InformaCam

SecureSmartCam Sub-Project

Specification

Harlo Holmes

Nathanial Freitas

0. Preliminaries

      The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL

      NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED",  "MAY", and

      "OPTIONAL" in this document are to be interpreted as described in

      RFC 2119.

* 1. Notation and encoding

INFORMA : The proposed Android application for compatible devices.

ACQUIRED DATA: All data gathered by the INFORMA application required for successful verification of the source image.

AUTHENTICATION DATA: All data that must be provided by the USER in order to confirm the validity and authenticity of a SOURCE object created with INFORMA. AUTHENTICATION DATA is unique to each user, and is generated with the SPONSORING ORGANIZATION upon first use of INFORMA, and must persist on the USER’S DEVICE.

BUNDLE: A unit of measurement in a digital object's ACQUIRED DATA.  One or more BUNDLES comprise the object's total ACQUIRED DATA.

SOURCE: The digital object captured by the INFORMA application, either digital video or image, depending on usage.

USER: The person or persons operating a device equipped with INFORMA for the purpose of recording a digital image or video.

SPONSORING ORGANIZATION: The entity receiving and hosting SOURCES captured with and submitted via INFORMA.

DEVICE: A smartphone or other compatible device with the INFORMA encoder installed.

DECODER: A compatible device used to decode digital objects rendered by INFORMA.

IMAGE REGION: A rectangular region within the SOURCE image that has been manipulated by INFORMA by the USER.  IMAGE REGIONS contain METADATA pertinent to the IMAGE REGION only, and can be manipulated visually by INFORMA'S various FILTERS.

FILTER: A visual or audio process that may change the material nature of a digital object.

METADATA: Human and/or machine-readable descriptions of ACQUIRED DATA.

HASH: A fixed-length bit string encoded to represent a larger set of data.

WATERMARK: A visual or audible symbol that can be resolved to pertinent information.  A WATERMARK is ostensibly material-- they have physical characteristics (sound, visual information) but are generally imperceptible by the human faculties of vision or hearing, and therefore can go unnoticed by USERS.

TIMESTAMP: The Unix timestamp as understood by the DEVICE.

GLOBAL TIME: The Unix timestamp as understood by the SPONSORING ORGANIZATION.

LAT/LNG: The latitude/longitude pair adhering to the GPS standard.

CELL ID: The identification code of the cellular tower nearest to the DEVICE.

ALTITUDE: The value deduced by the DEVICE'S software altimeter.

BEARING: The cardinal direction of the DEVICE, deduced by the DEVICE'S software compass.

IMEI: The unique handset identification of the DEVICE.

* 1. Security parameters

1. System overview

INFORMA is a tool for capturing, and visually manipulating digital photos and videos with enhanced metadata that may be used in forensic analysis of the SOURCE object at a later time. INFORMA employs certain methods to acquire and inscribe METADATA into and onto the SOURCE object so it is an infungible component of the object. To insure the authenticity of the object’s METADATA, AUTHENTICATION DATA must be linked to the DEVICE upon first installation/use of the system.

* 1. User Stories
  2. User interface

INFORMA consists of a CLIENT application (on the DEVICE) capable of capturing images and video. Once a photo or video is captured, the USER interacts with an easy-to-use visual editor to make required changes to the SOURCE. Once the desired effect has been reached, the USER may transmit the SOURCE object to the server of the SPONSORING ORGANIZATION, where it is stored in its most complete form for further viewing and analysis. USER may also publicly share (via any chosen method; email, MMS, or through other broadcast channels like Twitter, Facebook, etc.) a version of the media stripped of all sensitive information (both visual information and metadata) as one would normally share such objects.

* 1. Sensory and atmospheric data

BUNDLE(S) comprising the SOURCE'S ACQUIRED DATA must include the following parameters:

* Current TIMESTAMP
* DEVICE identification
* USER'S public key
* IMAGE REGIONS created in the SOURCE
* Current LAT/LNG of DEVICE

Additionally, BUNDLES should include the following parameters:

* CELL ID of DEVICE
* ALTITUDE
* BEARING

BUNDLE(S) comprising the SOURCE'S ACQUIRED DATA must be captured instantaneously from the moment of inscription.  In the case of digital images, a BUNDLE is created at the moment of inscription, which occurs when the shutterPressed function is called on the device.  In digital video, BUNDLES must be captured at the following instants:

* When the USER begins a recording
* When the USER terminates a recording
* Every 5 seconds of recorded video, at a regular interval
* When any of the parameters comprising a full BUNDLE of ACQUIRED DATA changes

1. Metadata Formats/Specs/Schema

Schematic for a SOURCE object's ACQUIRED DATA should be defined as follows:

1. Embedding strategies

A SOURCE object contains one or more BUNDLES of ACQUIRED DATA which must be embedded into the SOURCE in a persistent way, so as to be decoded and analyzed by DECODER or other DEVICE.  The method by which ACQUIRED DATA are embedded into the SOURCE object comprises both cryptographic and steganographic approaches.

* 1. Embedding metadata in digital image objects

After the SOURCE has been created on the DEVICE, its ACQUIRED DATA must be resolved to a HASH.  The resulting HASH must be physically added to the SOURCE image as an invisible WATERMARK.

* 1. Embedding metadata in digital video objects

Given the audio/visual nature of video, both the source video's audio and video track can be used to store authentication data.  In additon to techniques of embedding visual watermarks into the image at certain frames, INFORMA should also use an audio watermark, encoded in tones above the human-audible spectrum as an internal checksum for the video's frames.  INFORMA should log ACQUIRED DATA in a temporary buffer, to be flushed to a HASH at regular intervals.  A tonal representation of this HASH should be embedded into a separate audio track in the SOURCE.  Combining these two techniques minimizes the need to generate visual WATERMARKS for each video frame.

1. Cryptographic

SOURCE objects must contain encrypted data that only the SPONSORING ORGANIZATION may decrypt.

* 1. Initiating and authenticating DEVICES

Upon first use of INFORMA, the DEVICE must be registered to the SPONSORING ORGANIZATION. This inaugural step must be taken to establish certain fixed points of reference that must be used each time the DEVICE transmits an object.

The following permanent points of reference will be provided by the DEVICE and exchanged upon inauguration:

A unique identifier generated by the DEVICE

* TIMESTAMP (as understood by the DEVICE)
* IMEI
* PUBLIC KEY

This data is transmitted to the SPONSORING ORGANIZATION’S server using a 3-step asymmetric key exchange (employing commutative ciphers).

* 1. SOURCE object Signing, Encryption, and Transmission

With each subsequent transmission of SOURCE objects between a DEVICE and the SPONSORING ORGANIZATION, the DEVICE will encrypt the SOURCE object using a one-time pad (generated on the DEVICE). Transmission protocol has two steps:

* The transmission of the one-time pad using a 3-step asymmetric key exchange (where the pad is the payload)
* The subsequent transmission of the object in its entirety, encrypted by the one-time pad
  1. Pixel Region Hashing
  2. Media File Hashing

1. Decoding InformaCam objects
2. Storage and transmission of InformaCam data
3. Legal Opinions