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

藤　竜成[a)]・水田 陸[b)]・山場　久昭[c)]・油田　健太郎[d)]・岡崎　直宣[e)]

Examination of Dynamic CAPTCHA for Mobile Devices and Verification of Bot Tolerance Using Tracking Technology

Ryusei FUJI, Riku MIZUTA, Hisaaki YAMABA, Kentaro ABURADA, Naonobu OKAZAKI

Abstract

In recent years, illegal activities such as acquiring a large amount of web service accounts by using an automatic program called a bot have been problems. In order to prevent such activities, a discrimination method based on the Turing test for identifying a human and a bot called CAPTCHA was developed. Also, mobile devices such as smartphones have appeared and are often used to access web services. However, many of the existing CAPTCHA methods can't be adapted well to mobile devices, which is a cause of the decline in the success rate of the account registration of the web service. Therefore, it is necessary to design a CAPTCHA which is easy to use in mobile devices. In this paper, we propose a new CAPTCHA scheme that maintains convenience in mobile devices and has bot tolerance. In proposed method, several objects move randomly and continuously. One of the objects selected by the user from among several objects is set as a tracking target. According to the time that the users can track the target with their finger, the proposed system determines whether the users are humans or bots. In our proposed method, the transparency of color and the degree of change of transparency for each object are set at random, and by changing the transparency of the object as time proceeds, the method can withstand the bots that perform fraudulent activities using object tracking technology.

Keywords: dynamic CAPTCHA, mobile device, bot, game CAPTCHA, transparency of color

1. はじめに

近年、Web サービスに対してボットと呼ばれる自動プログラム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問題となっている。このような問題を防止するために CAPTCHA と呼ばれる人間とボットを識別するチューリングテストによる判別手法が開発された。また、スマートフォンなどのモバイルデバイスが登場し、Web サービスにアクセスするためによく利用されている。既存の CAPTCHA 方式の多くはモバイルデバイスにうまく適合できず、Web サイトの登録フォームなどのコンバージョン率の低下の原因となっている。そのため、モバイルデバイスで利用しやすい CAPTCHA の設計が必要である。本論文では、モバイルデバイスでの利便性を保ち、ボット耐性を持たせた新たな CAPTCHA 方式を検討する。提案方式は動的な CAPTCHA であり、ランダムかつ連続的に移動するオブジェクトを複数個用意している。その中からユーザが最初に選んだもの 1 つを追跡対象とし、一定時間以上指で追跡できるか否かで人間か機械かを判別する。この CAPTCHA 方式では、オブジェクトそれぞれに色の透明度と透明度の変化の度合いをランダムに設定し、オブジェクトの透明度を時間ごとに変化させることで、物体追跡技術などを用いたボットへの耐性を持たせている。また、人間は、変化の度合いとオブジェクトの軌跡で追跡対象を認識できると考える。

[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

2. 先行研究

2.1 リレーアタック耐性と BOT 耐性の両立を目指したインタラクティブな動画 CAPTCHA

先行研究において、立田らは、ランダムに位置を変える複数のオブジェクト (以降、妨害オブジェクトとする) の中から、連続的に移動するオブジェクト (以降、移動オブジェクトとする) をマウスカーソルで一定時間以上追跡する動画型の CAPTCHA[1)] を提案した。

立田らの CAPTCHA 方式では、妨害オブジェクトの視覚的特徴 (色、形、大きさ) が移動オブジェクトと全く同じであるため、ボットが CAPTCHA を突破しようとする場合、フレーム画像を解析しようとしても、視覚的特徴が同じオブジェクトが複数個所に存在しているように見え、移動オブジェクトを検出することは困難であった。人間の場合、連続して見ることで移動オブジェクトを見つけることは容易であるため、CAPTCHA として成立する。

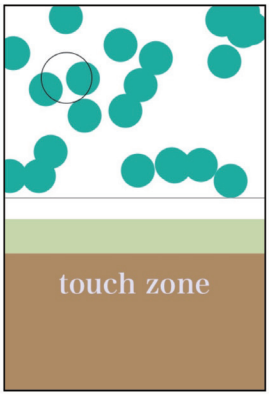


図 1. 妨害オブジェクトの中から移動オブジェクトを追跡するモバイルデバイス向け CAPTCHA[2)]

