Forensic Imaging for Art Diagnostics. What Evidence Should We Trust?

A Pelagotti¹,⁴ A Piva², F Uccheddu³, D Shullani², M F Alberghina³, S Schiavone⁵, E Massa¹ and C M Menchetti¹
¹ Italian National Institute of Applied Optics, INO-CNR, L.go E. Fermi 6, 50125 Florence, Italy, email: anna.pelagotti@ino.it
² Department of Information Engineering University of Florence, via S. Marta 3, 50139 Florence, Italy
³ Department of Industrial Engineering University of Florence, via S. Marta 3, 50139 Florence, Italy
⁴ Art-Test, via S.Spirito 11 50123 Florence, Italy
⁵ S.T.A-Test, Via Stoviglilai, 88, Niscemi (CL), Italy

Abstract. Diagnostics digital images are often used to assess artworks. However, as all digital images they are also concerned by the issue of integrity. Computer vision techniques can be employed to obtain physical evidence of possible tampering. In this paper we explore the possibility to apply state of the art forensic algorithms to typical painting diagnostic images, taking into consideration real case studies. State of the art algorithms have been applied to genuine and modified diagnostic images to detect if, and how, forgeries of such images could be automatically detected and documented. To the best of our knowledge this is the first time that such investigation is made. Results of the aforementioned tests prove that automatic assessment of the integrity of diagnostic images is challenging and that there are no reliable solutions currently available.

1. Introduction
In the process of authentication and attribution of artworks, scientific evidence is having an increasingly important role. Together with material analyses, diagnostic images often provide crucial information. Infrared reflectography, as well UV fluorescence and X-rays images are frequently acquired and analysed in order to evaluate whether e.g. a painting is a later copy or whether instead it can be considered an original by a specific author. Practically, such diagnostic images are often produced by specialised laboratories and then provided to professionals like (technical-) art historians. Such images can even be hold up in court as evidence in a litigation. However, as all digital images, also art diagnostic images are concerned by the issue of integrity. Integrity relates to the fact that the acquisition process of such digital images and any possible post processing applied to them, has not significantly modified them. Specific computer vision techniques, i.e. forensic techniques, have been long employed to obtain evidence of possible tampering in photographs. To the best of our knowledge this is the first time that forensic imaging techniques are applied to art diagnostic images.
2. Digital Art Diagnostic images and their technical evaluation for authentication and attribution.

Two paintings have been taken as case studies. The first one, belonging to the Museo Diocesano di Arte Sacra of Nicosia (Italy) (see Fig. 1a), has an uncertain attribution and it is considered either a copy by an unknown artist of a painting by Pietro Novelli (currently in Galleria Regionale di Palazzo Abatellis – Palermo, Italy), or a second version by Novelli himself. The second one is the painting “Saint Francis and Saint John”, recently attributed to El Greco (see Fig. 2a). In the following we further describe them and the evidence, as attainable using their X-rays images, on which their attribution is based, so to elucidate which ones are the relevant features generally being used for the purpose of attribution.

![Figure 1: Madonna delle Grazie con i Santi Rosalia e Giovanni Battista](image1)

*Figure 1.* a) “Madonna delle Grazie con i Santi Rosalia e Giovanni Battista” painting on canvas (205 × 158cm) Museo Diocesano di Arte Sacra - Nicosia (Italy), b) X-rays images of some details of the artwork

![Figure 2: Saint Francis and Saint John](image2)

*Figure 2.* a) “Saint Francis and Saint John” by El Greco, painting on canvas (110 × 86 cm) Uffizi Museum, Florence, Italy, b) X-rays image of the painting.
On the first case study, the pre-restoration diagnostic analyses revealed details of the execution technique confirming its closeness to that of Pietro Novelli [1]. The X-rays show a careful use of highlights, thin brushstrokes of pure white pigment (white lead), spread with a flat tip brush for the volumetric rendering of figurative details (eyes, nose, mouth, hands) and drapery contours. The dark background and the shaded areas are regular and thinner, the figurative details and especially the flesh tones in the areas of maximum light have a greater body and thickness and are characterized by a curvilinear shape giving an important 3D feature. Details that are no longer visible to the naked eye due to the darkening or thinning of the pictorial layout become here clearly legible. The details revealed by diagnostic investigation are exactly coinciding with those of the painting of the same subject and of undisputed attribution to Pietro Novelli of the Regional Gallery of Palazzo Abatellis (Palermo).

