

モバイルデバイスの利用に適した CAPTCHA 方式の検討

富田 旋^{a)}・初 蕾^{b)}・山場 久昭^{c)}・油田 健太郎^{d)}・岡崎 直宣^{e)}

Consideration of CAPTCHA System Suitable for Use of Mobile Device

Meguru TOMITA, Tsubomi HATSU, Hisaaki YAMABA, Kentaro ABURADA, Naonobu OKAZAKI

Abstract

CAPTCHA is one of the most widely used Turing tests to prevent unauthorized use of online services, and it is a technology to distinguish whether the subject is a human being or a machine. With the advent of mobile devices, smartphones, tablets, etc. are the most commonly used devices to access the Internet and online services. Most existing CAPTCHA methods are not for use on mobile devices, but for use in conventional desktop PC environments. Since existing CAPTCHA can not fit well with mobile devices and it causes the conversion rate of Web site registration form etc. to drop, it is necessary to design CAPTCHA which is easy to use in mobile devices. Therefore, in this paper, we will consider a new CAPTCHA method that maintains convenience in mobile devices and has sufficient robustness. The proposed method is a dynamic CAPTCHA, it can recognize moving objects that move continuously from among a plurality of disturbing objects appearing at random positions and change their positions, and can trace for more than a certain period of time Whether it is a human being or a machine is judged by whether or not.

Keywords: CAPTCHA, mobile device, PIX, reCAPTCHA

1. はじめに

CAPTCHA は、オンラインサービスの不正使用を防ぐために最も広く使われているチューリングテストの一種であり、対象者が人間であるか機械であるかを判別する技術である。モバイルデバイスの登場により、スマートフォンやタブレットなどは、インターネットやオンラインサービスにアクセスするために最もよく使用されるデバイスとなっている。既存の CAPTCHA 方式のほとんどはモバイルデバイスでの使用ではなく、従来のデスクトップ PC 環境での利用を対象としている。既存の CAPTCHA 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ので、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。そこで本論文ではモバイルデバイスでの利便性を保ち、十分な堅牢性を持つ新たな CAPTCHA 方式を検討する。提案方式は、動的な CAPTCHA であり、ランダムな位置に出現する複数の妨害オブジェクトの中から連続的に移動してその位置を変化させる移動オブジェクトを認識し、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。

2. 既存 CAPTCHA

この節では、既存の代表的な CAPTCHA について述べる。

2.1 文字 CAPTCHA

文字列 CAPTCHA は現在最も広く利用されている CAPTCHA である。文字列 CAPTCHA の多くは、英字 52 文字（大文字、小文字を含む）と数字 10 字の合計 62 字の半角英数字を歪ませ、ノイズを付加して表示し、表示された文字列をテキストボックスに正しく入力できていたら、解答者を人間と判断する。

文字列 CAPTCHA のメリットは、システムが単純であり、Web システムへの導入が簡単である点と、総当たり攻撃に強い耐性があるという点である。CAPTCHA の文字数を a とすると、CAPTCHA に使用される文字列画像のパターン数は、 62^a 通りであるため、ボットがこの文字列を総当たりで突破する場合、 62^a 通りの答えを試さなければならない。例えば、文字数が 4 であった場合、 1.48×10^7 のパターン数となる。しかし、光学文字認識 (OCR) の技術向上により、機械でも歪みやノイズを含んだ文字列を認識できるボットが出現し、問題となっている。

また、モバイルデバイスでの利用を考慮すると、大文字、小文字が混ざったランダムな文字列を入力しなければならない文字列 CAPTCHA 方式は、画面の大きさや入力方式の違いにより、利用しにくいものとなっている。

