., 2017]
- **Secure Face Identification (SCiFI)** [Osadchy et al., 2010]
- **Secure CBIR** [Shashank et al., 2008] [Fanti et al., 2013]
- **Secure Video Surveillance** [Upmanyu et al., 2009][Sohn et al., 2010] [Chu et al., 2014] [Jin et al., 2015; 2016a; 2016b]
- **Secure Machine Learning** [Bost et al., 2015]

Outline

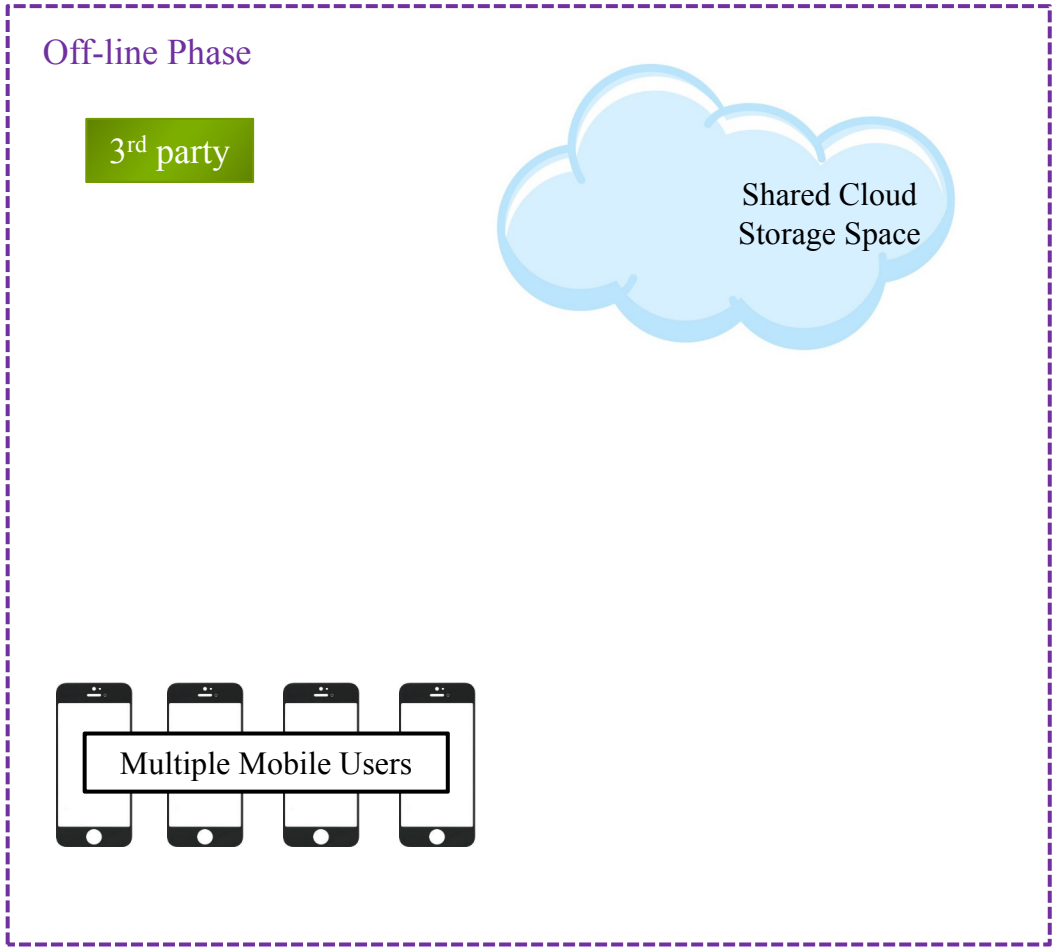
1. Motivation
2. Related Work
3. **Privacy Preserving Face Retrieval**
4. Experimental Results
5. Conclusion and Discussion

