The End is Nigh

Generic Solving of Text-based

Elie Bursztein, Jonathan Aigrain, Angelika Mosciki,
John Mitchell

\

Home | Notifications 11 | Discover | Me | Search Twitter

Elie Bursztein

@elie

Work at Google. Protect users. Disrupt bad guys. Make Chrome safer and faster. Wear berets. Do magic tricks and blog at elie.net/blog

Mountain View

elie.net

Joined July 2009

61 Photos and videos

TWEETS 2,053 | PHOTOS/VIDEOS 61 | FOLLOWING 54 | FOLLOWERS 6,975 | FAVORITES 38 | More

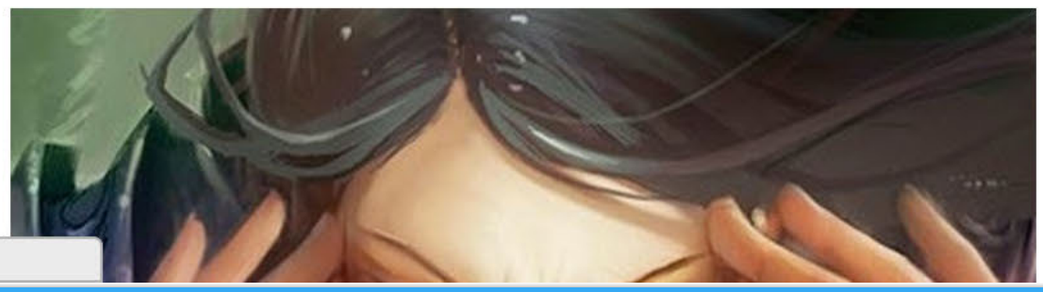
Tweets | Tweets and replies

Pinned Tweet

Elie Bursztein @elie · Aug 13

Predicting Hearthstone opponent deck using machine learning - bit.ly/Y5MTkn #hearthstone #game #defcon

Elie Bursztein



Who

Popular

https://twitter.com/elie#more

Home | Notifications 11 | Discover | Me | Search Twitter

Elie Bursztein

@elie

Work at Google. Protect users. Disrupt bad guys. Make Chrome safer and faster. Wear berets. Do magic tricks and blog at elie.net/blog

Mountain View

elie.net

Joined July 2009

61 Photos and videos

TWEETS 2,053 | PHOTOS/VIDEOS 61 | FOLLOWING 54 | FOLLOWERS 6,975 | FAVORITES 38 | More

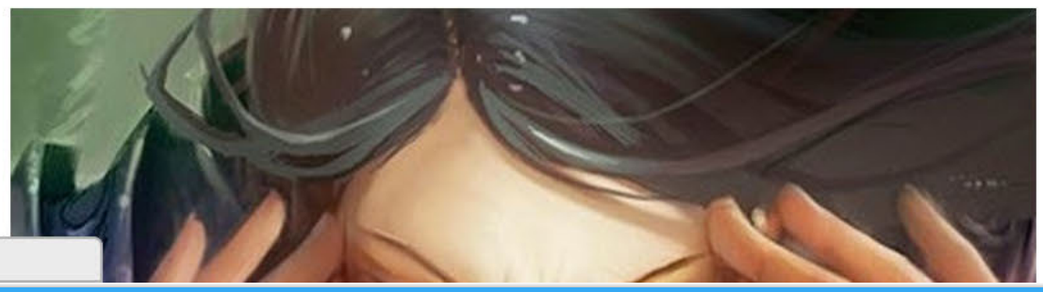
Tweets | Tweets and replies

Pinned Tweet

Elie Bursztein @elie · Aug 13

Predicting Hearthstone opponent deck using machine learning - bit.ly/Y5MTkn #hearthstone #game #defcon

Elie Bursztein



Who

Popular

https://twitter.com/elie#more

GetTwitterFollowers

HOME | TWITTER FOLLOWER PACKAGES | FAQ | ABOUT US | CONTACT | VIEW CART

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

Hom

twitter

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**

Password: •••••••••• — Good

Are you human?

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

Can't read this?
Get two new words
Hear a set of words
Powered by reCAPTCHA.
Help