^{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

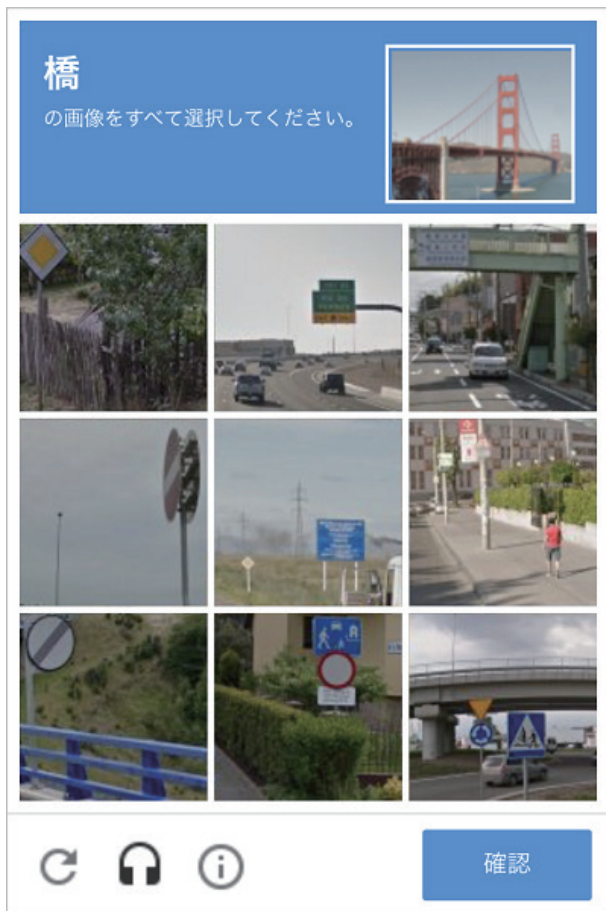


図 1: Google で利用される reCAPTCHA¹⁾

2.2 画像 CAPTCHA

画像 CAPTCHA は、具体物の画像を用いることで、人間と機械を判別する方式である。出題する問題の種類は、様々であり、用いる画像の枚数や解答方式に違いがある。主な画像 CAPTCHA 方式には、Asirra、PIX、reCAPTCHA などがある。画像 CAPTCHA の多くは、複数ある画像の中から、特定の画像を選択することを要求する。図 1 は、画像型の reCAPTCHA を示している。この例では、“橋の画像をすべて選択してください” という指示に従い、9 枚の画像の中から、橋の画像を選択する。画像に写っている具体物が何かを理解して、指定された具体物が写る画像を選択することは、機械にとって難しいため、文字列 CAPTCHA に代わる新たな方式として提案された。

しかし、画像 CAPTCHA は、誤って CAPTCHA の判定テストを偶然通過する確率（偽陽性率）が高いというデメリットがある。例えば、出題される CAPTCHA の画像が 9 枚、そのうち選択すべき正答の画像が a 枚である場合、偽陽性率は、式 1 となる。

$$FP = \frac{1}{9C_a} \quad (1)$$

正答画像の攻撃 a が明らかになっていない場合、攻撃者は式 2 のような確率で誤って判別テストを通過する可能性がある。

$$FP = \frac{1}{\sum_{a=1}^9 9C_a} = \frac{1}{511} \approx 0.001956 \quad (2)$$

この確率は、文字列 CAPTCHA の文字数が 4 つの場合と比

較して非常に高く、画像 CAPTCHA は偶然突破する確率が高いことが分かる。このように、偶然突破確率が高く CAPTCHA として堅牢性に欠けるが、文字列 CAPTCHA と比較すると、モバイルデバイスでの利用に適した方式になっている。モバイルデバイスにおいて、画像 CAPTCHA の解答タスクは、選択する画像をタップするだけで良いため、文字列 CAPTCHA と比べると利用しやすい。そのため、モバイルデバイスでの利便性を考慮した CAPTCHA は、ほとんど画像 CAPTCHA と同じ解答タスクになっている。例えば、VisualCAPTCHA²⁾ や sweetCAPTCHA³⁾ などが挙げられる。

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、十分な堅牢性を持つ新たな 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、モバイルデバイスでの利便性を考慮した既存の CAPTCHA は、画像 CAPTCHA のような出題形式のものが多く、偶然突破する確率が高い問題点があった。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 を考えなければならない。モバイルデバイスでの利便性を考慮すると、「仮想キーボードで文字を打つ」といったことよりも、「タップ」や「タッチパネル上で指を滑らせる」などといった単純な動作を要求するものが望ましい。そこで、画像 CAPTCHA のように、偶然突破確率が高い出題形式とならずに、モバイルデバイスにおいて、単純な操作を要求する CAPTCHA 方式を提案する。

