

3DCG を用いたチャレンジ画像生成プラットフォームの提案

～適用例 1: 画像 CAPTCHA～

池谷勇樹† 可児潤也†† 米山裕太†† 西垣正勝†††

†静岡大学情報学部情報科学科 ††静岡大学大学院情報学研究科
†††静岡大学創造科学技術大学院 432-8011 浜松市中区城北 3-5-1

あらまし 画像を利用した認証方式で肝要となるのは、画像認証においてはパス画像や囮画像、画像CAPTCHAにおいては出題画像の自動生成である。我々は、これらの画像をチャレンジ画像と定義し、3DCGを利用したチャレンジ画像生成プラットフォームを提案する。提案プラットフォームを用いることによって、目的のユーザ認証やCAPTCHAに適したチャレンジ画像を毎回自動生成することができる。本稿では特に画像CAPTCHAの出題画像の自動生成への適用例を示す。提案プラットフォームを用いて実現できる画像CAPTCHAとして、人間が感じる「違和感」を利用したNani-Kore CAPTCHAと、人間が有する「3次元物体の認識能力」を利用したDoko-Soko CAPTCHA を紹介する。

A 3DCG platform to generate challenge-images for authentication

～Case study 1: Image-based CAPTCHA～

Yuki Ikeya† Junya Kani†† Yuta Yoneyama†† Masakatsu Nishigaki†††

†Faculty of Informatics, Shizuoka University
††Graduate school of Informatics, Shizuoka University
†††Graduate School of Science and Technology, Shizuoka University,
3-5-1 Johoku, Naka, Hamamatsu, 432-8011 Japan

Abstract In image-based user authentication, how to prepare pass images and decoy images is one of big issues. Likewise, in image-based CAPTCHA, automatic generation of query images is an essential requirement. We propose a 3DCG platform to automatically generate these pass/decoy/query images (referred to as "challenge-images" in this paper). This paper is the first case study to demonstrate how image-based CAPTCHA is enhanced by the proposed platform. We here show a couple of examples of achieving new CAPTCHA: Nani-Kore CAPTCHA using the human ability of recognizing "strangeness", and Doko-Soko CAPTCHA with the human ability of recognizing 3D objects.

1 はじめに

ユーザ認証においては、パスワードを用いた認証が広く使われているが、推測されにくいパスワードは覚えにくく、ユーザの利便性が低下してしまう。この問題に対し、人間の画像認識能力の高さを利用して、パスワードの代わりにパス画像を用いることによって、認証情報の記憶負荷を軽減する画像認証方式が研究されている[11][12][13]。種々の画像認証が提案されているが、その典型的な方式の1つが、多数の囲画像の中からパス画像を選択するという方式である。

人間であることを認証する CAPTCHA においても、現在広く使われている文字判読型の CAPTCHA (図 1)[1] や動物の画像を用いた Asirra (図 2)[3] など、画像の利用が典型的な手法となっている。近年は、OCR 機能によって文字判読型 CAPTCHA を破るマルウェア[2] や機械学習によって Asirra を破る自動プログラム[4] が報告されており、人間の更に高度な認知能力を利用した画像 CAPTCHA が研究されている[5][7][8][10]。



図 1 文字判読型 CAPTCHA の認証画面例



図 2 Asirra の認証画面例

このように、認証技術と人間の画像処理能力は密接な関係がある。ここで、画像を利用した認証方式で肝要となるのは、画像認証においてはパス画像や囲画像、画像 CAPTCHA においては出題画像の自動生成である(以降、これらの画像を「チャレンジ画像」と呼ぶことにする)。そこで本研究では、3DCG を利用したチャレンジ画像生成プラットフォームを提案する。本稿では特に CAPTCHA の出題画像の自動生成への適用例を示す。提案プラットフォームを用いて実現できる画像 CAPTCHA として、人間が感じる「違和感」を利用した Nani-Kore CAPTCHA と、人間が有する「3次元物体の認識能力」を利用した Doko-Soko CAPTCHA を紹介する。

以下、2章で既存の画像 CAPTCHA を紹介する。3章で提案プラットフォームについて説明し、4章で提案プラットフォームを用いた Nani-Kore CAPTCHA と Doko-Soko CAPTCHA を示す。5章で本稿をまとめ、今後の課題を述べる。

2 画像 CAPTCHA

2.1 Asirra

メールアドレスの不正取得やブログへのスパムコメントの書き込みといった Web サービス提供サイトに対する自動プログラム(マルウェア)による DoS (Denial of Service, サービス不能) 攻撃が定期的に行われている。

