Online Fake Logo Detection System

Tathagata Bhattacharya*, Vivek Tanniru, Sai Teja Veeramalla
Department of Computer Science and Information Management Systems
Auburn University at Montgomery
Montgomery, Alabama,USA
tbhatta1@aum.edu, vtanniru@aum.edu,sveeram1@aum.edu

Abstract—Every day, hundreds of domain names, websites, and logos are being cloned by cyber criminals who want to gain our trust to steal our data. As a result, faking logos is becoming a big issue in the online world and needs to be addressed. As a result, fake logos on the internet have become a significant source of worry for businesses and consumers. The algorithm can detect differences in logo design, color, and positioning and assess the possibility of a fake logo. The system's accuracy was evaluated on a massive dataset of actual and false logos, and it obtained a high level of accuracy in recognizing fake logos. The fake logo identification technology has the potential to dramatically increase the credibility and dependability of online material, thereby protecting brand identity integrity. This research proposes a method for detecting fake logos using a Context-dependent similarity algorithm. Our approach involves extracting features from the logos and training a machine-learning classifier to distinguish between real and fake logos. We evaluate the performance of our method on a dataset of real and fake logos and demonstrate its effectiveness in detecting fake logos with high accuracy.

Keywords-Context-dependent kernel, logo detection, logo recognition, CDS.

1 Introduction

Today, the world has witnessed massive computing power. From the Banking sector to Academic institutions, from defense to the corporate sector, people are highly dependent on IT power which comes with massive energy consumption.[1] Energy consumption in the Information and Communication Technology (ICT) sector has grown exponentially[3]. We require a sizable database of archived photos to verify and distinguish between authentic and fake logos to establish whether a logo is legitimate [2]. However, this demands much room in data centers, and maintaining such data centers consumes much energy[3]. To determine if a logo is phony or genuine, each picture must be recorded in a database, necessitating several servers and data centers. Improving energy efficiency in data centers can save costs and help mitigate the environmental impact of data centers.[4] This system was created to detect when a customer logo is copied by someone else on social media or other websites without the customer's permission so that the customer can take appropriate action[5]. Our algorithm looks for nearly identical logos in shape and design but differs in one or more details (a color change or a few lines removed from an icon)[5]. Some logos, like the Starbucks logo, have many variations that can go unnoticed. This technology was developed to alert customers when their logo is being used without their consent on social media or other websites[6]. Customers can then take the necessary legal action[5]. Our search engine looks for almost identical logos in shape and design but differs in one or more specifics (a color change, a few lines removed from an icon). Certain logos, such as the Starbucks logo, have numerous versions that could be more noticed [7].

1.1 Origin of Logo's

A logo may be a powerful asset for a brand, as we have all heard. Often, a company's logo is more likely to be recognized than its name. There are many logos, and most consumers can quickly recognize well-known ones. So from where did the logo originate? How has it evolved throughout time? The Ancient Egyptians are where the logo first appeared. Up to the Middle Ages, they employed hieroglyphics to brand and identify their property. After that, to distinguish between the different nobility levels, graphic images like coats of arms were used[8]. Although the conventional translation is ”word,” logos are not used for a word in the grammatical sense—for that, the term lexis was used.[9] However, logos and lexis derive from the same verb, lego, meaning ”(I) count, tell, say, speak”[10]. New York University's Computer Vision Laboratory has developed a program that allows you to scan any logo and determine whether it is authentic. In addition, some AI software provides the ability to match the image of a random file to our company logo[33].

1.2 Modern Day Logo's

The appearance of the first abstract logo, the Bass red triangle, in the 1870s marked the start of the modern era of logo design. Due to the development of color printing and advertising, logos have become crucial for firms to stand out to potential customers[5]. There is a need for websites that function like LogoMotive because, as the author demonstrates via a case study,

We would like to thank College of Science, Auburn University at Montgomery for supporting and encouraging us to perform this research

DOI 10.1109/CSCE60160.2023.00380

phony websites might appear to be legitimate businesses. The post also includes figures on how many more businesses want LogoMotive to monitor their domains than do not [3]. The Internet is a vast, largely unknown, and poorly understood arena. Scammers can therefore profit from online anonymity and a general lack of knowledge[7]. Scams come in different kinds and sizes, but phishing efforts on e-commerce websites that employ brand logos as bait are one of the most common types of scams. Consumers may need help identifying this type of counterfeiting because it frequently blends in with reliable websites [12]. Recently, fake news has become a widespread phenomenon on the Internet[8]. It refers to written material produced and disseminated on social media platforms like Facebook and Twitter with the intention of misleading or misinforming readers. The most frequent motivations for this are moneymaking schemes, gaining political influence, and online fraud [13]. Today, falsehoods are pervasive, and disinformation frequently influences people's ideas and feelings. However, some of these fraudulent reports can be found using a technique known as multimodal multi-image fake news detection. It is challenging enough to try to identify fake news from a single photograph. When evaluating the veracity of images, humans rely on perception and context signals that machines do not fully grasp [14]. In comparison to evaluations that have been verified as accurate, there is a noticeable difference in the frequency and kind of behavior that online reviewers have been seen to exhibit[10]. As a result, review detection systems need to be personalized. A system should consider the reviewer's unique behaviors along with their verbal and nonverbal indicators. [15]

