Blind Inpainting Forgery Detection

DANG Thanh Trung, Azeddine BEGHDADI
L2TI, Institut Galilée, Université Paris 13
Villtaneuse, France
{dang.thanhtrung, azeddine.beghdadi}@univ-paris13.fr

Mohamed-Chaker LARABI
XLIM, Départment SIC, Université de Poitiers
Poitiers, France
chaker.larabi@univ-poitiers.fr

***Abstract*—The increasingly use of digital images in our daily life and the availability of powerful software for processing and editing images, open new challenges regarding illegal or unauthorized image manipulation. Thus, it becomes essential to authenticate digital copies, validate their content, and detect possible forgeries. In this paper, we focus on detection of a specific type of digital forgery, inpainting, where an object is removed using pixels coming from the same image. The problem of inpainting detection is investigated and an efficient and reliable detection method is proposed. The performance of the proposed method is demonstrated on several inpainted images using different inpainting techniques.**

***Index Terms*—Inpainting forgery detection, digital tamper detection, digital image forensics.**

I. Introduction

Digital images are powerful and widely used communication means because they can deliver a huge amount of information. However, due to the advent of low-cost, high-performance computers, and the availability of powerful software for processing and editing images, it becomes relatively easy to manipulate or edit digital images even for non-professional users. It is thus possible to change the information contained within an image and create digital forgeries that are undetectable by human viewers. Consequently, it becomes very important to proceed to authenticity verification of digital image in order to certify given information. This introduces a need for a reliable tamper detection system.

Recently, digital image forensics technology emerged as a new research field related to these issue. It could be divided into active evidence and passive-blind evidence based on whether the additional information into digital images is pre-embedded or post-embedded. Alternatively, active evidence is mainly about digital watermark proposed as a mean for fragile authentication, content authentication, tampering detection and so on. One drawback of such an approach is that the watermark must be inserted at the time of recording before the tampering occurs. In addition, the watermark cannot accurately detect areas where the image has been edited. In contrast to these approaches, passive techniques for image forensics should operate in the absence of any watermark or signature. These techniques rely on the only assumption that although digital forgeries may be applied without any hint of tampering, they may alter the underlying statistics of an image.

There have been many techniques to detect an image edition made by passive methods. An attempt of categorization has been proposed by Hany Farid [1]. The passive approaches are considered as a new direction and are promising techniques for handling this problem.

A common manipulation in tampering with digital images is known as region duplication, where a continuous portion of pixels is copied and pasted at a different location in the same image. Moreover, to create convincing and transparent forgeries, the geometry and illumination of duplicated regions are often adjusted to adapt to local characteristics. Copy-move detection algorithms have been largely addressed in the literature [2]. They are mainly block-based methods [3], [4], [5], [6] or keypoint-based methods [7], [8], [9] with variation regarding detected details and computational cost.

Nowadays, the creation of a high quality copy-move forgery has become particularly easy due to the availability of efficient and user-friendly image processing software. Therefore, forgery detection becomes increasingly more difficult. In this work, we focus on detecting a specific type of digital image forgery, namely image inpainting. The intent of this operation is to modify the content of an image in the most visually plausible way. This yields to what we call *inpainting forgery*. This technique is more sophisticated and complex than copy-move forgery because the source of copied information could be non-continuous. This means that an object may be filled by a set of multiple small parts located at different places in the same image (*cf.* Figure 1-b) and not a single continuous region (*cf.* Figure 1-a). Therefore, inpainting forgery is more difficult to detect than copy-move forgery as it can be seen on Figure 2 where state-of-the-art copy-move detection algorithms would fail.

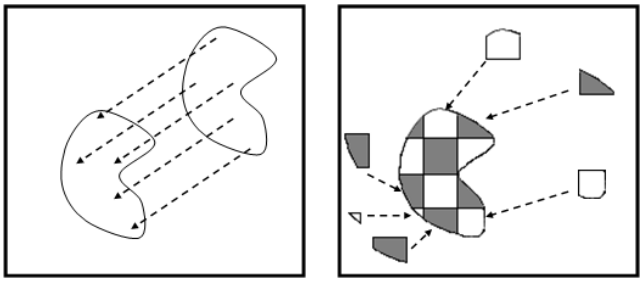


Fig. 1. The main difference between two forgery techniques. A tampered image using (a) copy-move method; (b) inpainting method.

