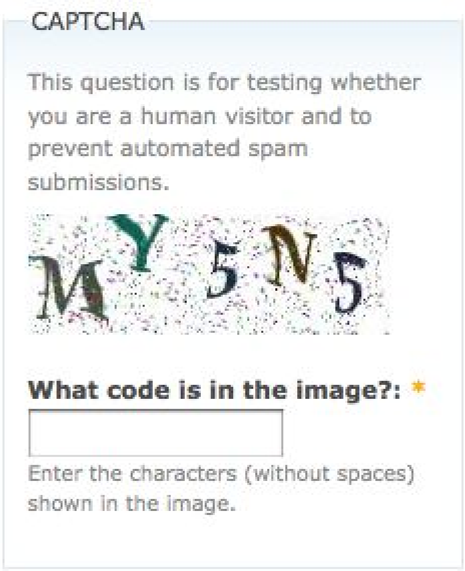
Leveraging Machine Learning for breaking captchas

Sarantopoulos Ilias
Dec. 2016

CAPTCHA

Completely **A**utomated **P**ublic **T**uring test to tell **C**omputers and **H**umans **A**part"



CAPTCHA

This question is for testing whether you are a human visitor and to prevent automated spam submissions.

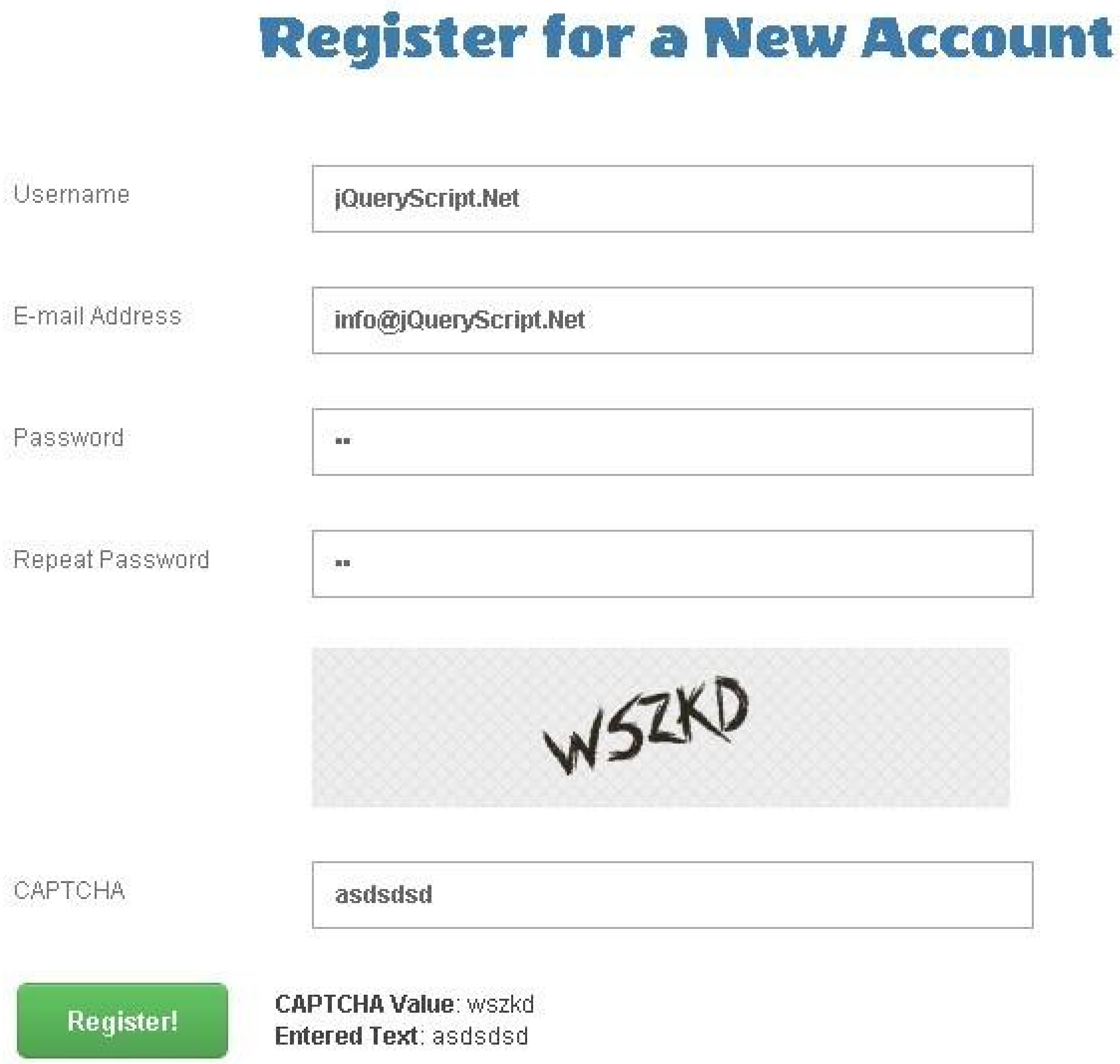
What code is in the image?: *