1.3 Contributions

One of the main issues is fraudulent online recruitment for employers in the expanding internet-based economy. This essay proposes an innovative methodology for online recruitment fraud detection in a paperless setting. Data collection, data preparation, categorization, and prediction are the four components of the suggested model[11]. The analysis's findings show that the suggested strategy can use its recruitment data to successfully identify possible suspects by detecting the occurrence of fraud. [16] The removal of logos from video footage can be accomplished using a variety of post-production procedures, which will be covered in this article. The first method uses an algorithm called optical flow and tracking, which looks for logos or other markers in the scene and, if it finds any, fixes them in place on the screen for the duration of the clip with a minor transform[12]. The second method involves using Premiere Pro's Advanced Composition Modes, automatically removing rectangular items within a specific color range [17]. In this novel paper we explore literature in Sec.2 and implement a brand new approach in designing a fake logo detection system in Sec.3 and revealed the results of fake logo detection in Sec.4

2 Evolution of Fake logo

In this section, we will discuss the literature review of fake logos and explore how and why logos are used and important. We also discuss how fake logos came into place and try to create awareness of how logos can be used for phishing attacks.

2.1 History of designing logos

Businesses and institutions produce increasingly large amounts of visual data, and social systems are becoming increasingly well-liked[13]. Graphics logos are a particular visual item crucial for establishing the identity of anything or someone. Logos are visual designs that emphasize a name, evoke real-world items, or present abstract indications that appeal to the eye. In order to facilitate the trademark registration process, the majority of trademark recognition research focuses on the issue of content-based indexing and retrieval in logo databases. In this instance, the image capture and processing chain is controlled to ensure that the photos are clear, undistorted, and of acceptable quality[56]. A generic system must meet many requirements to find and identify logos in images taken in realistic settings, and it is necessary to make various geometric and photometric changes[55]. As logos are not isolated in real-world pictures, logo detection and recognition should be robust to partial occlusions. Simultaneously, we must ensure that slight variations in Local descriptors maintain local structures. These are adequate differentiators for identifying malicious interference or obtaining logos with specific regional quirks. Because of advances in technology, the function of logos in our culture is changing. In addition, due to our increasingly complex lifestyles, we have encountered a visual overload that shows how logo design has changed from complexity to simplicity. Designing a genuine logo for a brand should aim to provide a singular, straightforward logo mark that is immediately distinguishable and recognizable[8]. A good logo nowadays may stand alone and is adaptive in design and use. Moreover, in today's society, a logo's recognition is increased the simpler it is. Shape, contour, and brightness are the three primary features recognized by the computer vision algorithm (which can be considered tonal value). For the machine to determine if it is genuine or fraudulent, these qualities must match. Therefore, the file will be recognized as authentic if these requirements are satisfied[9]. The technique can be used on any device with a Web browser because it is cloud-based and runs on the computer's graphics processing unit (GPU). However, the current method is restricted to looking for logos in pictures.

2.2 Origin of designing fake logo

Logos instill trust by making a website feel familiar. To take advantage of this trust, scammers use reputable companies' logos on dangerous websites[53]. Unaware Internet users view these logos and believe they are visiting a legitimate government website or online store when visiting a phishing website, a fake website, or a website designed to propagate false information[54]. We provide the most prominent website logo-detecting investigation to date[14] In two case studies, the Dutch national government and Thuiswinkel Waarborg, a company that offers verified webshop trust marks, were used to identify logo misuse. We demonstrate how to recognize spear phishing, latent phishing attempts, and brand exploitation. To that goal, we created LogoMotive, a program that uses supervised machine learning to crawl domain names, produce screenshots, and identify logos. In order to help identify abuse, LogoMotive is active in the.nl registry and is generalizable to detect any other logo in any DNS zone. [1] Unsolicited emails that pose as advertisements (i.e., pretend to be from a specific company) are called fake logos disguised as advertisements. These emails contain hidden phishing links that take us to a website where our personal information may be accessed without our knowledge or consent[51]. Some scams send emails with false logos impersonating scam vendors to give the impression that they are legitimate businesses rather than individuals looking for personal information. This is done so that when the user reads the email, there would be less doubt about its true purpose, allowing for gathering more information on the intended victim before any action is made. In some schemes, a celebrity's image is used as a phony logo to give the impression that the celebrity is endorsing a specific item[15]. To trick people into thinking they are dealing with the actual organization, some con artists even employ fake logos from businesses similar to the one they are trying to con[52].