Also for the painting by El Greco, more than one version of this same subject exist. In this case there are many signs of undisputed autography that are revealed by the performed scientific analyses [2]. In the X-rays image we find how El Greco uses many brushes (including their handle) of different types and sizes, from large to very fine, and how brush strokes, charged and discharged, are intertwined in all directions. Their relative radiopacity is also peculiar to the paintings of the master of Candia, where the flesh, thanks to the presence of lead white, reveals dense and persistent brush strokes. In addition, documented in the X-rays image, there are numerous variations, or “pentimenti”, i.e. parts of the composition that were initially different from the version which is currently visible. The most evident one concerns the lower end of Francesco's coat, this has in fact been lengthened, as shown by the presence of the Saint's right foot up to the ankle in the X-ray image. This part was then covered in the final version. It should be noted that in the other known paintings where the same subject is repeated, the foot is always partially covered by the clothing.

2.1. Acquisition methods

Most of the scientific evidence that is currently employed in the attribution of paintings consists of digital images. However, these images are not digital photos. Infrared images can be acquired using a digital scanner, rather than a commercial digital camera, and the resulting images consist of an array of b/w points each independently imaged, 12bit/pixel, arranged in a RAW format. They can be provided in a compressed format or not. UV images can be the result of a multispectral acquisition method and therefore produced as a result of a mathematical computation, making use of a number of different images, and X-rays images can be digitized b/w films or b/w images acquired with a direct method. Also these are provided in a number of formats. The JPG format, being mostly lossy, is generally avoided, to safeguard all of the valuable image information.

2.2. Image processing applied to simulate malicious altering of the diagnostic images

Generally, there could be two reasons to alter a diagnostic evidence: to help supporting an attribution or to contribute to dismiss it.

As was described in paragraph 2, often, when comparing two similar paintings and discussing which one is the original and which one is the copy, diagnostic images are analysed and the indication of a previous, hidden and different version, visible in the X-rays or in the InfraRed image, a so called “pentimento”, is used as proof of a creative process, and therefore of authenticity.
Figure 3. a) The original detail of an X-rays image of the “Saint Francis and Saint Giovanni” painting b) the tampered detail using the “simple approach”, the detail of a hand (indicated by the blue arrow, has been copy-moved to a new position

Figure 4. a) The original detail of an X-rays image of the “Madonna delle Grazie con i Santi Rosalia e Giovanni Battista” b) the tampered detail by an Advanced approach using a number of tools of the Adobe Photoshop® suite. The details now show a realistic “pentimento” for the head of the Madonna.
In order to test the option of X-rays images being manipulated to artificially introduce a “pentimento”, a new image has been produced, using the original X-rays image and “copy-move”-ing a detail of it (see fig. 4) using Adobe Photoshop®. Clearly such resulting image would not have deceived any expert, however, the one in fig. 5 is much more realistic and could have been considered unprocessed. In order to obtain this last image a number of processing tools have been used, all of them available in the Adobe Photoshop® suite. We would refer to the first processing as “simple” and the second as “advanced”.

3. Multimedia Forensics
Multimedia Forensics [3, 4, 5, 6], relies on the observation that each phase of the image history, from the acquisition process to its storing in a compressed format and to any post-processing operation, leaves a distinctive trace on the data, as a sort of digital fingerprint. It is then possible to identify the source of the digital image or determine whether it has been modified, by detecting the presence, the absence or the incongruence of such features intrinsically tied to the digital content itself. Therefore, the founding idea of image forensics is that inherent traces (like digital fingerprints) determined by the history of a digital image [5] can be extracted and analysed for understanding the integrity of a digital content. In this study, we focused on forensic tools that evaluate traces left during both the coding and the post-processing or editing phases of a digital image.

3.1. Coding Traces
Nowadays the most common image compression algorithm is JPEG. It is used to reduce the image storage space while maintaining a high perceived quality. A tampered JPEG image can hide a double quantization trace. It shows up when a portion of uncompressed pixels\(^1\) is pasted into a JPEG image, and the final result is JPEG saved, the untouched region undergoes a double compression. This causes its DCT coefficients to be doubly quantized, leaving a characteristic trace in their statistics. The forensic tools that focuses on image coding traces are:

- ADQ2 [7]: evaluates aligned double JPEG compression and returns a map giving the probability of being tampered.
- NADQ [8]: evaluates aligned and non-aligned double JPEG compression and returns a map giving the likelihood of being doubly JPEG compressed.
- JPEG Quantization Tables [15], [16]: are specific of the device/software that implements the JPEG algorithm and can be used to verify the tool that last saved the image (device or software). It is important noting that this is a fragile trace since it is possible to re-compress JPEG images using quantization tables associated with a known device signature.