Enter the characters (without spaces) shown in the image.

1.

The beginning

CAPTCHA : a way to protect forms



Register for a New Account

Username	jQueryScript.Net
E-mail Address	info@jQueryScript.Net
Password	••
Repeat Password	••
CAPTCHA	asdsdsd

CAPTCHA Value: wszkd
Entered Text: asdsdsd

Benefits

- Automated
- Reduce cost
- Boost reliability

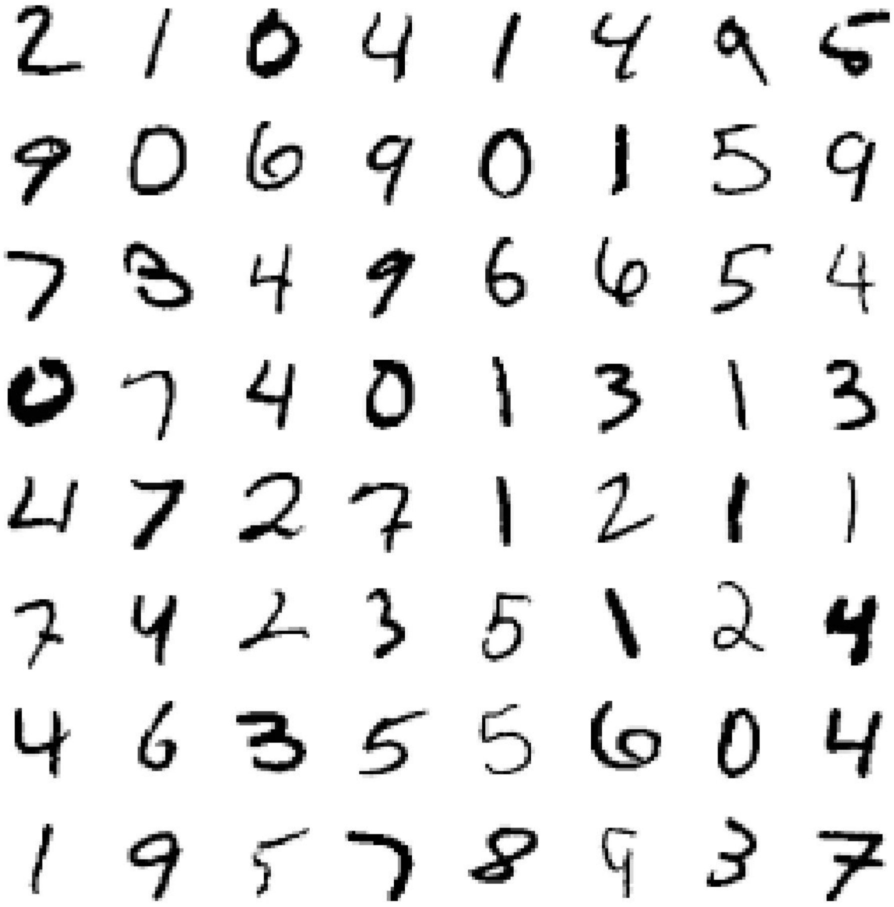
From 2003 and on it has ruled the web...

