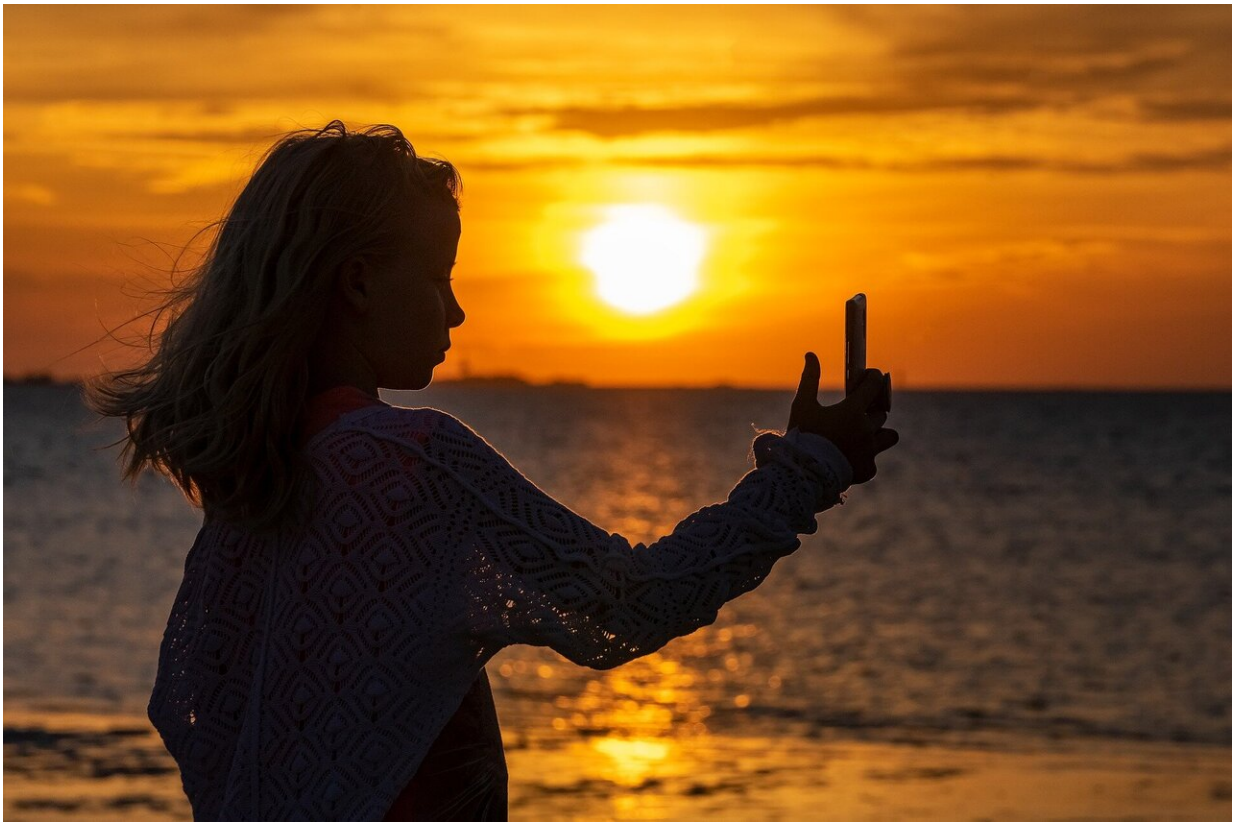
Encrypting photos on the cloud to keep them private

July 14 2021



Credit: CC0 Public Domain

The past decade has witnessed scandal after scandal over private images maliciously or accidentally made public. A new study from computer scientists at Columbia Engineering reveals what may be the first way to

encrypt personal images on popular cloud photo services, such as those from Google, Apple, Flickr and others, all without requiring any changes to—or trust in—those services.

Smartphones now make it easy for virtually everyone to snap photos, with market research firm InfoTrends estimating that people now take more than a trillion photos each year. The limited amount of data that smartphones hold, and the way in which they are vulnerable to accidental loss and damage, lead many users to store their images online via cloud photo services. Google Photos is especially popular, with more than a billion users.

However, these online photo collections are not just valuable to their owners, but to attackers seeking to unearth a gold mine of personal data, as the case of the 2014 celebrity nude photo hacks made clear. Unfortunately, security measures such as passwords and two-factor authentication may not be enough to protect these images anymore, as the online services storing these photos can themselves sometimes be the problem.

