

多数の不連続点に起因する画像の誤認識と その CAPTCHA への応用

原 亨¹ 佐藤 敬^{2,a)}

受付日 2019年3月11日, 採録日 2019年9月11日

概要: 自らがロボットではなく人間であることを証明する手段として CAPTCHA (completely automated public Turing test to tell computers and humans apart) という技術が多くの場所で用いられている。中でも, 人間の高度な画像認識能力に基づき, 利用者に画像内容や画像の共通性等を解答させる画像型 CAPTCHA が普及している。一方で, 画像内容を分類するアノテーションサービスを利用した攻撃が報告されており早急な対策が求められている。そこで, 本稿では, 人間は容易に正しく認識できるが, 機械が誤認識する画像の作成方法を提案する。そうした画像に基づいて構成した CAPTCHA が既存の代表的な画像認識システムに対する高い攻撃耐性と優れたユーザビリティを有することを示すと同時に, 画像処理攻撃への耐性について評価する。

キーワード: 画像認識, CAPTCHA, 不連続点

Fooling Images Recognition by Many Discontinuous Points and Its Application to CAPTCHA

TORU HARA¹ TAKASHI SATOH^{2,a)}

Received: March 11, 2019, Accepted: September 11, 2019

Abstract: CAPTCHA (completely automated public Turing test to tell computers and humans apart) technology is used in many places to prove that he is not a bot but a human. The image-based CAPTCHA allows users to solve contents and similarity among images with human's advanced image recognition capability. It has been become widespread, whereas image classification attacks using annotation services have been reported. Urgent countermeasures against such attacks are required. In this paper, we propose a method to create images that machines misrecognize, although humans can easily recognize them correctly. We show that a CAPTCHA using such images is robust to representative image recognition systems and is with good usability. Furthermore, we evaluate resistance to image processing attacks.

Keywords: image recognition, CAPTCHA, discontinuous points

1. はじめに

1.1 研究背景

自らがロボットではなく人間であることを証明する手段として CAPTCHA (completely automated public Turing

test to tell computers and humans apart) [1] という技術が多くの場所で用いられている。CAPTCHA には, 歪んだ文字画像の内容を入力させる文字型 CAPTCHA や, 人間の高度な画像認識能力に基づき, 利用者に画像内容や画像の共通性等を解答させる画像型 CAPTCHA が存在する。文字型 CAPTCHA の代表例としては Google の reCAPTCHA [2] があげられる。

しかし, 文字型 CAPTCHA に対しては 2012 年に歪んだ文字画像の内容を認識できるスクリプトが発表された [3].

¹ 北九州市立大学大学院国際環境工学研究科
The Graduate School of Environmental Engineering, The University of Kitakyushu, Kitayushu, Fukuoka 808-0135, Japan

² 北九州市立大学国際環境工学部
Faculty of Environmental and Engineering, The University of Kitakyushu, Kitakyushu, Fukuoka 808-0135, Japan

a) tsatoh@kitakyu-u.ac.jp

本稿は研究発表論文 [17] の内容を発展させたものである。

また、画像型 CAPTCHA に対しては、2016 年に Google 逆画像検索や画像内容を分類するアノテーションサービスを利用した攻撃 [4] や Google の Speech-to-Text API を利用して、画像を音声に変換し CAPTCHA を突破する攻撃 [5] が報告されている。これらの攻撃の対策をふまえた CAPTCHA が提案されているが、文献 [6] で「ボットの進化とともに徐々にクリア難度が高くなっていかざるを得ない」と論じられているように、最近の CAPTCHA は人間にとっても突破が面倒で困難になっている。