Characteristics

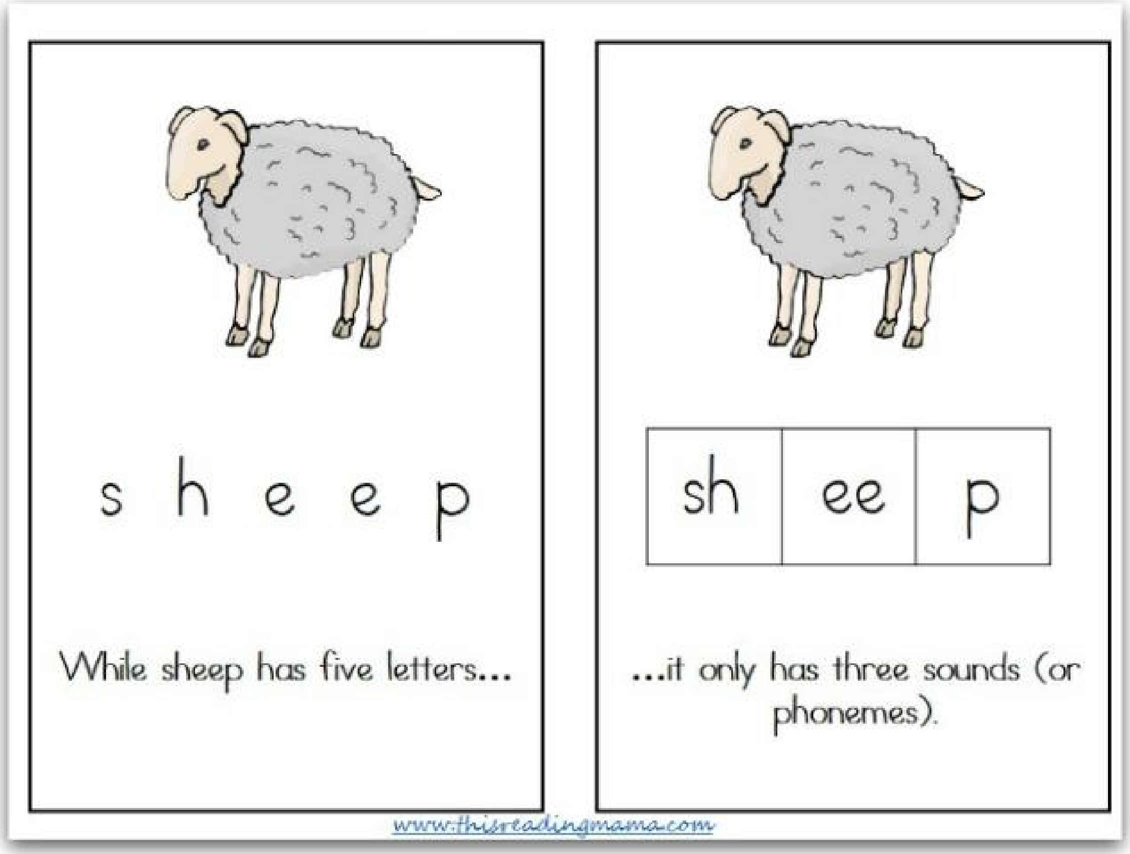
1.

Invariant recognition

There are infinite number of versions for each character that a human can identify



2. Segmentation



s h e e p

While sheep has five letters...

sh	ee	p

...it only has three sounds (or phonemes).

www.thisreadingmama.com

the ability to separate one letter from another

3.