2.2 モバイルデバイスの利用に適した CAPTCHA

この CAPTCHA 方式[2)] は、前述の動画 CAPTCHA[1)] をモバイルデバイスでの利用に適した形に変更している (図 1)。主な変更点としては、タッチパネル上で指を滑らせる仕様にした点と、画面をオブジェクト表示領域と操作領域の上下 2 つに分割している点である。これは、移動オブジェクトを直接指で追跡する方式にした場合、指に隠れて移動オブジェクトが見えなくなるなどの問題を避けるためである。操作領域に指を置くことで、オブジェクト表示領域の連動した位置に追跡用サークルを表示する。追跡用サークル内に移動オブジェクトを入れ続けることができるか否かでユーザが人間か機械かを判断する。

提案されていた論文では、ボット耐性を保持しているかを検証しておらず、セキュリティは保証されていない。1 つしかない移動オブジェクトの位置を特定された場合、ボットに追跡される可能性がある。

上記の 2 つの CAPTCHA 方式は、どちらも妨害オブジェクトが短時間に点滅しているように見え、光過敏性発作を引き起こす可能性がある。ユーザビリティの観点から変更の必要があると考える。

3. 提案手法

本研究では、モバイルデバイスでの利便性を保ち、ボット耐性を持たせた新たな CAPTCHA 方式を作成することを目的とする。

2. 章で述べたように、文献 [1)] と文献 [2)] の CAPTCHA は、移動オブジェクトが 1 つであるため、位置を特定されるとボットに追跡されてしまう可能性がある。CAPTCHA としての十分な堅牢性とモバイルデバイスでの利便性を両立するためには、新たな方式の CAPTCHA を考える必要がある。モバイルデバイスでの利便性を保つために、先行研究の操作領域部分は変更せず、表示するオブジェクトを変更する。

3.1 提案する CAPTCHA 方式

提案する CAPTCHA 方式では、先行研究の妨害オブジェクトを消去し、色、形、大きさが同じ移動オブジェクトを複数個用意した。複数のオブジェクトから、ユーザが最初に選んだもの 1 つを追跡対象とし、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。オブジェクトそれぞれに色の透明度と透明度の変化の度合いをランダムに設定し、オブジェクトの透明度を時間ごとに変化させることで、物体追跡技術などを用いたボットへの耐性を持たせている。人間の場合は、変化の度合いとオブジェクトの軌跡で追跡対象を認識できると考える。

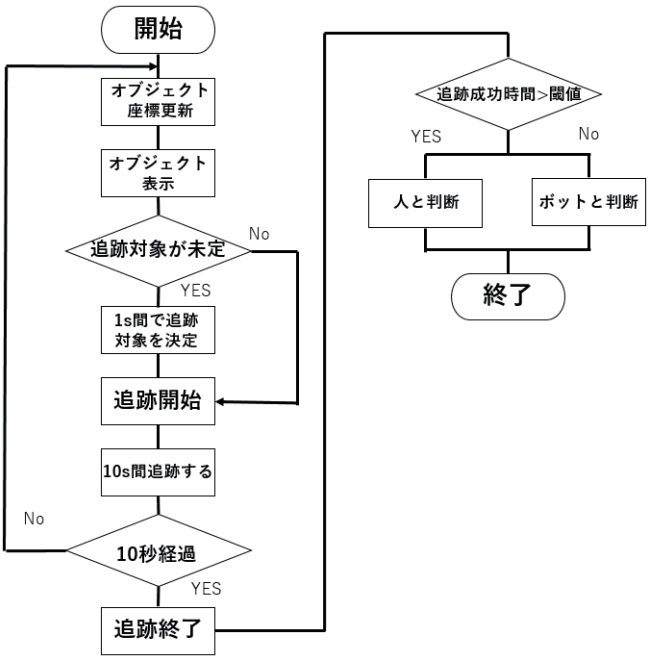


図 2. 提案手法のフローチャート

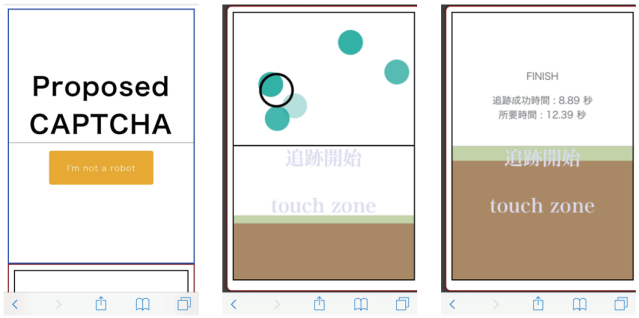
3.2 認証手順

提案する 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。画面中のボタン「I'm not a robot」をタップすると、追跡開始画面 (同図-(b)) に移行し、移動オブジェクトが複数個表示される。この段階で、モバイルデバイスの画面では、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。“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、追跡中の状態とする。追跡中の判断基準は、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。追跡対象が入っていれば、追跡中とみなし、入っていなければ、追跡中でない状態とみなす。

