

Text-based captchas strengths and weakness

Elie Bursztein, Matthieu Martin, John Mitchell
Stanford University

About this Research

- Presenter: [Elie Bursztein \(http://elie.im\)](http://elie.im)
- Conference: ACM CCS 2011
- Slides and paper freely available from <http://ly.tl/p22>
- Follow me for more security research
 - [Twitter @elie](#)
 - [Google+](#)
 - [Facebook](#)



Elie Bursztein

@elie Stanford

Researcher @Stanford University. Tweeting about information privacy and security, mobile, games and web technologies

<http://elie.im>

[Edit your profile](#) →

Tweets

[Favorites](#)

[Following](#)

[Followers](#)

[Lists](#) ▾



elie Elie Bursztein

Security researcher analyses shady shipping centers

bit.ly/oHEUOW #security #scam

2 hours ago



elie Elie Bursztein

Users are responsible for half of all infections according to Microsoft - bit.ly/pQMpwm #security #malware yfrog.com/j23wzp

13 Oct



elie Elie Bursztein

New exploit kit in the wild , Thousands of Owned Sites Redirecting Users to Attack Site - bit.ly/o4BgKC #security #malware

13 Oct



elie Elie Bursztein

Researchers hack crypto on RFID smart cards used for keyless entry and transit pass bit.ly/n28ahr #security

13 Oct



elie Elie Bursztein

Sony Playstation Network is under attack (again !) - bit.ly/pEeJQB #security #sony

12 Oct



elie Elie Bursztein

8 of 10 MySpace Users "Just Don't Feel Safe" according to a new study - bit.ly/n0uqVg #security #myspace

12 Oct



About @elie

1,067

Tweets

26

Following

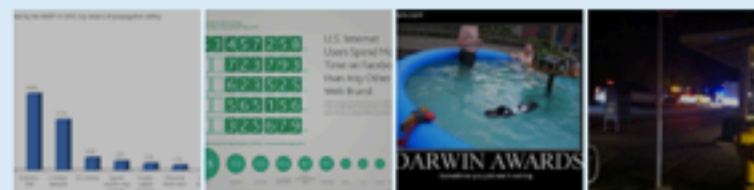
520

Followers

29

Listed

Recent Images · [view all](#)



Similar to you · [view all](#)



0x6D61726966F .mario 🔒



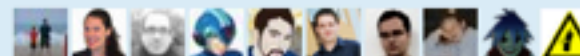
mozwebsec Mozilla WebSec



adambarth Adam Barth

I am not a penguin

Following · [view all](#)



[About](#) [Help](#) [Blog](#) [Mobile](#) [Status](#) [Jobs](#) [Terms](#) [Privacy](#)
[Shortcuts](#) [Advertisers](#) [Businesses](#) [Media](#) [Developers](#)
[Resources](#) © 2011 Twitter



Elie Bursztein

@elie Stanford

Researcher @Stanford University. Tweeting about information privacy and security, mobile, games and web technologies

<http://elie.im>

[Edit your profile](#) →

Tweets

[Favorites](#)

[Following](#)

[Followers](#)

[Lists](#) ▾



elie Elie Bursztein

Security researcher analyses shady shipping centers

bit.ly/oHEUOW #security #scam

2 hours ago



elie Elie Bursztein

Users are responsible for half of all infections according to Microsoft - bit.ly/pQMpwm #security #malware yfrog.com/j23wzp

13 Oct



elie Elie Bursztein

New exploit kit in the wild , Thousands of Owned Sites Redirecting Users to Attack Site - bit.ly/o4BgKC #security #malware

13 Oct



elie Elie Bursztein

Researchers hack crypto on RFID smart cards used for keyless entry and transit pass bit.ly/n28ahr #security

13 Oct



elie Elie Bursztein

Sony Playstation Network is under attack (again !) - bit.ly/pEeJQB #security #sony

12 Oct



elie Elie Bursztein

8 of 10 MySpace Users "Just Don't Feel Safe" according to a new study - bit.ly/n0uqVg #security #myspace

12 Oct



About @elie

1,067

Tweets

26

Following

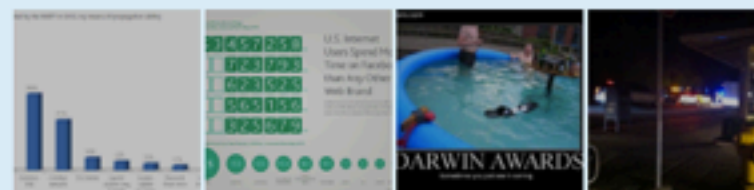
520

Followers

29

Listed

Recent Images · [view all](#)



Similar to you · [view all](#)



0x6D61726966F .mario 🔒



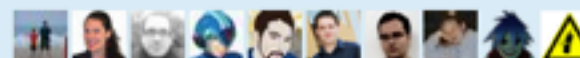
mozwebsec Mozilla WebSec



adambarth Adam Barth

I am not a penguin

Following · [view all](#)



[About](#) [Help](#) [Blog](#) [Mobile](#) [Status](#) [Jobs](#) [Terms](#) [Privacy](#)
[Shortcuts](#) [Advertisers](#) [Businesses](#) [Media](#) [Developers](#)
[Resources](#) © 2011 Twitter



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

Join the Conversation

Already on Twitter? [Sign in.](#)

 Already use Twitter on your phone? [Finish signup now.](#)

Full name

workshop

✓ ok

Your full name will appear on your public profile

Username

eliedemo

✓ ok

Your public profile: [http://twitter.com/ eliedemo](http://twitter.com/eliedemo)

Password

••••••••••

✓ Good

Are you human?

×


Before we create your account, we need to make sure you're not a computer.

edisibil from

Type the words
above

Can't read this?

 [Get two new words](#)

 [Hear a set of words](#)

Powered by reCAPTCHA.

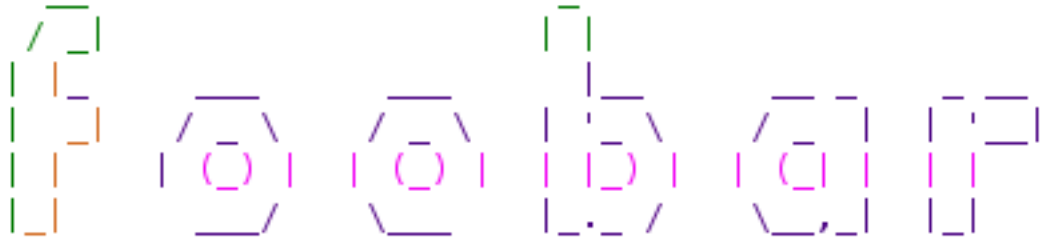
[Help](#)

Finish

Create my account

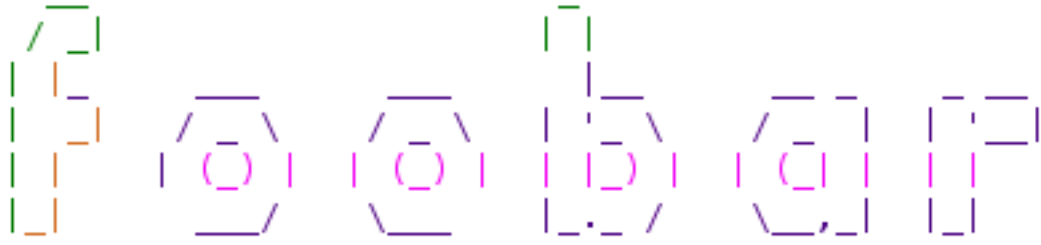
☒ I want the inside scoop—please send me email updates!

Funny Captchas



Captcha Validation: *

Funny Captchas



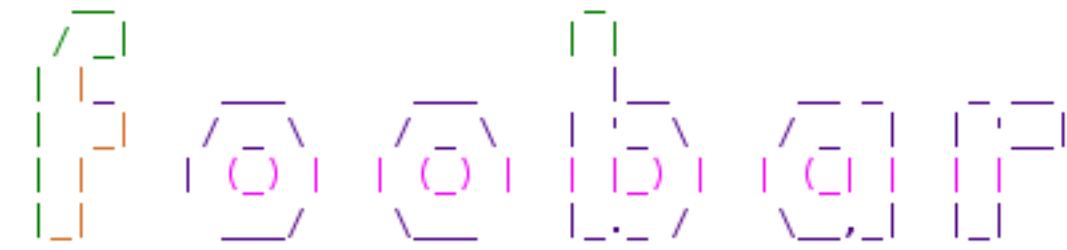
Captcha Validation: *

Защита от автоматической регистрации

$\lim_{x \rightarrow 0} \ln \left(2 + \sqrt{\operatorname{arctg} x \cdot \sin \frac{1}{x}} \right)$

Введите ответ

Funny Captchas



Captcha Validation: *

Защита от автоматической регистрации

$$\lim_{x \rightarrow 0} \ln \left(2 + \sqrt{\arctg x \cdot \sin \frac{1}{x}} \right)$$

Введите ответ

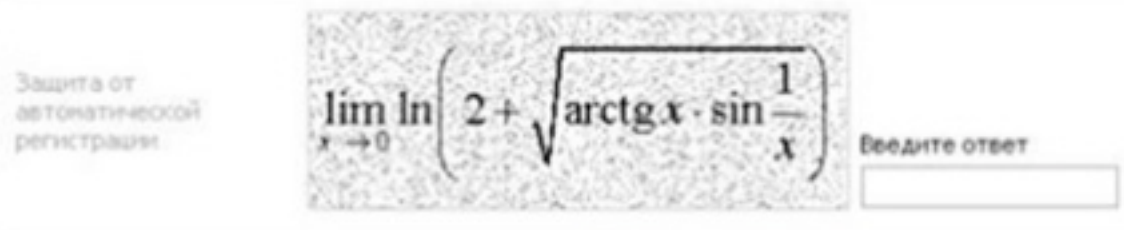
No premium user. Please enter the one that can NOT be created from the unfolded pattern. 29 seconds remain.

Download via Cogent #2

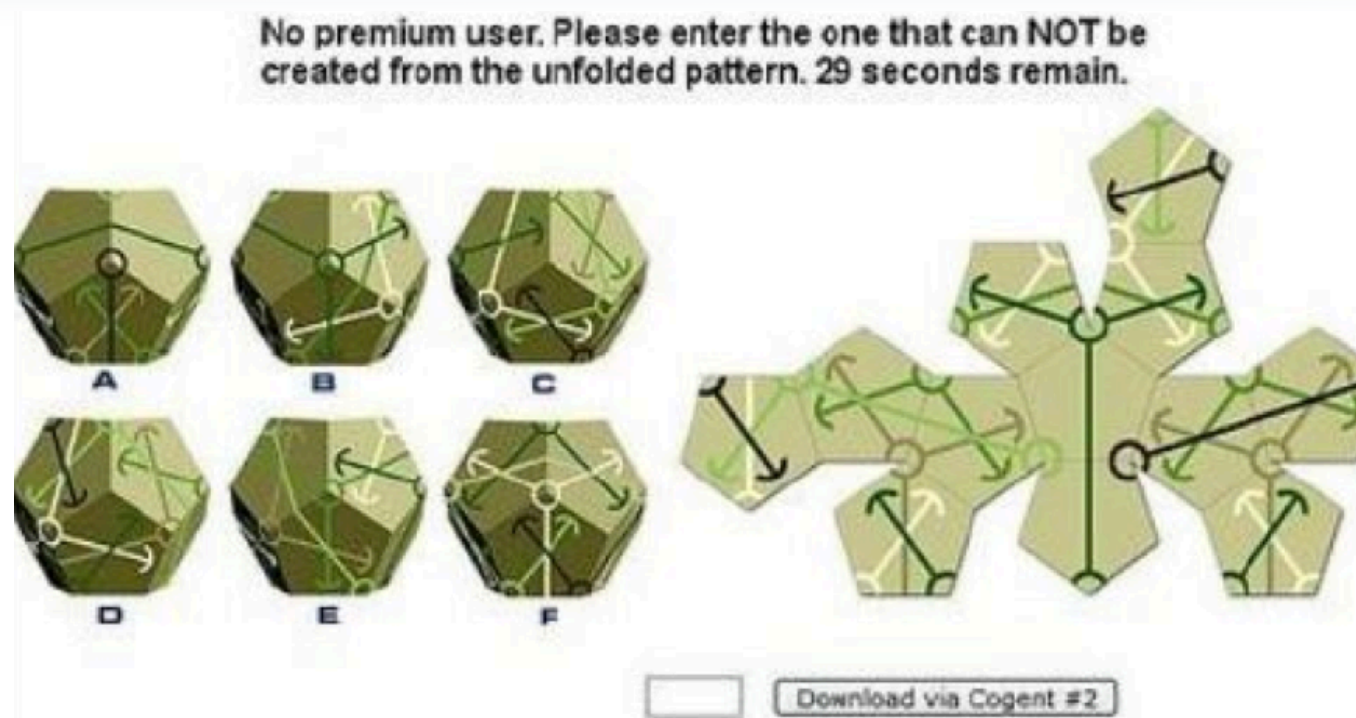
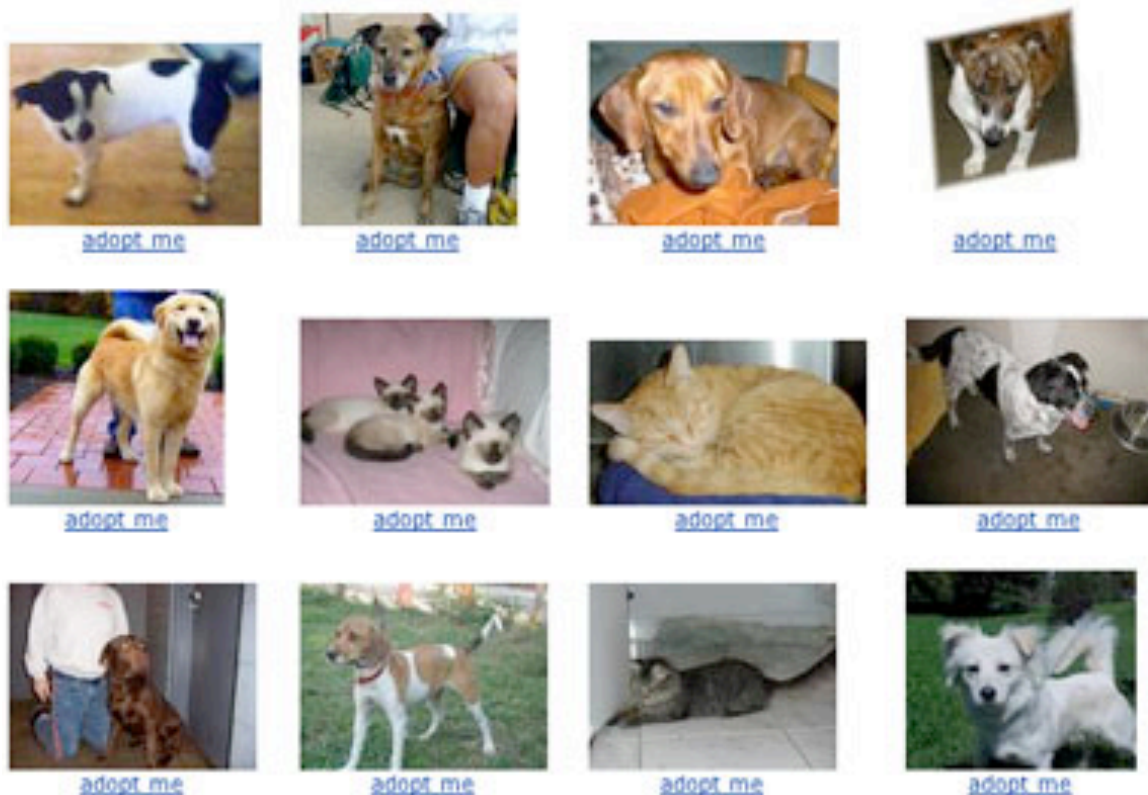
Funny Captchas



