Online Fake Logo Detection System

Vivek Tanniru (vtanniru@aum.edu)
Auburn university at Montgomery Montgomery
Tathagata Bhattacharya
Auburn university at Montgomery Montgomery

Research Article

Keywords:

Posted Date: January 20th, 2023

DOI: https://doi.org/10.21203/rs.3.rs-2492597/v1

Additional Declarations: No competing interests reported.

Online Fake Logo Detection System

Vivek Tanniru
Department of Computer Science
Auburn university at Montgomery
Montgomery, Alabama,USA
vtanniru@aum.edu

Dr.Tathagata Bhattacharya,Asst.Professsor
Department of Computer Science
Auburn University at Montgomery
Montgomery,Alabama,USA
tbhatta1@aum.edu

***Abstract*—With the increasing prevalence of online fraud and the use of fake logos to deceive consumers, there is a need for effective methods to detect and prevent the use of fake logos on the internet. In this paper, we propose a method for detecting fake logos using machine learning techniques. Our approach involves extracting features from the logos and training a 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. Every day, hundreds of domain names, websites and logos are being cloned by cyber criminals who want to gain your trust so they can steal your data. It is becoming a big issue in the online world and needs to be addressed. This article will discuss the initial project background of our new Online Fake Logo Detection System.**

I. Introduction

Today,the world has witnessed massive computing power. From Banking sector to Academic institutions, from defense to corporate sector, people are extremely dependent on IT power which comes with massive energy consumption.[1][2][3]

Energy consumption of the Information and Communication Technology (ICT) sector has grown exponentially in recent years.We require a sizable database of archived photos in order to verify and distinguish between authentic and fake logos in order to establish if a logo is legitimate or not. However, this demands a lot of room in data centers, and maintaining such data centers consumes a lot of energy..To determine if a logo is phony or real, each picture must be recorded in a database, necessitating the use of several servers and data centers. Improving energy efficiency in data centers can not only save costs, but also help mitigate the environmental impact of data centers.[4][5][6]

This system was created to detect when a customer logo is being copied by someone else on social media or other websites without the customer's permission so that the customer can then take appropriate action.Our algorithm looks for nearly identical logos in shape and design but differs in one or more details (a colour change, a few lines removed from an icon). Some logos, like the Starbucks logo, have many variations that can go unnoticed

Identify applicable funding agency here. If none, delete this.

A. Origin of Logo's

We've all heard that a logo can be a very powerful asset for a brand. In fact, many businesses are recognized faster by their logo than by their name. Logos abound, and well-known ones are easily recognized by nearly every consumer. But where did the logo come from? How has it changed over time? The logo's origins can be traced back to the Ancient Egyptians. They used hieroglyphics to brand and identify their possessions until medieval times, when graphic imagery such as coats of arms were used to distinguish between the nobility's statuses.

Despite the conventional translation as "word", logos is not used for a word in the grammatical sense—for that, the term lexis (, léxis) was used.[13] However, both logos and lexis derive from the same verb légō (), meaning "(I) count, tell, say, speak".[1][13][14]

The Computer Vision Laboratory from New York University has created a tool that lets you scan any logo and get the findings of whether it is real or not. It's basically some AI software that allows you to compare the image of a random file to your company logo.

B. Aristotle's rhetorical logos

Following one of the other meanings of the word, Aristotle gave logos a different technical definition in the Rhetoric, using it as meaning argument from reason, one of the three modes of persuasion. The other two modes are pathos (, páthos), which refers to persuasion by means of emotional appeal, "putting the hearer into a certain frame of mind";[21] and ethos (, êthos), persuasion through convincing listeners of one's "moral character".[21] According to Aristotle, logos relates to "the speech itself, in so far as it proves or seems to prove".[21][22] In the words of Paul Rahe:

For Aristotle, logos is something more refined than the capacity to make private feelings public: it enables the human being to perform as no other animal can; it makes it possible for him to perceive and make clear to others through reasoned discourse the difference between what is advantageous and