In fact, the technique of image inpainting can be used to detect a type of forged image. As a result, there very few

(a) (b)

Fig. 2. An example of a inpainting forgery. (a) The original image; (b) an inpainted image using method in [10].

study about image inpainting forgery. Das et al. [11] proposed a detection algorithm based on zero-connectivity feature and fuzzy membership. Chang et al. [12] has introduced a new detection based on multi-region relation to recognize tampered inpainting regions from the suspicious regions. A better results has been proposed by Cozzolino et al. [13] using the computation of a dense motion field by PatchMatch-based detector algorithm [14]. However, most of them either are complex or unreliable.

In this case, more efficient and reliable inpainting detection method has been introduced. The proposed method is designed based on the common principle used by inpainting algorithms. It aims at detecting whether the input image has been edited following the aforementioned principle or not. The performance of the proposed method is evaluated on a set of various natural images. We also report its robustness with regards to different inpainting techniques.

The remainder of this paper is organized as follows: Section 2 describes briefly some works related to actual forgery detection methods, followed by the description of our proposal in section 3. Section 4 is dedicated to the experimental results and performance evaluation using objective measurements. Finally, the paper ends by conclusions and future works.

II. Related works

In the literature, several methods have been proposed to detect copy-move forgery. Most of them are composed of two steps namely *feature matching* and *filtering*.

In the first step, *i.e. feature matching*, features extracted from the suspect image and then matched between the different regions. A high similarity between two feature descriptors is interpreted as a possible duplicated region. Due to differences in the computational cost, as well as detected details, there are two variants for feature vector computation: *block-based* and *keypoint-based* features. For block-based features, the input image is first divided into overlapping blocks. Then a feature vector is extracted from each block.

In [3], Fridrich *et al.* proposed the use of 256 coefficients of the discrete cosine transform (DCT) as features for each block. In order to reduce the dimension of the feature matching space, Popescu *et al.* [4] applied a principal component analysis (PCA) for each feature vector. Mahdian *et al.* [5] introduced the use of 24 blur-invariant moments as features while Bravo-Solorio *et al.* [6] considered the entropy of a block as a discriminating feature. Unlike block-based features, keypoint-based features rely on the identification and selection of high-entropy image regions in order to reduce computational complexity of feature matching. Consequently, fewer feature vectors are considered and estimated. For instance, SIFT features are used in [7], [8] while in [9], they rely on SURF features.

In the second step, a *filtering* scheme is applied to reduce the probability of false matches while preserving matches that exhibit a common behaviour. The matches that originate from the same copy-move action are likely to exhibit similar amounts of translation, scaling and rotation. The most widely used variant handles outliers by imposing a minimum number of similar shift vectors between matches. For instance, a number of blocks simply replicated, without rotation or scaling, would exhibit a peak on the histogram of shift vectors. Therefore, the forged region decision is based on the amount of shift in addition to the distance between the original and copied regions.

III. Our proposal for inpainting detection

Image inpainting, also known as blind image completion, refers to the action of filling missing parts or objects in an image. To date, several approaches of image inpainting have been proposed in the literature. Most of them could be categorized into two types based on the purpose [10].

The first category is diffusion-based approach [15], [16], [17] in which the missing regions is filled by diffusing the information from the known region into the missing one. These methods are suitable for filling narrow or small area like scratches but are less efficient for large area. The second category is the exemplar-based approach [10], [18], [19], [20]. Inspired by texture synthesis methods, these methods produce an impressive output in recovering large damaged regions.

In this work, we subscribe to the latter category since it is more suited for large regions restoration or hiding. In inpainting methods, the missing information is completed based on the most similar patches under a pre-defined priority. In this sense, the inpainting is similar to a copy-move operation regarding the notion of patches. Nevertheless, as described previously, in copy-move approaches a continuous region is duplicated and pasted into the missing one instead of having small patches coming from different parts as in the case of inpainting methods. This is why copy-move detection cannot be applied for inpainted images.

Following this observation and by analyzing principles of image inpainting algorithms, we introduce a novel approach to detect inpainted regions. The proposed algorithm can be summarized through three main steps as described below. Let consider a window centered at pixel p denoted as a patch Ψ_p. The patch size, three thresholds θ_1, θ_2 and θ_3 are global parameters for the proposed algorithm.