3.2. Post-processing Traces
Editing tools like Adobe Photoshop® or GIMP® are vastly used for image enhancement but also image tampering. The most common malicious alterations performed by editing tools are “copy-move” and “splicing”. The copy-move attack clones a portion of an image and adds it in a different position. The splicing attack copies an image patch onto a different image. Both of them can be used when trying to modify a diagnostic image e.g. to simulate a “pentimento” or a particular painting technique.

The forensic tools that focuses on image editing traces are:

- Splicebuster [11]: performs blind splicing detection and localization. It computes a block-based feature based on residuals high-pass filtering, residual quantization and the co-occurrences histogram. Statistics are also performed to discover where the features computed locally depart from the model, pointing to some possible image manipulation.
- Clone-block [13], [14]: locates replicated areas of an image, by performing for each pixel a feature vector based on Zernike moments [13]. Then it searches similar pixel pairs using the

\(^1\) or pixels that have been compressed according to a different grid
PatchMatch algorithm [14]. Matching pixels whose distance is very close to zero identify the possible duplicated regions. Is worth noting that the algorithm is more reliable when cloned areas are just copied, e.g. resizing and/or rotation are not performed to the clone patch.

- **Clone-Keypoints [12]:** looks for unique image locations carrying information of image content (keypoints) that match. In order to find regions with high similarity, each detected keypoint is represented as a feature vector consisting of a set of image statistics. These feature vectors are matched using the K-Nearest Neighbors (KNN) algorithm.

- **SIFT [10]:** is a keypoint-based method that uses the scale-invariant feature transform (SIFT) as a pixel descriptor. First, it builds clusters from the locations of detected features and then uses RANSAC to estimate the geometric transformation between the original area and its copy-moved version.

4. Results

4.1. Simple scenario

SIFT algorithm fails to detect manipulations. Only in the case of a “copy-move” tampering on the El Greco painting, it identifies one key-point, as shown in Fig. 5a. ADQ2 considers all the images analysed in this scenario as not tampered. NADQ applied to the copy-move-copy on El Greco identifies the white background as single compressed and the part related to the painting as overall tampered. Splicebuster is able to identify one of the manipulations as depicted in Fig. 5c where the hand-copy is clearly visible in warm colours. Similarly to the “Advanced” scenario the JPEG QT tool identifies the possible tampering from Adobe Photoshop or the NIKON D3000 device. The best performance on this scenario are given by the Clone tools, Fig. 5b and Fig. 5c, where are shown the block and keypoint localization maps over the copy-move-airbrush manipulation of “El Greco” painting.

4.2. Advanced scenario

The performance described in Table 1 show that most forensic tools fail to identify such manipulations. Only the analysis of the JPEG quantization tables show the compatibility of such contents with QTs usually used by the NIKON D3000 and Adobe Photoshop software suggesting a possible non authentic content.

Table 1. FORENSIC TOOLS PERFORMANCE OF MANIPULATION DETECTION.

| Forensic tool employed | Trace examined | “Simple” post-processed images | “Advanced” post-processed images |
|------------------------|----------------|--------------------------------|---------------------------------|
| ADQ2                   | JPEG CODING    | NO TAMPERING DETECTED          | NO TAMPERING DETECTED           |
| NADQ                   | JPEG CODING    | NO TAMPERING DETECTED          | NO TAMPERING DETECTED           |
| JPEG QT                | JPEG CODING    | NO TAMPERING DETECTED          | NO TAMPERING DETECTED           |
| Splicebuster           | IMAGE EDITING  | Adobe Photoshop OR NIKON D3000 DETECTED | Adobe Photoshop OR NIKON D3000 DETECTED |
| Clone-block            | IMAGE EDITING  | Blocks map DETECTED            | NO TAMPERING DETECTED           |
| Clone-keypoints        | IMAGE EDITING  | Keypoints map DETECTED         | NO TAMPERING DETECTED           |
| SIFT                   | IMAGE EDITING  | NO TAMPERING DETECTED          | NO TAMPERING DETECTED           |
Figure 5. Visual results of: a) SIFT, only one point identified; b) Clone block, the two related areas are correctly identified; c) Splicebuster, the tampered area is correctly identified, however with some false positives; d) Clone-keypoints, some of the key copied points are correctly identified