1.2 関連研究と本研究の位置付け

1.2.1 Turing test via failure

Amazon は新しい CAPTCHA として Turing test via failure [7] を提案し特許を取得している。この CAPTCHA は、人間が問題に対して答えを間違えるような問題を提示することで、ユーザが人間であることを確認するものである。問題の例を図 1 に示す。3つの画像が並んでおり、問題文として「このタイルはすべてが平面であるか？」と書かれている。この問題における正解は Yes である。3つの画像は2次元平面であり平面といえる。しかし、人間はこの画像の模様から左の画像は平面と認識するが、中央の画像は奥に凹んで見える、また右の画像は盛り上がって見えるであろう。これにより人間は No と答えることが期待される。問題を間違えたことが人間であることの証明になる。

1.2.2 DeepCAPTCHA

Osadchy らは敵対的サンプル (adversarial example) を用いた画像型 CAPTCHA を提案した [8]。敵対的サンプルは元画像にある摂動を加えることで機械に本来の意味とは異なる認識をさせるものを指す。DeepCAPTCHA は、この摂動をいくつか重ねることによって機械が誤認識する画像を生成し CAPTCHA に応用したものである。DeepCAPTCHA に使われている画像は、特定のタグに誤認識させるものとなっている。

1.2.3 Adversarial CAPTCHA

阿座上らは敵対的サンプルを用いた文字型 CAPTCHA である Adversarial CAPTCHA を提案した [9]。この CAPTCHA は、特定のタグに誤認識させるものではなく、どのような文字でも畳み込みニューラルネットワークが誤認識するような摂動を加えたサンプルを利用している。また、アモダグ補完を用いることで、機械による認識を困難にし、人間が認識しやすくなっている。

1.2.4 ランダム妨害図形を用いた CAPTCHA

田村らは文字認識攻撃に耐性を持つランダム妨害図形を用いた画像型 CAPTCHA を提案した [21]。この CAPTCHA は、画像にランダムな色や形の妨害図形を重ねて欠損を生じさせるもので、一般的な画像認識では正しく認識できないが、人間はアモダグ補完により画像を認識できるという特性を利用している。

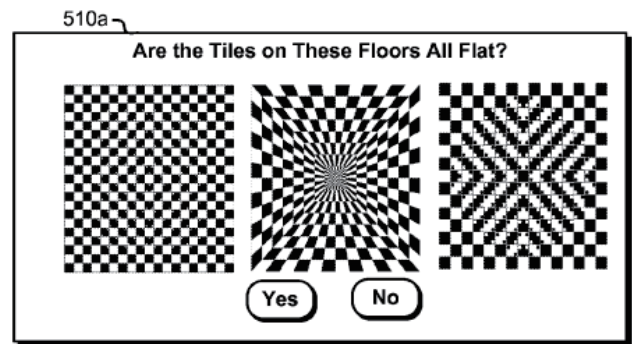


図 1 Turing test via failure の例 [7]

Fig. 1 An example of Turing test via failure [7].

1.2.5 本研究の位置付け

Turing test via failure では機械は錯視しないということが根底にあるが、文献 [10] において、動いているように見える静止画像について、人間の視覚情報を学習した人工知能も、人間と同様に動いていると誤って判断し、錯視が起きていることが明らかとなった。このことから、機械に対して、人間特有と思われた誤認識を機械に対して意図的に起こすことが可能であるため、Turing test via failure には脆弱性があると考えられる。

DeepCAPTCHA にて提案された摂動は、特定のモデルに対しては有効であるが、既存の画像認識システムにおいて同様の摂動が有効であるかは定かではない。また、Adversarial CAPTCHA は、アモダグ補完が使われているため、人間には認識しやすいとしているが、アルファベットの欠落部分や色合いによっては、見やすいとはいえないものも多い。ランダム妨害図形を用いた CAPTCHA においても、画像に図形を重ねるだけでは、配置の仕方、重ねる図形の形によって、人間にとって見やすいとはいえないものが生成される可能性がある。

これらの問題をふまえ、本稿では人間は容易に正しく認識できるが、既存の画像認識システムが誤認識する画像 (以降、加工画像と呼ぶ) の作成方法を提案する。また、この画像を応用した画像型 CAPTCHA を提案し、有用性、攻撃耐性の評価を行う。

