SYNTHETIC TEXT DETECTION: SYSTEMIC LITERATURE REVIEW

Jesus Guerrero
Texas A&M University - San Antonio
San Antonio
jguer017@jaguar.tamu.edu

Izzat Alsmadi
Texas A&M University - San Antonio
San Antonio
Izzat.Alsmadi@tamusa.edu

ABSTRACT

Within the text analysis and processing fields, generated text attacks have been made easier to create than ever before. To combat these attacks open sourcing models and datasets have become a major trend to create automated detection algorithms in defense of authenticity. For this purpose, synthetic text detection has become an increasingly viable topic of research. This review is written for the purpose of creating a snapshot of the state of current literature and easing the barrier to entry for future authors. Towards that goal, we identified few research trends and challenges in this field.

1 Introduction

Studies regarding text generation before 2017 were generally scarce and far between. As the body of research grew for synthetic text generation, so did the research for detectors, though lagging behind.

This paper discusses current trends of research and future viable research options with the goal of shortening the research process for Artificial Intelligence generated text detection. The main topic of discussion is the literature itself using the PRISMA methodology. Detection literature was reviewed systematically and put together in detail for novel research.

1.1 Related Surveys

There are seven surveys near the topic of synthetic text detection. Seven [14, 2, 21, 12, 26, 20, 7] are about reviewing the literature on the generation process whereby current techniques, domains, data sets and models are shown and reviewed as available. Those seven surveys are very useful for discovering where the body of research is today in regards to text generation.

In the current time very few detection based reviews and surveys exist, with only [21] truly narrowing itself down to actual detection. This survey on binary classification is a valuable contribution to the state of detecting fake text. This article shows techniques and models commonly used in 2020 and since then there have been more relevant publications than ever before.

1.2 Main contributions

At the time of the previous surveys/reviews the body of research was perhaps too small for a worthwhile review of primary sources. Since then many of the techniques, models and data sets have become more accessible and as a defense against attack, open-source. Now in the year 2022 we can update and add to these related surveys. For this literature review we have these main contributions:

- A review of 50 related articles about synthetic text detection
- Shows recent innovations for detection.
- Shows gaps in current research for future work.
This is perhaps one of the first literature reviews on the narrow topic of generated text detection. To the best of our knowledge there have been no systemic literature reviews on detecting synthetic text. This study focuses on exploring the current research literature, showing the current ecosystem behind synthetic detection and preparing for future research.

2 Research Design

For our systematic literature review, we used current research tools to aid in following the systemic process, PRISMA. The research design here is to find and compile the most relevant body of research for distinguishing fake text and making inquiries. We setup 3 research questions, followed the review process and distilled research to include in the literature review. There were stages of collecting the articles involved, starting with collecting many articles by title then following an exclusion/inclusion process down to 50 papers.

For the actual searching itself the main search engine used was Google Scholar as it is an aggregate of other databases and engines. The publisher, article type and year was recorded and notated in a 3rd party app, Mendeley. 1,211 related articles were chosen from their titles on Google Scholar using specified keywords, approved by a supervising author. The articles were scrapped from the Google Scholar website using Mendeley’s browser extension scrapper and were automatically added and kept in a database of Mendeley’s new reference manager to speed up the process. The collections feature of the application was used to separate the stages of the PRISMA methodology.

2.1 Research Questions

With the unifying goal of preparing for future research, the inclusion/exclusion process included more and more study of the given texts. These research questions and research objectives were created to guide the process of choosing articles and scrutinizing the literature for that purpose:

Table 1: Research Questions

| Research Question                                           |
|-------------------------------------------------------------|
| RQ1  Which datasets are currently used in the literature to detect deep fake models? |
| RQ2  What accuracy evaluation methods are there for detection effectiveness? |
| RQ3  What impact have recent innovations had on fake text detection? |

2.2 Research Objectives

For this study there are 5 objectives:

- To investigate the current existing techniques/approaches of detecting artificial text.
- To explore models and datasets created to detect artificial text.
- To explore accuracy evaluation of fake text detection.
- Show recent innovations since previous surveys.
- Show future work for further research.

