

Photo without a face

We have barely any control over where information about us and even photos bearing our likeness are displayed. In the future, however, it may at least be possible to prevent ourselves from appearing as bystanders in photos on other people's Facebook pages. This is thanks to technology developed by a team working under **Paarijaat Aditya, Rijurekha Sen** and **Peter Druschel** from the **Max Planck Institute for Software Systems**.

TEXT **TIM SCHRÖDER**

We are experiencing a cultural change: smartphones have transformed our everyday habits, especially when it comes to taking photographs. Nowadays, we not only take photos while on vacation and at family celebrations, but also while shopping, in the bar, or out for a walk. After all, the advent of the smartphone means we always have a camera at hand. The quality of the built-in cameras is now so good that they're virtually the only one you need. Also, no camera is as readily accessible as the one in your trouser pocket.

Figures obtained by the online industry association Bitkom confirm the trend toward taking photos with mobile phones: seven out of ten Germans use their smartphone to take photos while on vacation – and six out of ten amateur photographers immediately share the photos using Facebook, WhatsApp, or other services. There's no doubt about it: smartphone photography is an omnipresent phenomenon.

But this very phenomenon can become a problem when snaps capture not only friends and acquaintances but also

bystanders who accidentally appear in the photo. Many people feel uneasy when a stranger takes their picture – particularly because in the era of social media, you never know where the pictures might turn up in the future. It would therefore be reassuring if bystanders were simply unrecognizable in photos.

BYSTANDERS' FACES ARE PIXELATED

This was also the initial premise for Paarijaat Aditya and Peter Druschel of the Max Planck Institute for Software Systems in Saarbruecken. Together with colleagues from the neighboring Max Planck Institute for Informatics, the two researchers have developed a technique that pixelates bystanders' faces in photos, rendering them unrecognizable, while showing the faces of intentional subjects clearly. I-Pic, as they have named their app, could one day be installed as a special function in smartphones.

"These days, when it comes to taking photos, many people are concerned about their privacy," says Paarijaat Aditya. "Before we started developing

I-Pic, we launched a survey of our own. One thing we learned was that this depends a lot on the situation, among other factors: for instance, people find it particularly unsettling if their photo is taken in the hospital, while doing sports, or at the beach." In general, the researchers found that, even in the same situation, different people have different privacy preferences when it comes to photographs of themselves, and that an individual's preferences also vary considerably from one situation to another. Clearly, therefore, it was essential that I-Pic be able to take account of individual people's wishes depending on the situation.

I-Pic is currently at the prototype stage. In a video on YouTube, Paarijaat Aditya demonstrates how it works, taking a selfie that also captures people standing in the background. When the photo appears on the camera screen, the people who don't want their photo to be taken are pixelated, whereas the others are clearly visible. At first glance, I-Pic seems very straightforward. However, if you think about it for a moment, there is one puzzling aspect: how on earth can the camera know who



Photo: istockphoto

My image belongs to me: in snapshots taken by strangers, the I-Pic software pixelates the faces of people who don't want to be photographed accidentally.

» Even in the same situation, different people have different privacy preferences when it comes to photographs of themselves – and the preferences of the individual also depend strongly on the situation.

wants to be photographed and who does not? It quickly becomes clear that there's something special about I-Pic.

"Our achievement lies in the linking up of several sophisticated technologies in order to get the whole system to work," says Paarijaat Aditya. The prerequisite for providing effective protection against unintended walk-on parts in photos is that the photographer's and bystanders' smartphones must all be equipped with I-Pic technology. And, of course, it must be possible for the smartphones of everyone visible in a photo to communicate with the photographer's device – in order to tell it whether their owners want to be recognizable or not. With I-Pic, this communication takes place via Bluetooth, a classical wireless standard that allows devices to exchange data over distances of a few meters.

SMARTPHONES TRANSMIT PERSONAL PREFERENCES

To begin with, each user configures the software according to their personal preferences, i.e. whether or not they wish to be photographed by strangers in various situations or at various locations. Every phone equipped with I-Pic transmits this information constantly via Bluetooth. All nearby smartphones therefore tell the photographer's smartphone which people agree to appear in the photo that has just been taken and which do not.

Of course, the smartphone also receives Bluetooth signals from people who aren't visible in the image – for example, from bystanders standing just

out of shot. The photographer's smartphone must therefore be able to determine which Bluetooth signal belongs to whom or, to be precise, whether it originates from one of the people seen in the picture.

For this purpose, I-Pic is first fed with portrait photos of the smartphone's owner before it is able to do its job. Around ten photos is all it takes for I-Pic to get to know its owner's face and to store a record of its characteristics. All mobile phones equipped with I-Pic constantly transmit this facial information over the surrounding area – including to the smartphones of anyone taking a photo within Bluetooth range. This allows the photographer's smartphone to compare the faces in the photo it has just taken with facial information from people in the surrounding area.

In addition to data relating to faces, the photographer's smartphone also receives information about people's preferences ("Wants to be visible/Doesn't want to be visible") – and can then make the corresponding faces unrecognizable.

For the facial recognition, the team had to incorporate powerful algorithms known as "classifiers" into the software. These can recognize faces quickly and reliably – even in photos with poor lighting, shadows, or back-lighting. Researchers led by Bernt Schiele, Director at the Max Planck Institute for Informatics, have developed an extremely effective piece of software for facial recognition.