"There are many cases of employees at online services abusing their insider access to user data, like SnapChat employees looking at people's private photos," said John S. Koh, the lead author of the paper, who just finished his Ph.D. with professors of computer science Jason Nieh and Steven M. Bellovin. "There have even been bugs that reveal random users' data to other users, which actually happened with a bug in Google Photos that revealed users' private videos to other entirely random users."

A potential solution to this problem would be to encrypt the photos so no one but the proper users can view them. However, cloud photo services are currently not compatible with existing encryption techniques. For example, Google Photos compresses uploaded files to reduce their sizes,

but this would corrupt encrypted images, rendering them garbage.

Even if compression worked on encrypted images, mobile users of cloud photo services typically expect to have a way to quickly browse through identifiable photo thumbnails, something not possible with any existing photo encryption schemes. A number of third-party photo services do promise image encryption and secure photo hosting, but these all require users to abandon existing widely used services such as Google Photos.

Now Columbia Engineering researchers have created a way for mobile users to enjoy popular cloud photo services while protecting their photos. The system, dubbed Easy Secure Photos (ESP), encrypts photos uploaded to cloud services so that attackers—or the cloud services themselves—cannot decipher them. At the same time, users can visually browse and display these images as if they weren't encrypted. They presented their study, "Encrypted Cloud Photo Storage Using Google Photos," at MobiSys 2021, the 19th ACM International Conference on Mobile Systems, Applications, and Services, on June 30, 2021.

"Even if your account is hacked, attackers can't get your photos because they are encrypted," said Jason Nieh, professor of computer science and co-director of the Software Systems Laboratory.

ESP employs an image encryption algorithm whose resulting files can be compressed and still get recognized as images, albeit ones that look like black and white static to anyone except authorized users. In addition, ESP works for both lossy and lossless image formats such as JPEG and PNG, and is efficient enough for use on mobile devices. Encrypting each image results in three black-and-white files, each one encoding details about the original image's red, green, or blue data.

Moreover, ESP creates and uploads encrypted thumbnail images to cloud photo services. Authorized users can quickly and easily browse

thumbnail galleries using image browsers that incorporate ESP.

"Our system adds an extra layer of protection beyond your password-based account security," said Koh, who designed and implemented ESP. "The goal is to make it so that only your devices can see your sensitive photos, and no one else unless you specifically share it with them."

The researchers wanted to make sure that each user could use multiple devices to access their online photos if desired. The problem is the same digital code or "key" used to encrypt a photo has to be the same one used to decrypt the image, "but if the key is on one device, how do you get it to another?" Nieh said. "Lots of work has shown that users do not understand keys and requiring them to move them around from one device to another is a recipe for disaster, either because the scheme is too complicated for users to use, or because they copy the key the wrong way and inadvertently give everyone access to their encrypted data."

The computer scientists developed an easy-to-use way for users to manage these keys that eliminates the need for users to know or care about keys. All a user has to do in order to help a new device access ESP-encrypted photos is to verify it with another device on which they have already installed and logged into an ESP-enabled app. This makes it possible "for multiple trusted devices to still view encrypted photos," Nieh said.

"The need to handle keys, and handle them properly, has been the downfall of almost every other encryption system," Bellovin said.

The researchers implemented ESP in Simple Gallery, a popular photo gallery app on Android with millions of users. It could encrypt images from Google Photos, Flickr and Imgur without changes needed to any of these cloud photo services, and led to only modest increases in upload and download times.

"We are experiencing the beginning of a major technological boom where even average users move towards moving all their data into the cloud. This comes with great privacy concerns that have only recently started rearing their ugly heads, such as the increasing number of discovered cases of cloud service employees looking at private user data," Koh said. "Users should have an option to protect their data that they think is really important in these popular services, and we explore just one practical solution for this."

A number of companies have expressed interest in the new system. "We have a working implementation that we are releasing to developers and other researchers, but not yet to the general public," Koh said.

More information: John S. Koh et al, Encrypted cloud photo storage using Google photos, *Proceedings of the 19th Annual International Conference on Mobile Systems, Applications, and Services* (2021). DOI: 10.1145/3458864.3468220

Provided by Columbia University School of Engineering and Applied Science