違和感画像CAPTCHA：3DCGを用いた究極のチューリングテストとその応用

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成　３０　年　　６　月　１９　日現在

機関番号：　１３８０１
研究種目：　基盤研究(B)（一般）
研究期間：　2013～2017
課題番号：　２５２８００４６

研究課題名（和文）違和感画像ＣＡＰＴＣＨＡ：３ＤＣＧを用いた究極のチューリングテストとその応用

研究課題名（英文）Unrealistic image CAPTCHA: A sophisticated Turing test using 3DCG

研究代表者

西垣　正勝（NISHIGAKI, Masakatsu）

静岡大学・創造科学技術大学院・教授

研究者番号：２０２８３３３５

交付決定額（研究期間全体）：（直接経費）　　13,000,000円

研究成果の概要（和文）：CAPTCHAとは人間と機械を識別するチューリングテストであり、コンピュータには解読できないが人間ならば簡単に解くことができる問題を、コンピュータが無数に自動生成できることが実装上の要件となる。しかし、「コンピュータには解読できない問題」をコンピュータに自動生成（および正誤判定）させることは根本的には不可能である。本研究は、3次元コンピュータグラフィックス技術を巧みに駆使し、人間だけが「違和感」を感じる画像の自動生成を達成することによって、マルウエアに対する高い攻撃耐性とWEBシステムとしての十分な可用性を有する究極的なCAPTCHAを実現する。

研究成果の概要（英文）：The Turing test plays an important role in discriminating humans from malicious automated programs and the Completely Automated Public Turing test to tell Com-puters and Humans Apart (CAPTCHA) system has been widely used. CAPTCHAs are needed to exploit a high-level human recognition ability. However, CAPTCHAs inherently contain a contradiction: Web servers (computers) should be able to automatically generate the CAPTCHA questions that malware (computers) cannot understand. To overcome the issue, I propose to apply 3D computer graphics technology and crate an unrealistic image CAPTCHA using "something different from common sense".

研究分野：　情報セキュリティ

キーワード：　CAPTCHA　違和感　3DCG　認証

１．研究開始当初の背景

WEB サービスの発展にともない、人間と機械を識別するチューリングテストが必須となっている。無料 WEB メールやブログなどの WEB サービス提供サイトに対し、自動プログラム（マルウエア）を使って、大量にアカウントを不正取得する、スパム記事を不正投稿するなどの DoS（サービス不能）攻撃が定常的に頻発しているためである。チューリングテストは、このようなマルウエア（悪意の自動プログラム）と正規のユーザ（人間）を識別するために必須の技術であり、CAPTCHA [1]と呼ばれる方式が広く利用されている。

CAPTCHA の基本形態は、歪曲やノイズが付加された文字列画像を WEB ページに提示し、閲覧者がその文字を判読できるか否かを試すものである（図 1）。また、Asirra [2]という CAPTCHA では、複数の動物の絵を表示し、その中から特定の動物の絵を選ばせる。例えば「猫を選べ」という質問に対し、猫の絵を選択できれば人間であるとして判定する（図 2）。

図 1．Google で使用されている CAPTCHA

図 2．Asirra のイメージ図（猫選択の例）

しかし，近年，既存の CAPTCHA における脆弱性が多くの研究者によって指摘されている．例えば，文字列の判読能力を試す CAPTCHA においては，すでに高機能な OCR（自動文字読取）機能を備えるマルウエアが出回るようになっている[3]。Asirra でさえも、機械学習を利用して自動プログラムがこれを解読することが可能である[4]。多くの研究者が、（現時点の）コンピュータには「絵の意味を理解する」ことは不可能であろうと考えていたため、Asirra 攻略の報告は研究者に衝撃を与えた。

マルウエアの能力の向上は留まるところを知らない。マルウエアがいかに高度になろうとも、マルウエアによる不正解答が根本的に不可能である「究極的なチューリングテスト（CAPTCHA）」がいよいよ必要とされる時代になってきた。研究代表者は、既に「人間のより高度な知識処理」を利用して CAPTCHA を強化する方法の検討を重ねてきた。文献[5]は、機械翻訳によって生成された不完全な文章を利用した CAPTCHA である。人間であれば、文章に含まれる些細な不自然さを「違和感」として感じることができる。文献[6]の CAPTCHA では、4 コマ漫画の各コマをバラバラにして表示する。4 コマ漫画を起承転結の順序に並べることができるのは、「ユーモアを解する」ことができる人間だけである。