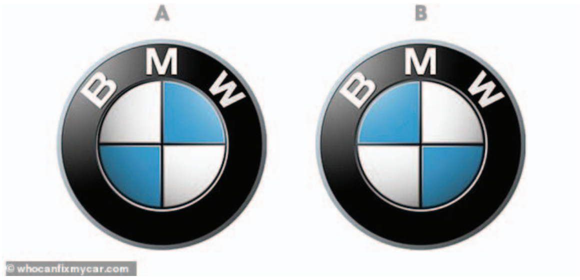


Fig. 1. Bmw's- Original vs Fake Logo

[51]

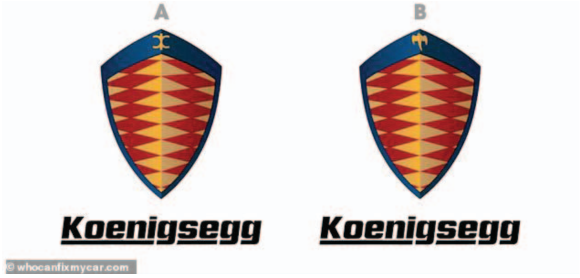


Fig. 2. Koeinseggg- Original vs Fake Logo

[51]

2.3 Awareness

The importance of learning to recognize the many logos that might be used in phishing emails cannot be overstated. Doing so will assist us in avoiding falling victim to fraud and phony logos. We must know what to look for to recognize phony logos and scams in time to prevent loss if we want to protect ourselves from falling for them[18]. Phishing attacks, also known as fake logo assaults, can be recognized and avoided using a variety of tactics. Antivirus software and spam filtering tools recognize and prevent malware from reaching the user's computer [49]. Unfortunately, these programs occasionally fail to identify the harmful stuff or may be sent due to a programming error. Anti-spam software filters out known phishing emails before they reach the inbox. Anti-spam software employs reputation filtering and content filtering (to recognize phishing emails by keywords) (to identify phishing emails by email address). Effective antivirus software and email filtering can identify and remove hazardous code from phishing emails that users have opened, stopping them from doing any harm. In addition, if antivirus software is frequently updated with malware definitions, it could detect and remove harmful software after it has infected a computer. Nevertheless, due to the way phishing attempts are created, antivirus software may be unable to identify them[19].

3 System Overview

In this section, we devise a plan to solve the issue of finding a fake logo by using two algorithms; we explain the steps we went through in detail and design the architecture of a fake logo detection system, and explain the steps involved in the workflow how do we collect the images for finding it out whether it is fake or genuine. Two algorithms are implemented within the system. When comparing two logos with the same shape but different colors and subtle alterations in a few lines of an icon, the first observes a minor color change on the logo ”A.” The second technique uses a straightforward BING image search to see if the customer whose company owns logo A's ”B” appears on any other website[48].

Whenever we look, we can see logos from all over the world. They represent various entities, including businesses, politicians, apparel, and coffee brands. People want their brand identification to be noticed on the digital web more than anything else[20]. However, there is a personal aspect to these logo graphics that we may have yet to notice: they may also be challenging to find online! Researchers must develop novel approaches to identify logotypes online using qualitative techniques or algorithms as computer-aided designers create more complex designs to scan and defy machine duplication[47]. However, researchers are discovering that things are shifting in this area. Overall, this system analyzes the characteristics of logos and determines whether they are authentic using a combination of machine learning and image processing approaches. The system can enhance its precision and efficacy in identifying fake logos by routinely upgrading and improving the machine-learning model and the library of authentic logos[21]. Each logo is scored using the qualitative technique of the online logo detection system, which rates each one on a scale of 1 to 5. It can identify, contrast, and rank logos by comparing them to the top-scoring examples in their class.

3.1 Proposed System

This study introduces a brand-new approach to logo recognition and identification based on ”ContextDependent Similarities”. First, users can upload the image they wish to check whether it is authentic using this method[26]. Then, the system analyzes the uploaded images by using distinct algorithms to identify different types of areas in them, comparing the results with a database of data that was previously generated by the same system, and reporting back to the user in multiple regions while also highlighting the types of errors that are found on the images, such as missing/wrong words/edges. The matching is accomplished by splitting the logo image into rows and columns [22]. After this process is finished, the matching will be quite precise. The method has proven to be effective in achieving the goals of logo detection and identification in actual photos[53]. Therefore, successful matching and detection are likely. A clear point of view on how the design flow will be depicted as shown in Fig.3.

- Logo Input: This is the system's input module, where logos are sent for examination. Many other places, including websites, social media networks, and e-commerce sites, may supply these logos[23].
- Preprocessing: The logos are cleaned up and ready for analysis in this module. Improve the quality of the logo for analysis; this may entail reducing the logos to a standard size, eliminating background noise or clutter, or taking other preprocessing actions[23].
- Feature Extraction: In this module, the system takes the logo's pertinent elements and extracts them for later study. These aspects of the logo could include its color, shape, font, and other elements.
- Machine Learning Model: The system's key component, a machine learning model, analyzes the logo's characteristics and compares them to a database of recognized authentic logos. The algorithm is trained to spot trends in the aspects of the logo that point to its legitimacy[23].
- Decision Making: Based on the output of the machine learning model, the system decides the authenticity of the logo. If the logo is fake, it is flagged for further review or removed from the system[23].
- Output: The system's final output includes a determination regarding the logo's veracity and any pertinent data or suggestions for additional action. This output could be displayed to the user or added to other processes or systems[23].

