Security and Usability Challenges of Moving-Object CAPTCHAs

Decoding Codewords in Motion

Yi Xu, Gerardo Reynaga, Sonia Chiasson, Jan-Michael Frahm, Fabian Monrose and Paul Van Oorschot

THE UNIVERSITY of NORTH CAROLINA at CHAPEL HILL

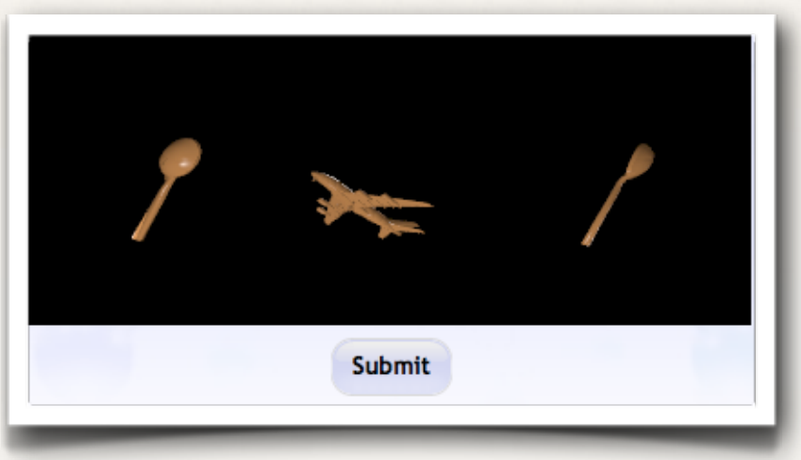
Carleton UNIVERSITY

CAPTCHAs

- Application of Turing Test to computer security
  - **C**ompletely **A**utomated **P**ublic **T**uring test to tell **C**omputers and **H**umans **A**part (**CAPTCHA**)
    - Sometimes called a Reverse Turing Test or Human Interactive Proof
- CAPTCHAs come in many flavors (text, audio, cognitive, 2D and 3D image, and now motion-based)

Applications

- Free email account registration
- Prevent automated guessing attacks
- Prevent mining of pseudo-public files
- Prevent abuse in online voting polls
- Restrict access in online social networks, multiplayer games, etc
- Many more ...



Moving-Image Object Recognition (**MIOR**) CAPTCHAs

Moving-Image Object Recognition (**MIOR**) CAPTCHAs

- Advantage
  - Ease of use 
- Security risks
  - Provides attacker multiple views of the target 
  - Temporal information can be used to enhance attacks
  - Relies on cognitive tasks based on object recognition, instead of object classification

Our Goals

- Assess the security and usability of this new class of CAPTCHAs:
  - focus on state-of-the-art MIOR by **NuCaptcha**
  - contrast with new approach based on **"Emerging Images"** by Mitra et al., 2009
- Security Analysis:
  - explore various attacks and mitigation strategies
- Usability Analysis:
  - assess usability of existing MIORs and extensions

Related Work

- Security: [Yan et al.,'07-11] provide a comprehensive treatment of character and image recognition CAPTCHAs and attacks; Similarly, [Bursztein et al., Soupionis et al.] analyze audio CAPTCHAs

- Usability: [Kluever et al., Bursztein et al., Yan et al.], study usability of both character and audio CAPTCHAs

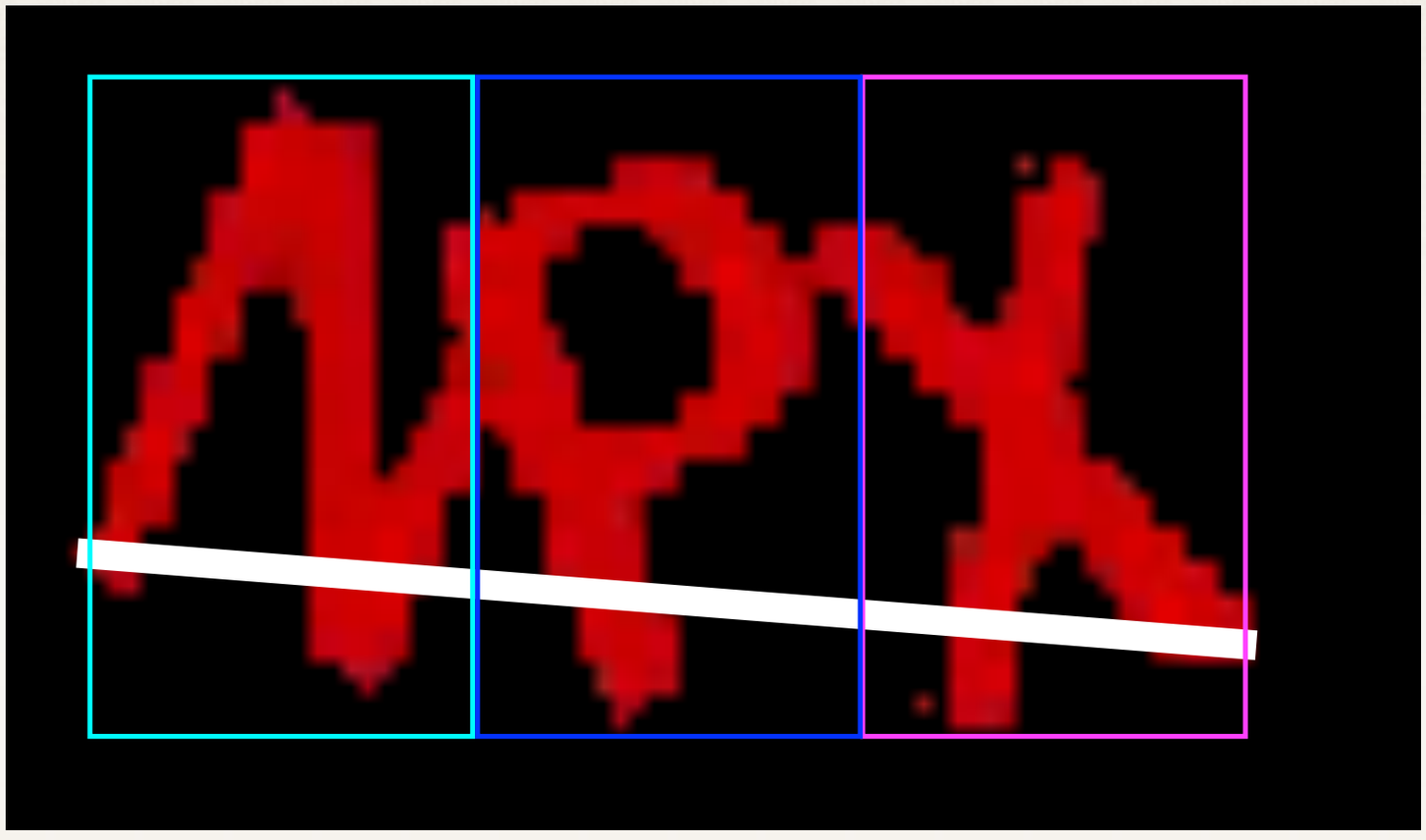
- Recently, [Bursztein,'12] discusses a similar technique on his blog to defeat MIOR CAPTCHAs by NuCaptcha

