L-010

アモーダル補完を応用した CAPTCHA における文字認識攻撃への耐性評価に関する検討
Study on amodal completion-based CAPTCHA to evaluate to robustness to character recognition

上妻 拓也† 梅澤 猛‡ 大澤 範高‡
Takuya Kozuma Takeshi Umezawa Noritaka Osawa

1. はじめに

CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart)は、応答者が人間なのか、サービスの悪用を目的としたボットなの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等への対策として利用されている。一般に文字型の CAPTCHA が利用されるが、光学文字認識や機械学習の技術発展に伴い、ボットによって自動認識されてしまう事例が増加している。ノイズや歪みを多く加える策があるが、人間の応答負担も大きくなる問題がある。そこで本研究では、人間にとっては負担が少なく、機械学習を用いた文字認識に対しては耐性を持つ CAPTCHA を作成することを目的とし、人間が部分的に遮蔽された物体を見たときに働く視覚の補完機能であるアモーダル補完を応用して CAPTCHA に適用する手法を検討する。

2. 関連研究

文字型 CAPTCHA において、文字に歪みやノイズを加えることで、ボットに対する堅牢性を向上させる手法がある。しかし、Chellapilla らはニューラルネットワークと人間による CAPTCHA の評価実験から、文字に歪みやノイズを多く加えても堅牢性は向上せず、人間の負担を大きくするだけであると述べている[1]。

森らは、アモーダル補完を動画に応用する手法を用いた文字型 CAPTCHA を提案している[2]。一部が欠けた 4 文字が表示されている状態で、画面内を移動する遮蔽物が提示される。遮蔽物が適切な位置に表示されたときに見ると、アモーダル補完の効果によって人間には文字が認識できる。このタイミングは 10 秒の動画中に 0.2 秒間ずつ計 4 回発生する。有効解答時間 30 秒に対し、コンピュータは解析に約 50 秒かかるという結果から、有用性のある CAPTCHA であると述べられている。しかし、10 秒間の動画から 0.2 秒間だけ現れる文字を 4 回読み取ることは人間にとっても大きな負担になると考えられる。そこで、本研究では静止画に対してアモーダル補完を応用する手法を検討する。

3. 提案手法

本研究では、背景色または文字色の遮蔽物を含む文字画像と遮蔽物を覆い隠すことができる背景色、文字色以外のマスク画像の 2 枚の画像を提示する手法について検討した。2 枚の画像を解答者が重ね合わせることで遮蔽物はマスクにより隠される。画像の例を図 1 に示す。解答者は提示された図 1(a)と図 1(b)を重ね合わせて図 1(c)を作成し、文字認識を行う。文字の一部はマスクによって遮蔽されてしまうが、人間はアモーダル補完によって文字認識が可能である。また、画像を重ね合わせるという処理は従来の CAPTCHA にはない新たなコストとなるため、ボットに対する耐性を高める効果があると考えられる。

† 千葉大学大学院融合理工学府数学情報科学専攻
‡ 千葉大学大学院工学研究院

4. SVM による評価実験

提案手法は、文字認識を行うために画像の重ね合わせを要求する。しかし、ボットによって遮蔽物を含む文字画像のみから文字認識を行われてしまうと、画像の重ね合わせは必要なくなってしまい、ボットに課すコストを増やすことができない。そこで、遮蔽物を含む文字画像として(ⅰ)背景色の円形遮蔽物を含む画像、(ⅱ)背景色＋文字色の円形遮蔽物を含む画像、(ⅲ)他の文字の一部を含む画像の 3 種類の画像を作成し、Support Vector Machine(SVM)による認識精度を調査することで評価を行った。