5. Conclusions and future work
As illustrated, none of the state of the art forensic methods used to assess the integrity of images, mainly developed for photographs acquired with commercial cameras are able to cope with diagnostic images. These are inherently dissimilar, both because of the acquisition devices and techniques employed and of non-compressed format. Therefore, specialized algorithms should be developed to be able to automatically assess the possible tampering in these cases.
6. References

[1] Mauro Sebastianelli, Technical and scientific research as an aid to art historians in the attribution of art works, Conservation Studies In Cultural Heritage, Vol 16 (2016).

[2] A. Pelagotti, L. Venerosi Pesciolini, “San Giovanni Evangelista e San Francesco d’Assisi di El Greco. Bigi petrosi e bianchi taglienti” in Arte e Dossier 285, Giunti, 2012.

[3] T. Van Lanh, K.-S. Chong, S. Emmanuel, and M. S. Kankanhalli, “A survey on digital camera image forensic methods,” in 2007 IEEE international conference on multimedia and expo. IEEE, 2007, pp. 16–19.

[4] H. Farid, “Image forgery detection,” IEEE Signal processing magazine, vol. 26, no. 2, pp. 16–25, 2009.

[5] A. Piva, “An overview on image forensics,” ISRN Signal Processing, vol. 2013, 2013.

[6] M. C. Stamm, M. Wu, and K. R. Liu, “Information forensics: An overview of the first decade,” IEEE access, vol. 1, pp. 167–200, 2013.

[7] T. Bianchi, A. DeRosa, and A. Piva, “Improved DCT coefficient analysis for forgery localization in JPEG images,” in ICASSP. IEEE, 2011, pp. 2444–2447.

[8] M. Zampoglou, S. Papadopoulos, and Y. Kompatsiaris, “A large-scale evaluation of splicing localization algorithms for web images,” Multimedia Tools and Applications.

[9] T. Bianchi and A. Piva, “Image forgery localization via block-grained analysis of jpeg artifacts,” IEEE Transactions on Information Forensics and Security, vol. 7, no. 3, pp. 1003–1017, 2012.

[10] I. Amerini, L. Ballan, R. Caldelli, A. Del Bimbo, and G. Serra, “A sift-based forensic method for copy–move attack detection and transformation recovery,” IEEE Transactions on Information Forensics and Security, vol. 6, no. 3, pp. 1099–1110, 2011.

[11] D. Cozzolino, G. Foggii, and L. Verdoliva, “Splicebuster: A new blind image splicing detector,” in 2015 IEEE International Workshop on Information Forensics and Security (WIFS), Nov 2015, pp. 1–6.

[12] X. Pan and S. Lyu, “Region duplication detection using image feature matching,” IEEE Transactions on Information Forensics and Security, vol. 5, no. 4, pp. 857–867, 2010.

[13] D. Cozzolino, D. Gragnaniello, and L. Verdoliva, “A novel framework for image forgery localization,” arXiv preprint arXiv:1311.6932, 2013.

[14] C. Barnes, E. Shechtman, A. Finkelstein, and D. B. Goldman, “Patchmatch: A randomized correspondence algorithm for structural image editing,” in ACM Transactions on Graphics (ToG), vol. 28, no. 3. ACM, 2009, p. 24.

[15] E. Kee, M. K. Johnson, and H. Farid, “Digital image authentication from jpeg headers,” IEEE transactions on information forensics and security, vol. 6, no. 3, pp. 1066–1075, 2011.

[16] J. D. Kornblum, “Using jpeg quantization tables to identify imagery processed by software,” digital investigation, vol. 5, pp. S21–S25, 2008.

Acknowledgments

The Authors would like to thank the Prof Carmela Russo and Dr Antonio D’Amico Director and Curator respectively of the Museo Diocesano di Arte Sacra of Nicosia (Sicily), for collaboration and authorization to use of the radiographic images of the Madonna della Grazie painting. We are also grateful to the Uffizi Gallery, and to Lisa Venerosi Pesciolini who supported the diagnostic campaign of the El Greco painting.