CAPTCHA Recognition with Active Deep Learning

Caner Hazîrbaş

Joint work with Fabian Stark, Rudolph Triebel and Daniel Cremers
Deep CNN for CAPTCHA Recognition
Deep CNN for CAPTCHA Recognition

Advantages

✓ No pre-segmentation
✓ Precise prediction
Deep CNN for CAPTCHA Recognition

Advantages
✓ No pre-segmentation
✓ Precise prediction

Drawbacks
✦ Millions of parameters to learn
✦ Need of huge training set
Deep CNN for CAPTCHA Recognition

Advantages
✓ No pre-segmentation
✓ Precise prediction

Drawbacks
✦ Millions of parameters to learn
✦ Need of huge training set

Solution
✓ Active Learning:
  ✿ required training data
  ✿ increase the accuracy
Active Learning for CAPTCHA Recognition
Uncertainty Estimation

Training Data

Train Classifier

Learnt Model

Predict Labels

Uncertainties

Ask Labels

Additional Training Data

Update Training Data

Test Data

Supervisor

Predictions,
Uncertainty Estimation

“entropy?”
Uncertainty Estimation

“entropy ?”

Not a good measure in the case of multi-class problems!
Uncertainty Estimation

Train Classifier → Predict Labels → Ask Labels

Uncertainties

Supervisor

Additional Training Data

Update Training Data

Training Data → Learnt Model

Test Data

Predictions,

“best-vs-second-best”

\[ \eta = \frac{1}{d} \cdot \sum_{i=1}^{d} \frac{\arg \max \mathcal{P}(x_i) \setminus \arg \max \mathcal{P}(x_i)}{\arg \max \mathcal{P}(x_i)} \]
No Human Intervention
No Human Intervention

Diagram:

- Training Data → Train Classifier → Learnt Model
- Test Data → Predict Labels
- Predictions, Uncertainties → Ask Labels → Additional Training Data → Update Training Data
- Supervisor
No Human Intervention

- Training Data
- Test Data
- Supervisor
- Additional Training Data
- Learnt Model
- Predict Labels
- Predictions, Uncertainties
- Ask Labels
- Update Training Data

*https://eu.clickandbuy.com/*
No Human Intervention

![Diagram showing the process flow with nodes for Training Data, Test Data, Learnt Model, Predict Labels, Ask Labels, Additional Training Data, and Update Training Data.]

*https://eu.clickandbuy.com/*
No Human Intervention

Training Data → Train Classifier → Predict Labels → Ask Labels → Additional Training Data → Update Training Data

Test Data → Predict Labels → Ask Labels

Supervisor

Learnt Model, Predictions, Uncertainties

*https://eu.clickandbuy.com/*
No Human Intervention

Training Data → Train Classifier → Learnt Model → Predict Labels

Test Data → Predict Labels

Supervisor → Ask Labels → Predictions, Uncertainties → Additional Training Data → Update Training Data

*https://eu.clickandbuy.com/
No Human Intervention

Diagram:
- Training Data → Train Classifier
- Test Data → Predict Labels
- Supervisor
- Predictions, Uncertainties → Ask Labels
- Additional Training Data → Update Training Data

Is correct?

*https://eu.clickandbuy.com/
No Human Intervention

Training Data → Train Classifier → Learnt Model

Test Data → Predict Labels

Predictions, Uncertainties

Ask Labels → Additional Training Data → Update Training Data

is correct?

yes → new training sample

no → no ground truth :/
No Human Intervention

Training Data → Learnt Model → Predict Labels → Ask Labels → Update Training Data

Train Classifier

Test Data

Predictions, Uncertainties → Additional Training Data

Supervisor

Learnt Model

Predictions, Uncertainties

is correct?

yes —> new training sample

no —> no ground truth :/

*https://eu.clickandbuy.com/
Results on Auto-generated CAPTHAs
Results on Auto-generated CAPTHAs

Increasing training set

Accuracy (%) vs. # Iterations \(\cdot 10^4\)

- Green line: added correct and uncertain samples
- Black line: added all correct samples
- Blue line: added random correct samples
- Red line: added correct and certain samples

Examples of CAPTHA images:
Results on Auto-generated CAPTHAs

Increasing training set

Fine-tuning on the new set
CAPTCHA Recognition with Active Deep Learning

Caner Hazırbaş  l  hazirbas@cs.tum.edu

is correct?

yes —> new training sample
no —> no ground truth :/

*https://eu.clickandbuy.com/