# Detecting Image Brush Editing Using the Discarded Coefficients and Intentions

Fernando López Hernández*, Luis de-la-Fuente Valentín, Íñigo Sarría Martínez de Mendivil

Technology and Engineering Department of UNIR (Universidad Internacional de La Rioja), Logroño (Spain)

Received 8 June 2018 | Accepted 6 August 2018 | Published 14 August 2018

## Abstract

This paper describes a quick and simple method to detect brush editing in JPEG images. The novelty of the proposed method is based on detecting the discarded coefficients during the quantization of the image. Another novelty of this paper is the development of a subjective metric named intentions. The method directly analyzes the allegedly tampered image and generates a forgery mask indicating forgery evidence for each image block. The experiments show that our method works especially well in detecting brush strokes, and it works reasonably well with added captions and image splicing. However, the method is less effective detecting copy-moved and blurred regions. This means that our method can effectively contribute to implementing a complete image-tampering detection tool. The editing operations for which our method is less effective can be complemented with methods more adequate to detect them.

## Keywords

Image, Forgery, Brush, Stroke, Caption.

DOI: 10.9781/ijimai.2018.08.003

## I. Introduction

Currently, an important level of research has emerged for detecting forgery in digital images [1]. The detection of forged images has applications ranging from tampered handwriting [2] to insurance claims [3]. Forgers use different image editing tools [4]. This paper focuses on detecting scene editing with one of the currently least researched tool: the digital brush.

There are two contributions in this paper. The main contribution is the design of a new approach to detect brush editing along with the algorithm of the filter that detects this editing (see Section IV.D). As further described in Section III, there are few approaches designed to detect brush strokes, compared to other image modification techniques, such as cloning or image composition. The second contribution of this paper is the introduction of intentions as a subjective metric, along with its assessment application to forgery detection, in contrast with the more classical objective forgery metrics (see Section III.B).

## II. Related Work

This section reviews the state of the art of forged image detection.

### A. Types of Digital Image Forgeries

Often authors [1][4][5][6] classify the forgery to be detected into five categories:

1. *Copy-moving* (or *cloning*). A region of the image is selected and then copy-pasted to a different region of the same image. This is the most popular form of forgery due to its simplicity to conceal unwanted portions of the image, and effectiveness in leaving no visible traits of manipulation. Although the texture, color and noise of the pasted region are compatible with the rest of the image, there exists a wide variety of techniques to detect it (see, for instance, the survey in [6]).
2. *Image splicing* (or *image composites*). Image editing software usually allows for combining image fragments (typically represented as layers) from different images. One difference with copy-move forgery is that in composite image forgery there are no duplicate regions to be identified. Another difference is that if the forgers want to create a realistic image, they often have to apply geometric transformations (rotation, scaling, skew, etc.) to the spliced regions before pasting them into the target image [7][8]. That is, the size or orientation of the spliced regions in the source and target image usually does not match without these geometric transformations. Logically, geometric transformation in copy-move forgery detection has also been researched (e.g. [9][10]).

   To identify the edited regions, often inconsistencies in region features are identified. For instance, [11] identifies JPEG compression features inconsistencies, the authors of [12][13][14] identify noise discrepancies in regions, [15] detects sharp changes surrounding the spliced region, and [16] identifies inconsistencies in shadow boundaries.
3. *Blurring and sharpening*. Blurring is an effective operation to remove traces in forged regions, especially at the edges of the manipulated regions. Fortunately, there are robust detection techniques to this attack (e.g. [17]). Sharpening is used to enhance the appearance of objects in an image, which is another form of forging. Cao et al. have studied sharpening detection in depth. They propose both, a method to detect unsharp masking (a popular sharpening operation) [18], and a method to detect sharpening in general though histogram aberration and ringing artifacts [19].

* Corresponding author.

E-mail address: fernando.lopez@unir.net

4. *Image painting*. This category includes image tampering by painting and drawing. [20]. Cutzu et al [21] have proposed a method to discriminate between drawn images and genuine photo images by detecting changes in the hue, edge and texture features. Elgammal et al. [22] have developed a method to analyze forged strokes in paintings by characterizing personal strokes in drawings. Farid [23] has modeled brush detection as a segmentation problem, using a graph-cut algorithm to detect changes in intensity or texture. Lin and Huang [24] have detected air-brush and brush strokes by: (1) using the expectation-maximization (EM) algorithm in the JPEG coefficients, (2) generating a probability map in the frequency domain and (3) segmenting the periodicity in the probability map.
5. *Image retouching*. This category groups more subtle changes in the image that enhance or reduce certain features. For instance, Sutthiwan et al. [25] have proposed a method to detect changes in clarity or color of the texture. Mahalakshmi et al. [26] have proposed a method to detect affine transformations (rotation, scaling, etc.) by analyzing changes in the texture of the transformed region.

### B. Current Approaches, Strategies and Features

Forged image detection techniques have been broadly divided into active and passive (or blind) *approaches* [4][5][6][27][28]. *Active approaches* usually watermark or sign the image in order to detect future changes. *Passive approaches* use only the received image to assess if the image has suffered some kind of post-processing. The rest of this paper focuses on passive approaches.