Privacy Preserving Face Retrieval Protocol

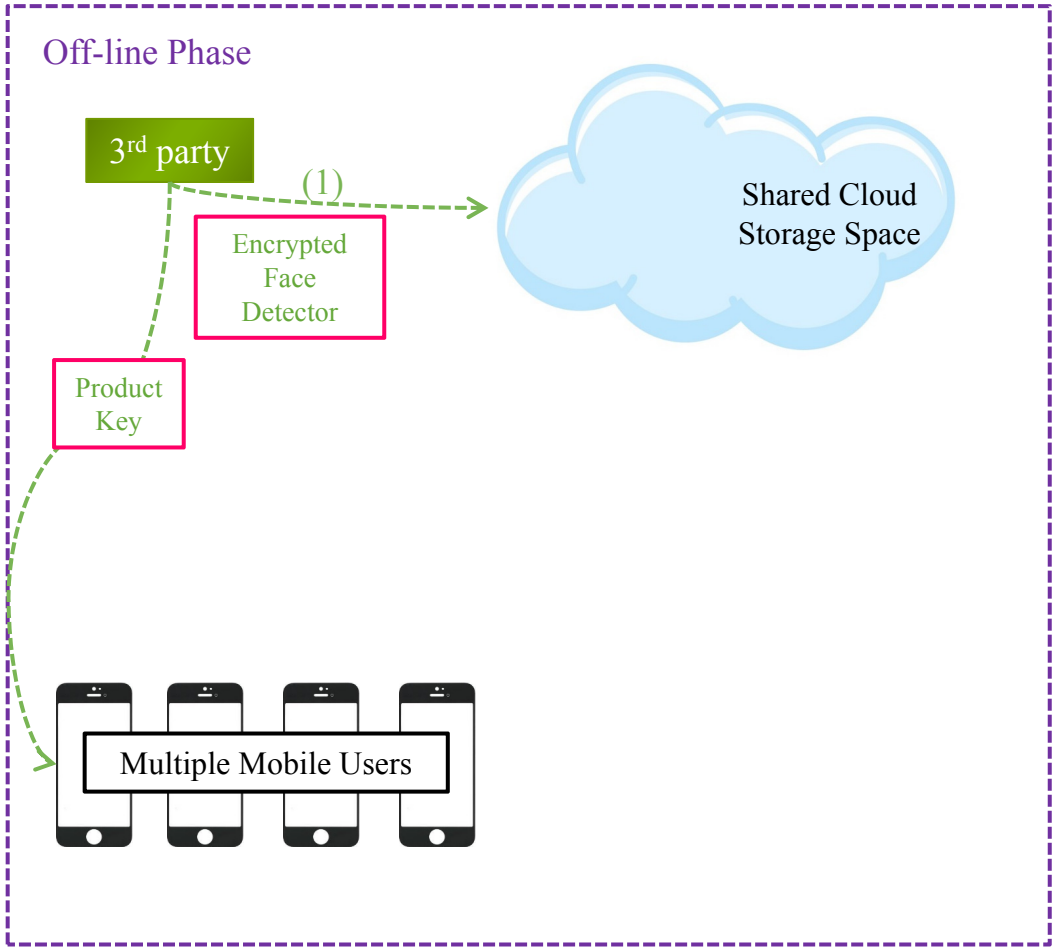
3rd party



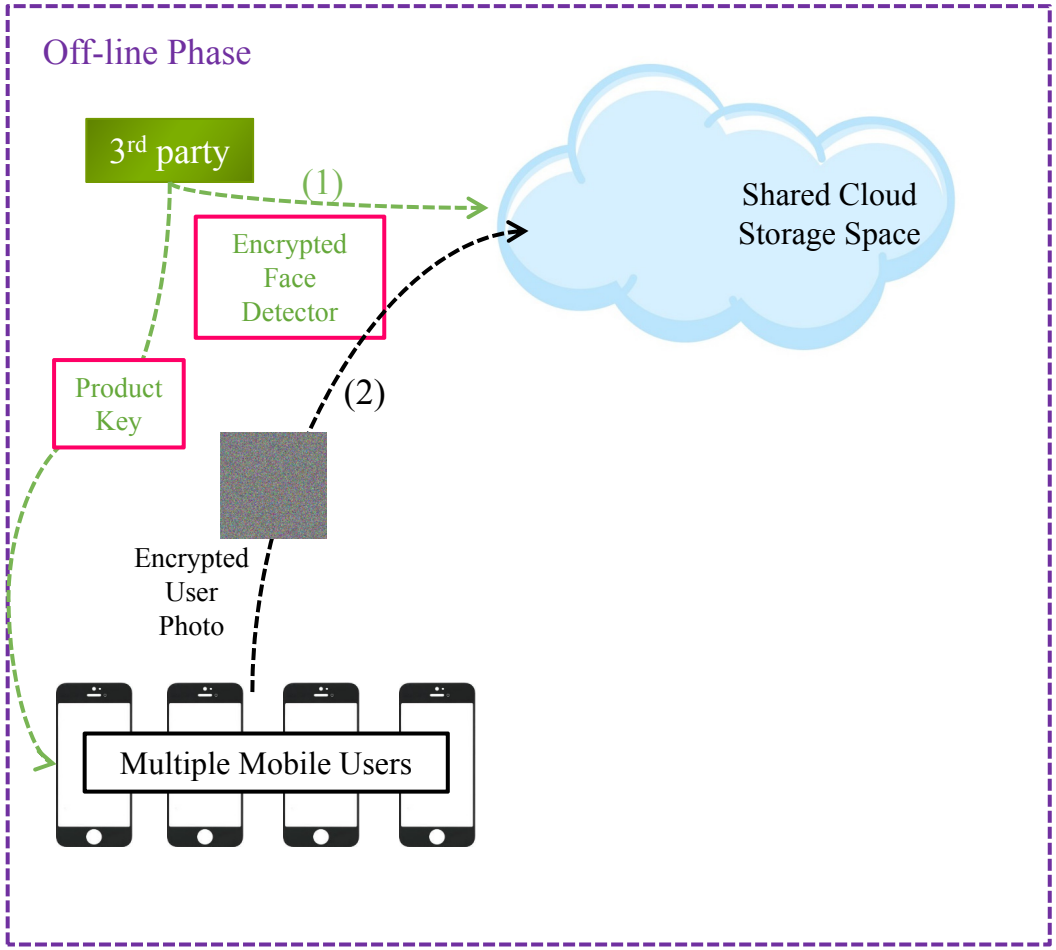
Privacy Preserving Face Retrieval Protocol



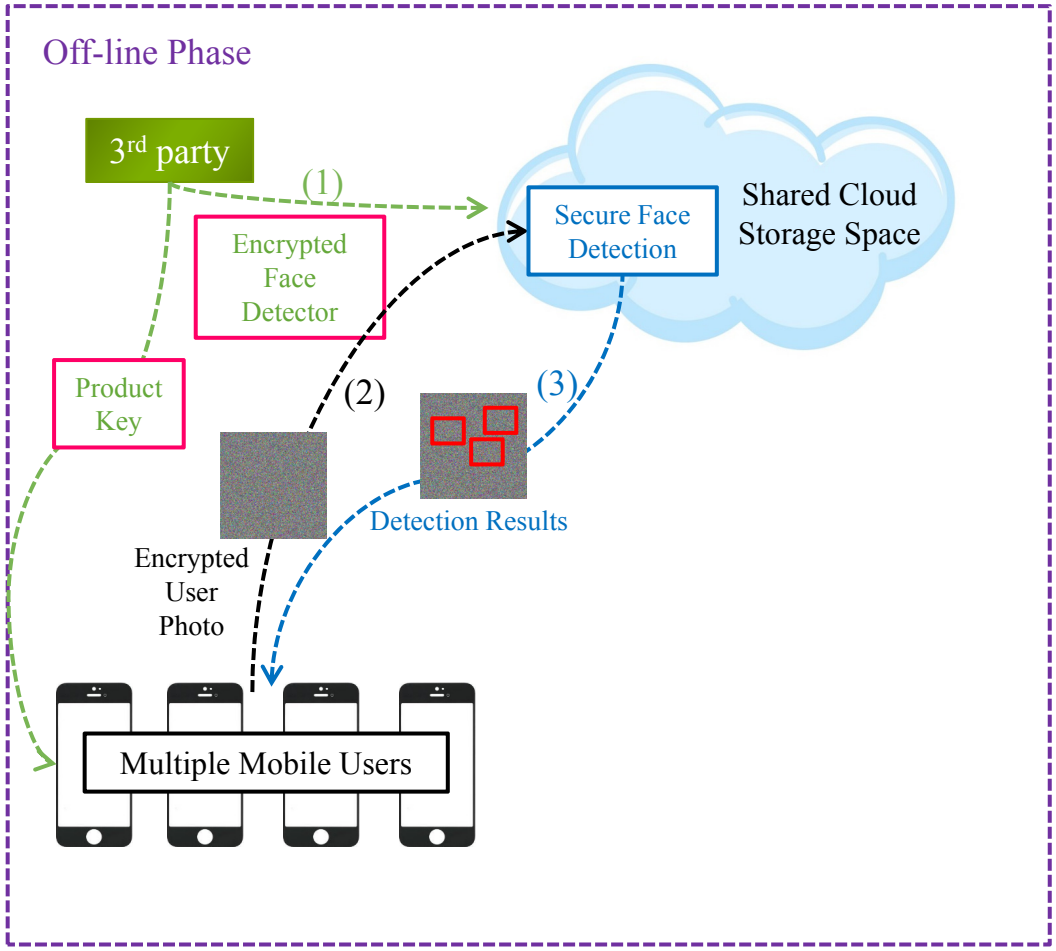
Privacy Preserving Face Retrieval Protocol



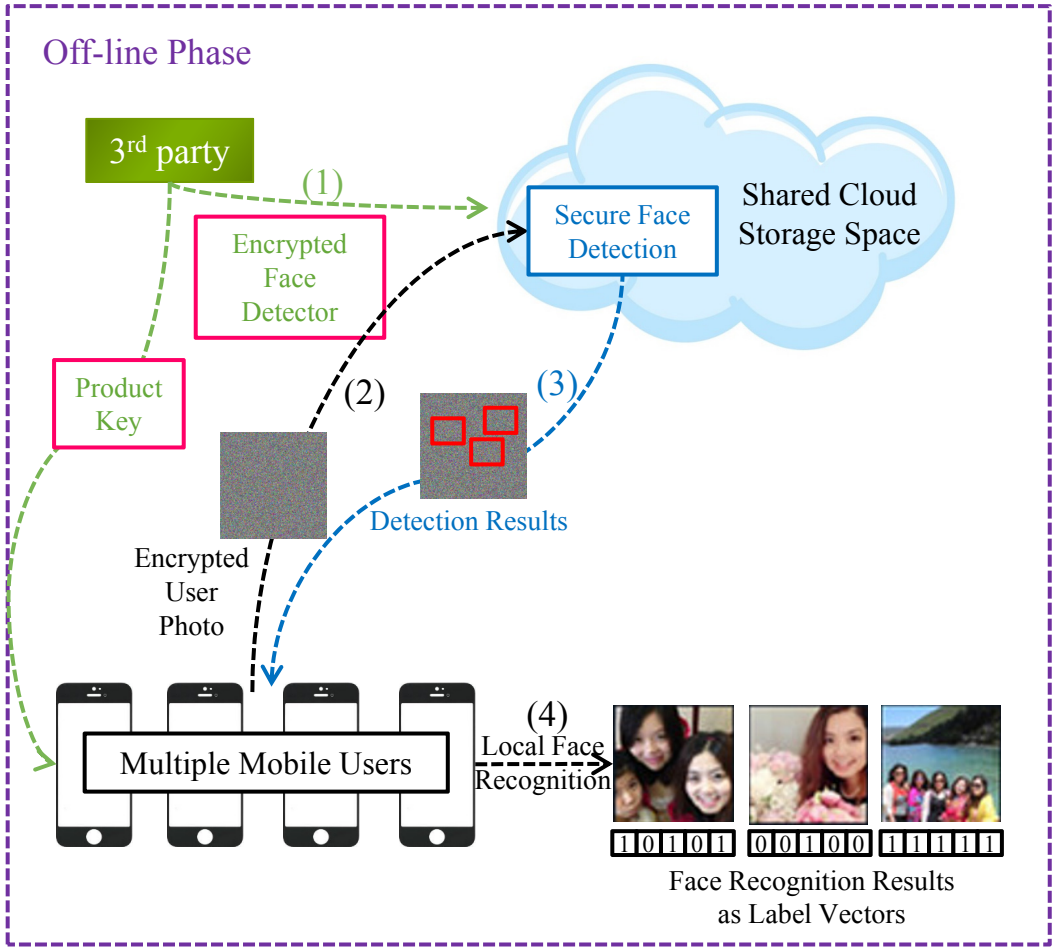
Privacy Preserving Face Retrieval Protocol