1.3 本稿の構成

本稿の構成は次のとおりである。2章で、機械が誤認識する画像について整理し、加工画像の作成方法を述べる。3章では、加工画像を CAPTCHA として用いた場合の実用性、機械耐性について評価実験を行う。4章では加工画像がフィルタ処理にどの程度の耐性があるのかを検証する。5章でまとめと今後の課題を述べる。

2. 機械が錯視する画像

2.1 機械が誤認識する画像のモデル

文献 [8] において CAPTCHA に使用する敵対的サン

ルが満たすべき要件として4つがあげられている。

- (1) Adversarial: ノイズの追加によって機械が100%に近い値で誤認識を行う。
- (2) Robust: 画像に追加したノイズは計算上効率的な方法でも取り除くことはできない。
- (3) Perceptually Small: 追加されるノイズは人間による画像内容の認識を妨げない程度に小さい。
- (4) Efficient: 画像の生成に時間をかけず、1秒間に数百万ものチャレンジを発生させる。

この満たすべき要件には検討の余地がある。(1)において機械が100%に近い値で誤認識を行うとあるが、これは特定のモデルにおいて、どのような画像に対しても機械が誤認識をするという意味である。想定しているモデル以外では通用しない。(3)においてはノイズが少ない方が確かに人間は認識しやすいが、ノイズの量が多い場合でも認識できるかは考えておらず、これは、人間の視覚特性を考慮していない。そこで、上記の要件のうち(1), (3)を改変し、機械が誤認識する画像作成のための満たすべき要件をあげる。

- (1) Adversarial: ノイズの追加によって機械がどのようなモデルにおいても100%に近い値で誤認識を行う。
- (2) Robust: 画像に追加したノイズは計算上効率的な方法でも取り除くことはできない。
- (3) Perceptually: 人間の視覚特性を考慮し容易に正しく認識できる。
- (4) Efficient: 画像の生成に時間をかけない。

要件(1)の機械の例としては、以下に示す既存の画像認識システムがあげられる。

- Watson Visual Recognition [11]
- Google Vision API [12]
- Clarifai [13]
- Caption [14]
- Google 逆画像検索 [15]

これらのシステムは、入力画像の認識結果を信頼度付きのタグ、文章、単語で出力する。本稿では上記5つのシステムを対象として機械による認識評価を行う。

2.2 ハーフトーン処理

人間は認識できるが機械が誤認識する画像を作成するために、画像に多数の不連続点が含まれるようにすることが有効ではないかと仮説を立て、ハーフトーン処理の可能性について検討した。不連続点とは平面に対して画素値が急激に変化する画素のことであり、ハーフトーン処理とは限られた色数だけでグレースケールやカラーを表現する処理である。

予備実験

グレースケール画像を、ハーフトーン処理にて表現した画像を10種類ずつ用意し、既存の画像認識システムに認

識させた。結果は18%の確率で正しく認識した。また、誤認識した画像であってもハーフトーン処理を加えていると認識されるものが見られた。ハーフトーン処理が行われていると認識されることは、ハーフトーン処理の効果を取り除く攻撃の手がかりを与える恐れがある。よって、機械の認識精度が低く、加工の種類が容易に認識できない画像の生成が必要である。

2.3 不連続点を有する画像の生成

筆者らは、錯視をテーマとした油谷勝海氏の「隠れたMM」[16]に出会う機会を得た[17]。この作品を既存の画像認識システムに認識させたところ、すべてのシステムで誤認識し、処理の内容を表すような出力は見られなかった。そこで、この作品と同様に、多数の不連続点を画像に加えることによって、加工の種類が容易に認識できない画像が生成されるのではと推測した。不連続点を有する加工画像の作成のフローチャートを図2に示す。処理は以下の手順で行われる。

