モバイル端末向けCAPTCHAのハフ変換を用いたボットへの耐性評価

モバイル端末向けCAPTCHAのハフ変換を用いたボットへの耐性評価

竹口　真理亜 [a)]・梁井　孝治 [b)]・山場　久昭 [c)]・油田　健太郎 [d)]・岡崎　直宣 [e)]

Evaluation of CAPTCHA for Mobile Devices against Bots Using Hough Transform

Maria TAKEGUCHI, Takaharu YANAI, Hisaaki YAMABA, Kentaro ABURADA, Naonobu OKAZAKI

Abstract

In recent years, CAPTCHAs (Completely Automated Public Turing test to tell Computers and Humans Apart) have been introduced on many Web sites.It is a discrimination method based on a Turing test that identifies humans and automatic programs called bots, and is used to prevent fraudulent acts on Web services. In particular, it is becoming necessary to design a CAPTCHA that is easy to use on mobile devices. In this laboratory, Mizuta et al. have proposed a CAPTCHA for mobile devices that is resistant to bots using object tracking technology. It makes the object recognition by the program difficult by changing the transparency of the tracked object every time, and the effectiveness is shown. However, it has only been confirmed that the bot resistance is resistant to the meanShift that tracks objects in the video. In this paper, we conducted an experiment to investigate the resistance to attack techniques using Hough transform. The Hough transform is one of the most commonly used methods to detect figures such as straight lines and circles from images, and is considered to be an effective means of attacking CAPTCHA by Mizuta et al. After implementing an attack program, experiments and investigations confirmed that it was not resistant. Based on the survey results, we proposed two improvement plans to improve bot resistance.

Keywords: CAPTCHA, Dynamic CAPTCHA, Bot, Hough Transform, Mobile devices

1. はじめに

近年、多くの Web サイトに CAPTCHA(Completely Automated Public Turing test to tell Computers and Humans Apart)[1] が導入されている。CAPTCHA は、人間とボットと呼ばれる自動プログラムを識別するチューリングテストによる判別手法であり、Web サービスに対する不正行為を防ぐために用いられる。例えば、ボットを用いてアカウントの大量取得を行うなどの不正行為が増えてきており、CAPTCHA の重要性も増してきている。

特に、モバイル端末で利用しやすい CAPTCHA の設計が必要となってきている。2017 年には、スマートフォンなどのモバイル端末の世帯保有率は 94.8%[2] と非常に高くなっており、Web サービスにアクセスするためによく利用されている。しかしキーボードやマウスの存在を前提とした CAPTCHA が多いため、モバイル端末では回答が難しいことが多い。しかも攻撃の高度化に対抗するため、画像 CAPTCHA や文字列 CAPTCHA などでは、大きなノイズや歪みを導入するようになり、人間の解読も困難になりつつある。特にスマートフォンなどの小さな画面では、解読が困難になってしまう [3]。これは、Web サイトの登録フォームのコンバージョン率の低下などにもつながるので、モバイル端末向けの CAPTCHA は重要になっている。

本研究室では、水田らによってモバイル端末での利便性を保った画像 CAPTCHA （以下、水田らの CAPTCHA と呼ぶ。図 1) が提案されており [4)5)]、その有用性が示されている。

しかしボット耐性は、meanShift 法に耐性を持つことしか確認できていないため、本研究では、ハフ変換を用いた攻撃手法に対する耐性を調べる。具体的には、攻撃用プログラムを実装したうえで実験・調査し、耐性を持たないことを確認したので報告する。

以下、本概要の構成を述べる。第 2 節では水田らの CAPTCHA について説明し、第 3 節ではハフ変換を用いた攻撃手法について説明する。第 4 節ではボット耐性の調査を行った結果を、第 5 節ではボット耐性を向上させるための改良案を述べる。第 6 節ではまとめと今後の課題について述べる。

2. モバイル端末向け CAPTCHA

水田らの提案した CAPTCHA[4)5)] について以下に示す。

2.1 提案された CAPTCHA 方式

この CAPTCHA は、色、形、大きさが同じ移動オブジェクトを複数用意し、その中に 1 つだけ含まれる追跡対象を一定時間以上追跡できるか否かで人間か機械かを判別する。ボット耐性が高くなることを期待し、追跡対象オブジェクトをあらかじめ決ておくのではなく、CAPTCHA を解く際にユーザ