Captcha Validation: *



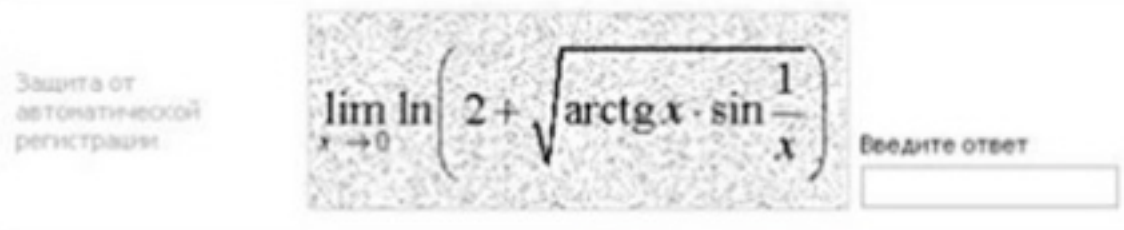
Please click on the images that show cats:



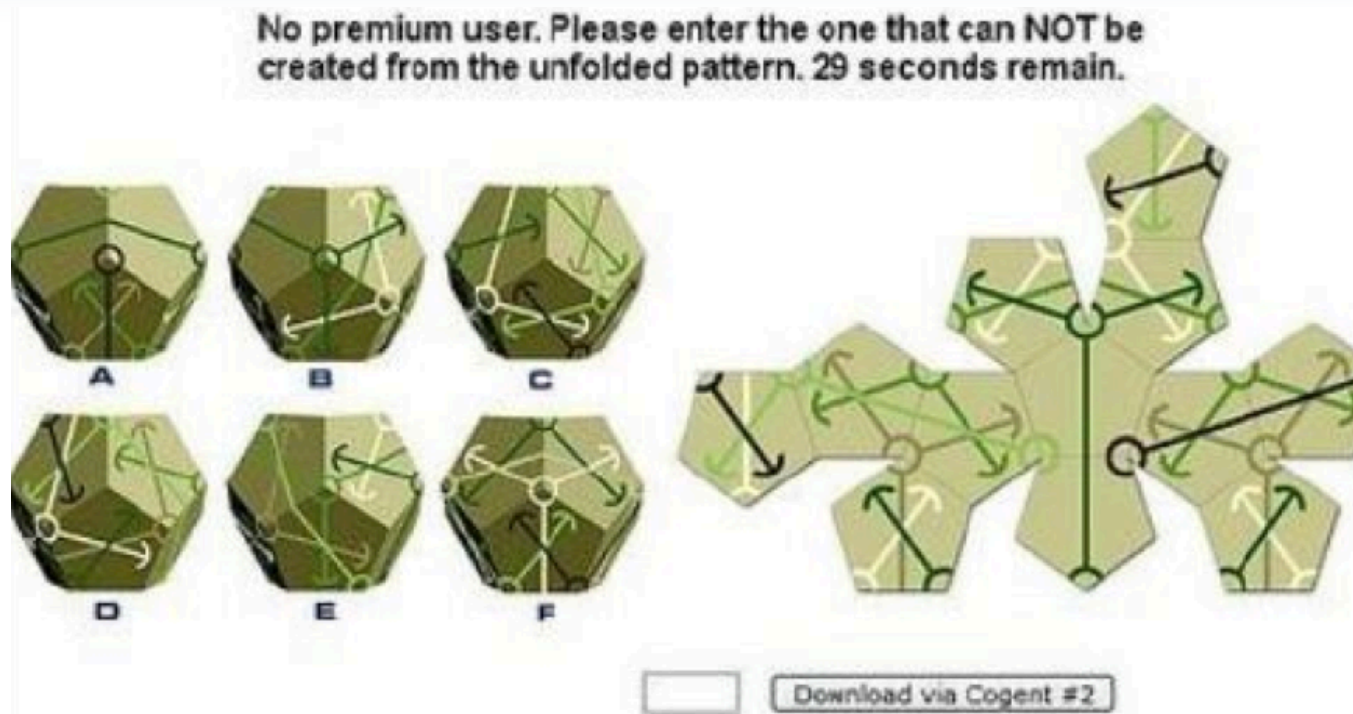
Funny Captchas



Captcha Validation: *



Please click on the images that show cats:



The world most-popular captchas

ZKW4

[Megaupload]



[Reddit]

944531

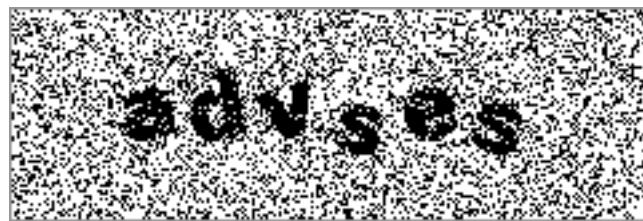
[eBay]



[CNN]

RAE3

[Baidu]



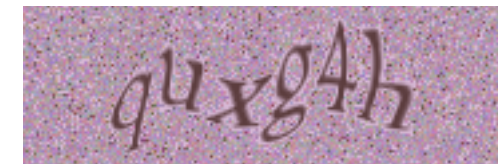
[Captcha.net]



[Authorize]

3-2 parks

[Recaptcha]



[Skyrock]



[NIH]



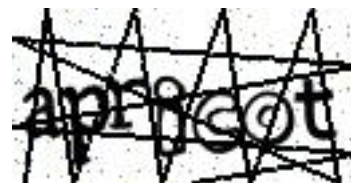
[Digg]



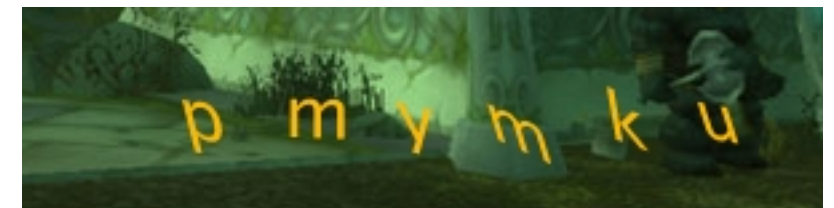
[Google]

trustother

[Wikipedia]



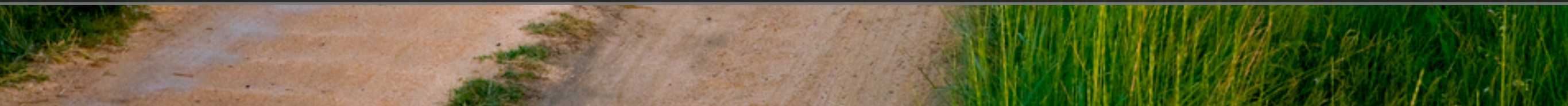
[Slashdot]



[Blizzard]



How to **break text captcha** and
design secure ones





Based on the **break of 13** of the most
popular schemes

Outline

Outline

- **How to break text-captchas ?**

Outline

- How to break text-captchas ?
- Evaluating anti-recognition techniques security

Outline

- How to break text-captchas ?
- Evaluating anti-recognition techniques security
- Attacking anti-segmentation techniques

Outline

- How to break text-captchas ?
- Evaluating anti-recognition techniques security
- Attacking anti-segmentation techniques
- Real-world captcha security summary

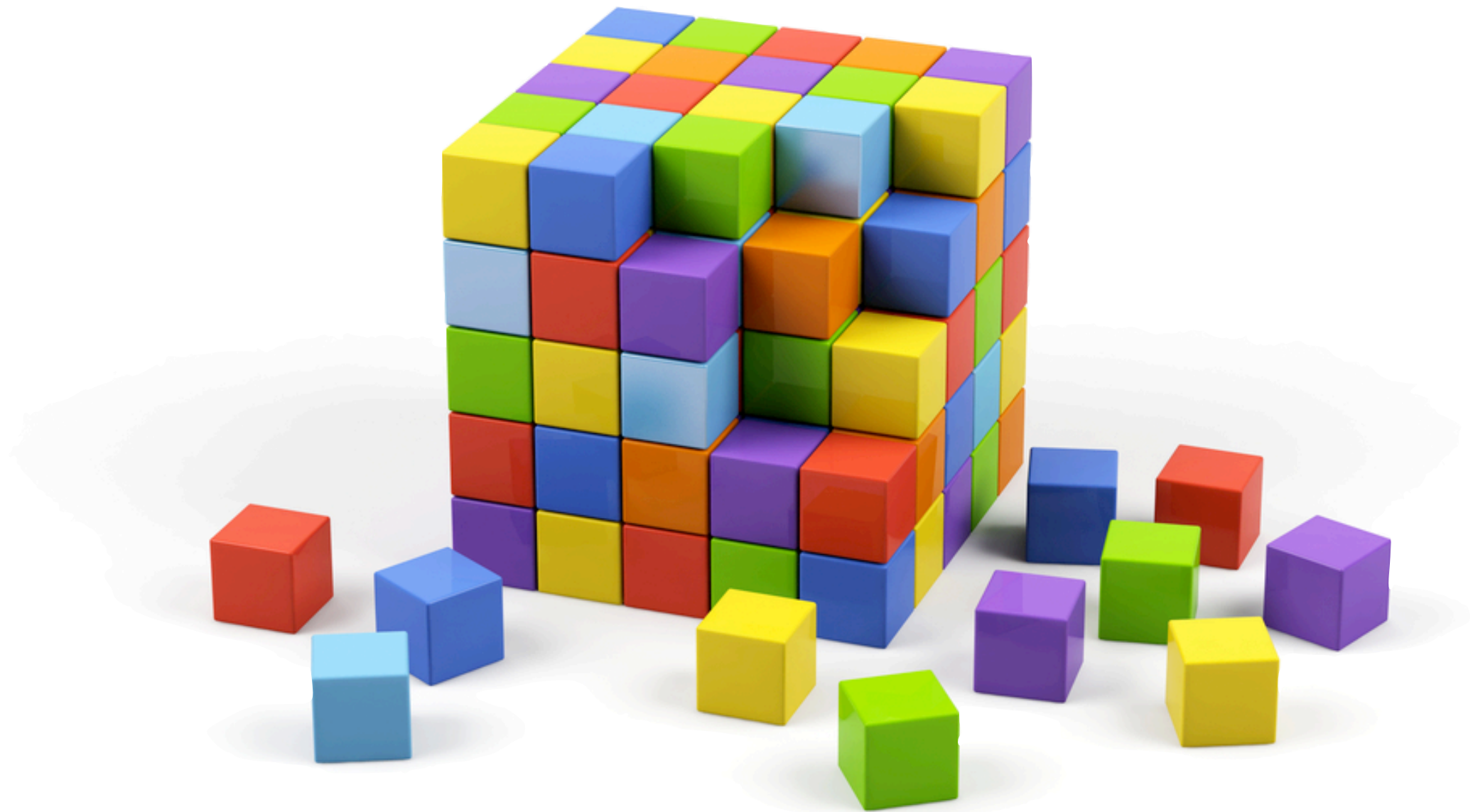
Outline

- How to break text-captchas ?
- Evaluating anti-recognition techniques security
- Attacking anti-segmentation techniques
- Real-world captcha security summary
- Decaptcha (our breaker) demo