Type the words above

Finish

Create my account

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

Elie B
@elie
Work at
bad guy
faster. W
blog at
Mour
elie.r
Joine
61 Ph

Who

Popular

https://twitter.com/

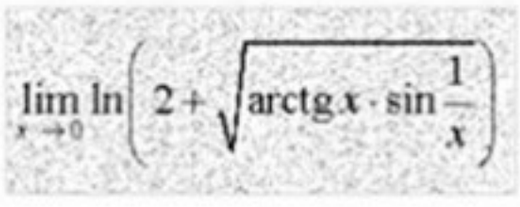
Elie Bursztein

captcha

Captcha Validation: *

Captcha Validation: *

Защита от автоматической регистрации



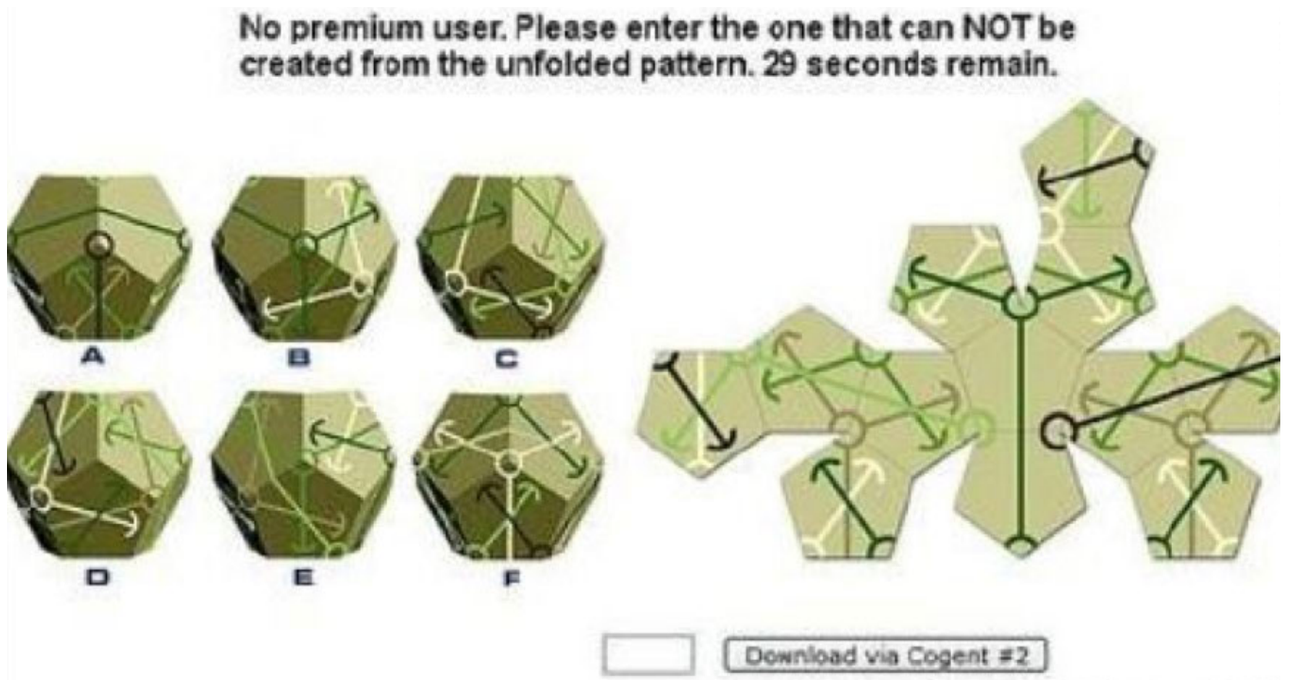
Введите ответ

Captcha Validation: *

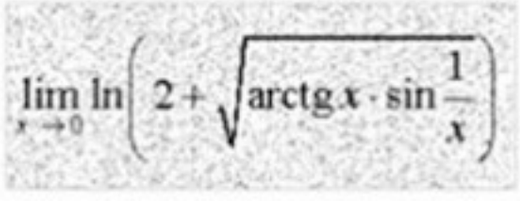
Защита от автоматической регистрации

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

Введите ответ

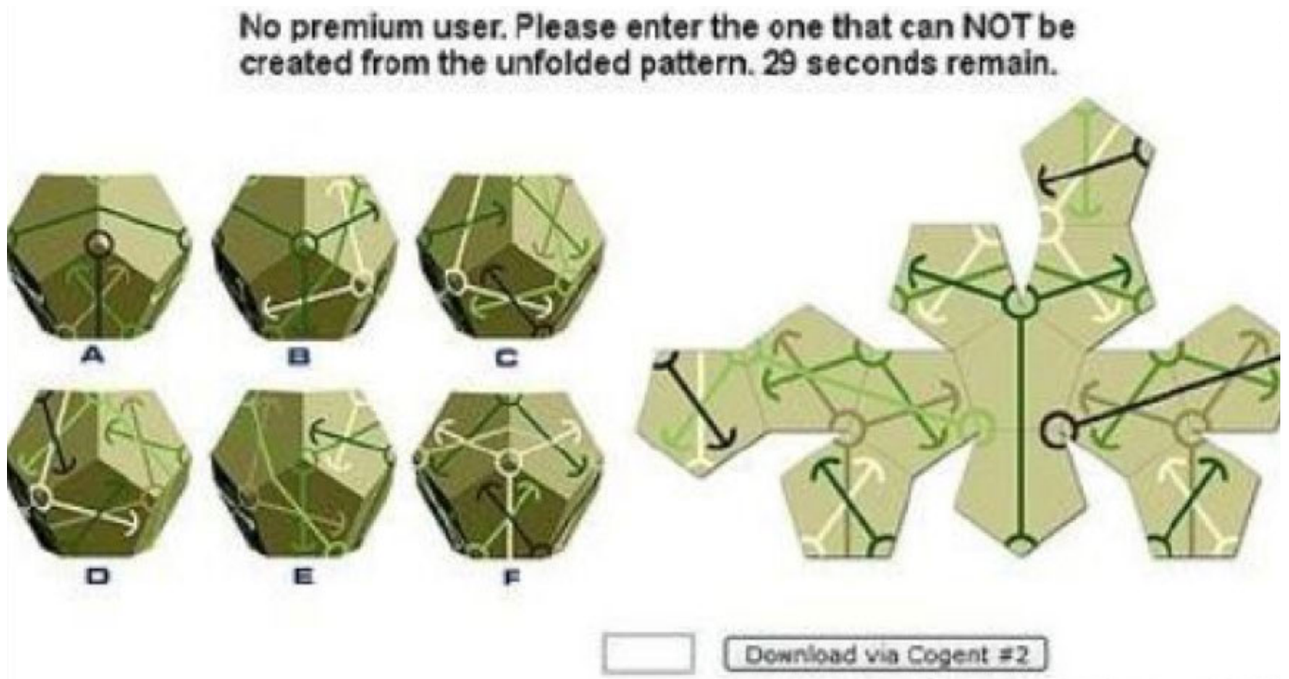


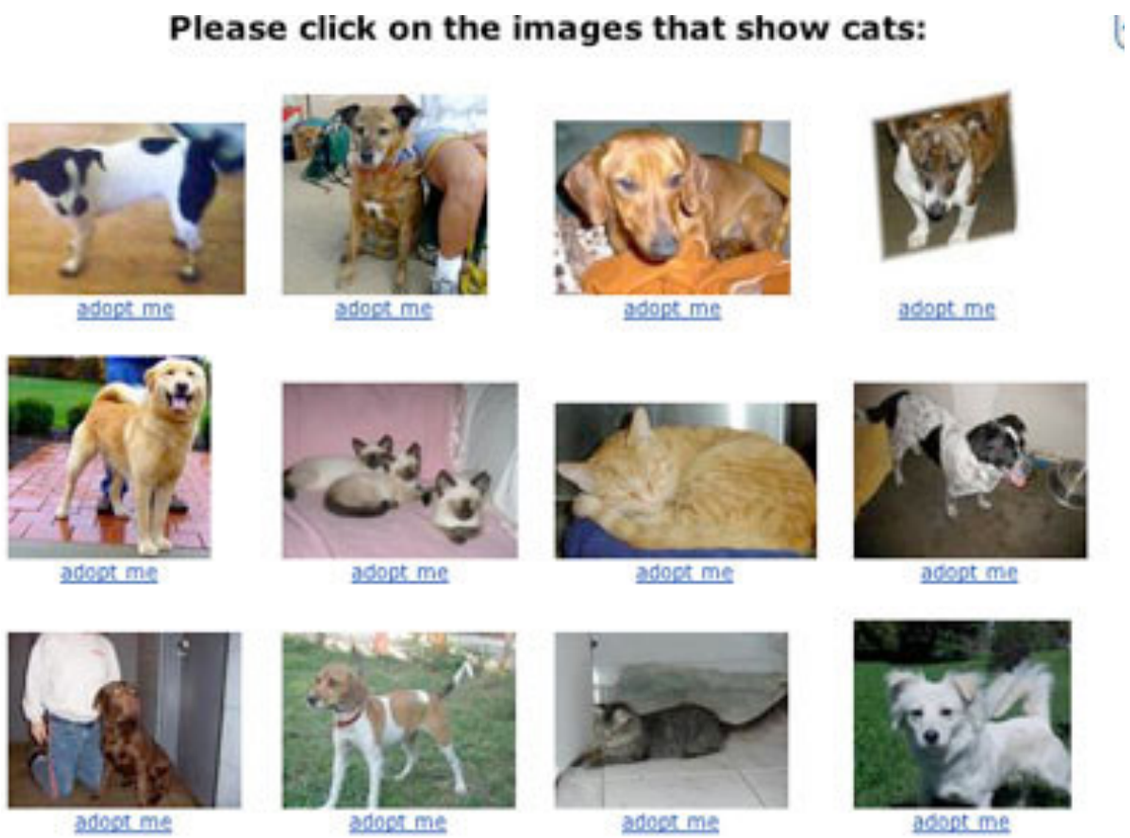
Captcha Validation: *

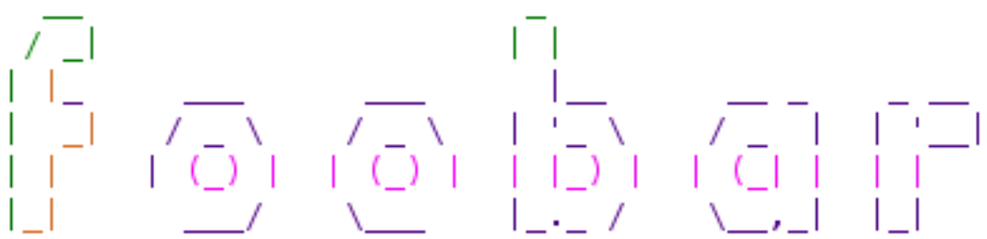


Защита от автоматической регистрации

Введите ответ





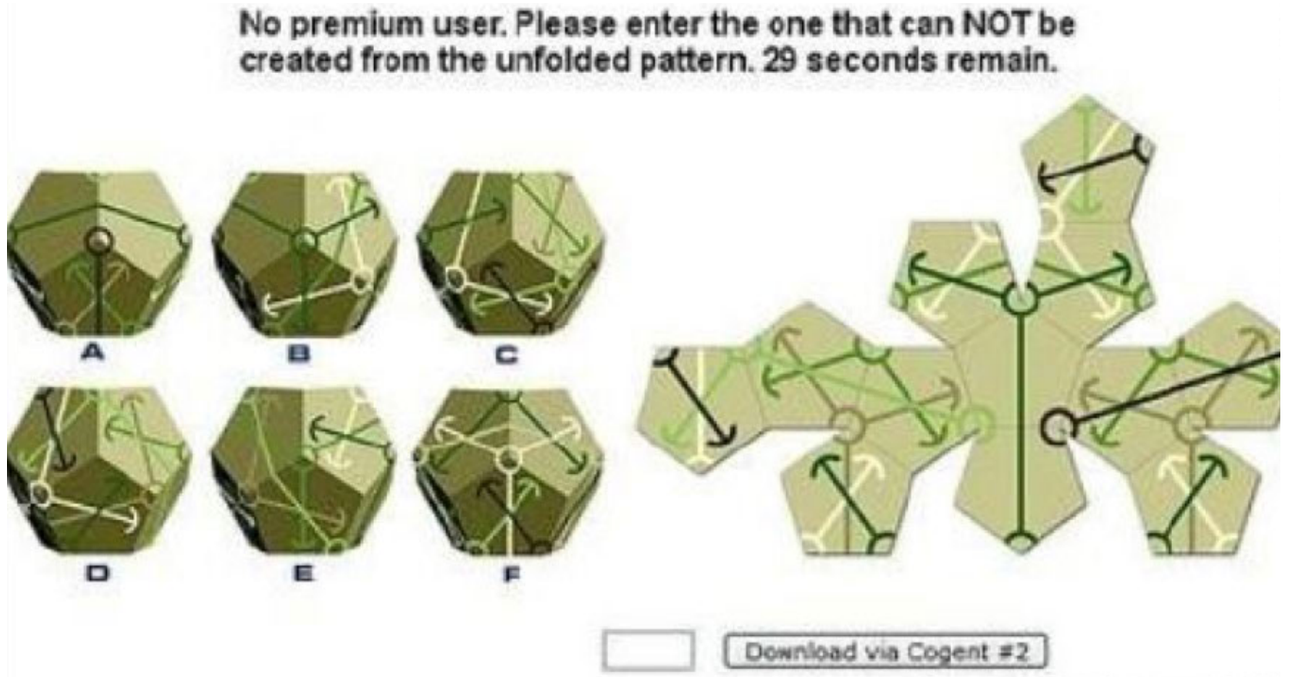


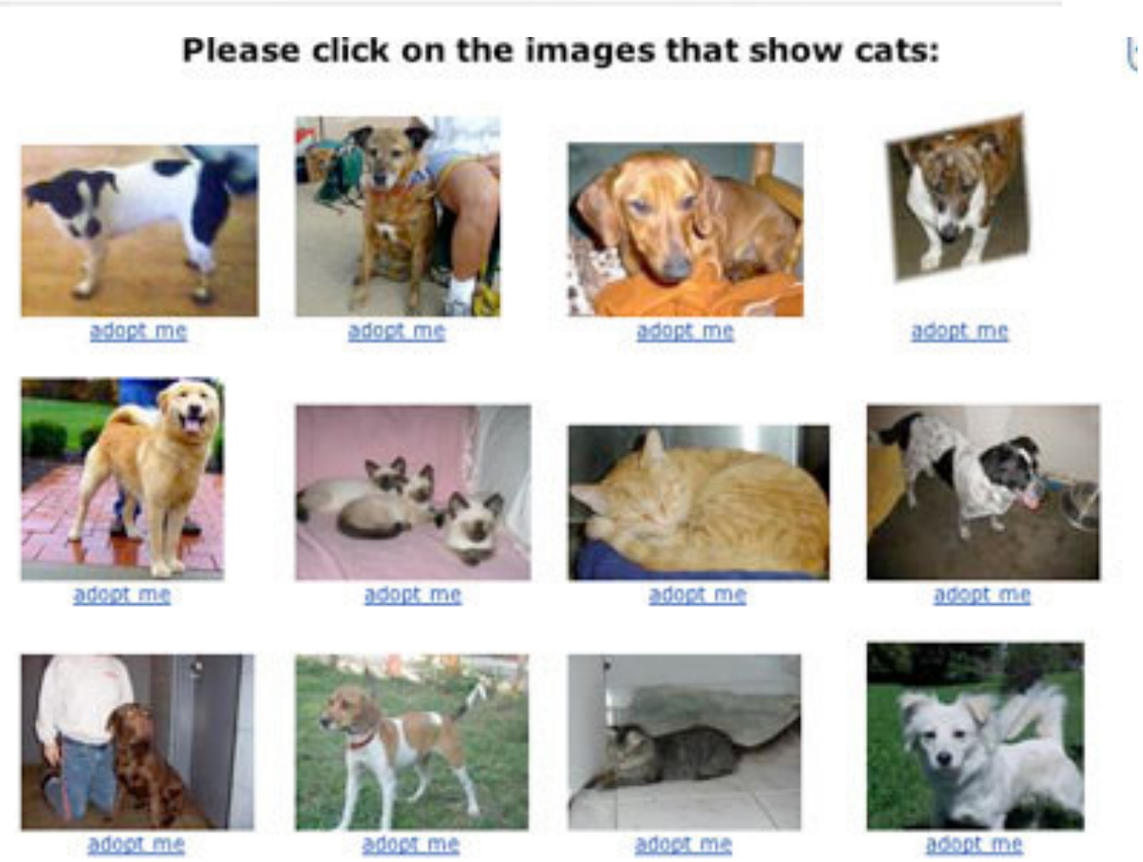
Captcha Validation: *

Защита от автоматической регистрации

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

Введите ответ

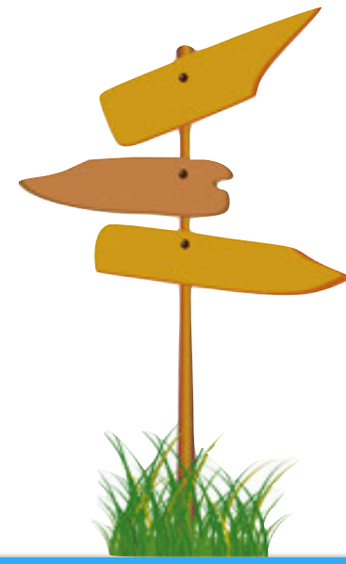




Real world Captchas

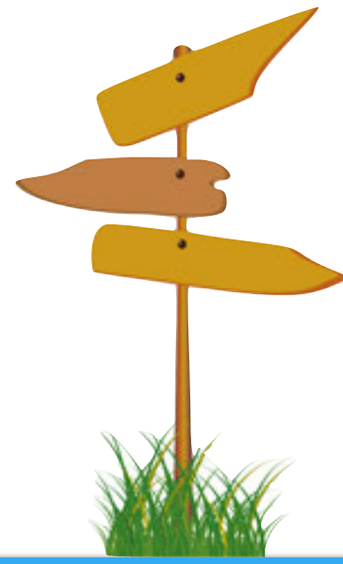
Baidu (2011)	
Baidu (2013)	
CNN	
eBay	
ReCaptcha (2011)	
ReCaptcha (2013)	
Wikipedia	
Yahoo	

Outline



Outline

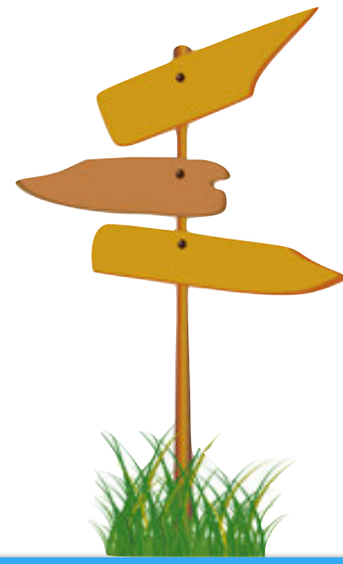
Old approach: segment then recognize



Outline

Old approach: segment then recognize

Our new approach: single machine learning step

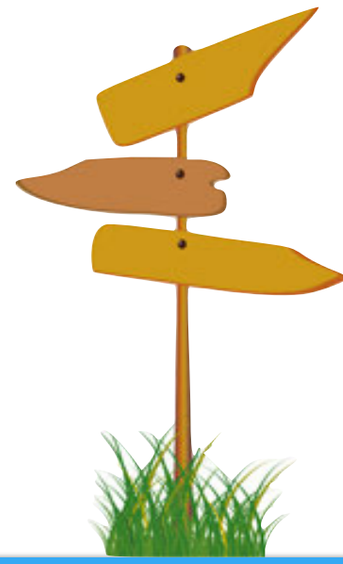


Outline

Old approach: segment then recognize

Our new approach: single machine learning step

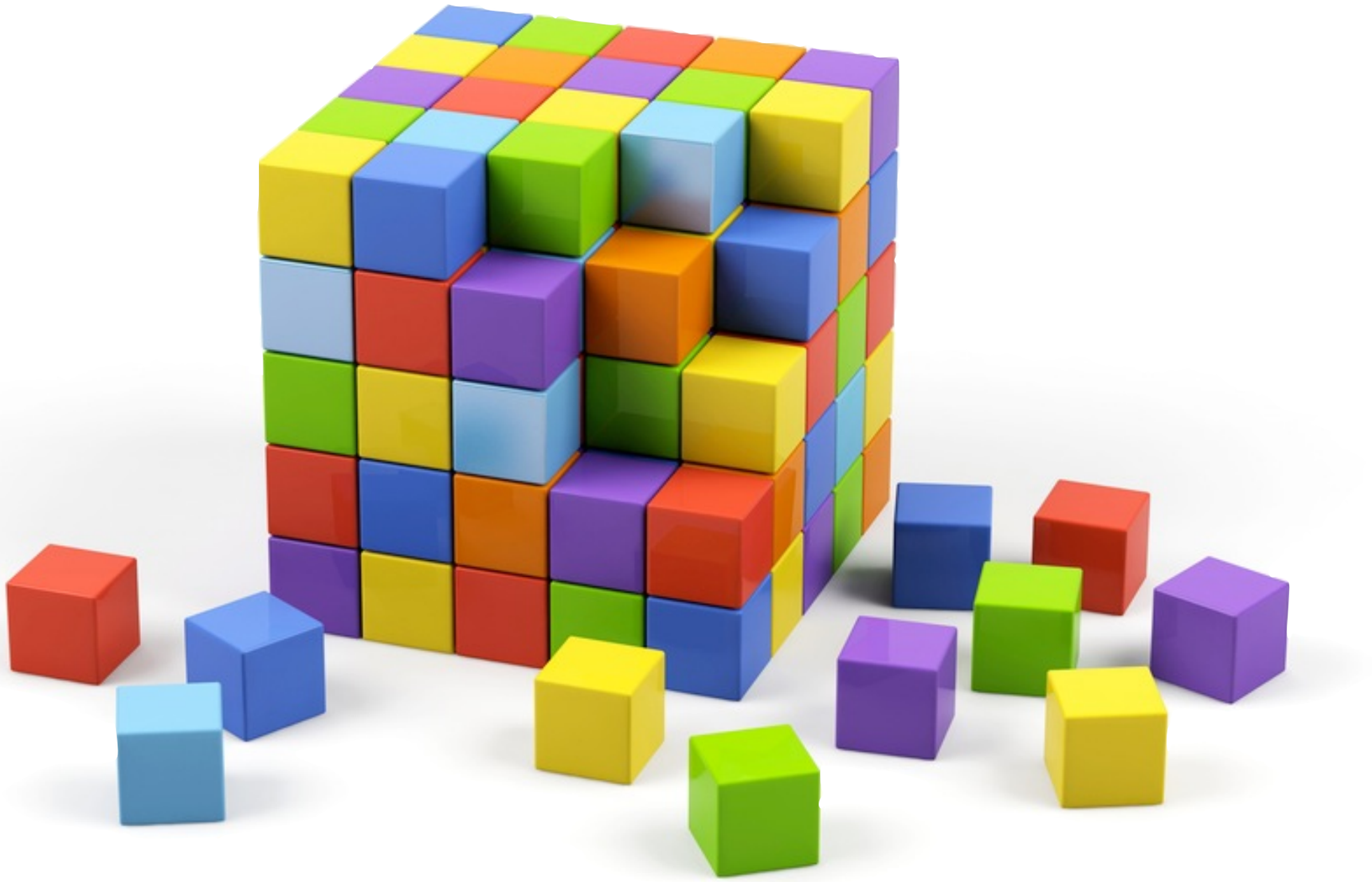
Evaluation: efficiency on real world captchas



