Distinguishing Computer Graphics from Natural Images Using Convolution Neural Networks

Citation for published version:
https://doi.org/10.1109/WIFS.2017.8267647

Digital Object Identifier (DOI):
10.1109/WIFS.2017.8267647

Link:
Link to publication record in Edinburgh Research Explorer

Document Version:
Peer reviewed version

Published In:
9th IEEE International Workshop on Information Forensics and Security (WIFS) 2017

General rights
Copyright for the publications made accessible via the Edinburgh Research Explorer is retained by the author(s) and / or other copyright owners and it is a condition of accessing these publications that users recognise and abide by the legal requirements associated with these rights.

Take down policy
The University of Edinburgh has made every reasonable effort to ensure that Edinburgh Research Explorer content complies with UK legislation. If you believe that the public display of this file breaches copyright please contact openaccess@ed.ac.uk providing details, and we will remove access to the work immediately and investigate your claim.
Distinguishing Computer Graphics from Natural Images Using Convolution Neural Networks

Nicolas Rahmouni  
Ecole Polytechnique  
Palaiseau, France  
Email: nicolas.rahmouni@polytechnique.edu

Vincent Nozick  
JFLI (UMI 3527)  
Tokyo, Japan  
Email: vincent.nozick@u-pem.fr

Junichi Yamagishi*, Isao Echizen†  
National Intitute of Informatics  
Email: *jyamagis@nii.ac.jp,  
†iechizen@nii.ac.jp

Abstract—This paper presents a deep-learning method for distinguishing computer generated graphics from real photographic images. The proposed method uses a Convolutional Neural Network (CNN) with a custom pooling layer to optimize current best-performing algorithms feature extraction scheme. Local estimates of class probabilities are computed and aggregated to predict the label of the whole picture. We evaluate our work on recent photo-realistic computer graphics and show that it outperforms state of the art methods for both local and full image classification.

I. INTRODUCTION

Digital image forensics is a research field mostly dedicated to the detection of image falsification. A large part of the current research focuses on the detection of image splicing, copy-past or camera identification [1]. This paper addresses the problem of identifying whether an image is a computer graphics or a natural photograph.

A. Computer Graphics vs Natural Photographs

Some recent advances in image processing, like the real-time facial reenactment face2face [2], show the importance of having some tools to distinguish computer graphics (CG) from natural photographic images (PG). Although the distinction between CG and PG depends not only on image properties, but also on cognitive characteristics of viewers [3], people show inaccurate skills at differentiating between altered and non-altered images [4].

B. State of the art

In 2003, Farid and Lyu [5] presented a method to detect steganography and suggested to apply it to distinguish CG from PG. Like the quasi-totality of the methods that followed, the authors perform a “wavelet-like” decomposition of the images to generate some features vectors, combined with machine learning for classification.

Distinguishing CG from PG is by nature strongly related to computer graphics performances in generating photo-realistic images. Ng et al. [6] is the first paper to mention the expected difference between CG and PG images, mainly consisting in the image smoothness due to triangles. Dirik et al. [7] consider that this difference better resides in the statistical noise properties of the image. Wang et al. [8] consider that the image edges are more relevant for this problem. Wang and Moulin [9] introduce the use of histograms on the wavelet filtered data, before classification. This approach will be followed by many similar methods, like [10] and [11]. Among these methods, Wu et al. [12] is clearly the easiest to implement. Li et al. [13] recommend to perform the computation in HSV color space.

Alternatives to the “wavelet-like” decomposition are to work directly on the noise image, as proposed by Khanna et al. [14], or to detect traces of demosaicing that should not appear in CG images, as proposed by Gallagher and Chen [15]. Note that this last method will handle only images at native resolution since scaling an image will strongly alter the demosaicing artifacts.

For more detailed overviews, the reader can refer to Tokuda et al. [16], as well as to Wang et al. [8] and Ng and Chang [17].

In the rest of the paper, we will mainly compare our method to Wu et al. [12], i.e. an histogram based method derived from [13], known as one of the most effective from the current state of the art.

C. Motivations

Statistical properties of filtered images are good discriminators for distinguishing CG from PG, whether computations involve image gradient [12] or more sophisticated wavelet transformations [9]–[11]. For all these methods, the question of using the best filters is central, i.e. finding the ones that will extract the most meaningful information. Most of the previous works used hand-crafted filtering step which is unlikely to be optimal.

Our aim is to show that optimizing this filtering step dramatically improves classification results compared to current state of the art. A promising way to do so is to use a Convolutional Neural Network (CNN) to intelligently brute-force the solution.

Deep-learning approaches, and in particular CNN, have recently become very popular for many computer vision problems: classification [18], denoising [19], steganalysis [20], etc. CNN are not only able to learn classification boundaries but also to find conjointly the best representation of the
data. We also remark that the overall structure is adapted to our problem: convolution layers model filters while densely connected layers can replace efficiently other classification methods. Motivated by those observations, we implemented a special pooling layer to extract statistical features within a CNN framework and trained the network to distinguish CG from PG.