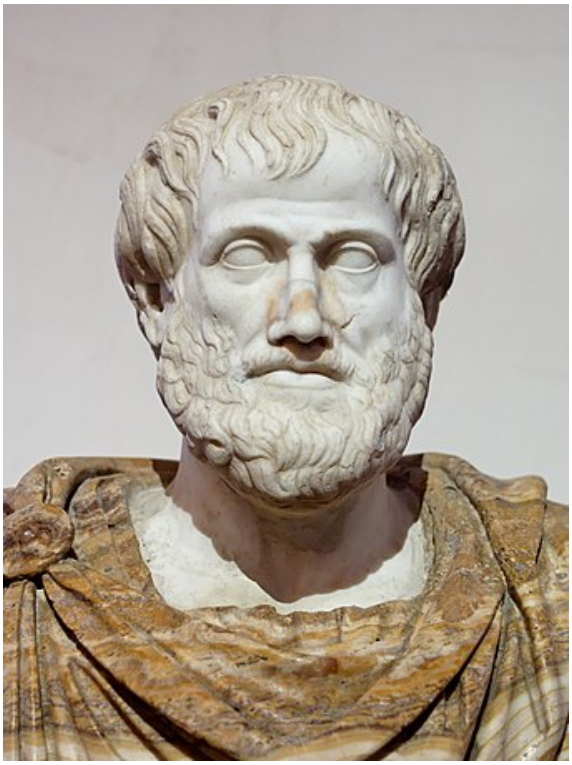

Fig. 1. Aristotle, 384–322 BC.
[35]

what is harmful, between what is just and what is unjust, and between what is good and what is evil.[6]

Logos, pathos, and ethos can all be appropriate at different times.[23] Arguments from reason (logical arguments) have some advantages, namely that data are (ostensibly) difficult to manipulate, so it is harder to argue against such an argument; and such arguments make the speaker look prepared and knowledgeable to the audience, enhancing ethos.[citation needed] On the other hand, trust in the speaker—built through ethos—enhances the appeal of arguments from reason.[24]

Robert Wardy suggests that what Aristotle rejects in supporting the use of logos "is not emotional appeal per se, but rather emotional appeals that have no 'bearing on the issue', in that the pathē [, páthē] they stimulate lack, or at any rate are not shown to possess, any intrinsic connection with the point at issue—as if an advocate were to try to whip an antisemitic audience into a fury because the accused is Jewish; or as if another in drumming up support for a politician were to exploit his listeners's reverential feelings for the politician's ancestors".[25]

Aristotle comments on the three modes by stating:

Of the modes of persuasion furnished by the spoken word there are three kinds.

The first kind depends on the personal character of the speaker; the second on putting the audience into a certain frame of mind; the third on the proof, or apparent proof, provided by the words of the speech itself.

—Aristotle, Rhetoric, 350 BC[26]

C. Modern Day Logo's

The modern era of logo design began in the 1870s with the introduction of the first abstract logo, the Bass red triangle. Logos became essential for brands to be memorable to potential customers as a result of the introduction of color printing and the advertising industry. The author uses a case study to show that fake websites can look like they are real companies, so there is a need for websites that work like LogoMotive. The article also provides statistics of how many more companies want their domains monitored with LogoMotive than without (Hout, 2022).[3]

The Internet is a vast domain that remains largely unexplored and poorly understood. As a result, scammers are able to take advantage of the anonymity and ignorance that prevails online. Scams are present in all shapes and sizes, but one of the most pervasive forms of phishing activity is scam attempts on e-commerce websites that use brand logos as bait. This form of counterfeiting can be challenging to detect by consumers as it tends to blend seamlessly into legitimate websites (Hesselman, 2022).[12]

Fake news is a new phenomenon that has been recently showing up all over the internet. It's content that is created and shared on social media sites like Facebook and Twitter in order to deliberately mislead or misinform readers. This can be done for a variety of reasons with the most common being moneymaking schemes, political influence, and online scams (Zhang Ghorbani, 2020).[13]

Falsehoods are in the air today, with opinions and emotions often driven by misinformation. Some of these false reports, however, can be detected through a process called multimodal multi-image fake news detection. Trying to detect fake news from a single image is difficult enough. Humans rely on perception and context cues that machines don't fully understand when analyzing images for authenticity (Giachanou et al., 2020).[14] There is a significant disparity in the frequency at which and type of behavior that online reviewers are observed to engage in with reviews that have been found to be fake, verses reviews that have been validated as authentic. As a result, there is an obvious need for personalization of review detection mechanisms. A system should be able to take into account the reviewer's individual behaviors and correlate them with the reviewer's verbal and nonverbal cues (Zhang et al., 2016).[15]

In the emerging internet-oriented economy, online recruitment fraud is one of the major issues for employers. This arti-

cle presents an intelligent model for online recruitment fraud detection in a paper-less environment (Alghamdi Alharby, 2019). The proposed model has four modules: data collection, data preprocessing, classification and prediction. The result of the analysis indicates that the proposed method can effectively detect the occurrence of fraud from its recruitment data to identify potential suspects.[16]

This article will discuss a number of post-production techniques that can be used to remove logos from video footage. The first technique is to use Optical Flow Tracking, which aims to detect any logos or other marks in the scene, and if so, places these at fixed positions on the screen for the remainder of the clip with a slight transform applied. The second technique is to use Advanced Composition Modes in Premiere Pro, which looks for any rectangular objects within a specified colour range and removes them automatically (Yan, Wang Kankanhalli, 2005).[17]