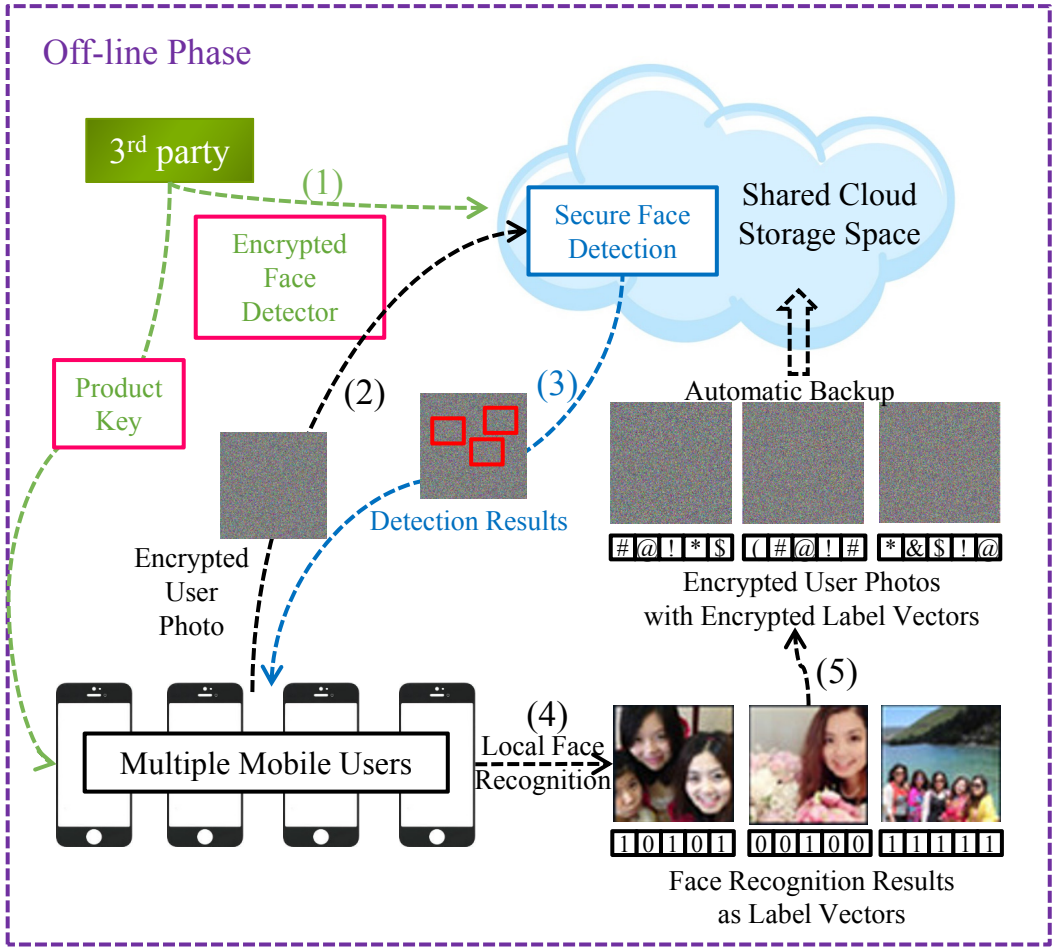
Privacy Preserving Face Retrieval Protocol



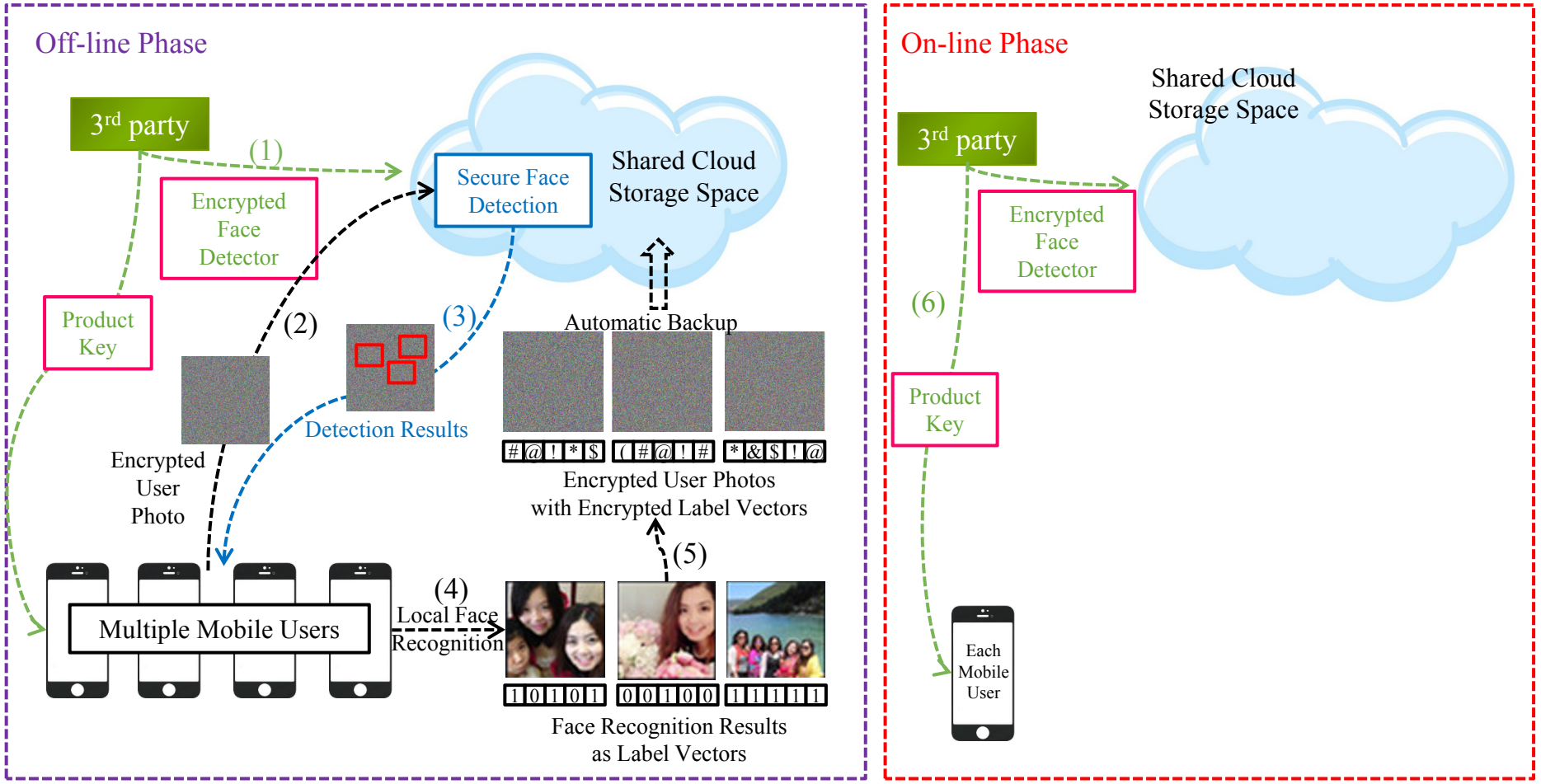
Privacy Preserving Face Retrieval Protocol



