Fake Face Detection

Ramesh Sankaranarayana
College of Engineering & Computer Science
the Australian National University
Canberra ACT 2600 Australia
ramesh@cs.anu.edu.au

Limin Deng
College of Engineering & Computer Science
the Australian National University
Canberra ACT 2600 Australia
u6849956@anu.edu.au

Abstract

Deepfake brings entertainment and boost productivity to human. But unrestricted usage of deepfake would post great danger to the public safety. Thus, developing effective detection methods are significant. In the Deepfake Detection Challenge(DFDC in short), my main task is to find a suitable face extractor, data preprocessing, fine-tune training strategies, and slight inference adjustments.

1 Introduction

2 Related Works

Noiseprint focus on device fingerprint to find manipulation trace. Mesonet and CapsuleNet was reported to perform well in deepfake detection. There are other methods like detecting eye blink, inconsistent color space, and inconsistent head pose. Deepfake detection can be grouped into 2 classes. One is to detect deepfake images and the other is to detect deepfake videos.

3 Experiments

3.1 Datasets

DFDC is the public dataset from the Deepfake Detection Competition. It is composed of about 119000 videos, each is played by actors with fixed video length(10 seconds) and large resolutions (1920 X1280 or 1280 X 1920). It utilized 2 faceswap methods. One is to create realistic faceswap effect, the other is relative simple manipulation such as adding a blur dot to cover the face features or mix a face in the cloud background.

In this competition, I made two datasets. One is to extract the first frame from 50 trunks by BlazeFace and remove noise face. The second is dataset is extract 10 frames from real videos and 3 frames from fake videos. The second dataset is made to prove feeding more data can decrease val_loss but it is never used since it is too big. It takes a lot of time to clean and train.

FaceForensics++ contains four types of face manipulation methods which include Deepfake, Face2Face, FaceSwap, NeuralTextures. The original videos are from actors and youtube. We used 200 videos for each category, 1400 videos in total, due to the limitation of the disk space. FF++ provides three compression types, which are raw, c30, and c40. We chose c40 out of two reasons. One is that the public test dataset hosted on Kaggle to calculate the public leaderboard, some of them have 3 augmentations, reduce the resolution to 1/4, compress videos and reduce video FPS from 30 to 15. So we the C40 might be more close to this dataset. In addition, the reality videos such as on facebook or youtube are compressed. The advantage of this dataset is that it includes diverse manipulation effects such as DeepfakesFace2Face, FaceSwap, NeuralTextures, Also, for the limitation of disk space, I only download 200 videos for each category.

33rd Conference on Neural Information Processing Systems (NeurIPS 2019), Vancouver, Canada.

name	total videos	training videos	val videos	test videos
DFDC	1400			
FF++				
Deepfake-TIMIT	640			
Celeb-DF-v2				

Table 1: Dataset overview

Deepfaek-TIMIT is a faceswap dataset which has 640 videos. The faceswap technique was from the open source GAN-based approach (adapted from here: https://github.com/shaoanlu/faceswap-GAN), which, in turn, was developed from the original autoencoder-based Deepfake algorithm (https://github.com/deepfakes/faceswap). When creating the database, we manually selected 16 similar looking pairs of people from publicly available VidTIMIT database (http://conradsanderson.id.au/vidtimit/). For each of 32 subjects, we trained two different models: a lower quality (LQ) with 64 x 64 input/output size model, and higher quality (HQ) with 128 x 128 size model (see the available images for the illustration). Since there are 10 videos per person in VidTIMIT database, we generated 320 videos corresponding to each version, resulting in 620 total videos with faces swapped. For the audio, we kept the original audio track of each video, i.e., no manipulation was done to the audio channel.(original, need to adapt)

CelebDF-v2. This dataset is

Kaggle-fake-and-real-faces

Following is the overview of the datasets

We use multiple datasets to show our model are robust in diverse settings. Regarding the train, validation, test split strategy. For DFDC, We used the same

3.2 Baselines

We compare our works with following networks.

EfficientNet-B4. Since our network is based on EfficientNet-B4, we compare our model with this to prove our model has better performance.

EfficientNetAtt. This is the 16 solution on Kaggle. We compare to show our models has surpassed existed solutions, achieving better result.

WS-DAN: This is the 4th solution on Kaggle. We compare to show our modes has better performance.

3.3 Experiment Settings

3.4 Results

4 Conclusion

5 Acknowledgment

6 Reference

7 Discussion and Future Works

8 Submission of papers to NeurIPS 2019

NeurIPS requires electronic submissions. The electronic submission site is

`https://cmt.research.microsoft.com/NeurIPS2019/`

Please read the instructions below carefully and follow them faithfully.

8.1 Style

Papers to be submitted to NeurIPS 2019 must be prepared according to the instructions presented here. Papers may only be up to eight pages long, including figures. Additional pages *containing only acknowledgments and/or cited references* are allowed. Papers that exceed eight pages of content (ignoring references) will not be reviewed, or in any other way considered for presentation at the conference.