H. Farid [27] (2009) classified forensic *strategies* into five categories. Ali Qureshi and Deriche [1] (2015) propose similar categories, but refer to these strategies as *tools*. In particular, these categories are:

1. *Pixel-based* strategies detect spatial irregularities in the pixel distribution properties. These strategies include, for instance, changes in noise level [12] or inter-block correlation [29]. These strategies have proved to be especially effective in identifying edited regions.
2. *Compression-based* strategies detect traces of forgery in the transformed domain, i.e., they are mainly designed for forensic analysis of JPEG images. These techniques can detect effects such as compression with a specific JPEG quantization table [30][31] or the quantization with two different quantization tables [32].
3. *Camera-based* strategies detect alterations in the characteristic artifacts that a specific camera model introduces. An example of these artifacts are the characteristic camera noise [33], or the remaining color after sensor interpolation (demosaicing) [34]. This means that they cannot be applied to analyze any image, since they only apply in certain camera models.
4. *Lighting-based* strategies detect inconsistencies in the 3D real world lighting effects, specular lighting or highlights in the surface geometry [35]. These techniques often require manual intervention to identify and analyze possible inconsistencies.
5. *Perspective-based* strategies detect when constraints are not met in the perspective of objects with respect to the camera, because the object has undergone a geometric transformation [36][37]. Although these strategies are named geometric-based in [1][27], we call them perspective-based, to distinguish them from the detection of geometric transformations in sliced regions (e.g. [7]).

Regardless of the strategy, most forgery detection methods are based on the general concept of *features*: the information extracted from the image to detect forgeries. These methods usually have two stages: 1) *Feature extraction* measures relevant characteristics of the image, and 2) *Feature matching* searches regions of the image with similar features. The existence of regions with similar features is an indicator that one region may have been cloned from the other.

The extracted features can in turn be divided into three main types:

1. *Block-based features* are extracted from (overlapping or non-overlapping) rectangular blocks. The most typical features are the frequency representation, such as the histogram (e.g. [38]), or the Discrete Cosine Transform (DCT) (e.g. [39][40]) of the blocks. Other features are the texture of the blocks (e.g. [41]) or the *moment invariant* features, which are block features invariant to rotation and scaling [42].
2. *Keypoint-based features* are extracted from distinctive parts of the image such as corners, edges, or textures [43]. With these features, [44] identifies three issues to address: the non-uniform distribution of the keypoints, the threshold to select keypoints with low contrast, and how to cluster forged areas. For instance, [17] uses a Gabor filter for keypoint texture retrieval. Most of these features tend to be more robust to affine transformations. SIFT (Scale Invariant Feature Transform) is the most popular affine transform invariant keypoint feature. SURF [45] is an improvement on SIFT to reduce the dimension of the features and the computational time. The authors of [46] combine a point of interest detector with SIFT to extract more features points.
3. *Multi-scale features* allow for analyzing the image at different levels to achieve better detection results. The authors of [47] analyze textures at different levels to find copy-moved regions. The authors of [48] use multi-scale representation to cluster regions based on geometric constraints. The authors of [14] use multi-scale variation in noise to detect spliced regions.

As indicated above, feature matching searches for similarities (copy-move) or dissimilarities (spliced regions, blurring, retouching) between image features. An example of an effective matching method is clustering: the search space is divided into regions with similar features-vector distributions (e.g. [38]). Another popular feature matching is sorting. For instance, the authors of [49] use as features a histogram of oriented gradients that are lexicographically sorted to find duplicated blocks.

## III. Proposed Approach

As we have described in Section II.A, there is an extensive bibliography addressing the detection of forgery techniques of copy-move (cloning), image splicing (composites), blurring and sharpening. However, although graphic designers use the brush on a daily basis, its detection has not received the same level of attention. In the forth category in Section II.A we have described, to the best of our knowledge, the current research in brush painting forgeries.

Disturbances in the JPEG compression coefficients have already been successfully used to detect spliced regions [15][50] or double-compression [29][51]. In this work, we have hypothesized that brush editing also alters the distribution of these coefficients. However, the metric we use to detect these disturbances is different. Specifically, we first cancel the effect of lighting, and then assess the number of normalized coefficients that the JPEG compressor has discarded.

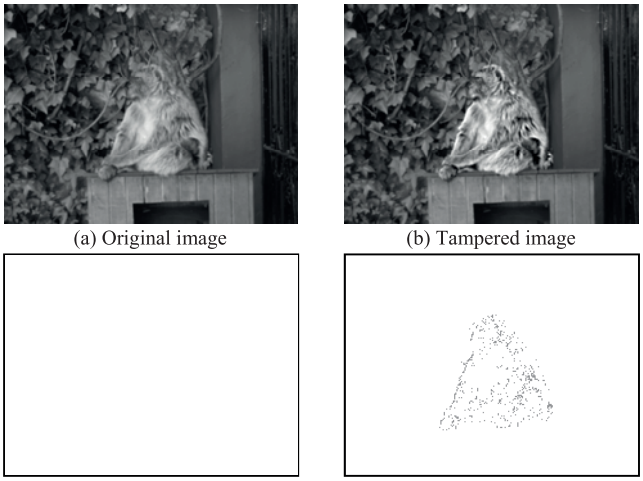
### A. Forgery Localization and Forgery Mask

There are two granularity levels to represent image forgery *localization*:

1. *Image-based* localization classifies the entire image. Binary classification determines whether the image is forged or not. In this case, the true / false and positive / negative rates of the classifier are evaluated (see, for instance [40]). One way to represent the fuzzyness in the classification decision is to assign

a forgery probability to the image. To evaluate this probability, it may be useful to have a confidence interval, rather than a single point estimate. For this reason, authors such as [52] study the confidence intervals of the probabilistic classification.

2. *Region-based* localization is used when the application requires identifying the parts of the scene that have been modified. This occurs when a change in the image modifies the semantics of the scene. For example, a change in the light of a traffic light might eliminate the traffic offense of the scene. The *forgery mask* is a tool to represent these areas of the image with high probability of falsification. Our experiments use this forgery mask to highlight tampering. For example, Fig. 1(c) shows the forgery mask for an unedited image, and Fig. 1(d) shows the forgery mask after sharpening the monkey's body. In particular, in our forgery mask dark pixels indicate high probability of alteration.