Outline

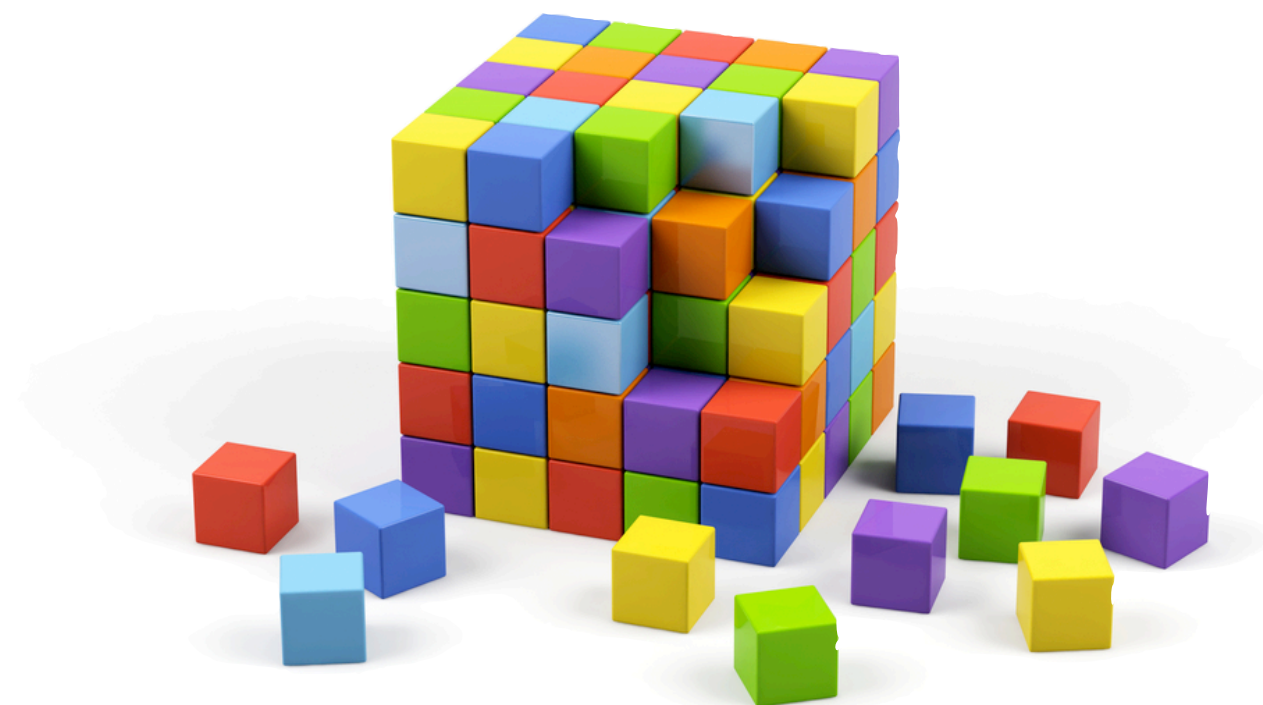
- How to break text-captchas ?
- Evaluating anti-recognition techniques security
- Attacking anti-segmentation techniques
- Real-world captcha security summary
- Decaptcha (our breaker) demo
- Lessons learned

Breaking captcha



Divide and Conquer approach

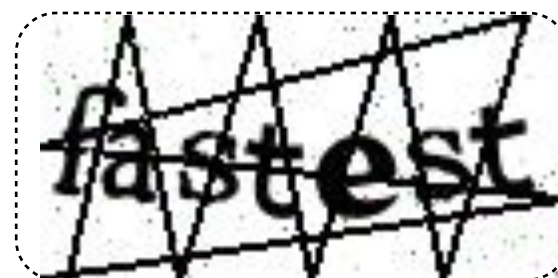
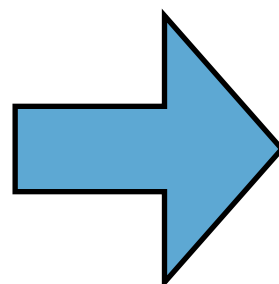
How to break captchas ?



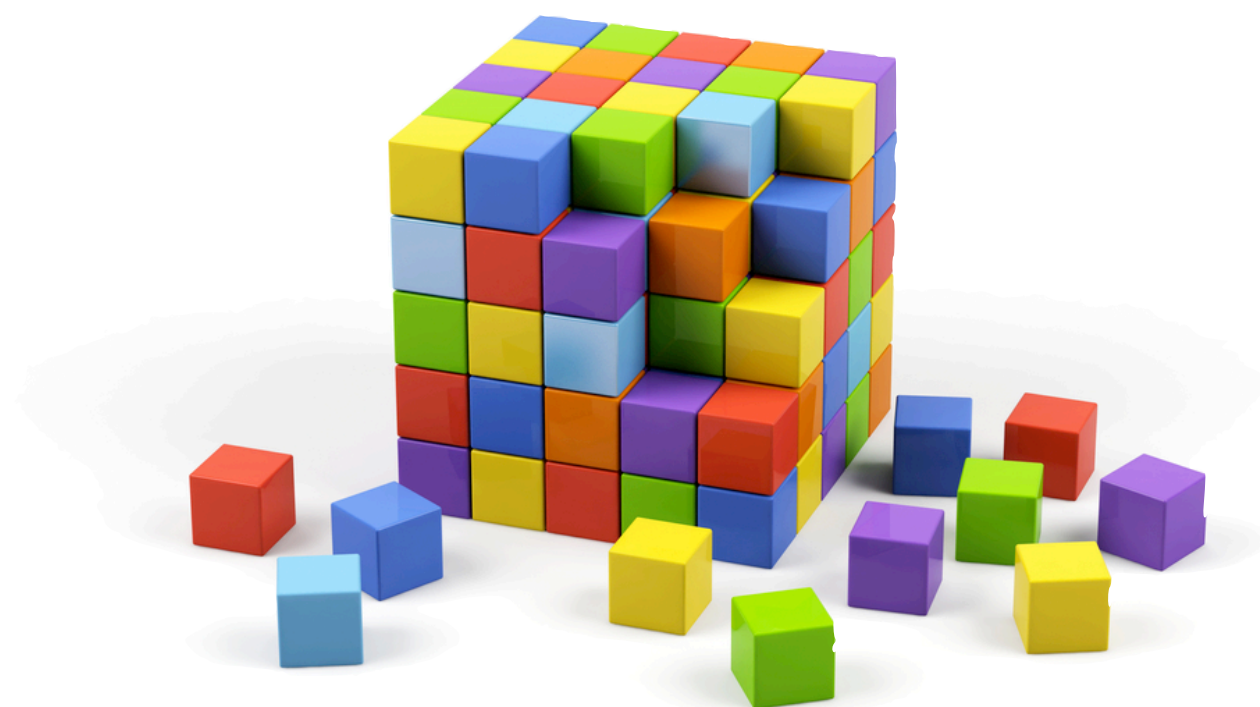
Slashdot captcha

How to break captchas ?

Preprocessing

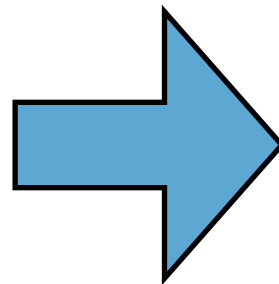


Slashdot captcha

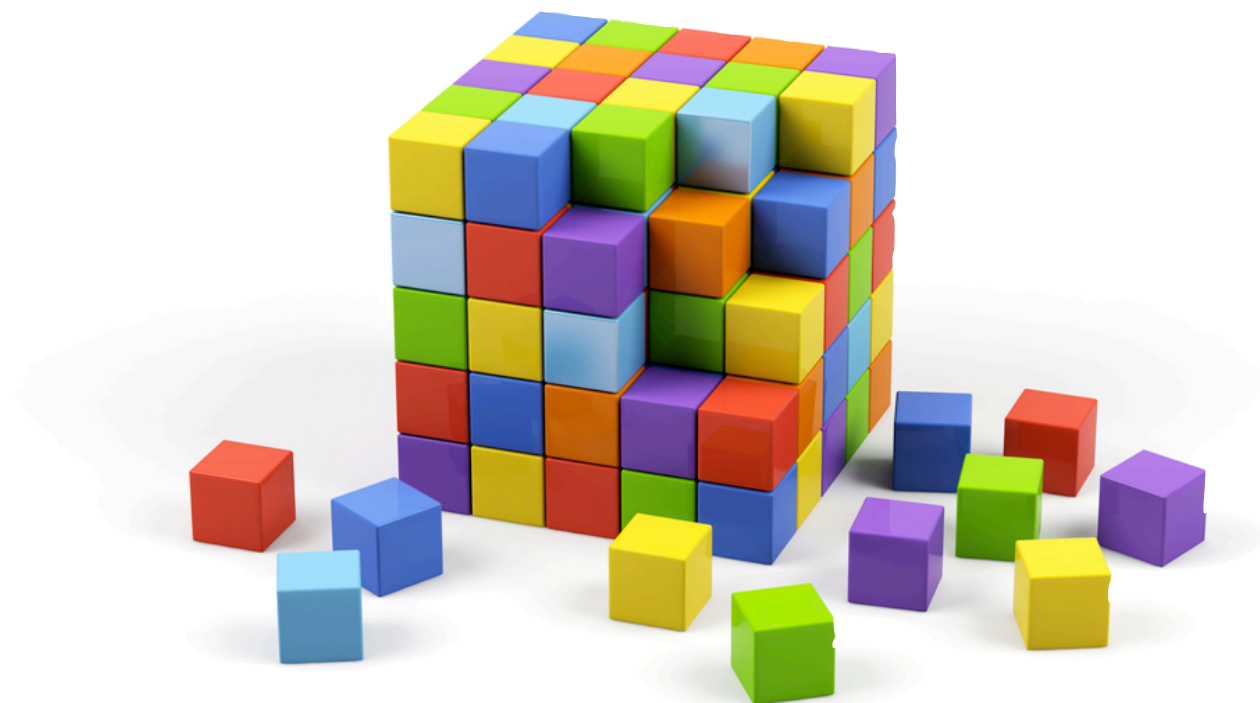


How to break captchas ?

Preprocessing

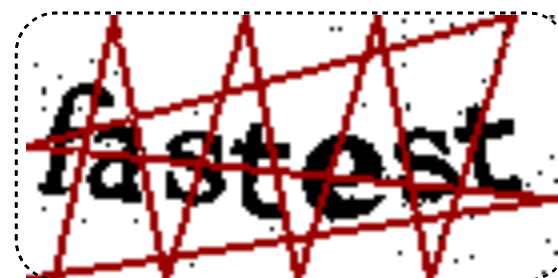
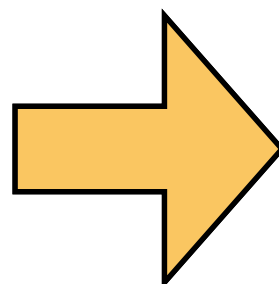


Slashdot captcha

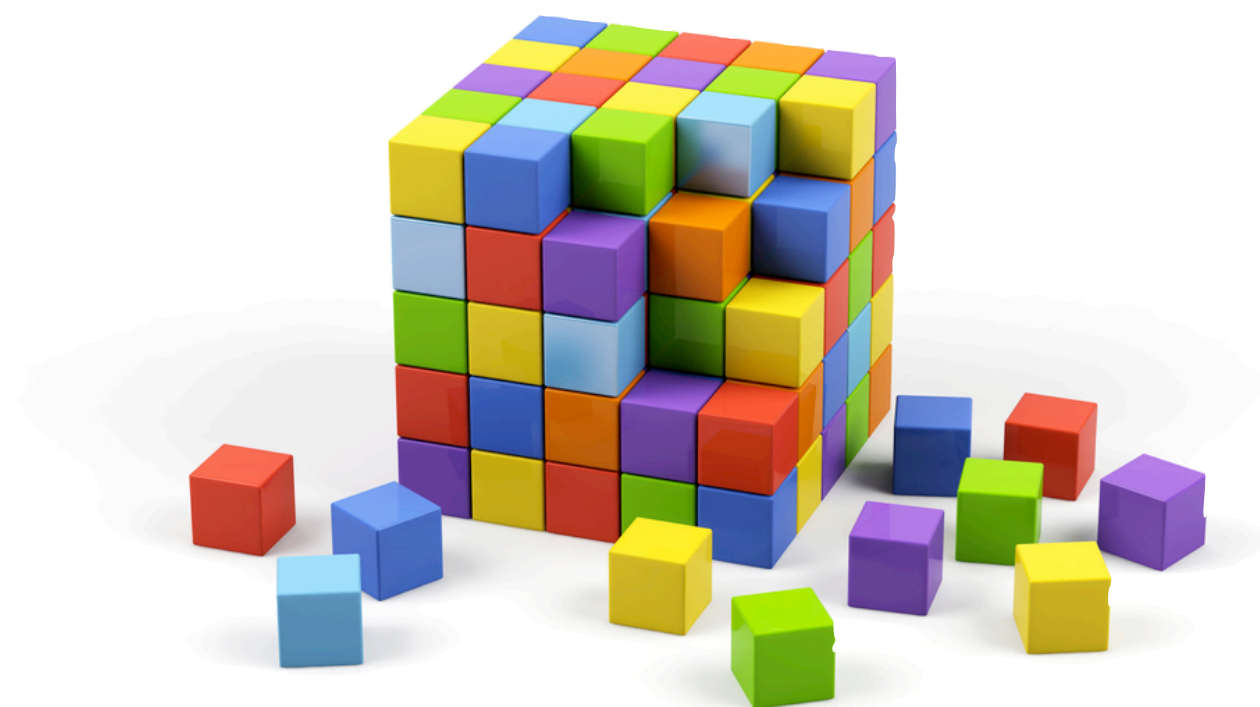


How to break captchas ?

Segmentation

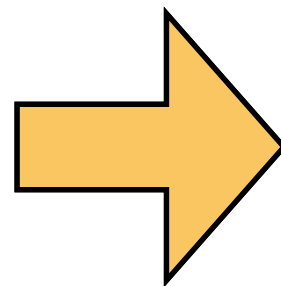


Slashdot captcha

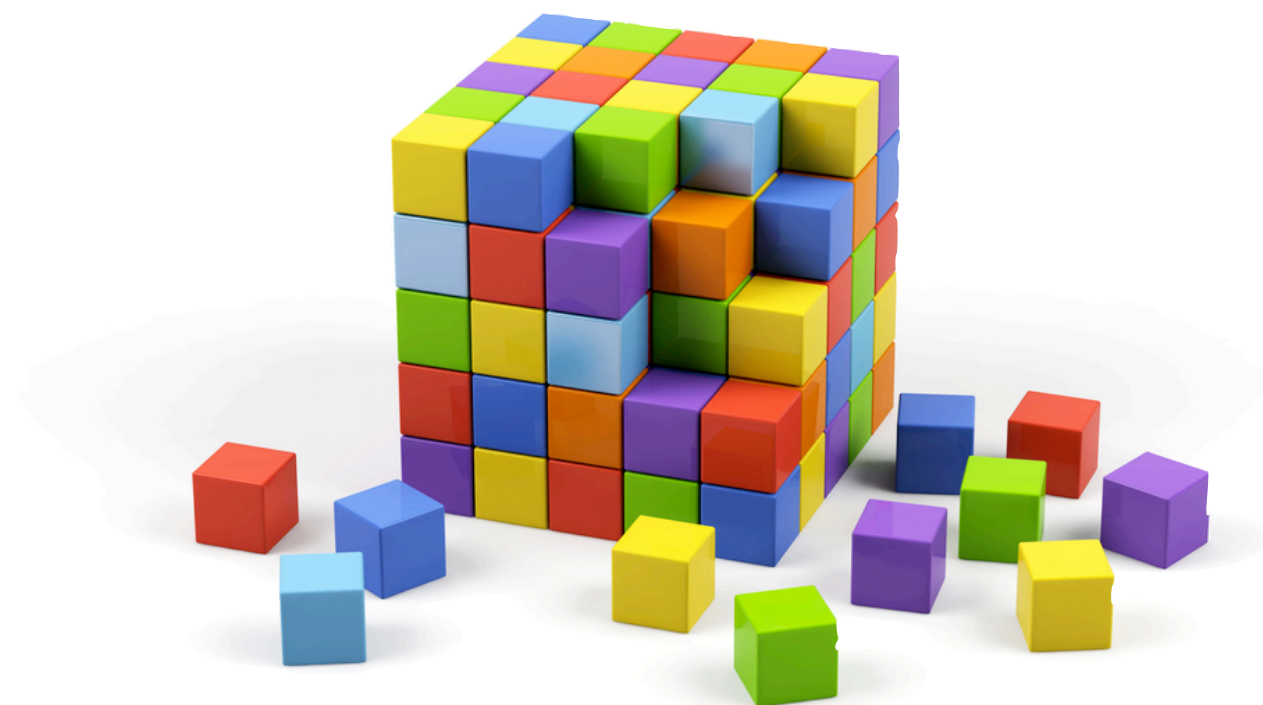


How to break captchas ?