Step 1 (グレースケール変換) 入力された画像をグレースケールに変換する。

Step 2 (多値化処理) n 値化を行い情報量を削減する。

Step 3 (不連続点を構成する線の描画) 一定間隔で輝度0, 輝度255の線を画像に描画する。

図3に加工画像の作成例を示す。左が元画像、右が7値化による加工画像である。加工画像は、線の密度が高い箇所が暗く見え、密度が低い箇所が明るく見える。画像の情報量を落とし不連続点を描画しているため、加工画像は単にラスタノイズを付加したものではない。また、多値化処理の後に不連続点を構成する線を描画しているため、画像の画素ごとに処理を行うハーフトーン処理とも異なる。

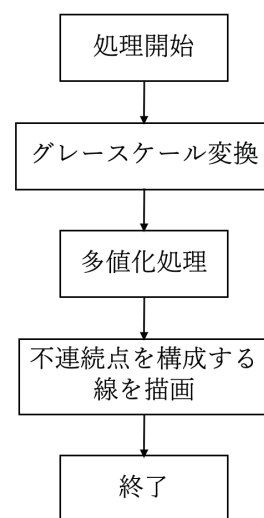


図2 画像の処理

Fig. 2 Processing of images.



図 4 元画像 [23]
Fig. 4 Original images [23].

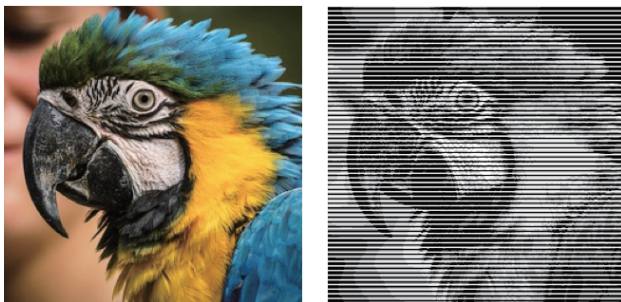


図 3 元画像 [23] (左) と加工画像 (右)
Fig. 3 Original image [23] (left) and processed image (right).

3. 機械が誤認識する CAPTCHA

3.1 実験目的

加工画像を用いた CAPTCHA の有用性について、人間の認識評価と機械による画像認識の2つの観点から検討する。

3.2 実験諸元

元画像とそれに対応する加工画像を 10 セット用意した。図 4 に元画像の一部を示し*1, 使用した画像の諸元を表 1 に示す。画像の処理にあたっては Python の画像処理ライブラリ Pillow を使用する。

評価実験 1 (人間の認識評価) では、加工画像 10 種類と各画像に対応する 10 単語を用いて実験を行った。評価実験 2 (機械による認識評価) では、元画像とそれに対応する加工画像を 10 セットを用いて実験を行った。

*1 このほかに人物画像等を利用している。

表 1 実験諸元

Table 1 Experimental specifications.

画像形式	PNG
画像サイズ	256 × 256
画像セット数	10



図 5 提案 CAPTCHA
Fig. 5 Proposed CAPTCHA.

3.3 評価実験 1: 人間の認識評価

3.3.1 評価内容

図 5 に示す CAPTCHA のプロトタイプを用いて、人間が加工画像を正しく認識できるか評価する。プロトタイプでは、ランダムに選択された 1 枚の加工画像とその画像に対して最適な 1 単語を含む 10 単語の選択肢が提示される。解答者は提示画像にあてはまる選択肢を解答する。この試行を 3 回繰り返す。評価では、10 代から 50 代までの被験者 30 人に対して問題の正誤、解答までにかかった時間を確認する。また、システムの有用性に関するアンケートを行った。このアンケートでは、システムのユーザビリティの評価指標の 1 つとして知られている System Usability Scale

表 2 評価結果の比較

Table 2 Comparison in images evaluation results.