[a)] 工学専攻機械・情報系コース大学院生
[b)] 情報システム工学科学部生
[c)] 情報システム工学科助教
[d)] 情報システム工学科准教授
[e)] 情報システム工学科教授

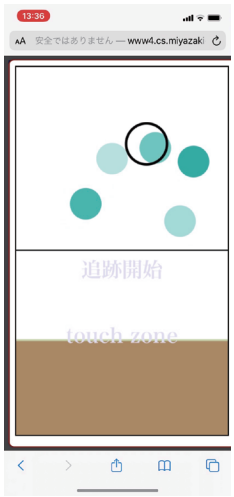


図 1. モバイル端末向け CAPTCHA[4)]

が選ぶものとしている。

物体追跡技術などを用いたボットへの耐性を持たせるため、ランダムに各オブジェクトの透明度が時間ごとに変化させるようにして、プログラムによる物体認識が困難になるようにしている。しかし、人間にとっては、オブジェクトの移動が連続的であるため色が変化しても、追跡が可能であると考えられる。

CAPTCHA の画面は、オブジェクトの表示領域と指での操作領域の 2 つに上下で分けられている。画面上部ではオブジェクトがランダムに移動してる。画面下部の “touch zone” と表示されている操作領域に指を置くと、オブジェクトの表示領域に追跡用のサークルが出現する。ユーザは touch zone 内で指をスライドさせ、その追跡用サークルを動かし、移動オブジェクトを追うことで、オブジェクトの追跡を行う。

追跡対象の選択はユーザが行う。ユーザが選んだオブジェクトがどれであるのかを CAPTCHA に伝える必要があるが、それは、そのオブジェクトの円の中心座標を追跡用サークルの円内に連続で 1 秒以上入れることで行う。

CAPTCHA が追跡対象を認識してから 10 秒の間に、追跡できていた秒数（以下、追跡成功時間とする。）を、人間か機械かの判断基準に用いる。この追跡成功時間が、設定した閾値よりも長ければ人間、短ければ機械と判断する。

オブジェクトを追跡に成功しているか否かの判断基準は、移動オブジェクトの円の中心座標が、追跡用サークルの円内に入っているか否かである。中心座標が入っていれば、追跡できているとみなし、入っていなければ、追跡できていない状態とみなす。

2.2 認証手順

水田らの CAPTCHA の認証手順を図 2 に示す。CAPTCHA のプログラムが動作を始めると、初期画面（図 3-(a)）が表示される。画面中のオレンジの開始ボタン（「I’m not a robot」と書かれている）をタップすると、追跡開始画面（図 3-(b)）に移行し、CAPTCHA へのチャレンジが始まる。ユーザが追跡オブジェクトを選択し、追跡が開始されてから 10 秒が経過すると追跡終了画面（図 3-(c)）へと移行し、人間か機械化の判定を行い終了となる。

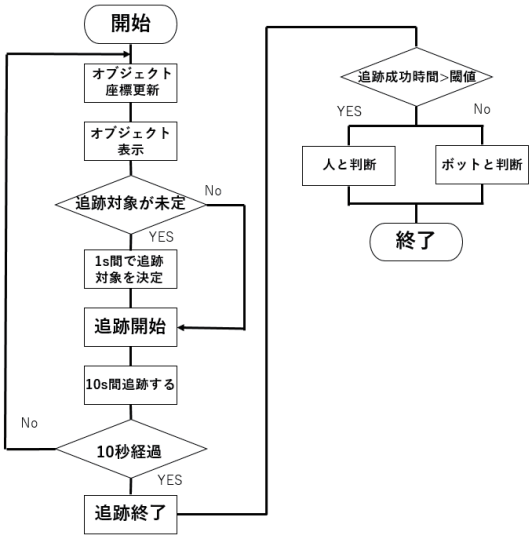
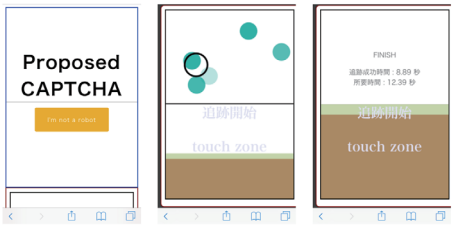


図 2. 提案された手法のフローチャート [4)]



（a）初期画面　（b）追跡開始　（c）追跡終了

図 3. 提案された CAPTCHA の構成 [4)]