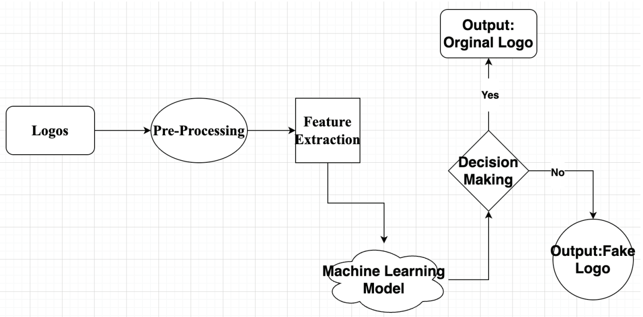


Fig. 3. Design flow of fake logo detection

3.2 Context-Dependent Similarity Algorithm

First, we take input such as an original logo as a test image as ly and a fake logo as lx, and we take interest points as sx and sy where differences are noticeable. In the first step, we iterate over the first image context matching for where it is the critical point of the referral image. We iterate over the second image context matching for where it is the critical point of the test image. In the second step, we compute the context-dependent similarity matrix till the maximum value of 30 and compute the values under limits over s and m. Finally, the logo is deleted or found if several matches, lines, and noticeable errors are found or greater than the referral image. This enables the system to process images with accuracy levels that are substantially greater than by chance. It compares logos by using the data that the user provides as they rate photos on a scale of 1 to 5[24]. The logo detection system, now known as the logo recognition system, can then accurately identify a collection of previously unknown logos[46]. This is partly because there are specific rules that all logos must adhere to, which makes comparing different logos much simpler. We decided to focus on data collection (i.e., image collecting) efforts on Instagram due to its picture-centered nature and popularity among marketers. Unfortunately, significant changes to the Instagram API drastically restrict access[28]. As a result, we decided to manually pull photos from the Instagram accounts of various athletes sponsored by Patagonia and Patagonia merchants. For the manual scraping, we used JavaScript on a Google Chrome console[45]. Although it was not flawless, it allowed us to gather pictures and start working with our model quickly! This was a significant problem, so we went through every picture We downloaded and put them in two folders: either 1) has the Patagonia logo (logo), or 2) does not have the Patagonia logo (no-logo). The logo detection model was where we spent most of our time iterating. The primary responsibilities included modifying the Inception v3 model with TensorFlow out of the box and the associated retraining script, training a new model, assessing model performance, and modifying model parameters as necessary[44].

Algorithm 1: Context Dependent Similarity

```
Input : $Reference\ logo\ image\ : l_x\ Test\ image :$
        $l_y, CDS\ parameter : \sigma, \alpha, \gamma, \beta$
for $i = 1 \leftarrow n$ do
    find context matching for xi where it is key point of
    referral image.
end
for $i = 1 \leftarrow n$ do
    find context matching for yiwhere it is key point of
    test image.
end
$t = 1 \leftarrow 30$
for $i = 1 \leftarrow n$ do
    for $j = 1 \leftarrow m$ do
        Compute CDS matrix Increment t i.e. does t++;
    end
end
$Repeat\ step\ 3\ until\ t\ >\ max\ or\ convergence.$
 for $i = 1 \leftarrow n$ do
    for $j = 1 \leftarrow m$ do
        $Compute\ K_{yj}\ |x_i\ x_i\ and\ x_j\ is\ declared\ only\ if\ K_{yj}$
        $\sigma\ K_{yj}\ |x_i\ where\ limits\ are\ s\ to\ m.$
    end
end
if $Number\ of\ matches\ in\ S_y >\ \tau S_x$ then
    $Then\ logo\ matched$
end
else
    $Logo\ not\ detected$
end
```

The most prevalent fonts used in internet logos, a technique for identifying logos without text, and a system for rating each logo as it is received; would provide an impartial benchmark that would make comparisons simple. Deep learning is a method that achieves excellent Upsampling of the logo class of

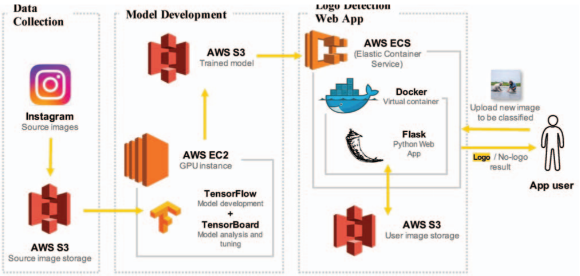


Fig. 4. Architectural flow for Fake logo detection

images and improved recall and accuracy for the unbalanced class. The architectural diagram is shown in Fig.4. A false logo detection system's design flow would include the following steps:

- Data Collection: The first step would be to create a dataset of both real and false logos. The bogus logo detection system would be trained and tested using this dataset[30].
- Feature Extraction: After gathering the dataset, the next step would be to identify traits in the photos that could be used to distinguish real logos from imitations. This may include features like shape, color, texture, and typography [43].
- Model Training: The next stage would be to train a machine learning model to distinguish the patterns and traits of real and false logos using the dataset and extracted features. Deep learning or computer vision techniques could be used for this[30].
- Model Evaluation: After training the model, it will be tested on a different dataset to see how well it can identify bogus logos. This might be accomplished by contrasting the model's predictions with the labels assigned to the logos in the assessment dataset.
- Model Deployment: The model can be deployed to the production environment once accurate enough to spot false logos in actual-world situations.
- Continuous monitoring and improvement: By upgrading the dataset and retraining the model, the system would need to be regularly monitored and improved to respond to new varieties of phony logos and raise its accuracy over time[30].

4 Results and Discussions

In this section, we discuss the Results and how they are visualized. In Fig.5, we can see that we tried to show the differentiation by using pie charts where the percentage of frauds is mentioned, In Fig.7, we collected many logos stored in a local Database where we could show what percentage of the logos turned out fake and how much percentage of them are genuine and total time taken in detecting the logo& Fig.8 demonstrate how a study of a single Fake logo results in a depiction of the kind of fraud and how much of it is covered in a pie chart. They also demonstrate the different results obtained when the findings are optimized and controlled using database management systems.

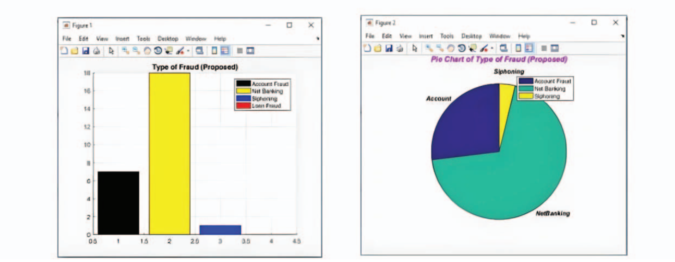


Fig. 5. illustrating how a bar graph and a pie chart are represented when analyzing a false logo.

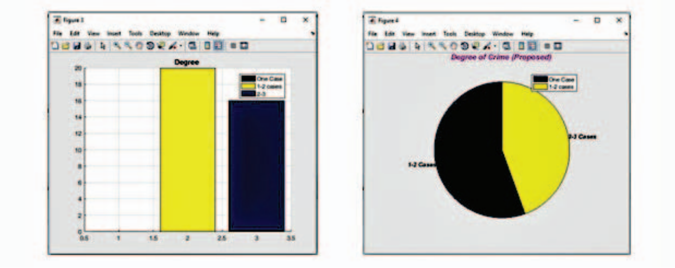


Fig. 6. Degree of fraud detection with optimization.

The confidence ratings for each of the five distinctive logos' validity are shown in Table 1 for each logo. We can assess the believability of an image using the confidence score, which ranges from 0.0 to 1.0, with zero being the lowest and 1.0 being the most. Based on the bogus logo identification system results, each logo is given a forecast of ”Real” or ”Fake,” as shown in Table 2. The confidence score, which ranges from 0 to 1, represents the system's confidence in its prediction[40]. A high confidence value (for example, 0.99) means the system is very sure of its forecast, whereas a low confidence level (for example, 0.50) means it is less confident [34].

The results of an online system for detecting Fake logos on a dataset of logos are shown in Fig.9. The logos in the dataset are displayed on the x-axis, and the confidence scores for each logo are displayed on the y-axis[36]. With the confidence ratings for the ”Real” logos shown on the line and the confidence scores for the ”Fake” logos shown on the bars, the confidence scores are presented as a line graph. The confidence scores in this graph are often more significant for the ”Real” logos than they are for the ”Fake” logos, showing that the false logo identification algorithm is more confident of its predictions for the ”Real” logos. Insights on the effectiveness of the false logo detection system may also be gained from the graph's general shape[37]. For instance, the system may need to be fixed or better if all logos have consistently high or low confidence scores.

The graph in Fig.10 displays the outcomes from a collection of logos using an online false logo identification method. The x-axis shows the logos in the dataset, and the y-axis shows the confidence ratings for each logo. The confidence ratings are displayed as a line graph, with the confidence ratings for the ”Real” logos shown on the line and the confidence ratings for the ”Fake” logos shown on the bars[38]. It is important to note that the results of a fake logo detection system will depend on the quality and variety of the training data used to develop the system, as well as the performance of the system itself. As such, the results of a fake logo detection system may vary and