どれか 1 つ、任意の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合計で 1 秒以上入ることで、システムは追跡対象を認識する。追跡対象を認識してから 10 秒計測し、その間に何秒、追跡中となっていたか（以下、追跡成功時間とする。）を人間か機械かの判断基準とする。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。

3.3 モバイルデバイスでの利便性

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可能である。文献 [3)] における、モバイルデバイスで



（a）初期画面　（b）追跡開始　（c）追跡終了

図 3. 提案する CAPTCHA の構成

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。提案 CAPTCHA は、文献 [3] のガイドラインを満たす、また、先行研究の CAPTCHA で短時間に点滅していた妨害オブジェクトを削除したことで、提案 CAPTCHA は人間の目に負担が少ない方式になっている。

3.4　提案手法のセキュリティについて

2 章で説明した先行研究の CAPTCHA は、移動オブジェクトが 1 つであるため、その位置が特定された場合、ボットによって追跡される可能性があった。提案手法は、色、形、大きさは同じ移動オブジェクトを複数用意し、それぞれが色の透明度を変えながら、時に交差しながらランダムに動くという形式を実装している。そのため、攻撃者がフレーム画像を取得し解析しようとしても、各フレーム画像は、透明度以外の視覚的特徴が同じオブジェクトが複数存在しているようにしか見えず、透明度を変えながら交差する移動オブジェクトを追跡することは困難であると考える。

4.　実験と考察

提案 CAPTCHA の実用性についての実験と、ボット耐性についての調査を目的とした実験を行う。

4.1　実用性についての実験

4.1.1　実験目的

3. 章で提案した CAPTCHA が、ユーザ（人間）による解答が可能なものか確認する。また、実験参加者に対してアンケート調査を行い、提案手法の有用性について検証する。

4.1.2　実験方法

実験は、宮崎大学工学部生 17 名が参加した。実験参加者には、モバイルデバイス (今回は iPhone 8) を利用して、移動オブジェクトの数を 5 個、10 個、15 個と設定した 3 つの提案 CAPTCHA(1、2、3) を 5 回ずつ解いてもらい、追跡成功時間と所要時間 (追跡開始までの時間) の計測を行った。また、先行研究の CAPTCHA と比較を行うため、同様に 5 回ずつ解いてもらった。

実験後、提案手法について、ユーザビリティに関するアンケートを記入してもらう。

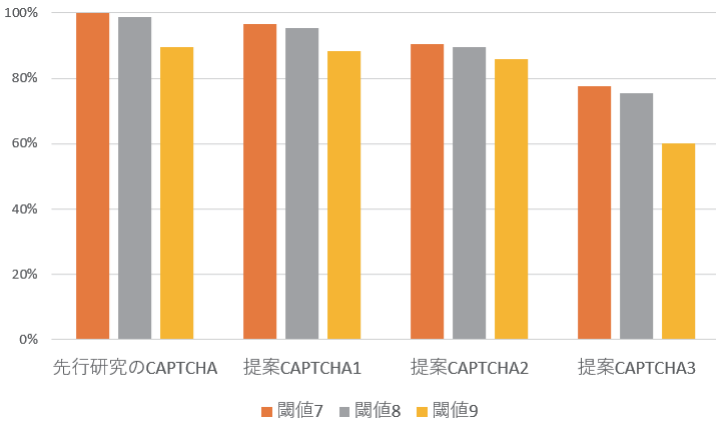


図 4. 成功率

表 1. 追跡開始までの時間

	最長時間	最短時間	平均時間
先行研究 CAPTCHA	4.89	0.39	1.52
提案 CAPTCHA1	7.09	1.59	2.83
提案 CAPTCHA2	7.49	1.79	2.93
提案 CAPTCHA3	12.80	1.49	3.24