Context

Interpretation of a letter may refer to the context of a whole word

If we see SWIM we probably understand that it is an “i” and not an l.

Forming a difficult problem

Each of these problems poses a significant challenge for a computer.

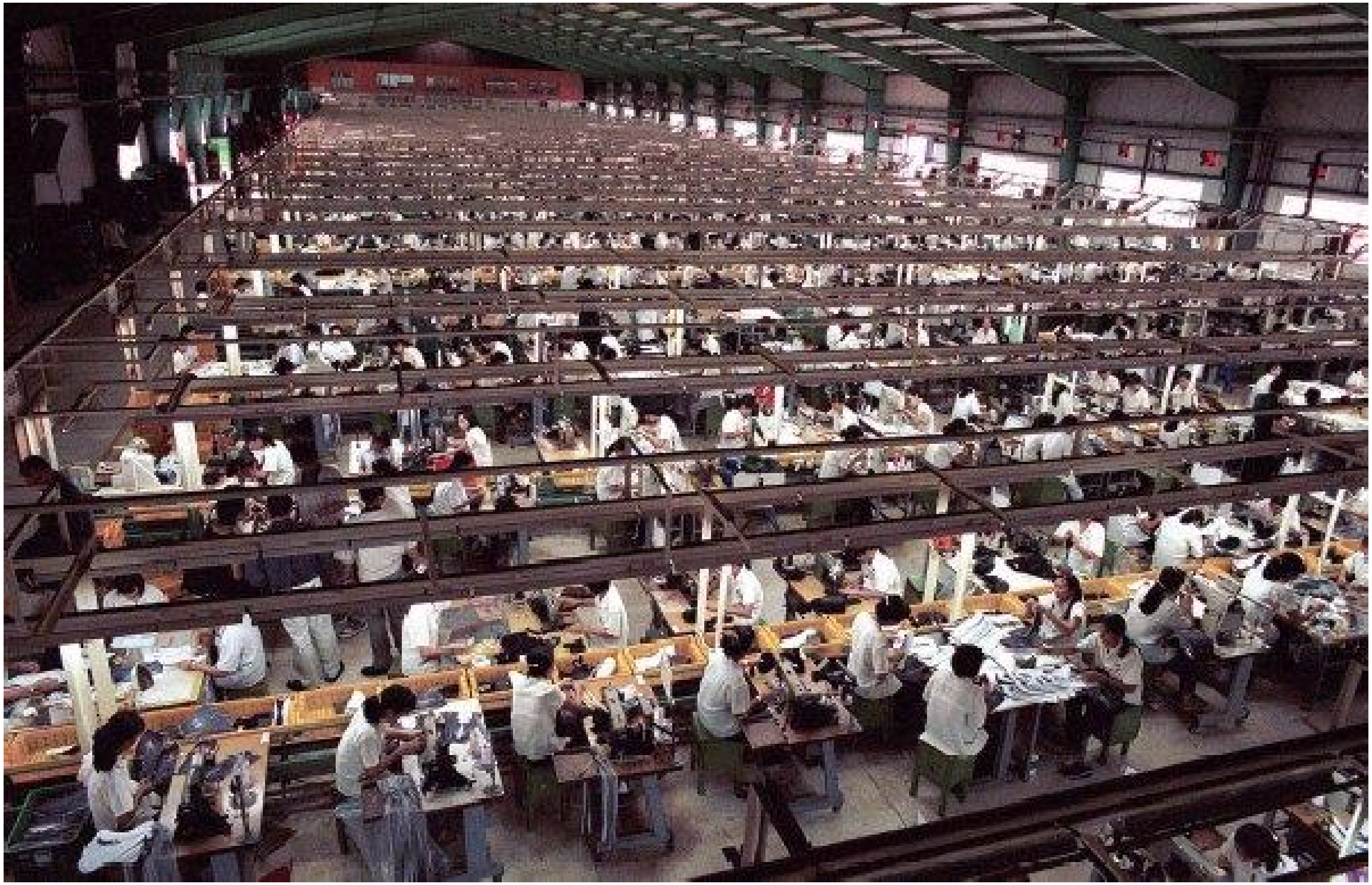
The combination of all three makes captcha solving a difficult AI problem

2.