Segmentation

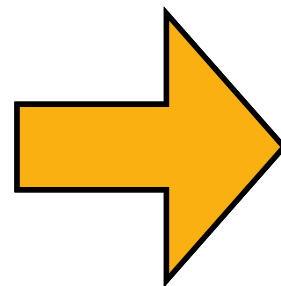


Slashdot captcha

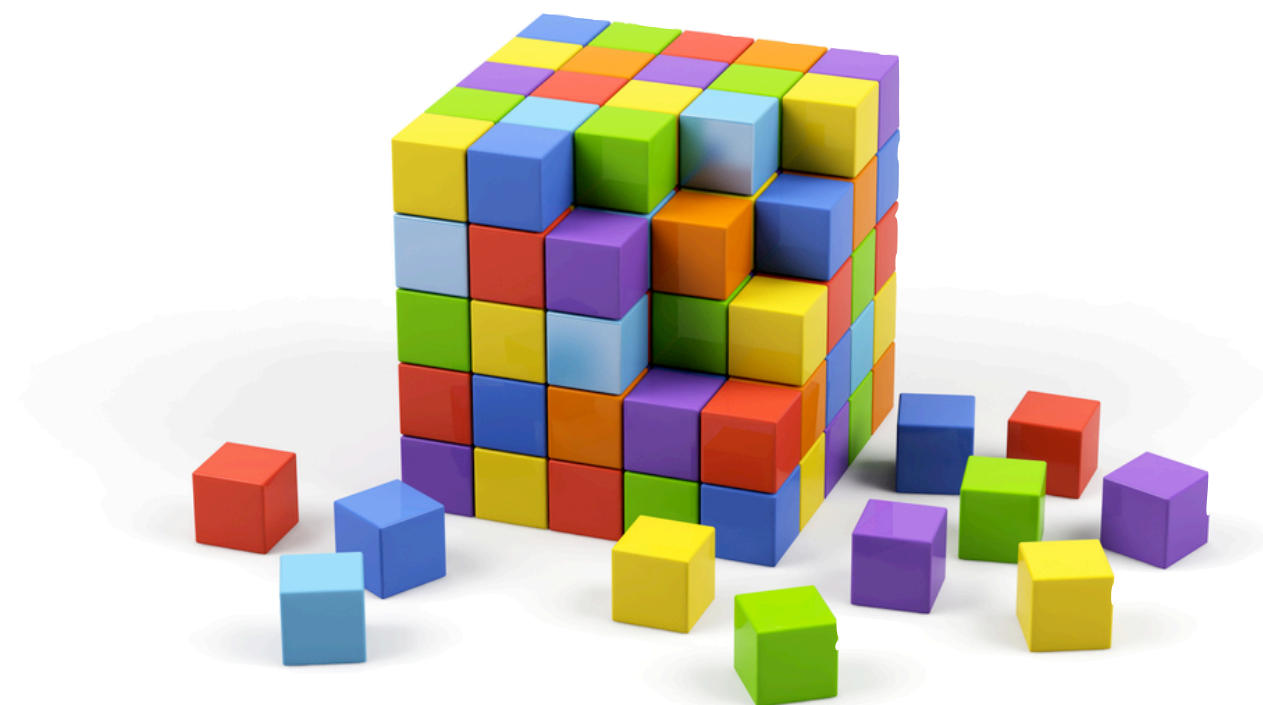


How to break captchas ?

Post-segmentation

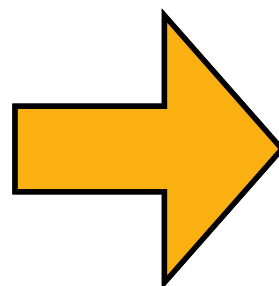


Slashdot captcha



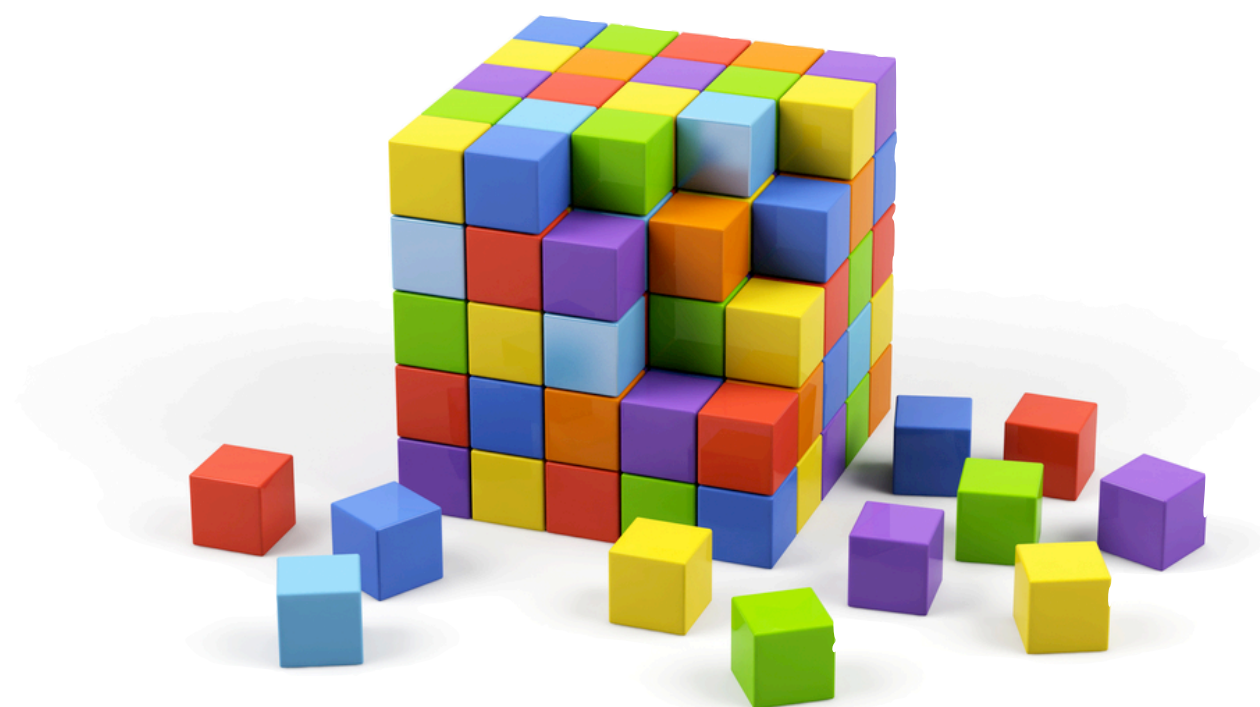
How to break captchas ?

Post-segmentation



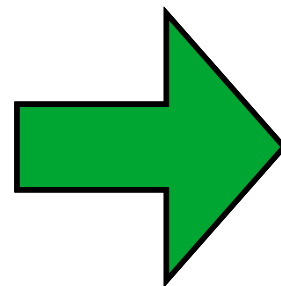
f a s t e s t

Slashdot captcha



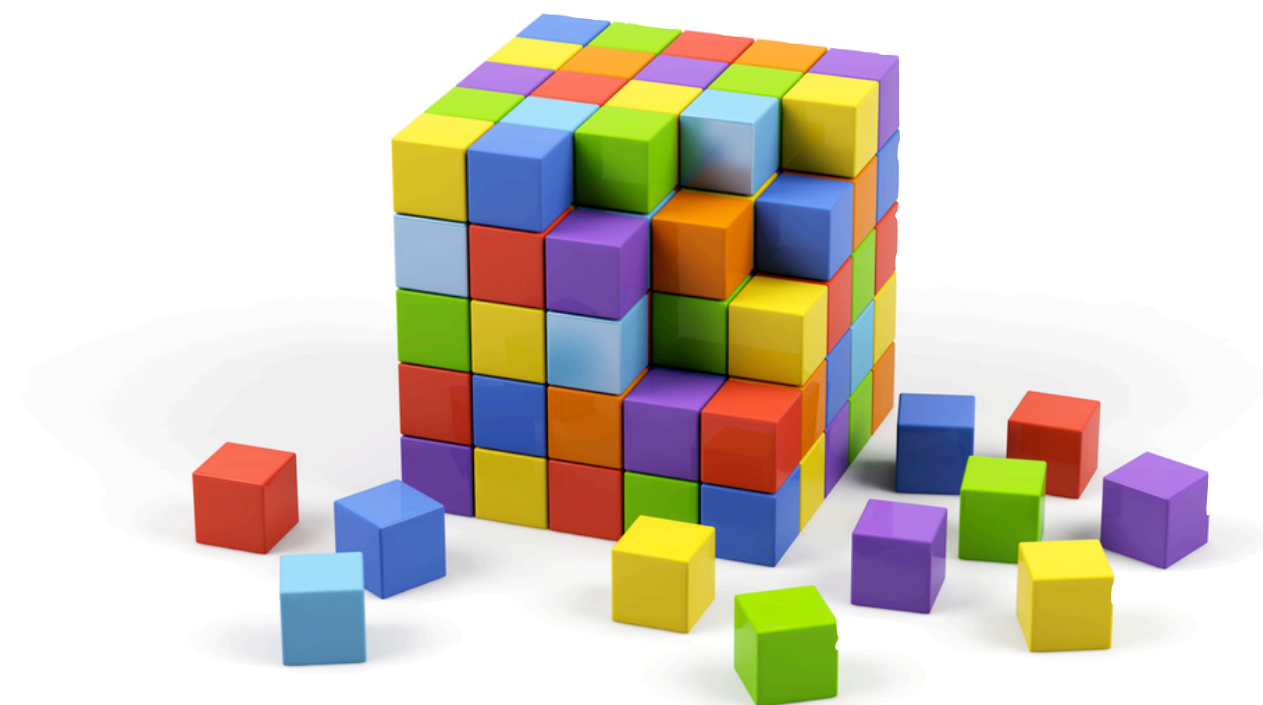
How to break captchas ?

Recognition



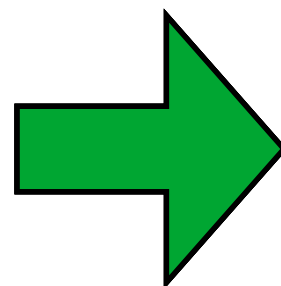
fastest

Slashdot captcha



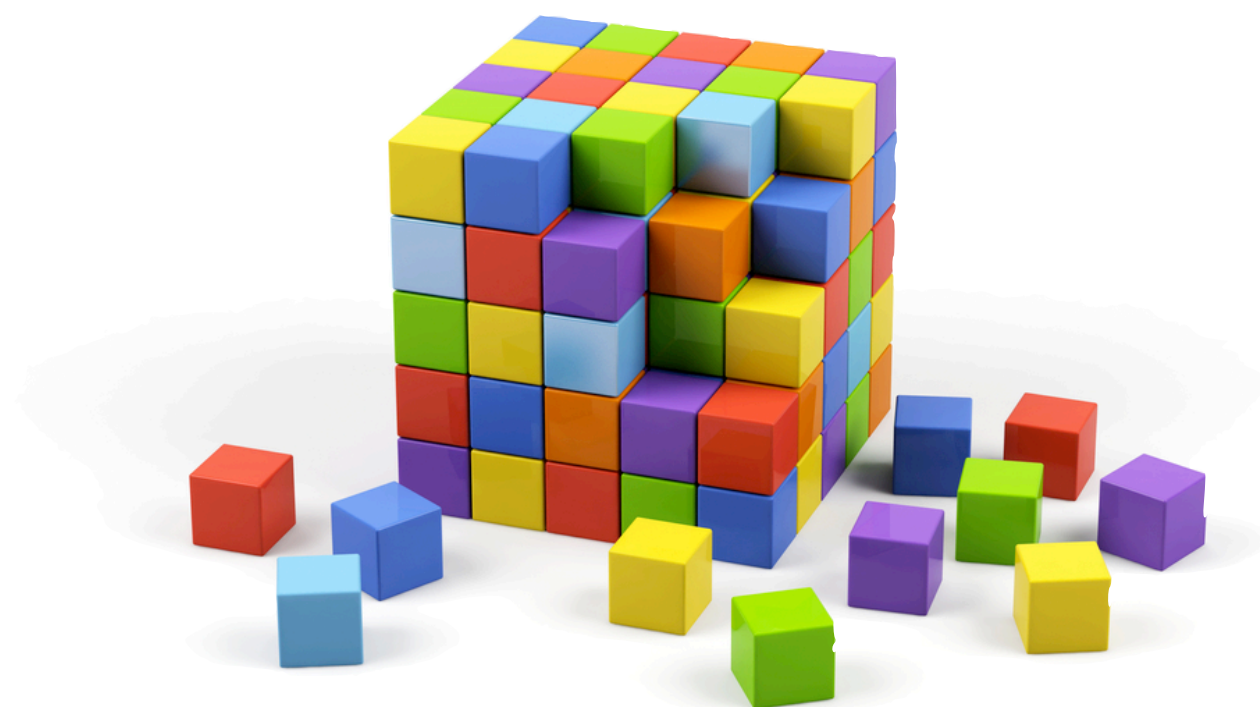
How to break captchas ?