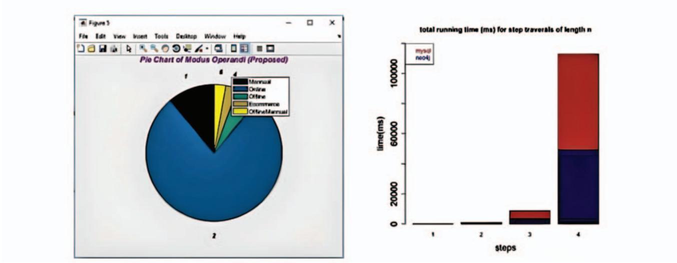
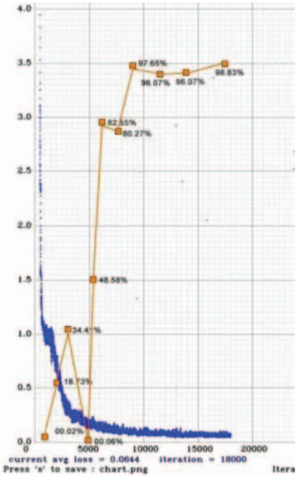


Fig. 7. Degree of fraud detection by DBMS



```
current avg loss = 0.0644    iteration = 18000
Press 's' to save : chart.png
```

Fig. 8. Tensor Flow of fake logo detection

should be interpreted with caution.

CONCLUSION AND FUTURE DIRECTIONS

In this research, we have developed a fake logo prediction system. In this study, we aim to use our original model's outcomes, which we were able to achieve by various dependent algorithms. Our intensive experiments demonstrate that our model is efficient in detecting logos. Finally, the creation of a fake logo detection system has the potential to greatly benefit businesses and consumers by increasing the trustworthiness and reliability of online content. The system analyzes and compares logos using powerful deep-learning algorithms and has shown high accuracy in recognizing fake logos.There are various possible future possibilities for online fake logo identification. For example, improving the system's capacity to recognize minor variances in logo design, such as variations in typeface, spacing, and other visual features, might be one area of attention. Furthermore, the system could be expanded to detect fake logos in video content, which could aid in the prevention of false information spreading on social media and other online platforms. Another potential future study topic is to investigate the feasibility of leveraging blockchain technology to build a safe and decentralized system for confirming the validity of logos. This might assist in limiting the production and distribution of fake logos while also giving customers more trust in the legitimacy of online information. Overall, the invention of a fake logo identification system is a significant step toward enhancing the integrity of online material. However, this subject has much room for additional study and improvement. We have been thinking about the following possible stages for this project's future: We must learn how a Fake logo detection system will work while protecting people's privacy. Then, boost the product prototype and gather input; enable RESTFUL API processing of bulk images. Finally, connect to the Instagram API (or the API of any social media picture provider) to automatically collect pictures. Boost and refine the model or process. By giving the model more training data, we can make it more capable of generalizing to more types of images.

Logo	Result	Confidence Score
1	Real	0.95
2	Fake	0.70
3	Real	0.99
4	Fake	0.60
5	Real	0.80
6	Real	0.89
7	Fake	0.66
8	Real	0.96
9	Fake	0.55
10	Real	0.82

TABLE I. Confidence scores for Test Logos

Prediction	Confidence Score	Mean confidence	Average Confidence
Real	0.97	0.94	0.93
Fake	0.89	0.86	0.88
Real	0.93	0.91	0.92
Fake	0.87	0.85	0.86
Real	0.99	0.97	0.98
Fake	0.77	0.65	0.66
Real	0.82	0.99	0.98
Fake	0.70	0.75	0.68
Real	0.93	0.97	0.98
Fake	0.55	0.67	0.78

TABLE II. Median and average scores of predicted logos

4.1 Ethics approval and consent to participate

NA

4.2 Consent for publication

Not Applicable

4.3 Availability of data and material

The datasets generated during and/or analyzed during the current study are available from the corresponding author upon reasonable request.

4.4 Competing interests

The authors declare that they have no competing interests

4.5 Funding

No Funding has been received to support this study.

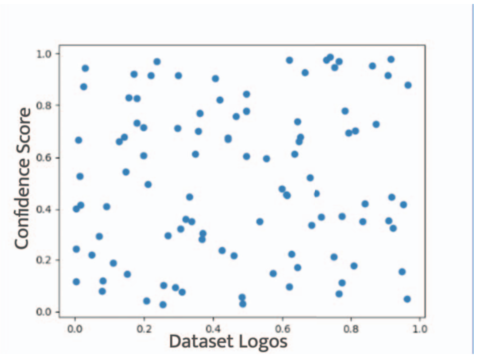


Fig. 9. scattered plot of the test logos

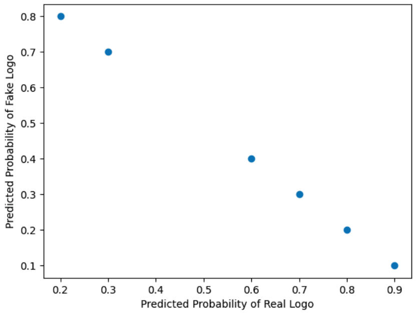


Fig. 10. scatter plot for prediction of fake logo

References

[1] Bhattacharya, Tathagata, et al ”Capping carbon emission from green data centers.” International Journal of Energy and Environmental Engineering (2022): 1-15.