The margins in 2019 are the same as since 2007, which allow for $\sim 15\%$ more words in the paper compared to earlier years.

Authors are required to use the NeurIPS LaTeX style files obtainable at the NeurIPS website as indicated below. Please make sure you use the current files and not previous versions. Tweaking the style files may be grounds for rejection.

8.2 Retrieval of style files

The style files for NeurIPS and other conference information are available on the World Wide Web at

`http://www.neurips.cc/`

The file `neurips_2019.pdf` contains these instructions and illustrates the various formatting requirements your NeurIPS paper must satisfy.

The only supported style file for NeurIPS 2019 is `neurips_2019.sty`, rewritten for LaTeX 2_ε. **Previous style files for LaTeX 2.09, Microsoft Word, and RTF are no longer supported!**

The LaTeX style file contains three optional arguments: `final`, which creates a camera-ready copy, `preprint`, which creates a preprint for submission to, e.g., arXiv, and `nonatbib`, which will not load the `natbib` package for you in case of package clash.

Preprint option If you wish to post a preprint of your work online, e.g., on arXiv, using the NeurIPS style, please use the `preprint` option. This will create a nonanonymized version of your work with the text "Preprint. Work in progress." in the footer. This version may be distributed as you see fit. Please **do not** use the `final` option, which should **only** be used for papers accepted to NeurIPS.

At submission time, please omit the `final` and `preprint` options. This will anonymize your submission and add line numbers to aid review. Please do *not* refer to these line numbers in your paper as they will be removed during generation of camera-ready copies.

The file `neurips_2019.tex` may be used as a "shell" for writing your paper. All you have to do is replace the author, title, abstract, and text of the paper with your own.

The formatting instructions contained in these style files are summarized in Sections 9, 10, and 11 below.

9 General formatting instructions

The text must be confined within a rectangle 5.5 inches (33 picas) wide and 9 inches (54 picas) long. The left margin is 1.5 inch (9 picas). Use 10 point type with a vertical spacing (leading) of 11 points. Times New Roman is the preferred typeface throughout, and will be selected for you by default. Paragraphs are separated by ½ line space (5.5 points), with no indentation.

The paper title should be 17 point, initial caps/lower case, bold, centered between two horizontal rules. The top rule should be 4 points thick and the bottom rule should be 1 point thick. Allow ¼ inch space above and below the title to rules. All pages should start at 1 inch (6 picas) from the top of the page.

For the final version, authors' names are set in boldface, and each name is centered above the corresponding address. The lead author's name is to be listed first (left-most), and the co-authors' names (if different address) are set to follow. If there is only one co-author, list both author and co-author side by side.

Please pay special attention to the instructions in Section 11 regarding figures, tables, acknowledgments, and references.

10 Headings: first level

All headings should be lower case (except for first word and proper nouns), flush left, and bold.

First-level headings should be in 12-point type.

10.1 Headings: second level

Second-level headings should be in 10-point type.

10.1.1 Headings: third level

Third-level headings should be in 10-point type.

Paragraphs There is also a `\paragraph` command available, which sets the heading in bold, flush left, and inline with the text, with the heading followed by 1 em of space.

11 Citations, figures, tables, references

These instructions apply to everyone.

11.1 Citations within the text

The `natbib` package will be loaded for you by default. Citations may be author/year or numeric, as long as you maintain internal consistency. As to the format of the references themselves, any style is acceptable as long as it is used consistently.

The documentation for `natbib` may be found at

`http://mirrors.ctan.org/macros/latex/contrib/natbib/natnotes.pdf`

Of note is the command `\citet`, which produces citations appropriate for use in inline text. For example,

```
\citet{hasselmo} investigated\dots
```

produces

Hasselmo, et al. (1995) investigated…

If you wish to load the `natbib` package with options, you may add the following before loading the `neurips_2019` package:

```
\PassOptionsToPackage{options}{natbib}
```

If `natbib` clashes with another package you load, you can add the optional argument `nonatbib` when loading the style file:

```
\usepackage[nonatbib]{neurips_2019}
```

As submission is double blind, refer to your own published work in the third person. That is, use "In the previous work of Jones et al. [4]," not "In our previous work [4]." If you cite your other papers that are not widely available (e.g., a journal paper under review), use anonymous author names in the citation, e.g., an author of the form "A. Anonymous."

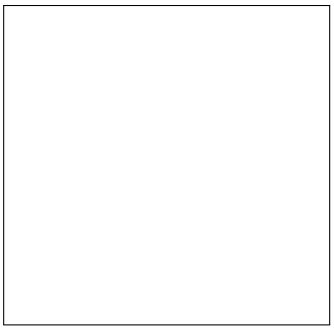

Figure 1: Sample figure caption.