Assumptions

- Movement of rigid objects
- Codewords have their own trajectories
- Dynamic background with moderate contrast to foreground
- Number of characters is known in advance
  - Recently shown to be no longer needed

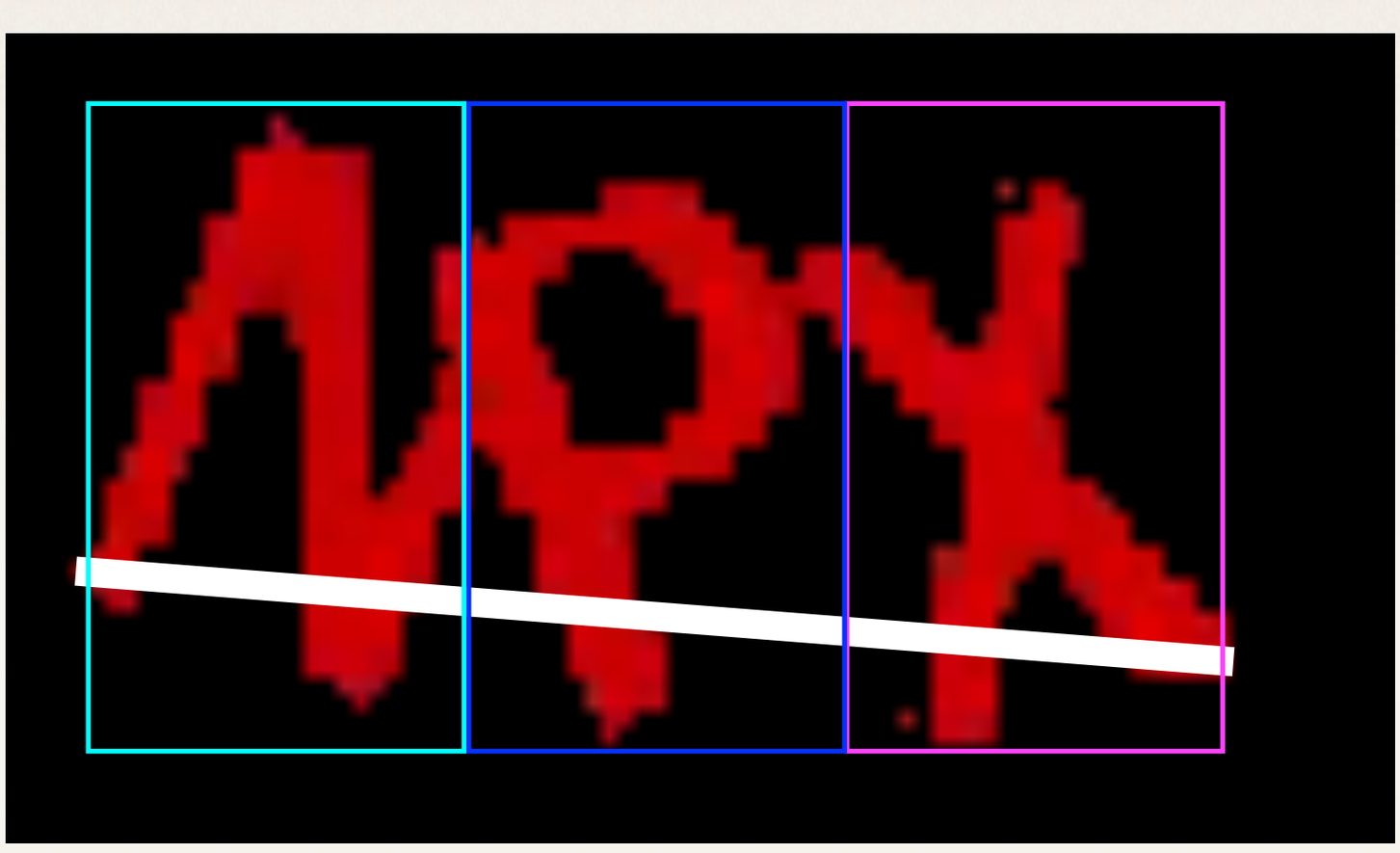
Naive attack

- Extract foreground based on color
- Equally divide the longest horizontal distance
- Get raw patches