	文献 [19]	文献 [20]	文献 [21]	文献 [8]	提案方式
平均正答率 (%)	66.7	92.86	97.85	82.57	100
平均解答時間 (秒)	9.8	12.63	6.37	7.89	4.65
最小解答時間 (秒)	4.9	-	-	-	2.59
最大解答時間 (秒)	13.5	-	-	-	7.43
解答時間の標準偏差	3.24	6.72	-	-	1.22
SUSスコア	-	-	-	-	82.3

(SUS) [18] を利用する。

比較対象として、以下の既存方式を取り上げる。

Deep CAPTCHA [8] 1.2.2 項で紹介した、敵対的サンプルを用いた画像型 CAPTCHA である。

SNOW NOISE CAPTCHA [19] グエンらによって提案された動画型の CAPTCHA である。この CAPTCHA はランダムなドットの背景画像を作成し、その上に正解となるパターンを 1 フレームごとに移動させ、解答者に正解パターンを発見させるものである。このパターンは各ドットが同じ方向に同じ距離だけ移動することから、人間はゲシュタルト知覚の共通運命の法則によって同じ方向に動くものを同じグループであると認識できるため 1 つのまとまりが動いているように知覚できる。

文字型 CAPTCHA [20] 文献 [20] にて比較対象として取り上げている文字型 CAPTCHA である。この CAPTCHA では、小文字アルファベット 26 種類からランダムに選ばれた 5~7 文字が赤、緑、青のいずれかの色で画面上に提示される。文字列には歪曲や部分的な消去等が施されている。解答者は画面上の文字列を認識し入力する。

ランダム妨害図形を用いた CAPTCHA [21] 1.2.4 項で紹介した、アモータル補完を用いた画像型 CAPTCHA である。

3.3.2 評価結果

人間の認識評価の結果を表 2 に示す。正答率は被験者ごとに出题に正しく解答できた割合である。また、解答時間とは、加工画像が表示されてから被験者がその画像に関する解答を終えるまでの 1 問あたりの解答時間を表し、標準偏差は不偏分散により計算している。ここに比較として列挙した数値は各論文からの引用であり実験環境は異なるものである。

提案方式では、全被験者が完全解答できており、他の CAPTCHA の正答率と同等である。また、被験者による解答時間のばらつきが少なく、かつ平均解答時間も 4.7 秒と短い。この結果より、被験者が加工画像に描かれたものを正しく容易に認識できていることが窺える。文献 [22] によると、SUS スコア 82.3 は等級スケール A (上位 10%) に相当することから、提案方式はユーザビリティにおいても

高評価が得られていることが分かる。

3.4 評価実験 2：機械による認識評価

3.4.1 評価内容

2.1 節にて示した画像認識システムを用いて、加工画像の認識状況について調査する。比較対象として、ランダム妨害図形を用いた画像型 CAPTCHA [21]、Deep CAPTCHA [8] を取り上げる。

3.4.2 評価結果

まず、オウムを元画像とする認識評価を行った。元画像、元画像をグレースケール変換した画像および対応する加工画像に対する各画像認識システムの認識結果を図 6 に示す。上段が元画像、中段がグレースケール変換画像、下段が加工画像である。元画像とグレースケール変換した画像の認識結果では、いずれの画像認識システムにおいても bird や parrot, animal 等のオウムを連想させるタグや記述がある。それに対して、加工画像の認識結果にはオウムに関連するタグや記述がまったく含まれていないことが分かる。ゆえに、オウムに関する加工画像は機械が誤認識しているといえる。

次に、オウム以外の加工画像について同様な認識評価を行った。元画像と対応する加工画像に対する各画像認識システムの認識成功率を表 3 に示す。認識成功とは、システムに画像を与えたときに画像の内容を表すいずれかのタグまたは単語を出力できることを表す。CaptionBot が 2 つの元画像を誤認識したが、その他のシステムはすべての元画像を正しく分類していた。一方、加工画像については、すべてのシステムで元画像の内容を表すタグまたは単語が出力されなかった。また、出力されたタグや単語のなかに、処理方法を表すようなものは見受けられなかった。

