Photo recognition that keeps personal interests private

November 14 2018

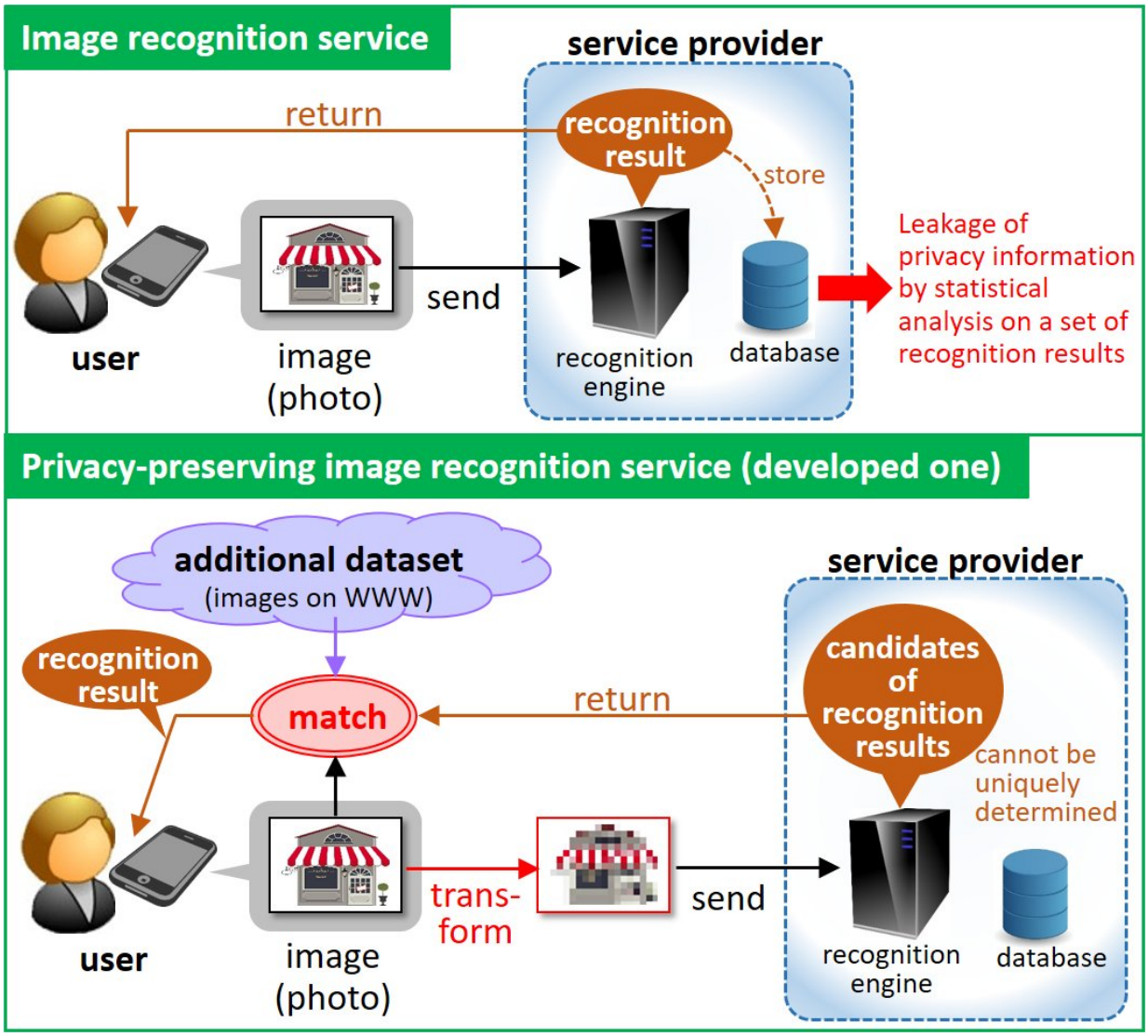

Fig.1: Overview of the privacy-preserving framework for image recognition services. Credit: Osaka University

From just a quick snapshot on a smartphone, image recognition technology can provide a wealth of information to help shoppers find in-store bargains and inform tourists of the name of a landmark. But these photos may be giving away more information about users' preferences and tendencies than they want to share.

Researchers at Osaka University have proposed an encryption-free framework for preserving users' privacy when they use photo-based information services.

