L-012

# 主観的輪郭を応用した CAPTCHA の強度評価
# Robustness of CAPTCHA based on Subjective Contour

小宮山 哲俊† 梅澤 猛† 大澤 範高†
Tetsutoshi Komiyama Takeshi Umezawa Noritaka Osawa

## 1. はじめに

CAPTCHA は，応答者が人間かプログラムかを判別するテスト手法であり，メールアカウントの不正取得や，掲示板・ブログへの不正書き込みを行う悪意あるソフトウェアプログラムを排除する目的で広く利用されている．現在一般的な文字判読型の CAPTCHA については，光学文字認識（OCR）の技術発展に伴い，OCR プログラムによって自動認識されてしまう事例が増加している[1]．錯視を利用した読み取りテストによって OCR に対する強度を高めた手法も提案されているが，パターンマッチングや機械学習を使った OCR プログラムによって，自動認識される可能性がある．

そこで本研究では，錯視の一例として，主観的輪郭と呼ばれる現象を応用した CAPTCHA について，パターンマッチングとサポートベクターマシン（SVM）による機械学習との 2 つの認識手法に対する強度を調べた．また，主観的輪郭を利用して提示する文字列画像に歪みを加えることで，パターンマッチングや SVM に対しても高い強度をもつ手法を提案する．更に，ユーザが CAPTCHA を読み取る際に感じる負担を調べるために，被験者による読み取り実験を行った．

## 2. 主観的輪郭を利用した CAPTCHA

主観的輪郭は，存在しない輪郭線が知覚される錯視現象である．主観的輪郭を利用した CAPTCHA [2]の画像例を図 1 に示す．輪郭線の知覚を誘導するための図形（誘導図形）を配置することで，文字の輪郭線を直接表示することなく文字‘A’を提示している．ユーザにとっては錯視効果により文字を読み取ることができるが，OCR プログラムにとっては輪郭線が存在しないため認識が困難となる．

しかし，ユーザが文字を読み取り易くするためには，輪郭の向き変化が大きい箇所に誘導図形を配置する必要があり，配置パターンには一定の制約が生じる．このため，予め提示される可能性のある文字の誘導図形配置パターンを用意しておくことで，パターンマッチングによる自動認識の恐れがある．さらに，SVM 等の機械学習手法を用いることで，提示画像を学習して認識される可能性もある．

## 3. 提案手法

本稿では，従来型の OCR だけではなく，パターンマッチングや機械学習に対しても高い強度を持った CAPTCHA を実現するため，主観的輪郭を利用して提示する文字形状に，歪みを加える手法を提案する．誘導図形の描画座標の組み合わせ総数，CAPTCHA 画像の生成パターン総数を増やし，OCR プログラムによる認識率を低減する手法を提案する．提案手法は，主観的輪郭錯視を利用して，アフィン変換等の画像処理により歪みを加えた文字列を表現する．提案手法の一例として，文字列‘ABC’を剪断変形させた形状を，主観的輪郭を応用して表現したものを図 2 に示す．主観的輪郭錯視で表現する文字の形状が増えることで，誘導図形の配置の組み合わせ数も増加するため，パターンマッチングや SVM を実装したプログラムによる認識率を大幅に低減できると期待できる．


図 1 主観的輪郭を利用した CAPTCHA 画像の例

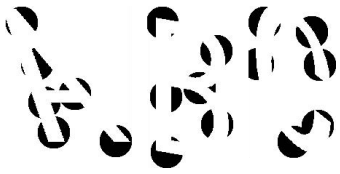

図 2 提案手法による CAPTCHA 画像の例

## 4. 強度評価

パターンマッチングと SVM の 2 通りの手法により，既存の主観的輪郭 CAPTCHA と提案手法の OCR プログラムに対する強度を評価した．

### 4.1 パターンマッチングに対する強度評価

主観的輪郭を利用した CAPTCHA について，パターンマッチングによる認識に対する強度を評価するため，歪みの有無による文字認識実験を行った．

まず，主観的輪郭を利用して‘A’から‘Z’の 26 種類の文字を表す画像（縦 300×横 300 ピクセル）をそれぞれ 20,000 件ずつ，計 520,000 件用意した．つぎに，用意した画像をテストデータとテンプレートデータとして 260,000 件ずつに等分した．この際，両方のデータに同種の文字が同数含まれるようにした．

そして，K 近傍法を用いた画像分類によって認識結果を得た．類似度の定義としては，誘導図形の座標値を利用した．誘導図形の（x，y）座標を特徴量とし，画像に含まれる全ての誘導図形の座標を x 座標によって昇順に並び替えて特徴ベクトルとした．テストデータとテンプレートデータの全組み合わせについて，特徴ベクトルの間のユークリッド距離を算出して類似度とした．なお，K の値を K={1, 2, 3, … 30}として，それぞれの場合の認識結果を得た．

実験の結果，最大の文字認識率は，歪みを加えない場合で 69.79%（K=14），歪みを加えた場合で 17.03%（K=21）であった．

### 4.2 SVM に対する強度評価

4.1 と同様の手順で，‘A’から‘Z’の 26 種類を 2,000 件ずつ，計 52,000 件の画像を用意し，テストデータと学習データとして 26,000 件ずつに等分した．得られた学習データ 26,000 件を使って SVM による学習を行い，one-against-all 法に従って画像を分類した．

† 千葉大学大学院融合科学研究科 Graduate School of Advanced Integration Science, Chiba University