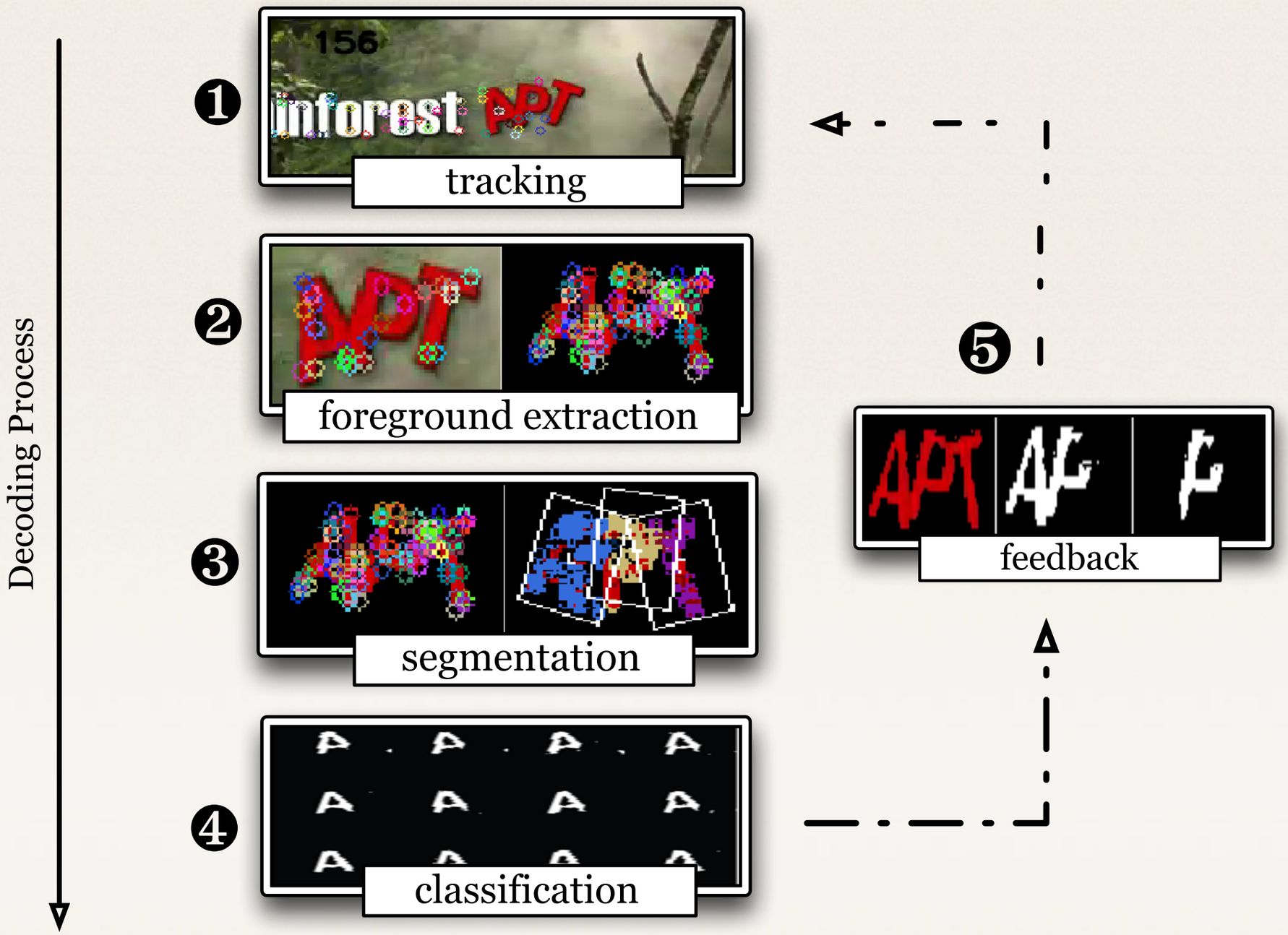


Naive attack

- Recognize the derived patches with standard captcha attack method
- Success Rate: 36.3% for 3 letters (4000 videos)



Enhanced Attack



❶ Optical Flow Tracking

- Extract corners

❶ Optical Flow Tracking

- Connect the corners to trajectories

❷ Foreground Extraction

- Remove background trajectories
- Find trajectories of foreground letters
- Infer trajectories of codeword characters

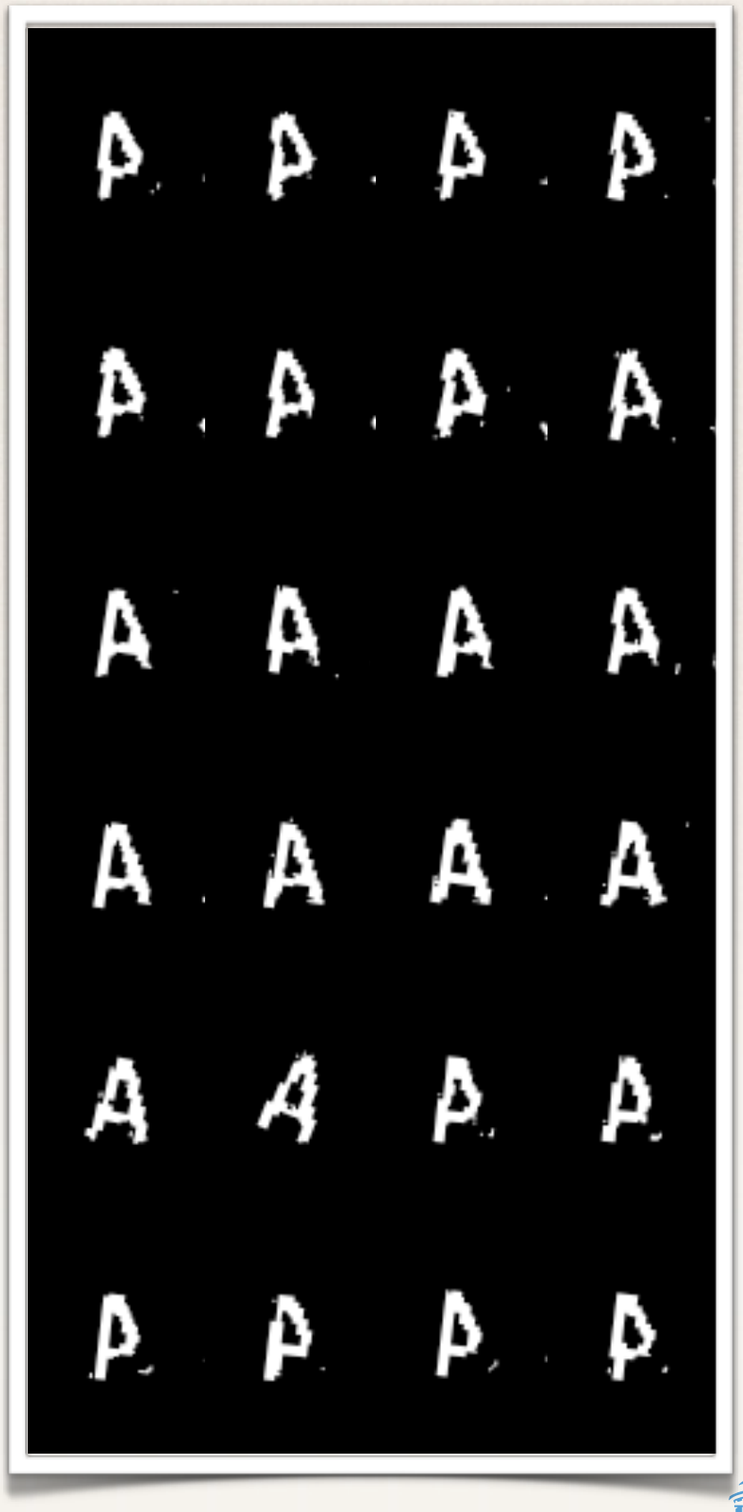
❸ Segmentation

- Increase the number of salient points
- Group trajectories of each character

❹ Classification

- Derive patches from each frame
  - Rotate to the correct orientation
- Classify the representative motif