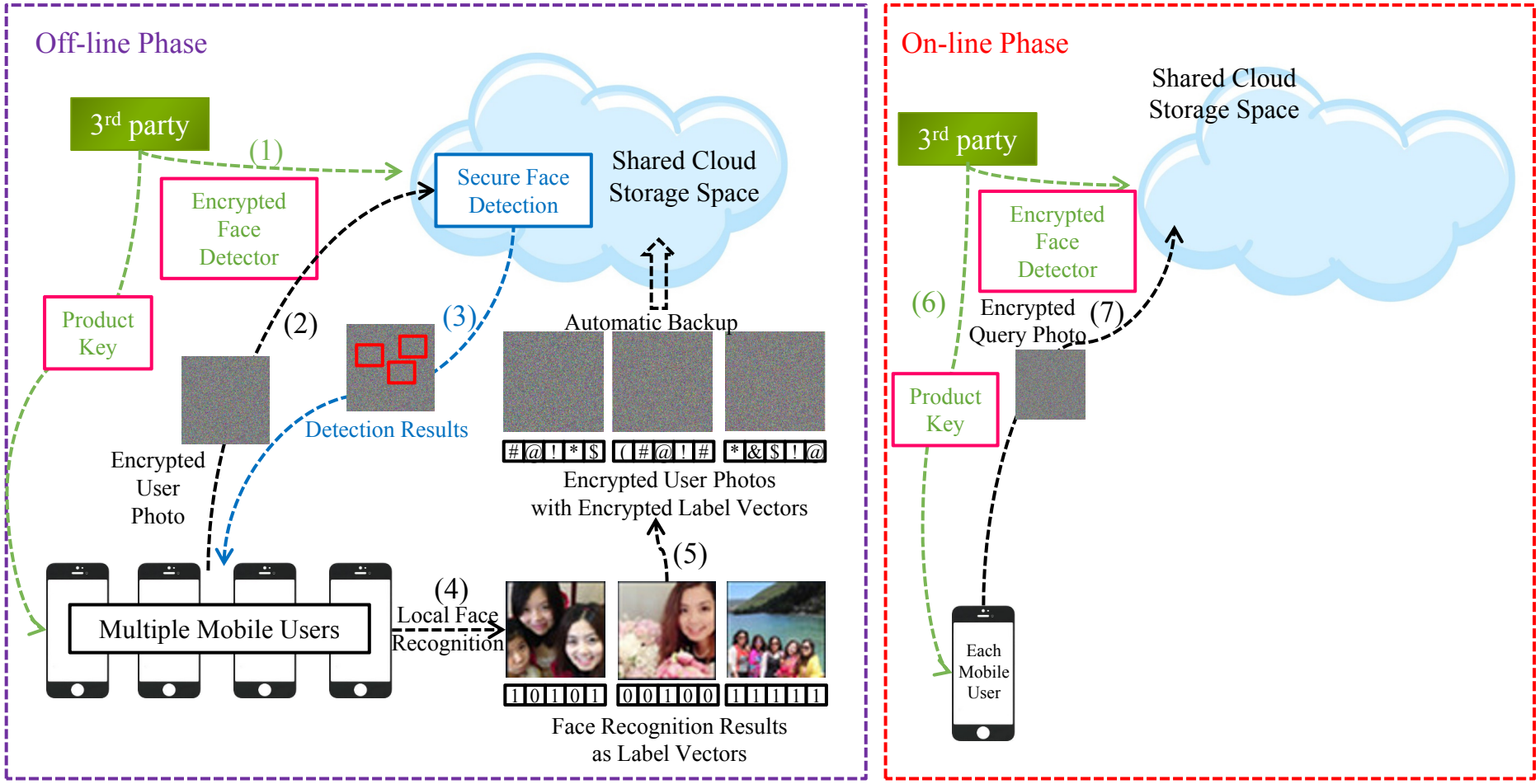
Privacy Preserving Face Retrieval Protocol



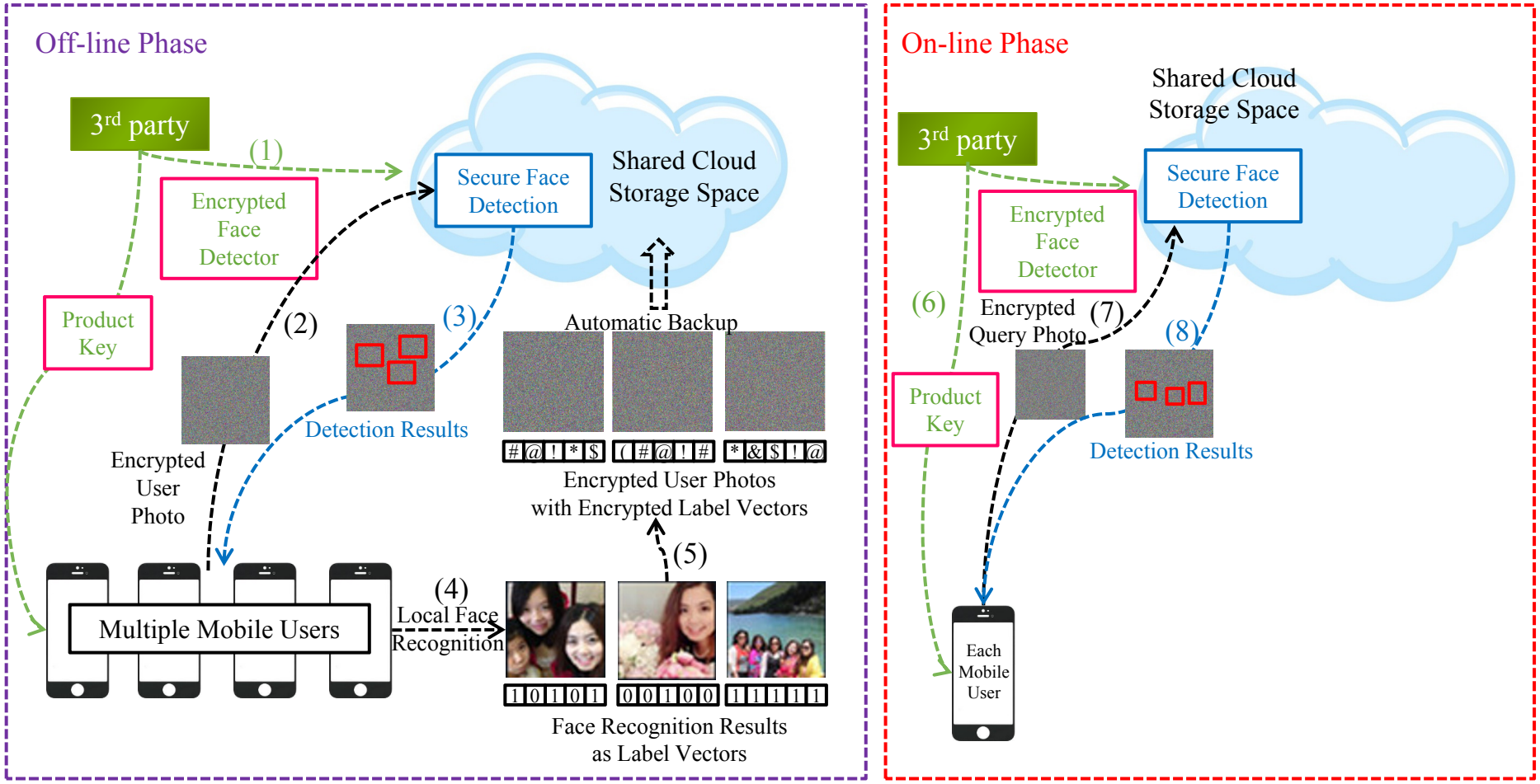
Privacy Preserving Face Retrieval Protocol



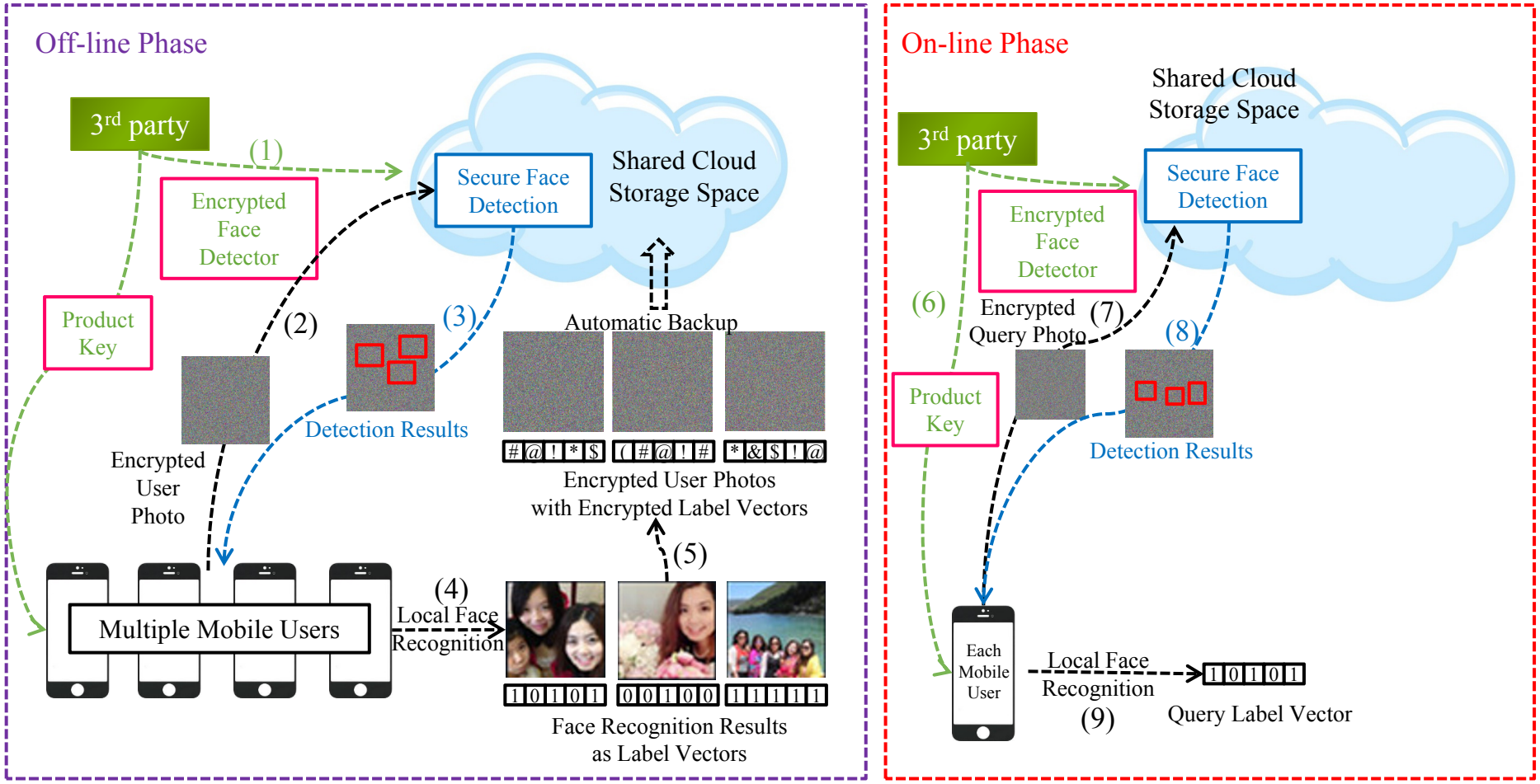
Privacy Preserving Face Retrieval Protocol