The paper is organized as follows: Section II presents the overall classification process while Section III to VI describe more precisely each step. Section VII provides a listing of our results and some comparison with Wu et al. [12].

II. ARCHITECTURE

Our approach mainly differs from the usual pipeline in the size of the image computed. Indeed, classifying smaller images is more challenging since the extracted statistics are less significant but dividing a large image into smaller tiles makes it possible to detect local splicing from a CG to a PG (and reciprocally). Moreover, smaller images are better suited to be used in a CNN due to hardware memory limitations.

In practice, we split the input images into \( N_p \) tiles (or patches) of resolution 100 × 100. This size was chosen as a trade-off between execution time and statistical meaningfulness. An image will be classified to be CG or PG according to a certain decision rule defined in Section VI that aggregates the results of all the tiles composing the image, as depicted in Fig.1.

As for the patch classifier, illustrated in Fig.2, our approach reproduces the usual 3-steps procedure: filtering, statistical feature extraction and classification. It computes \( N_f \) filtered images from 100 × 100 input tiles. Then, it extracts \( N_s \) statistical quantities for each filtered image and feeds the \( N_f \times N_s \) long feature vector to a usual classifier which estimates the posterior probability of each class. Those values are then used to decide the label of the global image.

The next sections detail each step of the overall procedure.

III. FILTERING

The filtering step consists in computing multiple convoluted images from which will be extracted statistical features. As filters are to be learned from the data, we use convolution layers instead of some fixed filters.

More precisely, we consider a finite set of \( N \) convolution kernels of size \( k \times k \). For example, with \( k = 3 \):

\[
K_{3,n} = \begin{pmatrix}
w_{0,0}^n & w_{0,1}^n & w_{0,2}^n \\
w_{1,0}^n & w_{1,1}^n & w_{1,2}^n \\
w_{2,0}^n & w_{2,1}^n & w_{2,2}^n
\end{pmatrix} \quad | \quad n \in [0..N-1] \tag{1}
\]

where the \( w_{i,j}^n \) are the weights which are to be optimized. Then, the input image is convoluted to each kernel. Biases are added and the result is composed with a Rectified Linear Unit (ReLU), a non-linear activation function which improves training performances [21].

Outputted images can be filtered again by stacking other convolution layers. This operation models simple filtering while creating new degrees of freedom (represented by weights and biases). Thus, not only the classifier but also the convolution kernels can be optimized.

After training, we found some well-known kernels used in previous methods but also one which are less trivial. Those results are shown in Fig.3. For example, kernels 24 and 25 are very close to horizontal difference while kernel 19 looks like a vertical difference. On the other hand, we observed filters like 3 or 11 which seem to combine different kernels (diagonal ones in this case). Searching the space of possible kernels permitted to obtain more complicated filters that would have been hard to find intuitively.
low-level image representations. All tested architectures are described in section VII.

IV. STATISTICAL FEATURES EXTRACTION

This Section explains how statistical information is extracted from the convoluted images. In a deep-learning context, this operation can be viewed as a pooling layer. Usually, after convolution layers, a local maximum pooling is computed to reduce the dimension of the data representation before classification. As for image forensics, other global statistical quantities are known to be more useful. Thus a special pooling layer is developed for adapting neural nets to this particular task.

We explored two different approaches: computing simple statistics or estimating the histogram of the convoluted images.

A. Simple statistics

Previous methods (for example [5]) suggest that deriving really simple quantities from filtered images, in general low-order moments of the distribution, is enough to solve our classification problem. In our implementation, for each filtered image $F_n$ with $n \in \{0..N-1\}$ of size $S_1 \times S_2$ we compute four quantities:

- The estimate mean: $m_n = \frac{\sum_{p \in F_n} p}{S_1S_2}$
- The estimate variance: $s_n^2 = \frac{\sum_{p \in F_n} (p - m_n)^2}{S_1S_2}$
- The maximum: $F_n^{\max} = \max_{p \in F_n} (p)$
- The minimum: $F_n^{\min} = \min_{p \in F_n} (p)$

Remark that those quantities are differentiable with respect to the pixel values which will allow gradients to be back-propagated through this layer during training. This gives a $4 \times N_f$ long features-vector (where $N_f$ is the number of filters in the last convolution layer) which is fed to the classifier.

B. Histograms

The second option is to compute the normalized histogram of the pixel distribution which may capture more information than simple statistical quantities [12]. In order to integrate this layer into our framework, we adapted the way bin values are usually calculated. Their computation includes the use of indicator functions which gradients value zero almost everywhere. This prevents the weights of the convolution layers to be updated during back-propagation. This issue can be avoided using Gaussian kernels instead of indicator function values. However, this layer is developed for adapting neural nets to this particular task.