(a) Original image (b) Tampered image

(c) Original image forgery mask (d) Tampered image forgery mask

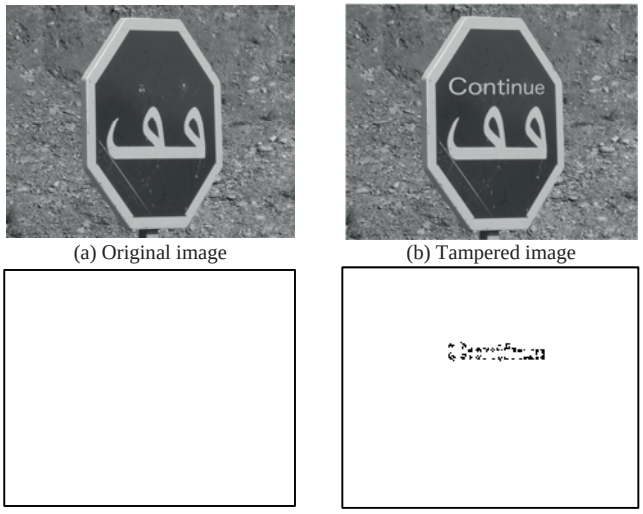
Fig. 1. Region based forgery localization for a sharpened monkey.

## B. Intentions and Interactive Forgery Mask

Typically, research in image forensics evaluates classification performance at either image or region level using an *objective metric*. For binary classification, they frequently use two metrics: *sensitivity*, i.e., the percentage of forgery correctly identified, and *specificity*, i.e., the percentage of unedited image correctly identified. Other alternative metrics, from the field of information retrieval, are *precision*, *recall* or the *F-score* (e.g., in [9][40]).

A drawback of these objective metrics is that a result like the one shown in our experiment in Fig. 2(d) has a relatively low sensitivity rate $Se = 0.5622$ (percentage of tampered pixels correctly detected). However, a visual inspection allows concluding that the image is forged. This is because a human is able to detect the intention of the forger without having to resort to soft computing techniques [53].

A second drawback of the objective metrics is their dependency on a threshold parameter. However, there is no general guideline to obtain this threshold, because usually each image has a threshold for maximum detection performance [54]. A human operator can effectively use semantics to effectively address this problem by means of an interactive gauge that allows the operator to visualize the forgery mask with different thresholds. We will refer to this gauge as the *interactive forgery mask*. Table I shows the sensibility *Se* and specificity *Sp* for different threshold values with Fig. 2(b). Fig. 3 shows the corresponding forgery masks. Note that for a human operator the interactive mask is more helpful than the objective metrics.




(a) Original image (b) Tampered image

(c) Original image forgery mask
*T*=20, *Se*=0/0, *Sp*=1.0

(d) Tampered image forgery mask
*T*=20, *Se* = 0.5622, *Sp*=0.9956

Fig. 2. First experiment (added caption).

(a) Threshold=5
*Se*=0.1542, *Sp*=0.9987

(b) Threshold=25
*Se*=0.6119, *Sp*=0.9951

(c) Threshold=35
*Se*=0.7065, *Sp*=0.9843

Fig. 3. Interactive forgery mask with three threshold levels in Fig. 2 (b).

TABLE I.
SENSIBILITY AND SPECIFICITY FOR DIFFERENT THRESHOLD VALUES IN FIG. 2(B)

| Threshold | Sensibility Se | Specificity *Sp* |
|---|---|---|
| 5 | 0.1542 | 0.9987 |
| 10 | 0.3781 | 0.9973 |
| 20 | 0.5622 | 0.9956 |
| 25 | 0.6119 | 0.9951 |
| 30 | 0.6517 | 0.9947 |
| 35 | 0.7065 | 0.9843 |
| 40 | 0.7811 | 0.7924 |

A third drawback of the objective metrics is that editing does not prove tampering. For instance, the experiments in [55] reported that frequently the double-compression artifact was merely due to an image resaved with a different quality level. A human operator can semantically interpret the image to effectively decide if the marked area corresponds to an intentional forgery. This operator can also use an interactive forgery mask to best "focus" each image at its appropriate threshold level.

In spite of this, in order to facilitate the comparison, we have added to the figures of the reported experiments the objective sensitivity *Se* and specificity *Sp*.

## IV. METHOD

The method does not require the *original image* (untampered image). It requires only an *analyzed image* (potentially tampered image) in JPEG format in order to calculate the editing evidence of

each block. There is a twofold output:

1. An *objective metric* with the sensibility *Se* and specificity *Sp* of the classification.
2. A *subjective metric* with the *interactive forgery mask* indicating the probability of edition of each block (see Fig. 3).

### A. Detected Effect

JPEG image compression uses the DCT to concentrate each block's energy in the low frequency coefficients, and high frequency coefficients are often reduced to zero. As described in [56], these high frequencies correspond to excessively sharp changes, which are the least noticeable for the human eye. The DCT tends to assign a low magnitude to these coefficients, and subsequently the JPEG compressor tends to round them to zero. In the rest of this paper we will refer to these zeroed coefficients as *discarded coefficients*.

Our working hypothesis is that brush strokes regenerate these unnoticeable sharp changes in the edited blocks. Consequently, 1) edited blocks will concentrate these high frequency coefficients, and 2) as a whole, the unedited blocks possesses a fewer count, in contrast with edited blocks.

Therefore, during recompression the JPEG compressor will need to discard a fewer number of coefficients to achieve the same compression ratio as the original image (as indicated in Section V, in our experiment we have used Adobe Photoshop default JPEG quality level: *Q*=12). This effect would be even more prominent when the forger saves the image in a lossless format with the intention of preventing detection by other methods (e.g. double-compression [55][57][58]). As a consequence, edited blocks will have fewer discarded coefficients.

Note that, we are not indicating that brush painting necessarily increases the number of high coefficients than are in a natural photo (e.g. there are blurring brushes). What we are hypothesizing is that a higher number of coefficients will remain in the tampered area because during recompression the compressor discards a fewer number of them.