Breaking a CAPTCHA

So how do we do it?

The stupid way



If its poorly designed...

- by reusing the session ID of a known CAPTCHA image
- If the CAPTCHA is being created on the client-side, then users can modify the client to display the un-rendered text

Or better use machine learning

- Manipulate image (remove noise etc)
- Image segmentation (extract letters)
- Learn abstract representations of letters from thousands of data
- Use the same abstract features to predict the letters from a new image

With great results!

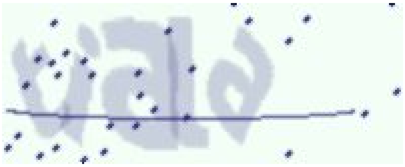
3.

Better captchas

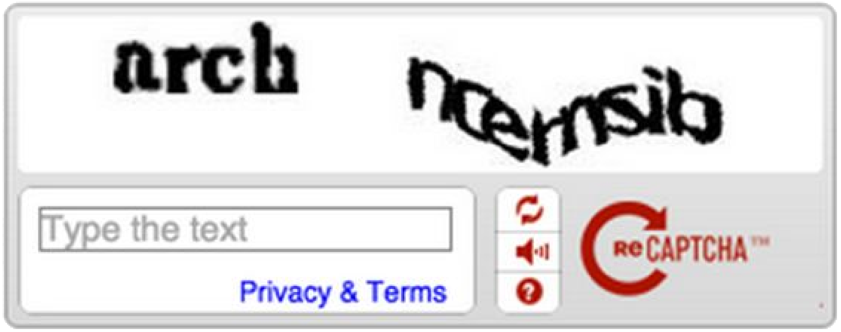
But how much better???

Try to make the more difficult for ML algorithms

- Rotate and perform “weird” transformations to each letter
- Uneven space between letters (more difficult for segmentation)
- Unconnected components