しかし、このような高度な CAPTCHA を実現するにあたって、大きく立ち塞がる壁があった。それは「問題の自動生成」である。コンピュータは、既存の文章を機械翻訳することはできる。しかし、機械翻訳によって生成された文章が不自然であるか否かを判定できない（生成された文章の不自然さがコンピュータには分からないので、翻訳結果が不自然な文章となっているのである）ので、コンピュータは、その翻訳文章が CAPTCHA の問題として適正なのかを自分で判断することができない。4 コマ漫画に関しては、コンピュータは、ユーモアや起承転結を理解して 4 コマ漫画を自動生成すること自体困難である。

そこで本研究は、(i)人間のより高度な認知処理を利用し、かつ(ii)コンピュータによる問題の自動生成（および正誤判定）が可能である「安全性と可用性を両立した究極の CAPTCHA」を実現する。

参考文献：

[1] The Official CAPTCHA Site, http://www.captcha.net.

[2] J.Elson, J.Douceur, J.Howell, J.Saul: Asirra: a CAPTCHA that exploits interest-aligned manual image categorization. 2007 ACM CSS, pp.366-374, 2007.

[3] J.Yan, A.S.E.Ahmad: Breaking Visual CAPTCHAs with Naïve Pattern Recognition Algorithms, 2007 Computer Security Applications Conference, pp.279-291, 2007.

[4] CAPTCHA 認証は“終わった”技術なのか、月刊 Computerworld 2008 年 10 月号.

[5] T.Yamamoto, J.D.Tyagr, M.Nishigaki: CAPTCHA Using Strangeness in Machine Translation, Proceedings of IEEE International Conference on Advanced Information Networking and Applications 2010, pp.430-437, 2010.

[6] T.Yamamoto, T.Suzuki, M.Nishigaki: A Proposal of Four-panel cartoon CAPTCHA, Proceedings of IEEE International Conference on Advanced Information Networking and Applications 2011, pp.159-166, 2011.

２．研究の目的

CAPTCHA とは人間と機械を識別するチューリングテストであり、コンピュータには解読できないが人間ならば簡単に解くことができる問題を、コンピュータが無数に自動生成できることが実装上の要件となる。しかし、「コンピュータには解読できない問題」をコンピュータに自動生成（および正誤判

定）させることは根本的には不可能である。本研究は、人間だけが「違和感」を感じる画像の自動生成を達成することによって、問題の自動生が可能であり、かつ、マルウエアに対する高い攻撃耐性を有する「違和感画像 CAPTCHA」を実現する。

3．研究の方法

3 次元コンピュータグラフィックス（3DCG）技術を巧みに駆使することによって、人間だけが違和感に気付く画像の自動生成を達成する。一般的に、3 次元モデルから 2 次元画像を生成することは可能であるが、2 次元画像から 3 次元モデルを再現することは（1 次元分の情報が落ちているため）不可能である。この不可逆性を活用し、「コンピュータが問題を作成することは可能であるが、その問題を解くことができない」という要件を満たす違和感画像をコンピュータ自身に自動生成（および正誤判定）させる。

（1）キメラ CAPTCHA

人間は日常生活を通じて多くの常識を身につけている。自身が身につけた常識から逸脱した場面に遭遇すると、人間は「しっくりこない」または「気持ちが悪い」といった感情を覚える。機械に常識を身につけさせることは、人間が有しているあらゆる知識を機械にすべて覚えさせることを意味しており、常識を備える人工知能の実現は現在もなお未踏の領域である。すなわち、「常識の逸脱を認識する能力」ことは、人間の高度な認知メカニズムであり、機械による模倣は（当面のところ）ほぼ不可能である。したがって、この能力を CAPTCHA へ適用することができれば、人間には判別できるが機械には突破不可能である CAPTCHA が実現できると期待される。