### B. Tools

The tools to search for the abovementioned effect are the following:

1. *Counting discarded coefficients*. In our preliminary experiments we have observed that brush edited and recompressed blocks (especially those in the borders) keep a larger number of high coefficients, i.e., have a fewer number of discarded coefficients. Therefore, we use this count to gauge the editing probability of each block.
2. *Normalized energy*. In our preliminary experiments we found that lighting also influences the count of discarded coefficients. In particular, lighted areas (original or tampered) yield a lower count of discarded coefficients. So, before counting discarded coefficients, we need to *normalize the energy* of the analyzed image to eliminate the bias in the coefficients due the effect produced by lighting. After normalization, the count of discarded coefficients will not depend on the lighting of the blocks. The following section describes this normalization in more detail.

### C. Canceling the Effect of Differences in Lighting

The magnitudes of the DCT coefficients indicate the energy of the block: lighter blocks will have larger DCT coefficients, and so fewer of them will be discarded. We cancel the effect of lighting in the magnitude of the coefficients by means of normalization.

To normalize the energy of the coefficients faster, we avoid converting them to their spatial representation, using the Parseval relationship. This relationship states that the mean energy of the spatial signal $x[n,m]$ is equal to the mean energy of the coefficients in the frequency domain $X[p,q]$. In particular, given an $N$x$N$ block, Parseval relationship states that:

$$\sum_{m=0}^{N-1}\sum_{n=0}^{N-1}|x[m,n]|^2 = \sum_{p=0}^{N-1}\sum_{q=0}^{N-1}|X[p,q]|^2 \quad (1)$$

Where $m,n$ are indexing the spatial block, p,q are indexing the coefficient of the corresponding block, and $|\cdot|$ refers to the absolute value of the samples. Note that the spatial samples $x[n,m]$ are integers in the range 0..255, while the coefficients $X[p,q]$ are, in general, complex numbers.

Therefore we accomplish normalization in two steps:

1. Squaring the coefficients to measure energy and eliminate negative values:

$$E[p,q] = |X[p,q]|^2 \quad (2)$$

2. Scaling the $E[p,q]$ values to the JPEG compressor storage range (i.e., 0..255). We can obtain these values using the following formula:

$$N[p,q] = 255\frac{E[p,q]-\min\{E[p,q]\}}{\max\{E[p,q]\}-\min\{E[p,q]\}} \quad (3)$$

Where min{} and max{} refer to the minimum and maximum value in the block.

### D. Filter Algorithm

The proposed filter algorithm is as follows:

1. Divide the image into non-overlapping blocks of 8x8 pixels each. We propose using N=8, as this is the block size that the JPEG encoder typically uses.
2. Calculate the DCT coefficients of each block.
3. Normalize the energy of the blocks as described in Section IV.C.
4. Calculate the forgery evidence for each block as the sum of discarded coefficients $S$ in the block (i.e., zeroed coefficients). In our implementation, for a given threshold $\boldsymbol{T}$, we calculate forgery evidence $E$ for each block with the following rule:

   if $S<\boldsymbol{T}$ then

   $E$=1.0

   else if $S<2\boldsymbol{T}$ then

   $E$=0.5

   else

   $E$=0.0

5. Create the forgery mask representing forgery evidence by assigning a grayscale level to each block. In our implementation a black pixel means definitely edited ($E$=1.0), a white pixel unedited ($E$=0.0), and a gray pixel that there is doubt ($E$=0.5).

Fig. 1(d) and Fig. 3 are examples of the result of applying this algorithm. Note that in our implementation the forgery mask uses 3 gray levels to visually show the forgery evidence for each block. It is always possible to increase the number of gray levels, but we believe that, in general, it is difficult for the user to visually interpret more than 3 levels.

## V. Validation Methodology

This section demonstrates and assesses the proposed filter with different forgery techniques. For this purpose, we have surveyed the ability of the tool to detect intentions according to the purposes described in Section III.B. In addition, we are adding the sensibility

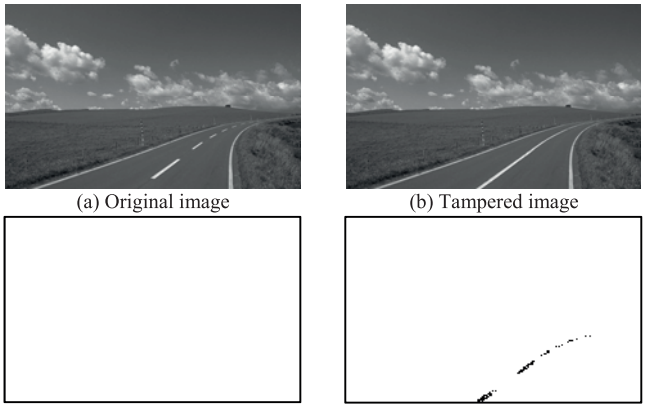
*Se* and specificity *Sp* to the figure of each experiment. Due to space limitations in this section we only show a representative experiment of each type of analyzed forgery. All reported experiments have been performed with grayscale images. In the case of RGB images, the described procedure can be repeated in each channel of the JPEG image.

## A. Detection of Brush Editing

For the reported experiments we have used Adobe Photoshop and done our best to create semantically realistic forgeries without sharp borders or any other forgery sign. We have saved the forged images with the default quality level of Adobe Photoshop ($Q$=12), assuming that this default value is the more likely to be used by a forger. The figure of each experiment indicates a threshold $T$ manually chosen for the interactive forgery mask.

### 1) Experiment 1: Added Caption

The first experiment was made by adding a caption with perspective and blended border to the original image in Fig. 2(a). The forged image is shown in Fig. 2(b). Fig. 2(c) shows the forgery mask that the filter produces with threshold $T$=20 on the original image.