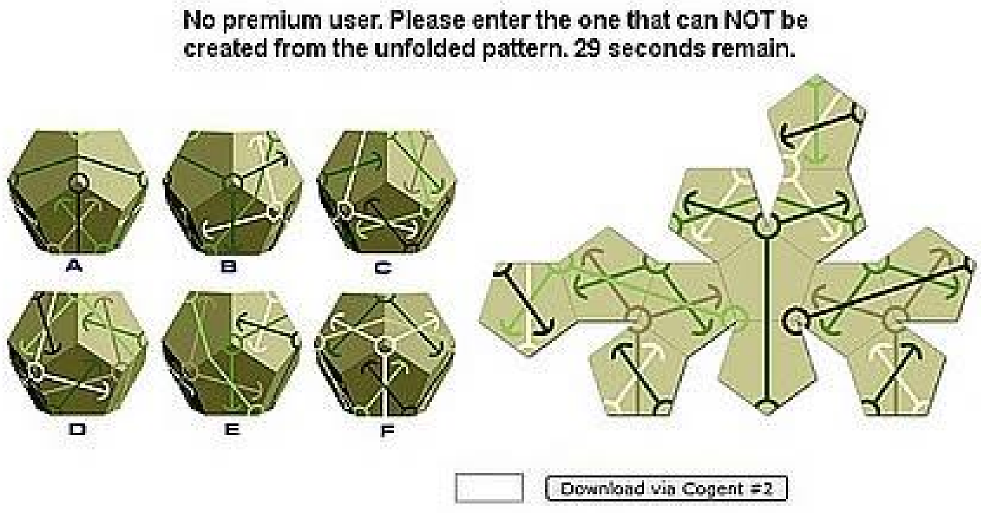


Known as reCAPTCHA

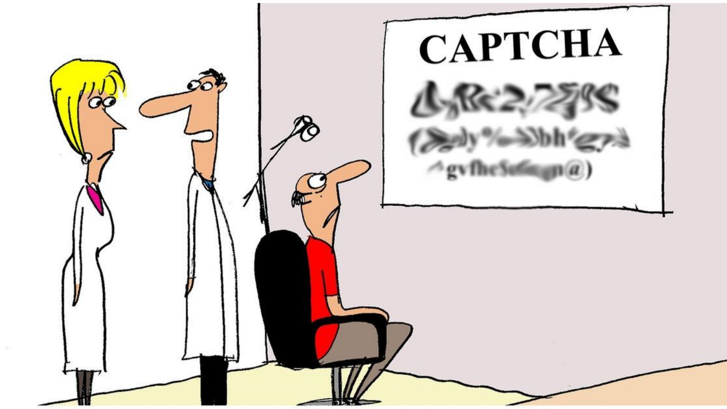


But still algorithms can achieve 90% accuracy…

So we end up with this…

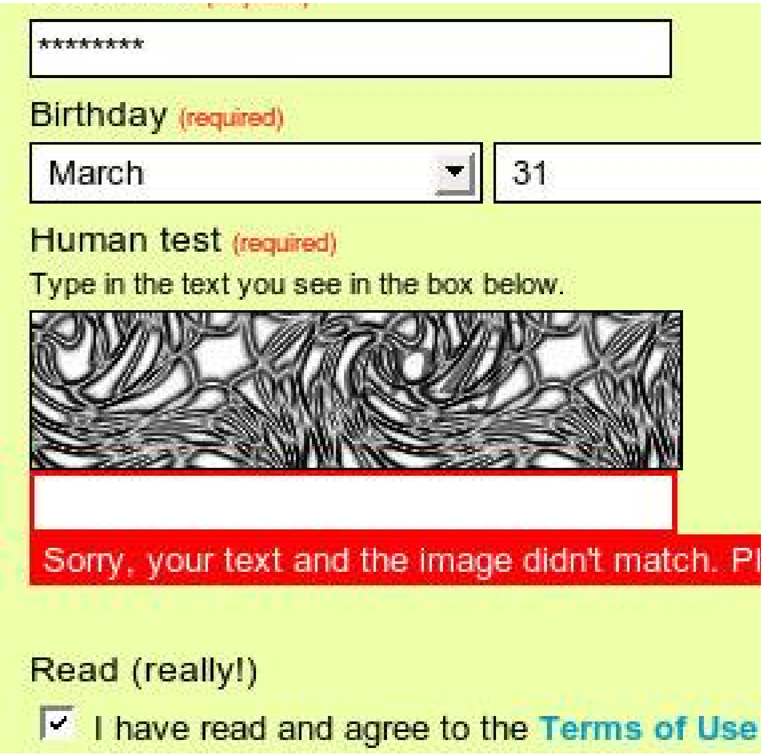


No premium user. Please enter the one that can NOT be created from the unfolded pattern. 29 seconds remain.



"Since I switched to the CAPTCHA eye chart business has been great."

But can humans read this??? Probably not…



****

Birthday (required)

March

31

Human test (required)

Type in the text you see in the box below.

Sorry, your text and the image didn't match. Pl

Read (really!)

☑ I have read and agree to the Terms of Use

4.

