C12 Social Network Image Ballistics Through Automatic Reverse Engineering

Oliver Giudice, PhD, Roma 00044, ITALY; Antonino Paratore, MS*, ICT Lab S.R.l. Spinoff of Università di Catania, Catania 95125, ITALY; Sebastiano Battiato, PhD*, Università di Catania, Catania 95125, ITALY; Luca Guarnera, MS*, Università di Catania, Catania 95125, ITALY*

Learning Overview: After attending this presentation, attendees will be aware of new possibilities in digital images forensic analysis—the so-called social image ballistics, a technique that derives its name from the traditional ballistics science that attempts to identify the weapon that exploded a certain projectile, exploiting traces left on the projectile itself or on cartridges. Attendees will discover how to reconstruct the history of a digital image by understanding how they are manipulated by different social networks. Moreover, attendees will be able to identify the device that uploaded the original image and the corresponding timeframe.

Impact on the Forensic Science Community: This presentation will impact the forensic science community by serving as a key aspect for different fields of investigation (e.g., child pornography, terrorism, etc.) and, in general, for all investigations in which it is necessary to verify the origin of an image to the user profile who published it.

The software utilized by social networks is known to alter images for bandwidth, storage, and layout reasons. Recent works have demonstrated that, although the platform heavily modifies an image, this processing leaves traces on the image itself. [1-4] Previous works have discussed those alterations and proposed a classification solution able to identify whether an image was processed by one of the ten social network services taken into account.[4]

Understanding the origin of a digital image in the era of social networks means analyzing all traces left by the social network software. Every component of a digital image will be discussed and the corresponding manipulation performed by ten social networks will be presented (filenames, Jpeg-structures, meta-data). This process may be considered a reverse engineering of social network image processing modules. Toward this goal, an automatic reverse engineering solution will be discussed.

The Classification Engine solution limit lies in its reference dataset, where the images analyzed presented fingerprints of social networks related to the time at which the dataset itself was built.[4] Social networks are always changing their software functioning and parameters. Thus, the dataset on which the classification engine was built could become obsolete (and in turn the Classification Engine as well). To mitigate this, it is possible to build a software solution (Continuous-Collecting Social Images) able to automatically and periodically conduct the collection and reverse engineering analysis of a social network by storing the images and all collected meta-data in a specific database and extracting new fingerprints. The automatic image collection performed during a period of one year allowed improvement in the results achieved by the Classification Engine, not only for the classification task, but also for developing additional information regarding the timeframe in which an image was supposedly uploaded.[4]

Finally, a use-case scenario of this type of digital image analysis will be presented and applied to the forensic and investigative domains.

Reference(s):

1. M. Moltisanti, A. Paratore, S. Battiato, L. Saravo. *Image Manipulation on Facebook for Forensics Evidence*. ICIAP 2015, LNCS 2015.
2. A. Castiglione, G. Cattaneo, A. De Santis. *A Forensic Analysis of Images on Online Social Networks*. Third International Conference on Intelligent Networking and Collaborative Systems (INCoS), 2011.
3. R. Caldelli, R. Becarelli, I. Amerini. *Image Origin Classification Based on Social Network Provenance*. IEEE Transactions on Information Forensics and Security, 2017;
4. O. Giudice, A. Paratore, M. Moltisanti, S. Battiato. *A Classification Engine for Image Ballistics of Social Data*. ICIAP 2017, LNCS 2017

Social Media Ballistics, Multimedia Forensics, Source Identification