Patch matching: Since most of the patch-based inpainting algorithms rely on patch similarity analysis, the first step in our detection scheme is searching all pairs of similar patches (Ψ_p, Ψ_i) in the input image, Ψ_i being candidate patche. A

list of pair of patches satisfying the three following criteria, formalized by equation (1), is built and considered as potential candidates.

$$\exists_{i\in\Phi}\Psi_p \simeq \Psi_i \Leftrightarrow \begin{array}{l}(Sim(\Psi_p,\Psi_i) < \theta_1)\\ \wedge(Dist(\Psi_p,\Psi_i) < \theta_2)\\ \wedge(Card(\Psi_p \cap \Psi_i) > \theta_3)\end{array} \quad (1)$$

- The similarity between two patches, $Sim(\Psi_p, \Psi_i)$, should be less than a threshold, θ_1. This threshold is used in order to reduce the probability of false matches while preserving suitable matches.
- The distance between two similar patches, $Dist(\Psi_p, \Psi_i)$, should be greater than a threshold, θ_2. This criterion is applied to preclude nearby patches or identical patches.
- The number of the same pixels in two patches, $Card(\Psi_p \cap \Psi_i)$, should be greater than a threshold, θ_3. This constraint is introduced to ensure that at least θ_3 pixels are copied between two patches.

The challenge in this step is related to minimizing the computation cost. In our algorithm, we used the *kd*-tree algorithm [21] to get approximate nearest neighbors. Typically, the Euclidean distance is used as a similarity measure as in the inpainting methods [18], [19], [20]. In prior work [2], it has been shown that the use of *kd*-tree matching leads, in general, to better results than lexicographic sorting as in [3], [4].

Mask generation: A binary mask, in which pixels belonging to candidate patches are labelled as "1" and the others as "0", is generated for detecting inpainted regions. This mask is a collection of connected regions composed of pixels labelled "1" on a background of pixels labelled "0". In our experiment, we assume that only one region has been restored in the input image. Thus, we evaluated only the largest connected area. The centroid of the largest connected region is located based on position of all pixels belonging to this region.

Patch filtering: A filtering scheme is applied to reduce the false detected patches. Indeed, for each couple of matches, one of the two patches is an original and the other is the inpainted version that should be marked as forged patch. The filtering is implemented for all matches based on their distance to the calculated centroid. The patch closer to the centroid is kept and the remaining patch is discarded. The morphological operation could be applied to connect nearby regions. Finally, the largest connected region is considered as the latest output.

IV. Experimental results

In this section, we evaluate the performance of the proposed inpainting detection algorithm first by visual inspection of the obtained results and then by using objective measurement.

A. Test for inpainting forgery

We implemented the proposed detection algorithm using C language and tested on a set of natural images with various contents. The output of the algorithm is a binary mask where white pixels correspond to detected inpainted regions and black pixels are non-inpainted areas. Green patch is added to identify the centroid of the inpainted region. In order to evaluate the visual performance of our detection, an experimental scheme is applied and described as follows.

First, an original image is used as ground truth with a binary mask image identifying an area need to be inpainted. An inpainting method is applied to the latter to generate an inpainted image. Finally, the inpainted image is used as input for our detection scheme to generate the detection mask. Figure 3 shows some results for our detection with the inpainting method in [18].

The parameters of our algorithm have been tuned as follows: patch size $l = 5$ and thresholds $\theta_1 = 0.1$; $\theta_2 = l/2$ and $\theta_3 = l^2/3$. It can be easily noticed that the proposed approach achieves good results by localizing quite precisely the inpainted object. The results yield to a direct conclusion about the presence of forgery or not.

(a) (b) (c)

Fig. 3. Inpainting detection results of our proposal for a set of inpainted images. (a) original images; (b) inpainted images; (c) detected masks.