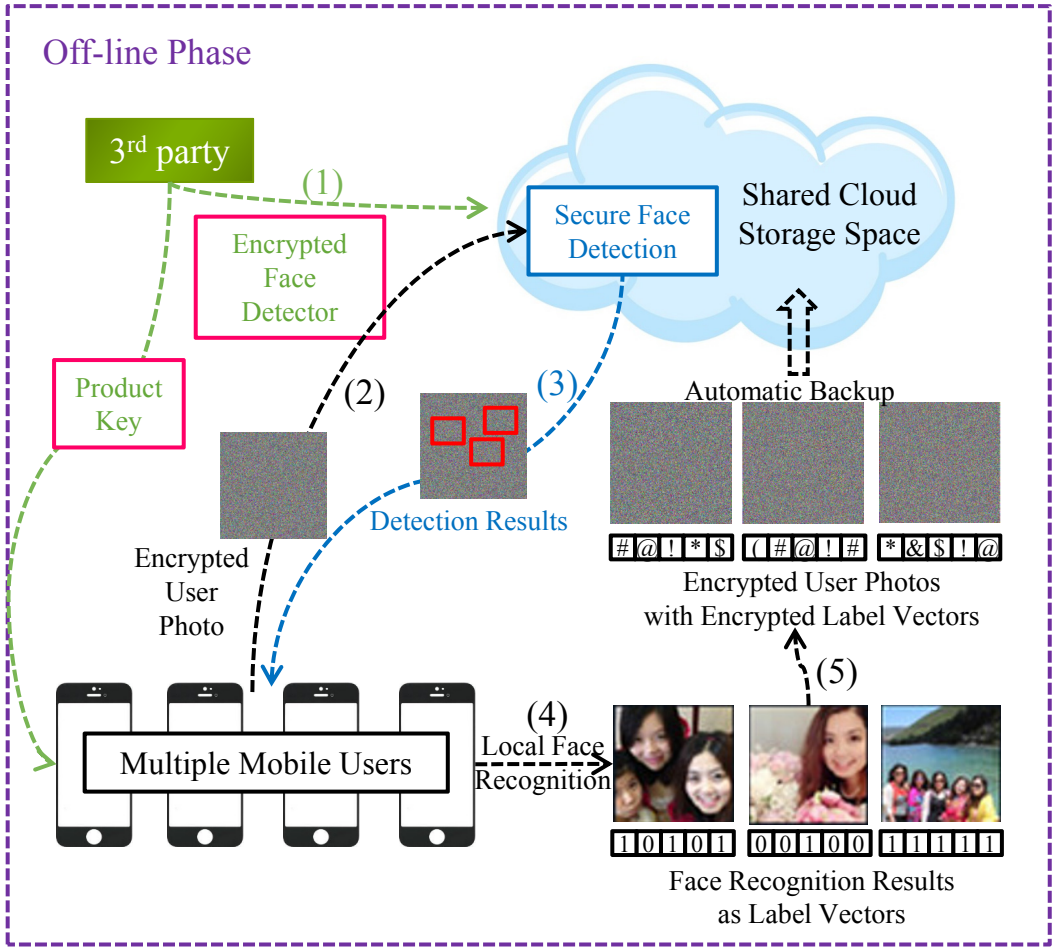
Privacy Preserving Face Retrieval Protocol