Segment then recognize

How to break captchas the old way

\



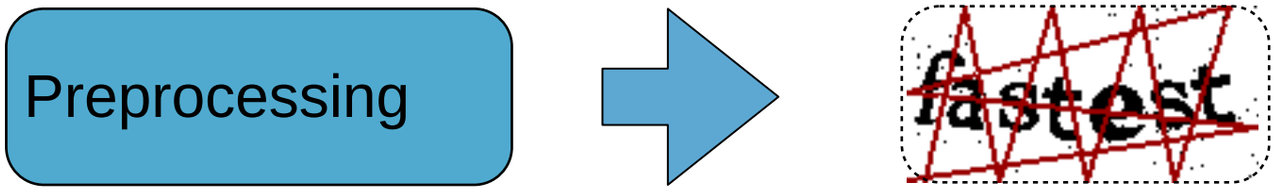
Think lego

The segment then recognize approach

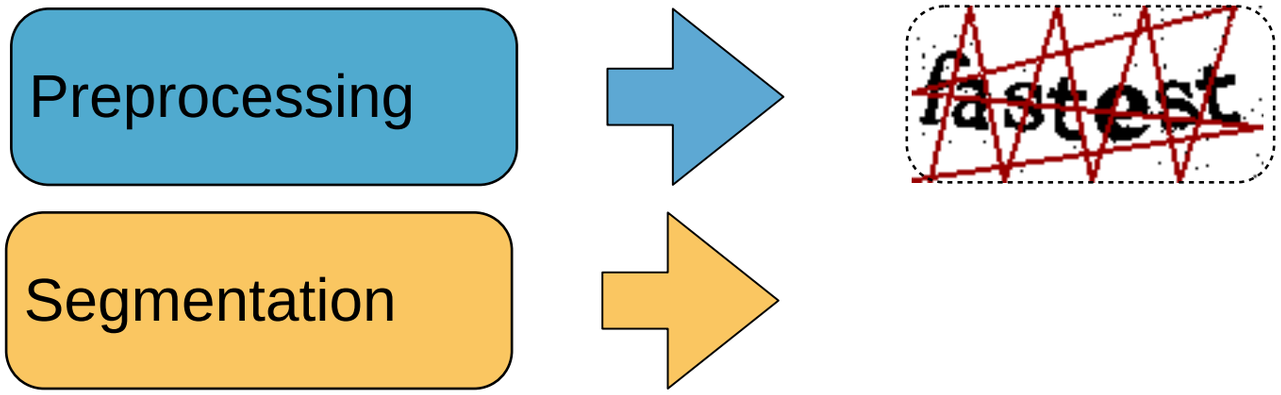
Slashdot captcha

The segment then recognize approach

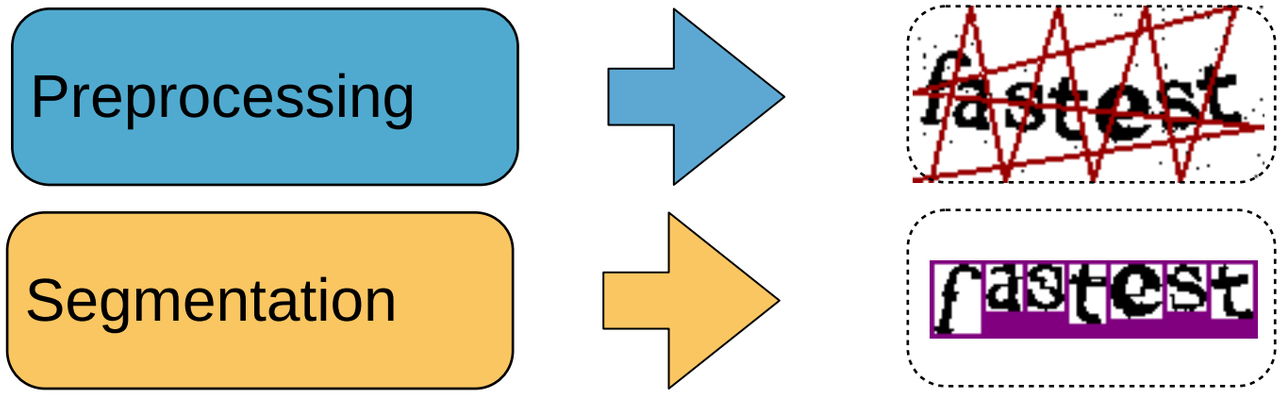
The segment then recognize approach



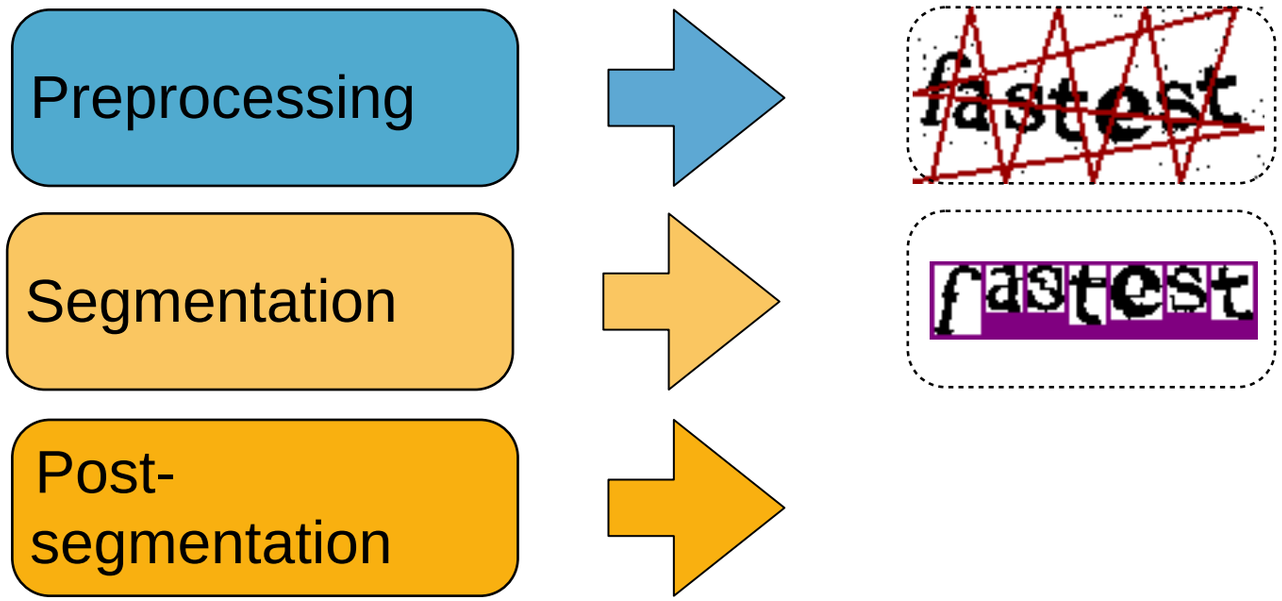
The segment then recognize approach



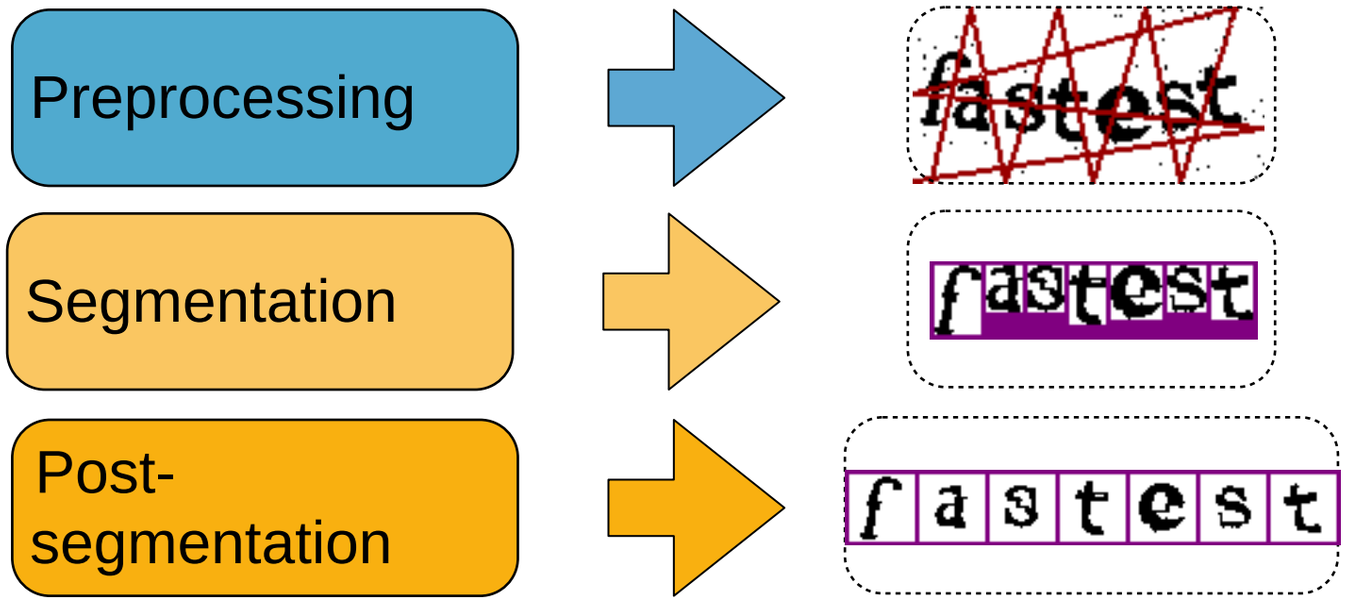
The segment then recognize approach



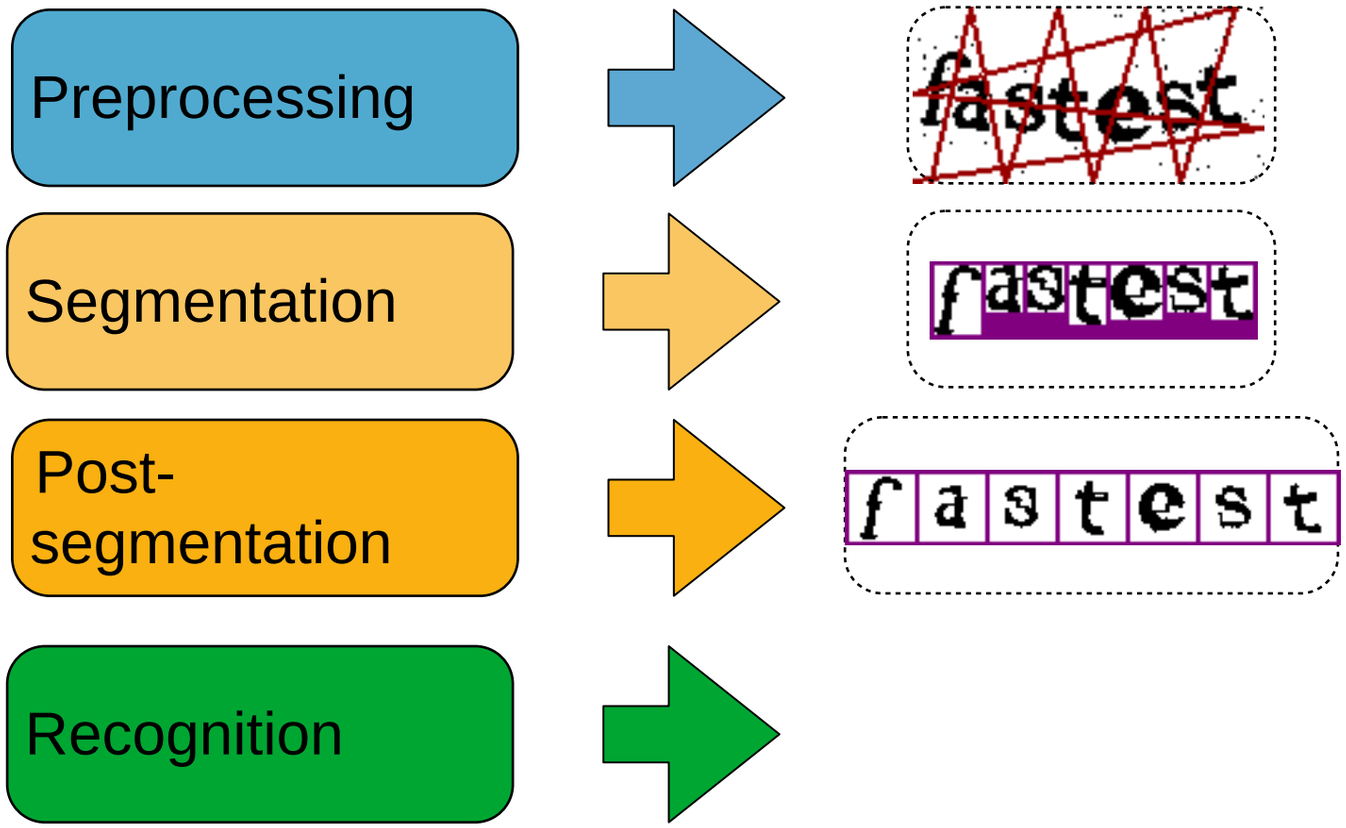
The segment then recognize approach



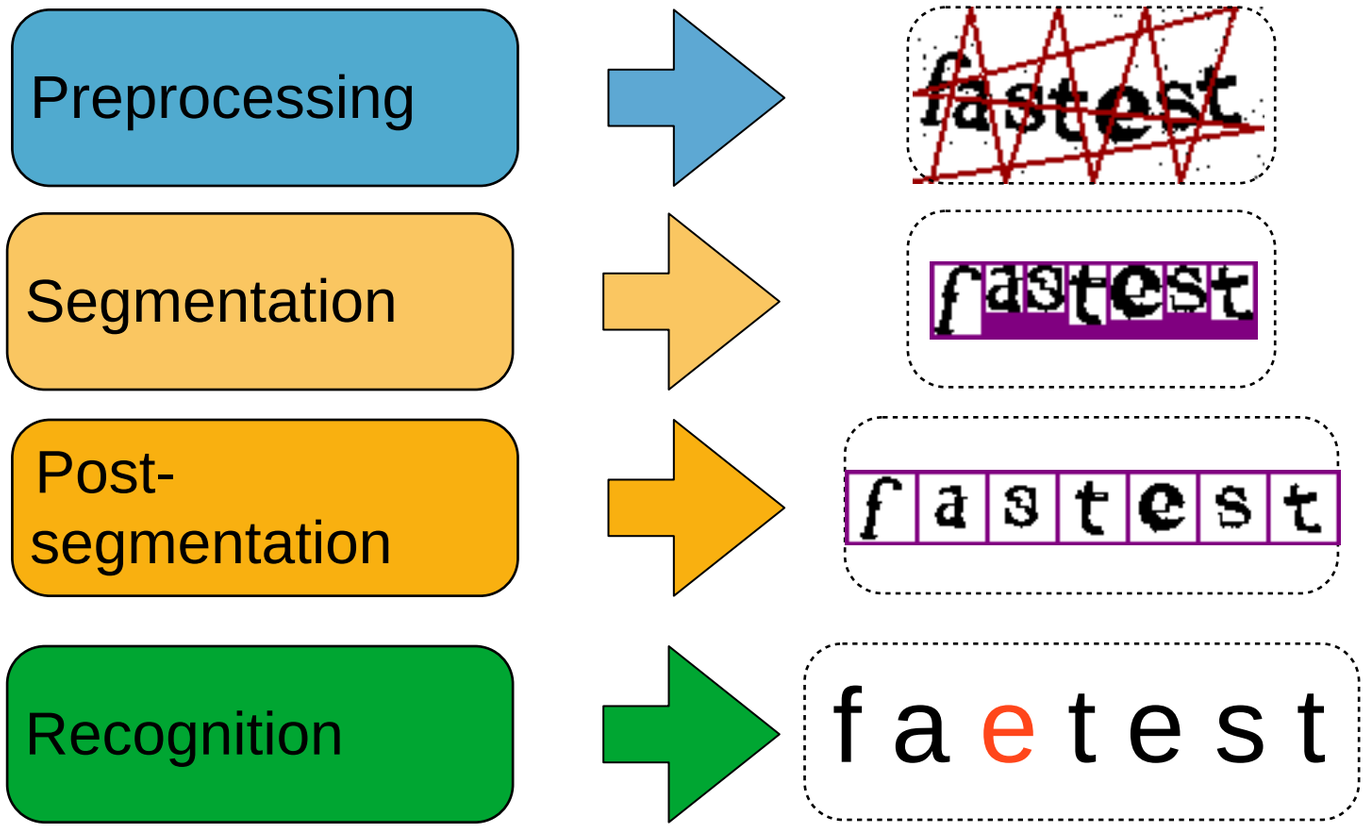
The segment then recognize approach



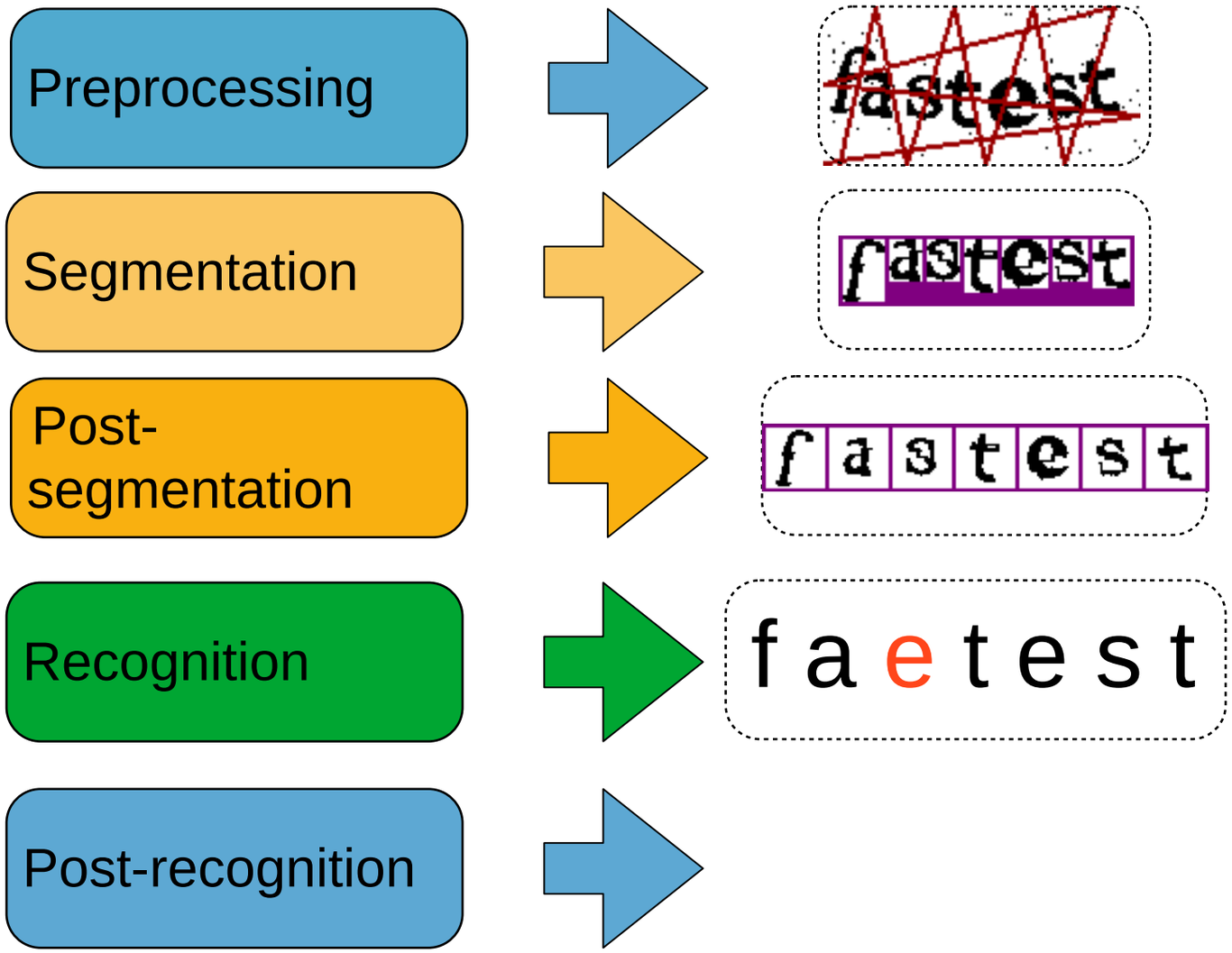
The segment then recognize approach



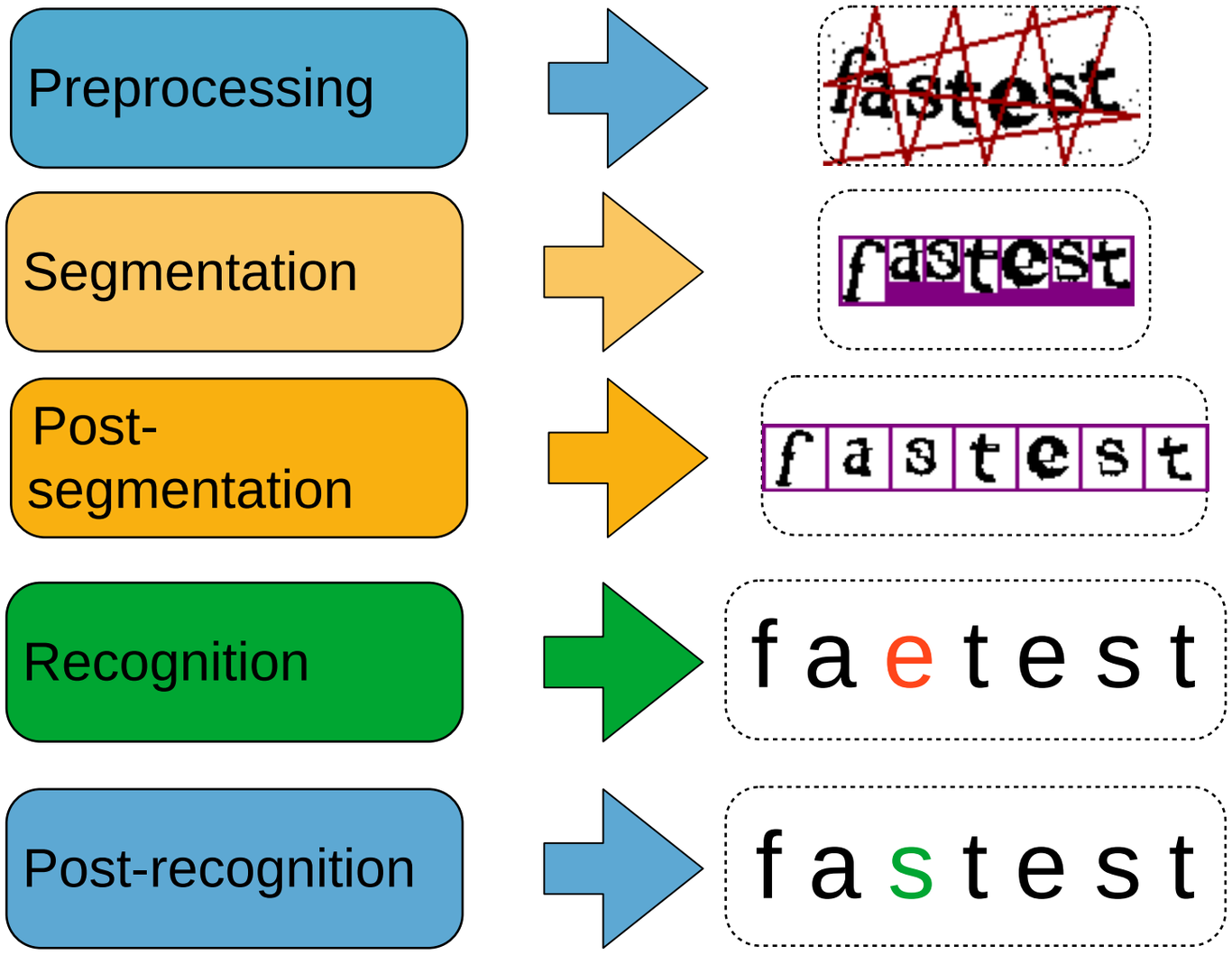
The segment then recognize approach



The segment then recognize approach



The segment then recognize approach



How about collapsing?

Baidu (2011)

Baidu (2013)

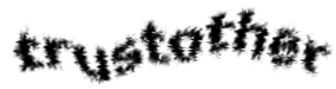
CNN

eBay

ReCaptcha (2011)

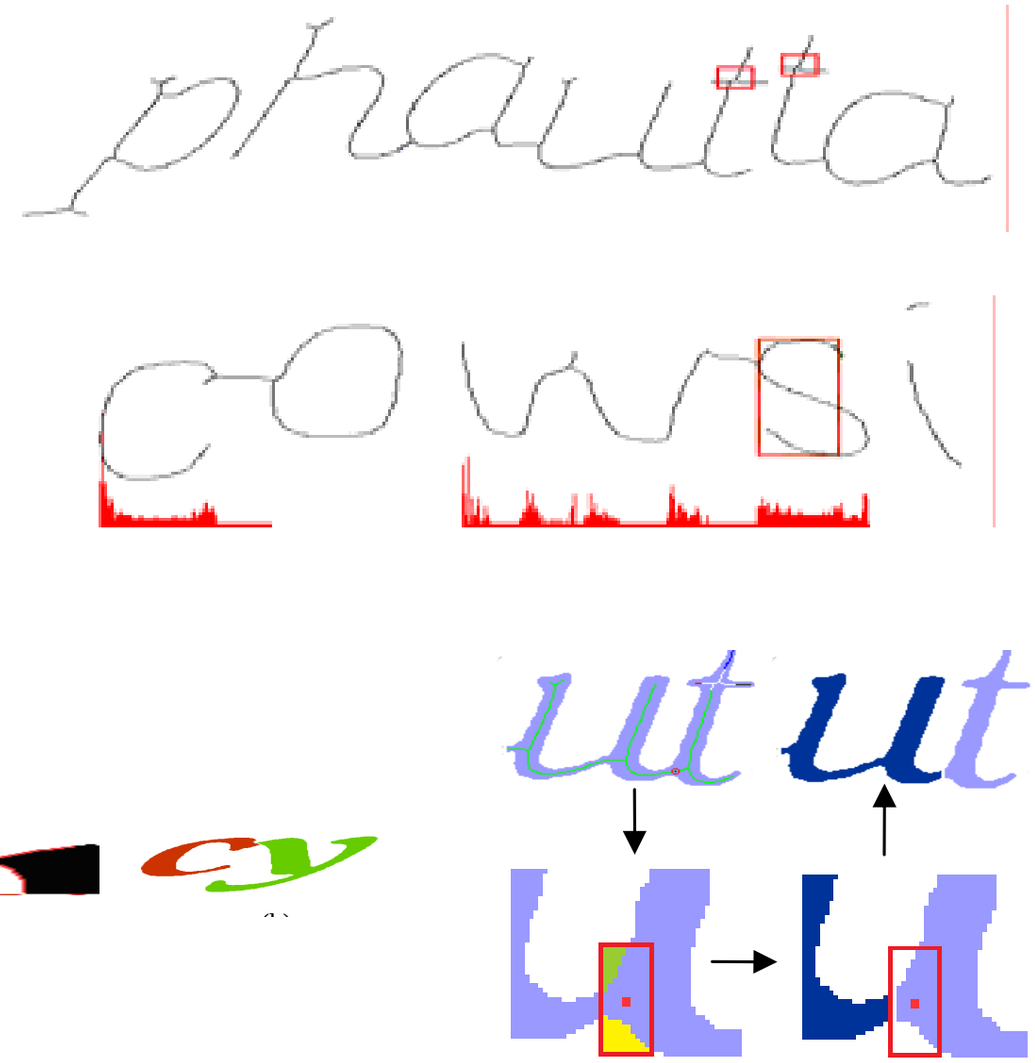
ReCaptcha (2013)