2.3 モバイル端末での利便性

水田らの CAPTCHA は、文献 [6)] におけるモバイル端末での CAPTCHA のガイドラインを満たしている。文献 [6)] における、モバイル端末での CAPTCHA の推奨設計によると、「CAPTCHA の解答方式がタップやスワイプなどに依存するよう設計する必要がある。」としているが、オブジェクトの追跡は、タッチパネル上で指を滑らせる動作で実現されている。

2.4 ボット耐性

動画内の物体を追跡する方法に meanShift 法がある。meanShift 法は、画像中の画素の分布密度や、画素数が最大になる領域を探すアルゴリズムである。

水田らの CAPTCHA が、meanShift 法を用いたボットに対して耐性を持つことはすでに確認されている [4)]。meanShift 法は画像中の画素値によって物体を追跡するアルゴリズムであるため、水田らの CAPTCHA のような、オブジェクトが透明度を変えながら移動し、また、互いに交差するようなことが起きると、追跡対象のオブジェクトを追跡し続けるのは困難である。

しかし、水田らの CAPTCHA は他の手法に対する耐性は確認できていない。

3. ハフ変換を用いたボット

本研究では、水田らの CAPTCHA がハフ変換を用いたボットへ耐性を持つか否かを調査する。

3.1 ハフ変換

ハフ変換は、画像の中から直線や円などの図形を検出したい際によく用いられる手法の一つであり、水田らの CAPTCHA へ

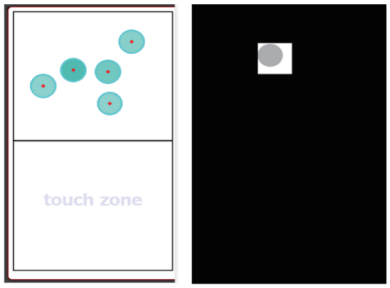


図 4. ハフ変換による円の検出

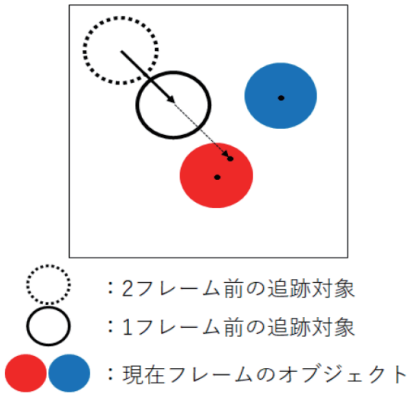


図 5. 移動ベクトルによる追跡対象の選択

の攻撃手段として有効だと考えられる。水田らの CAPTCHA は各オブジェクトの色の透明度が変化し、交差することでボットによる追跡を困難にしているが、ハフ変換による円の検出には、オブジェクトの透明度は影響しないのがその理由である。

3.2 ハフ変換を用いたオブジェクトの追跡

ハフ変換を用いて円形の物体の検出を行うと、移動オブジェクトは円形であるので図 4-(a) に示すように検出が可能である。ただし水田らの CAPTCHA を解くには、そのうちの 1 つを追跡対象として選び、それを追跡し続けなければならない。本研究では、追跡対象は 1 番目に検出されたオブジェクトとする。しかし、それ以降のフレームにおいて、検出される複数の円の中から同じオブジェクトを特定することは容易ではない。

そこで図 4-(b) に示すように、直前のフレームでの追跡対象のオブジェクト周辺をマスク処理によって覆い隠すことで、検出されるのが追跡対象だけになるようにする。そしてマスク処理を行った画像に対して、ハフ変換による円の検出を行い、そのオブジェクトを追跡対象とする。

次に、複数のオブジェクトが検出されてしまった場合の追跡対象の選択方法を図 5 を用いて説明する。(1) 2 フレーム前と 1 フレーム前の追跡対象の中心座標から移動ベクトルを計算し、(2) 1 フレーム前の追跡対象の中心座標に、求めた移動ベクトルを足した位置を得て、(3) この位置に中心座標が最も近いオブジェクトを選択する。図 5 の例では、赤色のオブジェクトが追跡対象になる。

