The art of breaking and designing captchas

Elie Bursztein
null
Twitter Follower Packages

Please Select One Of Our Targeted Follower Pages

Silver Package

- 1000 Targeted Followers
- Guaranteed REAL, Targeted People Interested In Your Business
- Added To Your Page Within 25 days
- Targeted To Your Business/Niche
- Select The Country/s Where You Want Your Followers From
- No Automatic Bots/Programs To Get Followers, We Proudly Target 100% Of Your Followers Manually

$49.99

Order Now »

Gold Package

- 5000 Targeted Followers
- Guaranteed REAL, Targeted People Interested In Your Business
- Added To Your Page Within 40 Days
- Targeted To Your Business/Niche
- Select The Country/s Where You Want Your Followers From
- No Automatic Bots/Programs To Get Followers, We Proudly Target 100% Of Your Followers Manually

$139.99
Castry Validation: *

\[
\lim_{x \to 0} \ln \left( 2 + \sqrt{\arctg x \cdot \sin \frac{1}{x}} \right)
\]

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

Download via Cogent #2

Elie Bursztein (@elie)
https://elie.net
World Most-Popular Captchas

[Megaupload]

[Reddit]

[eBay]

[Recaptcha]

[CNN]

[Baidu]

[Authorize]

[Recaptcha]

[NIH]

[Digg]

[Skyrock]

[Captcha.net]

[3nc9z]

[Google]

[Slashdot]

[Blizzard]

[trustother]

[Slashdot]

[pmynku]
World Most-Popular Captchas
Captcha Design Goal
Captcha Design Goal

Hard for computer

Hard for human

Human
Captcha Design Goal

Hard for computer

Hard for human

AI ?

Human
Captcha Design Goal

Hard for computer

sweet spot

Hard for human

AI?

Human

Elie Bursztein (@elie)
https://elie.net
Focus of this talk

How to **break** and **design** CAPTCHAs
Based on the breaking 21 of the most popular schemes and designing the new Wikipedia captcha
Outline
Outline

- How to break text captcha
Outline

- How to break text captcha
- How to make captchas easier for human
Outline

- How to break text captcha
- How to make captchas easier for human
- How to break audio captcha
Outline

- How to break text captcha
- How to make captchas easier for human
- How to break audio captcha
- How to break video captcha
Evaluation metrics

Accuracy
Evaluation metrics

Accuracy

Solving time
Evaluation metrics

- Accuracy
- Solving time
- Learnability
How to Break Text-Captchas
Think Lego
How to break a captcha: example
Pre-processing: background removal
Pre-processing: background removal
Pre-processing: captcha binarization
Pre-processing: captcha binarization
Pre-processing: Line detection
Pre-processing: Line detection
Pre-processing: Line removal
Pre-processing: Line removal
Segmentation: clustering algorithm
Segmentation: clustering algorithm
Segmentation: cluster separation
Segmentation: cluster separation
Post-segmentation: inverting rotation
Post-segmentation: inverting rotation
Recognition:
Breaker 5 Stages Pipeline

Slashdot captcha
Breaker 5 Stages Pipeline

Preprocessing
Breaker 5 Stages Pipeline

Preprocessing

fastest
Breaker 5 Stages Pipeline

1. Preprocessing
2. Segmentation

The word "fastest" is crossed out.
Breaker 5 Stages Pipeline

- Preprocessing
- Segmentation

Elie Bursztein (@elie)
https://elie.net
Breaker 5 Stages Pipeline

1. Preprocessing
2. Segmentation
3. Post-segmentation
Breaker 5 Stages Pipeline

- Preprocessing
- Segmentation
- Post-segmentation

Output:
- fastest
- fastest
- fastest
Breaker 5 Stages Pipeline

1. Preprocessing
2. Segmentation
3. Post-segmentation
4. Recognition

Example text: fastest
Breaker 5 Stages Pipeline

- Preprocessing
- Segmentation
- Post-segmentation
- Recognition

Result: fastest
Breaker 5 Stages Pipeline

- Preprocessing
- Segmentation
- Post-segmentation
- Recognition
- Post-recognition

The process starts with preprocessing, followed by segmentation. Post-segmentation is then applied, leading to recognition. Finally, post-recognition continues the process.
Breaker 5 Stages Pipeline

1. **Preprocessing**
2. **Segmentation**
3. **Post-segmentation**
4. **Recognition**
5. **Post-recognition**