Wikipedia



Yahoo

ad hoc/complicated heuristics



The Robustness of Google CAPTCHAs
Ahmad S El Ahmad, Jeff Yan, Mohamad Tayara

I don’t know how to do it (in the general case)

Captcha breaking reloaded

When AI over-come human limitations

\

What is wrong with the previous approach?

What is wrong with the previous approach?

Segmentation requires to find an invariant to exploit

color, cluster size, number of characters, shape ...

What is wrong with the previous approach?

Segmentation requires to find an invariant to exploit

color, cluster size, number of characters, shape ...

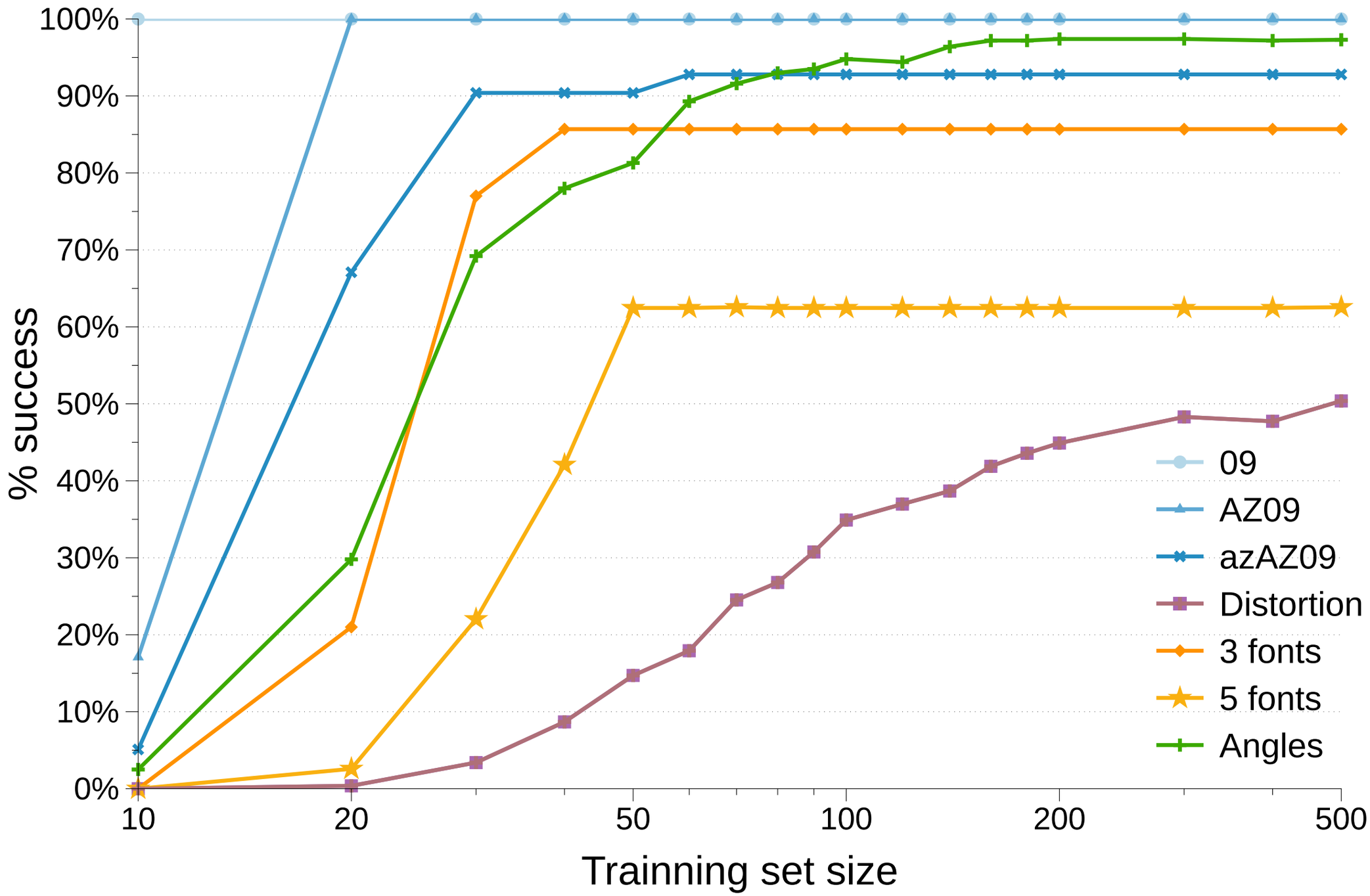
What is wrong with the previous approach?

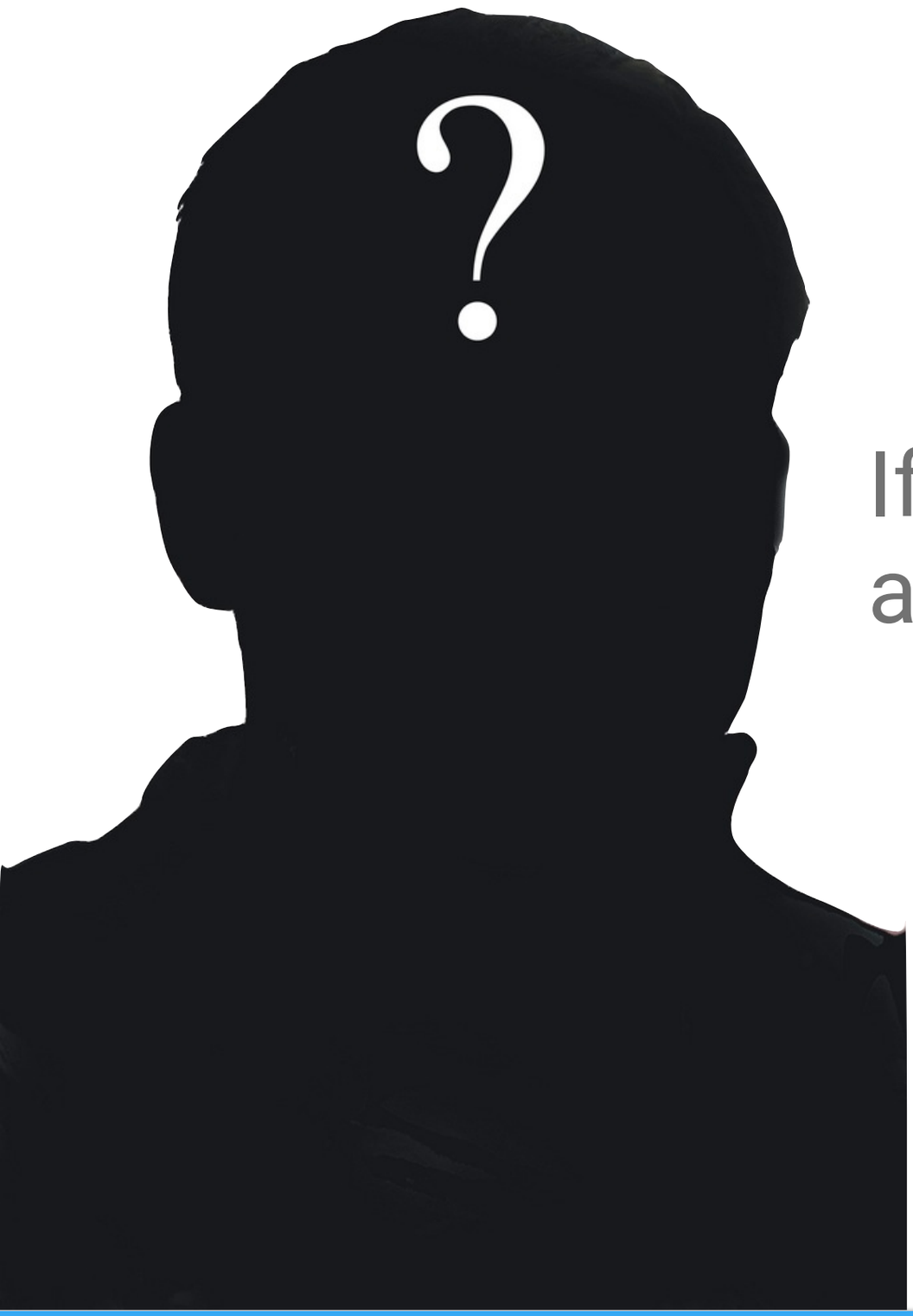
Segmentation requires to find an invariant to exploit

color, cluster size, number of characters, shape ...

Captcha breaking is more exploit writing than machine learning

Classifiers are extremely accuracy (e.g KNN/SVM)





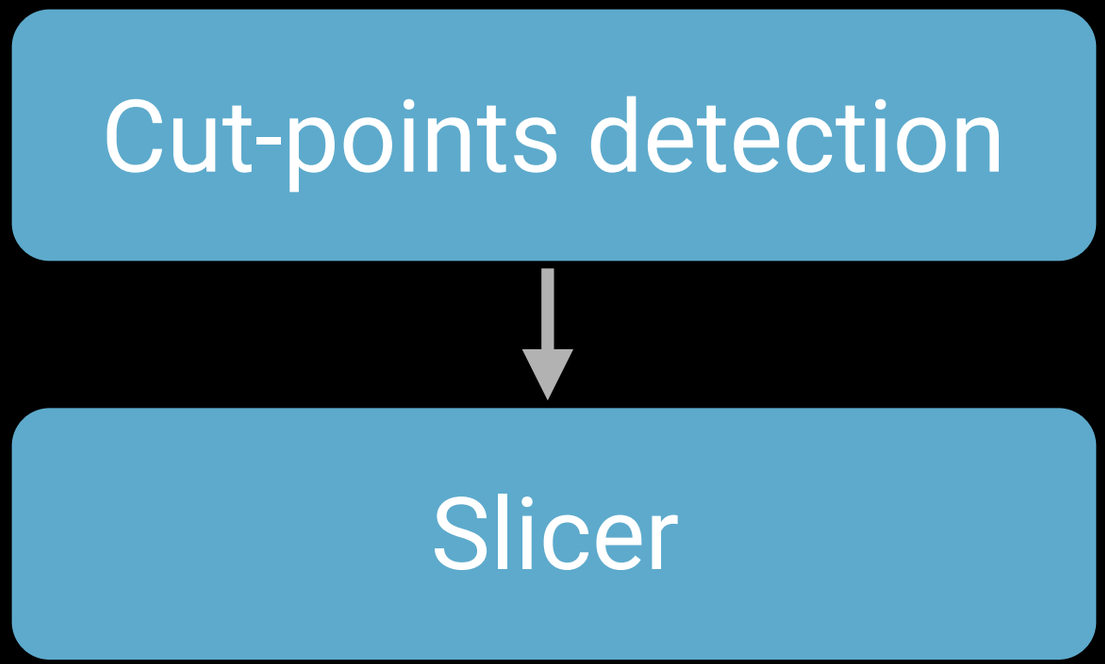
If classifiers are that good, why are we doing pre-processing ?