3.1 提案する CAPTCHA 方式

提案方式の CAPTCHA では、ランダムに出現し、消失するオブジェクトの中から、スムーズに移動するオブジェクト（以下、移動オブジェクトとする。）を発見し一定時間、追跡できるか否かでユーザが人間か機械かを判断する。この CAPTCHA 方式では、物体追跡技術などを用いて自動的に移動するオブジェクトの追跡を困難にするために、1 フレームごとにランダムに位置を変える妨害オブジェクトを複数、設置することで機械への耐性を持たせた。

3.2 認証手順

提案する CAPTCHA の認証手順を図 2 に示す。まず、図 3 に示す (a) 初期画面が表示される。

CAPTCHA を開始するボタンをタップすると、図 3 に示す (b) 追跡開始画面に移行し、移動オブジェクトと妨害オブジェクトが表示される。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。オブジェクトの表示領域には、追跡用のサークルが設置してあり、ユーザは、“touch zone” で指をスライドさせて、その追跡用サークルを動かすことで移動オブジェクトを追跡する。追跡成功の判断基準は、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。入っていれば、追跡に成功しているとみなし、入っていなければ、追跡に失敗しているとみなす。

最初に、移動オブジェクトの円の中心座標が、追跡用サー

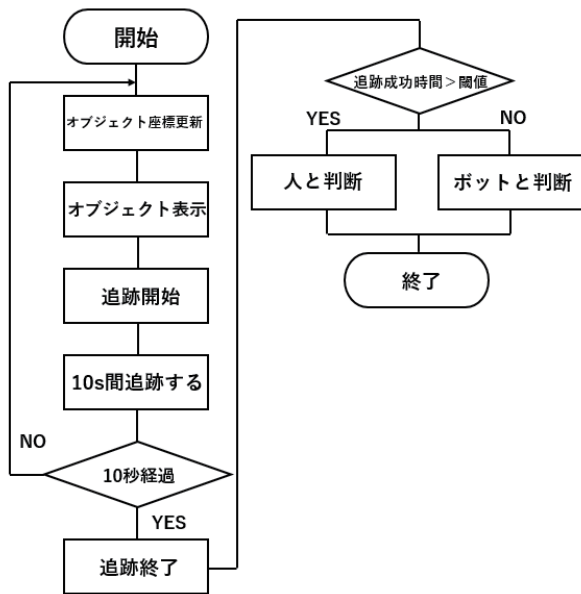


図 2: 提案手法のフローチャート



図 3: 提案する CAPTCHA の構成

クルの円内に入ってから 10 秒計測し、その 10 秒の解答時間の間に何秒間、追跡に成功していたか（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

移動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⁴⁾における、モバイルデバイスでの 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。今回の提案手法は、文献⁴⁾のガイドラインを満たす、モバイルデバイスでの単純な動作による解答方式が可能のため、利便性を損なわないと考えられる。

しかし、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点があった。そこで、オブジェクトの表示領域と、指での操作領域の 2 つを設置し、指で直接、移動オブジェクトを追跡しないように設計した。

3.4 提案手法のセキュリティについて

モバイルデバイスでの利便性を考慮した既存の CAPTCHA は、画像 CAPTCHA のような出題形式のため、偶然突破す

る確率が高いという問題点があった。提案手法の CAPTCHA は、ランダムな動きで移動するオブジェクトを追跡するという形式である。攻撃者が偶然突破を狙って、追跡用サークルをランダムに動かした場合、一定時間の追跡は不可能である。そのため、提案手法の偶然突破確率は、限りなく低い。

しかし、何らかの方法で移動オブジェクトの位置を特定された場合、機械による移動オブジェクトの自動的な追跡は、容易に実現できる。提案手法では、移動オブジェクトの位置の特定を困難にするために、移動オブジェクトと妨害オブジェクトの視覚的特徴（色、形、大きさ）は全く同じに設定している。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、視覚的特徴が同じオブジェクトがランダムに配置されているようにしか見えないため、移動オブジェクトを検出することは困難になると考えられる。