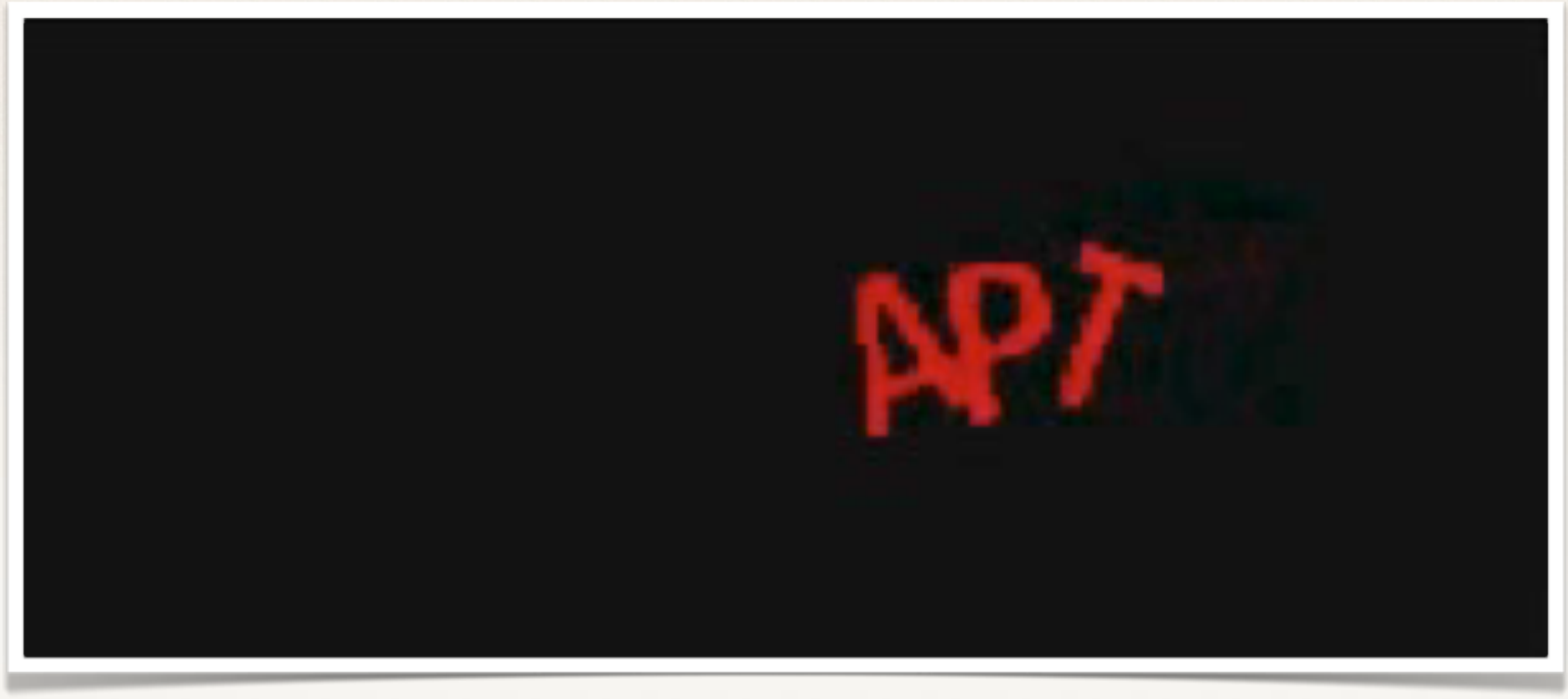
patches from different frames



Motif

❺ Feedback

Repeatedly mask most confident guess and then classify remaining patches



Guess: **A P T**

Evaluation (NuCaptcha)

- Training:
  300 MIOR videos, 1800 patches
- Testing
  200 MIOR videos across 19 backgrounds

Attack Strategy	Single Character Accuracy	3-Character Accuracy
Naive Approach	68.5% (8216/12000)	36.3% (1450/4000)
Without Feedback	90.0% (540/600)	75.5% (151/200)
With Feedback	90.3% (542/600)	77.0% (154/200)

Why does the Enhanced Attack work?

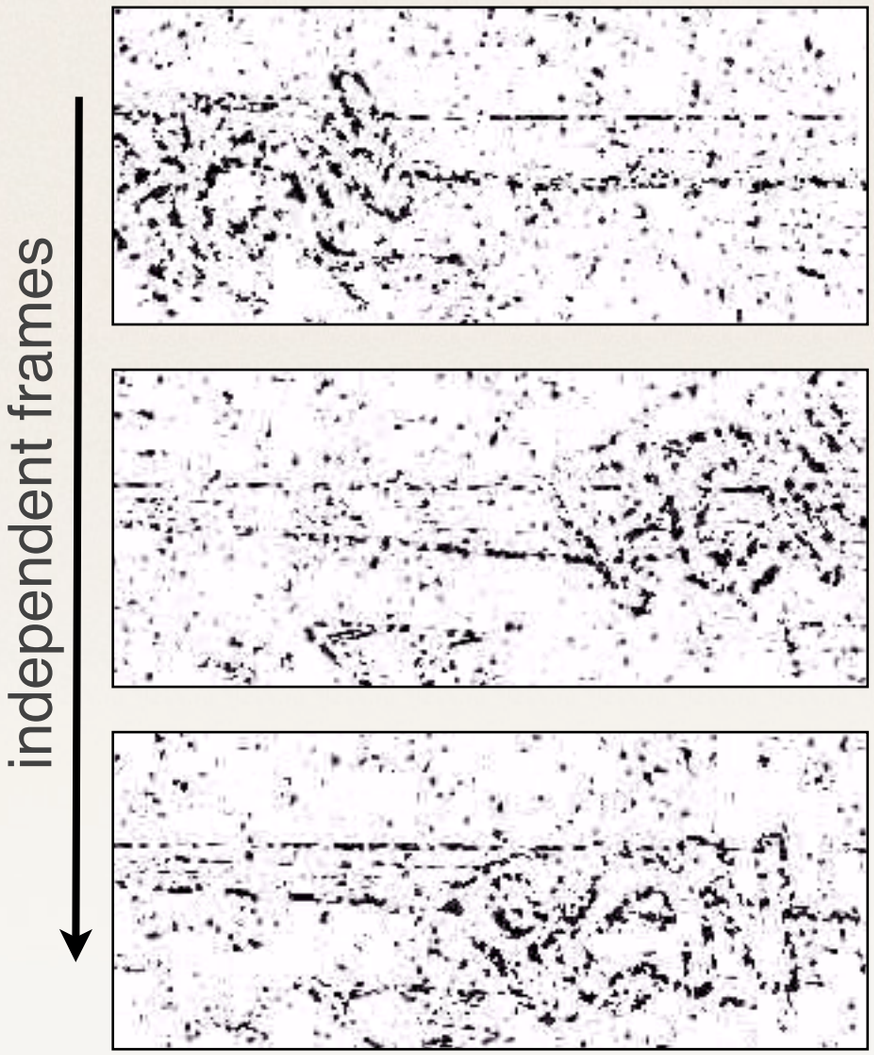
- Temporal information
  - Reveal the foreground
  - Segmentation
  - Feedback loop
- Optical flow provides temporal information