[2] Peng, Xiaopu, et al. ”Exploiting Renewable Energy and UPS Systems to Reduce Power Consumption in Data Centers.” Big Data Research 27 (2022): 100306.

[3] Bhattacharya, Tathagata, and Xiao Qin. ”Modeling Energy Efficiency of Future Green Data centers.” 2020 11th International Green and Sustainable Computing Workshops (IGSC). IEEE, 2020.

[4] Bhattacharya, Tathagata, et al. ”Accelerating the Energy Efficient Design of Traditional Data Centers Through Modeling.” 2022 IEEE International Conference on Networking, Architecture and Storage (NAS). IEEE, 2022.

[5] Bhattacharya, Tathagata, et al. ”Performance modeling for I/O-intensive applications on virtual machines.” Concurrency and Computation: Practice and Experience 34.10 (2022): e6823.

[6] Cao, Ting, et al. ”DDoS Detection Systems for Cloud Data Storage.” 2021 Third IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA). IEEE, 2021.

[7] Henry George Liddell and Robert Scott, An Intermediate Greek–English Lexicon: logos, 1889.

[8] Entry at LSJ online.

[9] . Owl.purdue.edu // Purdue Writing Lab ”Aristotle's Rhetorical Situation // Purdue Writing Lab”. Owl.purdue.edu. Retrieved 2022-03-16.

[10] Cambridge Dictionary of Philosophy (2nd ed): Heraclitus, (1999).

[11] Paul Anthony Rahe, Republics Ancient and Modern: The Ancien Régime in Classical Greece, University of North Carolina Press (1994), ISBN 080784473X, p. 21.

[12] Rapp, Christof, ”Aristotle's Rhetoric”, The Stanford Encyclopedia of Philosophy (Spring 2010 Edition), Edward N. Zalta (ed.)

[13] David L. Jeffrey (1992). A Dictionary of Biblical Tradition in English Literature. Grand Rapids, Michigan: Wm. B. Eerdmans Publishing Co. p. 459. ISBN 978-0802836342.

[14] Cambridge Dictionary of Philosophy (2nd ed): Philo Judaeus, (1999).

[15] Adam Kamesar (2004). ”The Logos Endiathetos and the Logos Prophorikos in Allegorical Interpretation: Philo and the D-Scholia to the Iliad” (PDF). Greek, Roman, and Byzantine Studies (GRBS). 44: 163–181. Archived from the original (PDF) on 2015-05-07.

[16] May, Herbert G. and Bruce M. Metzger. The New Oxford Annotated Bible with the Apocrypha. 1977.

[17] Afroz, S., Greenstadt, R.: PhishZoo: detecting phishing websites by looking at them. In: 2011 IEEE Fifth International Conference on Semantic Computing. IEEE, September 2011. https://doi.org/10.1109/icsc.2011.52

[18] Bozkir, A. S., & Aydos, M. (2020). LogoSENSE: A companion HOG based logo detection scheme for phishing web page and E-mail brand recognition. Computers & Security, 95, 101855.

[19] Hout, T. V. D., Wabeke, T., Moura, G., & Hesselman, C. (2022, March). LogoMotive: detecting logos on websites to identify online scamsa TLD case study. In International Conference on Passive and Active Network Measurement (pp. 3-29). Springer, Cham.

[20] Hesselman, C. (2022). LogoMotive: Detecting Logos on Websites to Identify Online Scams-A TLD Case Study. In Passive and Active Measurement: 23rd International Conference, PAM 2022, Virtual Event, March 28-30, 2022: Proceedings (Vol. 13210, p.

[21] Zhang, X., & Ghorbani, A. A. (2020). An overview of online fake news: Characterization, detection, and discussion. Information Processing & Management, 57(2), 102025.

[22] Giachanou, A., Zhang, G., & Rosso, P. (2020, October). Multimodal multi-image fake news detection. In 2020 IEEE 7th International Conference on Data Science and Advanced Analytics (DSAA) (pp. 647-654). IEEE.

[23] Zhang, D., Zhou, L., Kehoe, J. L., & Kilic, I. Y. (2016). What online reviewer behaviors really matter? Effects of verbal and nonverbal behaviors on detection of fake online reviews. Journal of Management Information Systems, 33(2), 456-481.

[24] Alghamdi, B., & Alharby, F. (2019). An intelligent model for online recruitment fraud detection. Journal of Information Security, 10(03), 155.

[25] Yan, W. Q., Wang, J., & Kankanhalli, M. S. (2005). Automatic video logo detection and removal. Multimedia Systems, 10(5), 379-391.

[26] Bao, Y., Li, H., Fan, X., Liu, R., & Jia, Q. (2016, August). Region-based CNN for logo detection. In Proceedings of the International Conference on Internet Multimedia Computing and Service (pp. 319-322).