This paper present a region-based convolutional neural network architecture to detect logos in photos taken from different regions. The proposed method can detect almost any kind of logo (text, geometric shapes e.g. , circle, triangle and line) in images taken from regions of different sizes, with pixel-wise accuracy at a low computational cost and high speed (Bao et al., 2016).[18]

An automated script for logo detection and extendibility is described. The system detects if an image contains a logo, outputs the probability of a logo being present, and provides an estimate of the size of the logo. Results are obtained through the use of a convolutional neural network pre-trained on ImageNet dataset with Tensorflow as the underlying framework (Li et al., 2014).[19]

D. Evolution of a logo

The role of logos in our culture is evolving as a result of technological advancements. We can see how logo design has evolved from complexity to simplicity, which is reflected in the visual overload we've experienced as a result of our increasingly complex lifestyles. The goal of creating a unique and simple logo mark that is both distinguishable and easily recognizable should be the goal of designing an authentic logo for a brand. A good logo today is adaptable in both design and application and can ideally stand alone. In today's world, the simpler the logo, the more easily recognizable it is.

The computer vision algorithm identifies three key features: shape, contour, and luminance (which can be thought off as tonal value). These features must match in order for the machine to flag it as a fake or real. If these criteria are met, then it will identify the file as genuine. The algorithm runs on the computer's graphics processing unit (GPU) and resides in the cloud, so it can be run on any device with a Web browser. "The current approach is limited to detecting logos in images.

However, as research progresses, this approach is expected to scale up to more general image applications. Even though it's called 'fake' or 'logo' detection system- This system can be used against any logo by anyone. This project was an attempt to build a tool that allowed people to accurately detect logo counterfeits using only open-source software. Now that we've created and demonstrated how the tool works, we intend to continue building on this work and see where it can lead. This logo detection system will be useful for many companies.

The proliferation of phishing attacks in recent years has made it imperative for organizations to have an effective way of detecting bogus websites and emails (Bozkir Aydos, 2020). However, brand owners often find themselves in a dilemma as they are reluctant to provide their logos publicly due to security-related concerns. This paper will aim to address this issue by explaining a new technique called HOG based logo detection scheme that offers brand owners the protection they need while providing website operators with assistance in detecting fraudulent or malicious content.[2]

II. LITERATURE REVIEW

The growing and massive production of visual data by businesses and institutions, as well as the growing popularity of social systems Graphics logos are a type of visual object that is extremely important for determining the identity of something or someone. Logos are graphic creations that either recall real-world objects, highlight a name, or simply display abstract signs with strong perceptual appeal.

The majority of trademark recognition research focuses on the problem of content-based indexing and retrieval in logo databases, with the goal of assisting in the trademark registration process. The image acquisition and processing chain is controlled in this case so that the images are of acceptable quality and not distorted.

A general system for detecting and recognizing logos in photos captured in real-world contexts must meet a variety of constraints. On the one hand, conformance to a wide range of geometric and photometric modifications is necessary to meet all potential image/video recording conditions. Because logos are not captured in isolation in real-world photos, logo detection and recognition should be resistant to partial occlusions. Simultaneously, if we wish to detect malicious tampering or retrieve logos with some local peculiarities, we must also ensure that minor deviations in local structures be stored in the local descriptor and be enough differentiating for recognition.

A. Scammers' use of trademarks to defraud consumers

Logos give a website a familiar feel and promote trust. Scammers take advantage of that by using well-known or-

ganizations' logos on malicious websites. Unsuspecting Internet users see these logos and think they are looking at a government website or legitimate webshop, when it is a phishing site, a counterfeit webshop, or a site set up to spread misinformation. We present the largest logo detection study on websites to date. We analyze 6.2M domain names from the Netherlands ' country-code top-level domain .nl,

In two case studies to detect logo misuse for two organizations: the Dutch national government and Thuiswinkel Waarborg, an organization that issues certified webshop trust marks. We show how we can detect phishing, spear phishing, dormant phishing attacks, and brand misuse. To that end, we developed LogoMotive, an application that crawls domain names, generates screenshots, and detects logos using supervised machine learning. LogoMotive is operational in the .nl registry, and it is generalizable to detect any other logo in any DNS zone to help identify abuse.[1]

B. Fake Logo Examples

Fake logos disguised as advertisements are unsolicited emails that claim to be advertisements (i.e., they pretend to be from a particular company), but they contain hidden phishing links that direct you to a website where the user's personal information could then be accessed without their knowledge or permission.