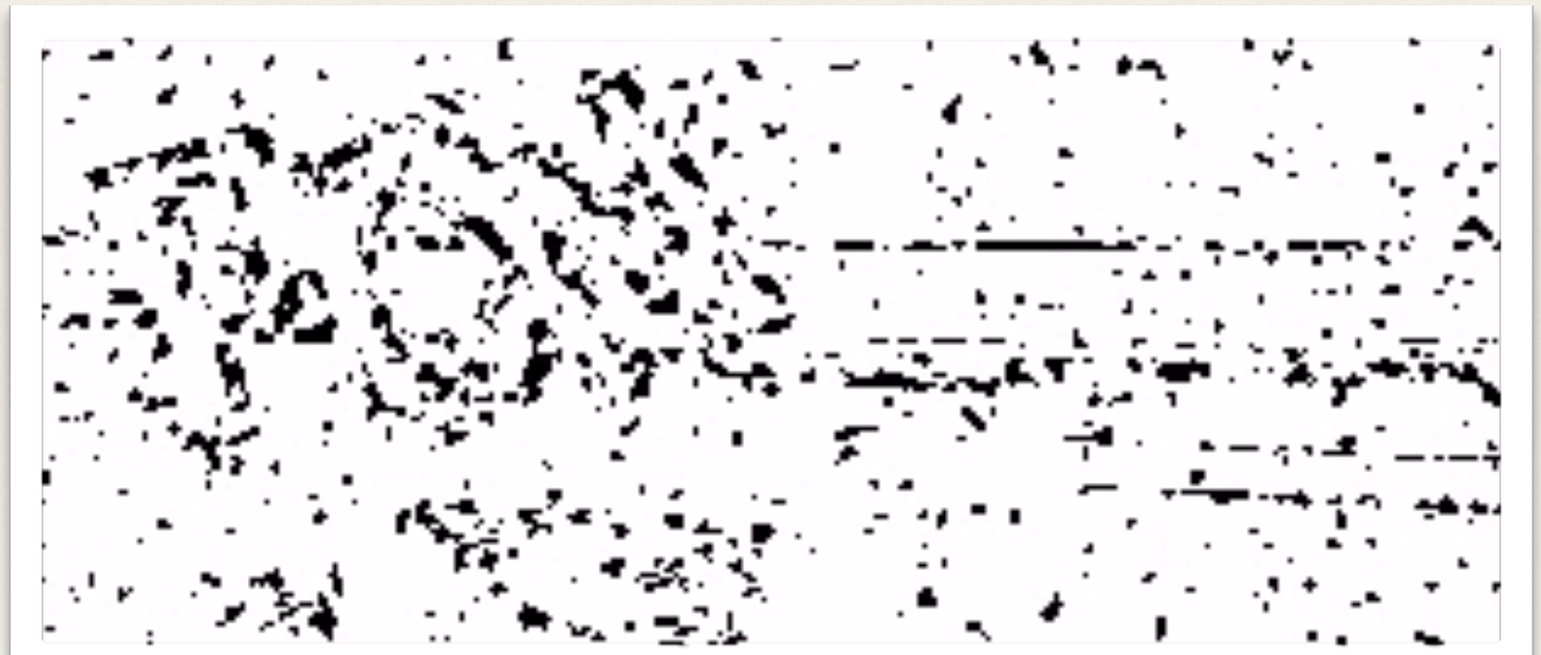
"Emerging Images" as an Alternative MIOR CAPTCHA

- A synthesis technique to generate images of 3D objects that are detectable by humans, but difficult for an automatic algorithm to recognize
- Attempts to thwart both optical flow tracking and any segmentation or recognition procedures
  - We implemented our own instantiation of this concept for 2D objects

EMERGING IMAGES
Niloy J. Mitra, Hung-Kuo Chu, Tong-Yee Lee, Lior Wolf, Hezy Yeshurun, Daniel Cohen-Or , ACM SIGGRAPH ASIA 2009

Emerging Images





MIOR CAPTCHA

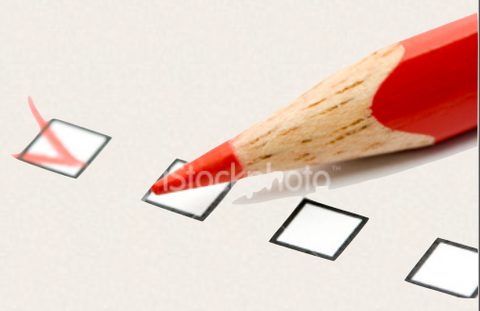
Evaluation: “Emerging Images”

- We applied our attack to 100 Emerging Image MIOR CAPTCHAs, but none succeeded
- The current attack fails because:
  - no single frame has enough visual cues to help distinguish the characters from the background
  - the codewords have no temporally consistent appearance

Evaluation

- At what point should we consider a CAPTCHA to be *fundamentally* flawed?
  - 1 in 100 success rate for automated programs? 1 in 10? 1 in 5? ...
- Are there natural extensions to NuCaptcha that could easily mitigate these attacks, ***without*** impairing **usability**?
- How *usable* is the Emerging Image approach?