CAPTCHA は, このようなマルウェアによる Web サービスの不正利用と, 人間による正規のサービス利用を識別するための必須の技術である。人間には容易に解答できるがコンピュータには判別が困難である問題をユーザに出題し, 正解できたユーザを人間だと判定する。

OCR を用いて文字判読型 CAPTCHA を解読するマルウェアに対抗するために提案された画像 CAPTCHA として Asirra がある[3]。Asirra では, 合計 12 枚の犬と猫の出題画像を表示し, それらの画像の中から猫の画像だけを全て選択できたユーザを人間として判定する(図 2)。画像の意味を理解することは人間の高度な認知メカニズムの 1 つであり, マルウェ

アによる不正解答は不可能であると考えられていた。

しかし, 猫の画像の特徴や犬の画像の特徴を抽出し, 機械学習技術を利用することによって, Asirra は破られ得るという研究報告がなされた[4]。Asirra が破られた原因として, Asirra が画像の表面的な意味を問うものであったためと考えられる。人間のより高度な認知処理に基づく CAPTCHA が求められている。

2.2 4コマ漫画 CAPTCHA

4 コマ漫画 CAPTCHA [5]は, 人間の「ユーモアを解する能力」と「違和感を判別する能力」を利用した CAPTCHA である(図 3)。4 コマ漫画の各コマの順番を入れ替えて 4 枚の出題画像として表示し, 正しい順番に並べることができたユーザを人間として判定する。人間は起承転結の崩れを違和感として認識し, ユーモアを理解して 4 コマ漫画を正しい起承転結の順番に再構築することができる。しかし, 起承転結を備えた 4 コマ漫画の自動生成が難しいという問題がある。



図 3 4コマ漫画 CAPTCHA の認証画面例

(出展:左から1番目の図:文献[6]の p.25 の 4コマ漫画の 1コマ目, 2番目の図:同, p.25 の 4コマ目, 3番目の図:同, p.25 の 3コマ目, 4番目の図:同, p.25 の 2コマ目)

2.3 SEMAGE

SEMAGE [7]は、人間の持つ「画像間の関連を理解する能力」を利用した画像 CAPTCHA である。N 枚の出題画像をユーザに提示し、関連のある K 枚の画像を全て選択できたユーザを人間として判定する。文献[7]では、SEMAGE の実装例の 1 つとして、動物の写真とイラストを合計 6 枚表示し、その中から同じ動物の写真とイラストをそれぞれ 1 枚ずつ(合計 2 枚)をユーザに選択させる方式が示されている(図 4 の例では、上段中央のライオンのイラストと下段中央のライオンの写真を選択できれば正解となる)。



図 4 SEMAGE の認証画面例

SEMAGE は画像データベースを利用して出題画像を生成する。画像データベースの主な構築方法としては、インターネット上にある画像ファイルを収集する方法があるが、現在はまだ画像検索技術の精度が高くないため、画像収集の際に不適切な画像が混ざってしまう(例えば、画像検索によってライオンの画像を収集しようとしても、ライオン以外の画像が少なからず混入する)。現時点では、不適切な画像は手動で取り除く必要があり、完全な自動化ができていないという問題がある。

2.4 3D 画像 CAPTCHA

YUNiTi.com [8]は、人間が有する「3次元物体の認識能力」を利用した3D画像 CAPTCHA を実装し、運用している。3次元オブジェクトを3個並べた出題画像を表示し、それぞれのオブジェクトが何であるかを18個の候補画像の中から正しく選択できたユーザを人間として判定する(図 5)。出題画像は、候補画像のオブジェクトを別の角度から写した画像となっている。

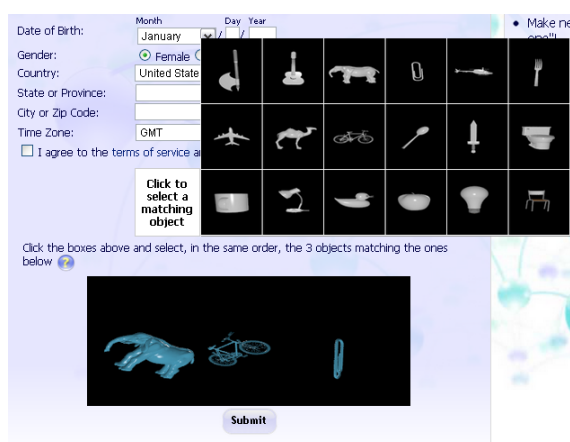


図 5 3D 画像 CAPTCHA の認証画面例

一旦 3DCG オブジェクトを生成してしまえば、任意の視点からの 2D 画像を描画することができるため、出題画像の自動生成が可能である。しかし、web ページに候補画像の一覧が表示される方式となっているため、テンプレートマッチングを巧みに行って出題画像と一番近い候補画像を探すという方法によって、自動プログラムが正解画像を特定でき得るという問題が指摘されている[9]。