The pipeline processes the input text, removing errors and improving the recognition of the final word "fastest."
From the image to the matrix representation
From the **image** to the **matrix representation**
From the **image** to the **matrix representation**
From the image to the matrix representation
From the **image** to the **matrix representation**
From the **matrix representation** to the **vector representation**
From the **matrix representation** to the **vector representation**
From the **matrix representation** to the **vector representation**
From the matrix representation to the vector representation
From the matrix representation to the vector representation
From the matrix representation to the vector representation
From the vector representation to the segment value (classification)
From the vector representation to the segment value (classification)
From the **vector representation** to the **segment value** (classification)
From the vector representation to the segment value (classification)
From the vector representation to the segment value (classification)
From the vector representation to the segment value (classification)
From the vector representation to the segment value (classification)
From the **vector representation** to the **segment value** (classification)
From the **vector representation** to the **segment value** (classification)
Breaker efficiency

Solver accuracy = Coverage * Precision^{length}

Coverage: Segmentation rate
Precision: Recognition rate
Anti-recognition techniques
Anti-recognition techniques

Blurring

3tr2bb
Anti-recognition techniques

- Blurring
- Distortion
Anti-recognition techniques

Blurring

Distortion

Rotation
Anti-recognition techniques

- Blurring

- Distortion

- Rotation

- Fonts
Anti-recognition techniques

Blurring

Distortion

Rotation

Fonts

Charsets
Anti-recognition techniques

- Blurring
- Distortion
- Rotation
- Fonts
- Charsets

Elie Bursztein (@elie)
http://elie.im
SVM learning rate

% success vs Trainning set size

- 09
- AZ09
- azAZ09
- Distortion
- 3 fonts
- 5 fonts
- Angles

Elie Bursztein (@elie)
https://elie.net
KNN learning rate

% success vs training set size for different font sets and distortion levels.

- 09
- AZ09
- azAZ09
- Distortion
- 3 fonts
- 5 fonts
- Angles

Elie Bursztein (@elie)
https://elie.net
Anti-recognition taxonomy
Anti-recognition taxonomy

Background Confusion
Anti-recognition taxonomy

Background Confusion

3nc9z
Anti-recognition taxonomy

Background Confusion

3nc9z

quxg4th
Anti-recognition taxonomy

Background Confusion

3nc9z
quxg4h
p y m k u
Anti-recognition taxonomy

Background Confusion

3nc9z

Lines

pmymku
Anti-recognition taxonomy

Background Confusion

Lines
Anti-recognition taxonomy

Background Confusion

Lines

Elie Bursztein (@elie)
http://elie.im
Anti-recognition taxonomy

Background Confusion

Lines

Elie Bursztein (@elie)
http://elie.im
Anti-recognition taxonomy

Background Confusion

Lines

Collapsing

Elie Bursztein (@elie)
http://elie.im
Anti-recognition taxonomy

Background Confusion

Lines

Collapsing
Anti-recognition taxonomy

Background Confusion

3nc9z
quxg4th
pmynku

Lines

2pbc0
aprigot
dramacharm

Collapsing

984505
RAE3
Anti-recognition taxonomy

Background Confusion

Lines

Collapsing
Breaking World of Warcraft
Breaking World of Warcraft
Breaking World of Warcraft
Breaking World of Warcraft
Breaking World of Warcraft
Breaking Captcha.net
Breaking Captcha.net
Breaking Captcha.net

Elie Bursztein (@elie)
http://elie.im
Breaking Captcha.net
Breaking Captcha.net

Elie Bursztein (@elie)
http://elie.im
Breaking Wikipedia

dramacharm
Breaking Wikipedia

dramacharm
dramacharm
Breaking Wikipedia

dramacharm

dramacharm

dramacharm
Breaking Wikipedia
Breaking Digg
Breaking Digg

Elie Bursztein (@elie)
http://elie.im
Breaking Digg
Breaking Digg
Breaking Slashdot
Breaking Slashdot

dissent

dissent

Elie Bursztein (@elie)
http://elie.im
Breaking Slashdot

Elie Bursztein (@elie)
http://elie.im
Breaking Slashdot

dissents
dissents
dissents
dissents
Breaking Slashdot

dissents

dissents

dissents

dissents
Breaking eBay
Breaking eBay
Breaking eBay
Failing to break eBay
Failing to break eBay

Elie Bursztein (@elie)
http://elie.im
Failing to break eBay
Failing to break eBay

Elie Bursztein (@elie)
http://elie.im
Failing to break eBay
Breaking Baidu
Breaking Baidu
Breaking Baidu

Elie Bursztein (@elie)
http://elie.im
Breaking Baidu
Breaking Baidu
## Overall results