We use a 11-bin histogram for each filtered image and the bin values are concatenated into a $11 \times N_f$ long feature vector.

V. CLASSIFICATION

From the feature vectors computed previously (either simple statistics or histograms), we train a classifier to separate the two classes CG and PG. We tried the following popular methods.

A. LDA

Fisher’s Linear Discriminant Analysis (LDA) [22] is one of the most widely used tool for linear classification. It aims to maximize the “between class variance” and minimize the “within class variance” over a set of linear classifiers.

B. SVM

Support Vector Machines (SVM) [23] are also very popular and present more flexibility than LDA. In its linear form, SVM is quite similar to LDA (although it minimizes another loss function), but it can also be applied for non-linear classification using the kernel trick. Indeed, feature vectors can be mapped to a higher dimensional space with a kernel function, in our case the radial basis function (RBF).

C. Neural network

Multi-layers perceptrons (MLP) are another example of flexible “model free” classifying method. This kind of neural networks show very good results on various classification problems [24]. It uses a back-propagation algorithm for training which permits to plug our feature extraction layers on top and optimize both at the same time.

Our MLP is composed of a hidden layer with 1024 ReLU activated neurons and a read-out layer with 2 SoftMax activated neurons (one per class). We also use dropout on the hidden layer as described by Strivastava et al. [25] to avoid over-fitting. The loss to minimize is the cross-entropy function for the two-classes problem, which can be interpreted as the minus log-likelihood of the label data under our model. Finally, we used Adam algorithm [26] to optimize synchronously MLP’s and convolution layers’ weights.

In practice, MLP will be used as the default classifier for training the CNN while SVM and LDA will only be tested by plugging them instead of the MLP after the already trained feature extraction layer.

VI. OUTPUT AGGREGATION

A regular image is usually big enough to be composed of many tiles. The classification of a full image will be decided according to the classification probability of each of its tiles. In practice, we use a weighted voting scheme where each patch contribution is the log likelihood of the label:

$$y_{pred} = \text{sgn} \left( \sum_{i=1}^{N_p} \log \frac{\mathbb{P}(Y = 1 \mid X_i = x_i)}{\mathbb{P}(Y = -1 \mid X_i = x_i)} \right)$$

with $Y$ and $X_i$ the random variables modeling the labels and the patches, $x_i$ the real observations and $\text{sgn}(x)$ a function that returns $\pm 1$ according to the sign of $x$.

We used this rule because it is fairly easy to obtain posterior probabilities (with our MLP for example, it just corresponds to the two output values of the read-out layer) but also because it can be interpreted as a global Maximum Likelihood Estimation criterion for the parameter $Y$. 


VII. TESTS AND RESULTS

A. Database

State of the art methods classically use the Columbia dataset [27] to estimate their performances. Since this dataset was created in 2004, it is obvious that the CG images are completely out of comparison with current CG images and it makes no sense to use them anymore. Thus, we collected our own dataset as follows.

Our CG were downloaded from the Level-Design Reference Database [28] which contains more than 60,000 good resolution (1920×1080 pixels) video-game screenshots in JPEG format. Only 5 different video-games were judged photo-realistic enough (namely The Witcher 3, Battlefield 4, Battlefield Bad Company 2, Grand Theft Auto 5 and Uncharted 4) which reduces the set to 1800 images. Some examples are shown in Fig.4. Furthermore, in-game information (dialogues, life bar, mini-maps, ...) were removed by cropping the images.

The Photographic images are high resolution images (about 4000×3200 pixels) taken from the RAISE dataset [29], directly converted from RAW format to JPEG. Some samples are shown in Fig.5.

B. Experimental setup

Our method was implemented using the Tensorflow framework [30]. Our statistical and histogram layers were directly integrated to the pipeline, using Tensorflow native functions. Models are developed and trained on Tesla K80 GPU from NVIDIA.

During training, we set batch size to 50 images and dropout probability to 0.25 for the MLP hidden layer. Adam algorithm parameters are set as follows: learning rate is $l = 10^{-4}$ and the momentum exponential decay rates are respectively $\beta_1 = 0.9$ and $\beta_2 = 0.999$.