Recognition



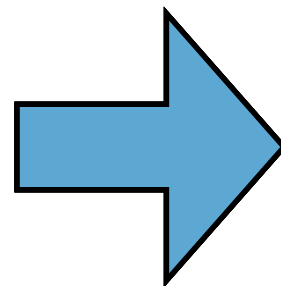
f a e t e s t

Slashdot captcha



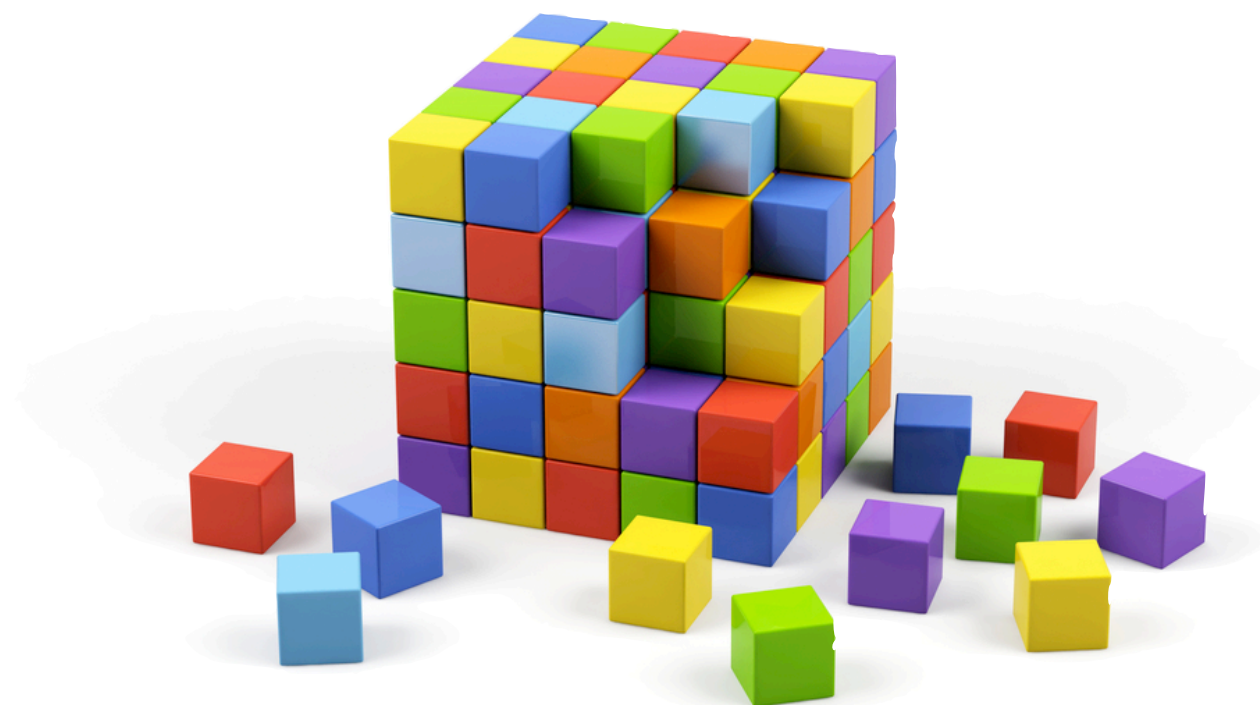
How to break captchas ?

Post-recognition



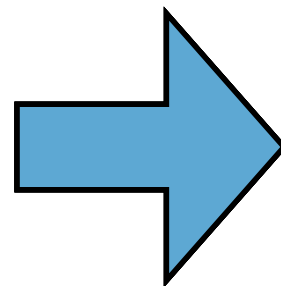
faetest

Slashdot captcha



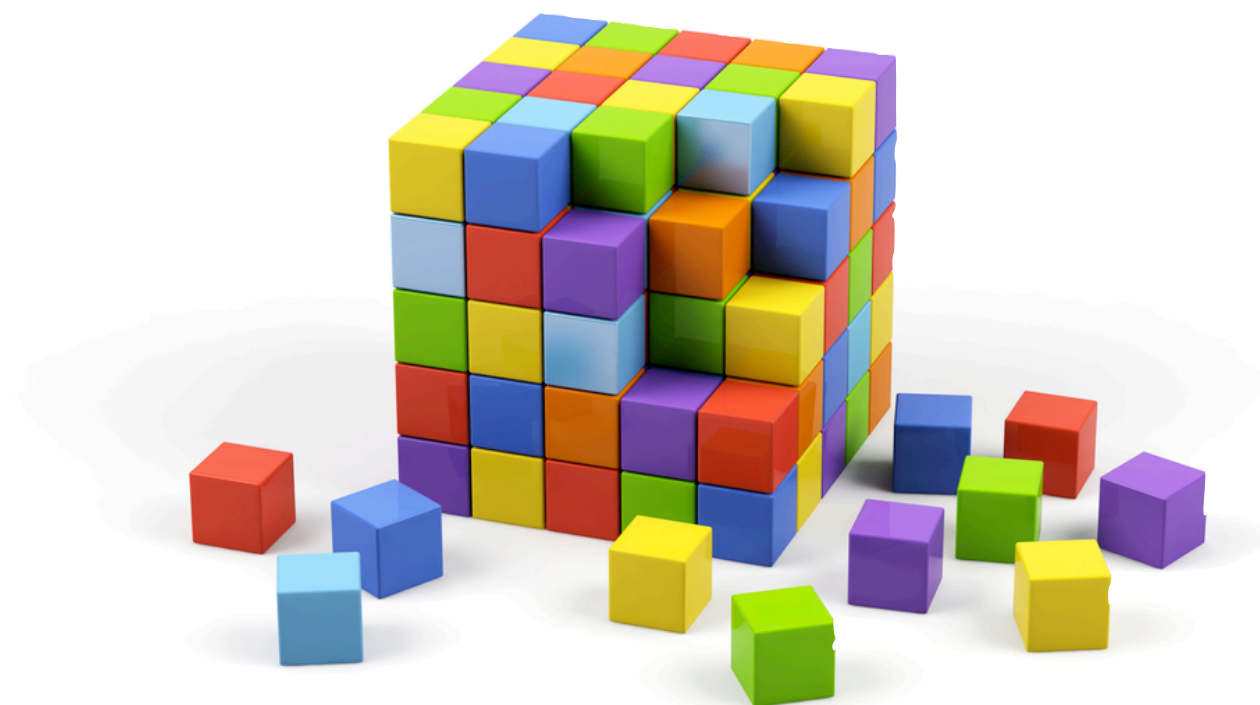
How to break captchas ?