(a) Original image (b) Tampered image

(c) Original image forgery mask $T$=10, $Se$=1.0, $Sp$=1.0

(d) Tampered image forgery mask $T$=10, $Se$=0.7794, $Sp$=0.9997

Fig. 4. Second experiment (brush painting).

The forgery mask in Fig. 2(c) does not indicate signs of forgery in any block ($Se$=0/0, $Sp$=1.0). Fig. 2(d) shows the forgery mask with $T$=20 on the forged image. The signs of forgery are evident, and a human can easily detect the semantic intention. However, the objective metric is reporting relatively low sensibility $Se$=0.5622, i.e., the proportion of forged blocks that are correctly identified as such is 56.22%. Fig. 3 shows the result of the analysis of the same image with three different threshold values.

### 2) Experiment 2: Brush Painting

For the second experiment in Fig. 4 we have used an 80% solid brush to turn the broken lines into a solid line. Note that the forgery mask in Fig. 4 correctly detects the edited blocks without leaving doubt about the forger's intention. In addition, the forgery mask reaches a high objective detection score: $Se$=0.7794, $Sp$=0.9997.

## B. Detection of Other Forgeries

Our experiments have revealed promising results with the detection of other types of forgeries, although without reaching the same level of precision. Therefore, we are demonstrating below the results that we are obtaining with these other types of forgeries.

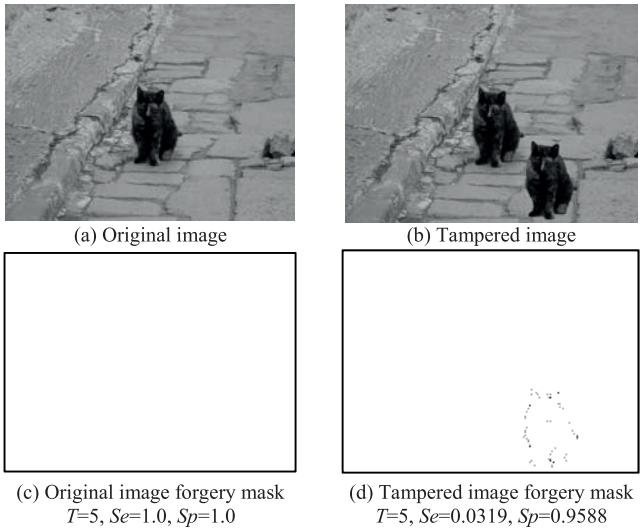
### 1) Experiment 3: Copy-move (Cloning)

The third experiment is for copy-move forgery. Fig. 5(b) shows a copy-moved cat from the original photo in Fig. 5(a). The forgery mask gives some evidence of forgery, but mainly detects forgery in the edges of the forged region. Note that while the forgery mask enables us to perceive the forgery, the objective metric indicates a very low detection rate $Se$=0.0319.

### 2) Experiment 4: Splicing (Composite)

The fourth experiment is for image splicing. In Fig. 6(b) a duck has been added to the lake. The forgery mask in Fig. 6(c) shows some sign of editing in the original image. We have downloaded the original lake image from the Internet, so we do not have access to the original photo. However, we think that the vegetation of the lower right corner has been edited (possibly with a contrast enhancement filter). Also the shadow over the water seems to have been artificially generated.

Regarding the forgery mask in Fig. 6(d), it gives some evidence of forgery, mainly in the edges of the spliced region.

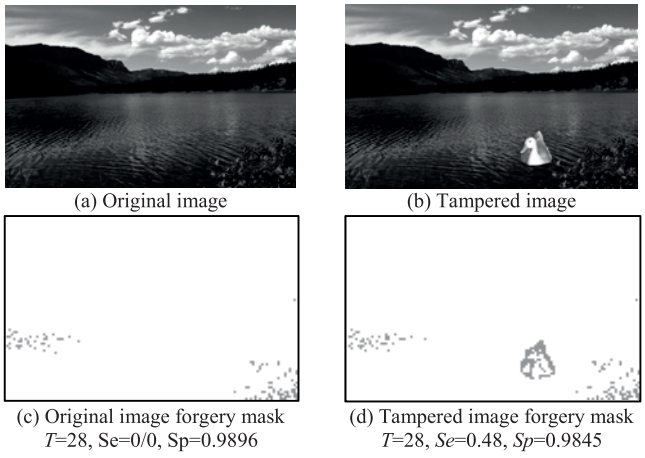


(a) Original image (b) Tampered image

(c) Original image forgery mask $T$=5, $Se$=1.0, $Sp$=1.0

(d) Tampered image forgery mask $T$=5, $Se$=0.0319, $Sp$=0.9588

Fig. 5. Third experiment (copy-move).



(a) Original image (b) Tampered image

(c) Original image forgery mask $T$=28, Se=0/0, Sp=0.9896

(d) Tampered image forgery mask $T$=28, $Se$=0.48, $Sp$=0.9845

Fig. 6. Fourth experiment (splicing).
Original image source: http://www.northamericatouring.com/images/10

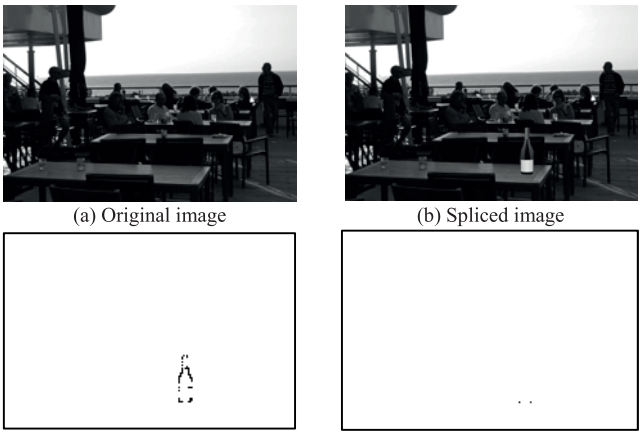
### 3) Experiment 5: Blurring

For the fifth experiment we have spliced a bottle image in Fig. 7(b) obtaining the forgery mask in Fig. 7(c), which has traces of forgery on the edges. Then we have applied a Gaussian Blur filter with radius 3 to the tampered image in Fig. 7(b), and then recalculated the forgery mask in Fig. 7(d). These results show that our method loses it effectiveness

when the forger applies a blurring filter to the edited image.