Table 2: Sample table title

	Part	
Name	Description	Size (μm)
Dendrite	Input terminal	$\sim$100
Axon	Output terminal	$\sim$10
Soma	Cell body	up to 10^6

11.2 Footnotes

Footnotes should be used sparingly. If you do require a footnote, indicate footnotes with a number[1] in the text. Place the footnotes at the bottom of the page on which they appear. Precede the footnote with a horizontal rule of 2 inches (12 picas).

Note that footnotes are properly typeset *after* punctuation marks.[2]

11.3 Figures

All artwork must be neat, clean, and legible. Lines should be dark enough for purposes of reproduction. The figure number and caption always appear after the figure. Place one line space before the figure caption and one line space after the figure. The figure caption should be lower case (except for first word and proper nouns); figures are numbered consecutively.

You may use color figures. However, it is best for the figure captions and the paper body to be legible if the paper is printed in either black/white or in color.

11.4 Tables

All tables must be centered, neat, clean and legible. The table number and title always appear before the table. See Table 2.

Place one line space before the table title, one line space after the table title, and one line space after the table. The table title must be lower case (except for first word and proper nouns); tables are numbered consecutively.

Note that publication-quality tables *do not contain vertical rules.* We strongly suggest the use of the `booktabs` package, which allows for typesetting high-quality, professional tables:

`https://www.ctan.org/pkg/booktabs`

This package was used to typeset Table 2.

[1] Sample of the first footnote.

[2] As in this example.

12 Final instructions

Do not change any aspects of the formatting parameters in the style files. In particular, do not modify the width or length of the rectangle the text should fit into, and do not change font sizes (except perhaps in the **References** section; see below). Please note that pages should be numbered.

13 Preparing PDF files

Please prepare submission files with paper size "US Letter," and not, for example, "A4."

Fonts were the main cause of problems in the past years. Your PDF file must only contain Type 1 or Embedded TrueType fonts. Here are a few instructions to achieve this.

- You should directly generate PDF files using `pdflatex`.
- You can check which fonts a PDF files uses. In Acrobat Reader, select the menu Files>Document Properties>Fonts and select Show All Fonts. You can also use the program `pdffonts` which comes with `xpdf` and is available out-of-the-box on most Linux machines.
- The IEEE has recommendations for generating PDF files whose fonts are also acceptable for NeurIPS. Please see `http://www.emfield.org/icuwb2010/downloads/IEEE-PDF-SpecV32.pdf`
- `xfig` "patterned" shapes are implemented with bitmap fonts. Use "solid" shapes instead.
- The `\bbold` package almost always uses bitmap fonts. You should use the equivalent AMS Fonts:

  ```
  \usepackage{amsfonts}
  ```

  followed by, e.g., `\mathbb{R}`, `\mathbb{N}`, or `\mathbb{C}` for $\mathbb{R}$, $\mathbb{N}$ or $\mathbb{C}$. You can also use the following workaround for reals, natural and complex:

  ```
  \newcommand{\RR}{I\!\!R} %real numbers
  \newcommand{\Nat}{I\!\!N} %natural numbers
  \newcommand{\CC}{I\!\!\!\!C} %complex numbers
  ```

  Note that `amsfonts` is automatically loaded by the `amssymb` package.

If your file contains type 3 fonts or non embedded TrueType fonts, we will ask you to fix it.

13.1 Margins in LaTeX

Most of the margin problems come from figures positioned by hand using `\special` or other commands. We suggest using the command `\includegraphics` from the `graphicx` package. Always specify the figure width as a multiple of the line width as in the example below:

```
\usepackage[pdftex]{graphicx} ...
\includegraphics[width=0.8\linewidth]{myfile.pdf}
```

See Section 4.4 in the graphics bundle documentation (`http://mirrors.ctan.org/macros/latex/required/graphics/grfguide.pdf`)

A number of width problems arise when LaTeX cannot properly hyphenate a line. Please give LaTeX hyphenation hints using the `\-` command when necessary.

Acknowledgments

Use unnumbered third level headings for the acknowledgments. All acknowledgments go at the end of the paper. Do not include acknowledgments in the anonymized submission, only in the final paper.

References

References follow the acknowledgments. Use unnumbered first-level heading for the references. Any choice of citation style is acceptable as long as you are consistent. It is permissible to reduce the font

size to `small` (9 point) when listing the references. **Remember that you can use more than eight pages as long as the additional pages contain *only* cited references.**

[1] Alexander, J.A. & Mozer, M.C. (1995) Template-based algorithms for connectionist rule extraction. In G. Tesauro, D.S. Touretzky and T.K. Leen (eds.), *Advances in Neural Information Processing Systems 7*, pp. 609–616. Cambridge, MA: MIT Press.

[2] Bower, J.M. & Beeman, D. (1995) *The Book of GENESIS: Exploring Realistic Neural Models with the GEneral NEural SImulation System.* New York: TELOS/Springer–Verlag.

[3] Hasselmo, M.E., Schnell, E. & Barkai, E. (1995) Dynamics of learning and recall at excitatory recurrent synapses and cholinergic modulation in rat hippocampal region CA3. *Journal of Neuroscience* **15**(7):5249-5262.