この評価実験では、異なる加工画像に対してシステムの出力結果が類似するという興味深い結果が得られた。たとえば、Watson Visual Recognition ではすべての画像の認識結果に screen というタグ、Google Vision API では Black というタグ、Clarifai では pattern というタグが出力された。このことから、加工画像の出力結果はある程度の一意性が期待でき、誤認識を誘発することができる。以上より、提案方法で作成した画像が既存の画像認識システムによる画像認識においても十分な耐性を有することを確認できた。

比較のために、文献 [21] で提案されたランダム妨害図形を用いた画像型 CAPTCHA の提示画像の認識結果を表 3 に含める。文献で使用された画像をそのまま用いて同様な検証を行うことができなかったため、文献に記載の数値を引用している。また、この数値は 2015 年時点での Google 逆画像検索での結果であり、他の画像検索システムあるいは現在の Google 逆画像検索では認識精度が向上している可能性がある。さらに、Deep CAPTCHA の論文に掲載さ

	Watson Visual Recognition	Google Vision API	Clarifai	CaptionBot	Google 逆画像検索
	bird animal greenish blue color parrot macaw	Bird Vertebrate Beak Macaw Parrot	bird parrot feather macaw zoo	I think it's a colorful bird perched on top of a parrot.	parrot
	black color bird animal bird of prey vulture	Bird Vertebrate Beak Bird Of Prey Eye	bird eagle animal feather wildlife	I think it's a close up of a bird.	parrot
	screen protective covering black color gray color Venetian blind	Line Monochrome Pattern Parallel Black-and-white	desktop texture pattern abstract wallpaper	I think it's a close up of a window.	monochrome

図 6 各オウム画像の認識結果
Fig. 6 Recognition result of each parrot image.

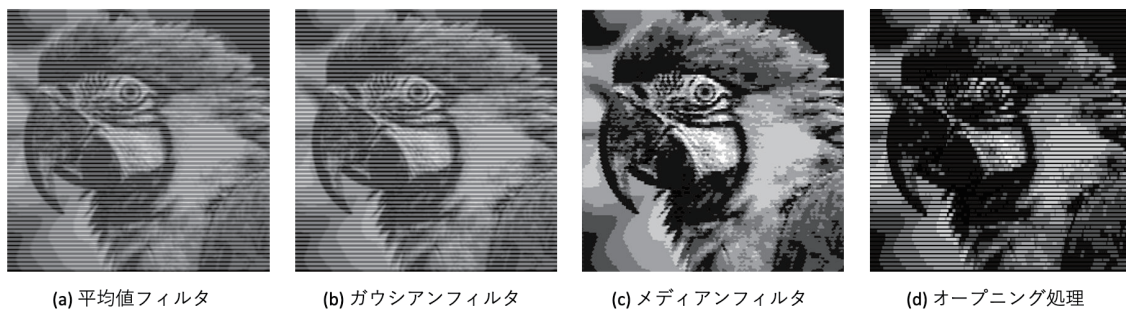


図 7 加工画像へのフィルタ適用
Fig. 7 Filtering on processed image.

表 3 元画像と加工画像に対する画像認識成功率
Table 3 Comparison in image recognition rates.

	文献 [21]	元画像	加工画像
Watson Visual Recognition	-	100%	0%
Google Vision API	-	100%	0%
Clarifai	-	100%	0%
CaptionBot	-	80%	0%
Google 逆画像検索	11.3%	100%	0%

れた画像の1つを既存の画像認識システムが正しく認識できるか検証したが、いずれのシステムでも画像内容が正しく認識されるという結果であった。

以上より、提案方法では、加工画像に含まれる多数の不連続点により、画像認識の精度が劣化し機械に誤認識を引き起こしていると推測される。と同時に、他の既存のCAPTCHAと比較して画像認識システムに対して誤認識を誘発させる可能性が高く、画像内容を分類するアノテ

ションサービスを利用した攻撃に対する耐性が高いことが期待できる。

4. 画像処理に対する耐性

機械による加工画像の誤認識を回避するために、加工画像に次のような画像処理を適用する攻撃が考えられる。

- 平均値フィルタ
 - ガウシアンフィルタ
 - メディアンフィルタ
 - モルフォロジー変換の1つであるオープニング処理
- 例として、オウム画像に各フィルタを適用して得られた画像を図7に示す。

作成した加工画像がどのような処理に対して耐性があるかを既存の画像認識システムを用いて評価する。使用する加工画像は3.4節の評価実験で用いたものである。各フィルタ適用後の既存の画像認識システムの認識状況（画像認識に成功した画像数と成功率）を表4に示す。

表 4 加工画像に対する画像処理攻撃の結果

Table 4 The results of filter attacks on processed images.