<table>
<thead>
<tr>
<th>Website</th>
<th>Segmentation</th>
<th>Solving rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authorize</td>
<td>84%</td>
<td>66%</td>
</tr>
<tr>
<td>Baidu</td>
<td>98%</td>
<td>5%</td>
</tr>
<tr>
<td>Blizzard</td>
<td>75%</td>
<td>70%</td>
</tr>
<tr>
<td>Captcha.net</td>
<td>96%</td>
<td>73%</td>
</tr>
<tr>
<td>CNN</td>
<td>50%</td>
<td>16%</td>
</tr>
<tr>
<td>Digg</td>
<td>86%</td>
<td>20%</td>
</tr>
<tr>
<td>eBay</td>
<td>95%</td>
<td>43%</td>
</tr>
<tr>
<td>Google</td>
<td>0%</td>
<td>0%</td>
</tr>
<tr>
<td>MegaUpload</td>
<td>n/a</td>
<td>93%</td>
</tr>
<tr>
<td>NIH</td>
<td>87%</td>
<td>72%</td>
</tr>
<tr>
<td>Recaptcha</td>
<td>0%</td>
<td>0%</td>
</tr>
<tr>
<td>Reddit</td>
<td>71%</td>
<td>42%</td>
</tr>
<tr>
<td>Skyrock</td>
<td>30%</td>
<td>2%</td>
</tr>
<tr>
<td>Slashdot</td>
<td>52%</td>
<td>35%</td>
</tr>
<tr>
<td>Wikipedia</td>
<td>57%</td>
<td>25%</td>
</tr>
</tbody>
</table>
Learning rate for real schemes

% Success

Trainning set size

Authorize
Baidu
Blizzard
Captcha.net
CNN
Digg
eBay
Megaupload
NIH
Reddit
Skyrock
Slashdot
Wikipedia
Decaptcha main interface
Apply design principles

- Core design principles
  - Randomize length
  - Randomize character size
  - Wave the captcha
- Use anti-recognition as a means of strengthening captcha security
- Don’t use a complex charset
  - Bad for human (see our research on this)
  - Useless for security
- Use collapsing or lines
Designing Better Captchas
Think Lego again

- Decompose in features
- Analyze
  - feature in isolation
  - features interaction
Evaluation system
### Experiment details

The table below summarizes the experiment details:

<table>
<thead>
<tr>
<th>Round</th>
<th>Task</th>
<th>N possible</th>
<th>N sampled</th>
<th>N tests per sample</th>
<th>Total tests</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Baseline (&quot;Control&quot;)</td>
<td>1</td>
<td>1</td>
<td>1000</td>
<td>1000</td>
</tr>
<tr>
<td>2</td>
<td>Real world captchas</td>
<td>8</td>
<td>8</td>
<td>1000</td>
<td>8000</td>
</tr>
<tr>
<td>3</td>
<td>Features in isolation</td>
<td>496</td>
<td>496</td>
<td>200</td>
<td>99200</td>
</tr>
<tr>
<td>4</td>
<td>2 feature interactions</td>
<td>60950</td>
<td>60950</td>
<td>5</td>
<td>304750</td>
</tr>
<tr>
<td>5</td>
<td>3 feature interactions</td>
<td>1 303 224</td>
<td>25000</td>
<td>10</td>
<td>250000</td>
</tr>
<tr>
<td>6</td>
<td>4 feature interactions</td>
<td>113 951 684</td>
<td>25000</td>
<td>10</td>
<td>250000</td>
</tr>
<tr>
<td></td>
<td>Total</td>
<td></td>
<td></td>
<td></td>
<td>912150</td>
</tr>
</tbody>
</table>
Some of the features tested

- Blurring
- Text color
- Font
- Background color
- Collapsing
- Tilting
- Waving
- Distortion
- Line angle
- Line shape
- Line size
- Line coverage
- Line position
- Noise
Angle of rotation

![Graph showing the relationship between rotation angle and solving time and accuracy. The x-axis represents the rotation angle in degrees, ranging from 0 to 360. The y-axis represents solving time (s) and accuracy, ranging from 0 to 1. The graph includes two lines: one for solving time and another for accuracy. There are labels for the axes and a legend indicating the colors used for the lines.]
Collapsing

![Graph showing the relationship between character gap width and solving time and accuracy.]
Character size

![Graph showing the relationship between character size, solving time, and accuracy.](image)
Resolution invariant

Accuracy

captcha length (number of characters)

- <= 1024
- > 1024
- all captchas
2D interactions
Length vs Angle interaction
Perception Does Not Match Number
The New Wikipedia

- Use digit
- Wave the captcha
- Use random length (5-7)
- Use random size (34-50)
- Rotate letter (-25/ 25)
- Add a line for a super secure version
End result

trustother

Accuracy

Solving time
End result

Accuracy 84.8%

Solving time
End result

Accuracy 84.8%

Solving time 7.8s
End result

Accuracy  84.8%

Solving time  7.8s
### End result

<table>
<thead>
<tr>
<th></th>
<th>Accuracy 1</th>
<th>Solving time 1</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Accuracy</strong></td>
<td>84.8%</td>
<td></td>
</tr>
<tr>
<td><strong>Solving time</strong></td>
<td>7.8s</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Accuracy 2</th>
<th>Solving time 2</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Accuracy</strong></td>
<td>89.2%</td>
<td></td>
</tr>
<tr>
<td><strong>Solving time</strong></td>
<td>82.6%</td>
<td></td>
</tr>
</tbody>
</table>