2.3 Searching Strategy To Retrieve Studies

Given most to all studies were queried on Google Scholar with keywords including text generation, detection and synthetic text, the engine includes searches into various other databases such as IEEE, ArXiv, Semantic Scholar, Springer, ACM journals, Elsevier and more, even including schools inside one search page. Keywords were used in regards to their category. Specifically in this SLR each set of keywords contributed a number of articles but some were more valuable than others. “Text generation detection” was perhaps the most fruitful, though, the body of research is quite small. A wide variety of query keywords had to be used to gather the largest possible pool of articles regarding text generation. For a few cases the title did not appear to be about synthetic detection, though upon further reading was in fact relevant to detection and vice versa.
Table 2: Keywords used by category

| Domain            | Text generation method | Sample size | Text generation innovations | Classifier          |
|-------------------|------------------------|-------------|-----------------------------|---------------------|
| Social Networks   | GANs                   | Large       | Natural Language Processing | Word embedding      |
| Fake news         | Fake text              | Small       | Text analysis               | CNN                 |
| Domain            | Augmentation           | Sample      | Text classification         | RNN                 |
| Low resource      |                        | Training    |                             | Transformers        |
|                   |                        | Models      |                             | Detection           |
|                   |                        |             |                             | LSTM                |
|                   |                        |             |                             | Ensemble            |

From these keywords they were assorted with AND, OR and quotation required clauses. Certain key words like “text generation” AND “language processing” were especially effective together at finding articles while “fake text” led to irrelevant topics. Though some keywords were only useful for finding niche articles.

2.4 Article Inclusion Exclusion Criteria

A total of 1,211 articles were found using the above queries. With duplicates removed, the remaining 1,041 articles were sifted. Many articles containing relevant keywords and titles were not about text generation, Natural Language Processing (NLP) and detection. Some articles were not machine centric and were about societal or human reading of generated text though they were about generated text detection. Others mentioned fake text as trolling, which is not the focus of this review.

In the partial review many of these papers were excluded by abstract because they were not machine centric or were based on societal differences. Out of the 1,041 articles after removing duplicates, a partial review left 381 articles eligible for full review. The following criteria was used to include or exclude these papers from this point on:

The following is the inclusion criteria:

- The article must include machine generated text classification or be highly relevant
- The article can include other languages in its dataset
- The article itself must be written in English
- Surveys on text generation are allowed

The following is the exclusion criteria:

- The models used must be machine-centric, meaning they require machine learning to determine if a sample is generated text.

3 Systematic Mapping Study Results

Here we show the results of the systematic study, stages of the inclusion/exclusion process, publisher names and dates of publication. This overviews the current status of synthetic text detection literature in late 2022 and records potential research gaps to be filled by future authors.
**RQ1:** Which datasets/models are currently used in the literature to detect generated text?

According to literature, the more training data for both human and machine generated text the better the outcome will become. Though there are many sources for both real and fake it is good to see the popular ones for specific domains. Below are datasets usable for training a model for actual detection and research in the time to come:

**Open-source Datasets**

- **Hugging face:** [https://huggingface.co/datasets](https://huggingface.co/datasets)
  
  This website is the first place to look for datasets and models. Hugging face has a plethora to choose from across many regards of machine learning. Most to all of those below can be found on the platform.
Synthetic Text Detection: Systemic Literature Review

- GPT-3: https://openai.com/api/
  This is a high quality source of generated text. There are several models to choose from for GPT-3 though the models are not free to use.
- GPT-2: https://github.com/openai/gpt-2-output-dataset/
  For a while this dataset was standard in its use for text generation. This dataset includes samples of both synthetic and real text.
- Grover: https://github.com/rowanz/grover
  This is more of a collection of scripts for making a dataset oriented for news articles. The repo includes a detection model, text generator, accuracy evaluator and a web crawler for gathering authentic text source data.
- Authorship Attribution: https://bit.ly/3DNlLxw
  This is a dataset for detecting specific popular text generators. The csv samples for these generators are placed in the above link. The focus is more based on news/political articles.
- TuringBench: https://github.com/TuringBench/TuringBench
  The main website for TuringBench is more of a leaderboard about detecting which generator is being used. The dataset is given in a zip file and whoever gets the highest accuracy rating for detecting the generator wins.
- Academia papers: https://github.com/vijini/GeneratedTextDetection/tree/main/Dataset
  A niche dataset for synthetic academia papers, though, it is small and is not condensed in one file. This would be good to expand upon as a separate research paper.
- TweepFake: https://github.com/tizfa/tweepfake_deepfake_text_detection/
  A popular twitter dataset with human and machine tweets

