Solving reCAPTCHA v2 Using Deep Learning

David Krajewski
Carnegie Mellon University
dkrajews@andrew.cmu.edu

Eugene Li
University of Florida
lieugene@ufl.edu

1 Introduction

While deep learning has significant breakthroughs in recent years, there are rising concerns over how the technology could be misused. One such concern is over the ability of deep learning models to bypass mechanisms that are used to prevent unwanted automated access of websites.

Currently, the most popular mechanism for mitigating this type of spam is Google's reCAPTCHA. While researchers have previously shown that reCAPTCHA v1—a text recognition task–and reCAPTCHA v3—a zero-user-interaction, behind-the-scenes tracker—can be consistently bypassed with deep learning models, reCAPTCHA v2 has proven to be a more difficult challenge. To verify a human user, reCAPTCHA v2 presents a task where one must select all images that satisfy a certain prompt. For example, in Figure 1, the user is asked to select all images that contain traffic lights in them.

In this paper, we explore how deep learning could be used to crack the security of reCAPTCHA v2.

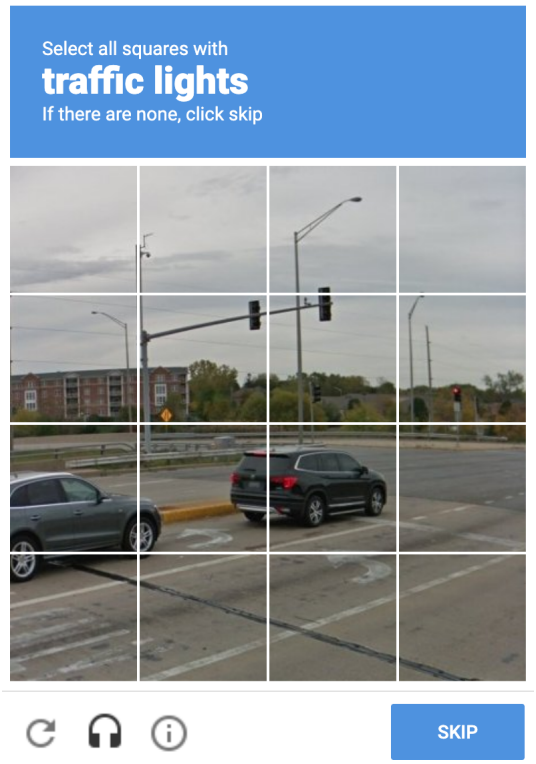

Figure 1: reCAPTCHA v2

2 Data Gathering

To create our model, we first required a large dataset of solved reCAPTCHA v2 examples. Due to the lack of a public dataset, we (actually, just David) volunteered to collect the necessary training data. While doing so, David also maintained a journal documenting the process. To improve the transparency and reproducibility of our methods, we have included select journal entries below.

Day 1

I decided to skip class today to focus on gathering training data for the model. My goal is solve at least a thousand reCAPTCHAs a day. This should allow me to reach the target size of ten thousand in a week and a half.

To find a renewable source of reCAPTCHAs to solve, I decided to simply entice Google to give them to me. The first step was to change my Gmail password to something I wouldn't remember. I opened the reset password page, closed my eyes, and haphazardly mashed my keyboard. Now, when I try to access my email, I am

greeted with plenty of reCAPTCHAs from my many failed login attempts.

After only 9 hours (including one 5-minute break), I completed today's quota. All in all, I quite enjoyed the day. I'm looking forward to beginning again tomorrow.

Day 2–5

I'm starting to feel a little fatigued. The work has proven to be rather monotonous, but I know that this dataset is the key to a successful deep learning model. I have considered outsourcing the training; however, funding is non-existent for this project.

Halfway there already.

Day 6–9

I haven't been reaching my thousand-a-day goal. It's taking me a lot more time to solve each reCAPTCHA. I think it has to do with my lack of sleep, but that's the least of my concerns at the moment.

My friends are worried about my mental well-being, my hygiene is beginning to suffer, and my eyes have not seen daylight since Day 1. But none of that matters to me. I only want more training data.

Day 10

I was supposed to be done today. I'm not.

I feel asleep at my computer last night. I don't remember much, but I can take a guess as to what I was doing. In my dreams, I was solving reCAPTCHAs as well, though I suppose those don't count towards my goal.

Day 11

My error rate has become exceedingly high. I am failing every other reCAPTCHA at this point, and the ones that I do pass are more a matter of luck than skill. I barely got through 100 today. Perhaps I need to take a break.

Day 12

You can't take a break. You need this paper to get into a good grad school. Just shut up and keep solving.

Day 13

I should have never gotten myself into this. Why couldn't Eugene have done it? Or at least we could have split the work. I bet he's living the life right now.

I despise every second I sit here. I tried going outside for some fresh air, but the sight of the street signs and traffic lights only reminded me of the work I still had to do.

Day 14

I've lost the ability to solve reCAPTCHAs. I've been utterly stuck on the same one since yesterday.

Select all images with cars in them.

How? Everything looks the same to me: cars, buses, crosswalks, fire hydrants, traffic signs. I can't tell the difference anymore. I know I'm not a robot. Please, just let me through.

Day 15

I'M NOT A ROBOT. I'M NOT A ROBOT. I'M NOT A ROBOOOOOT.

3 Conclusion

David has been powered off. His inability to do anything other than repeatedly proclaim "I'm not a robot" after Day 15 unfortunately left us no other choice.

In conclusion, our investigation has demonstrated that the state-of-the-art in deep learning— the **D**eep **A**rtificial **V**isual **I**mage **D**ecoder (**DAVID**)—is unable to solve reCAPTCHAs after a certain threshold. Even placing him inside a fully-immersive simulation and pretending the work was for a very important research paper was not enough for complete fidelity. We hope to wipe his memory, increase his RAM, and conduct the study once again.