EI2023 MWSF-382

Making Digital Cameras Less Attractive Targets For Theft

University of Kentucky

Aggregate.Org UNBRIDLED COMPUTING

Henry Dietz & Oluwatofunmi Oyetan

Abstract

Cameras are easy targets for theft. They are expensive, small, usually carried in the open, and not easily identifiable when stolen. Unlike cell phones, cameras typically don't have passwords or other login procedures, so the full functionality is generally available to anyone with physical access to the camera, and stolen cameras behave indistinguishably from ones operated by their legitimate owners. The current work examines various methods for making cameras less attractive targets for theft without significantly increasing either camera cost or the complexity of the user interface and interactions. Many of the new methods use various forms of anomalous behavior identification to enable the camera to passively recognize when it is likely that the person operating the camera is not the owner.

Goals

Do not interfere with normal user operation

The key to this is the concept of **Anomalous Behavior Detection**: being able to passively recognize when something is not as usual, for example, that the user is not the owner.

Render the stolen equipment worthless to the thief

There is little motivation for theft where there is no profit to be made from equipment use or sale, nor access to the owner's personal information.

Aid in recovery of the stolen camera

This has been the primary goal in most prior work, but most approaches catch the potentially naive and innocent unauthorized user rather than the thief.

Key

- 🦖 Existing Methods
- 👧 Methods partly explored by others
- UK Methods based on our earlier work
- 🚀 Relatively unexplored methods

- 🦖 Internet search for images from the same camera based on EXIF data (e.g., *StolenCameraFinder.com*)†
- 👧 Internet search for images from the same camera, based on other forensic markers
- 🦖 Add-on trackers (e.g., *AirTag*, *SmartTag*, *Tile Pro*, *Chipolo*, and *Cube Shadow*)
- 🦖 In-camera WiFi or BlueTooth for tracking, actively calling home
- 🚀 Wireless network population familiarity to recognize owner (e.g., seeing owner's cell phone)
- 🦖 Conventional passwords and other types of mandatory login sequences (e.g., HCI events during boot)
- 🚀 Mandatory login required only when triggered by anomalous behavior detection*
- 🦖 User biometrics (e.g., operator face ID)
- 🚀 Photo subject biometrics (e.g., familiar faces in some images)†
- 🚀 Photo subject pattern/style recognition to recognize owner†
- 🚀 HCI action history statistics (e.g., when used, modes used, etc.) to recognize owner†*
- UK Camera shake profile to recognize owner*
- UK Camera orientation profile to recognize owner†*
- 🚀 Battery charge/recharging pattern to recognize owner†*
- 🚀 Thermal sensors to recognize owner†*
- 👧 Encrypted file storage with automatic decryption in camera enabled only for owner
- UK Recognition of which removable lens is attached by lens ID or out-of-focus PSF analysis†*

† EXIF Properties

No one field identifies the user, but statistics over many EXIF fields can. E.g., image orientation frequencies for a user are surprisingly consistent:

Image Set	0°	90°	180°	270°
Alaska	6843	550	0	247
Hawaii	2716	223	1	62
Paris	3035	689	14	343
Turkey	3398	413	0	57

* Experimental Prototypes

Prototyping using CHDK (Canon Hack Development Kit) to reprogram Canon PowerShot cameras confirms that cost is feasible for in-camera implementation.