There is no segmentation

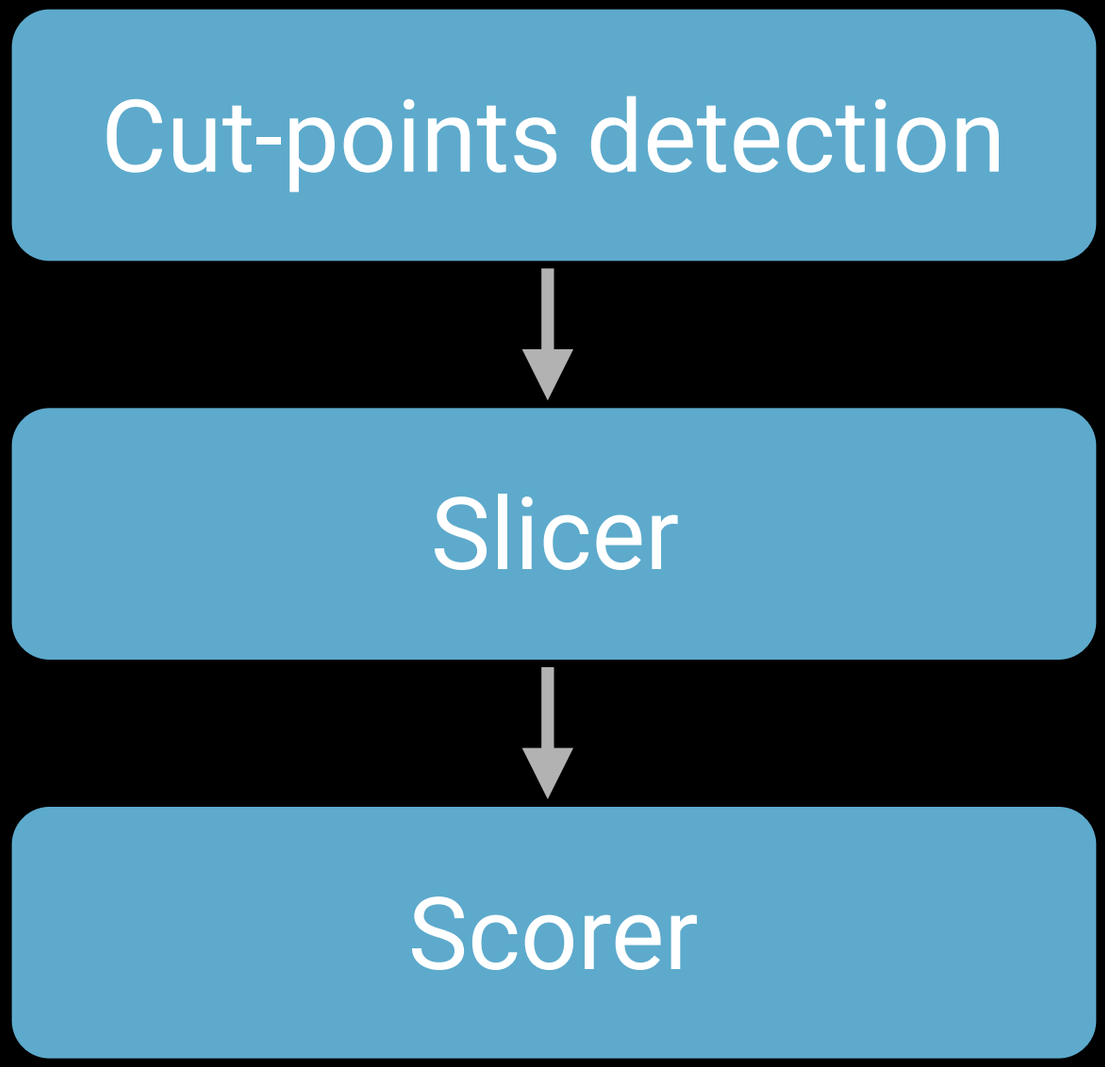
Approach overview

Cut-points detection

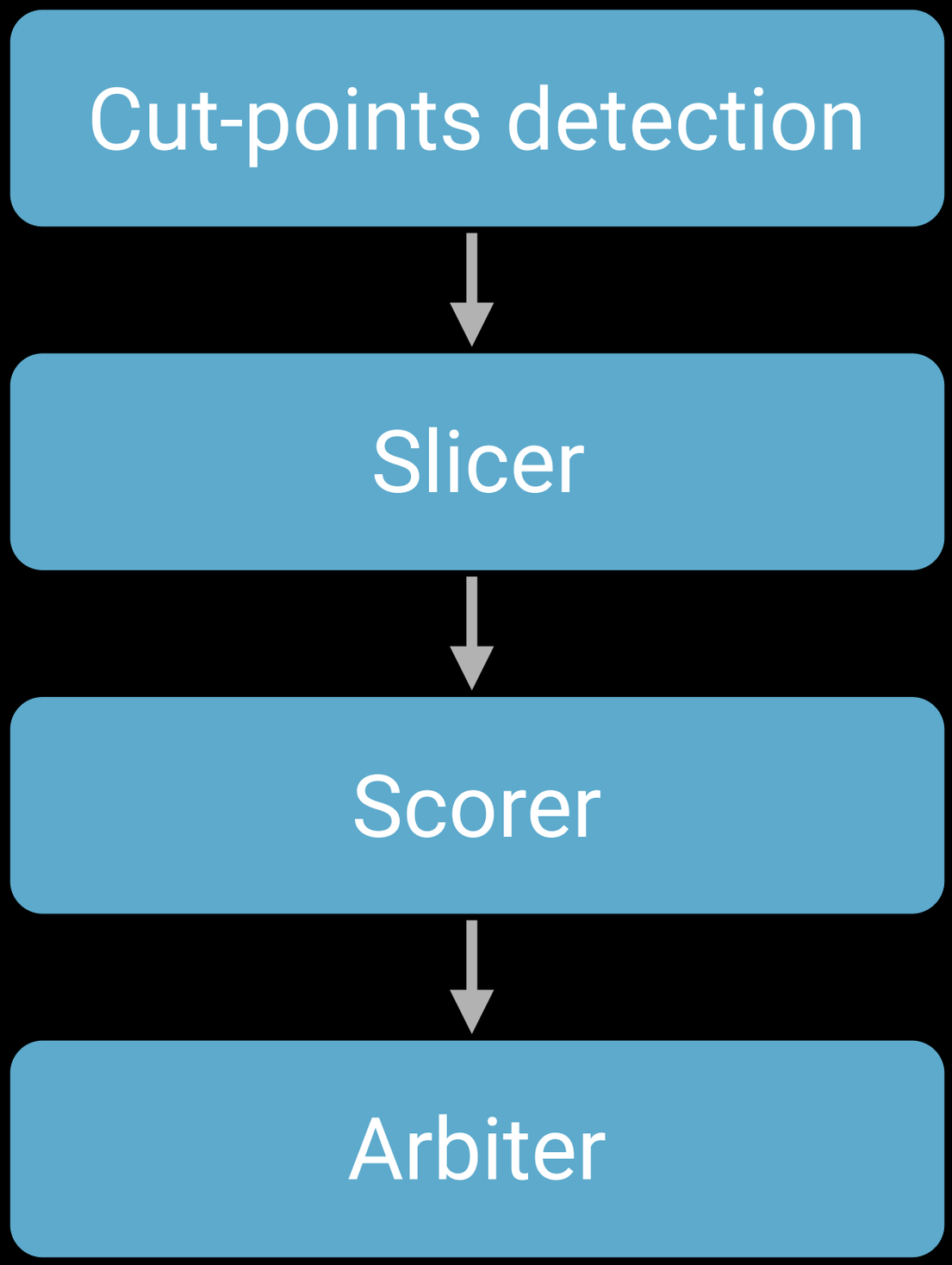
Approach overview



Approach overview



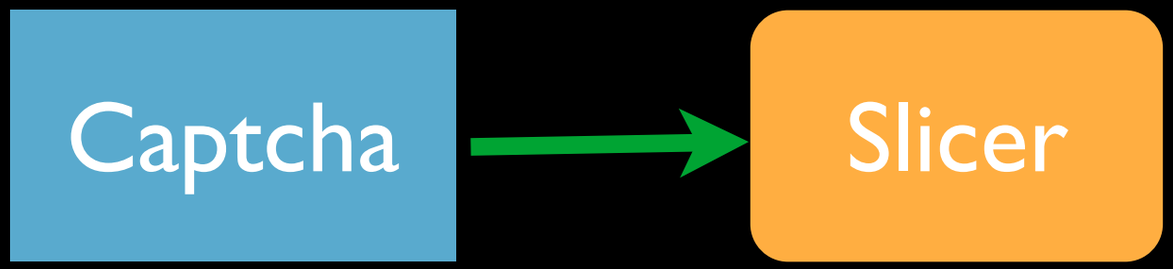
Approach overview



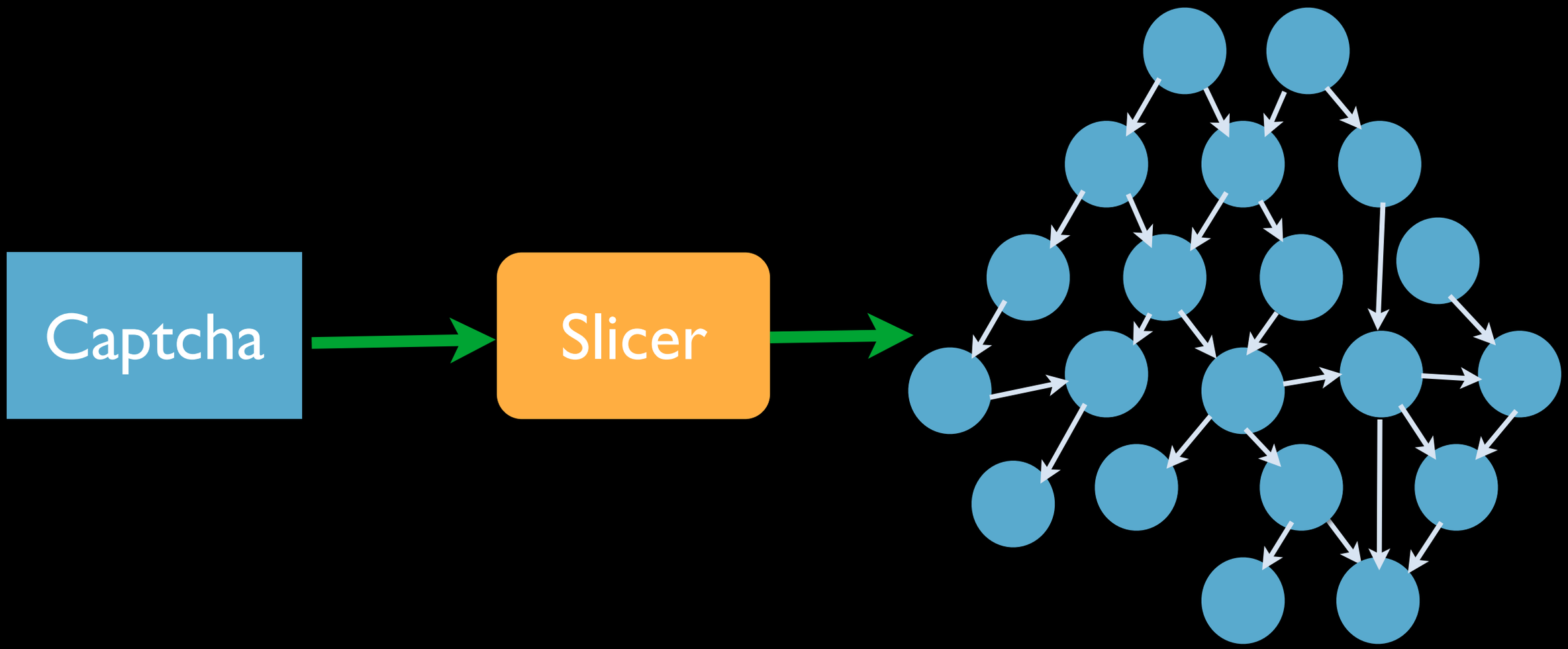
New approach

Captcha

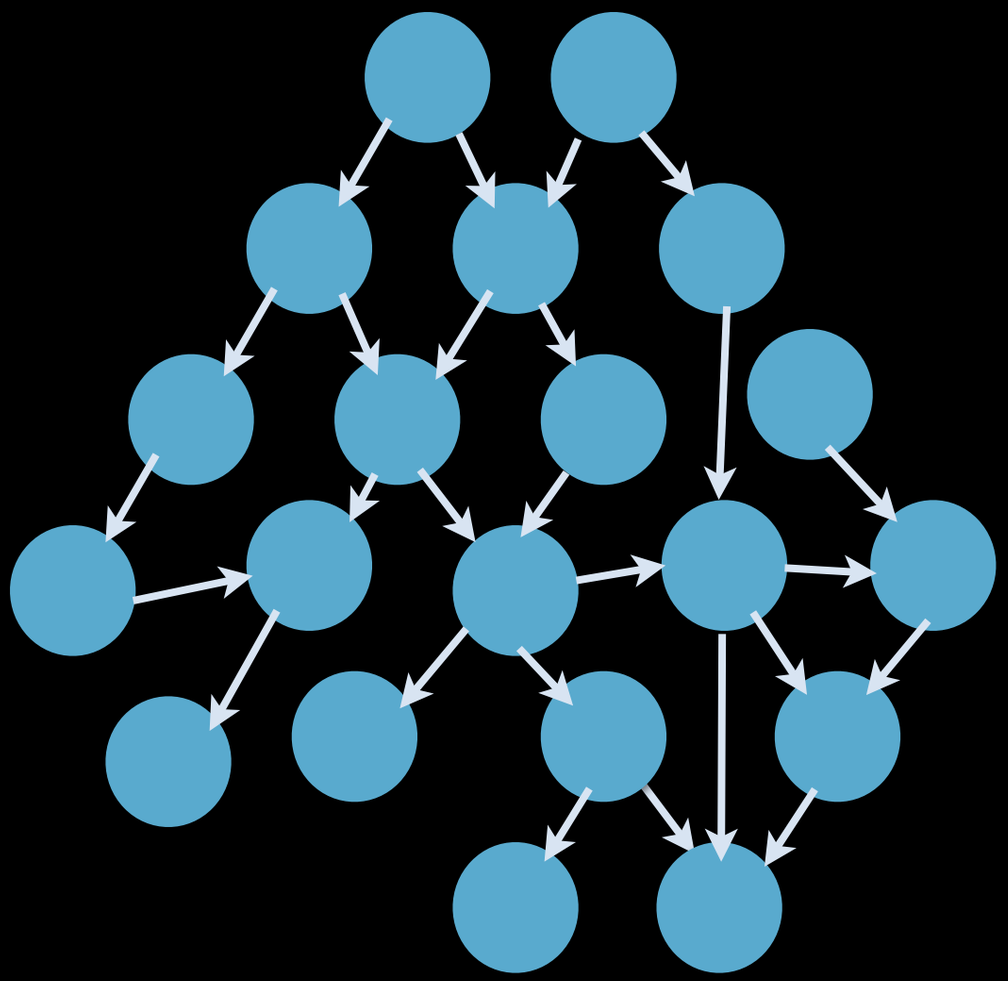
New approach



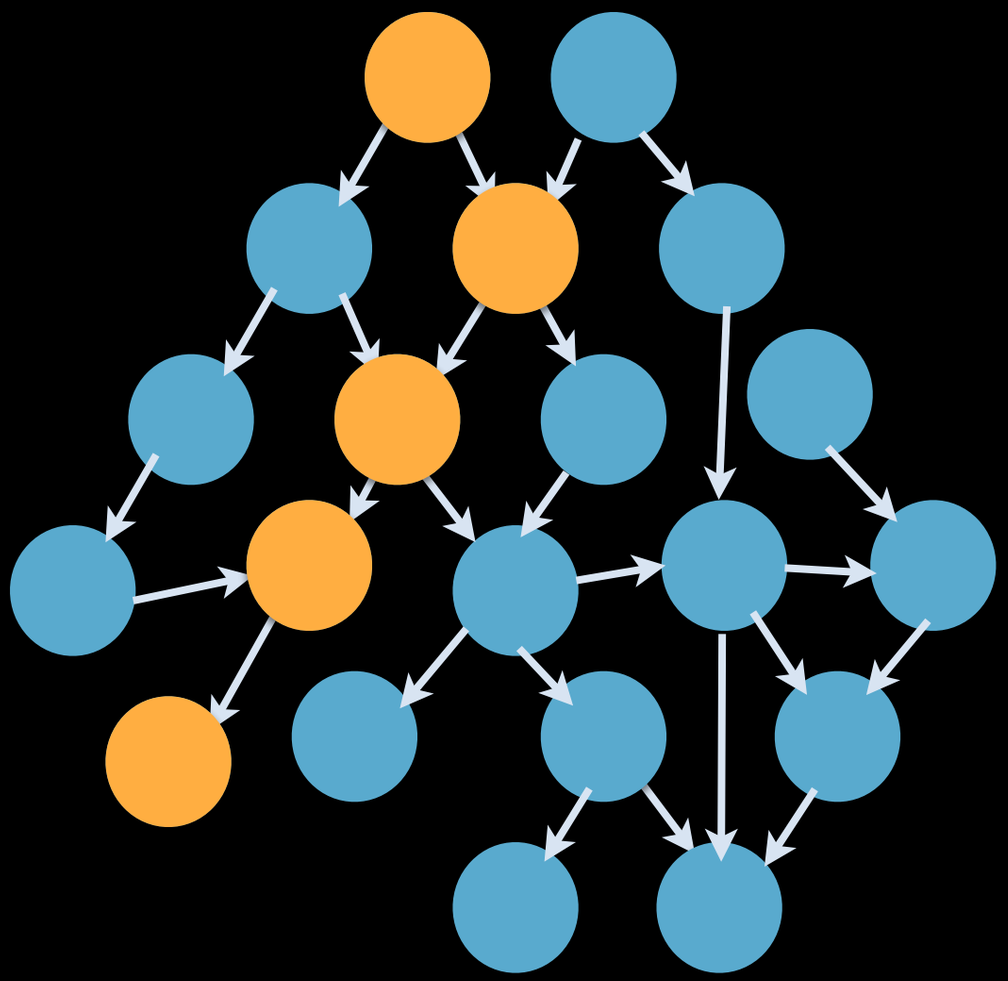
New approach



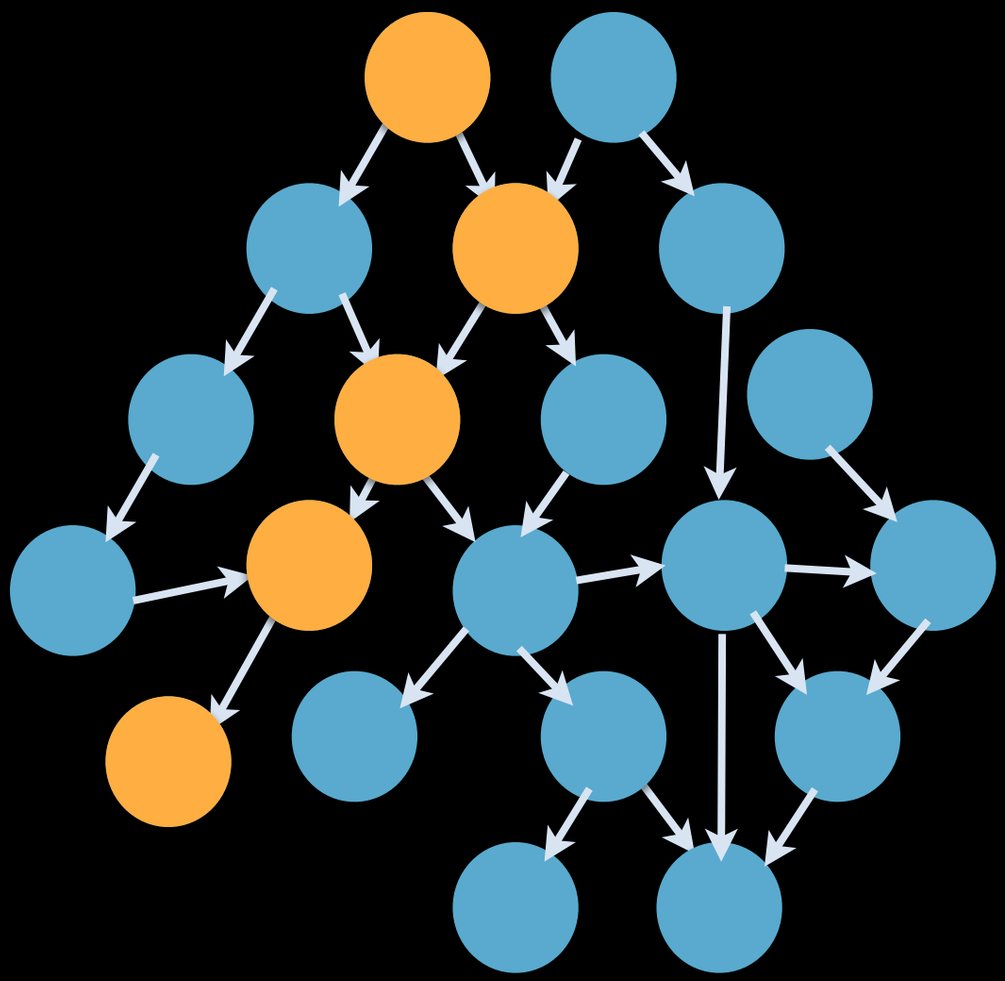
Scorer

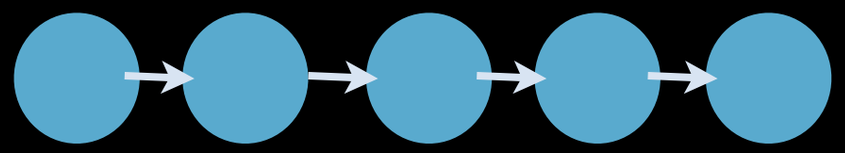


Scorer

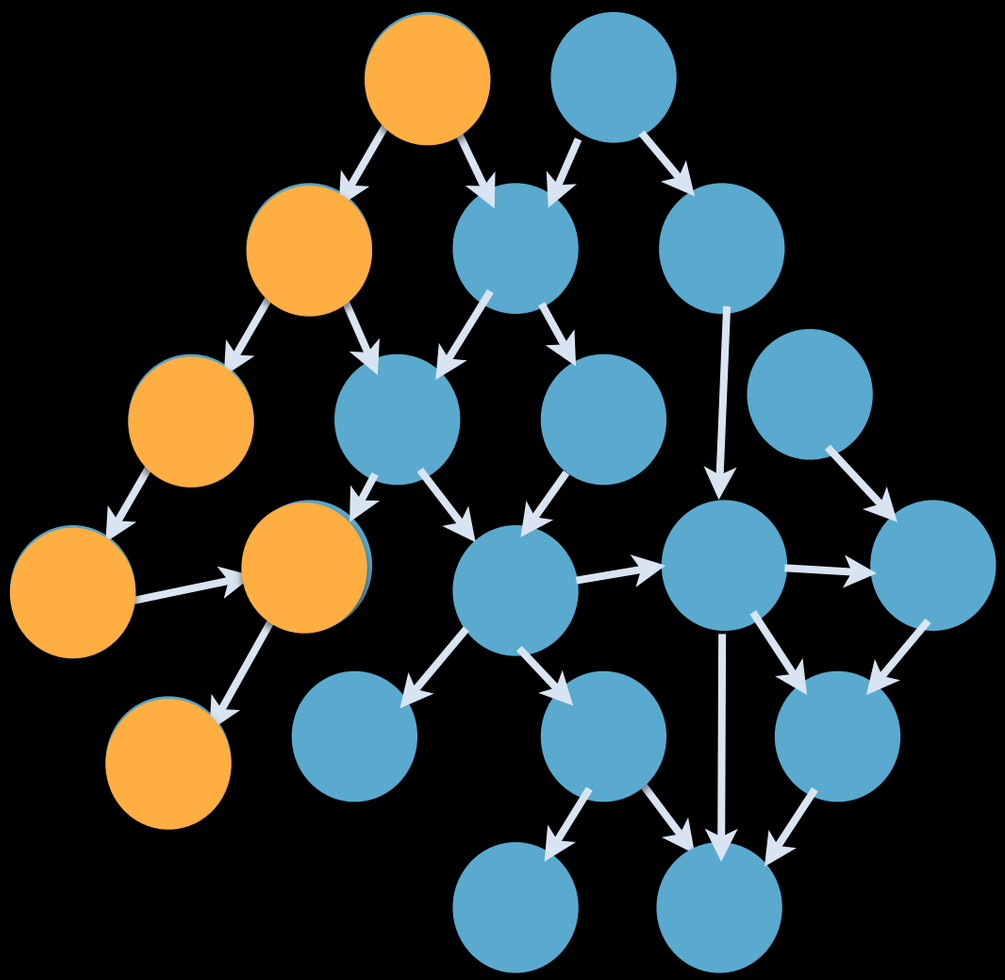


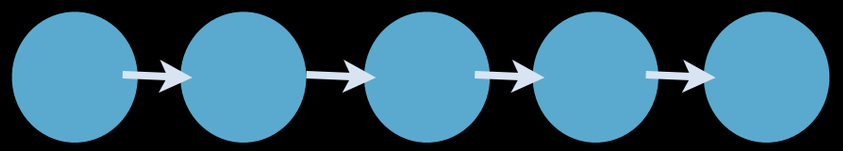
Scorer



