

A Solver-resistant Challenge Response Spam Protection System

Or simply a 3D CAPTCHA

Alexander Pyattaev,
Tampere University of Technology
Vladimir Sadovnikov,
Saint-Petersburg State University of
Telecommunications

Agenda

- 1 Problem specification
- 2 Current solutions and their problems
- 3 Proposed method
- 4 Implementation details
- 5 Future work

1.1 Sword vs Shield

- Spam bots have only one goal – post spam
- Spam messages mean money for spammers
- Admins and users do not like spam
 - So they try to block it
 - Without blocking other content...
- Problem is – it does not quite work
- In a fight between sword and shield sword wins
 - So let us exploit the talent of spammers...

1.2 Turing test 2.0

- When Turing formulated his idea of the test, it was text based, machine was supposed to chat with human. Problem is – they broke it.
- Some smart guy made the first CAPTCHA:



- Unfortunately, it worked well only for a while...
 - Yet it boosted progress in OCR considerably

1.3 Threat assessment

- A good CAPTCHA has to meet some criteria:
 - Not solvable by computers
 - Not crackable by brute force (10^{-6} probability of correct guess)
 - Not annoying for users
 - Not crackable by professional solvers
 - That guys from developing countries... they do miracles
 - They can generate dictionaries of solutions for picture-select based tests, for example
 - Portable and suitable for mobile devices

2.2 What does not work?







- There are few common approaches to CAPTCHA design:



- semantic questions (made by humans)
 - Pre-rendered video or audio
- All of them share common problems:
 - Limited dictionary of semantics
 - Computers are a lot better in noise filtering

2.3 Why it does not work?

- Any CAPTCHA works in 3 steps
 - Create an answer
 - Perform a transformation of it (add noise)
 - Ask human to revert transformation
- Let's see how it works:

Characters under typical distortions	Recognition rate
	~100%
	96+%
	100%
	98%
	~100%
	95+%

Not so nice,
probably...

3.1 Breaking stereotype?

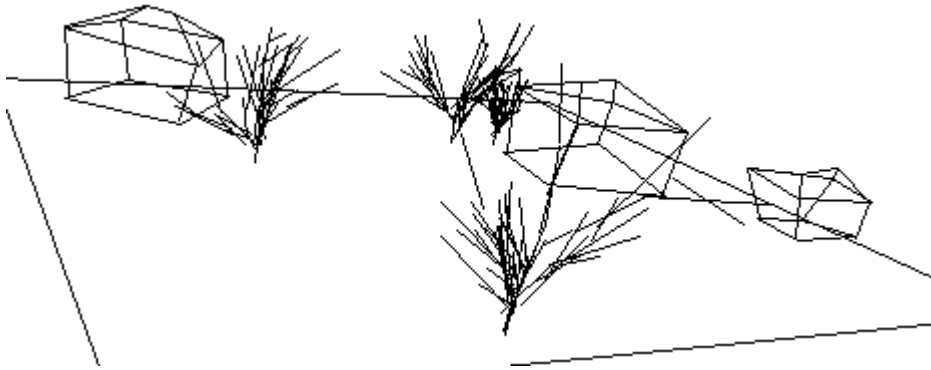
- Pick a **transform** that **can not be reverted** by machine
- Make the solver **spend more time** but **less effort** (fight slave labor, user-friendliness)
- Make delivery system **standards-compliant**
- Generate challenges **automatically** to fight dictionary attacks
 - **So in fact we are not breaking anything**

3.2 Our solution

- Transform: 3D scene to 2D perspective projection of it
- Time constrains: Top and bottom constrains, animation as delivery system
- Delivery: HTML5 + Java script
- Generation: Fully automated generation of scenes that have target object and noise objects. Target has to be located.