4. 実験と考察

提案 CAPTCHA の実用性について実験を行い、ユーザビリティ評価を調査する。

4.1 実験目的

3. 章で、提案した CAPTCHA 方式が、ユーザ（人間）による解答が可能なのか確認する。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。

4.2 実験方法

実験は、宮崎大学工学部生 10 名に参加してもらった。実験参加者には、各自が所有しているモバイルデバイス（Xperia Z5、iphone 8 など）を利用して、提案 CAPTCHA を 5 回ずつ解いてもらい、追跡成功時間と所要時間の計測を行った。また、現在、最も用いられている reCAPTCHA との比較を行うため、reCAPTCHA も同様に解いてもらった。reCAPTCHA は、⁵⁾ のデモを利用した。

この実験の後に、それぞれの CAPTCHA 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。

4.3 実験結果と考察

4.3.1 成功率

成功率は、各実験を 5 回ずつ行ったうち、被験者が正常に CAPTCHA を完了した回数の割合である。reCAPTCHA は、実験参加者が解答を提出した後に、画面に「もう一度お試しください」というメッセージが提示された場合、失敗（機械とみなされる。）と判断する。

提案 CAPTCHA の追跡成功時間の閾値を 7 秒に設定（7 秒以上の追跡成功時間であれば、人間であると判定する。）すると、reCAPTCHA より提案 CAPTCHA は、成功率が高くなる。図 4 に各 CAPTCHA の成功率の結果を示す。

4.3.2 所要時間

所要時間は、実験参加者が CAPTCHA を開始してから完了するまで掛かった時間のことである。各 CAPTCHA の所要時間について、表??にまとめた。この結果から、提案 CAPTCHA の所要時間は、ほぼ 10 秒~13 秒以内に収まっていることが分かる。それに対して、reCAPTCHA は、最短で 6 秒で終了しているが、最長で約 22 秒掛かっており、人によっては、所要

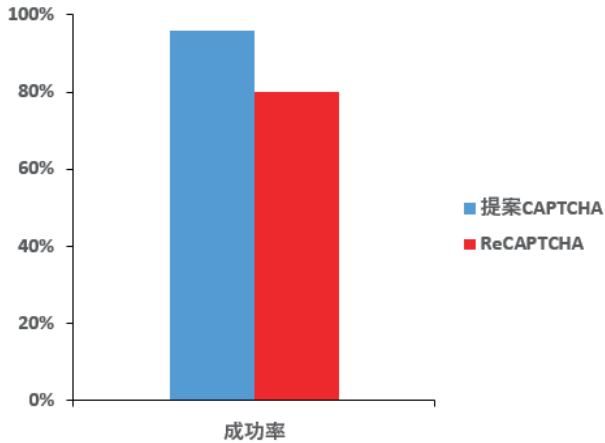


図 4: 成功率

表 1: 実験結果

	最長時間	最短時間	平均時間
提案 CAPTCHA	12.79	10.49	11.43
ReCAPTCHA	22.86	6.11	13.71

時間が長くなっている。reCAPTCHA は、選択しなければならない画像の捉え方が人によって異なるという意見があったため、画像選択する際に時間が掛かってしまった人がいたと考えられる。

提案手法は、reCAPTCHA よりも安定した所要時間になっており、reCAPTCHA よりも利便性が優れていることが示唆される。

4.4 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、システムユーザビリティスケール (System Usability Scale Facts : SUS) ⁶⁾ 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 CAPTCHA の実用性を確認する。システムユーザビリティスケールは、ジョン・ブルック (John Brooke) により、1986 年に開発され、ユーザビリティの評価のために多く利用されている質問票である。質問は 10 項目で成り立っており、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。評価値の集計方法は、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 倍した値がシステムユーザビリティスケールの評価値となる。システムユーザビリティスケールの平均点数は 68 点と定められているので、本実験で得られた SUS の得点が 68 点を超えていたら、最低限のユーザビリティが確保できたと考えられる。