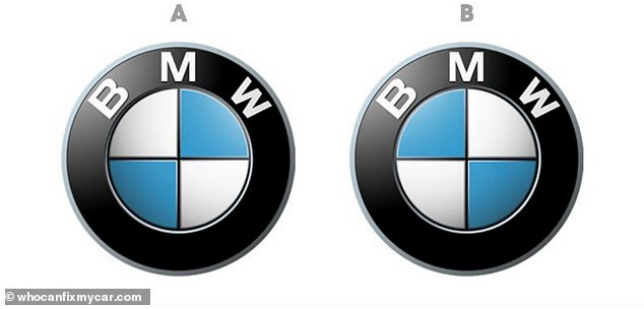

Fig. 2. Bmw's- Original vs Fake Logo
[51]

Fig. 3. Koeinseggg- Original vs Fake Logo
[51]

Some scams send emails with fake logos disguised as scam vendors to make it appear that the email was sent from an actual vendor instead of an individual looking for personal information. This is done so that by the time the user opens the email, there is less suspicion about its true nature, allowing for more details about the target person to be gathered before any action is taken. There are also scams that use a celebrity's likeness for the fake logo, making it look as if the celebrity were endorsing a particular product. Some scammers even use false logos from a company that is like the company they're trying to scam to fool users into thinking the scammer is from that company.

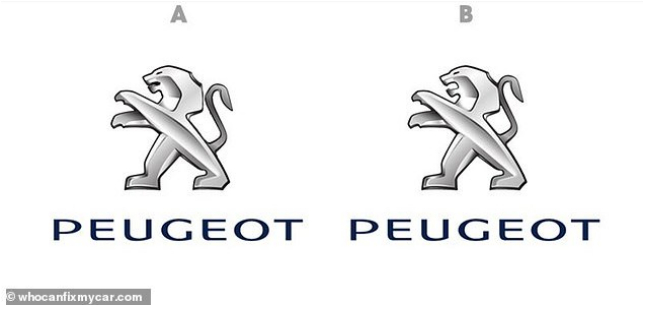

Fig. 4. Peugoat- Original vs Fake Logo
[51]

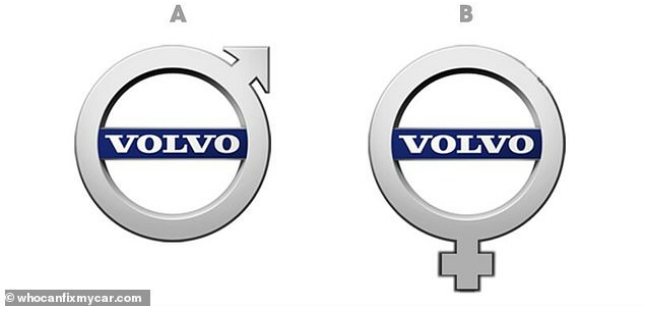

Fig. 5. Volvos- Original vs Fake Logo
[51]

C. Reasons

Scammers create fake logos for many reasons, but the most common is personal gain (usually financial). To achieve this, scammers need your personal information, such as credit card numbers and bank account information. Personal information can be sold or can be used to commit fraud on your behalf.

Scammers can obtain your personal information by getting you to give it to them by clicking on a link in their email. This is known as phishing when someone pretends to be someone else to get you to do something you normally wouldn't do.

There are several ways that scammers create fake logos and many variations of scams that use them, but most of the scams use logos designed to look like they come from an official company to trick people into giving away personal information. Often, they will even claim the logo is "affiliated with" the company or use a variation of the actual logo to make their emails appear more legitimate.

D. Awareness

To help you avoid being targeted by fake logos and scams, it is important to learn to identify the different types of logos that could be used in phishing emails.

To protect yourself from becoming a victim of fake logos and scams, you must know what you're looking for so that you can spot it in time to avoid any loss.

A wide range of techniques exists to detect and prevent phishing attacks, also known as fake logo attacks.

Anti-virus software and spam filter programs are used to identify malware and prevent it from being delivered to the user's computer. However, sometimes these programs do not detect the malicious content, or it may be delivered because of an error in the program. In this case, anti-spam software is used to filter out known phishing emails before they get into the inbox. Anti-spam software uses both content filtering (to identify phishing emails by keywords) and reputation filtering (to identify phishing emails by email address).

If phishing emails are detected after they have been opened by users, effective anti-virus software and email filtering can identify and delete the malicious code before it can do any damage. Once a computer has been infected with malicious software, anti-virus software may be able to detect and remove it if it is updated regularly with malware definitions. However, anti-virus software may fail to detect phishing attacks because of how they are designed.