## VI. Conclusions and Future Work

We have observed that the recompression of an edited image block leaves a significant amount of undiscarded high frequency coefficients, and we have identified that the compressor is the responsible for it. In particular, this effect occurs because the first compression of the original JPEG image removes a large portion of these coefficients, and so the compressor is not as greedy for high coefficients when recompressing. The effect is more noticeable when the forger saves the image in a lossless format, but it is enough if the forger saves the image in a lossy format, as is the case in the reported experiments. The experiments also show that this effect is more prominent with brush-edited images, but is also able to detect other forgeries.



(a) Original image (b) Spliced image

(c) Splicing forgery mask
*T*=20, *Se*=0.2577, *Sp*=0.9973

(d) Splicing + blurring forgery mask
*T*=20, Se=0, Sp=0.9997

Fig. 7. Fifth experiment (splicing and blurring).

The experiments also reveal that the clustering of potentially modified blocks in semantically noticeable areas (intentions) has two benefits. 1) It makes the subjective human evaluation best determine forged areas that with a classical objective classification rate. For example, the forgery mask in the traffic infraction photo in Fig. 4 serves to provide enough evidence to identify an intentionally tampered image. 2) The interactive forgery mask (see Fig. 3) eases the determination of a suitable threshold with the help of an human operator, compared to using an optimal automatic threshold search algorithm (e.g., [54]).

The major limitation of our method is that the forger can easily erase the effect that we search for by blurring the edited region. This means that to detect blurred edited areas, our method should be combined with other methods, such as [18][59].

### A. Future Work

The first pending future work is to assess and compare intention recognition in alternative state of the art methods. The second future work is the execution of the implemented method with a standard forgery image database, such as [60][61].

## References


[1] M. A. Qureshi and M. Deriche, "A bibliography of pixel-based blind image forgery detection techniques," *Signal Process. Image Commun.*, vol. 39, pp. 46–74, Nov. 2015.

[2] Y. Boulid, A. Souhar, and M. E. Elkettani, "Multi-agent Systems for Arabic Handwriting Recognition," *Int. J. Interact. Multimed. Artif. Intell.*, vol. 4, no. Regular Issue, 2017.

[3] W. Lin *et al.*, "Survey on blind image forgery detection," *IET Image Process.*, vol. 7, no. 7, pp. 660–670, Oct. 2013.

[4] G. K. Birajdar and V. H. Mankar, "Digital image forgery detection using passive techniques: A survey," *Digit. Investig.*, vol. 10, no. 3, pp. 226–245, 2013.

[5] C.-Z. X. Tanzeela Qazi, Khizar Hayat, Samee U. Khan, Sajjad A. Madani, Imran A. Khan, Joanna Kołodziej, Hongxiang Li, Weiyao Lin, Kin Choong Yow *et al.*, "Survey on blind image forgery detection," *IET Image Process.*, vol. 7, no. 7, pp. 660–670, Oct. 2013.

[6] N. Choo *et al.*, "Copy-move forgery detection: Survey, challenges and future directions," *J. Netw. Comput. Appl.*, vol. 75, pp. 259–278, Nov. 2016.

[7] M. Jaberi, G. Bebis, M. Hussain, and G. Muhammad, "Accurate and robust localization of duplicated region in copy–move image forgery," *Mach. Vis. Appl.*, vol. 25, no. 2, pp. 451–475, Feb. 2014.

[8] Seung-Jin Ryu, M. Kirchner, Min-Jeong Lee, and Heung-Kyu Lee, "Rotation Invariant Localization of Duplicated Image Regions Based on Zernike Moments," *IEEE Trans. Inf. Forensics Secur.*, vol. 8, no. 8, pp. 1355–1370, Aug. 2013.

[9] N. B. Abd.Warif, A. W. AbdulWahab, M. Y. IdnaIdris, RosliSalleh, and FazidahOthman, "SIFT-Symmetry: A robust detection method for copy-move forgery with reflection attack," *J. Vis. Commun. Image Represent.*, vol. 46, pp. 219–232, Jul. 2017.

[10] D. Cozzolino, G. Poggi, and L. Verdoliva, "Splicebuster: A new blind image splicing detector," in *2015 IEEE International Workshop on Information Forensics and Security (WIFS)*, 2015, pp. 1–6.

[11] Juxian Zuo, Shengjun Pan, Benyong Liu, and Xiang Liao, "Tampering detection for composite images based on re-sampling and JPEG compression," in *The First Asian Conference on Pattern Recognition*, 2011, pp. 169–173.

[12] W. C. Hu, J. S. Dai, and J. S. Jian, "Effective composite image detection method based on feature inconsistency of image components," *Digit. Signal Process. A Rev. J.*, vol. 39, 2015.

[13] W. Wang, J. Dong, and T. Tan, "Tampered Region Localization of Digital Color Images Based on JPEG Compression Noise," Springer, Berlin, Heidelberg, 2011, pp. 120–133.

[14] C.-M. Pun, B. Liu, and X.-C. Yuan, "Multi-scale noise estimation for image splicing forgery detection," *J. Vis. Commun. Image Represent.*, vol. 38, pp. 195–206, Jul. 2016.

[15] Z. Fang, S. Wang, and X. Zhang, "Image Splicing Detection Using Color Edge Inconsistency," in *2010 International Conference on Multimedia Information Networking and Security*, 2010, pp. 923–926.