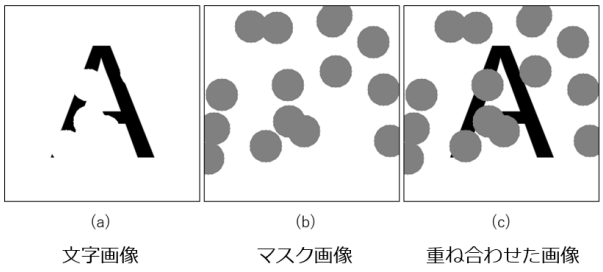


図 1 画像の重ね合わせの例

4.1 データセットの作成手順

まず、縦横 300pixel の白で初期化された画像中央に 240pixel の大きさで文字を描画した。文字はアルファベットの大文字'A'から'Z'の 26 文字、フォントは Arial とした。つぎに、各遮蔽物を描画した後、画像を縦横 64pixel に縮小し、二値化した画像の全画素値を特徴量として使用した。画像は各文字 1,000 件ずつの計 26,000 件を 2 回作成し、それぞれ学習データとテストデータとした。なお、遮蔽物については次の 3 通りの描画方法によるものを用意した。

4.1.1 背景色の円形遮蔽物を含む画像

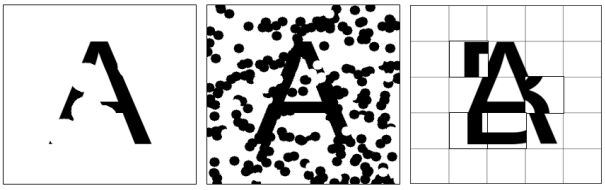
文字を描画した画像上に、背景色（白）の円形をランダムな座標に描画することで画像を作成した。遮蔽物の個数は 5 個、10 個、15 個、遮蔽物の直径は 10pixel から 100pixel まで 10pixel ずつ変化させて、それぞれデータセットを作成した。作成した画像例を図 2(a)に示す。

4.1.2 背景色＋文字色の円形遮蔽物を含む画像

文字を描画した画像上のランダムな座標を選択し、その座標が文字上であれば背景色の円形、文字上でなければ文字色の円形を描画した。遮蔽物の個数は 10 個、100 個、500 個、遮蔽物の半径は 1pixel、2pixel、4pixel、8pixel、16pixel と変化させて、それぞれデータセットを作成した。作成した画像例を図 2(b)に示す。

4.1.3 他の文字の一部を含む画像

文字を描画した画像を 25 分割されたパネル画像の集合とみる。ランダムに選ばれた複数のパネルを他の文字画像の同じ座標のものと置き換えることで文字画像を作成した。選ばれたパネルを全て他の 1 文字の画像のパネルと置き換える方法 A と、パネル 1 枚ごとに置き換える文字をランダムに選択する方法 B の 2 つの方法でそれぞれデータセットを作成した。作成した画像例を図 2(c)に示す。



(a)背景色　(b)背景色＋文字色　(c)他の文字の一部

図 2　作成した 3 種類の画像例

4.2 結果

各文字画像について SVM を用いて文字認識を行い、認識精度を調査した。背景色の円形遮蔽物を含む画像について結果を図 3、背景色＋文字色の円形遮蔽物を含む画像についての結果を図 4、他の文字を含む画像についての結果を図 5 に示す。

5. 考察

図 3、図 4 より、背景色、背景色＋文字色の円形遮蔽物を加えた文字画像であっても SVM を用いること高精度で認識されてしまうことがわかる。図 3 では遮蔽物の個数と直径を大きくすることで認識率を 70%にまで下げることができているが、これは遮蔽物によって文字情報の殆どが隠されてしまっているからである。図 4 の遮蔽物の個数 500 個、半径 16pixel の場合も同様である。提案した手法ではこの文字画像にマスク画像を重ねることで文字認識が可能になるが、画像中の遮蔽物の面積が多くなると、マスクの面積も多くなり、人間が画像の重ね合わせを行っても文字認識が不可能になってしまう。