3 チャレンジ画像生成プラットフォーム

4コマ漫画 CAPTCHA には出題画像の自動生成が難しいという問題があった。SEMAGE においても、出題画像を生成するための画像データベースの自動構築の精度に問題を抱えて

いた。また, Asirra や 3D 画像 CAPTCHA では, 機械学習やパターンマッチングに耐性のある出題画像の生成が課題となっていた。このように, 画像を利用した CAPTCHA においては解読耐性の高い出題画像(チャレンジ画像)の自動生成が肝要となる。これを解決するための取り組みとして, 本研究では, 3DCG を利用したチャレンジ画像生成プラットフォームを提案する。提案プラットフォームのコンセプトを図 6 に示す。

提案プラットフォームは, 3D モデルデータと設定データからチャレンジ画像を自動生成する機能を有する。

3D モデルデータは, 3DCG オブジェクトの構成データであり, オブジェクトの頂点情報やレンダリング情報など種々のデータを含む。提案プラットフォームの中にはデフォルトで多数の 3DCG オブジェクトのモデルデータが登録されており, 管理者が新たな 3DCG オブジェクトのモデルデータを新規登録することもできる。設定データは, 3DCG オブジェクトをどのように加工することによって CAPTCHA チャレンジ画像を生成するかを規定する定義ファイルである。具体的な CAPTCHA の手法ごとに, それに対応した設定データが用意される。

設定データによって規定された方法によって 3D モデルデータを加工することによってチャレンジ画像が自動生成される。データの加工は, ①3D モデルデータの選択, ②3D オブジェクトの配置, ③視点の決定, の一連の操作によって行われる(図 7)。プラットフォームは, ①②③のそれぞれの加工における操作パラメータをランダムに変更することによって, 毎回異なるチャレンジ画像を生成する。

① 3D モデルデータの選択

使用する 3D モデルデータを選択する。各オブジェクトの色や背景となる画像も選ばれる。人間や動物などのオブジェクトが選択された場合は, その姿勢も決定する。チャレンジ画像生成の度に異なったオブジェクトが選

択されるが, 例えば「赤い車」のように, 選択範囲を指定することも可能である。

② 3D オブジェクトの配置

①で選択された複数の 3D オブジェクトをどこにどのように配置するかを決定する。チャレンジ画像生成の度に, 必要に応じて, 各オブジェクトの大きさ, 位置, 向きなどのパラメータが毎回ランダムに変更される。

③ 視点の決定

②で生成された 3D 仮想世界をどの視点から写して画像化するかを決定する。視点は, チャレンジ画像生成の度に毎回ランダムに変更される。

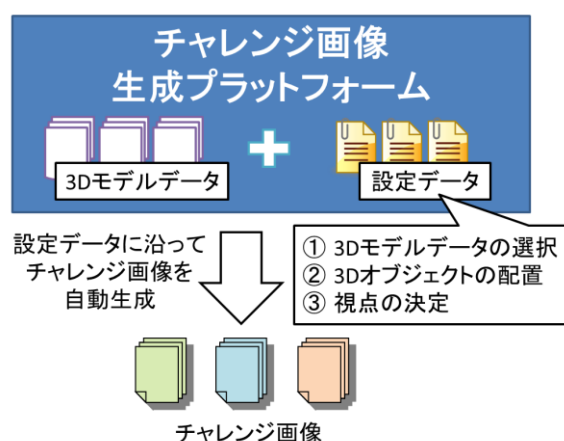


図 6 提案プラットフォームの概念図

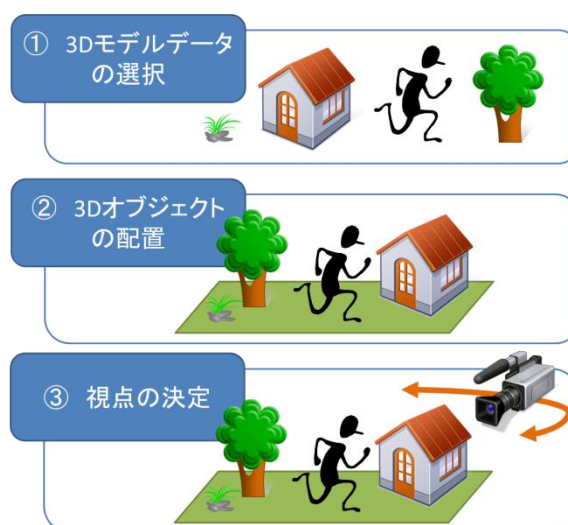


図 7 チャレンジ画像生成におけるデータ加工手順

本稿では紙面の都合で詳細な説明を割愛しているが、画像認証においても、パス画像や囲画像の自動生成は大きな未解決問題の1つとなっている。本研究で構築を目指すチャレンジ画像生成プラットフォームは、画像認証のチャレンジ画像(パス画像、囲画像)の自動生成ツールとしても有効に利用できる。