	平均値フィルタ	ガウシアンフィルタ	メディアンフィルタ	オープニング処理
Watson Visual Recognition	1	1	7	1
Google Vision API	1	0	6	3
Clarifai	0	0	5	0
CaptionBot	3	1	2	1
Google 逆画像検索	0	0	3	0
成功率	10%	4%	46%	10%

提案方法で作成した加工画像は、平均値フィルタ、ガウシアンフィルタ、オープニング処理という画像処理攻撃に対して耐性があることが確認できた。一方で、メディアンフィルタを利用した攻撃では、加工画像の認識成功率が5割弱である。これは、フィルタ処理により不連続点が補完されることで、一部の加工画像の認識精度が向上しているためと考察される。メディアンフィルタを利用した攻撃では、システムにより認識成功数に差が生じている。これにはシステムの出力の仕様（出力できるタグ数等）が影響している。

5. まとめと今後の課題

本稿では、機械は誤認識し、人間は正しく認識できる多数の不連続点を有する画像の新たな作成方法を考案した。画像に多数の不連続点を画像に加えることにより、認識精度が劣化し機械が誤認識を起こしやすくなった。この方法を応用した CAPTCHA は人間が答えやすく、扱いやすいものであり、既存の画像認識システムに対して強い耐性を有するものであることが確認できた。実験により、メディアンフィルタ等の不連続点を補完する処理を加えることにより、一部の画像の認識精度が向上することが分かった。

一方で、他の不連続点を生む画像の生成方法に対する提案方法の優位性や、他の画像処理よりも誤認識を誘発しやすくなっている理由が不明瞭である。これらの未解決である問題に取り組むとともに、機械学習による不連続点の補完処理を考慮した画像の生成方法の検討が今後の課題である。

謝辞 改訂にあたり大変有益な助言をくださった査読者および編集委員の皆様にお礼申し上げます。

参考文献

[1] von Ahn, L., Blum, M. and Langford, J.: Telling Humans and Computers Apart Automatically, *Comm. ACM*, Vol.47, No.2, pp.57–60 (2004).

[2] von Ahn, L., Maurer, B., McMillen, C., et al.: reCAPTCHA: Human-based character recognition via Web security measures, *Science*, Vol.321, No.5895, pp.1465–1468 (2008).

[3] The H Security: Google's reCAPTCHA briefly cracked, available from (<http://www.honline.com/security/news/>

item/Google-sreCAPTCHA-briefly-cracked-1586689.html) (accessed 2018-12-14).

[4] Sivakorn, S., Polakis, J. and Keromytis, A.D.: I'm not a human: Breaking the Google reCAPTCHA, *Black Hat Asia 2016* (2016).

[5] Bock, K., Patel, D., Hughey, G., et al.: unCaptcha: A Low-Resource Defeat of reCaptcha's Audio Challenge, *11th USENIX Workshop on Offensive Technologies WOOT 17* (2017).

[6] Dzieza, J.: Why CAPTCHAs have gotten so difficult, The Verge, available from (<https://www.theverge.com/2019/2/1/18205610/googlecaptcha-ai-robot-human-difficult-artificial-intelligence>) (accessed 2018-12-14).

[7] McInerney, M.J., Brighton, M.E. and Demirjin, S., et al.: Turing test via failure, United States Patent 9,767,263, 2017/9/19.