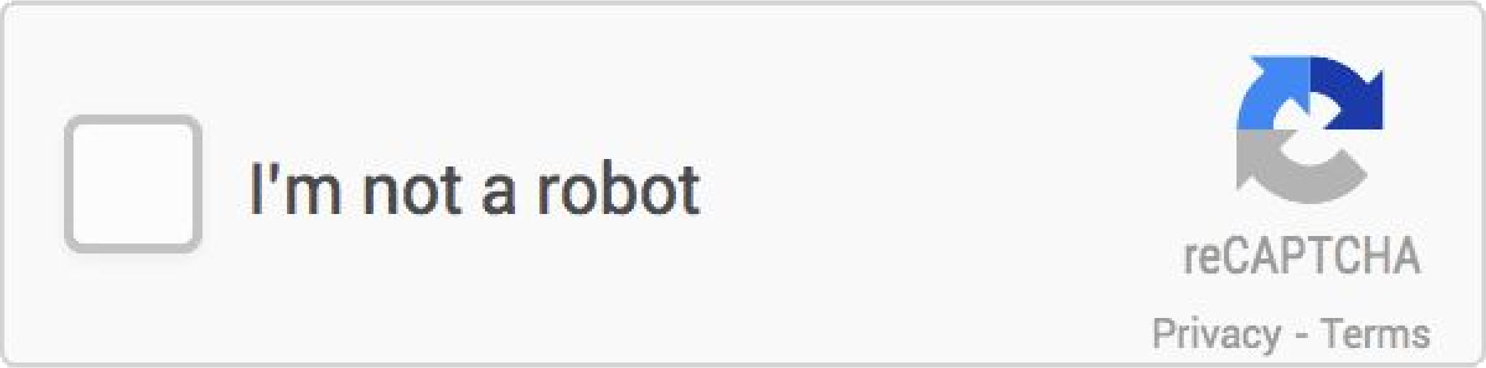
No CAPTCHA reCAPTCHA

No more CAPTCHAs

Machine Learning : the counter-attack

In 2014 Google launched the No CAPTCHA reCaptcha

- Implements ML/Data Mining algorithms to distinguish human/machine behavior before displaying a captcha