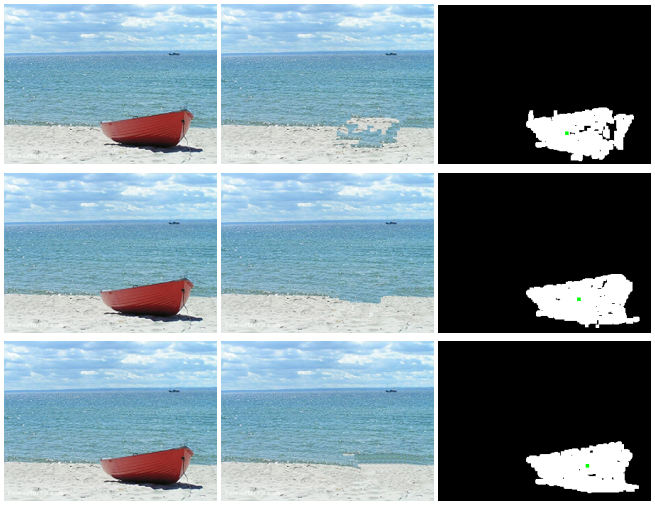
In order to evaluate the robustness of our method, we applied three different inpainting methods [18], [19], [20] to modify the original images. This leads to a set of inpainted images for the same input image. Figure 4 depicts an example for one original image (a), inpainted images using respectively methods described in [18], [19] and [20] (b) and the obtained detection masks (c). Again, the proposed approach allows detecting the presence of inpainting forgery even with the use of different inpainting techniques.

B. Performance evaluation

In order to quantify the efficiency of our inpainting forgery detection, we used objective measures namely *Precision*, *Recall* and F_1 often used for information retrieval performance evaluation [22].

Precision and *Recall* correspond to exactness and completeness of the results. In our perspective, the *Precision* is applied to estimate the probability that a detected region is correct. This probability is defined as follows:

$$P = \frac{|I_I \cap I_D|}{|I_D|} \times 100\% \quad (2)$$



(a) (b) (c)

Fig. 4. Inpainting detection results of our proposal for a set of inpainted images. (a) original images; (b) inpainted images using [18], [19] and [20] (top to bottom) ; (c) detected masks.

where I_I and I_D denote the inpainted region and detected region, respectively. The operator $|\Omega|$ counts the number of pixels in the region, Ω. Alternatively, *Recall* is used to measure the probability that a corrected region is detected. It is defined as follows:

$$R = \frac{|I_I \cap I_D|}{|I_I|} \times 100\% \tag{3}$$

However, there is a trade-off between *Precision* and *Recall*. Greater *Precision* might decrease *Recall* and vice versa. To consider both *Precision* and *Recall* together, the F_1 measure, the harmonic-mean of *Precision* and *Recall* is proposed and calculated as given in equation (4).

$$F_1 = \frac{2PR}{P+R} \tag{4}$$

We tested the proposed method to fifteen images. The corresponding *Precision*, *Recall* and F_1 measurements are shown in Figure 5. The average rates of *Precision*, *Recall* and F_1 are 78.68%, 84.49% and 80.73%, respectively. These values are nearly the same and relatively high. This shows that the detected region is not only correct but also quite complete. On the other hand, the obtained output demonstrates the important ability of the proposed method to detect inpainting forgery in the digital images. It thus confirms that our proposal is efficient for inpainting forgery detection.

V. Conclusion

It is admitted that forgery techniques became more complicated and sophisticated. In this paper we addressed the problem of inpainting forgery detection by proposing a novel approach relying on the behavior of most known inpainting algorithms. Therefore, based on the analysis of many exemplar-based inpainting methods, we have predicted the inpainted regions by similar patches and located it by the centroid

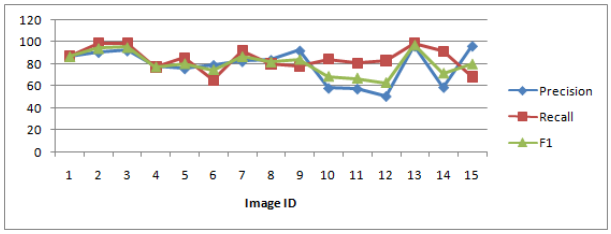


Fig. 5. Detection rates for inpainting forgery

connected component. Experimental results supported that the proposed method was appropriate to identify and localize the inpainted region with high accuracy even though the image could be modified by many different inpainting methods.

Although having achieved promising performance in detecting inpainted region, our method still contains limitation in some images. One example is shown as the top image in Figure 3 where the unexpected matches have been detected in the homogeneous or flat regions. This is because there always are similar patches in these kinds of region with any thresholds. Thus, it could be considered as an important future work to improve the detection performance for such case.

References

[1] H. Farid, "Image forgery detection," *Signal Processing Magazine, IEEE*, vol. 26, no. 2, pp. 16–25, 2009.