[8] Osadchy, M., Hernandez-Castro, J., Gibson, S., et al.: No Bot Expects the DeepCAPTCHA! Introducing Imutable Adversarial Examples with Applications to CAPTCHA, *IEEE Trans. Information Forensics and Security*, Vol.12, No.11, pp.2640–2653 (2017).

[9] 阿座上知香, 柴田千尋, 宇田隆哉: Adversarial CAPTCHA: 畳込みニューラルネットワークに耐性のある CAPTCHA の提案と評価. 情報処理学会論文誌, Vol.60, No.2, pp.680–695 (2019).

[10] Watanabe, E., Kitaoka, A., Sakamoto, K., et al.: Illusory Motion Reproduced by Deep Neural Networks Trained for Prediction, *Frontiers in Psychology*, Vol.9, No.345, DOI: 10.3389/fpsyg.2018.00345 (2018).

[11] IBM Corporation: Watson visual recognition, available from (<https://www.ibm.com/watson/services/visualrecognition/>) (accessed 2018-12-14).

[12] Google LLC: Vision API - image content analysis, available from (<https://cloud.google.com/vision/>) (accessed 2018-12-14).

[13] Clarifai Inc.: Computer Vision AI demo, available from (<https://www.clarifai.com/demo>) (accessed 2018-12-14).

[14] Microsoft Corporation: CaptionBot — For pictures worth the thousand words, available from (<https://www.captionbot.ai/>) (accessed 2018-12-14).

[15] Google LLC: Google images, available from (<https://images.google.com/>) (accessed 2018-12-14).

[16] 種村季弘 (編): 図説アイ・トリック (ふくろうの本), 油谷勝海: 隠れた MM, p.86, 河出書房新社 (2001).

[17] 原 亨, 佐藤 敬: Stripe CAPTCHA: ゲシュタルト知覚に基づく画像認証, 2019 年暗号と情報セキュリティシンポジウム (SCIS 2019) 予稿集 (2019).

[18] Brooke, J.: SUS: A quick and dirty usability scale, *Usability Evaluation in Industry*, pp.189–194, Taylor Francis (1996).

[19] グエンスアンギア, 藤田真浩, 池谷勇樹ほか: SNOW NOISE CAPTCHA: 無意味な情報を利用した動画

- CAPTCHA の提案, 情報処理学会研究報告マルチメディア通信と分散処理 (DPS), Vol.2014-DPS-158, No.29, pp.1–7 (2014).
- [20] 可見潤也, 鈴木徳一郎, 上原章敬ほか: 4 コマ漫画 CAPTCHA, 情報処理学会論文誌, Vol.54, No.9, pp.2232–2243 (2014).
- [21] 田村拓己, 久保田真一郎, 油田健太郎ほか: 文字認識攻撃に耐性を持つランダム妨害図形を用いた画像ベース CAPTCHA 方式の提案, 情報処理学会論文誌, Vol.56, No.3, pp.808–818 (2015).
- [22] Bangor, A., Kortum, P.T. and Miller, J.T.: Determining what individual SUS scores mean: Adding an adjective rating scale, *Journal of Usability Studies*, Vol.4, No.3, pp.114–123 (2009).
- [23] Pixabay GmbH: Pixabay, available from (<https://pixabay.com>) (accessed 2018-12-14).



原 亨

2019年北九州市立大学国際環境工学部情報メディア工学科卒業。同大学大学院国際環境工学研究科博士前期課程在学中。情報セキュリティに関する研究に従事。



佐藤 敬 (正会員)

1991年東京工業大学工学部電気・電子工学科卒業。1993年同大学大学院理工学研究科修士課程電気・電子工学専攻修了。1994年同研究科博士後期課程中退。同年同大学工学部助手。1999年北九州市立大学国際環境工学部設置準備室講師。2001年北九州市立大学国際環境工学部助教授。2007年同准教授。2014年同教授。現在に至る。博士(工学)。数理工学全般, 特にセキュリティ, 情報システム等に関する研究に従事。電子情報通信学会, 情報処理学会, ACM, IEEE 各会員。