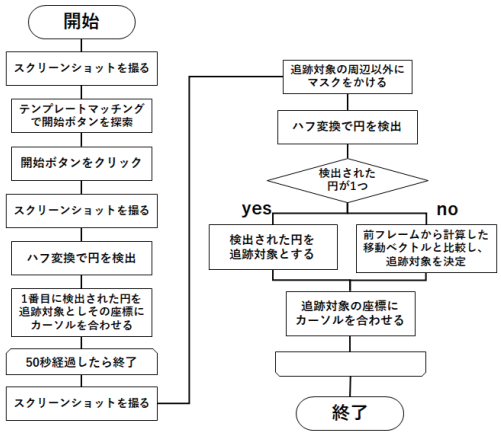


図 6. 実装したボットのフローチャート

3.3 攻撃手順

設計したボットが CAPTCHA を解く手順を図 6 に示す。ボットプログラムが動作を始めると、ボットは CAPTCHA 画面のスクリーンショットを撮り、テンプレートマッチングにより画面中のボタン「I'm not a robot」を探索し、その座標をクリックし CAPTCHA を開始させる。

再び、ボットは CAPTCHA 画面のスクリーンショットを撮り 3.2 の方法で追跡オブジェクトを認識し、追跡対象を選び、そのオブジェクトの座標にカーソルを合わせる。

追跡対象を選択した後、ボットは CAPTCHA 画面のスクリーンショットを撮り、3.2 の方法でマスク処理と追跡オブジェクトの認識を行い、そのオブジェクトの座標にカーソルを合わせる。以上を繰り返し 1 つのオブジェクトを追跡し続ける。

3.4 実装

開発言語は Python を、画像処理ライブラリは OpenCV を用い、Windows10 上でハフ変換を用いたボットを実装した。

4. ボット耐性についての実験

4.1 実験目的

ハフ変換を用いたボットが、水田らの CAPTCHA を自動的に突破することが可能であるかを確認するための実験を行った。ここでは、設定した閾値以上の時間、ボットが追跡を継続できれば突破可能であるものとする。

4.2 実験方法

実験は、モバイル端末のブラウザではなく、Windows10 のデスクトップ環境で、Chrome のデベロッパーツールを用いてモバイル端末の Web ブラウザをエミュレートして行う。水田らの CAPTCHA に対して 100 回ずつ攻撃を行い、追跡成功時間と所要時間 (追跡成功時間) の計測を行った。攻撃には 3 節で実装したボットを使用した。CAPTCHA の移動オブジェクトの数を 5,10,15 個の 3 種類、閾値を 7,8,9 秒の 3 種類とし、その組み合わせの 9 通りの条件で実験を行った。このように設定したのは、水田らがこの条件で meanShift 法での実験を行っていたからである。

ボットによる CAPTCHA 突破率は、各 CAPTCHA を 100 回攻撃したうち、追跡成功時間が閾値以上になった回数の割

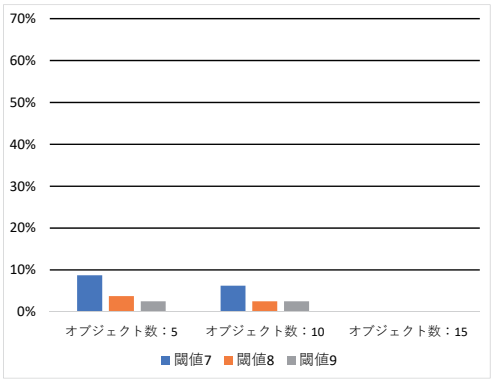


図 7. meanShift 法を用いたボットの CAPTCHA 突破率 [4)]

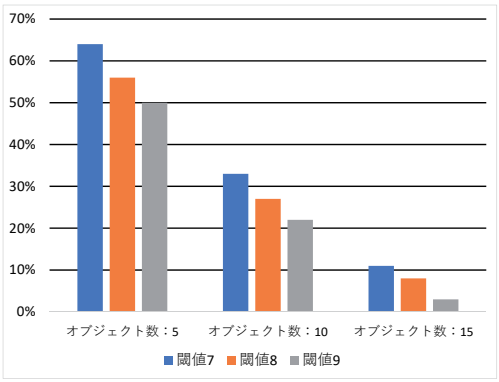


図 8. ハフ変換を用いたボットの CAPTCHA 突破率

合である。

4.3 実験結果と考察

実験の結果、水田らの CAPTCHA はハフ変換を用いたボットに対して、脆弱であることがわかった。meanShift 法用いたボットとハフ変換を用いたボットの CAPTCHA 突破率を、それぞれ図 7、図 8 に示す。meanShift 法では、すべてのオブジェクト数、閾値の組み合わせにおいて突破率は 10%を下回っている。一方ハフ変換を用いたボットでは、すべてのオブジェクト数、閾値の組み合わせにおいて meanShift 法よりも高い突破率となった。