4 画像 CAPTCHA への適用

提案プラットフォームを web サーバと連動させることによって、任意の画像 CAPTCHA を実装することができる。

本章では、提案プラットフォームを用いて実現できる画像 CAPTCHA として、人間が感じる「違和感」を利用した Nani-Kore CAPTCHA と、人間が有する「3次元物体の認識能力」を利用した Doko-Soko CAPTCHA を紹介する。

4.1 Nani-Kore CAPTCHA

人間は、自分の経験や常識と少しでも異なるような場面に遭遇すると、「しっくりこない」または「気持ちが悪い」といった感情を、違和感として覚える。より多くの常識を知れば知るほど、また、より豊富な経験を積みれば積むほど、違和感を感じる能力は研ぎ澄まされ、非常に些細な違いにも気付くことができるようになって考えられている。すなわち、「違和感を覚える」ことは、人間が有する高度な認知メカニズムの1つであり、機械による模倣は非常に困難であると期待できる。

Nani-Kore CAPTCHA は、この人間の感じる「違和感」を利用した画像 CAPTCHA である。提案プラットフォームを用いて、画像全体の中で一部につじつまの合わない画像を生成する。人間であれば、つじつまの合わない部分に違和感を覚え、その場所を答えることが可能である。

違和感のある画像を生成する方法は様々なものを採用することができると考えているが、例え

ば、画像中の1つのオブジェクトのパラメータのみを他のオブジェクトのパラメータから大きく変化させる方法がその一例となるだろう。例えば図8の例では、画像中の複数の車の中に1台だけ車両の向きが大きく異なっている車が配置されている。

3章で説明した手順②(図7の②)の時点で各オブジェクトのパラメータを決定する際に、任意のオブジェクト(車)を1台ランダムに抽出し、そのオブジェクトのパラメータ(車の向き)だけ他のオブジェクトのパラメータとは大きく異なる値をセットすることによって、図8のようなチャレンジ画像が自動生成される。プラットフォームは、その際に選ばれたオブジェクト(車)がどこに配置されたかという情報を知っているため、人間が「つじつまが合わない」と感じる場所(CAPTCHAの回答)を特定することができる。



図8 パラメータの変化を利用した違和感画像

現時点における最先端技術を用いたとしても、インターネット上から「違和感のある画像」を自動的に収集する手段はないと思われる。違和感を用いた画像 CAPTCHA は、提案プラットフォームを用いることで初めて実現できる CAPTCHA であると言えるだろう。

4.2 Doko-Soko CAPTCHA

人間は、高い画像認識能力を有するだけでなく、空間認識能力にも長けている。このため、3Dオブジェクトが写っている画像から、そのオブジ

エクトの3次元形状を理解することができる。すなわち、「3次元物体を認識する」ことは、人間が有する高度な認知メカニズムの1つであり、機械による模倣は非常に困難であると期待できる。

Doko-Soko CAPTCHA は、この「人間の3次元物体の認識能力」を利用した画像 CAPTCHA である。提案プラットフォームを用いて、1つのオブジェクトを別の方向から見た2枚の画像 A と B を自動生成する。画像 A が出題画像であり、オブジェクトのある部位にマーカが付されている。画像 B は回答画像である。画像 B にはマーカはない。人間であれば、「画像 A においてマーカが付されている部位が、画像 B においてはどこに当たるのか」を答えることができる。画像 A の例を図 9(a) に、画像 B の例を図 9(b) に示す。ユーザは、画像 A の赤い丸の部位が画像 B ではどこに当たるのかを回答する。