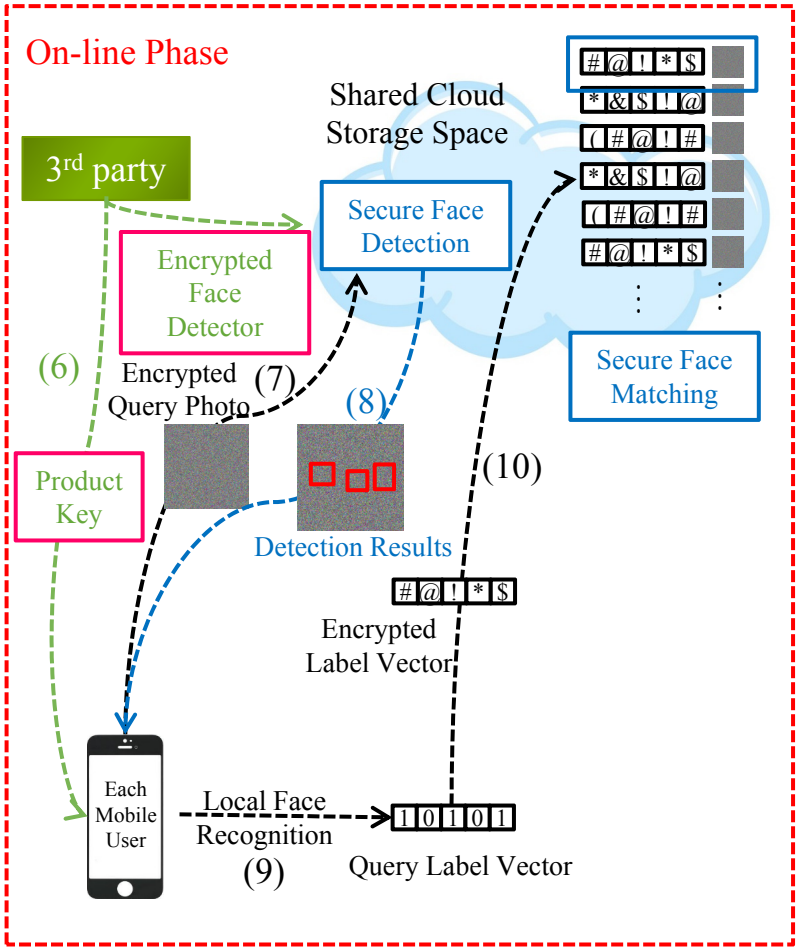


Privacy Preserving Face Retrieval Protocol

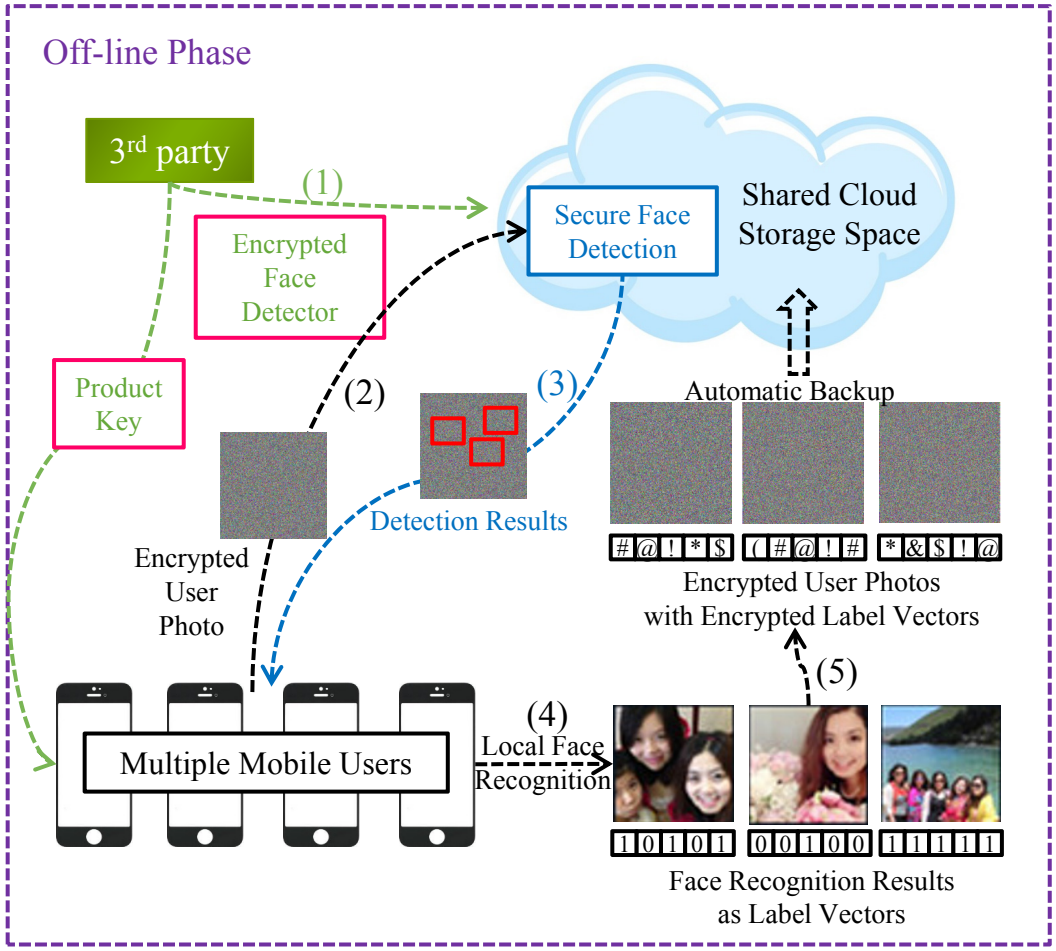


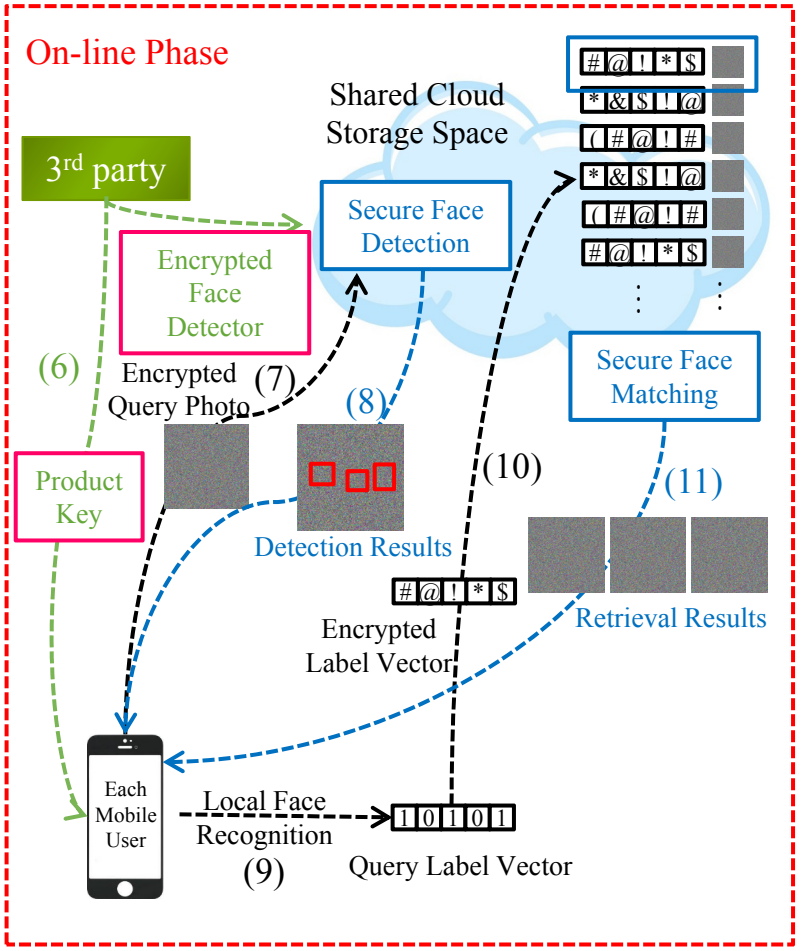
Privacy Preserving Face Retrieval Protocol



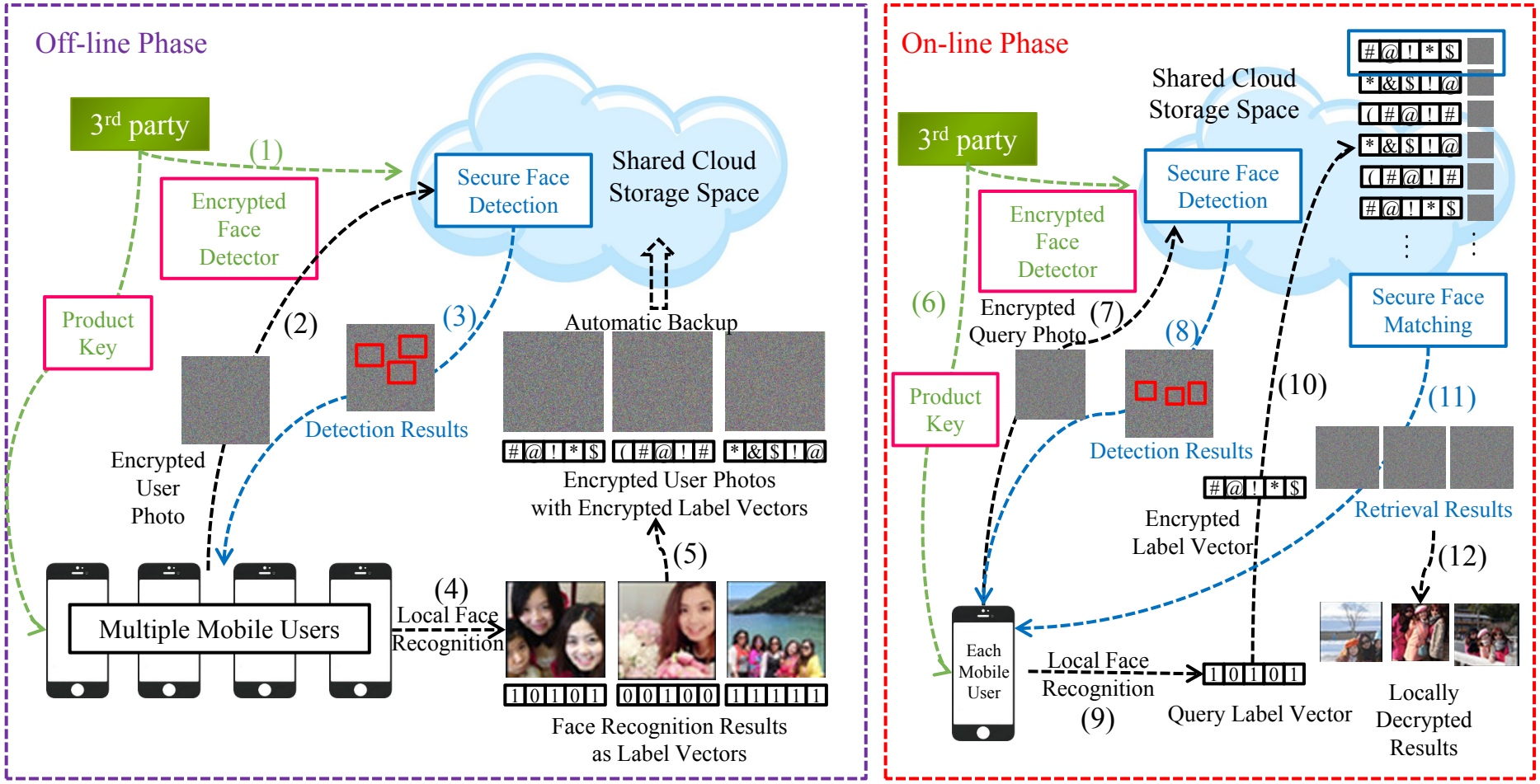


Privacy Preserving Face Retrieval Protocol





Privacy Preserving Face Retrieval Protocol



Privacy Preserving Face Retrieval Protocol

- Face Detection
- Face Recognition and Label Vector
- Face Label Matching

Traditional Face Retrieval

Privacy Preserving Face Retrieval Protocol

- Face Detection
- Face Recognition and Label Vector
- Face Label Matching

Traditional Face Retrieval

Viola & Jones Face Detector

Weak Classifier

$$h_n(x) = \begin{cases} \alpha_n & \text{if } x^T y_n > \theta_t \\ \beta_n & \text{otherwise} \end{cases}$$

Inner Production

Strong Classifier

$$H(\mathbf{x}) = sign(\sum_{n=1}^{N} h_n(\mathbf{x}))$$

[Viola and Jones, 2004] Paul A. Viola and Michael J. Jones. Robust real-time face detection. International Journal of Computer Vision, 57(2):137–154, 2004.