User Study



- 25 participants, lab-based, within-subjects experimental design
- 5 variants tested, ordered based on Latin Square
  - for each variant, parameters in MIOR CAPTCHA were set to match the point where our attacks only succeed 5% of the time
- 10 random challenges per participant, per variant
- We analyzed participants' solutions, time to solve, errors made, and responses to a questionnaire

Variants

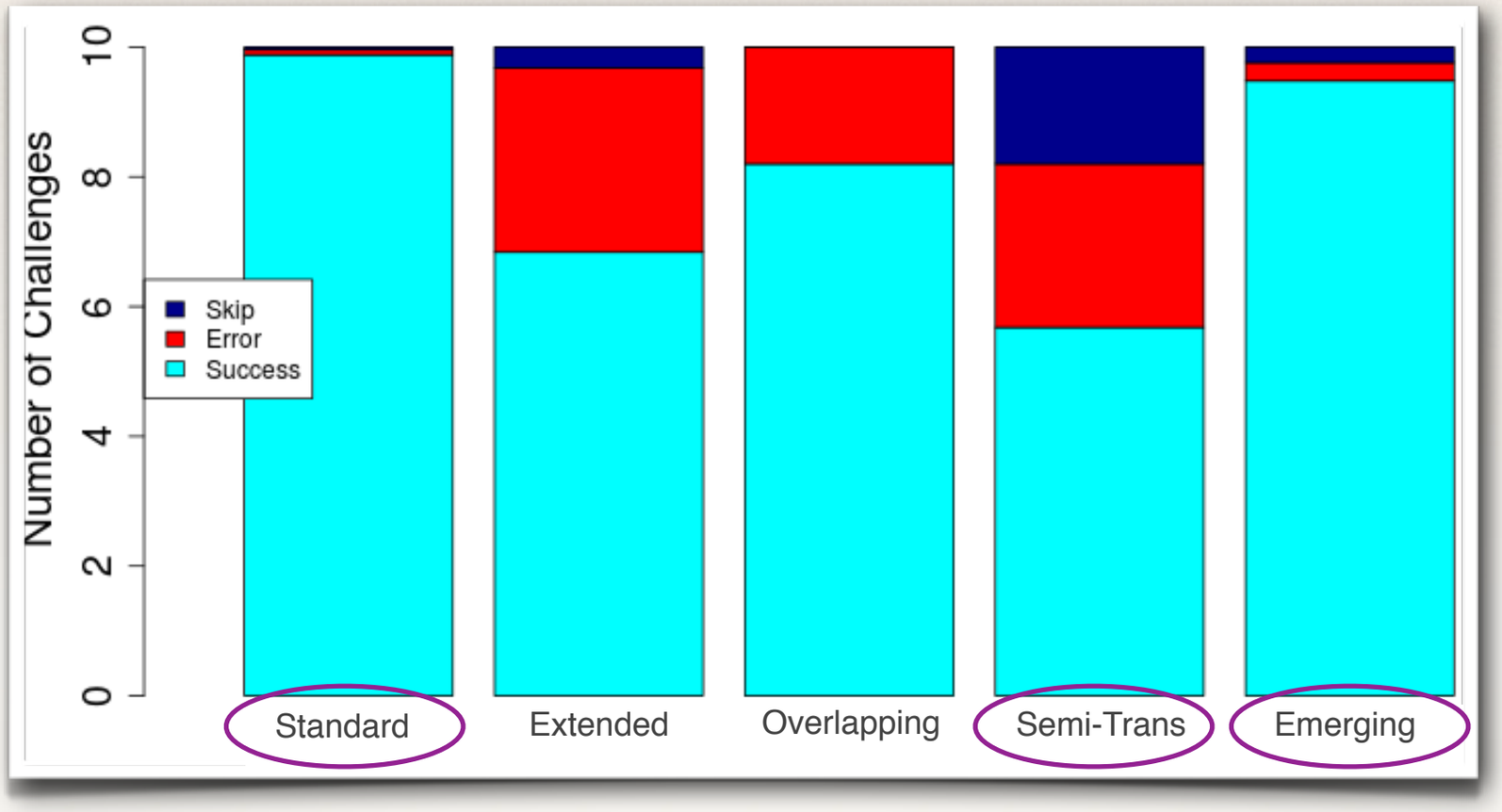
- Extended
  - attempt to increase MIOR security by increasing length of codeword

- Overlapping
  - attempt to thwart segmentation

- Semi-Transparent
  - attempt to thwart foreground extraction

User Study: Success rates

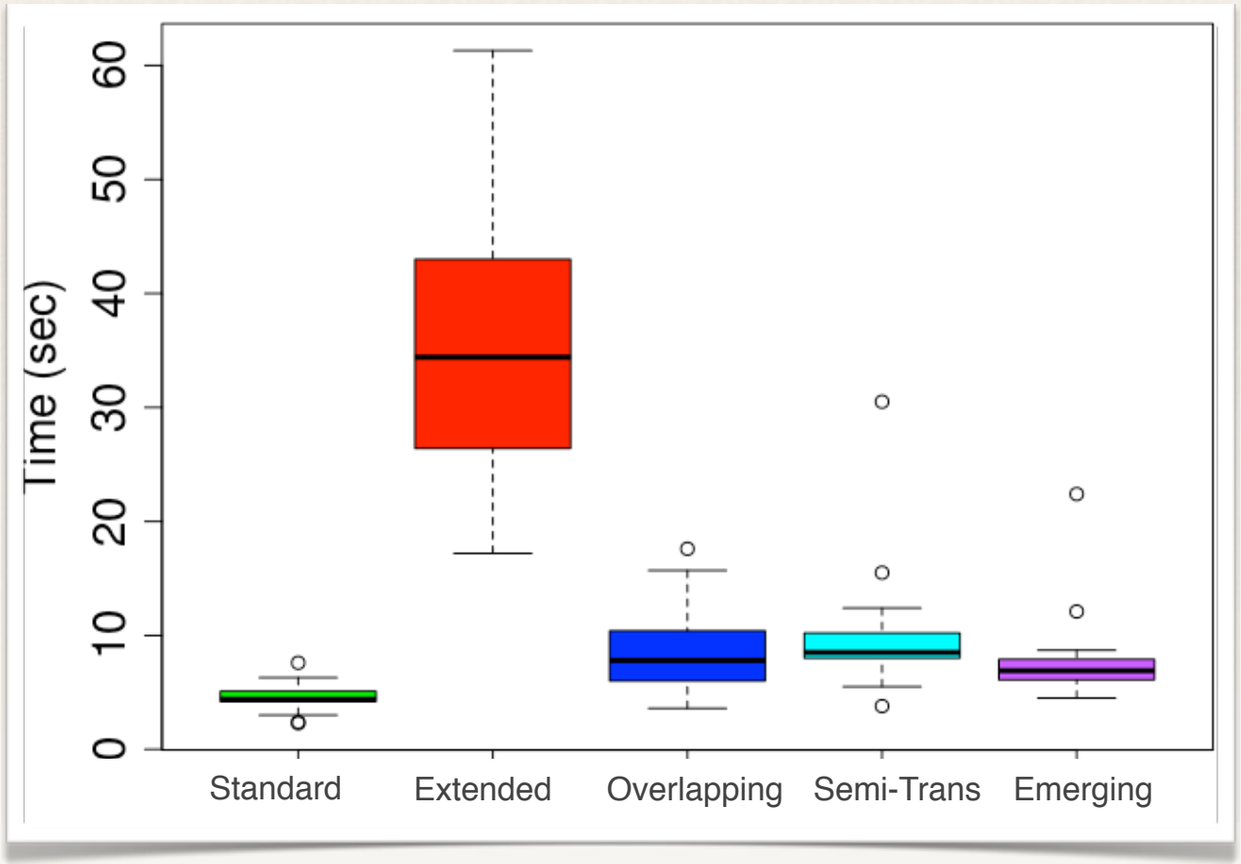
- Extended, Overlapping, and Semi-Transparent had significantly lower success rates compared to Standard
- No statistically significant difference between Standard and Emerging