3.3 Action

- This is how it looks like:



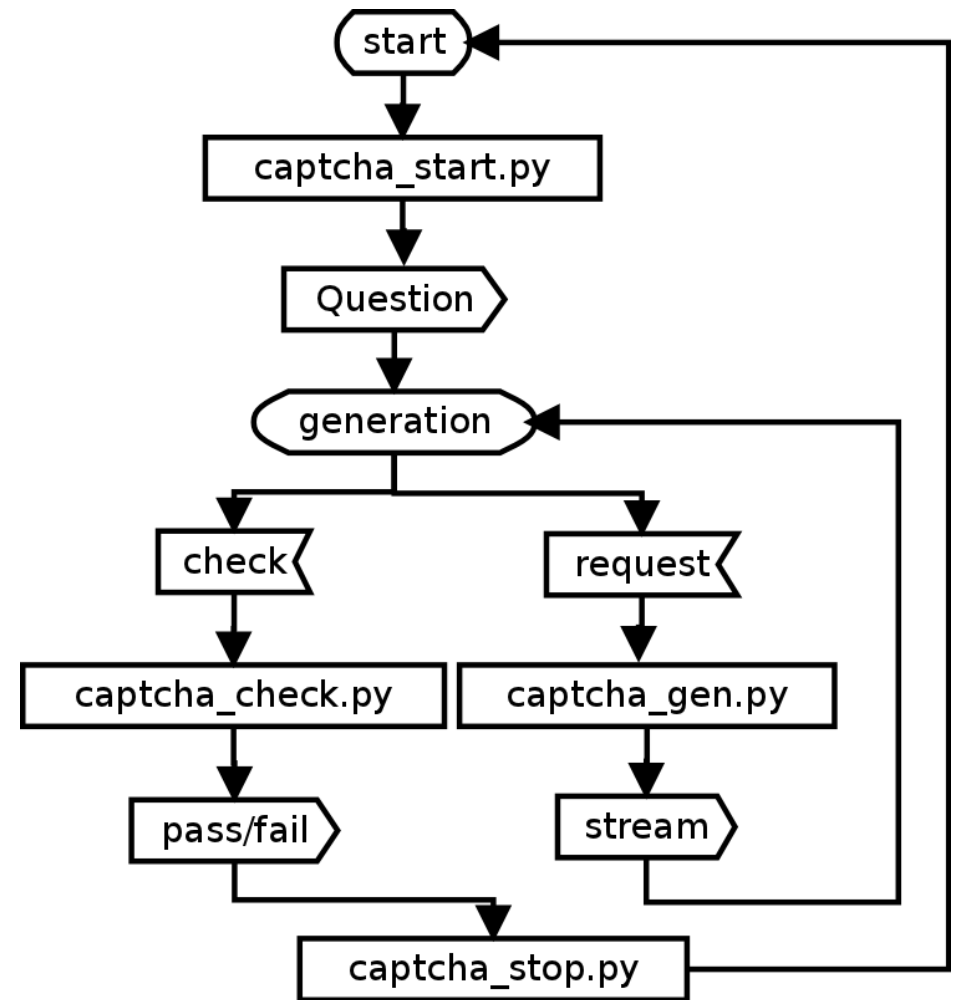
- It has trees and houses as base objects
 - More could be added easily
 - Trees are fractals (hard to match pattern → more fractals are good)

4.1 Implementation - client

- HTML5 canvas
 - Rendering
 - Downloading the video stream
 - Decompression
 - Playback
 - User input
 - Mouse click as the only input
 - Total compatibility with touchscreen devices
- AJAX
 - Interactivity in near real-time

4.2 Implementation - server

- Some python magic
- Primitive state machine that can use files or DB as state storage
- Driven by requests from user
- Critical functions implemented in C



5.1 First prototype

- The first prototype is just a proof-of-concept
- The whole project is 3 weeks old.
- It might be not really suitable for deployment
 - We may have missed something
 - It could be more user-friendly
 - Proper testing on embedded is needed

5.2 Working prototype

- Has to be better documented
- Has to work reliably
- The generated picture could look nicer
- Someone should actually try to break it to see how far they can get
 - Even if it gets broken we get a nice algorithm for analysis of video streams that can reconstruct 3D structure and rotation information...

Thank you for your attention.

- FAQ:
 - Yes we like monochrome things
 - Yes it might not be a best idea
 - Your proposals are welcome
 - Email to alexander.pyattaev@tut.fi
 - You can download the source from <http://shimlar.tontut.fi/captcha>
 - Yes it might not compile
 - You are welcome to the demo session to see more