Privacy Preserving Face Retrieval Protocol

- Face Detection
- Face Recognition and Label Vector
- Face Label Matching

Traditional Face Retrieval

Number of persons in the query photo:

3

=1 (NOT Matching)

=3 (Matching)

Inner Production

Privacy Preserving Face Retrieval Protocol

- Face Detection
- Face Recognition and Label Vector
- Face Label Matching

Traditional Face Retrieval

+

Secure Inner Production

=

- Secure Face Detection
- Face Recognition and Label Vector
- Secure Face Label Matching

Privacy Preserving Face Retrieval

Privacy Preserving Face Retrieval Protocol

Secure Inner Production

3rd party detector

y | 2 | 4 | 6 | 8 | 0 |

Dimension: m

w | 8 | 6 | 4 | 0 | 2 |

Dimension: m

User image

$$(y \cdot x) = y^T w = 64$$

Privacy Preserving Face Retrieval Protocol

Secure Inner Production

3rd party detector

y | 2 | 4 | 6 | 8 | 0 |

Dimension: m

w | 8 | 6 | 4 | 0 | 2 |

Dimension: m

User image

$$(y \cdot x) = y^T w = 64$$

Keys: (M_1, M_2, S)

$m * m$ invertible matrix

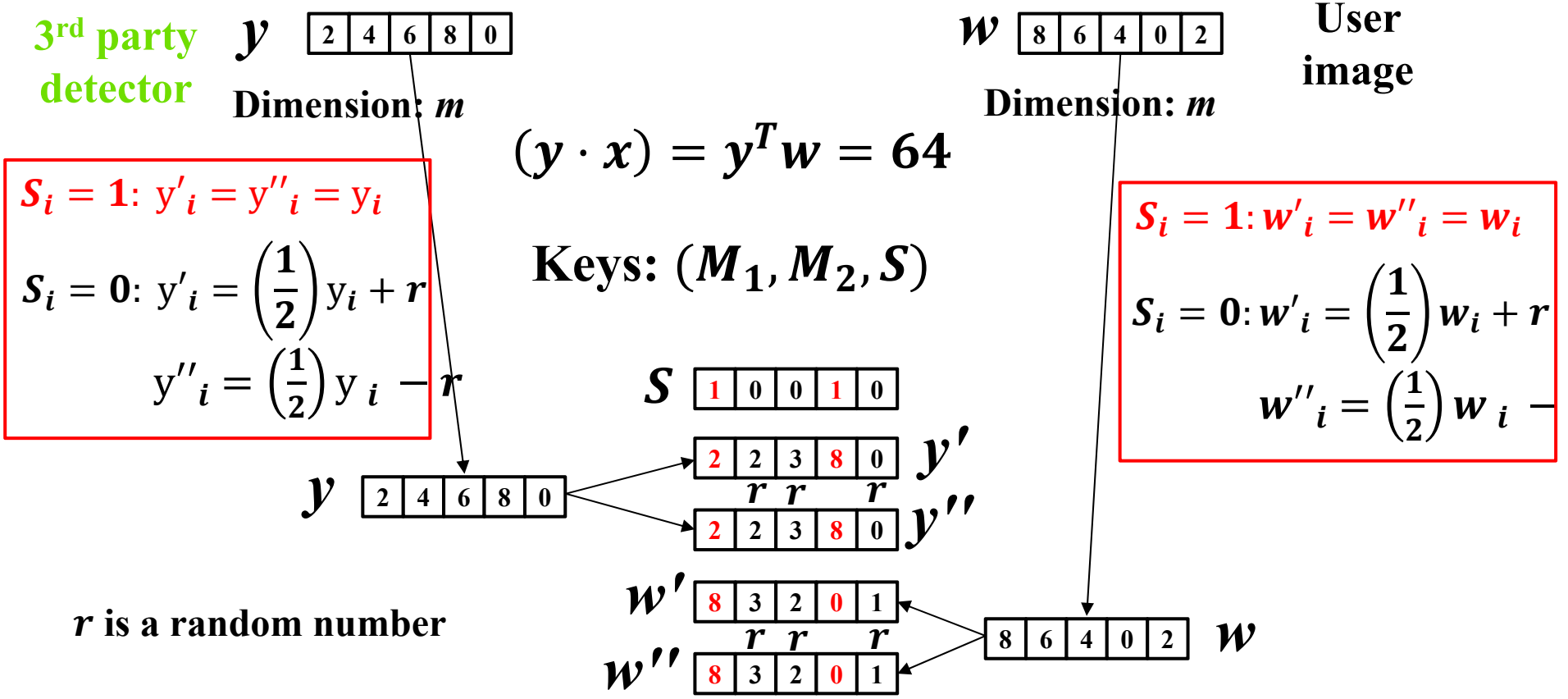
| 1 | 0 | 0 | 1 | 0 |

random binary vector

Dimension: m

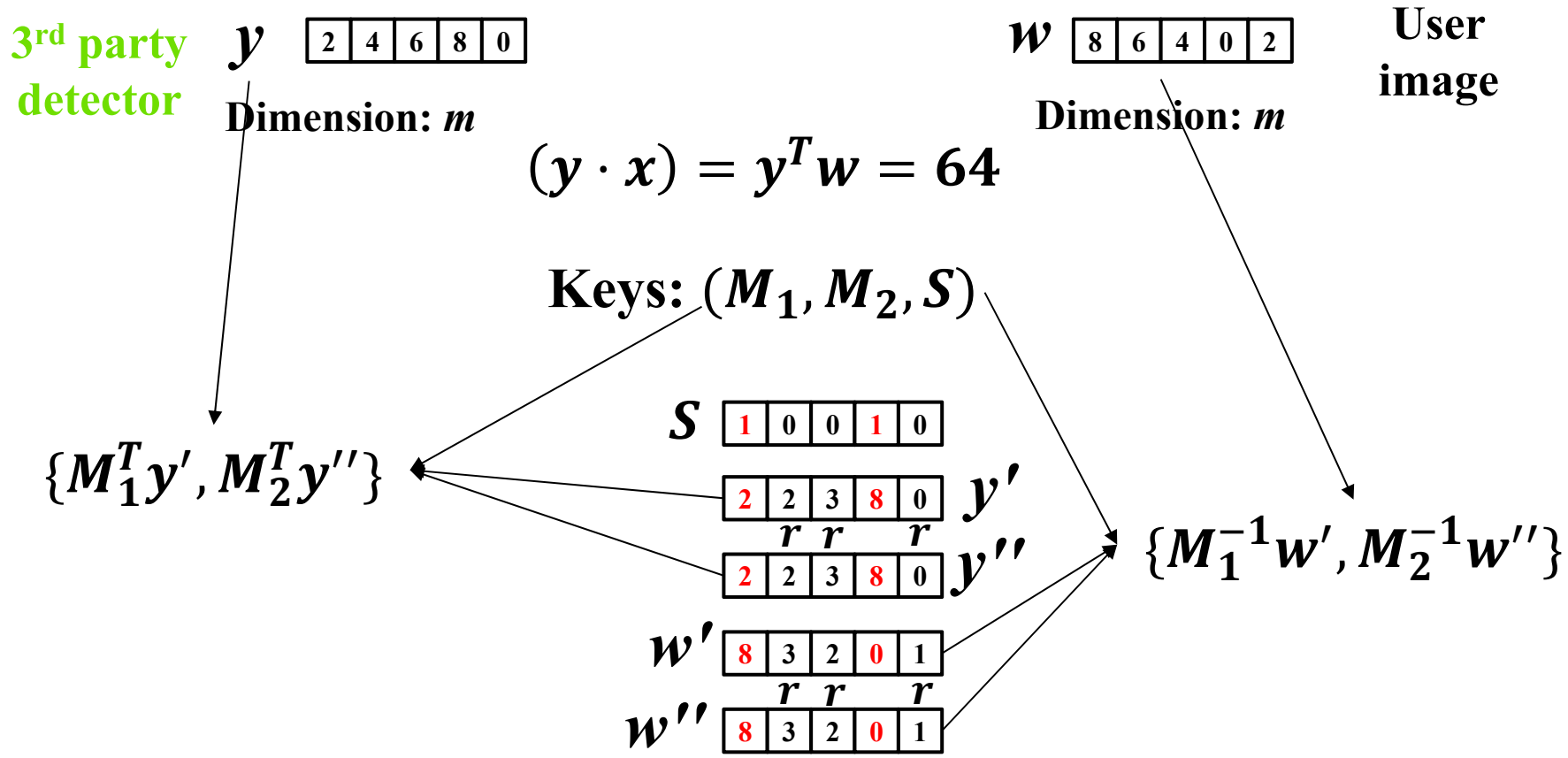
Privacy Preserving Face Retrieval Protocol