[16] Qiguang Liu, Xiaochun Cao, Chao Deng, and Xiaojie Guo, "Identifying Image Composites Through Shadow Matte Consistency," *IEEE Trans. Inf. Forensics Secur.*, vol. 6, no. 3, pp. 1111–1122, Sep. 2011.

[17] G. Muzaffer, O. Makul, B. Ustubioglu, and G. Ulutas, "Copy Move Forgery Detection Using Gabor Filter and ORB," *Proc. 2016International Conf. Image Process. Prod. Comput. Sci.*, pp. 23–29, 2016.

[18] G. Cao, Y. Zhao, R. Ni, and A. C. Kot, "Unsharp Masking Sharpening Detection via Overshoot Artifacts Analysis," *IEEE Signal Process. Lett.*, vol. 18, no. 10, pp. 603–606, Oct. 2011.

[19] Gang Cao, Yao Zhao, and Rongrong Ni, "Detection of image sharpening based on histogram aberration and ringing artifacts," in *2009 IEEE International Conference on Multimedia and Expo*, 2009, pp. 1026–1029.

[20] E. Verdú, C. P. G. Bustelo, M. Á. M. Sánchez, and R. G. Crespo, "A System to Generate SignWriting for Video Tracks Enhancing Accessibility of Deaf People," *Int. J. Interact. Multimed. Artif. Intell.*, vol. 4, no. Regular Issue, 2017.

[21] F. Cutzu, R. Hammoud, and A. Leykin, "Distinguishing paintings from photographs," *Comput. Vis. Image Underst.*, vol. 100, no. 3, pp. 249–273, 2005.

[22] A. Elgammal, Y. Kang, and M. Den Leeuw, "Picasso, Matisse, or a Fake? Automated Analysis of Drawings at the Stroke Level for Attribution and Authentication," *CoRR*, vol. abs/1711.0, 2018.

[23] H. Farid, "Exposing Digital Forgeries in Scientific Images," in *Proceedings of the 8th Workshop on Multimedia and Security*, 2006, pp. 29–36.

[24] T. Lin and C.-L. Huang, "Digital Image Forensics Using EM Algorithm," in *PCM*, 2009.

[25] P. Sutthiwan, Y. Q. Shi, W. Su, and T.-T. Ng, "Rake transform and edge statistics for image forgery detection," in *2010 IEEE International*