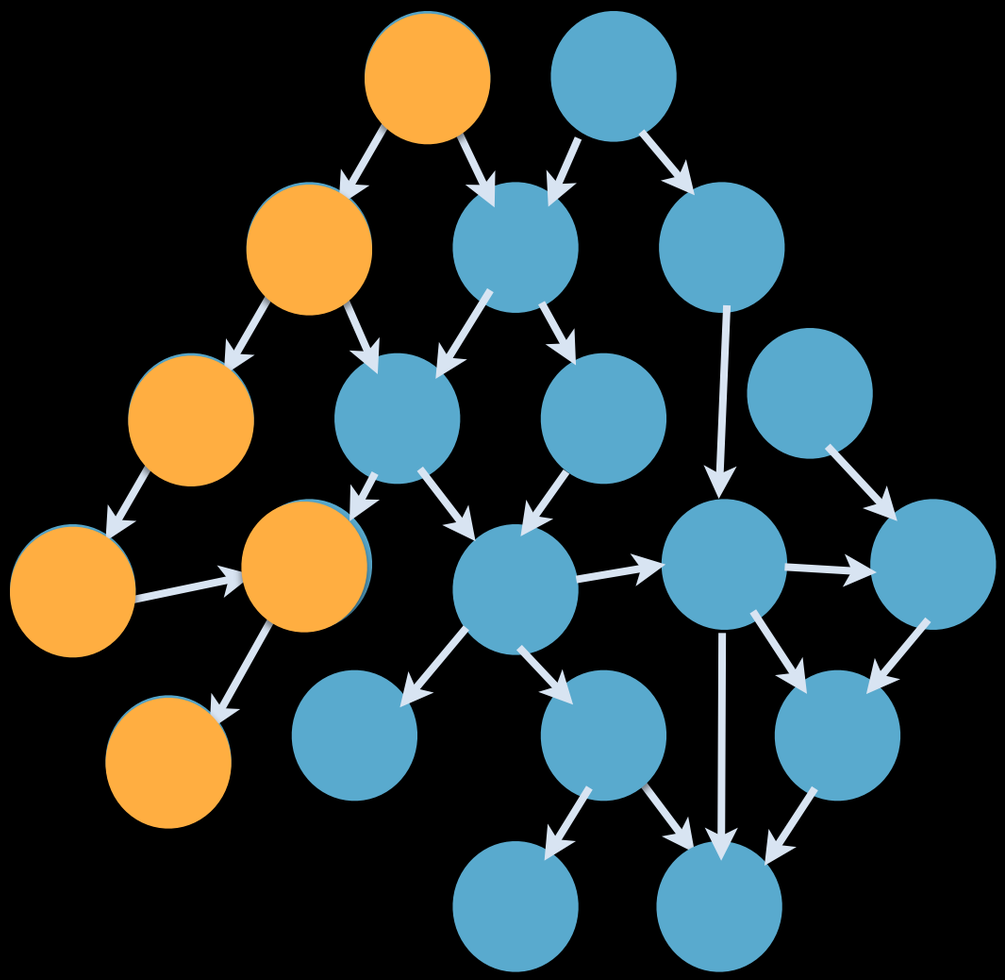


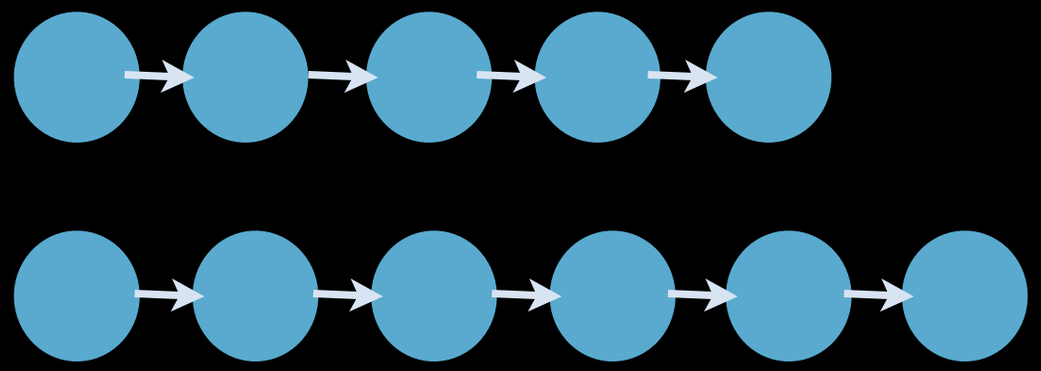
Scorer



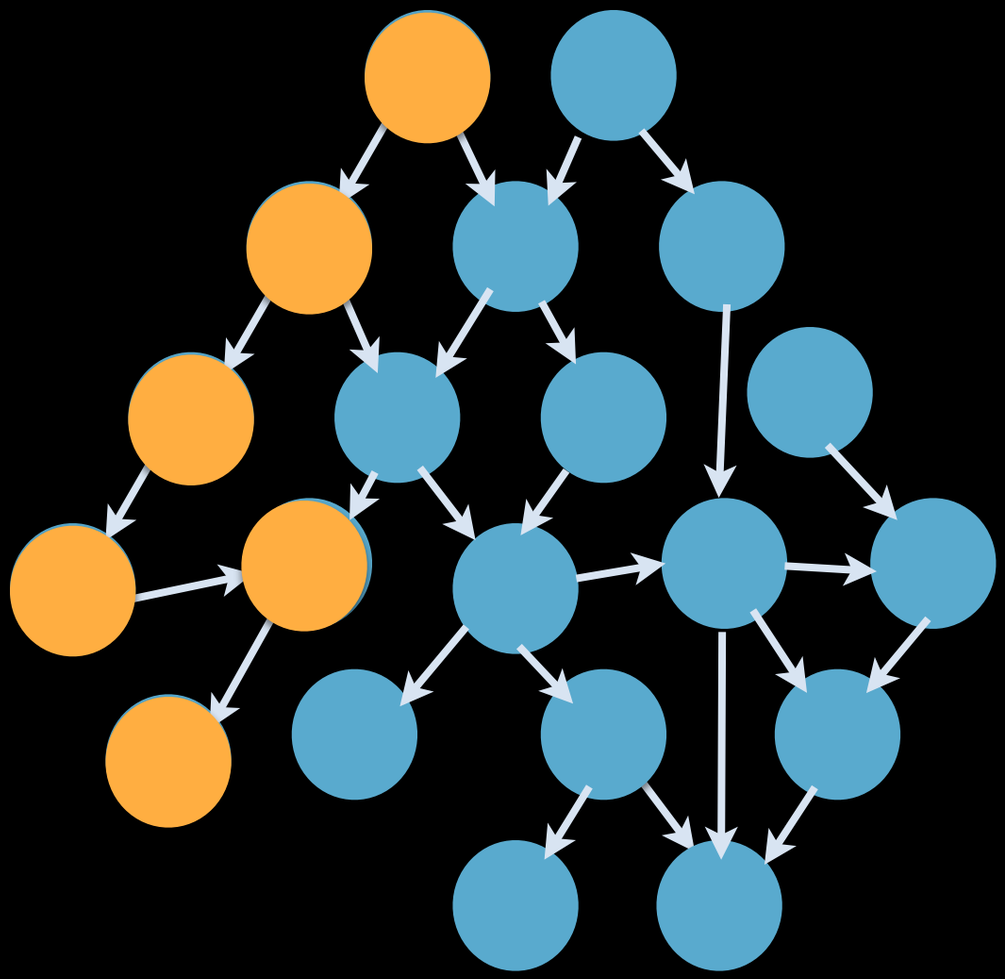


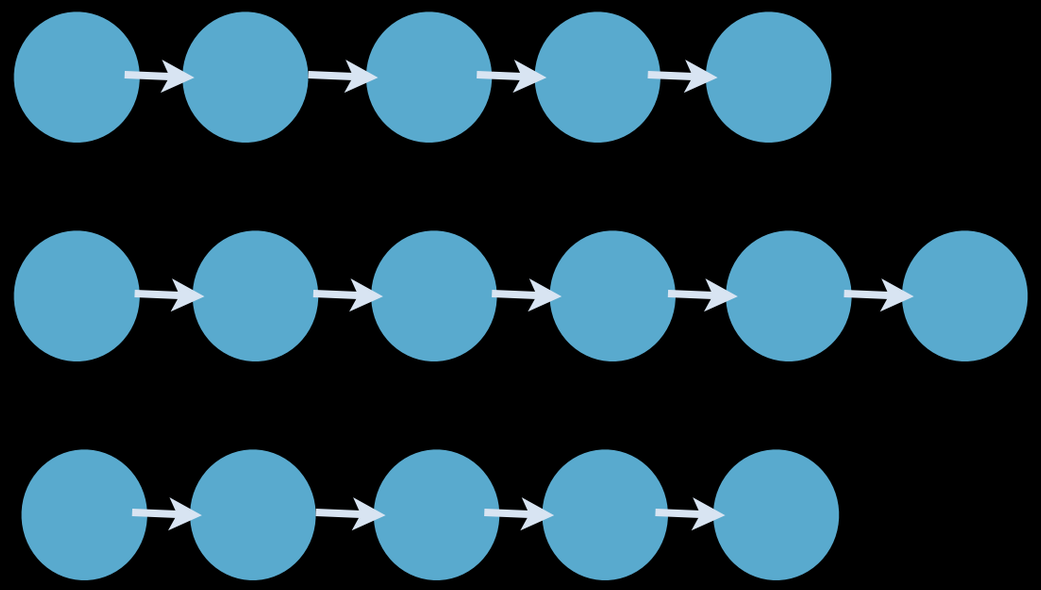
Scorer





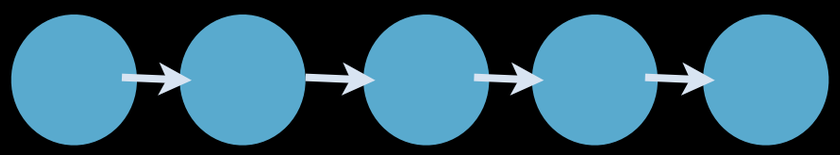
Scorer





Arbiter

Arbiter



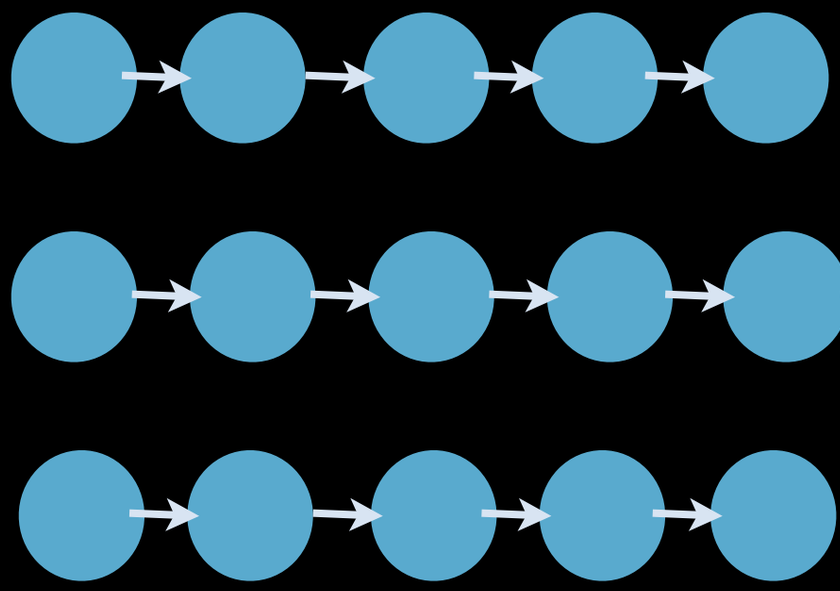
ilebe

Arbiter

ilebe

kinedi

Arbiter

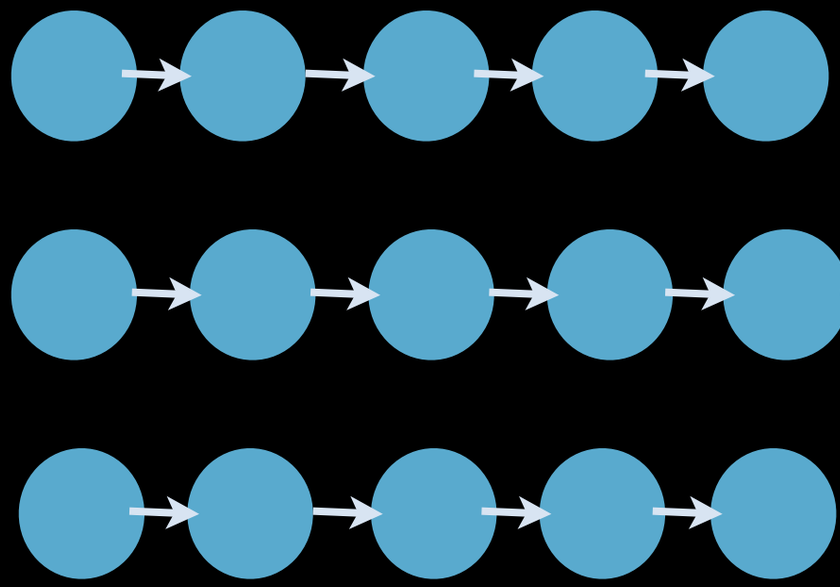


ilebe

kinedi

ilebe

Arbiter



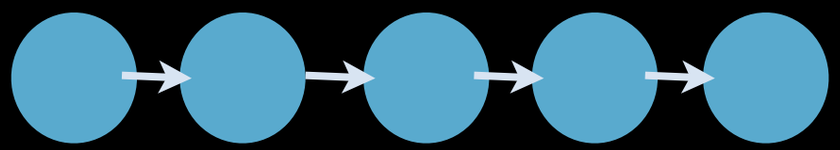
ilebe

kinedi

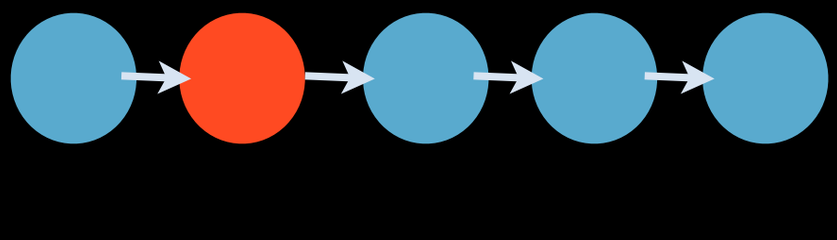
ilebe

ilebe

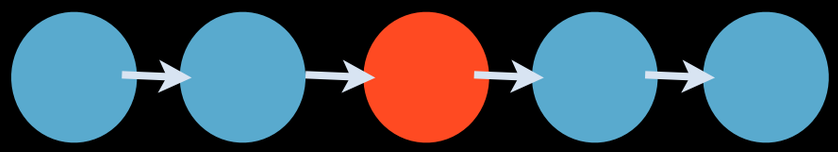
Improving accuracy using reinforcement learning