### Table II: Tested architectures for patch classifier

<table>
<thead>
<tr>
<th>Name</th>
<th>$N_L$</th>
<th>$N_f^L$</th>
<th>$N_f^T$</th>
<th>$N_f^E$</th>
<th>Features</th>
<th>$N_e$</th>
<th>CLF</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stats-1</td>
<td>1</td>
<td>32</td>
<td>NA</td>
<td>NA</td>
<td>Simple stats</td>
<td>128</td>
<td>MLP</td>
</tr>
<tr>
<td>Stats-2L</td>
<td>2</td>
<td>32</td>
<td>64</td>
<td>NA</td>
<td>Simple stats</td>
<td>256</td>
<td>MLP</td>
</tr>
<tr>
<td>Stats-2S</td>
<td>2</td>
<td>16</td>
<td>32</td>
<td>NA</td>
<td>Simple stats</td>
<td>128</td>
<td>MLP</td>
</tr>
<tr>
<td>Stats-3</td>
<td>3</td>
<td>32</td>
<td>64</td>
<td>64</td>
<td>Simple stats</td>
<td>256</td>
<td>MLP</td>
</tr>
<tr>
<td>Hist-2</td>
<td>2</td>
<td>32</td>
<td>64</td>
<td>NA</td>
<td>Histogram</td>
<td>256</td>
<td>SVM</td>
</tr>
<tr>
<td>SVM</td>
<td>2</td>
<td>32</td>
<td>64</td>
<td>NA</td>
<td>Simple stats</td>
<td>256</td>
<td>LDA</td>
</tr>
<tr>
<td>LDA</td>
<td>2</td>
<td>32</td>
<td>64</td>
<td>NA</td>
<td>Simple stats</td>
<td>256</td>
<td>LDA</td>
</tr>
</tbody>
</table>

Evaluated architectures are described in Table II, with the corresponding number of layers $N_L$, the number of output filtered images of each layer $N_f^L$, $N_f^T$ and $N_f^E$ (NA if the layer does not exist), the feature extraction method (simple statistics or 11-bin histogram), the length of the extracted feature vector $N_e$ and the final classifying method CLF. We recall that all convolution kernels have a fixed size $k = 3$.

To set up optimal hyper-parameters for the filtering step, we evaluated the first 4 models by plotting the validation accuracy, i.e. the proportion of true classification among the images in the validation set, along training.

Fig.6 shows that the best performing model after training (when the validation curve flattens), has two layers. For this number of layer, using a larger number of kernels is a better choice.

C. Benchmark

For next tests, we have chosen the parameters that gave the best results during validation: $N_L = 2$, $N_f^T = 32$ and $N_e = 64$.

Our method is then evaluated by computing the detection accuracy and the area under ROC curve (AUC). The closer accuracy/AUC are to 100%/1.0, the more efficient is the classification.
We compared those results with our implementation of Wu et al. method [12] (the number of histogram features was set to \( k = 7 \) as suggested by the authors). Final classification was done with LDA and the training/testing procedure was performed on the corresponding part of our datasets. TABLE III shows accuracy for different methods and datasets.

TABLE III: Accuracy results comparison for each dataset (An asterisk \(^*\) indicates that patch aggregation is used)

<table>
<thead>
<tr>
<th>Method</th>
<th>Low-size</th>
<th>Full-size</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wu et al. [12]</td>
<td>75.0%</td>
<td>88.5%</td>
</tr>
<tr>
<td>Proposed method - SVM</td>
<td>79.7%</td>
<td>91.4%*</td>
</tr>
<tr>
<td>Proposed method - LDA</td>
<td>79.2%</td>
<td>91.1%*</td>
</tr>
<tr>
<td>Proposed method - Hist-2</td>
<td>82.7%</td>
<td>92.4%*</td>
</tr>
<tr>
<td>Proposed method - Stats-2L</td>
<td>84.8%</td>
<td>94.4%*</td>
</tr>
</tbody>
</table>

We can see that optimizing the filtering step improves significantly the accuracy for patch by patch classification compared to one of the most effective state of the art method (accuracy rises by 9.8%).

For low-size and full-size datasets, we used the aggregation scheme described in Section VI for all four of the proposed algorithm, with the patch classifier trained on the Patch database. For a fair comparison, Wu et al. baseline was trained on whole images which makes classification straightforward. In this configuration, our method shows better accuracy results on both datasets. Furthermore, ROC curves and AUC scores concur with this observation on full-size images as depicted in Fig.7.

The best performance is obtained using the Stats-2L model, showing that plugging a SVM or a LDA on top of our feature extractor instead of an MLP leads to less accurate classification.

We also see that training the network with the histogram layer does not improve the results. This can be explained by the lack of training samples which prevents efficient training for more complex models (256 features for simple statistics against 704 for histograms).

Finally, Fig. 8 exhibits some examples of local CG detection using our method. Sample PG have been corrupted by copy/pasting computer graphics and we show that our method permits to visualize which area have been modified.

VIII. CONCLUSION

In this study, we described a novel method for classifying computer graphics and real photographic images that integrates a statistical feature extraction to a CNN frameworks and finds the best features for efficient boundary. A boosting method is used to aggregate local estimations of the label. To confront our algorithm with nowadays computer graphics, we collected a photo-realistic video-game screenshots database. Compared to state of the art methods, this work is superior in terms of detection accuracy.

REFERENCES