Artificial intelligence, such as deep learning, has dramatically improved the performance of image recognition. Users can send a photo to a server, which identifies the content using an image recognizer and returns relevant information. This is advantageous to shoppers, tourists, and others, but the results can disclose private information, such as a user's current location. The server can also use identifiers from the smartphone to link current results with past results to build a location history that contains even more private information: "Photos reflect private aspects of their owner, such as interests, preferences, and tendencies," explains co-author Naoko Nitta, "which can be leaked by web-based image recognition services. To address this problem, we developed an encryption-free framework for privacy-preserving image recognition called EnfPire."

To use the framework, the user extracts a feature from the photo. EnfPire transforms the feature before it's sent to the server. Because the server cannot uniquely identify the transformed image, it returns a set of candidates to the user, who compares them with the original feature using a simple recognizer. "With our framework, the provider of the photo-recognition services is unable to receive enough information for unique image recognition, while the user obtains the correct recognition

result and its related service information," says lead author Kazuaki Nakamura.

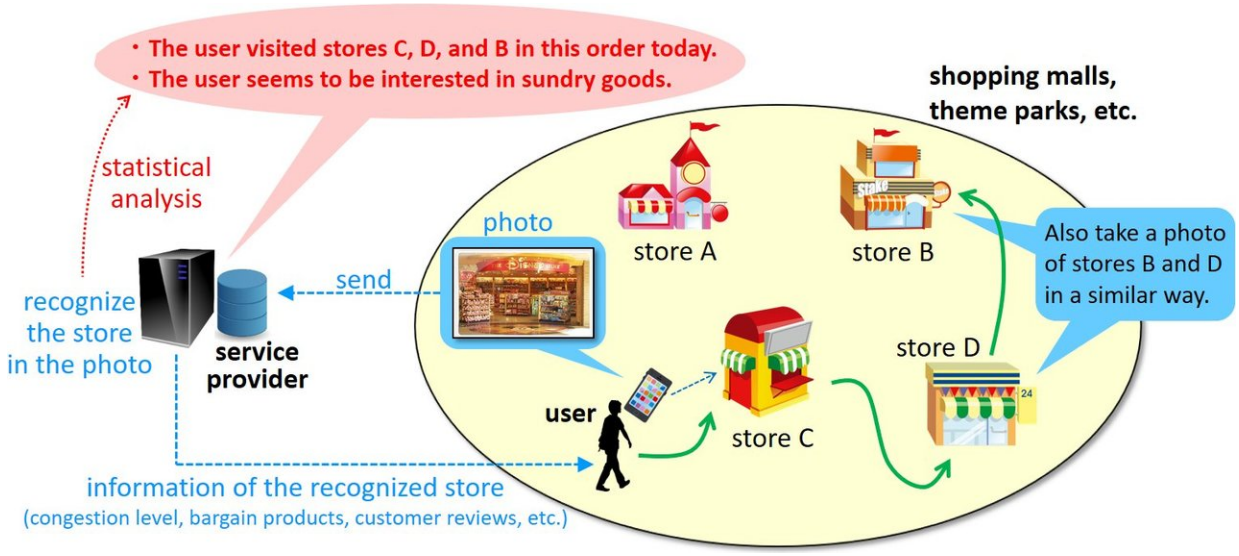

Fig.2: Example of image recognition services that can leak users' privacy information about their private aspects such as interests, preferences, and tendencies. Credit: Osaka University

EnfPire successfully abstracts location information, but this is not sufficient to protect the user's history, which could still be approximated from geographical relationships between results. So, the research team proposed a countermeasure by which dummy requests are automatically sent from the smartphone to the server, which returns results based on the dummy requests that are automatically removed from the device without the user being aware of the process. The dummy features are chosen carefully so that the server does not identify them as such.

In real-world experiments, EnfPire degraded the server's recognition accuracy from 99.8 percent to 41.4 percent, but the user's accuracy was

86.9 percent. "We expect this framework to make a major contribution to research, development, and application of safe and secure artificial intelligence," adds senior author Noboru Babaguchi.

More information: Kazuaki Nakamura et al. Encryption-Free Framework of Privacy-Preserving Image Recognition for Photo-Based Information Services, *IEEE Transactions on Information Forensics and Security* (2018). DOI: 10.1109/TIFS.2018.2876752

Provided by Osaka University