Open source generative models

- Grover: https://grover.allenai.org/
- GPT-2: https://github.com/openai/gpt-2
- GPT-3 group(Paid): https://openai.com/api/
- Hugging face: https://bit.ly/3LwGszE
  I mention this again, with over 5,000 models to choose from, you can see the limitations of text generation, GPT-2 being the most popular on the platform.
- Web app w/ text generation (GPT-2), (Grover): https://app.inferkit.com/demo

Existing detective models

In late 2022 detectors usually are rarer, have to be trained with a generated text dataset, and are not often pre-built. Though new models and prebuilt detectors are being created all the time and now popping up more rapidly. There are likely many on the HuggingFace platform for example. Some models also serve a dual usage, having both detector and generator.

Below, an example of a pre-trained model, BERT, is good for general text classification modeling, requiring further building to fully classify generated text as real or fake. GLTR is another example model, a human detection helper which improves human-centric detection. GLTR colors words which are most suspiciously generated, boosting accuracy quite a bit with minimal learning from the person. The rest below are pre-built and available for detection testing:

- BERT based modeling
- GLTR: gltr.io
- Grover: https://grover.allenai.org/ (2019)
- Open-AI GPT-2: https://huggingface.co/openai-detector/ (2019)
- RoFT: https://roft.io/ (gamification of human detection)

RQ2: What accuracy evaluation methods are there for detection effectiveness?

According to [25] a good general rule of model evaluation is testing the mislabel or error rate. This can mean testing against a given test/validation set or testing against an outside dataset. Using a recorded error rate you can also distinguish how effective a detector is per generative model.

The standard way most detectors are evaluated in the literature is to stay in the same domain and use similar datasets. The error rates are based on a narrow binary classification and due to this there are much better error rates. You can see
this throughout the literature where there is one domain, like TweepFake [30], news oriented models [48], language based models [3], and other niche categories sticking to their own evaluated domains.

To truly test a model against more real data here are two things done in the literature; adversarial testing [45] and sourcing different generators [25]. For adversarial testing this means accounting for a post-processing phase of text generation whereby Greek and uncommon symbols are added along with misspellings and surely other techniques in adversarial fashion to cause the detector to mislabel the text as human written. Testing against this noise is a very good way to evaluate a real-world model. A typical solution for adversarial attack is with a preprocessing phase for the detector.

For evaluating accuracy against different sources, a good idea from [25] is to record the error rates of different common and popular generator. Below is an example of how a detector can mislabel a text.

**Figure 4** Example evaluation based on source, [?]

The authors of the article found human text was most mislabeled as synthetic. This can be used to adjust a model and evaluate its accuracy and can further be divided by which sources the human written text originated. Though a major flaw later stated by the author is how common it is to fine tune a generator, making labelling all generators unfeasible.

Lastly, how a model will be used should always be part of the evaluation. Low resource training may be better for something like TweepFake, captioning or microblog detection. Though general language detection would require more resources and vary in effectiveness based on the text in question plus how similar the training set had been. So the evaluation can be divided up in some cases or narrowed in others. This way the evaluation is accurate to the model’s purpose.

**RQ3: What impact have recent innovations had on fake text detection?**

Across the literature the general setting of recent innovations is to combat fake text, detecting and removing its effect on public discourse. Paid models like GPT-3 are generally superior at creating advanced generated text for fooling human detection but is made relatively open source for research against itself and other high quality generators.

There is a trend to open source datasets and models to protect the community from synthetic text by making it easier to create both generation and detection models. These motivations perhaps have had the greatest impact on future research. Many articles, as seen in Figure 2; publications by year, have been written more recently. Synthetic text will likely be more highly researched in the next few years.