Post-recognition



fastest

Slashdot captcha



Anti-recognition techniques

Anti-recognition techniques

Anti-recognition techniques

Blurring



3tr2bb

Anti-recognition techniques

Blurring

3tr2bb

Distortion

0zt99n

Anti-recognition techniques

Blurring

3tr2bb

Distortion

0zt99n

Rotation

0 a v y < b

Anti-recognition techniques

Blurring

3tr2bb

Distortion

0zt99n

Rotation

0 a v y < b

Fonts

0HGP22

Anti-recognition techniques

Blurring

3tr2bb

Distortion

0zt99n

Rotation

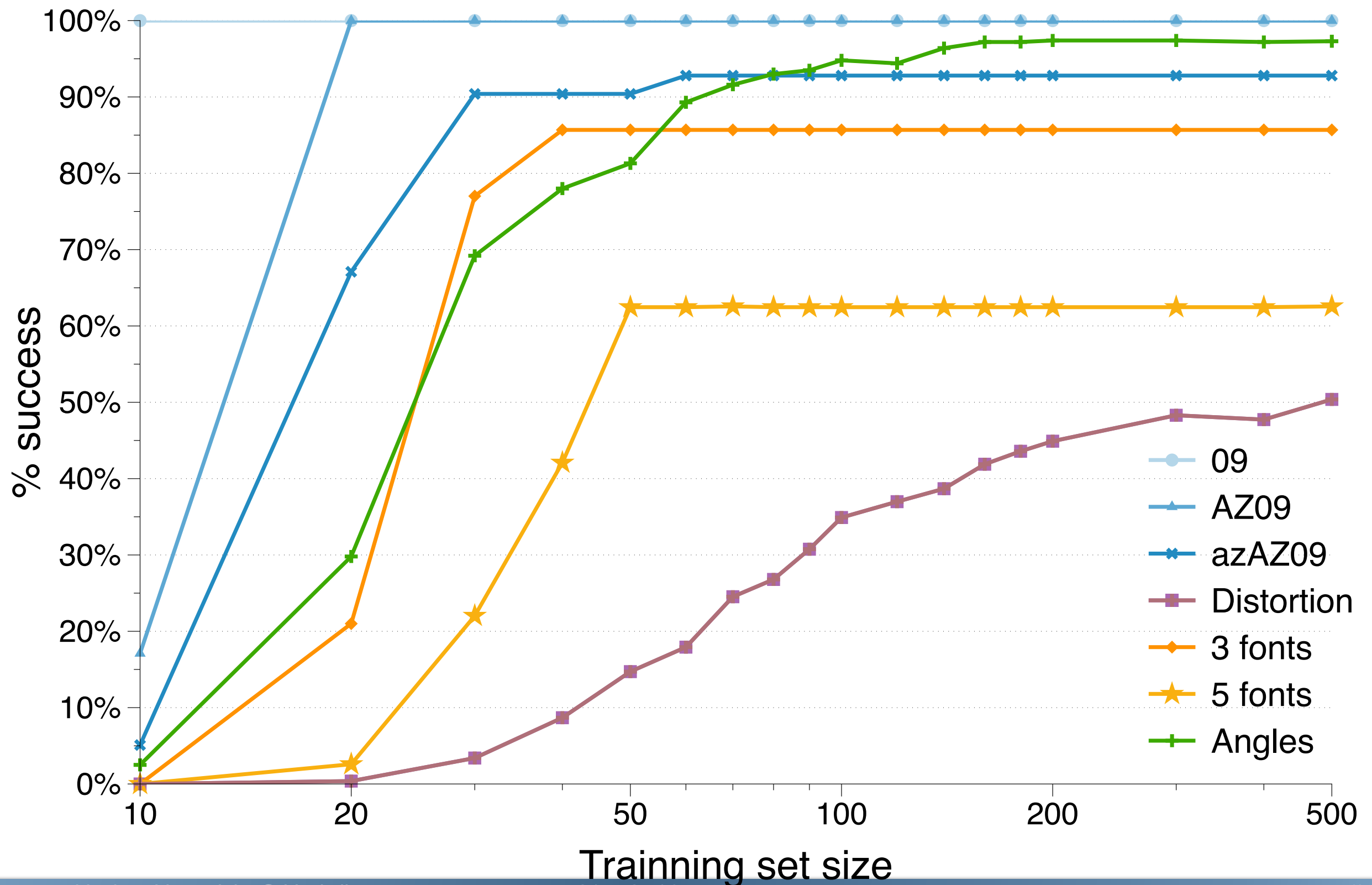
0 a v y < b

Fonts

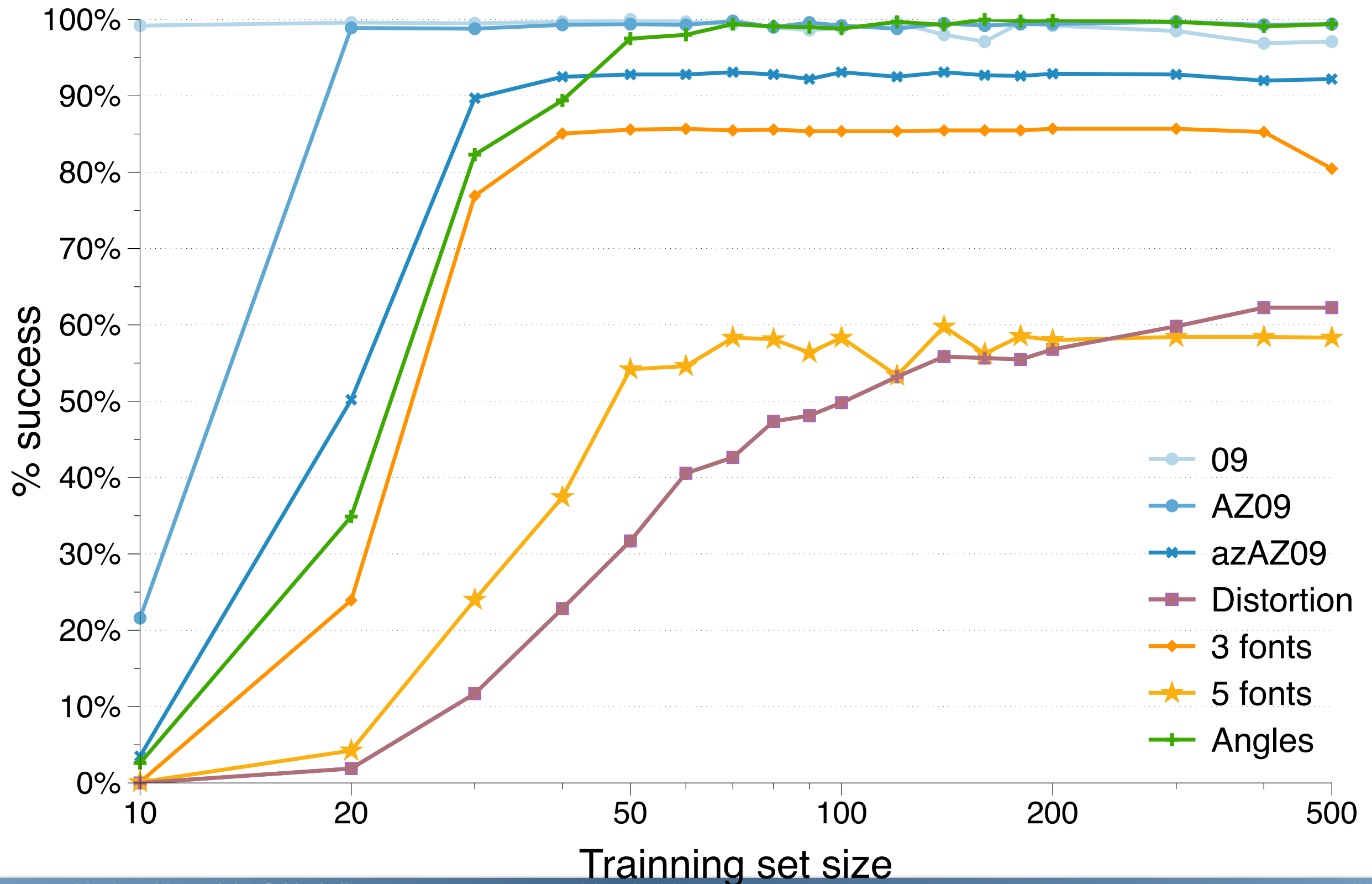
0HGP22

Charsets

SVM learning rate



KNN learning rate



Anti-segmentation techniques

Anti-recognition taxonomy

Anti-recognition taxonomy

Background Confusion

Anti-recognition taxonomy

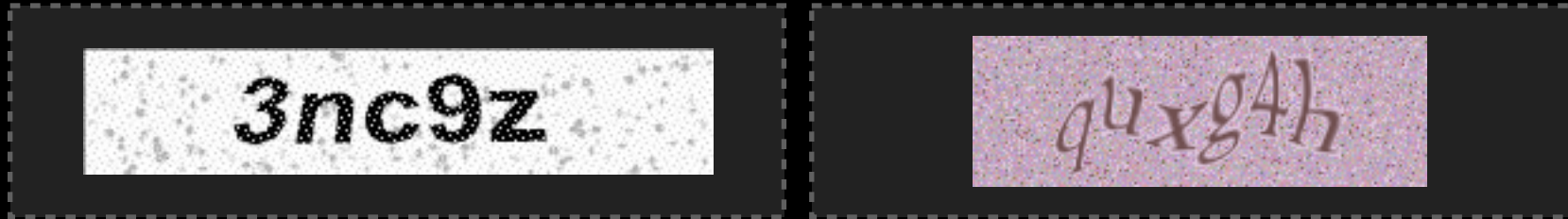
Background Confusion



3nc9z

Anti-recognition taxonomy

Background Confusion



Anti-recognition taxonomy

Background Confusion



Anti-recognition taxonomy

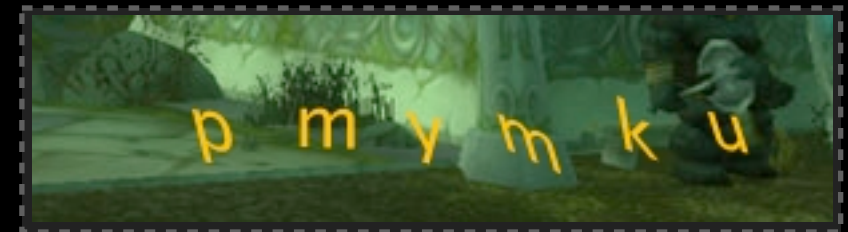
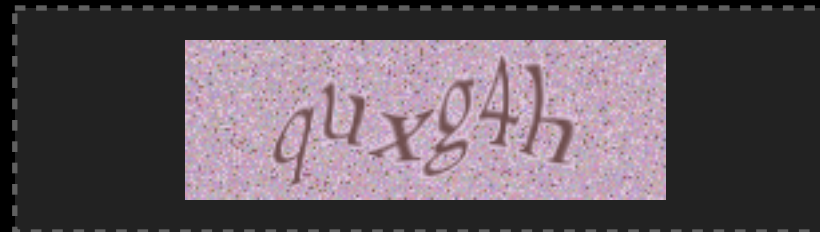
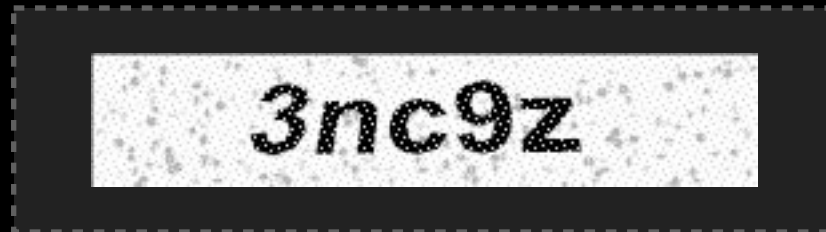
Background Confusion



Lines

Anti-recognition taxonomy

Background Confusion



Lines

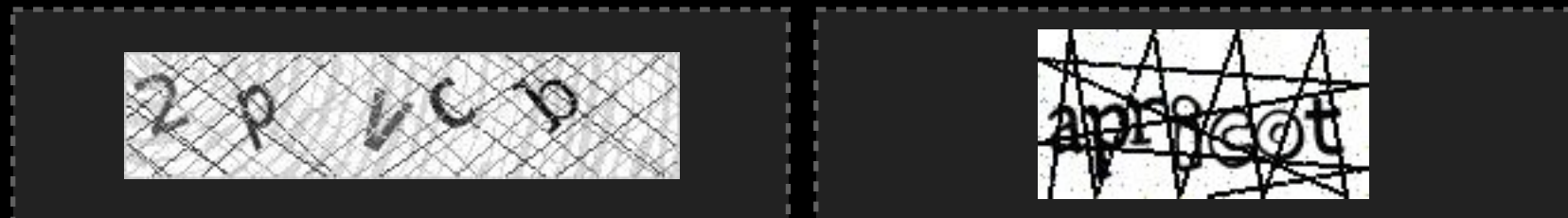


Anti-recognition taxonomy

Background Confusion



Lines



Anti-recognition taxonomy

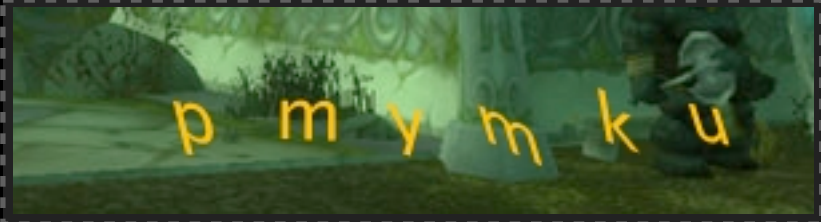
Background Confusion



3nc9z



quxg4h



p m y m k u

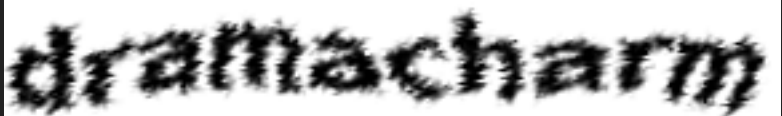
Lines



2 p 1 c b



apfscot



dramacharm

Anti-recognition taxonomy

Background Confusion



Lines



Collapsing

Anti-recognition taxonomy

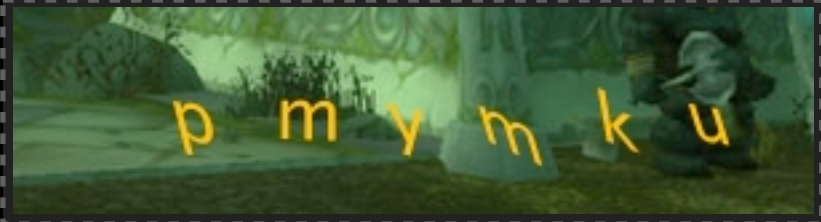
Background Confusion



3nc9z



quxg4h




p m y m k u

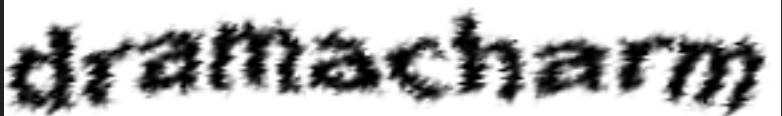
Lines



2 p 1 c b



apfscot



dramacharm

Collapsing



984505

Anti-recognition taxonomy

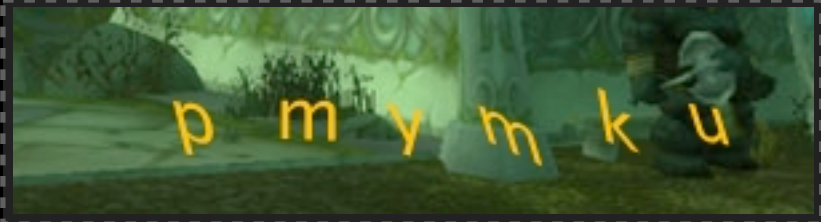
Background Confusion



3nc9z



quxg4h



p m y m k u

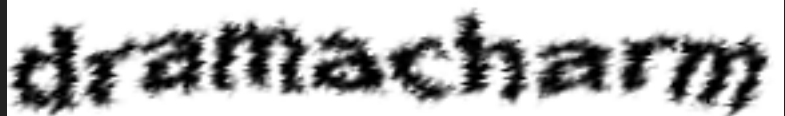
Lines



2 p 1 c p



apfscot



dramacharm

Collapsing



984505



RAE3

Anti-recognition taxonomy

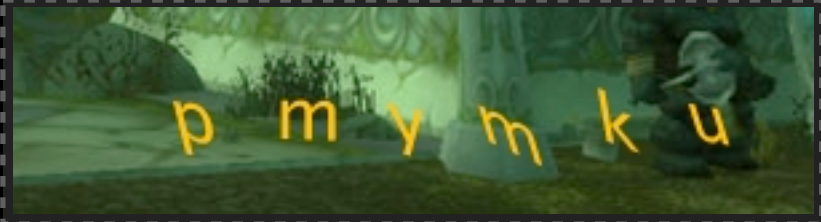
Background Confusion



3nc9z



quxg4h




p m y m k u

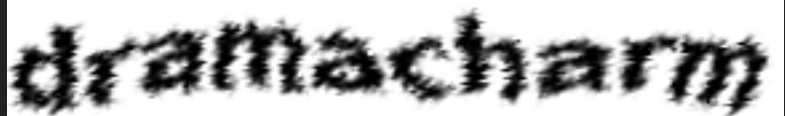
Lines



2 p 1 c p



apfscot



dramacharm

Collapsing



984505

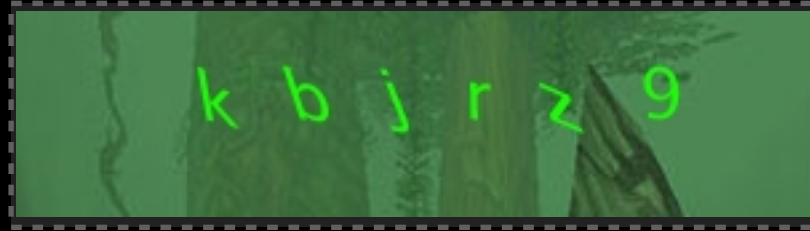


RAE3

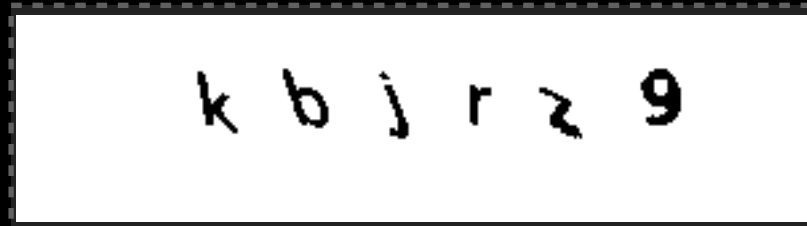
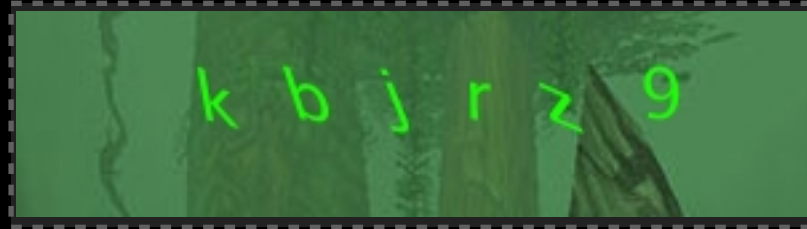


deactiesge

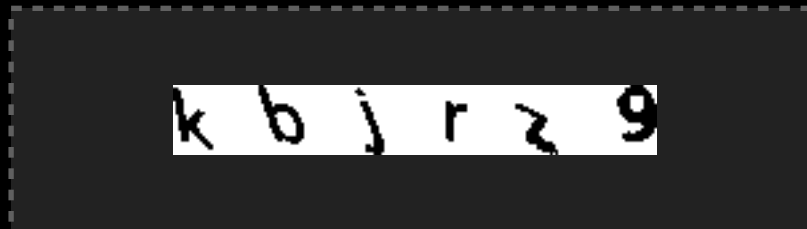
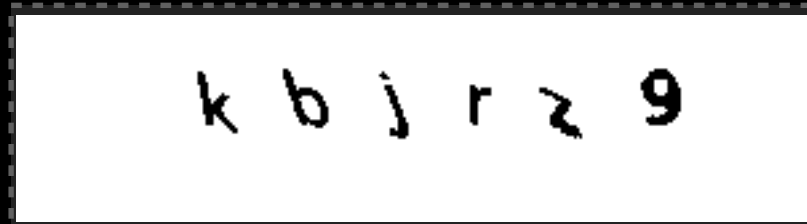
Breaking World of Warcraft