このような結果となった理由としては、水田らの CAPTCHA の持つ特徴が、meanSift 法の弱点を突くものであったのに対し、ハフ変換を用いる手法には優位に働かなかったからだと考えられる。具体的には、第一に meanShift 法では CAPTCHA がオブジェクトが一定時間で透明度を変えるものであるために、ある一定の透明度を下回ると、ボットがオブジェクトを認識できなくなることがある。第二に、オブジェクト同士が交差した場合、複数のオブジェクトであると判断できなくなることが考えられる。

ハフ変換を用いたボットでは、円としてオブジェクト 1 つ 1 つを別に検出することができるため、透明度によってオブジェクトが認識できないということがなく、オブジェクト同士の交差にも対応することができたからだと考えられる。

以上の結果から、水田らの提案した CAPTCHA のボットに対する耐性は不十分であると考えられる。

5. ボット耐性向上のための改良案

ボット耐性を向上させるための改良案についての考察を以下に示す。

5.1 オブジェクトの変形

提案された CAPTCHA では、オブジェクトの形が常に円形で検出が容易であった。そこで、オブジェクトの透明度だけでなく形もランダムに変化させることでボットに対する耐性が向上するのではないかと期待できる。しかし、常に円形であったものをランダムに変形させるというのは、CAPTCHA に歪みを加える行為であり、ユーザビリティの低下を招いてしまう懸念がある。

5.2 追跡対象の限定

水田らの CAPTCHA では、表示されているオブジェクトの中から任意の 1 つを選ぶことができるが、ハフ変換を用いたボットに対してそれは不利に働いてしまう。そこで、追跡対象をあらかじめ CAPTCHA 側で決めておき、ほかのオブジェクトを妨害オブジェクトとすることでボット耐性が向上すると期待できる。追跡対象となるオブジェクトは、オブジェクトを点滅させるなどほかの妨害オブジェクトとは違った挙動をさせる。あらかじめ CAPTCHA 側が追跡対象を決めておくことにより、1 秒間の追跡対象を決定するための時間が無くなるため、ユーザビリティの向上にもつながると考えられる。

6. まとめ

本研究では、ハフ変換を用いた攻撃手法に対する水田らの CAPTCHA の耐性を攻撃用プログラムを実装したうえで実験・調査し、耐性を持たないことを確認した。実験の結果、水田らの提案した CAPTCHA が meanShift 法を用いたボットよりもハフ変換を用いたボットに対して脆弱であることが分かった。同時に、提案された CAPTCHA のボットに対する耐性は不十分であると考えられる。

今後は、提案された CAPTCHA のハフ変換による攻撃手法への耐性向上のためにシステムを改善する必要がある。また、提案された CAPTCHA は動的 CAPTCHA であるため、年代別のユーザビリティに関する調査が必要であり、多くの人間が使いやすいシステムに改善していかなければならない。

参考文献

1) L. V. Ahn, M. Blum, N. Hopper, and J. Langford: CAPTCHA: Telling humans and computers apart,Lecture Notes in Computer Science, Vol.2656, pp.294-311, 2003.

2) https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h30/html/nd252110.html, (2020/1/30 閲覧)

3) M. Guerar, A. Merlo, M. Migliardi, and F. Palmieri: Invisible CAPPCHA: A usable mechanism to distinguish between malware and humans on the mobile IoT,Computers & Security, Vol.78, pp.255-266, 2018.

4) 藤　竜成, 水田　陸, 山場　久昭, 油田　健太郎, 岡崎　直宣: モバイル端末向けの動的 CAPTCHA の検討と追跡技術を用いたボット耐性の検証, 宮崎大学工学部紀要（48）,pp.257-262,2019.

5) Kentaro Aburada, Shotaro Usuzaki, Hisaaki Yamaba, Tetsuro Katayama, Masayuki Mukunoki, Mirang Park, Naonobu Okazaki: Implementation of CAPTCHA suitable for mobile devices, IEICE Communications Express,Vol.8,pp.601-605,2019.

6) N. Jiang, H. Dogan and F. Tian: Designing Mobile Friendly CAPTCHAs: An Exploratory Study, Proceedings of British HCI 2017,pp.1-7,2017.