Particularly niche and low resource domains are being filled in with working models and novel solutions. Short and long form AI generated document detection models are now more numerous with their accuracy reported in their respective papers. These new models give us more options than the standard detector, opening up more difficult and niche types.

### 4 Identified research gaps

Here we discuss the limitations of current research. The gaps are separated by 5 aspects of synthetic text detection gathered from our research questions. From these gaps future research can be studied.
1. **Limited overall research.** As of mid 2022 there is a scarcity of research papers regarding artificial text detection. The majority of time spent creating this SLR was in curating as many articles as possible and even with that time spent there were still a relatively few papers.

2. **Limited research on adversarial attacks.** Pre and post processing methodologies are missing for attacking detectors. Here is one example on adversarial attacking [45].

3. **Limited evaluation methodologies for detectors.** Several papers existed for evaluation methods though nothing thorough. For RQ2 the information was pulled from small parts of a group of papers but there was not much research outside of that.

4. **Low resource detector optimization.** Low resource training also had limited research. TweepFake [30] and fake academic paper detection [27] were perhaps the most optimization related articles. There is a gap here.

5. **Research in other languages.** Most other languages have very limited research though some articles do exist [8], [7], [37]. Data sets exist for Chinese, Russian and other languages as well but very few synthetic language detectors outside English.

### 5 Recommendations and future research directions

There is plenty of room for research in AI text detection across different aspects. Given the limited overall research the field can be taken from many angles. This includes studies on increasing accuracy for specific domains such as news, blogs, social media outlets, books, academia. Most to all domains are open for detection modeling.

Language specific research is a definite direction a person can take. Spanish, Hindu and many others do not have synthetic text detection research. Remaking previous research paper detectors in different languages is a good bet as well as dataset creation for future authors. There is little to no research on low resource generated text detection languages and domains as well.

Better, more robust, evaluation methods for detectors is a potential topic. Tasks like generalized accuracy tests or post/pre processing methodologies are open game. In this vein of evaluation adversarial detector attacks are a great and open avenue for research. In [45] adding simple homoglyphs break most detectors and can easily be added to generation models. Misspelling also helps in adversarial text generation. Together the detector recall goes from 97% down to 0.26%, massively fooling detection.

In addition there are many niche domains where text generation and even some detectors exist but there is no adversarial research behind the domain. A paper like [24] takes an adversarial approach to generating synthetic comments to fool detectors. To this end only a handful of research was found.

Another open but more difficult research niche is authorship attribution. Not just binary detection but multi-label detection for the most popular models. An example of this research is previously mentioned TuringBench, whereby an online leaderboard was created to detect which model the generator is sourced.

### 6 Conclusion

Natural language processing is trending in good fashion with plenty of open source projects and ideas for novelty. Automated AI text generation has grown tremendously in the past four years and now there is a fresh need for detection. As we enter a phase of defending trolls, bots and generated commentary recent advancements have allowed for more of itself. In this paper, our focus is on synthetic text generation with possible research trends and challenges.

### References

[1] David Ifeoluwa Adelani, Haotian Mai, Fuming Fang, Huy H. Nguyen, Junichi Yamagishi, and Isao Echizen. Generating sentiment-preserving fake online reviews using neural language models and their human- and machine-based detection, 2020.

[2] Izzat Alsmadi, Nura Aljaafari, Mahmoud Nazzal, Shadan Alhamed, Ahmad H. Sawalmeh, Conrado P. Vizcarra, Abdallah Kheisnah, Muhammad Anan, Abdulelah Algosaei, Mohammed Abdulaiziz Al-Naeem, Adel Aldalbahi, and Abdulaziz Al-Humam. Adversarial machine learning in text processing: A literature survey. IEEE Access, 10:17043–17077, 2022.

[3] C Wong arXiv preprint arXiv:1712.05419, undefined 2017, and Catherine Wong. Dancin seq2seq: Fooling text classifiers with adversarial text example generation. arxiv.org, 12 2017.
[4] R Avros, Z Volkovich International conference on machine learning, , and undefined 2018. Detection of computer-generated papers using one-class svm and cluster approaches. Springer, 2018.