"However, exchanging personal data – such as facial information – between smartphones is an extremely sensitive area in terms of data protec-

tion," says Peter Druschel, Director at the Max Planck Institute for Software Systems. For this reason, the researchers have also equipped I-Pic with sophisticated encryption technology, allowing it to convert all of the data into encrypted combinations of characters before it is sent back and forth. Information about the face is not therefore transmitted simply as a JPEG image or in a similar format. Instead, I-Pic encrypts the numerous characteristics of the face into what is known as a high-dimensional vector.

COMPARISON BETWEEN ENCRYPTED SETS OF DATA

I-Pic then compares the faces in the photo with the facial information sent to the photographer's smartphone via Bluetooth. The key thing is that the comparison takes place between the encrypted files. In other words, the picture information is not revealed at any point in time. "It may sound strange, but it's actually possible to process two encrypted files together," says Rijurekha Sen, another researcher at the Max Planck Institute for Software Systems. "This is referred to as homomorphic encryption. It allows you to determine whether two images are the same without actually having to reveal them."

As a result, the photographer's smartphone never stores a person's real image data if they have set their preference to "not recognizable". The face is not shown as such in the picture that has just been taken, nor is it possible to read the picture information sent from the other mobile phones via Bluetooth.



And the face in the picture has already been pixelated by the time it appears on the phone's screen.

But there is more to I-Pic than Bluetooth, facial recognition, and encryption technology. During the software's development, the researchers were faced with another problem: securing data by encryption always involves highly complex computing processes. These calculations require a great deal of RAM and consume huge amounts of power. In locations where lots of photographs are being taken, I-Pic would have to perform a large number of image calculations, quickly draining the phone's battery or overburdening its processor.

The researchers therefore equipped I-Pic with technology that outsources the encryption and comparison of image pairs to the cloud – a worldwide network of computers – via a mobile data connection. The encrypted data is therefore processed on a large server elsewhere, which reports back to the smartphone with the result of the “Wants to appear in the photo/Doesn't want to appear in the photo” analysis.

“I-Pic works astonishingly well despite all this complexity,” says Paarijaat Aditya, who has already presented I-Pic at an international IT conference, where it attracted considerable praise. Peter Druschel adds: “We're the first team in the world to devise such an application and to have put it into practice successfully despite the wealth of technologies involved. And we're already thinking about how to expand it.”

Specifically, the question is how to make faces unrecognizable in photos in an aesthetically pleasing manner. >

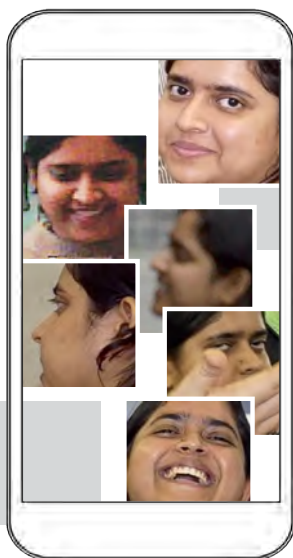


If the people in a photo have the I-Pic app installed on their smartphone, it synchronizes their facial information and data protection preferences with the photographer's device. Those who do not wish to be recognizable are then blurred out in the final image.





Helping to safeguard the right to one's own likeness: Paarijaat Aditya and Peter Druschel developed the I-Pic app based on technically sophisticated components (above). The central feature of this app is technology that recognizes a person even when they are photographed from totally different angles, while partly obscured or in poor lighting (below).




After all, images with pixelated faces are not particularly attractive. Peter Druschel therefore wants to extend I-Pic with a software module that can modify faces, make them look older, or specifically manipulate the skin and hair color as well as other characteristics: "In the photo, unfamiliar faces are no longer simply pixelated. Instead you see people who, in reality, don't even exist."

There is another thing to consider: I-Pic should allow users to configure their preferences in detail. Those selecting "Never wants to appear in strangers' photos" as standard could run into problems. For example, photos taken at large family gatherings might actually be welcome, but the person would always be pixelated in the images. The Saarbruecken-based researchers are therefore developing a set of preferences for future users to choose from.

For example, one possibility could be to allow contacts stored on the phone to make the owner's face visible in photos. Apparently, it will also be possible to set preferences for various locations in the future. Users could therefore select the unrecognizable mode for the office or gym but allow their likeness to be displayed unpixelated in all other locations.

It may also be possible to adapt the I-Pic technology to similar applications, such as videos. "At any rate, I-Pic has reached the stage where it can soon be refined into a market-ready product," says Peter Druschel. "Ideally, the technology would be adopted by smartphone manufacturers and installed in mobile phones as standard – that would represent a huge gain in terms of privacy and data security."

 www.mpg.de/podcasts/digitale-gesellschaft
(in German)

SUMMARY

- Now that smartphones are equipped with powerful cameras and people are taking more and more photos, there is a growing risk that bystanders will be photographed and that their images will be distributed on social media without their consent, for example.
- The I-Pic software could ensure that people are only recognizable in photos if they have given their approval. Faces of people who do not wish to appear in the photo would then be pixelated or rendered unrecognizable.
- In order to safeguard the right to one's own likeness, I-Pic combines various technologies, such as facial recognition based on artificial intelligence and the encryption and comparison of image data in the cloud.

MAX PLANCK SCHOOLS

Obtain your PhD in a highly innovative,
interdisciplinary and international environment.

PASSION FOR SCIENCE

maxplanckschools.org

Max Planck School of Cognition | Max Planck School of Photonics
Max Planck School Matter to Life