実験の結果，SVM による文字認識率は，歪みを加えない場合で 95%，歪みを加えた場合で 60%であった．

## 5. ユーザの読み取り負担評価

実際に主観的輪郭を利用した CAPTCHA に回答する際に，ユーザが感じる負担を調べるために被験者による文字読み取り実験を行った．

CAPTCHA の提示手法による違いを調べるため，1）Google で利用されているのと同様に 3 桁の数字を読み取る画像，2）主観的輪郭を利用した英字 3 字を読み取る画像，3）主観的輪郭を利用した上で歪みを加えた英字 3 字を読み取る画像の 3 通りについて読み取り実験を行った．被験者が各画像の読み取りに掛かる時間を計測した後，質問紙調査によって負担の程度を調査した．質問は次の 3 つで，1（強く不同意）～5（強く同意）の 5 段階による回答を得た．

Q1．数字 CAPTCHA の負担は軽い
Q2．主観的輪郭を利用した CAPTCHA の負担は軽い
Q3．主観的輪郭を利用した上で歪みを加えた CAPTCHA の負担は軽い

実験は被験者 10 人に対して行い，3 種の CAPTCHA 手法についてそれぞれ用意した 100 枚の画像から 1 枚ずつ計 3 枚の画像を被験者毎にランダムに提示した．また，被験者が回答を誤った場合には，同じ CAPTCHA 手法による別画像を再提示し，正解するまで回答を繰り返すこととした．

実験の結果，3 つの CAPTCHA 提示手法それぞれの読み取りに要した平均時間は，それぞれ 1）6.1 秒，2）7.6 秒，3）6.6 秒であった． また，正解率はそれぞれ 1）100%，2）90%，3）100%であった．なお，唯一の誤答は 2）において‘P’を‘F’と誤ったものであった． 質問紙による負担調査の結果は図 3 に示す通りで，全ての提示画像について読み取りの負担を「非常に重い（強く不同意）」と 回答した被験者はいなかった．

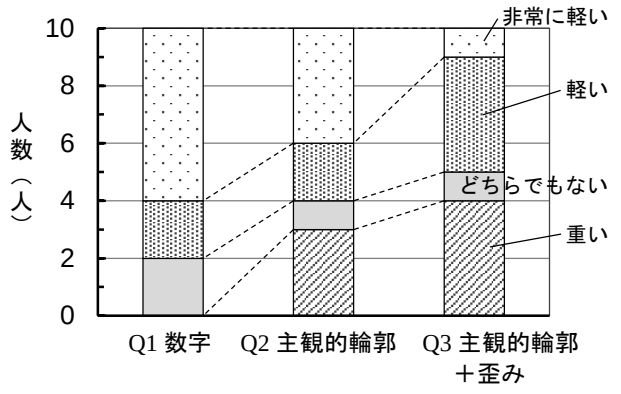


図 3　ユーザが CAPTCHA 読み取りに感じる負担

## 6. 考察

### CAPTCHA の強度

パターンマッチングに対する強度評価の結果によると，歪みを加えない主観的輪郭による CAPTCHA は，誘導図形の座標を特徴量とすることで，1 文字であれば 70%程度が自動認識できる．これに対し，歪みを加えた場合の文字認識率は 17%程度と 4 分の 1 以下に低下していることから，パターンマッチングによる自動認識率を大幅に低減できることがわかる．また，SVM による自動認識についても，歪みを加えない主観的輪郭による CAPTCHA の認識率が 95%であるのに対して，歪みを加えた場合の認識率は 60%であり，自動認識を難しくする効果があることがわかる．

提案手法は，既存の主観的輪郭 CAPTCHA と比べるとプログラムによる自動認識が難しくなっているものの，認識率は 60%と依然高い．しかし，例えば提案手法によって 5 文字を提示する場合について試算すると，認識率は 7.8%（$0.6^5 \times 100$）程度にまで低減できる．

### ユーザの負担

ユーザが読み取りに要した時間を比較すると，提案手法による CAPTCHA は，他の手法と比べて，その差は 1 秒以下であった．また，正解率について比較すると，3 つの CAPTCHA 提示手法の正解率は全て 90%以上であり，大きな差はみられなかった．従って，読み取りの所要時間および正解率の点で，提案手法がユーザ与える負担増は限定的であると考えられる．

つぎに，ユーザが感じる負担感について，図 3 の Q1 および Q2 を，Q3 と比較すると，数字 CAPTCHA については負担が重いと答えた被験者がいなかったが，主観的輪郭を利用した CAPTCHA については負担が重いと答えた被験者がいた．従って，数字 CAPTCHA と比べると，主観的輪郭を利用した CAPTCHA の読み取りにユーザが感じる負担感は大きいと考えられる．しかし， Q2 と Q3 を比較すると，負担が非常に軽いと答えている数は歪みなしの方が多いものの，負担が重いと答えた数には大きな違いはみられなかった．このことから，歪みの有無に関しては，ユーザの感じる負担感に大きな差はないと考えられる．

## 7. 結論

本稿では，既存の主観的輪郭 CAPTCHA が OCR プログラムにより自動認識可能であることを示した．また，歪みを加えた文字を主観的輪郭錯視を利用して表現することで，OCR プログラムによる認識率を低減する手法を提案した．強度評価実験の結果，提案手法を用いることで，誘導図形の座標を特徴量として文字を認識する OCR プログラムに対する強度が高まることが分かった．さらに，被験者実験の結果，ユーザが読み取りに要する負担は歪みを加えない主観的輪郭を応用した CAPTCHA と比べて大きな違いがないことが示唆された．今後は，回転等の画像処理を加えて画像の生成パターン数を増やし，OCR による認識率のさらなる低減を目指す．

### 参考文献

[1] Bursztein Elie, Matthieu Martin, and John Mitchell “Text-based CAPTCHA strengths and weaknesses.” Proc. of 18th ACM conference on computer and communications security, pp. 125-138, 2011.
[2] 橋本弥弦“主観的輪郭の CAPTCHA への応用.”早稲田大学大学院理工学研究科修士論文，2008.