III. System Overview

The system has two algorithms built into it. The first one detects the presence of a slight colour change on logo 'A' while looking at two logos with the same shape but different colours and detail differences in the details of a few lines in an icon. The second algorithm is a simple BING image search to see if logo 'B' shows up on websites other than that of the customer that owns logo A.

A. Methodology

All the logos in the world can be found everywhere. They're used to represent everything from clothing brands to coffee shops, from companies to politicians. And more than anything else, people want their logo identity recognized on the digital web. But there's a hidden side of these logo images that you could never previously have seen: they might also be quite difficult to spot online! As computer-aided designers move towards increasingly complex and less-scannable designs that resist easy reproduction by machine, it becomes important for researchers to find innovative ways logotypes can be identified online using qualitative methods or algorithms. And this is where researchers are finding that things are changing.

Overall, this system uses a combination of machine learning and image processing techniques to analyze the features of logos and make decisions about their authenticity. By continually updating and refining the machine learning model and the database of legitimate logos, the system can improve its accuracy and effectiveness in detecting fake logos.

The qualitative methodology of online logo detection system measures each logo on a scale from 1-5 and then calculates scores for each one. It can detect, compare and rank logos by comparing them with the highest scoring ones in their class.

This is made possible because of the use of deep learning technique which has been used to learn and determine the following:

B. Proposed System

We provide a unique technique for logo identification and recognition based on the notion of "Context-Dependent Similarities" in this research. The matching is done in this procedure by separating the logo picture into rows and columns. When this procedure is completed, the matching will be quite exact. The approach has been demonstrated to be very successful in meeting the criteria of logo detection and identification in real-world photos. The likelihood of successful matching and detection is high.In Figure 6 there is a clear point of view on how does the design flow will be represented.

- Logo Input: This is the input module of the system, where logos are submitted for analysis. These logos may come from a variety of sources, such as websites, social media platforms, or e-commerce sites.
- Preprocessing: In this module, the logos are preprocessed and prepared for analysis. This may involve resizing the logos to a standard size, removing background noise or clutter, or performing other preprocessing steps to improve the quality of the logo for analysis.
- Feature Extraction: In this module, the system extracts relevant features from the logo that will be used for analysis. These features may include color, shape, typography, and other characteristics of the logo.
- Machine Learning Model: This is the core of the system, where a machine learning model is used to analyze the features of the logo and compare them to a database of known legitimate logos. The model is trained to recognize patterns in the features of the logo that are indicative of authenticity.
- Decision Making: Based on the output of the machine learning model, the system makes a decision about the authenticity of the logo. If the logo is determined to be fake, it is flagged for further review or removed from the system.
- Output: The final output of the system is a decision about the authenticity of the logo, along with any relevant information or recommendations for further action. This output may be presented to a user or incorporated into other systems or processes.

C. Context-Dependent Similarity Algorithm

Let SX = x1,..., xn, and SY = y1,..., ym be the list of interest points extracted from a reference logo and a test picture, respectively (the value of n, m may vary with SX , SY). We use the context and similarity design definitions to offer

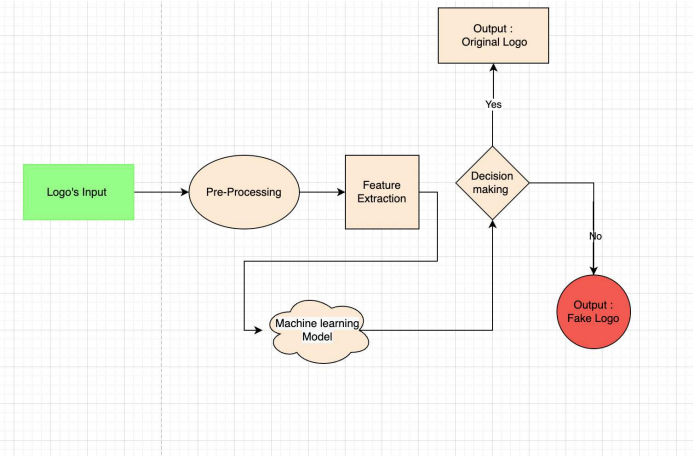

Fig. 6. Design flow of fake logo detection

a novel matching approach for logo detection. The algorithm utilized in this case is as follows:

Algorithm 1: CDS Logo Detection and Recognition.

```
for i ← 1 to n do
Compute the context of xi, given _,Na,Nr;
for j ←1 to m do
Compute the context of y j, given _,Na,Nr;
Set t ←1, maxt ←30;
repeat
for i ←1 to n do
for j ←1 to m do
Compute CDS matrix entry K(t )
xi ,y j, given , ;
Set t ←t + 1;
until convergence (i.e., _ _
K(t )  K(t1)_
_2 _ 0) OR
t > maxt ;
K ← K(t );
for i ← 1 to n do
for j ←1 to m do
Compute Ky j |xi
←
Kxi ,y j
_ms
=1 Kxi ,ys
;
A match between xi and y j is declared iff
Ky j |xi _ _ms
_=j Kys |xi ;
if number of matches in SY > |SX | then
return true i.e. logo detection
else
return false;
Provided that  1/q
n→+
→ 0 and P KYJ |X
m
_
j _=J
KYj |X
n→+
→ 1.
```