3DCG 技術における 3 次元モデルは、動物や車のように「現実に存在する有形物」をモデル化したものであることが多い。人間はモデル化前のオブジェクトを少なくとも一度は現実世界で見た経験を持っており、それらのモデルを「常識」として保持していると考えられる。したがって、3 次元モデルは人間が保持している「常識」そのものを表していると考えられ、「常識的な事象」の生成には 3 次元モデルそのものを使うことができる。

人間の常識から逸脱した画像は、現存の 3 次元オブジェクトを適切に加工することで自動生成する。加工の方法には種々のアプローチが考えられるが、本研究では、ランダムに選んだ 2 つの 3 次元オブジェクト同士をめりこませることで新しいオブジェクト（以下、「キメラオブジェクト」と呼ぶ）を生成する．たとえば，犬のオブジェクトに猫のオブジェクトがめりこんでいれば，犬と猫が結合されたキメラオブジェクトが生成される．

提案方式では、複数の通常の 3 次元オブジェクトの中に、1 体のキメラオブジェクトを配置した一枚の画像を CAPTCHA として出題する。画像中から非現実オブジェクトを選択できたユーザを正規ユーザ（人間）と判断する。

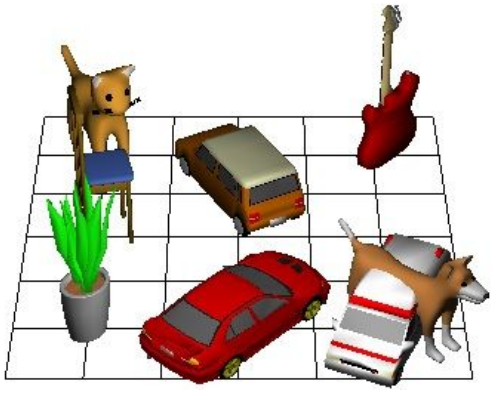

図 3．キメラ CAPTCHA

（2）メンタルローテーション CAPTCHA

人間は、3 次元オブジェクトが写っている 2 次元画像から、そのオブジェクトの 3 次元形状を容易に推測することができる。また、人間は、1 つの視点から写された 2 次元物体や 3 次元物体を頭の中で回転させ、異なる視点から写された形姿を認識することが可能である。この能力は「メンタルローテーション」と呼ばれる。したがって、人間であれば 3 次元オブジェクトを撮影した 2 枚の画像を見たとき、一方の画像に写っている 3 次元オブジェクトを頭の中で回転させ、もう一方と比較することで、2 枚の画像に写っている 3 次元モデルが同一のモデルであるか否かを判定することができる。

本研究では、メンタルローテーションタスクを「異なる形状を持つ 2 つのオブジェクト間における部位の対応関係を問う」という課題へと昇華し、これを用いることで、より攻撃耐性が高いメンタルローテーション CAPTCHA を実現する。

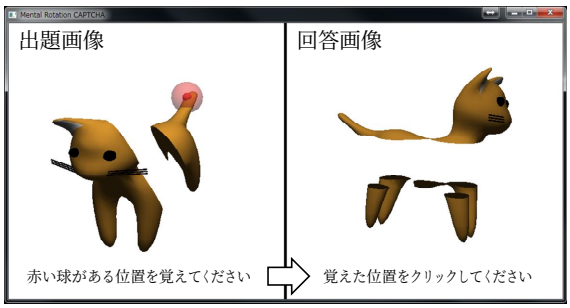

図 4．メンタルローテーション CAPTCHA

（3）方向 CAPTCHA

人間のメンタルローテーションタスクには、「オブジェクトの回転角度が大きいほどタスクに要する時間も長くなる一方で、オブジェクトが左向きか右向きかについては即座に識別している」という興味深い特徴が存在することが知られている。すなわち人間は、「右向きか左向きか」、「前向きか後向きか」

という程度の雑駁な方向識別については直感的な判定が可能である。この特徴を利用して、「3 次元オブジェクトの向いている方向を回答する」というメンタルローテーションタスクに基づく新たなメンタルローテーション CAPTCHA「Directcha」を実現する。