図 5 では、入れ替えるパネルを多くすると認識率が低下している。これは、正解文字の情報よりも入れ替えた文字の情報が多くなっていくためであると考えられる。方法 B は色々な文字の情報を含むので、正解文字の情報を上回るために置き換えるパネル数が多く必要になっている。この手法の課題としては、方法 A では 2 文字の情報しか含まれていないため容易に文字認識される恐れがある。一方、方法 B では認識率を下げるために多くのパネルの入れ替えが必要となり、正解文字の情報が減ってしまい、マスク画像と合わせても文字認識が行えないことが予想される。

3 種類の文字画像には、遮蔽物の量が少ない時に高精度で認識されてしまうという共通の問題があるが、これは文字の描画条件が一因になっていると考えられる。実験では領域分割が完全に行われたという仮定で、文字を無回転で画像の中央に描画しているが、実際には文字に多少の位置、角度のすれがあると予想される。文字の位置、角度についての条件を適切な範囲で許容することで、正確に SVM による評価が行うことができる。

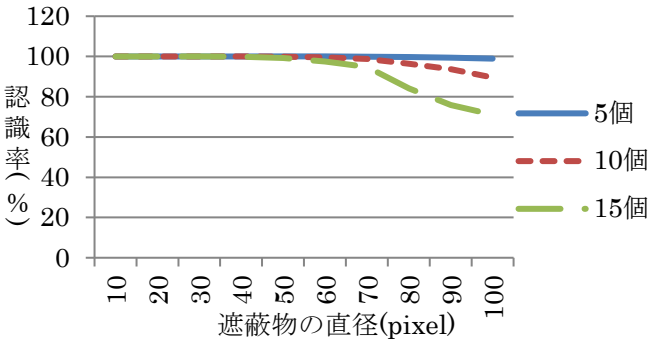


図 3 背景色の円形遮蔽物を含む画像の認識率

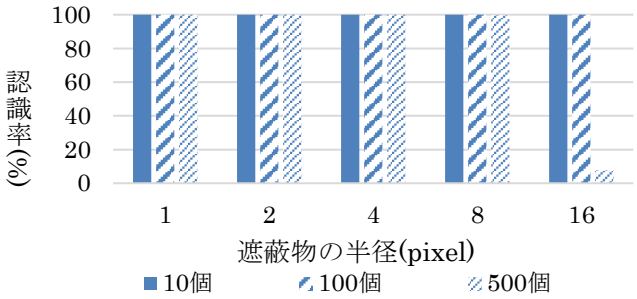


図 4　背景色＋文字色の円形遮蔽物を含む画像の認識率

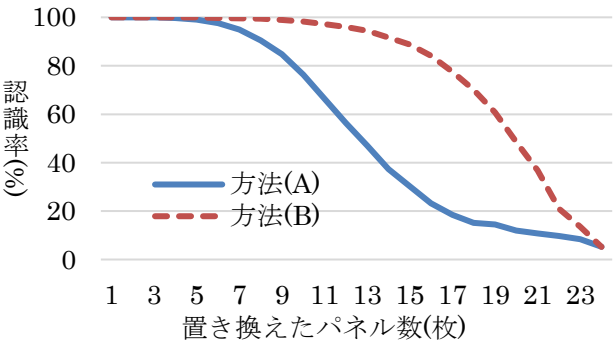


図 5 他の文字の一部を含む画像の認識率

6. 今後の課題

CAPTCHA の評価はボットに対しての堅牢性の評価だけでなく、人間にとっての可読性についても評価が必要であるため、被験者実験により人間が応答する際の負担についても調査していく。また、今回の実験では CAPTCHA の単一文字認識を対象としていたが、領域分割の難化についても錯視を応用する手法を検討していきたい。

参考文献

[1] K. Chellapilla, K. Larson, P. Simard, and M. Czerwinski, "Computers beat humans at single character recognition in reading based human interaction proofs," The Second Conference on Email and Anti-Spam, 2005.

[2] 森拓真, 宇田隆哉, 菊池眞之. "アモーダル補完を利用した動画 CAPTCHA の提案." マルチメディア, 分散協調とモバイルシンポジウム 2011 論文集, pp.1518-1525, 2011.