図 9(a) 画像 A(出題画像)の例

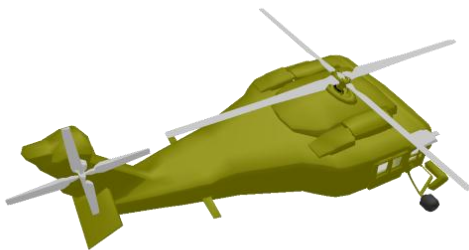


図 9(b) 画像 B(回答画像)の例

立体認識の分野では、1つのオブジェクトを

異なる2つの視点から撮影した画像からそのオブジェクトの3次元形状情報を再構築する技術が研究されている[14]。機械は、この技術を利用して Doko-Soko CAPTCHA の解読を試みるだろう。この攻撃に対処するために、Doko-Soko CAPTCHA においては、画像 B の画像を生成する際にはオブジェクトの3Dモデルデータに適度な変形を加える。図 9 の例では、画像 B(図 9(b))の生成の際に、オブジェクト(ヘリコプタ)の頂点データを操作して「丸く太ったヘリコプタ」へと変形させている。画像 A(図 9(a))の生成の際にオブジェクトを加工することもできる。

3章で説明した手順②(図 7 の②)の時点で、あるオブジェクトの中の部位の1つを任意に選択し、画像 A を生成する際にはその部位にマーカを追記する。プラットフォームは、どの部位が選択されたかという情報を知っているため、画像 B における当該部位の位置(CAPTCHA の回答)を特定することができる。

YUNiTi.com [8]の3D画像 CAPTCHA は、人間が有する「3次元物体の認識能力」を利用している点、チャレンジ画像の自動生成を達成している点で秀逸な画像 CAPTCHA である。しかし、「複数の候補画像の中から一番近い画像を選ぶ」という形の質問形態となっているため、テンプレートマッチングに対する脆弱性を残していた。Doko-Soko CAPTCHA は、「複数の候補画像の中から一番近い画像を選ぶ」という質問形態をとっておらず、テンプレートマッチングに対する耐性も向上していると期待される。

5 まとめと今後の課題

3DCG を利用したチャレンジ画像生成プラットフォームを提案した。本稿では提案プラットフォームの画像 CAPTCHA への適用に焦点を当て、人間の高度な認知処理である「違和感を感じる能力」を利用した Nani-Kore CAPTCHA

の実現例, および, 「3次元物体の認識能力」を利用した Doko-Soko CAPTCHA の実現例を通じて, 提案プラットフォームの有用性を示した.

本稿においては, 提案プラットフォームはまだコンセプト提案の段階である. 今後, 実際にプラットフォームの構築を進めていく. また, Nani-Kore CAPTCHA と Doko-Soko CAPTCHA の実装および評価と, 提案プラットフォームの画像認証への適用についても予定している.

参考文献

- [1] <http://www.gmailhelp.com/2009/10/unlocking-gogles-gmail-captcha/>
- [2] J.Yan,A.S.E.Ahmad: Breaking Visual CAPTCHAs with Naïve Pattern Recognition Algorithms, 2007 Computer Security Applications Conference, pp.279-291, 2007
- [3] <http://research.microsoft.com/en-us/um/redmond/projects/asirra/>
- [4] P.Golle:Machine Learning Attacks Against the ASIRRA CAPTCHA, 2008 ACM CSS, pp.535-542, 2008
- [5] 鈴木徳一郎, 山本匠, 西垣正勝:4コマ漫画 CAPTCHA の提案 2009 年暗号と情報セキュリティシンポジウム予稿集, 3D3-3(CD-ROM), 2009
- [6] 植田まさし, 「新コボちゃん 8」, 芳文社, 2006
- [7] Shardul Vikram, Yinan Fan, Guofei Gu: SEMAGE: A New Image-based Two-Factor CAPTCHA, 2011 Annual Computer Security Applications Conference, pp.237-246, 2011
- [8] <http://www.yuniti.com/>
- [9] <http://technobabblepro.blogspot.jp/2009/04/how-theyll-break-3d-captcha.html>
- [10] Takumi Yamamoto, J.D.Tygar, Masakatsu Nishigaki: CAPTCHA Using Strangeness in Machine Translation, Proceedings of IEEE International Conference on Advanced Information Networking and Applications 2010, pp.430-437, 2010
- [11] Dhamija, R. and Perrig, A.: Deja Vu: A User Study Using Images for Authentication, Proc. 9th USENIX Security Symposium, pp.45-58, 2002
- [12] 高田哲司, 小池英樹:あわせ絵:画像登録と利用通知を用いた正候補選択方式による画像認証方式の強化法, 情報処理学会論文誌, Vol.44, No.8, pp.2002-2012, 2002
- [13] 原田篤史, 漁田武雄, 水野忠則, 西垣正勝:画像記憶のスキーマを利用したユーザ認証システム, 情報処理学会論文誌, Vol.46, No.8, pp.1997-2013, 2005
- [14] 安居院猛, 長尾智晴, 「画像の処理と認識」, 昭晃堂, 1992