PhD inInformation Technology and Electrical Engineering

Università degli Studi di Napoli Federico II

PhD Student: Francesco Marra

XXX Cycle

Training and Research Activities Report – First Year

Tutor: Carlo Sasone – co-Tutor: Luisa Verdoliva

1. Information

PhD Student : Francesco Marra

MS title: Computer Engineering – University of Naples Federico II

PhD cycle: XXX – ITEE University of Naples Federico II

Fellowship type: PhD student gran

Tutor: Carlo Sansone – **co-Tutor:** Luisa Verdoliva

I received my MS degree (cum laude) in Computer Engineering from the Univesità degli Studi di Napoli Federico II.

I've been Research Fellow at University of Cagliari from October 2013 to October 2014, in collaboration with SIVA and GRIP group of University of Naples. In this period I published the following conference paper:

F. Marra, F. Roli, D. Cozzolino, C. Sansone, L. Verdoliva, "Attacking the triangle test in sensor-based camera identification," in *Image Processing (ICIP), 2014 IEEE International Conference on* , vol., no., pp.5307-5311, 27-30 Oct. 2014

2. Study and Training activities

Courses

(1) Ad hoc Course, "Project Management", Jan-2015 (3 CFU)

(2) Ad hoc Course, "Elettromagnetismo e Relatività", Feb-2015 (da completare) (4 CFU)

(3) Modulo mutuato, "Elaborazione Numerica dei Segnali", Mar-2015 (6 CFU)

(4) Ad hoc Course, "Fondamenti di Analisi Funzionale", Mar-2015 (7 CFU)

Seminars

(1) Modelli matematici e calcolo scientifico nell'ingegneria e nell'innovazione tecnologica - Dipartimento di Matematica ed Applicazioni "Renato Caccioppoli" e la Scuola Politecnica e delle Scienze di Base - Unina- 15 april 2015

(2) Social Signal Processing: understanding social interactions through nonverbal behavior analysis – Prof. Alessandro Vinciarelli – 5 May 2015

(3) Partial possibilistic regression path modeling – Rosaria Romano – 20 April 2015

External courses

(1) PhD Course: "Statistical Signal Processing for Multimedia Forensics and Security" - Prof. Fernando Perez Gonzales at Politecnico di Milano, Dipartimento di Elettronica, Informazione e Bioingegneria - 25 al 29 May 2015.

Year	Modules	Seminars	Research	Tot.
1	16 (20)	5.2 (5)	35(35)	56.2 (60)*
2	(11)	(5.8)	(45)	61.8(60)
3	(3)	(1)	(58)	63 (60)
Tot.	30 (30-70)	12 (10-30)	138 (80-140)	180 (180)

* Ad-hoc module: "Elettromagnetismo e relatività" – 4 CFU (to acquire)

3. Research activity

Digital forensics is a branch of forensic science concerned with the use of digital information produced, stored and transmitted by computers as source of evidence in investigations and legal proceedings [1].

When the digital information we deal are images, we talk about Digital Image Forensics.

Questions regarding image authenticity are of growing relevance, especially in contexts where nowadays' multimedia society bases important decisions on them. Particular attention has to be drawn to courtroom applications, in which the authenticity of photographs as pieces of evidence deserves utmost importance [2].

The area of digital image forensics can be broadly divided into two branches:

- **image integrity detection**, for determining if a digital image has undergone malicious post-processing or tampering;
- **image source identification**, with which determines whether an image is taken from a given camera or model.

In my study, I focused mainly on studying about the image source identification. The identification problem could be done on various level of granularity: we can distinguish between methods to determine the *type* of acquisition device *(Computer generated, digital camera, scanner)*, its *make/brand* or *model*, and ultimately also the actual *device* itself.

Of course, working with the specific source camera identification is desirable and gives good result with state of the art methods, but often is not possible without the collaboration of the camera owner and, in any case, is extremely time-consuming. A more viable intermediate step is the identification of the camera model. Finding the model may significantly narrow the search, which can be completed also by more conventional methods.

Camera model identification is made possible by the distinctive traces left in images as a result of the unique combination of in-camera processing steps like demosaicing and JPEG compression.

The majority of the features used for this problem, are evaluated globally on the whole image (both original and high-pass filtered) or a decimated version of it, if wavelet sub-bands are considered [3][4][5]. However, in order to capture subtle image patterns which may correspond to discriminative features, it is important to consider local features, extracted from a small neighborhood of each pixel of the image, as it happens for the work of Xu et al. [6], where LBP features are evaluated both on the original image and on some residuals, and gives promising results.

In my work [7] I show that co-occurrence based local features, computed on gray-scale image residuals and proposed originally in [8] for steganalysis, may represent a valuable tool for this task. These kinds of feature outperform all previous method on a subset of the Dresden image database [9], either using whole images or a cropped version of it for reducing the computation time.

After that, I extended this work, using all the Dresden dataset and the color information, and testing the robustness of the features on jpeg compression, resizing and cropping, obtaining very good results.

References

[1] R. Kaur, A. Kaur : Digital Forensics In International Journal of Computer Applications V.50 – No.5, 2012

[2] T. Gloe, M. Kirchner, A. Winkler, R. Bohme: Can we trust digital image forensics?" In Multimedia '07: Proceedings of the 15th international conference on Multimedia, p. 78-86, 2007. ACM Press

[3] M. Kharrazi, H., Sencar, N. Memon: Blind source camera identification. In: IEEE International Conference on Image Processing. (2004) 709-712

[4] O. Celiktutan, B.S., Avcibas, I.: Blind identification of source cell-phone model. IEEE Transactions on Information Forensics and Security 3(3) (2008) 553-566

[5] T. Gloe: Feature-based forensic camera model identification. In: LNCS Transactions on Data Hiding and Multimedia Security VIII. Volume 7228. (2012) 42-62

[6] G. Xu, Y. Shi: Camera model identification using local binary patterns. In: IEEE International Conference on Multimedia and Expo. (2012) 392-397

[7] F. Marra, G. Poggi, C. Sansone, L. Verdoliva - "Evaluation of Residual-Based Local Features for Camera Model Identification" at BioFor - New Trends in Image Analysis and Processing -- ICIAP 2015 Workshops

[8] J. Fridrich, J. Kodovsky.: Rich models for steganalysis of digital images. IEEE Transactions on Information Forensics and Security 7 (2012) 868-882

[9] T. Gloe, R. Bohme: The Dresden image database for benchmarking digital image forensics. Journal of Digital Forensic Practice 3(2-4) (2010) 150-159

4. Products

Conference papers

F. Marra, G. Poggi, F. Roli, C. Sansone, L. Verdoliva "Counter-forensics in machine learning based forgery detection" - SPIE Media Watermarking, Security and Forensics

F. Marra, G. Poggi, C. Sansone, L. Verdoliva - "Evaluation of Residual-Based Local Features for Camera Model Identification" at BioFor - New Trends in Image Analysis and Processing -- ICIAP 2015 Workshops

Journal papers

F. Marra, G. Poggi, C. Sansone, L. Verdoliva - "Camera model identification through SPAM features" at Multimedia Tools and Applications, 2015 (**submitted)**

5. Conferences and Seminars

IEEE International Conference on Multimedia and Expo (*ICME 2015*) at Turin. Jun 29 - Jul 3, 2015.