4.1.3　実験結果と考察

成功率　成功率は、各実験を 5 回ずつ行ったうち、追跡成功時間が閾値以上になった回数の割合である。

先行研究の CAPTCHA では追跡成功時間の閾値を 7 秒に設定していたが、提案手法では、適切な閾値を調査するために閾値を 7〜9 秒に設定して比較を行った。

図 4 に各 CAPTCHA の成功率の結果を示す。どの閾値に設定しても先行研究の CAPTCHA の成功率は高く、それに次いで提案 CAPTCHA1、2、3 と続く結果となった。閾値が 7 秒と 8 秒を比較すると、成功率は大きく変化しない。しかし、閾値が 9 秒の場合は、どの CAPTCHA も成功率が著しく低下する。特に提案 CAPTCHA3 は、成功率が 6 割ほどになっており、実用性は難しいと考える。しかし、提案 CAPTCHA の 1 と 2 の成功率は、閾値 9 の場合、約 9 割となっており、先行研究の CAPTCHA と近しくなっている。成功率だけを見ると、十分実用性があると考える。

追跡開始までの時間　所要時間は、実験参加者が CAPTCHA を開始してから終了するまで掛かった時間のことである。先行研究の CAPTCHA と提案手法は、追跡の計測時間は同じ 10 秒であるため、所要時間から 10 秒引いた追跡開始までの時間を比較する。各 CAPTCHA の追跡開始までの時間を、表 1 にまとめた。

この結果から、先行研究の CAPTCHA は、0.3〜4.9 秒以内に収まっていることがわかる。提案 CAPTCHA1 は最短で 1.5 秒で終了しているが、最長で約 7 秒掛かっており、追跡対象を定めるまでの時間に若干の個人差があると考える。それぞれの CAPTCHA の平均時間を見ると、提案 CAPTCHA は先行研究の CAPTCHA よりも 1 秒以上長くなっている。これは、追跡対象を定めるために設定している 1 秒を含んでいるためである。提案手法は、先行研究の CAPTCHA と比べて時間にばらつきがあり、改善の必要があると考える。

4.1.4 ユーザビリティに関するアンケート調査

実験参加者には本実験の後に、SUS（System Usability Scale Facts）[4] によるアンケートを回答してもらった。このアンケート結果に基づいて、提案手法の実用性を確認する。

SUS は、ユーザビリティの評価のために多く利用されている 10 項目の質問票であり、奇数項目がポジティブな質問、偶数項目がネガティブな質問となっている。評価する回答番号は、1（強く反対する）から 5（強く賛成する）の 5 評価から成り立っている。SUS の評価値は、奇数項目に関しては回答番号から 1 を引く、偶数項目に関しては 5 から回答番号を引いた後、すべての項目を足し合わせた合計値を 2.5 倍した値である。本実験で得られた SUS の得点が、SUS の平均点数である 68 点以上なら、最低限のユーザビリティが確保できたと考えられる。

アンケートの結果、SUS の平均点は 76.5 点となった。SUS の平均点数 68 点と比較すると、提案手法は比較的解答のしやすい CAPTCHA であるといえる。しかし、先行研究の CAPTCHA のシステムユーザビリティの平均点数は 84 点であり、実用性は先行研究の CAPTCHA の方が優れていると言える。

ユーザからの意見として、「同じ透明度の円が重なったとき、追跡対象を見失いやすい」や「動体視力が低い人や高齢者、色覚異常の人は難しい」という意見があった。これについては透明度の最低値を適切に決めたり、オブジェクトの移動速度を調整する必要があると考える。

4.2 ボット耐性についての実験

4.2.1 実験目的

3. 章で、提案した CAPTCHA 方式が、ボットを用いて自動的に突破することが可能なものか確認する。具体的には、ボットが追跡を継続できるか否かを確認する。

4.2.2 実験方法

実験は、文献 [1] で用いられたボットを調整して、Chrome のデベロッパーツールを用いてモバイルデバイスの Web ブラウザをエミュレートし、デスクトップ環境で行う。ボットは「meanShift 法を用いた物体追跡」のプログラムであり、自動的にマウスカーソルで移動オブジェクトを追跡する。このボットのマウスカーソル位置を操作領域の位置に調整する。また、追跡のための探索窓の初期位置をオブジェクトの表示領域中央付近に設定した。移動オブジェクトの数を 5 個、10 個、15 個と設定した 3 つの提案 CAPTCHA(1、2、3) に対して 80 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。先行研究の CAPTCHA に対しても同様に 80 回ずつ攻撃を行った。

4.2.3 実験結果と考察

ボットによる CAPTCHA 突破率を考察する。ボットによる CAPTCHA 突破率は、各 CAPTCHA を 80 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合である。ボットによる追跡開始までの時間は、実用性についての実験同様に追跡開始となるまでの時間である。