*Conference on Multimedia and Expo*, 2010, pp. 1463–1468.
[26] S. Devi Mahalakshmi, K. Vijayalakshmi, and S. Priyadharsini, "Digital image forgery detection and estimation by exploring basic image manipulations," *Digit. Investig.*, vol. 8, no. 3, pp. 215–225, 2012.
[27] H. Farid, "Image Forgery Detection -- A survey," 2009.
[28] S. . V. Ashima Gupta, Nisheeth Saxena, "Detecting Copy move Forgery using DCT," *Int. J. Sci. Res. Publ.*, vol. 3, no. 5, 2013.
[29] Wei Wang, Jing Dong, and Tieniu Tan, "Exploring DCT Coefficient Quantization Effects for Local Tampering Detection," *IEEE Trans. Inf. Forensics Secur.*, vol. 9, no. 10, pp. 1653–1666, Oct. 2014.
[30] J. D. Kornblum and J. D., "Using JPEG quantization tables to identify imagery processed by software," *Digit. Investig.*, vol. 5, pp. S21–S25, Sep. 2008.
[31] S. Q. Fu D, Shi YQ, "A generalized Benford's law for JPEG coefficients and its applications in image forensics," in *Proc. SPIE Electronic Imaging, Security and Watermarking of Multimedia Contents*, 2007.
[32] Bin Li, Tian-Tsong Ng, Xiaolong Li, Shunquan Tan, and Jiwu Huang, "Statistical Model of JPEG Noises and Its Application in Quantization Step Estimation," *IEEE Trans. Image Process.*, vol. 24, no. 5, pp. 1471–1484, May 2015.
[33] J. Fan, H. Cao, and A. C. Kot, "Estimating EXIF Parameters Based on Noise Features for Image Manipulation Detection," *IEEE Trans. Inf. Forensics Secur.*, vol. 8, no. 4, pp. 608–618, Apr. 2013.
[34] A. E. Dirik and N. Memon, "Image tamper detection based on demosaicing artifacts," in *2009 16th IEEE International Conference on Image Processing (ICIP)*, 2009, pp. 1497–1500.
[35] E. Kee and H. Farid, "Exposing digital forgeries from 3-D lighting environments," in *2010 IEEE International Workshop on Information Forensics and Security*, 2010, pp. 1–6.
[36] H. Yao, S. Wang, Y. Zhao, and X. Zhang, "Detecting Image Forgery Using Perspective Constraints," *IEEE Signal Process. Lett.*, vol. 19, no. 3, pp. 123–126, Mar. 2012.
[37] A. Pacheco, H. B. Barón, R. G. Crespo, and J. Pascual-Espada, "Reconstruction of High Resolution 3D Objects from Incomplete Images and 3D Information," *Int. J. Interact. Multimed. Artif. Intell.*, vol. 2, no. Regular Issue, 2014.
[38] H. Zhou, Y. Shen, X. Zhu, B. Liu, Z. Fu, and N. Fan, "Digital image modification detection using color information and its histograms," *Forensic Sci. Int.*, vol. 266, pp. 379–388, Sep. 2016.
[39] Rohini.A.Maind, A. Khade, and D.K.Chitre, "Image Copy Move Forgery Detection using Block Representing Method," *Int. J. Soft Comput. Eng.*, vol. 4, no. 2, p. 49.53, 2014.
[40] A. Alahmadi, M. Hussain, H. Aboalsamh, G. Muhammad, G. Bebis, and H. Mathkour, "Passive detection of image forgery using DCT and local binary pattern," *Signal, Image Video Process.*, pp. 1–8, Apr. 2016.
[41] E. Ardizzone, A. Bruno, and G. Mazzola, "Copy-move forgery detection via texture description," in *Proceedings of the 2nd ACM workshop on Multimedia in forensics, security and intelligence - MiFor '10*, 2010, p. 59.
[42] J. Zhong, Y. Gan, J. Young, and P. Lin, "Copy Move Forgery Image Detection via Discrete Radon and Polar Complex Exponential Transform-Based Moment Invariant Features," *Int. J. Pattern Recognit. Artif. Intell.*, vol. 31, no. 02, p. 1754005, Feb. 2017.
[43] A. D. Warbhe, R. V. Dharaskar, and V. M. Thakare, "A Survey on Keypoint Based Copy-paste Forgery Detection Techniques," *Procedia Comput. Sci.*, vol. 78, pp. 61–67, Jan. 2016.
[44] G. Jin and X. Wan, "An improved method for SIFT-based copy–move forgery detection using non-maximum value suppression and optimized J-Linkage," *Signal Process. Image Commun.*, vol. 57, pp. 113–125, Sep. 2017.
[45] V. T. Manu and B. M. Mehtre, "Detection of copy-move forgery in images using segmentation and SURF," in *Advances in Signal Processing and Intelligent Recognition Systems*, Springer, 2016, pp. 645–654.
[46] F. Yang, J. Li, W. Lu, and J. Weng, "Copy-move forgery detection based on hybrid features," *Eng. Appl. Artif. Intell.*, vol. 59, pp. 73–83, Mar. 2017.
[47] X. Bi, C.-M. Pun, and X.-C. Yuan, "Multi-Level Dense Descriptor and Hierarchical Feature Matching for Copy–Move Forgery Detection," *Inf. Sci. (Ny).*, vol. 345, pp. 226–242, Jun. 2016.
[48] E. Silva, T. Carvalho, A. Ferreira, and A. Rocha, "Going deeper into copy-move forgery detection: Exploring image telltales via multi-scale analysis and voting processes," *J. Vis. Commun. Image Represent.*, vol. 29, pp. 16–32, May 2015.
[49] J.-C. Lee, C.-P. Chang, and W.-K. Chen, "Detection of copy–move image forgery using histogram of orientated gradients," *Inf. Sci. (Ny).*, vol. 321, pp. 250–262, Nov. 2015.
[50] J. He, Z. Lin, L. Wang, and X. Tang, "Detecting Doctored JPEG Images Via DCT Coefficient Analysis," Springer Berlin Heidelberg, 2006, pp. 423–435.
[51] I. Amerini, R. Becarelli, R. Caldelli, and A. Del Mastio, "Splicing forgeries localization through the use of first digit features," in *2014 IEEE International Workshop on Information Forensics and Security (WIFS)*, 2014, pp. 143–148.
[52] A. S. Alfraih, J. A. Briffa, and S. Wesemeyer, "Forgery Localization Based on Image Chroma Feature Extraction," in *5th International Conference on Imaging for Crime Detection and Prevention (ICDP 2013)*, 2013, p. 2.11-2.11.
[53] F. López Hernández, E. Giménez de Ory, S. Ríos Aguilar, and R. González Crespo, "Residue properties for the arithmetical estimation of the image quantization table," *Appl. Soft Comput.*, vol. 67, pp. 309–321, Jun. 2018.
[54] B. Ustubioglu, G. Ulutas, M. Ulutas, and V. V. Nabiyev, "A new copy move forgery detection technique with automatic threshold determination," *AEU - Int. J. Electron. Commun.*, vol. 70, no. 8, pp. 1076–1087, Aug. 2016.
[55] A. Taimori, F. Razzazi, A. Behrad, A. Ahmadi, and M. Babaie-Zadeh, "A novel forensic image analysis tool for discovering double JPEG compression clues," *Multimed. Tools Appl.*, vol. 76, no. 6, pp. 7749–7783, 2017.
[56] G. K. Wallace, "The JPEG still picture compression standard," *Commun. ACM*, pp. 30–44, 1991.
[57] J. Yang, J. Xie, G. Zhu, S. Kwong, and Y.-Q. Shi, "An Effective Method for Detecting Double JPEG Compression With the Same Quantization Matrix," *IEEE Trans. Inf. Forensics Secur.*, vol. 9, no. 11, pp. 1933–1942, Nov. 2014.
[58] H. Farid, *Photo Forensics*. MIT Press, 2016.
[59] B. Y. and B. LIU, "Feature Fusion for Blurring Detection in Image Forensics," *IEICE Trans. Inf. Syst.*, vol. E97.D, no. 6, pp. 1690–1693, 2014.
[60] J. Dong, W. Wang, and T. Tan, "CASIA Image Tampering Detection Evaluation Database," in *2013 IEEE China Summit and International Conference on Signal and Information Processing*, 2013, pp. 422–426.
[61] M. G. Dijana Tralic, Ivan Zupancic, Sonja Grgic, "CoMoFoD -New Database for Copy-Move Forgery Detection," in *Proceedings ELMAR-2013 : 55th International Symposium ELMAR-2013, 25-27 September 2013, Zadar, Croatia*, 2013.

Fernando López Hernández

He is a full-time associate professor at UNIR. His current research interests lie in image and video processing, data-driven science, machine learning, and programming languages.

Luis de la Fuente Valentín

He is a full-time associate professor at UNIR. His current research interest is on data analysis and data mining, and data visualization mainly in the educational field.

Íñigo Sarría Martínez de Mendivil

He is a full-time professor at UNIR. His research focuses on mathematical modeling in Banach spaces, convergence of iterative methods and their dynamics.