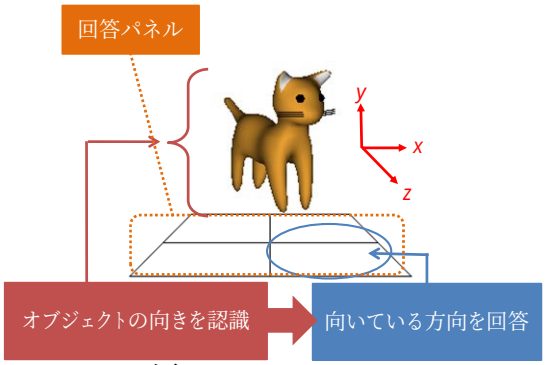

図 5. Directcha

4．研究成果

（1）キメラ CAPTCHA

複数の通常のオブジェクトの中に紛れるキメラオブジェクトをユーザが容易に見つけることができるか否かを回答時間と正答率の視点から評価した。

Web 上から収集した 34 体の 3 次元モデルを使用し、キメラ CAPTCHA 生成システムを実装した。被験者は、情報セキュリティ系の研究室に所属する学生 10 名である。被験者には、画像中のオブジェクト数 N が 4、8、12、16 のケースに対して各 5 問、計 20 問のキメラ CAPTCHA を解くよう求めた。キメラ CAPTCHA 1 問あたりの正答率は N=4, 8, 12, 16 すべてで 9 割以上であった。1 問当たりの平均回答時間はオブジェクト数に伴って増加する傾向がみられるが、もっとも長い 16 体でも 5.5 秒であった。

（2）メンタルローテーション CAPTCHA

1 体の 3 次元モデルを 2 つの異なる視点から描写した 2 体の 3 次元オブジェクトにおいて、対応する部位をユーザが容易に見つけることができるか否かを回答時間と正答率の視点から評価した。

Web 上から収集した 10 体の 3 次元モデルを使用し、メンタルローテーション CAPTCHA 生成システムを実装した。被験者は、情報セキュリティ系の研究室に所属する学生 20 名である。被験者には 5 問のメンタルローテーション CAPTCHA を解くよう求めた。メンタルローテーション CAPTCHA 1 問あたりの平均正答率は 80.0%であった。1 問当たりの平均回答時間は 5.1 秒であった。

（3）方向 CAPTCHA

3 次元モデルの方向をユーザが容易に正当することができるか否かを回答時間と正答率の視点から評価した。

Web 上から収集した 16 体の 3 次元モデルを使用し、Directcha 生成システムを実装した。被験者は、情報セキュリティ系の研究室に所属する学生 6 名である。被験者は、4 方向（総当たり数 4）の Directcha を 8 問解く 3 名と、8 方向（総当たり数 8）の Directcha を 16 問解く 3 名に分け実験を行った。総当たり数 4 の Directcha の平均正答率と平均回答時間は、91.7%と 1.5 秒であった。総当たり数 8 の Directcha の平均正答率と平均回答時間の平均は、97.9%と 1.8 秒であった。

5．主な発表論文等

（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計 3 件）

① 藤田真浩，池谷勇樹，可児潤也，西垣正勝：Locimetric 型メンタルローテーション CAPTCHA，情報処理学会論文誌，査読有, Vol.57, No.9, 2016, pp.1954-1964. http://id.nii.ac.jp/1001/00174627

② 藤田真浩，池谷勇樹，可児潤也，西垣正勝：非現実画像 CAPTCHA：常識からの逸脱を利用した 3DCG 画像 CAPTCHA，情報処理学会論文誌，査読有，Vol.56, No.12，2015，pp.2324-2336. http://id.nii.ac.jp/1001/00146616

③ 可児潤也，鈴木徳一郎，上原彰敬，山本匠，西垣正勝：4 コマ漫画 CAPTCHA，情報処理学会論文誌，査読有，Vol.54, No.9，2013，pp.2232-2243. http://id.nii.ac.jp/1001/00095206

〔学会発表〕（計 18 件）

① 佐野絢音，藤田 真浩，西垣正勝，機械解読耐性の向上とユーザのメンタル負荷軽減を両立する CAPTCHA 出題形式に関する検討(その 2), 暗号と情報セキュリティシンポジウム 2018，2018.

② Ayane Sano, Masahiro Fujita, Masakatsu Nishigaki: Directcha-maze: A Study of CAPTCHA Configuration with Machine Learning and Brute-Force Attack Defensibility Along with User Convenience Consideration, 2017 International Conference on Broad-Band Wireless Computing, Communication and Applications, 2017.

