April 2020

# A MORE SECURE DESIGN TO STORE AND ACCESS SENSITIVE PICTURES TAKEN BY A SMARTPHONE

HP INC



# A More Secure Design to Store and Access Sensitive Pictures Taken by a Smartphone


## Abstract

From time to time we hear of disasters of people accidentally leaking their sensitive pictures. It's surprising that users take so many digital pictures today but smartphone makers still store pictures in such an easy-to-access way. A design is proposed to automatically encrypt sensitive pictures and apply a strict authorization when accessing them.


## Problems Solved

Sensitive pictures are usually stored together with other normal pictures in a smartphone. They don't have extra protections. They are not encrypted and could be accessed via a hacking method. And, if anyone gets access to an unlocked phone, the person can then freely browse and use all stored pictures including sensitive ones. A better store and usage design is proposed to protect sensitive pictures from unauthorized use.

## Prior Solutions

1. Encrypt a whole phone.
   This prevents direct access to the smartphone storage by hardware\software hacking methods, but it slows down device performance. This also doesn't prevent improper use when someone can access an unlocked phone.
2. Use software to encrypt sensitive images.
   This requires users to specifically install and use special software. Users have to import\export pictures between the secure storage of the software and the original phone image storage. It’s very inconvenient and doesn’t provide protection if a user forgets to take action.

Surprisingly there are no other solutions!

## Description

A few methods are provided together to secure the storage and use of sensitive pictures.

**- Secure Album and Confidential Pictures**

A "Secure Album" is built into a mobile phone. It works like an "album" function most modern phones have - it is actually more like a tag or category and users may add pictures to one or more albums. Pictures added to Secure Album become Confidential Pictures. Confidential Pictures are stored in an encrypted way. They don't go to Recycle Bin when deleted, but are destroyed immediately or in a few minutes by users' settings. When removing Confidential Pictures from the Secure Album, an immediate authentication is required.

Additional access protection is provided to Confidential Pictures and will be explained later.

**- Secure Viewing**

Confidential Pictures are shown as totally black pictures with a red "lock" icon in the center when users browse all pictures. There are two ways to unlock and see the real pictures. (1) When tapping a single Confidential Picture, the system will ask for authentication. Passing it would unlock only the one Confidential Picture. If users leave the picture, the picture is locked again. (2) There is a button to unlock all Confidential Pictures and make them visible. The button asks for authentication.

In both methods, the phone system uses two possible ways to control when the viewing ends. (1) Showing users a timer. When the timer ends, all Confidential Pictures become locked again even when users are still using the phone. (2) The phone system uses its camera to monitor users' eyesight. If users look away from a phone screen for more than 5 seconds, Confidential Pictures will become locked again. This design ensures Confidential Pictures are hidden during the time gap between the point when users stop watching a phone and the point at which (e.g., 3 minutes) the phone is auto locked.

**- Separate Password**

A separate password can be set to protect Confidential Pictures. The authentication to view Confidential Pictures requires this separate password.

When sending a phone for repair, users don't give out this password and so Confidential Pictures remain secure.

When viewing or restoring a backup image of a phone, if the separate password is not given, Confidential Pictures will be inaccessible.

**- Auto Identify and Store Sensitive Pictures**

Modern image identification technology can identify many sensitive pictures like nudes. When a phone system detects a sensitive picture is taken, the picture will be added to the Secure Album automatically or ask for users' confirmation to do this.

Or, when a phone system is not capable of doing it, the system can provide a function to allow users to declare "the pictures taken in the following 10 minutes will be added to Secure Album automatically."

**- Forbid Forwarding or Saving Sensitive Pictures**

If using a communication application supporting Confidential Pictures to send a sensitive picture, senders can option to forbid receivers from saving or forwarding the picture.

If the phone system of a receiver also supports Confidential Pictures, it will stop the receiver from screen capturing a Confidential Picture if the sender desires that the receiver doesn't save it.

We may not be able to stop receivers from taking pictures of a phone screen directly but at least we can help prevent a direct spread.

## Advantages

A much more secure design is proposed to protect confidential pictures from leaking or improper access.

*Disclosed by Hsuan-Chieh Li, Shu-Min Chang and Tomax Tai, HP Inc.*