[27] Li, K. W., Chen, S. Y., Su, S., Duh, D. J., Zhang, H., & Li, S. (2014). Logo detection with extendibility and discrimination. Multimedia tools and applications, 72(2), 1285-1310.

[28] Eggert, C., Winschel, A., Lienhart, R.: On the benefit of synthetic data for company logo detection. In: Proceedings of the 23rd ACM International Conference on Multimedia. ACM, October 2015. https://doi.org/10.1145/2733373.2806407

[29] FBI: FBI Warns Public to Beware of Government Impersonation Scams, April 2021. https://www.fbi.gov/contact-us/field-offices/boston/news/press-releases/fbi-warns-public-to-beware-of-government-impersonation-scams

[30] Fielding, R., Reschke, J.: Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content. RFC 7231, IETF, June 2014. http://tools.ietf.org/rfc/rfc7231.txt

[31] FTC: How To Avoid a Government Impersonator Scam, April 2021. https://www.consumer.ftc.gov/articles/how-avoid-government-impersonator-scam

[32] Goel, R.K.: Masquerading the government: drivers of government impersonation fraud. Public Finan. Rev. 49(4), 548–572 (2021)

[33] Google: Google Public DNS (2021). https://developers.google.com/speed/public-dns/

[34] Google Inc.: Certificate transparency. https://certificate.transparency.dev/

[35] Han, Y., Shen, Y.: Accurate spear phishing campaign attribution and early detection. In: Proceedings of the 31st Annual ACM Symposium on Applied Computing. ACM, April 2016. https://doi.org/10.1145/2851613.2851801

[36] Hesselman, C., Moura, G.C., Schmidt, R.D.O., Toet, C.: Increasing DNS security and stability through a control plane for top-level domain operators. IEEE Commun. Mag. 55(1), 197–203 (2017). https://doi.org/10.1109/mcom.2017.1600521cm

[37] Hill, K.: The Secretive Company That Might End Privacy as We Know It, January 2020. https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html

[38] Hoffman, P., Sullivan, A., Fujiwara, K.: DNS Terminology. RFC 8499, IETF, November 2018. http://tools.ietf.org/rfc/rfc8499.txt

[39] Introna, L.D.: Disclosive ethics and information technology: disclosing facial recognition systems. Ethics Inf. Technol. 7(2), 75–86 (2005). https://doi.org/10.1007/s10676-005-4583-2

[40] Kingma, D.P., Ba, J.: Adam: a method for stochastic optimization (2017)

[41] David L. Jeffrey (1992). A Dictionary of Biblical Tradition in English Literature. Grand Rapids, Michigan: Wm. B. Eerdmans Publishing Co. p. 460. ISBN 978-0802836342.

[42] Henry George Liddell and Robert Scott, An Intermediate Greek–English Lexicon: lexis, 1889.

[43] Henry George Liddell and Robert Scott, An Intermediate Greek–English Lexicon: legō, 1889.

[44] F. E. Peters, Greek Philosophical Terms, New York University Press, 1967.

[45] W. K. C. Guthrie, A History of Greek Philosophy, vol. 1, Cambridge University Press, 1962, pp. 419ff.

[46] The Shorter Routledge Encyclopedia of Philosophy

[47] Translations from Richard D. McKirahan, Philosophy before Socrates, Hackett, (1994).

[48] Handboek geschiedenis van de wijsbegeerte 1, Article by Jaap Mansveld & Keimpe Algra, p. 41

[49] W. K. C. Guthrie, The Greek Philosophers: From Thales to Aristotle, Methuen, 1967, p. 45.

[50] Aristotle, Rhetoric, in Patricia P. Matsen, Philip B. Rollinson, and Marion Sousa, Readings from Classical Rhetoric, SIU Press 1990), ISBN 0809315920, p. 120.

[51] In the translation by W. Rhys Roberts, this reads ”the proof, or apparent proof, provided by the words of the speech itself”.

[52] Eugene Garver, Aristotle’s Rhetoric: An art of character, University of Chicago Press (1994), ISBN 0226284247, p. 114. Garver, p. 192.

[53] Robert Wardy, ”Mighty Is the Truth and It Shall Prevail?”, in Essays on Aristotle’s Rhetoric, Amélie Rorty (ed), University of California Press (1996), ISBN 0520202287, p. 64.

[54] Translated by W. Rhys Roberts, http://classics.mit.edu/Aristotle/rhetoric.mb.txt (Part 2, paragraph 3)

[55] https://logos-world.net/nike-logo/

[56] https://www.dailymail.co.uk/femail/article-7747625/Tricky-pictures-challenge-players-spot-real-logo-fake.html

[57] https://raw.githubusercontent.com/ilmonteux/logohunter/master/pipeline.gif

[58] M. Iswarya, S. Arun Shankar and S. Abdul Hameed, ”Fake Logo Detection,” 2022 1st International Conference on Computational Science and Technology (ICCST), CHENNAI, India, 2022, pp. 998-1001, doi: 10.1109/ICCST55948.2022.10040325.