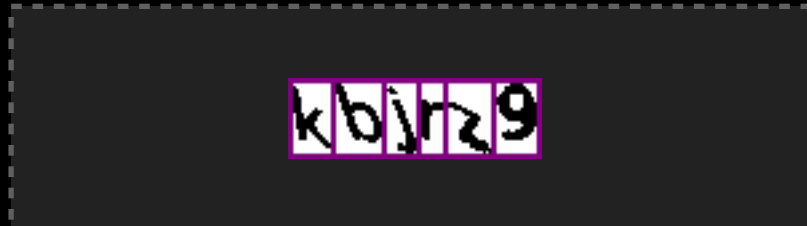
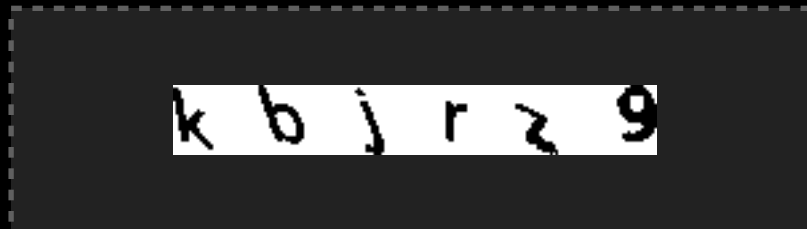
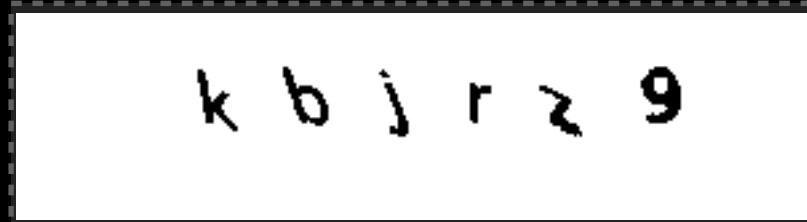
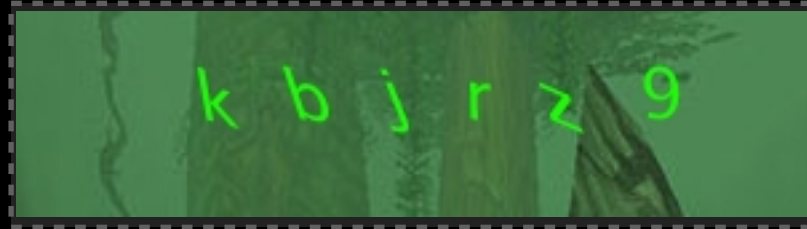
Breaking World of Warcraft



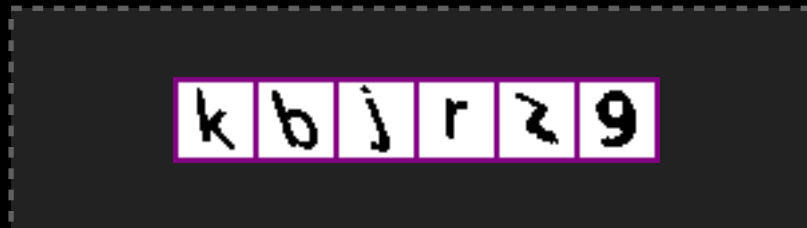
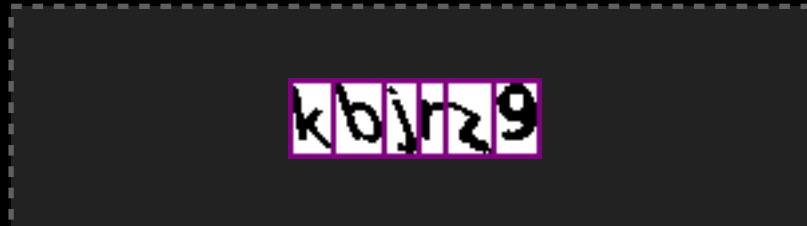
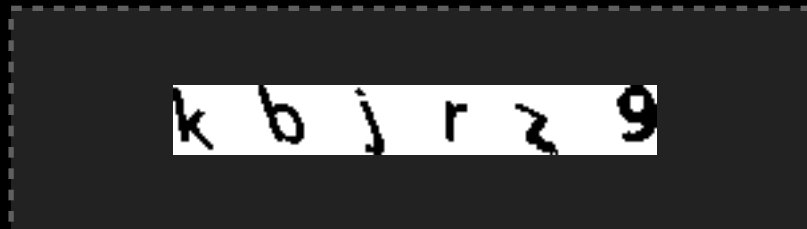
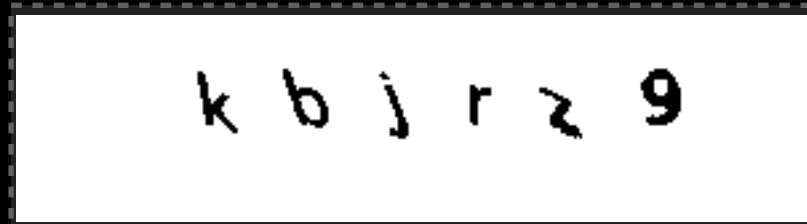
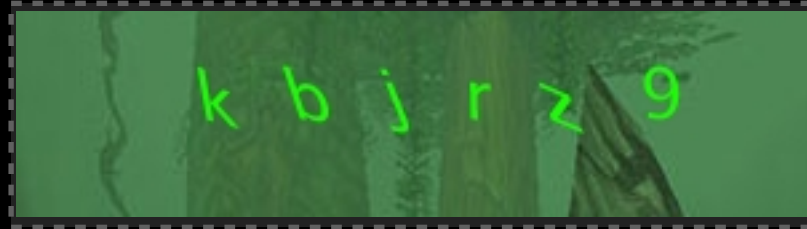
Breaking World of Warcraft



Breaking World of Warcraft



Breaking World of Warcraft



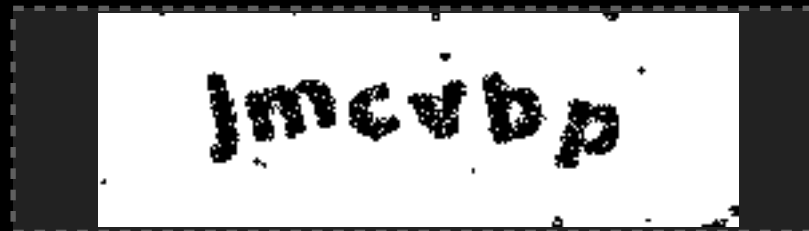
Breaking Captcha.net



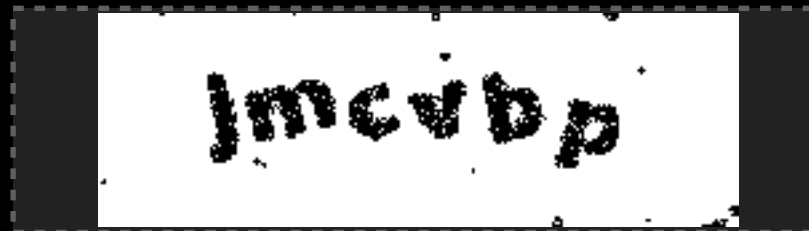
Breaking Captcha.net



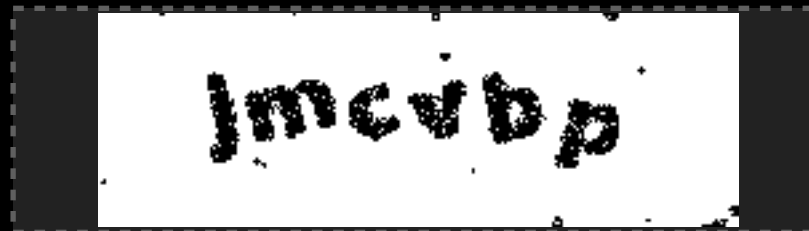
Breaking Captcha.net




Breaking Captcha.net



Breaking Captcha.net



Breaking Wikipedia



dramacharm

Breaking Wikipedia

dramacharm

dramacharm

Breaking Wikipedia

dramacharm

dramacharm

dramacharm

Breaking Wikipedia

dramacharm

dramacharm

dramacharm

dramacharm

Breaking Wikipedia

dramacharm

dramacharm

dramacharm

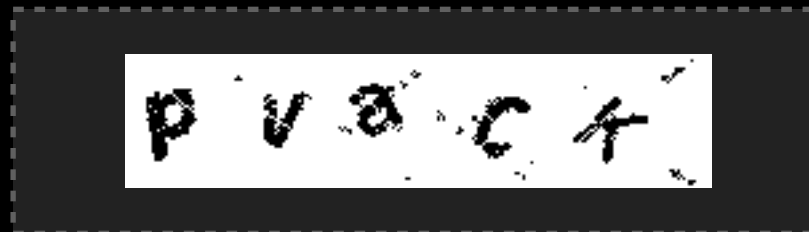
dramacharm

d r a m a c h a r m

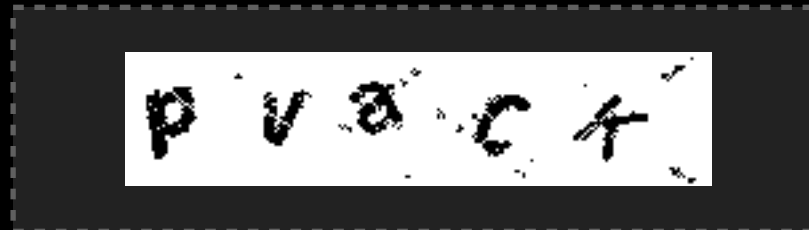
Breaking Digg



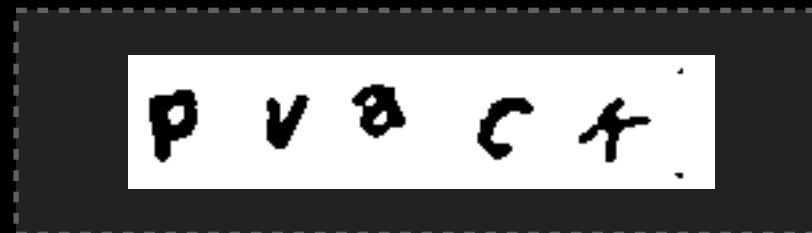
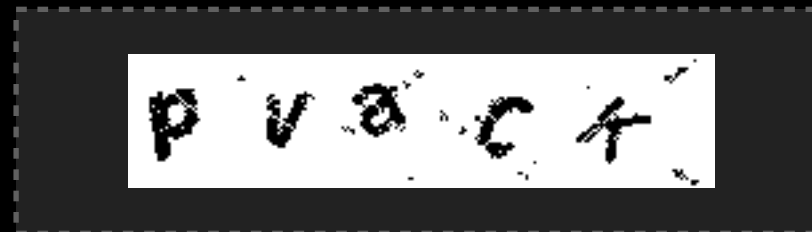
Breaking Digg



Breaking Digg



Breaking Digg



Breaking Digg

p v a c t

p v a c t

p v a c t

p v a c t

p v a c t

Breaking Slashdot



Breaking Slashdot



dissents



dissents

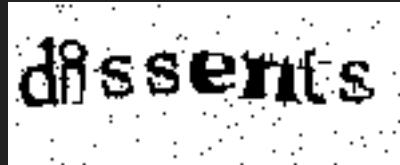
Breaking Slashdot



dissents



dissents



dissents

Breaking Slashdot



dissents



dissents



dissents



dissents

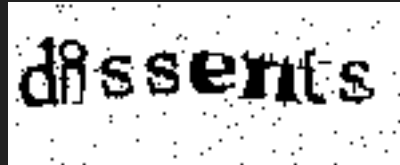
Breaking Slashdot



dissents



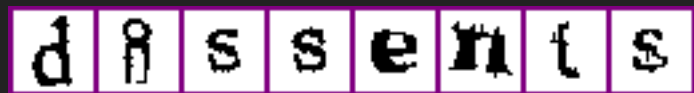
dissents



dissents



dissents



d i s s e n t s

Breaking eBay



944531

Breaking eBay

944 531

944 531

Breaking eBay

944 531

944 531

944 531

Breaking eBay

944 531

944 531

944 531

944 531

Breaking eBay

944531

944531

944531

944531

9 4 4 5 3 1

Failing to break eBay



584671

Failing to break eBay

584671

584671

Failing to break eBay

584671

584671

584671

Failing to break eBay

584671

584671

584671

584671

Failing to break eBay

584671

584671

584671

584671

5 8 4 6 7 1

Breaking Baidu



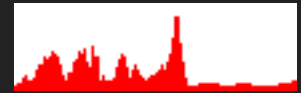
Breaking Baidu



Breaking Baidu



5A

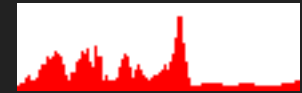


5A

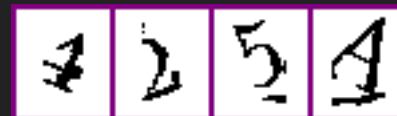
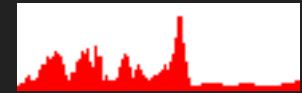
Breaking Baidu