[5] M Bao, J Li, J Zhang, H Peng 2019 International Joint . . . , and undefined 2019. Learning semantic coherence for machine generated spam text detection. ieeeexplore.ieee.org, 2019.

[6] Jérémie Bogaert, Marie-Catherine de Marneffe, Antonin Descampes, and Francois-Xavier Standaert. Automatic and manual detection of generated news: Case study, limitations and challenges. pages 18–26. ACM, 6 2022.

[7] Asli Celikyilmaz, Elizabeth Clark, and Jianfeng Gao. Evaluation of text generation: A survey. 6 2020.

[8] X Chen, P Jin, S Jing, C Xie 2022 IEEE 10th Joint International, and undefined 2022. Automatic detection of chinese generated essays based on pre-trained bert. ieeeexplore.ieee.org, 2022.

[9] Ayesha Priyambada Das, Ajit Kumar Nayak, and Mamata Nayak. A survey on machine learning based text categorization. academia.edu, 2018.

[10] GH de Rosa, JP Papa Pattern Recognition, and undefined 2021. A survey on text generation using generative adversarial networks. Elsevier, 2021.

[11] Nirav Diwan, Tanmoy Chakravorty, and Zubair Shafiq. Fingerprinting fine-tuned language models in the wild. 6 2021.

[12] Chenhe Dong, Ying Shen, Min Yang, Yinghui Li, Haifan Gong, Miaoxin Chen, and Junxin Li. A survey of natural language generation. undefined, 1:38, 2021.

[13] Liam Dugan, Daphne Ippolito, Arun Kirubarajan, and Chris Callison-Burch. Roft: A tool for evaluating human detection of machine-generated text. pages 189–196, 10 2020.

[14] Noureen Fatima, Ali Shariq Imran, Zenun Kastrati, Sher Muhammad Daupota, and Abdullah Soomro. A systematic literature review on text generation using deep neural network models. IEEE Access, 10:53490–53503, 5 2022.

[15] Matthias Gallé, Jos Rozen, Germán Kruszewski, and Hady Elsahar. Unsupervised and distributional detection of machine-generated text. arxiv.org, 11 2021.

[16] M Gambini. Developing and experimenting approaches for deepfake text detection on social media. 2020.

[17] Margherita Gambini, Tiziano Fagni, Fabrizio Falchi, and Maurizio Tesconi. On pushing deepfake tweet detection capabilities to the limits. pages 154–163. ACM, 6 2022.

[18] Sebastian Gehrmann, Hendrik Strobelt, and Alexander M. Rush. Gltr: Statistical detection and visualization of generated text. ACL 2019 - 57th Annual Meeting of the Association for Computational Linguistics, Proceedings of System Demonstrations, pages 111–116, 6 2019.

[19] Daphne Ippolito, Daniel Duckworth, Chris Callison-Burch, and Douglas Eck. Automatic detection of generated text is easiest when humans are fooled. pages 2296–2309, 1 2020.

[20] Touseef Iqbal and Shaima Qureshi. The survey: Text generation models in deep learning. Journal of King Saud University - Computer and Information Sciences, 34:2515–2528, 6 2022.