ilebe

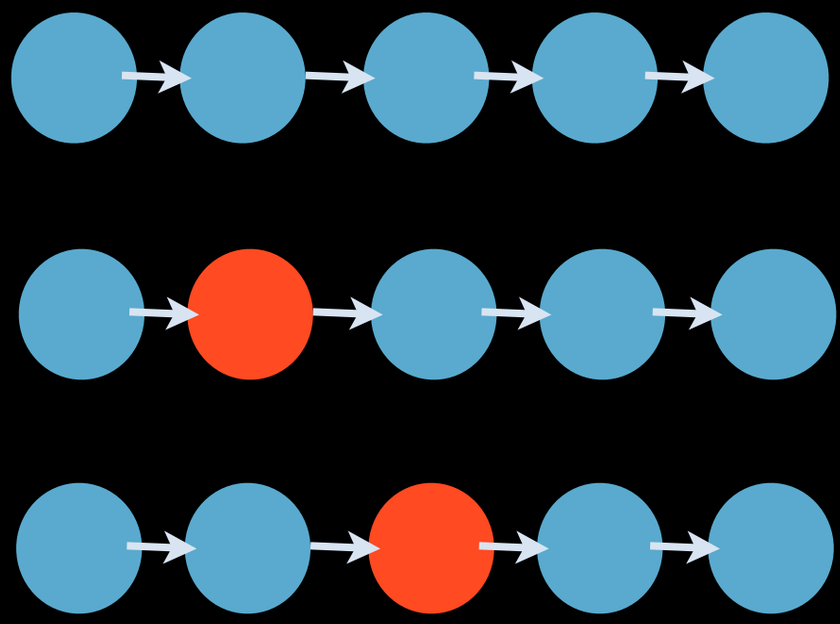


ikebe



ilabe

Improving accuracy using reinforcement learning



ilebe

ikebe

ilabe

The classifier guide the learning process and tell humans when it need help

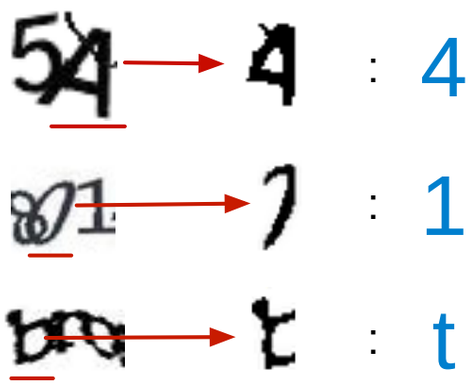
Reinforcement illustrated

A K E

Reinforcement illustrated

A K E

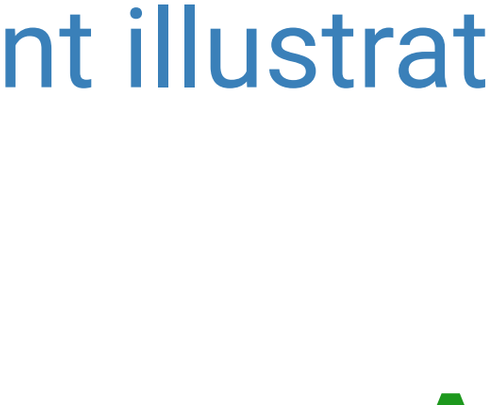
Bad segmentation



Reinforcement illustrated

A K E

Bad segmentation



Bad recognition

Reducing complexity

Algorithm complexity is extremely high

up to 9h on a single captcha

Reducing complexity

Algorithm complexity is extremely high
up to 9h on a single captcha

Solutions

Reducing complexity

Algorithm complexity is extremely high

up to 9h on a single captcha

Solutions

Reduce the number of possible cuts

inflection points, smart elimination

Reducing complexity

Algorithm complexity is extremely high
up to 9h on a single captcha

Solutions

Reduce the number of possible cuts
inflection points, smart elimination

Faster and less accurate recognition sequentia
recognition, left to right

Evaluation on real world captchas

Yahoo

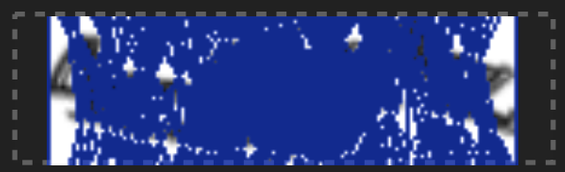
Yahoo

Inflection points

Yahoo

Inflection points

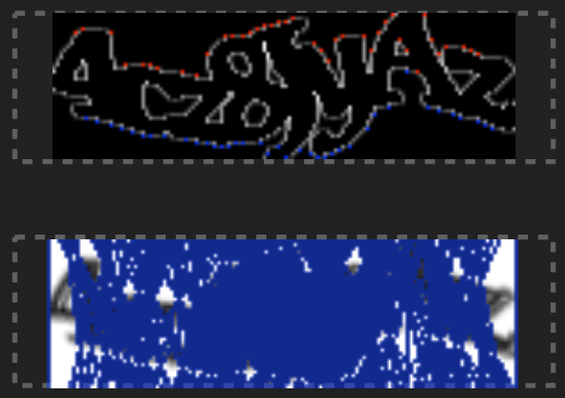
Potential cuts



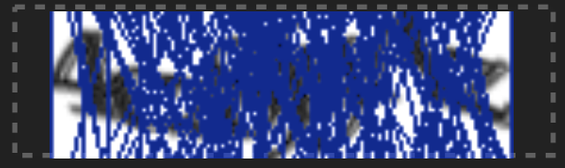
Yahoo

Inflection points

Potential cuts



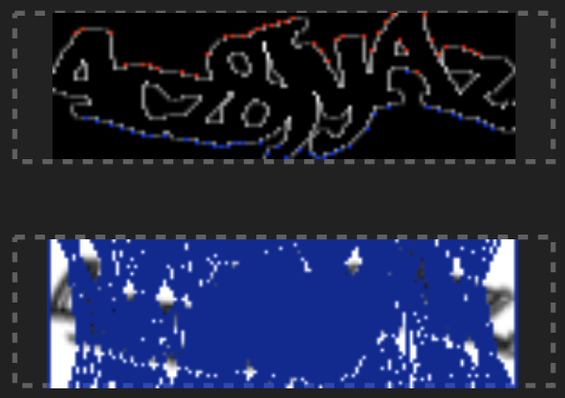
Removing bad cuts



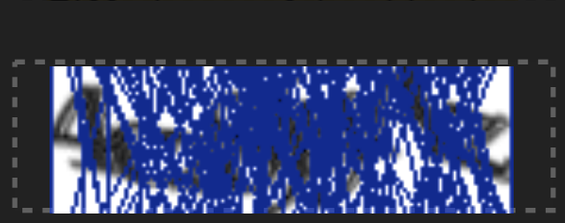
Yahoo

Inflection points

Potential cuts



Removing bad cuts

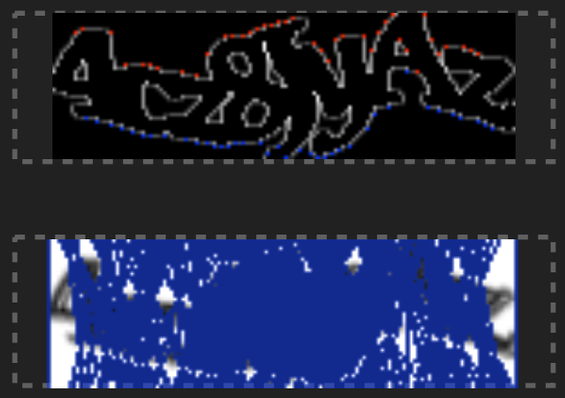


Compatible cuts with start

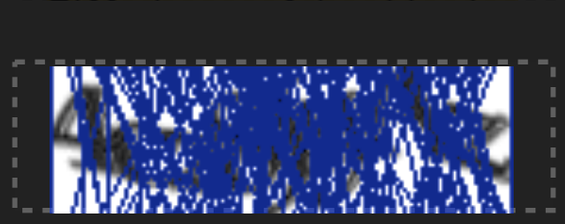
Yahoo

Inflection points

Potential cuts



Removing bad cuts



Compatible cuts with start

Iterative

4cz8jyaz

Recaptcha example

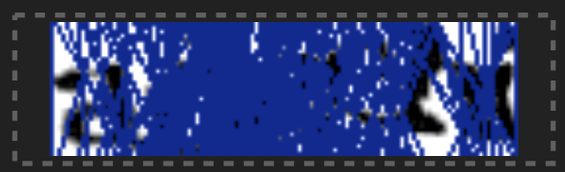
Recaptcha example

Inflection points

Recaptcha example

Inflection points

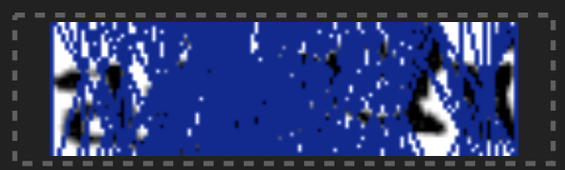
Potential cuts



Recaptcha example

Inflection points

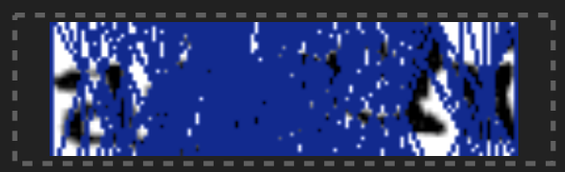
Potential cuts



Recaptcha example

Inflection points

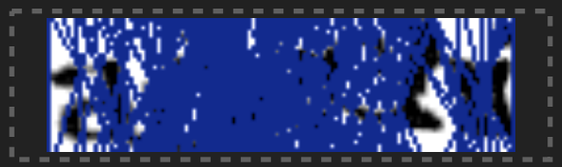
Potential cuts



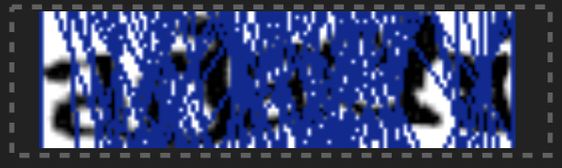
Recaptcha example

Inflection points

Potential cuts



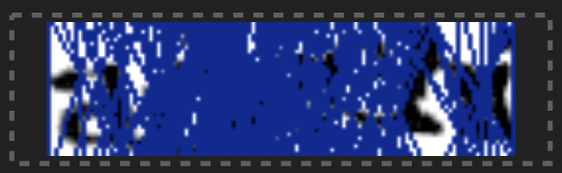
Removing bad cuts



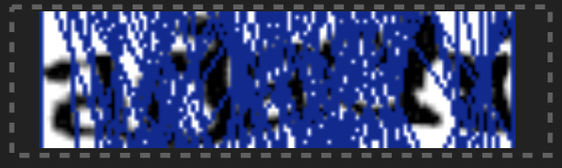
Recaptcha example

Inflection points

Potential cuts



Removing bad cuts

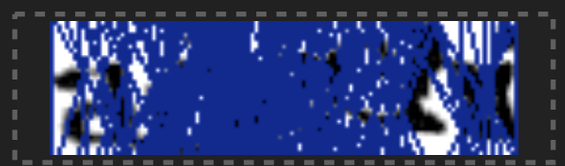


Compatible cuts with start

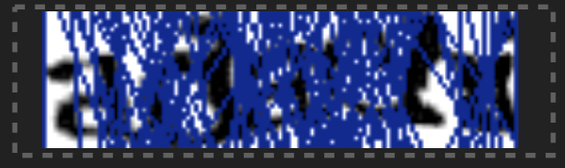
Recaptcha example

Inflection points

Potential cuts



Removing bad cuts



Compatible cuts with start

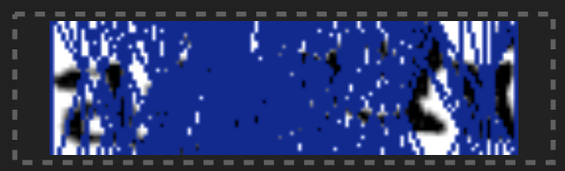
Iterative

adaclv

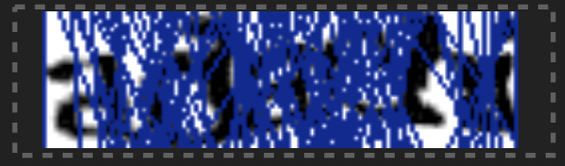
Recaptcha example

Inflection points

Potential cuts



Removing bad cuts