Secure Inner Production



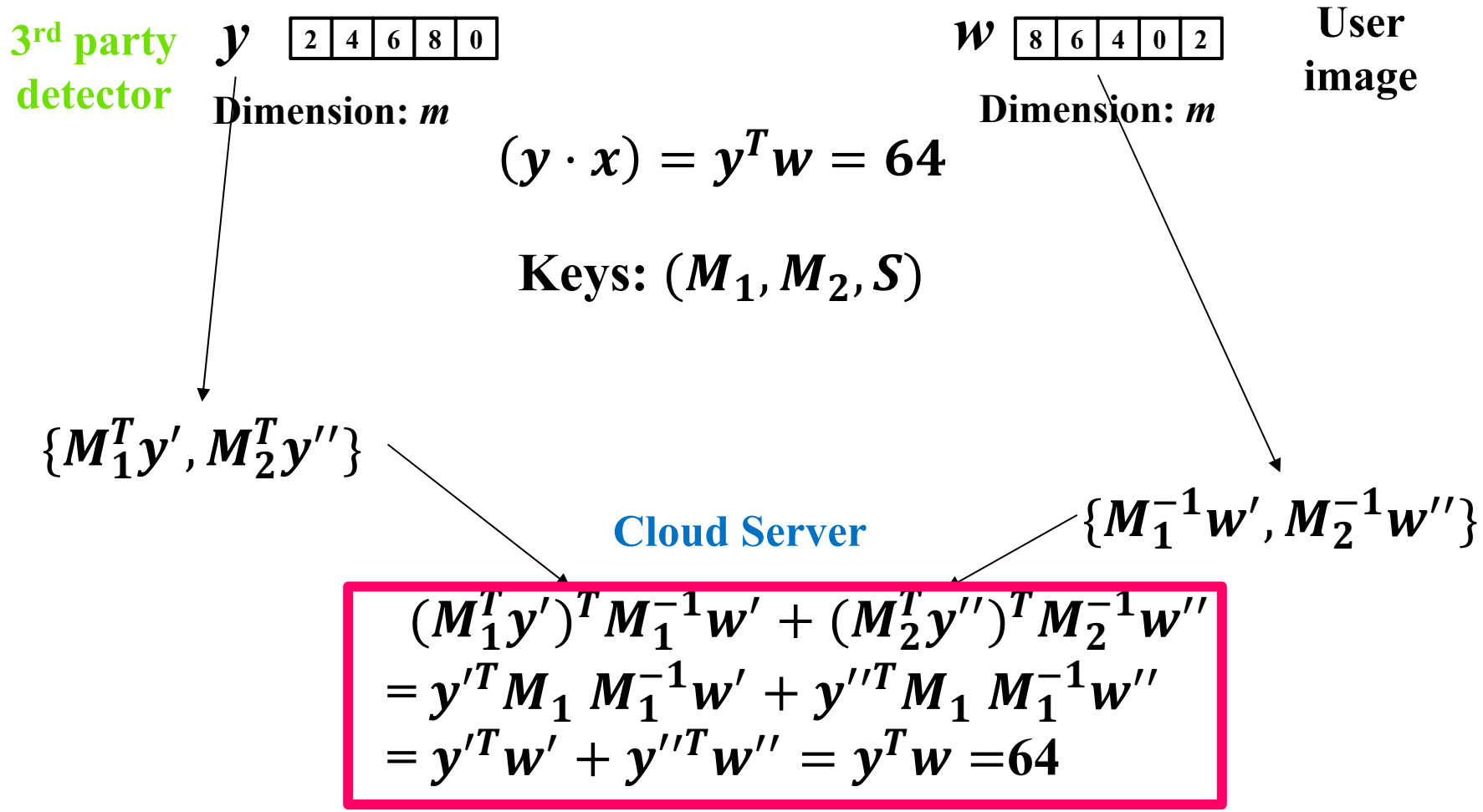
Privacy Preserving Face Retrieval Protocol

Secure Inner Production



Privacy Preserving Face Retrieval Protocol

Secure Inner Production



Outline

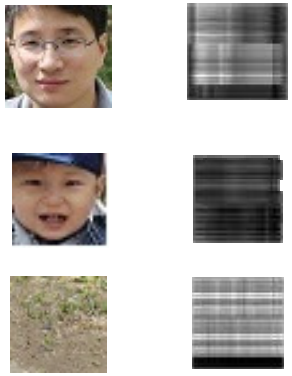
1. Motivation
2. Related Work
3. Privacy Preserving Face Retrieval
4. Experimental Results
5. Conclusion and Discussion

The Experimental Setup

- A family of 5 members
- 4 mobile phones
- 100 photos are used to build our dictionary for face recognition
- 1000 photos in the cloud for retrieval

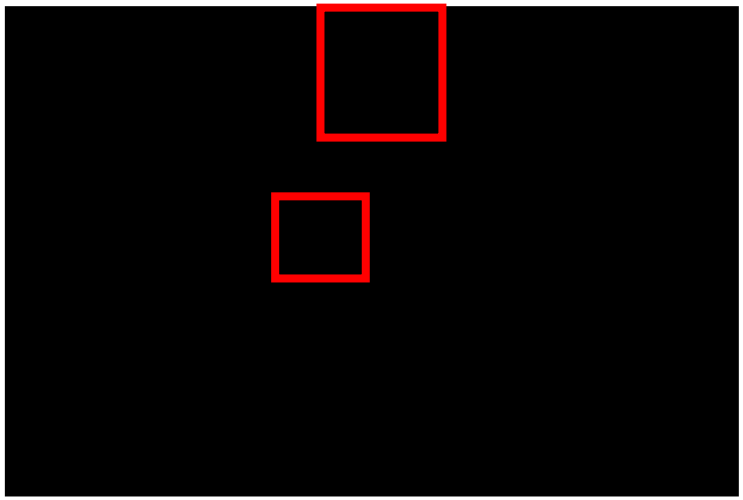
The Secure Face Detection

User Photo



Sample Detection Windows

Encrypted Detection Windows

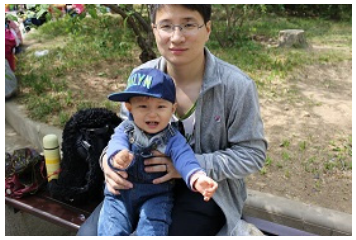


Detection Results in Encrypted Photo

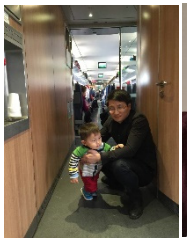
The Local Face Recognition Results

[Wright et al., 2009] John Wright, Allen Y. Yang, Arvind Ganesh, Shankar S. Sastry, and Yi Ma. Robust face recognition via sparse representation. IEEE Trans. Pattern Anal. Mach. Intell., 31(2):210–227, 2009.

The Face Label Matching Results



Query Photos



Parts of the Retrieval Results

Outline

1. Motivation
2. Related Work
3. Privacy Preserving Face Retrieval
4. Experimental Results
5. Conclusion and Discussion

Conclusion and Discussion

- The first work that addresses the private face retrieval in a shared cloud server by a group of persons.
- We propose a novel protocol to preserve the privacy of the cloud users' photos and the parameters of the commercial face detector simultaneously in such mobile cloud scenarios.
- Both the storage security and the computation security are taken into consideration in one protocol.
- The protocol is designed for a real world application.

Paper arXiv:
https://arxiv.org/abs/1708.02872

Paper download:
http://jinxin.me/downloads/papers/025-APDM2017/APDM2017-IJCAI2017Workshop.pdf

APDM2017 (IJCAI2017 workshop36)

Thanks!

Xin Jin[1], Chenggen Song[1], Shiming Ge[2,*]

[1]Beijing Electronic Science and Technology Institute
GOCPCCC Key Laboratory of Information Security
[2]Institute of Information Engineering, Chinese Academy of Sciences
*Corresponding author: geshiming@iie.ac.cn

http://kislab.besti.edu.cn/victory/

Homepage

北京電子科技学院 Beijing Electronic Science and Technology Institute

VICTORY besti

中国科学院信息工程研究所 INSTITUTE OF INFORMATION ENGINEERING,CAS

Official WeChat
官方微信