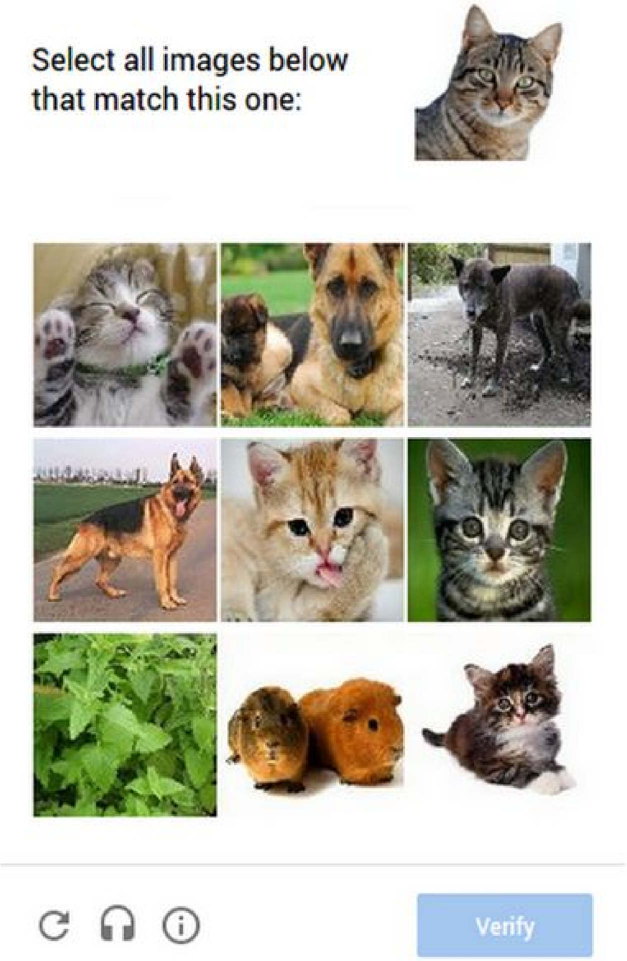


□ I'm not a robot

Machine Learning : the counter-attack

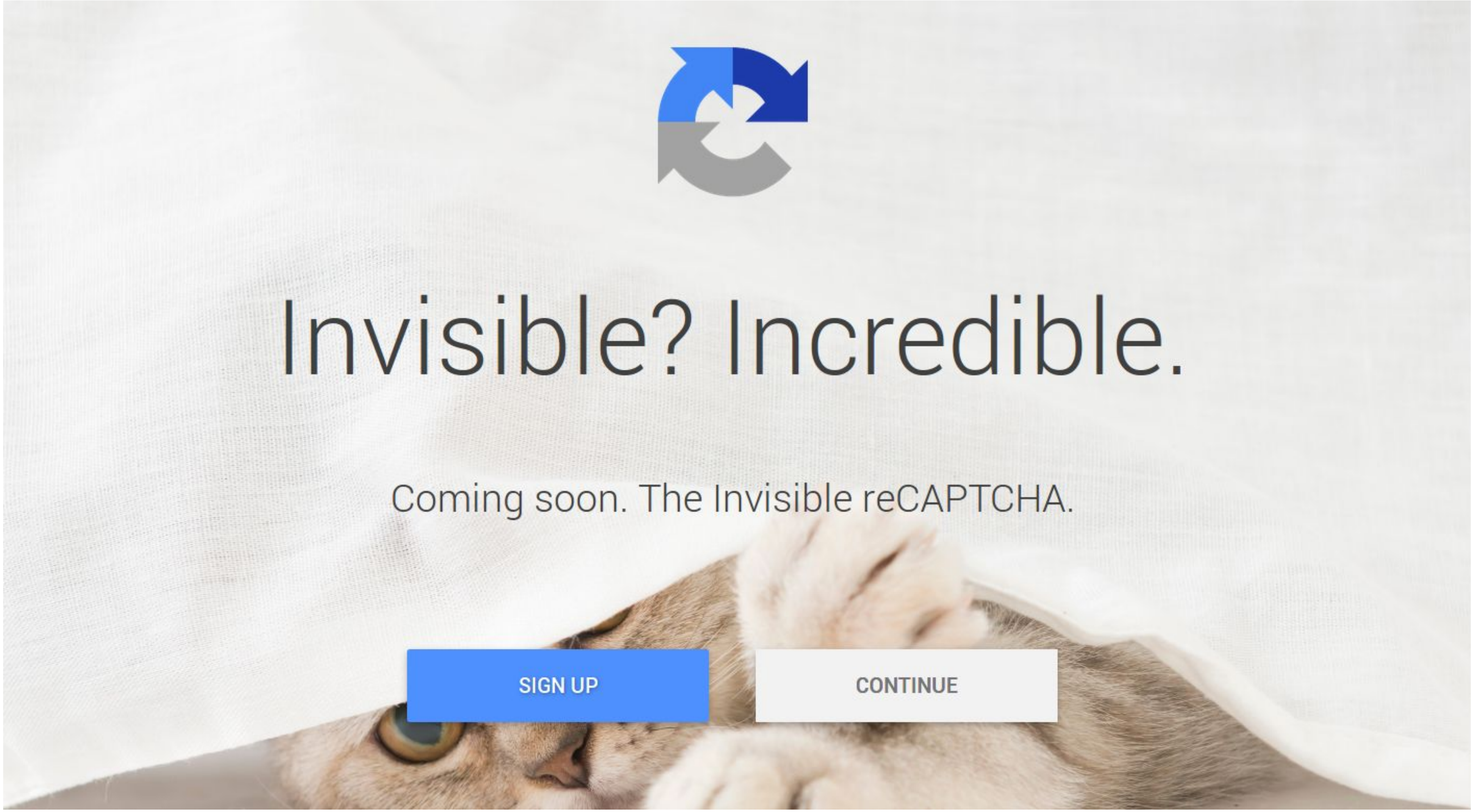
Try breaking this…

Even the best results are below 30%...



Select all images below that match this one:

The Future...



Invisible? Incredible.

Coming soon. The Invisible reCAPTCHA.