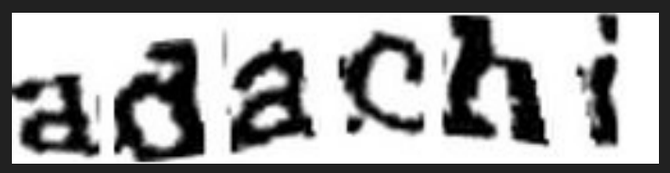


Compatible cuts with start

Iterative

adaclv

full graph



adachi

How about lines ?

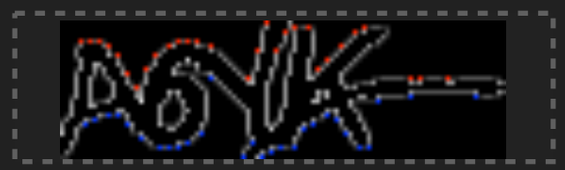
Realize that lines are known shape

Train classifier to recognize them as empty character

Baidu example

Baidu example

Inflection points



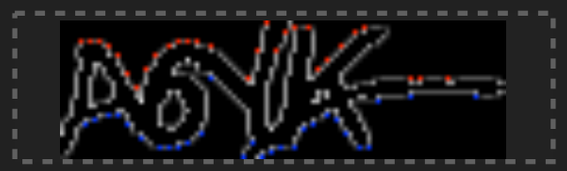
Baidu example

Inflection points

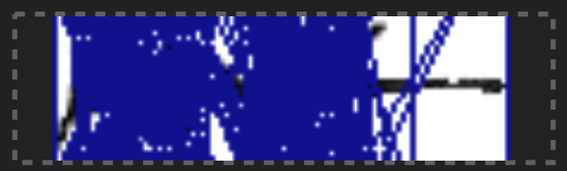
Potential cuts

Baidu example

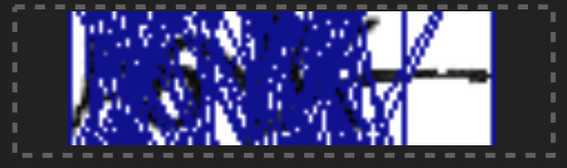
Inflection points



Potential cuts



Removing bad cuts

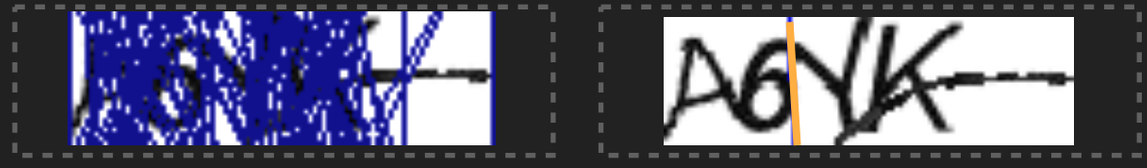


Baidu example

Inflection points

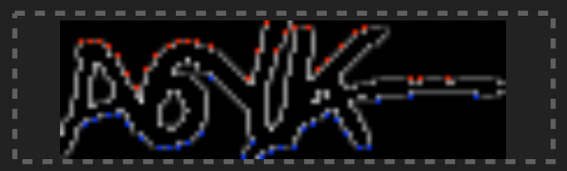
Potential cuts

Removing bad cuts

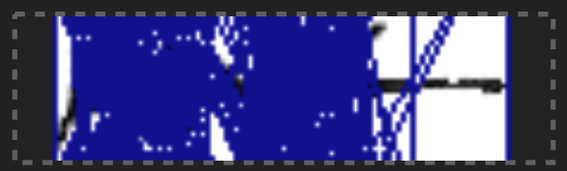


Baidu example

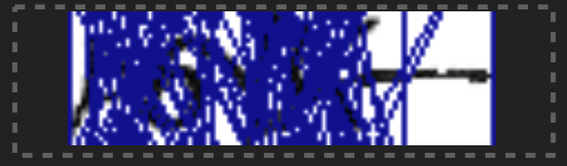
Inflection points



Potential cuts



Removing bad cuts



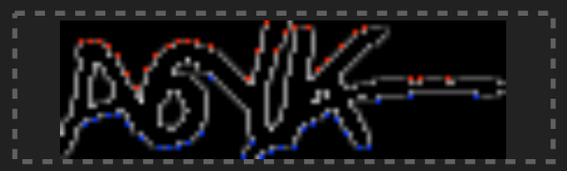
Baidu example

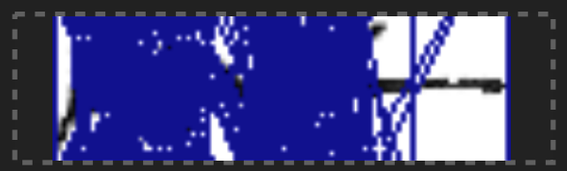
Inflection points

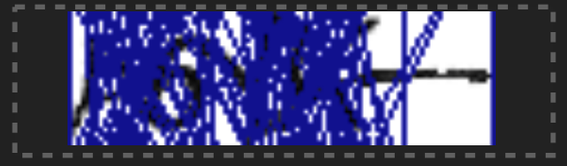
Potential cuts

Removing bad cuts

Compatible cuts with start

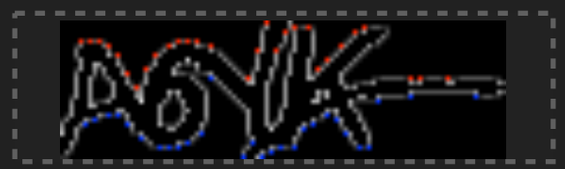




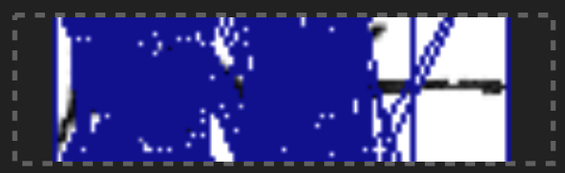


Baidu example

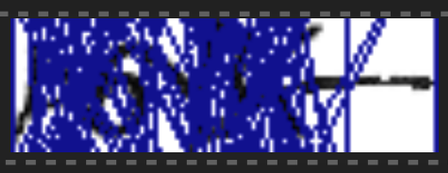
Inflection points



Potential cuts



Removing bad cuts



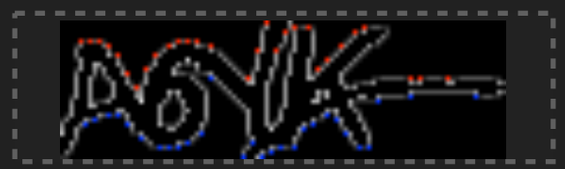
Compatible cuts with start

Iterative

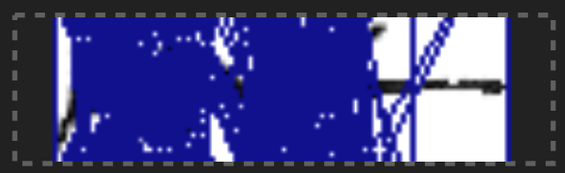
a6yk--

Baidu example

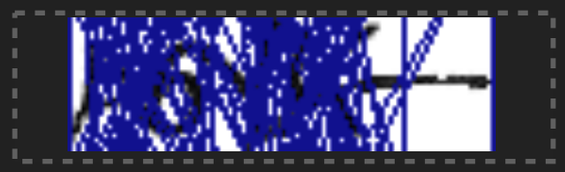
Inflection points



Potential cuts



Removing bad cuts



Compatible cuts with start

Iterative

a6yk--

full graph

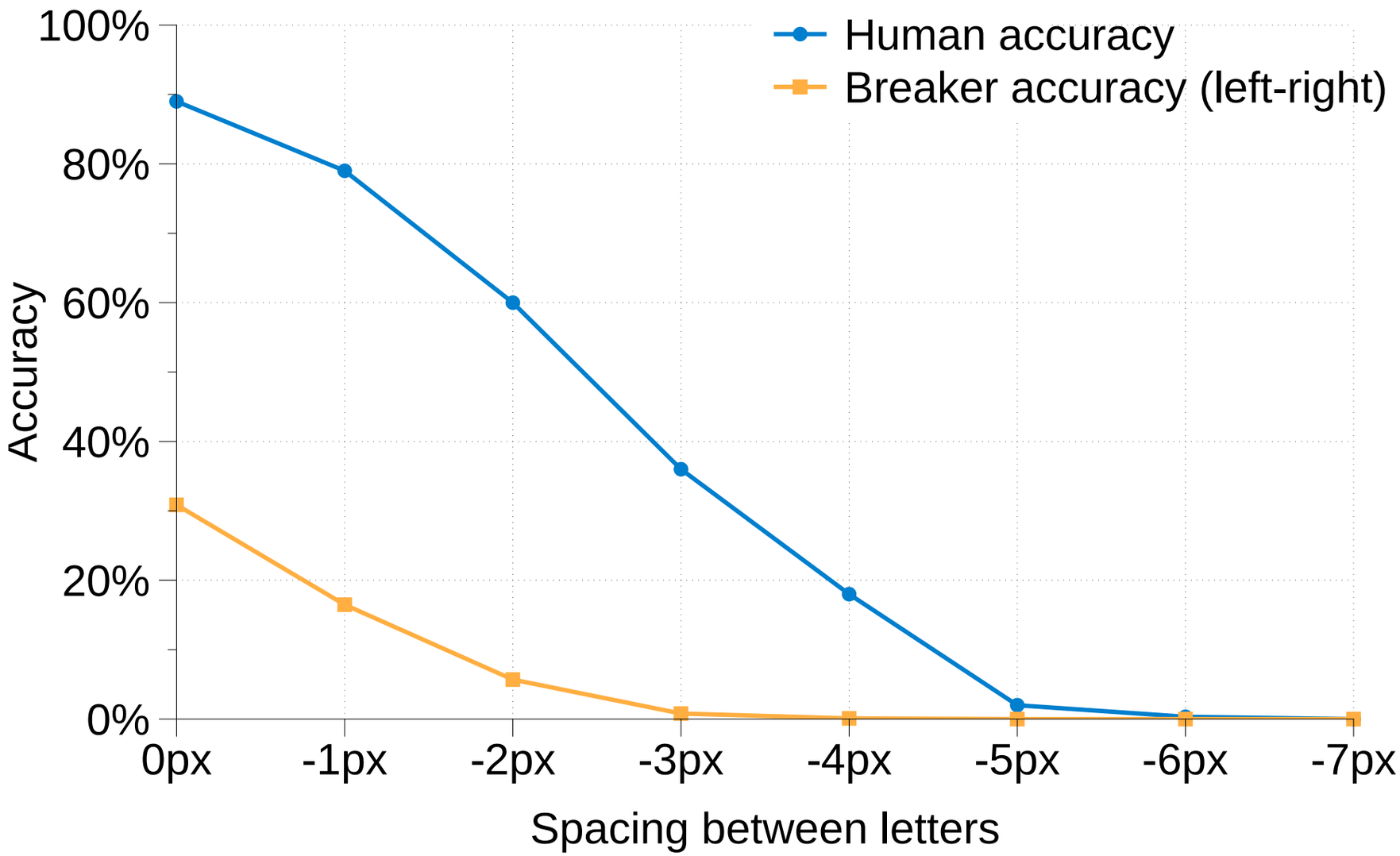
a6yk--

Overall results

	Reinforcement learning				Simple learning			Previous Work		
	Full	L-R	L-R Time	Seq.	Full	L-R	Seq	Accuracy	Delta	Ref.
Baidu (2011)	38.68%	33.42%	3.94 s	36.58%	17.27%	16.55%	16.69%	5%	+33.6%	[10]
Baidu (2013)	55.22%	54.38%	1.9 s	54.38%	-	-	-	51%	+4.22%	[21]
CNN	-	51.09%	4.9 s	48.54%	-	46.40%	45.96%	16%	+35.09%	[10]
eBay	51.39%	47.92%	2.31 s	48.61%	39.43%	40.14%	36.29%	43%	+11.4%	[10]
ReCaptcha (2011)	22.67%	21.74%	7.16 s	19.25%	19.86%	18.25%	17.10%	40.4%	-17.73%	[15]
ReCaptcha (2013)	22.34%	19.22%	4.59 s	19.74%	20%	14.61%	12.77%			
Wikipedia	-	28.29%	-	26.36%	-	27.02%	26.24%	25%	+3.3%	[10]
Yahoo	-	3.67%	7.95 s	5.33%	-	2.72%	2.29%			

Generic approach: Succeed where the old approach fail and most often beat it where it worked

Human vs computers



The gap between Human and computer recognition is now too narrow to be considered secure

The end of an era, the dawn of a new one

Summary

Deprecated

Segment and Recognize attacks

Text distortions defense

New generation

Purely based AI Attack

Risk analysis defense

Questions ?

Captcha research
https://www.elie.net/tag/captcha

Follow-me on Twitter
@elie