閾値を 7〜9 秒に設定した時のボットによる CAPTCHA 突破率を、先行方式と本提案方式それぞれ、図 5、図 6 に示す。

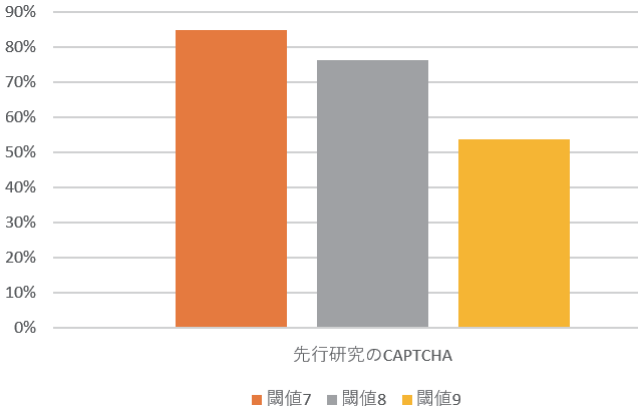


図 5. ボットによる先行研究の CAPTCHA 突破率 1

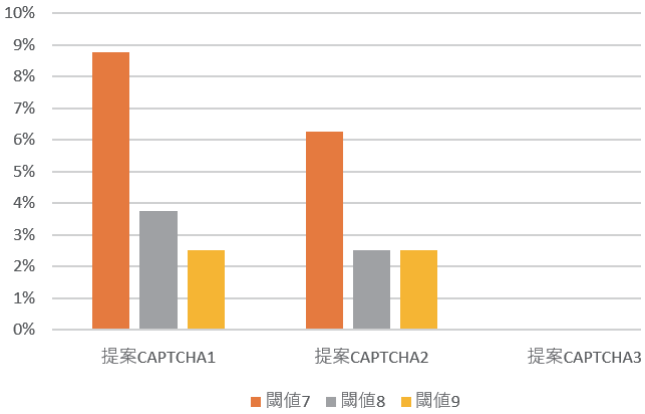


図 6. ボットによる提案 CAPTCHA 突破率 2

先行研究の CAPTCHA では、CAPTCHA 突破率が閾値 7 の時に 85 %、閾値 8 の時に 76 %という高い割合になった。一方提案 CAPTCHA では、閾値 7 以上の時は CAPTCHA 突破率は軒並み 10 %を下回り、閾値 8 以上では 4 %以下という結果になった。また、ある一定の透明度を下回ると、ボットの追跡が外れてしまうことがあった。このことから、このような結果となった理由としては、提案手法のオブジェクトが一定時間で透明度を変えるものとなっていたからだと考える。

以上の結果から、先行研究の CAPTCHA はボット耐性が低く、提案手法はボット耐性が高いと考える。

5. まとめ

本研究では、従来の CAPTCHA 方式はモバイルデバイスにうまく適合できず、ユーザの利便性を損なう問題に着目し、モバイルデバイスに適する使いやすい動的な CAPTCHA を提案し、実用性について検討を行った。先行方式と本提案方式を比較するために、モバイルデバイスでの対照実験を行い、また、ボット耐性についての実験を行った。実験の結果、提案手法のモバイルデバイスでの人間の成功率は比較的高く、所要時間については安定化のために改善する必要があることがわかった。SUS を用いたアンケート調査を行った結果、提案手法は平均スコアを超えたが、先行研究の CAPTCHA を上回ることはできなかった。ボット耐性については、先行研究の CAPTCHA と比べて、ボットによる CAPTCHA 突破率は非常に低い値となった。

今後の課題として、多くの人間が使いやすいようにシステムを改善する必要がある。また、meanShift 法以外のアルゴリズムを用いたボットによる追跡や、機械学習などを用いて、より高度化したボットによる攻撃について検証していかなければならない。

参考文献

1) 立田 怜平, 山場 久昭, 油田 健太郎, 朴美娘, 岡崎 直宣: リレーアタックに耐性を持つインタラクティブな動画 CAPTCHA 方式の検討, 情報処理学会研究報告,Vol.2017-SPT-24,No.11,pp.1-6,2017.

2) 富田 旋, 初 蕾, 山場 久昭, 油田 健太郎, 岡崎 直宣: モバイルデバイスの利用に適した CAPTCHA 方式の検討, 宮崎大學工學部紀要 (47),pp.279-283,07,2018.

3) N.Jiang,H.Dogan and F.Tian: Designing Mobile Friendly CAPTCHAs: An Exploratory Study, Proceedings of British HCI 2017,doi:10.14236/ewic/HCI2017.92,2017.

4) The System Usability Scale (SUS) available from `https://www.usability.gov/how-to-and-tools/methods/system-usability-scale.html`, (accessed 2019/01/18).