Time to solve

Not surprising, Extended approach took the longest time to solve

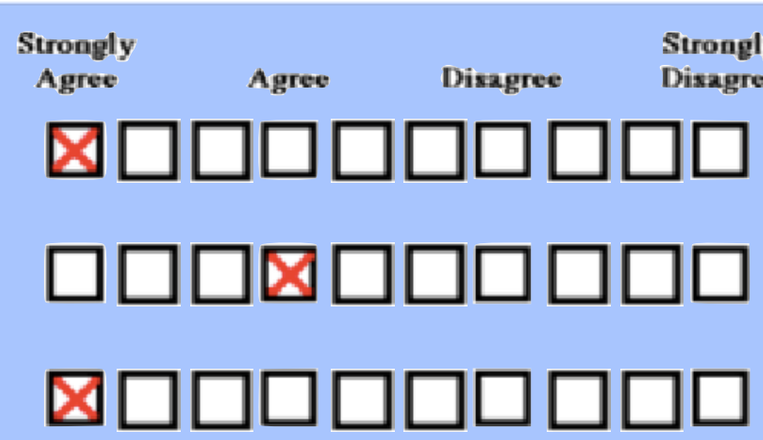
No statistically significant difference found between Standard, Emerging, Semi-Trans and Overlapping



User Perception

Perception:

- ☐ Was it easy to accurately solve the challenge?
- ☐ Were the challenges easy to understand?
- ☐ Was this CAPTCHA mechanism pleasant to use?

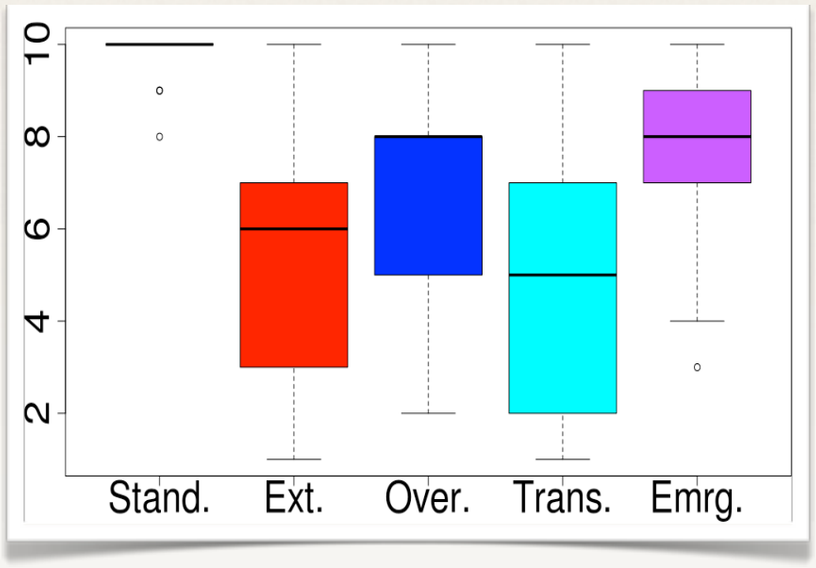


Participants completed a **Likert-scale** questionnaire to collect their opinion and perception of that variant (1 is most negative, 10 is most positive)

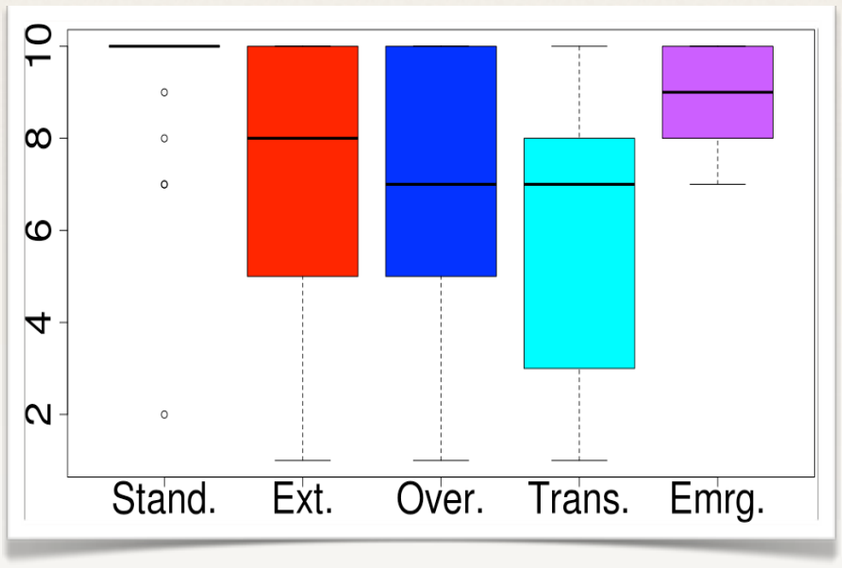
User Perception

- Users preferred Standard over other variants, although Extended and Emerging variants were viewed as no more difficult to understand than Standard

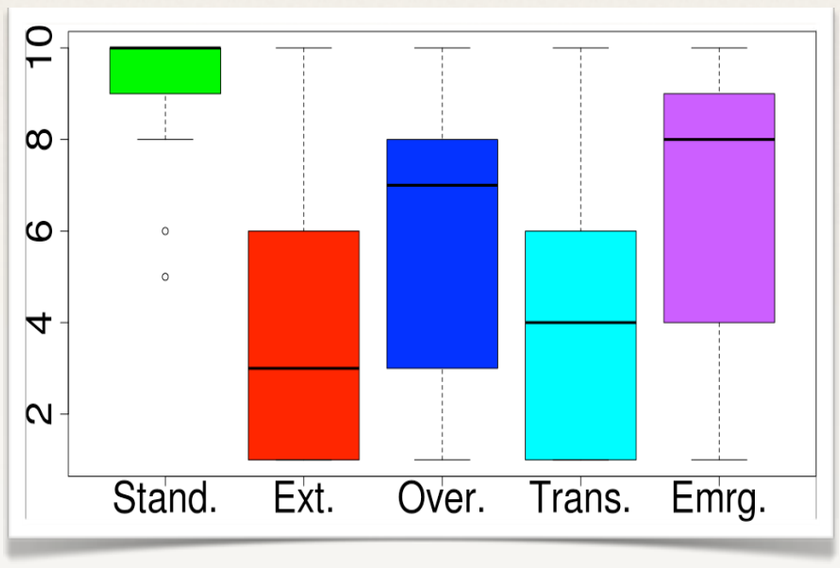
Accuracy



Easy to understand



Pleasant to use



Comparison of Standard, Extended, Overlapping, Transparent and Emerging variants, respectively