③ 佐野絢音，藤田真浩，西垣正勝：機械解読耐性の向上とユーザのメンタル負荷軽減を両立する CAPTCHA 出題形式に関する検討，コンピュータセキュリティシンポジウム 2017，2017.

④ Ayane Sano, Masahiro Fujita, Masakatsu Nishigaki: Directcha-maze: A Study of CAPTCHA configuration with Machine Learning Attack Defensibility and User Convenience Consideration, 2017 International

Workshop on Security, 2017.
⑤ 佐野絢音，藤田真浩，西垣正勝，総当たり数の確保とユーザのメンタル負荷軽減を実現する CAPTCHA 出題形式の検討，2017 年暗号と情報セキュリティシンポジウム，2017.
⑥ Ayane Sano, Masahiro Fujita, Masakatsu Nishigaki: Directcha: A Proposal of Spatiometric Mental Rotation CAPTCHA, 2016 International Conference on Privacy, Security and Trust, 2016.
⑦ 佐野絢音，藤田真浩，西垣正勝：Spatiometric 型メンタルローテーション CAPTCHA の提案，2016 年暗号と情報セキュリティシンポジウム，2016.
⑧ Masahiro Fujita, Yuki Ikeya, Junya Kani, Masakatsu Nishigaki: Chimera CAPTCHA: A Proposal of CAPTCHA Using Strangeness in Merged Objects, Proceedings of 2015 International Conference on Human-Computer Interaction, 2016.
⑨ 藤田真浩，池谷勇樹，西垣正勝：全周囲型メンタルローテーション CAPTCHA の提案，情報処理学会マルチメディア，分散，協調とモバイルシンポジウム，2015.
⑩ 藤田真浩，池谷勇樹，可児潤也，西垣正勝：キメラ CAPTCHA：3DCG を利用した違和感画像 CAPTCHA，インタラクティブシステムとソフトウェアに関するワークショップ 2014，2014.
⑪ Masahiro Fujita, Yuki Ikeya, Junya Kani, Masakatsu Nishigaki: Chimera CAPTCHA: A Proposal of CAPTCHA using Strangeness in Merged Objects, International Workshop on Security 2014 , 2014.
⑫ 藤田真浩，池谷勇樹，可児潤也，西垣正勝：非現実画像 CAPTCHA：オブジェクトのめり込みを利用した違和感画像 CAPTCHA，画像の認識・理解シンポジウム 2014，2014.
⑬ Yuki Ikeya, Masahiro Fujita, Junya Kani. Yuta Yoneyama, Masakatsu Nishigaki: An Image-Based CAPTCHA Using Sophisticated Mental Rotation, 2014 International Conference on Human-Computer Interaction, 2014.
⑭ 藤田真浩，池谷勇樹，可児潤也，米山裕太，西垣正勝：高度なメンタルローテーションを利用した画像 CAPTCHA の提案，電子情報通信学会，2014.
⑮ 藤田真浩，池谷勇樹，可児潤也，西垣正勝：オブジェクトのめり込みを利用した違和感 CAPTCHA の提案，2014 年暗号と情報セキュリティシンポジウム，2014.
⑯ Yuki Ikeya, Junya Kani, Yuta Yoneyama, and Masakatsu Nishigaki: An image-based CAPTCHA using sophisticated mental rotation, at International Workshop on Security 2013, 2013.
⑰ Junya Kani, Masakatsu Nishigaki: Gamified CAPTCHA, 2013 International Conference on Human-Computer Interaction, 2013.
⑱ 池谷勇樹，可児潤也，米山裕太，西垣正勝：メンタルローテーションを利用した画像 CAPTCHA の提案, 日本セキュリティ・マネジメント学会 2013，2013.

〔その他〕
ホームページ
https://wwp.shizuoka.ac.jp/nishigaki/

６．研究組織

(1)研究代表者
西垣　正勝（NISHIGAKI，Masakatsu）
静岡大学・創造科学技術大学院・教授
研究者番号：20283335

(2)研究分担者
なし

(3)連携研究者
なし

(4)研究協力者
なし