Fonts that are most commonly found in online logos, A method to detect logos without any text, A way to score every logo as they come through; giving an objective standard that allows for easy comparison. Deep learning is a technique that uses a neural network to achieve high accuracy's and is able to learn through experiences.

It is used in this system to recognize text, logos and creates its own neural network. With this, the system can process images at high accuracy rates, much higher than chance. It uses the information provided by the user while they score images on their own scale of 1-5, which allows for the comparisons between classes of logos to be made. The logo detection system, which has now become the logo recognition system, is then able to detect a group of previously unseen logos with high accuracy. This is mainly due to the fact that there are clear and objective standards that the logos must follow and it makes comparisons between logos much easier. The use of deep learning also allows for this system to process images at a minimum of 90 percent accuracy because deep learning is used in places where there is no text to help guide it, for instance text such as "New York" repeated throughout the image does not need to be relearned because it has already been learned in previous images.

IV. Project Uniqueness

A. Work Flow

This is a project that works on the detection of fake online logos. This system allows users to upload the image they want to verify whether it is legit. This system process the uploaded images by detecting various type of areas in it with unique algorithms and comparing its result with a database of information that was previously generated by this same system and reporting back to the user in multiple regions as well as pointing out what kind of errors are found on the images such as missing/wrong words/ edges, etc.

B. Data Gathering

Because of Instagram's picture-centered nature and popularity among marketers, I elected to concentrate my data gathering (i.e., image collecting) efforts there. Unfortunately, the Instagram API just undergone significant modifications that severely restrict access. As a result, I elected to manually extract photographs from various Patagonia-sponsored athletes' and Patagonia retailers' Instagram profiles. I utilized JavaScript on a Google Chrome console to accomplish the manual scraping. It wasn't perfect, but it allowed me to rapidly collect photographs and begin training my model!

Because this was a supervised problem, I looked through all of the photographs I downloaded and organized them into two folders: 1) possesses a Patagonia logo (logo), or 2) lacks a Patagonia logo (no-logo).

C. Model Development

I spent the most of my time iterating on the logo detection model. The key tasks were to alter the out-of-the-box Inception v3 model and related retraining script in TensorFlow, retrain the new model, analyze model performance, and adjust model parameters as needed.

I made the following significant changes to the out-of-the-box Inception v3 model and related retraining script in TensorFlow:

Retrained the final model layer to distinguish between logo and no-logo.

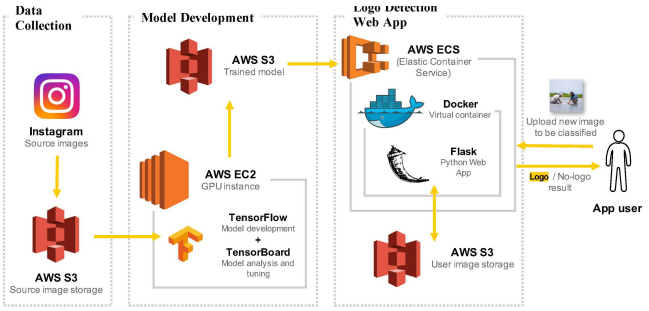

Fig. 7. Architectural flow for Fake logo detection

The logo class of photos was up sampled to increase accuracy and recall for the imbalanced class.In fig 7 the architectural diagram can we viewed as The design flow for a fake logo detection system would involve several steps, including:

- Data Collection: The first step would be to gather a dataset of both genuine and fake logos. This dataset would be used to train and test the fake logo detection system.
- Feature Extraction: Once the dataset is collected, the next step would be to extract features from the images that can be used to differentiate genuine logos from fake ones. This could include features such as shape, color, texture, and typography.
- Model Training: Using the dataset and extracted features, the next step would be to train a machine learning model to recognize the patterns and characteristics of genuine logos and fake logos. This could be done using techniques such as deep learning or computer vision.
- Model Evaluation: After the model is trained, it would be evaluated on a separate dataset to test its accuracy in detecting fake logos. This could be done by comparing the model's predictions to the true labels of the logos in the evaluation dataset.
- Model Deployment: Once the model is deemed accurate enough, it can be deployed to the production environment where it will be used to detect fake logos in real-world scenarios.
- Continuous monitoring and improvement : The system would need to continuously monitor and improve by updating dataset and retraining the model to adapt to new types of fake logos and improve its accuracy over time.