今回提案した CAPTCHA のユーザビリティを評価するためのアンケートを以下に記載する。

1. この CAPTCHA をしばしば利用したいと思う
2. この CAPTCHA を利用するには説明が必要となるほど複雑であると感じた
3. この CAPTCHA は容易に使いこなす事ができると思

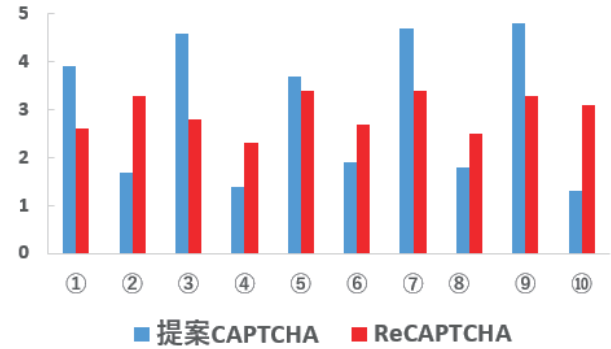


図 5: SUS アンケート調査結果

った

4. この CAPTCHA を利用するのに専門家のサポートが必要だと感じる
5. この CAPTCHA にあるコンテンツやナビゲーションは十分に統一感があると感じた
6. この CAPTCHA では一貫性のないところが多々あったと感じた
7. たいいていの人、この CAPTCHA の利用方法をすぐに理解すると思う
8. この CAPTCHA はとても操作しづらいと感じた
9. この CAPTCHA を利用できる自信がある
10. この CAPTCHA を利用し始める前に知っておくべきことが多くあると思う

本研究でのシステムユーザビリティスケールの評価項目ごとの平均スコア結果を図 5 に示す。各 10 項目の平均スコアでは、提案 CAPTCHA は ReCAPTCHA よりいずれも評価が高く、アンケート結果により、システムユーザビリティスケールの平均点数 68 点と比較すると、提案 CAPTCHA の平均スコアは 84 点であり、ReCAPTCHA の平均スコアは 54 点であることから、本研究での提案 CAPTCHA は ReCAPTCHA よりユーザに大きな負担を強いることもなく、解答のしやすい CAPTCHA であることがいえる。

5. まとめ

本研究では、従来の CAPTCHA 方式は PC 環境の利用を対象となっているため、モバイルデバイスの画面にうまく適合できない一貫性の悪さとモバイルデバイスで利用した際のコンバージョン率の低下などの問題に着目し、インターネットやオンラインサービスを安全に利用するために、モバイルデバイスに適する使いやすい動的な CAPTCHA を提案した。また、提案 CAPTCHA 方式は、ReCAPTCHA 方式と比較し、モバイルデバイスでの対照実験を行った。実験の結果、提案 CAPTCHA はモバイルデバイスでの利用の成功率が高く、所要時間についての安定性を保つことが可能であることを示した。システムユーザビリティスケールアンケート調査を行った結果、提案 CAPTCHA 方式は ReCAPTCHA 方式をすべての質問項目で上回り、提案 CAPTCHA の実用性を確認した。今後の課題として、ボットに対する耐性を保持しているかを検証していかなければならない。

参考文献

- 1) Google reCAPTCHA available from <https://www.google.com/recaptcha/intro/android.html>, (2018/02/01 アクセス).
- 2) VisualCAPTCHA available from <https://wordpress.org/plugins/visualcaptcha/>, (2018/02/05 アクセス).
- 3) sweetCAPTCHA available from <https://blog.sucuri.net/2015/06/sweetcaptcha-service-used-to-distribute-adware.html>, (2018/02/05 アクセス).
- 4) Nan Jiang: Designing Mobile Friendly CAPTCHAs: An Exploratory Study(2017) .
- 5) reCAPTCHA demo available from <https://www.google.com/recaptcha/api2/demo>, (2018/02/05 アクセス).
- 6) The System Usability Scale (SUS) available from <https://www.usability.gov/how-to-and-tools/methods/system-usability-scale.html>, (2018/02/01 アクセス).
- 7) 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.