Image origin classification based on social network provenance

Abstract

- Recognizing information about the origin of a digital image has been individuated as a crucial task to be tackled by the image forensic scientific community.
- Understanding something on the previous history of an image could be strategic to address any successive assessment to be made on it:
- knowing the kind of device used for acquisition or, better, the model of the camera could focus investigations in a specific direction.

- Sometimes just revealing that a determined post-processing such as an interpolation or a filtering has been performed on an image could be of fundamental importance to go back to its provenance. This paper locates in such a context and proposes an innovative method to inquire if an image derives from a social network and, in particular, try to distinguish from which one has been downloaded. The technique is based on the assumption that each social network applies a peculiar and mostly unknown manipulation that however leaves some distinctive traces on the image; such traces can be extracted to feature every platform

EXISTING SYSTEM

- In this context, both the identification of the origin of a digital content and the reconstruction of its history are crucial issues for disciplines such as multimedia forensics and security.
- In fact, recovering as much information as possible about the originating device or on the processing that has been applied could be fundamental to comprehend if, for instance, an image is authentic or has been manipulated to change its initial representation and meaning.

- In particular, it could be of basic importance to succeed in reconstructing the history of a specific digital document that might help in addressing an on-going investigation and/or excluding some suspected subjects. In the case of an image or a video, the aim of retracing its history can be achieved primarily by resorting at the metadata (e.g. EXIF) contained within the file itself but this grants only a limited degree of reliability being them easily modifiable or even erasable.

PROPOSED SYSTEM

- In this paper, we have proposed a novel methodology to distinguish images coming from different social networks. The main contributions of the actual work are the following:
- the introduction of the usage of feature-based descriptors able to allow a distinction among the processing suffered by the images when uploaded on a specific social net-work.
- the definition of a technique based on such features which by resorting at trained classifiers is able to identify the social platform of provenance and also to detect the quality factor before uploading.

- the achievement of satisfactory performances in terms of SN source identification.

HARDWARE REQUIREMENTS

- System : Pentium IV 2.4 GHz.
- Hard Disk : 40 GB.
- Floppy Drive : 1.44 Mb.
- Monitor : 15 VGA Colour.
- Mouse : Logitech.
- Ram : 512 Mb.

SOFTWARE REQUIREMENTS

- Operating system : Windows XP/7.
- Coding Language : ASP.net, C#.net /java

Conclusion

- This paper locates in such a context and proposes an innovative method to inquire if an image derives from a social network and, in particular, try to distinguish from which one has been downloaded. The technique is based on the assumption that each social network applies a peculiar and mostly unknown manipulation that however leaves some distinctive traces on the image; such traces can be extracted to feature every platform.

- By resorting at trained classifiers, the presented methodology is satisfactorily able to discern different social network origin. Experimental results carried out on diverse image datasets and in various operative conditions witness that such a distinction is possible. In addition, the proposed method is also able to go back to the original JPEG quality factor the image had before being uploaded on a social network.

Reference

- [1] M. Stamm, M. W., and K. Liu, "Information forensics: An overview of the first decade," Access, IEEE, vol. 1, pp. 167–200, 2013.
- [2] M. Barni, "A game theoretic approach to source identification with known statistics," in 2012 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), March 2012, pp. 1745–1748.
- [3] N. Khanna, G. T.-C. Chiu, J. P. Allebach, and E. J. Delp, "Forensic tech-niques for classifying scanner, computer generated and digital camera images," in Proc. of IEEE ICASSP, Las Vegas, USA, 2008.