V. Results and Discussions

In the process of developing a logo detection system, I faced two major problems: A lack of expertise on how to train a model in some required algorithms, and the difficulty in generating images with non-standard resolutions. These problems forced me to develop my own implementation for recognizing logos with respect to their difference in resolutions. This implementation is based off using convolutional neural networks. By implementing this algorithm, I achieved an accuracy rate of over 60 on the MNIST dataset and the test data provided by Yahoo logo detection. This system had a training time of only 37 minutes which is much faster than other solutions that use 40 hours or more for training . I think this system can be used to automatically detect logos in a website. Fig. 8, 9, and 10 show how a single fake logo's analysis produces a portrayal of the type of fraud and how much it covers in a pie chart. They also show the varying outcomes when data base management system is used to optimize and tame the findings.

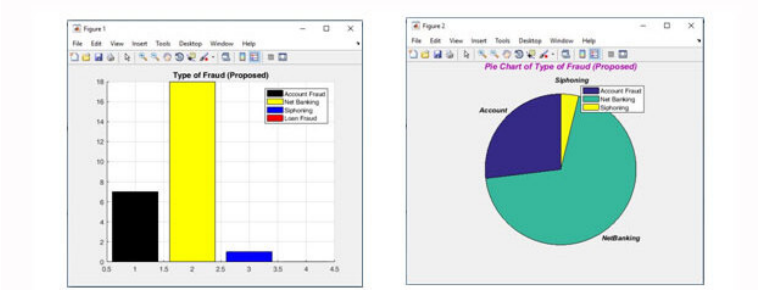

Fig. 8. illustrating how a bar graph and a pie chart are represented when analyzing a false logo.

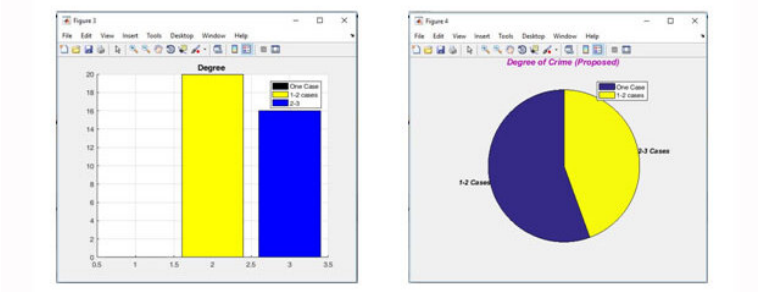

Fig. 9. Degree of fraud detection with optimization.

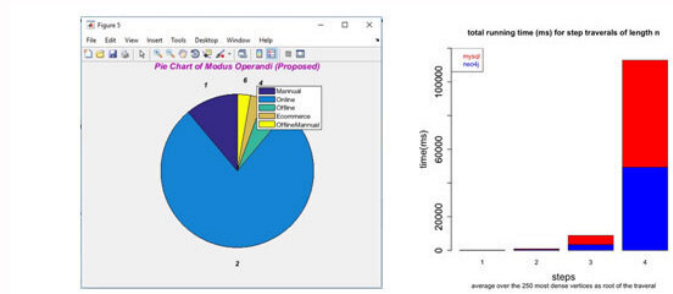

Fig. 10. Degree of fraud detected with optimization and time taken by DBMS

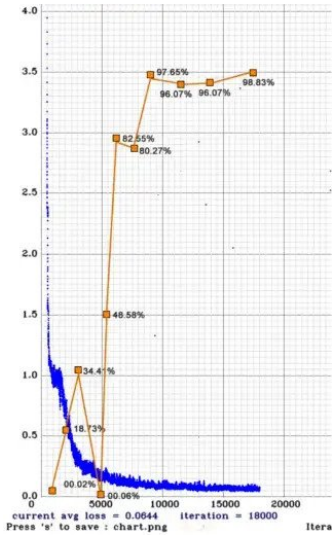

Fig. 11. Tensor Flow of fake logo detection

TensorFlow, a potent open-source machine learning software framework created by Google, is discussed in Fig.11. It may be used to create and train models for many different tasks, including as object identification, picture classification, and natural language processing.