User comments

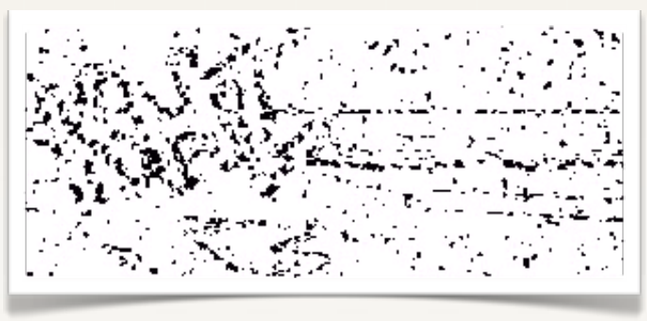
Variant	Comments
Standard	Much easier than traditional captchas
Extended	Giant Pain in the Butt! Sheer mass of text was overwhelming and I got lost many times
Overlapping	Letters too bunched – several loops needed to decipher
Semi-Transparent	With some backgrounds I almost didn't realize there were red letters It was almost faded and very time consuming. I think I made more mistakes in this mechanism
Emerging	It was hideous! Like an early 2000s website. But it did do the job.

User Study: Summary

- The Standard variant perceived as the most usable

- The Extended variant proved extremely difficult and users voiced strong dislike (and outrage!)

- The Emerging variant performed almost as well as the Standard approach on certain criteria (e.g., time to solve), and it also resisted our current attacks



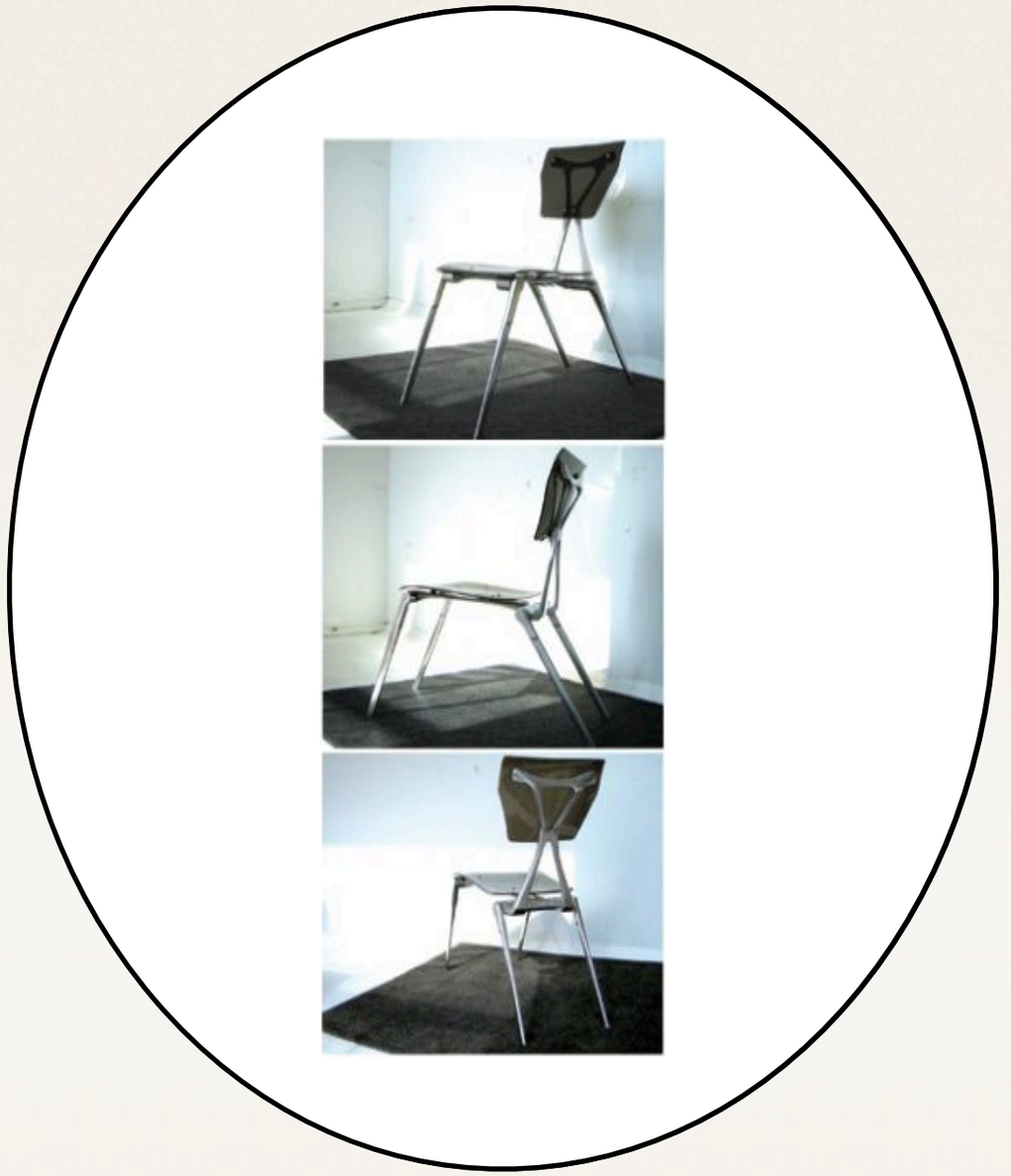
Conclusion

- Current state-of-the-art MIOR CAPTCHAs does *not* offer adequate security protections
- Emerging Images concept offers a viable alternative, per *today's* attacks

Conclusion

Object Recognition

Object Classification



Conclusion

- Current state-of-the-art MIOR CAPTCHAs does *not* offer adequate security protections
- Emerging Images concept offers a viable alternative, per *today's* attacks
- MIORs may focus instead on classification tasks or identification of high-level semantics
- See http://cs.unc.edu/videocaptchas for more info