[21] Ganesh Jawahar, Muhammad Abdul-Mageed, V.S. Laks Lakshmanan, M Abdul-Mageed arXiv preprint arXiv:2202.02013, undefined 2022, and Adeline Nazarenko. A benchmark corpus for the detection of automatically generated text in academic publications. arxiv.org, 2 2022.
[28] Sidi Lu, Yaoming Zhu, Weinan Zhang, Jun Wang, and Yong Yu. Neural text generation: Past, present and beyond. 3 2018.
[29] Narek Maloyan, Lomonosov Msu, Bulat Nutfullin, and Eugene Ilyushin. Dialog-22 ruatd generated text detection. 6 2022.
[30] Tiziano; Falchi Fagni Fabrizio; Gambini Margherita; Martella Antonio; Tesconi Maurizio. Tweepfake: about detecting deepfake tweets. PloS one, 16:e0251415–NA, 2021.
[31] Ahmad Najee-Ullah, Luis Landeros, Yaroslav Balytskyi, and Sang-Yoon Chang. Towards detection of ai-generated texts and misinformation, 2022.
[32] AS Nayak. Deepsot: spotting fake reviews with sentiment analysis and text generation. 2019.
[33] Minh Tien Nguyen. Detection of automatically generated texts. 2018.
[34] Saad Ahmed Qazi, Hina Kirn, Muhammad Anwar, Ashina Sadiq, Hafiz M Zeeshan, Imran Mehmood, and Rizwan Aslam Butt. Deepfake tweets detection using deep learning algorithms. mdpi.com, 2022.
[35] Sina Mahdipour Saravani, Indrakshi Indrajit Ray, and Indrakshi Indrajit Ray. Automated identification of social media bots using deepfake text detection. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 13146 LNCS:111–123, 2021.
[36] T Schuster, R Schuster, DJ Shah Computational . . . , and undefined 2020. The limitations of stylometry for detecting machine-generated fake news. direct.mit.edu, 2020.
[37] Tatiana Shamardina, Vladislav Mikhailov, Daniil Chernianskii, Alena Fenogenova, Marat Saidov, Anastasiya Valeeva, Tatiana Shavrina, Ivan Smurov, Elena Tutubalina, and Ekaterina Artemova. Findings of the the ruatd shared task 2022 on artificial text detection in russian. arxiv.org, 6 2022.
[38] Harald Stiff and Fredrik Johansson. Detecting computer-generated disinformation. International Journal of Data Science and Analytics, 5 2021.
[39] Reuben Tan, Bryan A. Plummer, and Kate Saenko. Detecting cross-modal inconsistency to defend against neural fake news. 9 2020.
[40] Chen Tang, Frank Guerin, Yucheng Li, C Lin arXiv preprint arXiv:2203.03047, undefined 2022, and Chenghua Lin. Recent advances in neural text generation: A task-agnostic survey. arxiv.org, 3 2022.
[41] Senait G. Tesfagergish, Robertas Damaševičius, and Jurgita Kapočiūtė-Dzikienė. Deep fake recognition in tweets using text augmentation, word embeddings and deep learning. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 12954 LNCS:523–538, 2021.
[42] Julien Tourille, Babacar Sow, Adrian Popescu, A Popescu of the 1st International Workshop on . . . , undefined 2022, and Adrian Popescu. Automatic detection of bot-generated tweets. dl.acm.org, pages 44–51, 6 2022.
[43] Adaku Uchendu, Vladislav Mikhailov, Jooyoung Lee, Saranya Venkatraman, Tatiana Shavrina, and Ekaterina Artemova. Tutorial on artificial text detection. artificial-text-detection.github.io, 2021.
[44] W Wang, A Feng Mathematical Problems in Engineering, and undefined 2021. Self-information loss compensation learning for machine-generated text detection. hindawi.com, 2021.
[45] Max Wolff and Stuart Wolff. Attacking neural text detectors. 2 2020.
[46] Congying Xia, Chenwei Zhang, Hoang Nguyen, Jiawei Zhang, and Philip Yu. Cg-bert: Conditional text generation with bert for generalized few-shot intent detection. arxiv.org, 4 2020.
[47] Seyhmus Yilmaz, S Zavrak arXiv preprint arXiv:2207.08230, undefined 2022, and Sultan Zavrak. Troll tweet detection using contextualized word representations. arxiv.org, 7 2022.
[48] Rowan Zellers, Ari Holtzman, Hannah Rashkin, Yonatan Bisk, Ali Farhadi, Franziska Roesner, and Yejin Choi. Defending against neural fake news. Advances in Neural Information Processing Systems, 32, 5 2019.
[49] Wanjun Zhong, Duyu Tang, Zenan Xu, Ruize Wang, Nan Duan, Ming Zhou, Jiahai Wang, and Jian Yin. Neural deepfake detection with factual structure of text. arxiv.org, 10 2020.