Breaking Baidu



Breaking Baidu

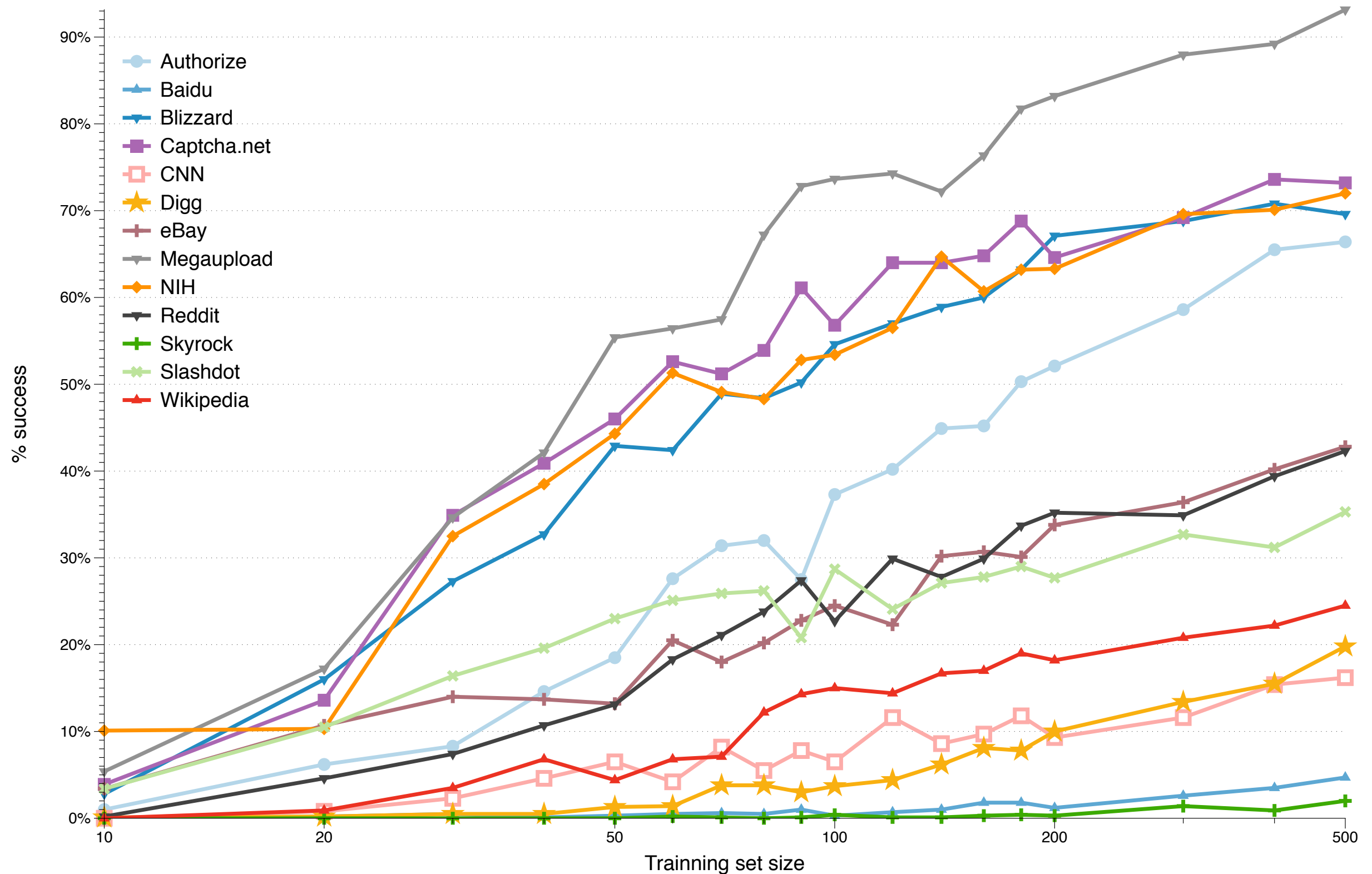


Real-world captchas security summary

Overall results

	Segmentation rate	Solving rate
Authorize	84%	66%
Baidu	98%	5%
Blizzard	75%	70%
Captcha.net	96%	73%
CNN	50%	16%
Digg	86%	20%
eBay	95%	43%
Google	0%	0%
MegaUpload	n/a	93%
NIH	87%	72%
Recaptcha	0%	0%
Reddit	71%	42%
Skyrock	30%	2%
Slashdot	52%	35%
Wikipedia	57%	25%

Learning rate for real schemes



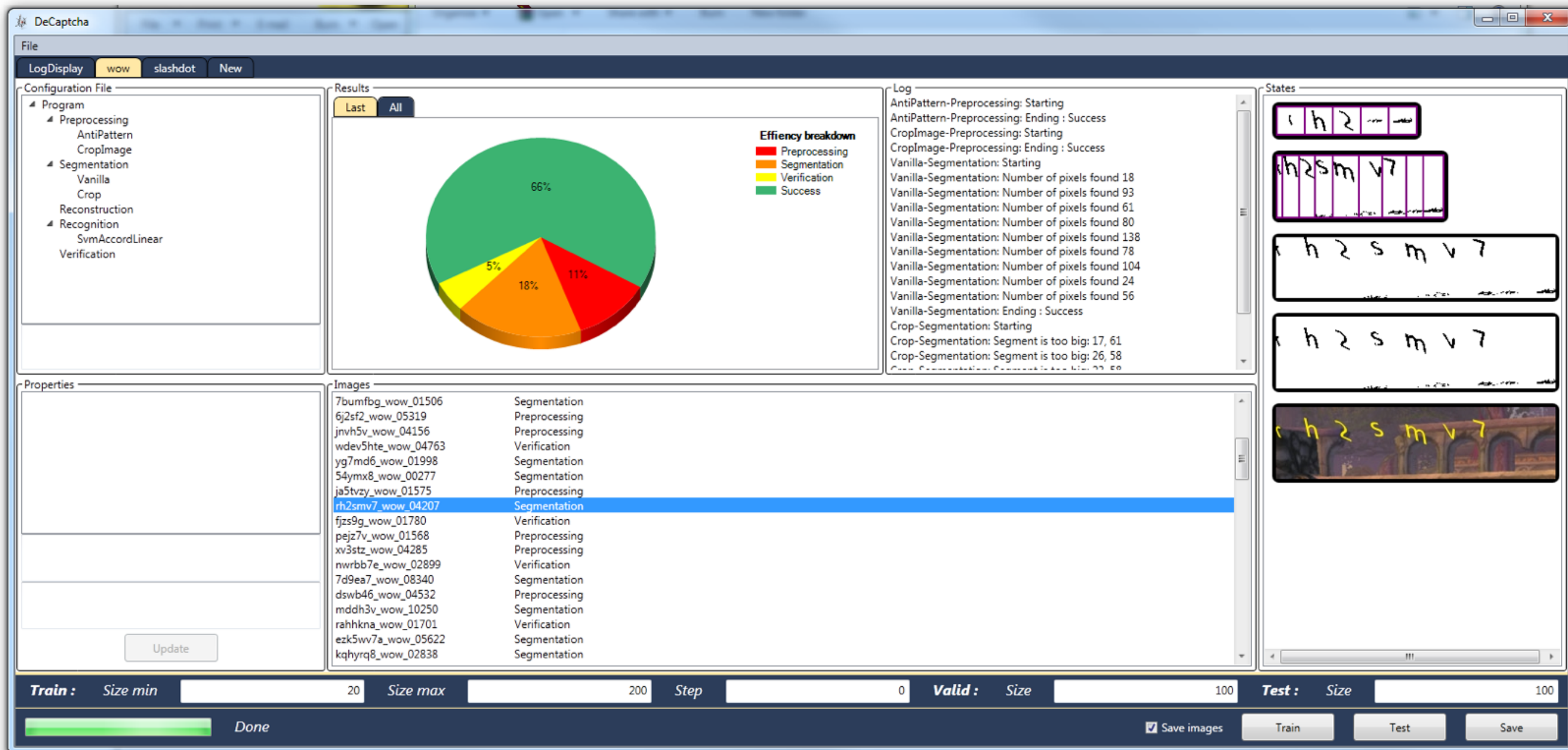
Lessons learned

Building a breaker guidelines

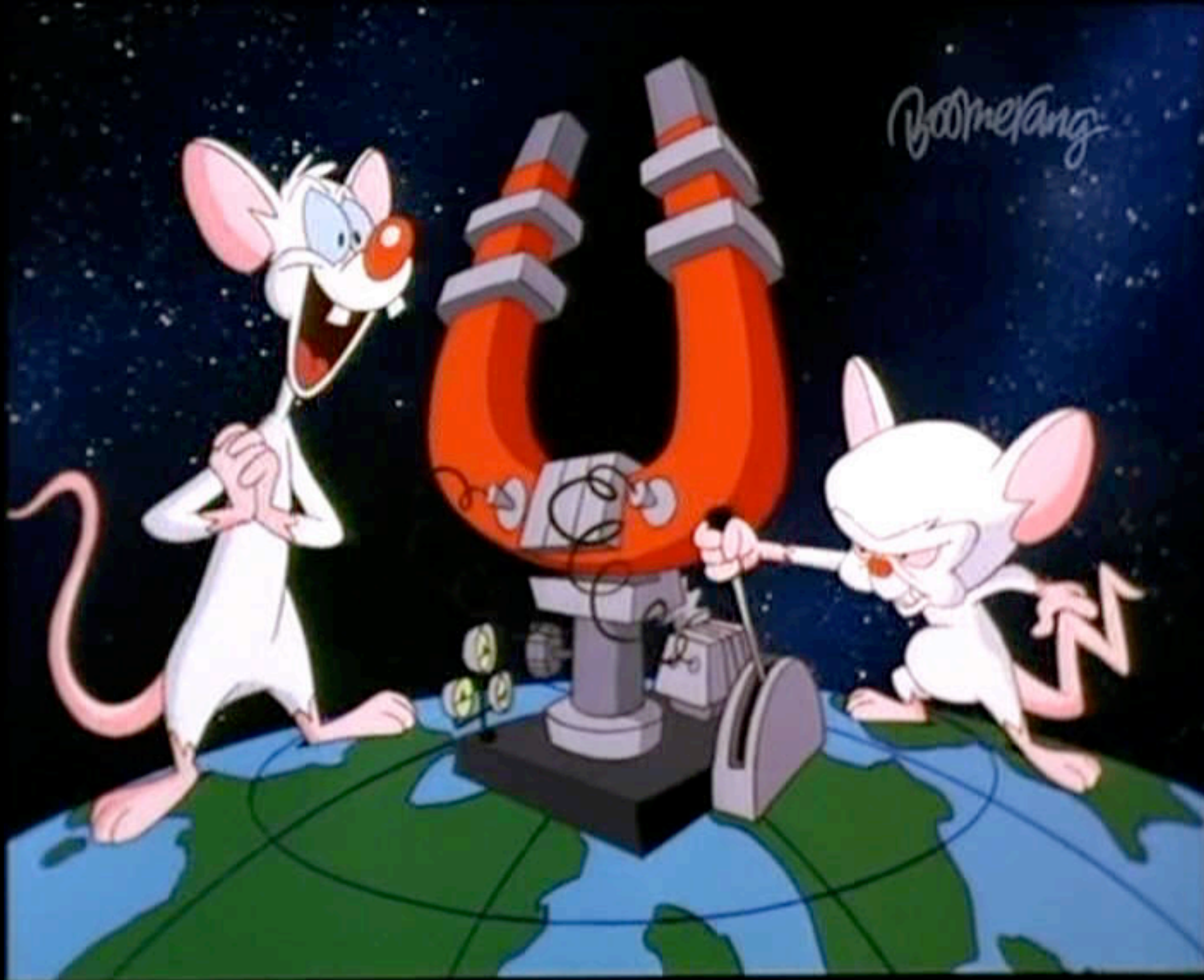
- Immediate visual feedback
- Visual debugging
- Algorithm independence
- Exposing algorithm parameters



Decaptcha main interface



Demo time



Core principles

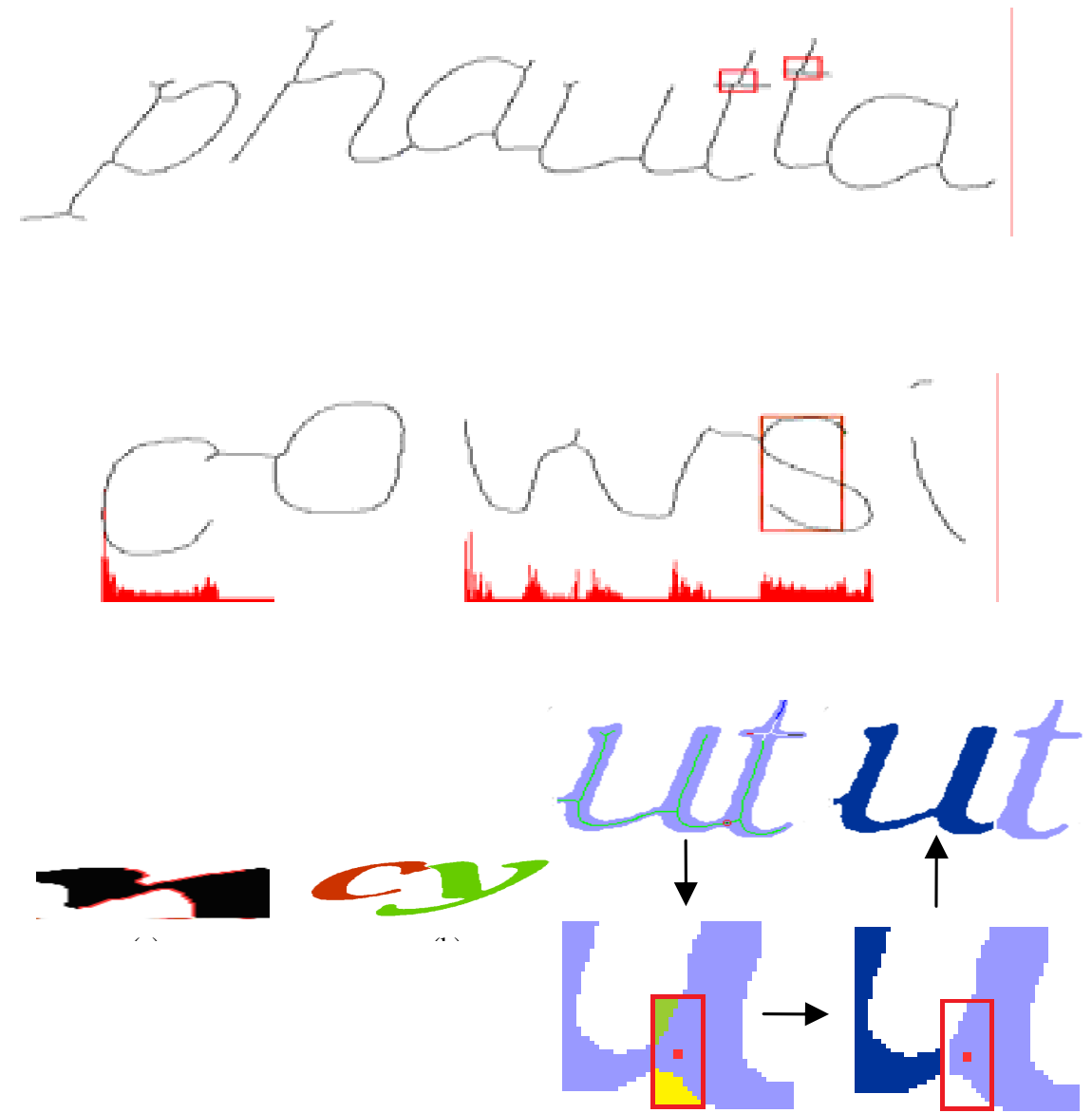
- Randomize the length
- Randomize the character size
- Wave the captcha

Anti-recognition principles

- 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

The Robustness of Google Captchas

- New heuristic to break the easy version of Google / Recaptcha
- Published online in May 2011
- Use letters shape as a side-channel
- Conclusion reduce your charset (not t or s...)



Anti-segmentation principles

- Use collapsing or lines
- Be careful in the implementation
- Create alternative schemes

Future

- Generic breaker for weak captchas
- Use higher-order features
 - to remove lines
 - Breaking collapsed captchas

Questions ?



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

Follow-me on Twitter
[@elie](#)