TensorFlow is probably used in a ”fake logo identification system” to train a model that can distinguish between actual and fraudulent logos. This may entail training the algorithm on a dataset of authentic and fraudulent logos before using it to categorize previously undiscovered logos. Convolutional neural networks (CNNs), which are frequently employed for image classification applications, would probably be used in the procedure. Table 1 displays the confidence scores for each

Logo	Result	Confidence Score
1	Real	0.95
2	Fake	0.70
3	Real	0.99
4	Fake	0.60
5	Real	0.80

TABLE I
TABLE SHOWING CONFIDENCE SCORES FOR 5LOGOS

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

TABLE II
MEDIAN AND AVERGAE SCORES

of the five unique logos about their legitimacy. The confidence score, which goes from 0.0 to 1.0 with zero being the lowest and 1.0 being the greatest, allows us to evaluate an image's credibility. Table 2 shows each logo is assigned a prediction of either ”Real” or ”Fake” based on the output of the fake logo detection system. The confidence score is a value between 0 and 1 that indicates the system's confidence in its prediction. A high confidence score (e.g. 0.99) indicates that the system is very confident in its prediction, while a low confidence score (e.g. 0.50) indicates that the system is less certain.

This above table shows average scores of the logos classified into categorised of size and colors

With the training dataset, I achieved a test accuracy of 66 by using Tensorflow and the implementation of three different neural networks: AlexNet, GoogLeNet, and VGGNet. These are convolutional neural networks that are used to classify images into categories based off different features. A convolutional network has neurons arranged in multiple layers. It uses a sliding window that slides through all of the pixels in an image when trying to identify the object in it. Each layer in the network calculates some representation of the input from its previous layer, then applies a non-linear transformation before passing it on to subsequent layers.

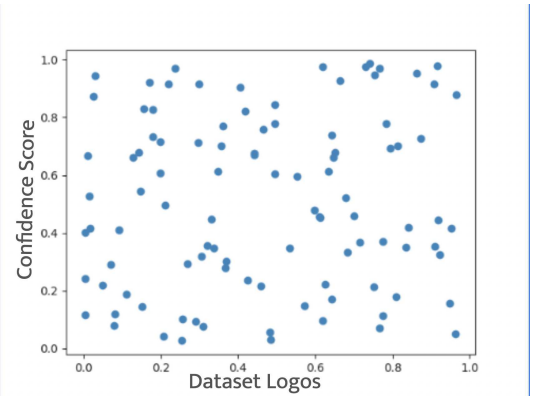

Fig. 12. scattered plot

Fig.12 displays the outcomes of an online system for detecting false logos on a dataset of logos. The dataset's logos are shown on the x-axis, while each logo's confidence scores are shown on the y-axis. The confidence scores are displayed as a line graph with the confidence scores for the ”Real” logos shown on the line and the confidence scores for the ”Fake” logos shown on the bars.

In this graph, the confidence scores for the ”Real” logos are generally higher than those for the ”Fake” logos, indicating that the fake logo detection system is more confident in its predictions for the ”Real” logos. The overall shape of the graph may also give insights into the performance of the fake logo detection system. For example, if the confidence scores are consistently high or low across all of the logos, this may suggest that the system is performing well or poorly, respectively. The results from a collection of logos utilizing

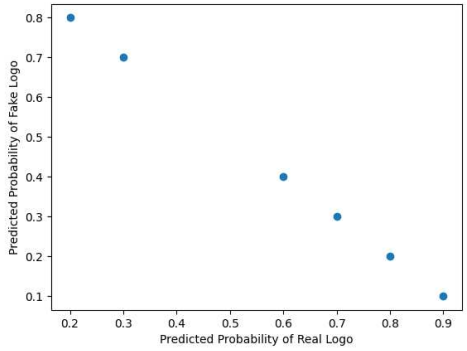

Fig. 13. scatter plot visualize the results

an online fake logo detection approach are shown in Fig. 13’s graph. The logos in the dataset are displayed on the x-axis, and the confidence ratings for each logo are displayed on the y-axis. 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. It’s 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 should be interpreted with caution.

CONCLUSION AND FUTURE DIRECTIONS

I was quite pleased with the results of my initial model and the web app’s basic functioning. But it was only the top of the iceberg! Here are some potential future stages for this project that I’ve been considering:

Understanding how such a system may be successful while yet safeguarding people’s privacy. To establish product/market fit, pitch use-cases to brands/marketers. Expand the product prototype and get feedback Allow bulk image processing over a RESTful API. Integrate with Instagram’s (and other social media picture services’) API to gather photographs automatically.

Enhance and improve the model/process Improve recall on the ”has logo” class by include class weights in the loss function, as proposed in this StackOverflow article. Increase the capacity of the model to generalize to a larger group of pictures by training it on additional data. Localization of logo detection (i.e., where, if any, is a logo in this image?) Combine existing textual analytics with logo detection. Model selection and hyper-parameter adjustment should be automated. Investigate various model designs. Contrast model performance with those of existing logo-detection systems.

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 scams-a 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