Elie Bursztein (@elie)
https://elie.net
## End result

<table>
<thead>
<tr>
<th></th>
<th>Solving time</th>
<th>Accuracy</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>7.8s</td>
<td>84.8%</td>
</tr>
<tr>
<td></td>
<td>4.9s</td>
<td>89.2%</td>
</tr>
<tr>
<td></td>
<td>5.3s</td>
<td>82.6%</td>
</tr>
</tbody>
</table>
End result

Accuracy
84.8% 89.2%

Solving time
7.8s 4.9s
5.3s

Elie Bursztein (@elie)
https://elie.net
End result

Accuracy: 84.8%  89.2%
Solving time: 7.8s  4.9s

confusing
## End result

<table>
<thead>
<tr>
<th></th>
<th>00x08</th>
<th>00x20</th>
<th>01x20</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accuracy</td>
<td>89.2%</td>
<td>82.6%</td>
<td>97%</td>
</tr>
<tr>
<td>Solving time</td>
<td>4.9s</td>
<td>5.3s</td>
<td></td>
</tr>
</tbody>
</table>

*Elie Bursztein (@elie)*

[https://elie.net](https://elie.net)
End result

Accuracy: 84.8% 89.2% 97%
Solving time: 7.8s 4.9s 4.9s
How to Break Audio-Captcha
Audio Captchas

The not-so-fine print

For added security, please enter the verification code hidden in the image.

Elie Bursztein (@elie)
https://elie.net
Audio Captchas

The not-so-fine print
For added security, please enter the verification code hidden in the image.

Elie Bursztein (@elie)
https://elie.net
Creating Audio Captcha

Captcha Maker

Elie Bursztein (@elie)
https://elie.net
Creating Audio Captcha
Creating Audio Captcha
Creating Audio Captcha

Super secure captcha
Noise intensity (RMS/SNR)

![Waveform and spectrogram](image)

**Authori**

**Dia**

**Micros**

Elie Bursztein (@elie)
https://elie.net
Sound representation

WAV → DFT → Cep → TFR → TDC

TCR
Solving an audio captcha
Solving an audio captcha
Solving an audio captcha
Solving an audio captcha
Solving an audio captcha
Solving an audio captcha
Solving an audio captcha
Dealing with random noise

- Statistical learning
- Supervised learning
- RLS (Regularized least square) classifier

5:
- Authorize
- eBay
- Recapcha

J:
- Authorize
- Digg
## Results

<table>
<thead>
<tr>
<th></th>
<th>Length</th>
<th>Coverage</th>
<th>Digit</th>
<th>Captcha</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authorize</td>
<td>5</td>
<td>100</td>
<td>97</td>
<td>89.2%</td>
</tr>
<tr>
<td>Digg</td>
<td>5</td>
<td>100</td>
<td>76</td>
<td>41.4%</td>
</tr>
<tr>
<td>eBay</td>
<td>6</td>
<td>85.6</td>
<td>92.5</td>
<td>82.9%</td>
</tr>
<tr>
<td>Microsoft</td>
<td>10</td>
<td>80.6</td>
<td>89.6</td>
<td>48.9%</td>
</tr>
<tr>
<td>Recaptha</td>
<td>8</td>
<td>99.9</td>
<td>40.5</td>
<td>1.5%</td>
</tr>
<tr>
<td>Yahoo</td>
<td>7</td>
<td>99.1</td>
<td>74.7</td>
<td>45.4%</td>
</tr>
</tbody>
</table>
Recaptcha semantic noise

![Recaptcha semantic noise graph]

Elie Bursztein (@elie)
https://elie.net
Recaptcha semantic noise

Elie Bursztein (@elie)
https://elie.net
How many captchas do you need?

![Graph showing the relationship between corpus size and captcha precision for various websites.]

- Authorize
- Digg
- Ebay
- MSLive
- Recaptcha
- Yahoo

Corpus Size (in Digits)

Per-Captcha Precision (%)
Video captcha

- Interesting direction -> more design space
- Good for human
- Good for computer :(  
  - Working on it

See blog post for more information: http://elie.im/blog
Apply

- **Within 3 months**
  - Make sure you have a strong captcha scheme (use mine if you want)
  - Ensure that your site is accessible

- **Within 6 months**
  - Log your captchas failure rate and monitor them
  - Have a backup captcha scheme in case your scheme is broken
Thank you

Questions?

Follow-me!

Twitter: @elie

Captcha research: http://elie.im/tag/captcha