[2] V. Christlein, C. Riess, J. Jordan, C. Riess, and E. Angelopoulou, "An evaluation of popular copy-move forgery detection approaches," *IEEE Transaction on information forensics and security*, vol. 7, pp. 1841 – 1854, 2012.

[3] J. Fridrich, D. Soukal, and J. Luks, "Detection of copy-move forgery in digital images," *Proceedings of Digital Forensic Research Workshop*, 2003.

[4] A. C. Popescu and Hany, "Exposing digital forgeries by detecting duplicated image regions," Tech. Rep., Department of Computer Science, 2004.

[5] B. Mahdian and S. Saic, "Detection of copy-move forgery using a method based on blur moment invariants," *Forensic Science International*, vol. 17, no. 2, pp. 180 – 189, 2007.

[6] S. Bravo-Solorio and A. K. Nandi, "Exposing duplicated regions affected by reflection, rotation and scaling," in *ICASSP*. 2011, pp. 1880 – 1883, IEEE.

[7] 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.

[8] 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 Trans. on Information Forensics and Sec*, vol. 6, no. 3, pp. 1099 – 1110, Sep. 2011.

[9] X. Bo, W. Junwen, L. Guangjie, and D. Yuewei, "Image copy-move forgery detection based on surf," in *Proceedings of the 2010 International Conference on Multimedia Information Networking and Security*, Washington, DC, USA, 2010, MINES '10, pp. 889–892, IEEE Computer Society.

[10] T. T. Dang, C. Larabi, and A. Beghdadi, "Multi-resolution patch and window-based priority for digital image inpainting problem," *3rd International Conference on Image Processing Theory, Tools and Applications*, pp. 280–284, 2012.

[11] Sreelekshmi Das, Gopu Darsan, Shreyas L, and Divya Devan, "Blind detection method for video inpainting forgery," *International Journal of Computer Applications*, vol. 60, no. 11, pp. 33–37, December 2012, Published by Foundation of Computer Science, New York, USA.

[12] I.-Cheng Chang, J. Cloud Yu, and Chih-Chuan Chang, "A forgery detection algorithm for exemplar-based inpainting images using multi-region relation.," *Image Vision Comput.*, vol. 31, no. 1, pp. 57–71, 2013.

[13] Davide Cozzolino, Diego Gragnaniello, and Luisa Verdoliva, "A novel framework for image forgery localization," *CoRR*, vol. abs/1311.6932, 2013.

[14] Connelly Barnes, Eli Shechtman, Adam Finkelstein, and Dan B Goldman, "Patchmatch: A randomized correspondence algorithm for structural image editing," *ACM Trans. Graph.*, vol. 28, no. 3, pp. 24:1–24:11, July 2009.

[15] M. Bertalmio, G. Sapiro, V. Caselles, and C. Ballester, "Image inpainting," *Proceedings of ACM Conference Computer Graphics*, pp. 417–424, 2000.

[16] D. Tschumperle, "Fast anisotropic smoothing of multi-valued images using curvature-preserving pde's," *International Journal of Computer Vision*, vol. 68, pp. 65–82, 2006.

[17] J. Shen and T.F. Chan, "Mathematical models for local nontexture inpainting," *IEEE Conference on Computer Vision and Pattern Recognition*, pp. 1019–1043, 2002.

[18] A. Criminisi, P. Perez, and K. Toyama, "Region filling and object removal by exemplar-based image inpainting," *IEEE Transaction of Image Processing*, vol. 13 (9), pp. 1200–1212, Apr. 2004.

[19] Q. Zhang and J. Lin, "Exemplar-based image inpainting using color distribution analysis," *Journal of Information Science and Engineering*, pp. 1–12, 2011.

[20] J. Wu and Q. Ruan, "Object removal by cross isophotes exemplar based image inpainting," *Proceeding of International Conference of Pattern Recognition*, pp. 810–813, 2006.

[21] J. S. Beis and D. G. Lowe, "Shape indexing using approximate nearest-neighbour search in high-dimensional spaces," in *In Proc. IEEE Conf. Comp. Vision Patt. Recog*, 1997, pp. 1000–1006.

[22] C. D. Manning, P. Raghavan, and H. Schütze, *Introduction to information retrieval*, Cambridge University Press, New York, NY, USA, 2008.