視覚の補完機能を利用した 文字型CAPTCHAの一検討

西 秀峻[1]　鎌田 大貴[1]　臼崎 翔太郎[1]　油田 健太郎[1]　山場 久昭[1]　朴 美娘[2]　岡崎 直宣[1]

概要：従来の CAPTCHA 技術が抱える課題に対応するため，人間の視覚補完機能を利用した新しい文字型 CAPTCHA を提案する．具体的には，中央を黒塗りで隠した文字を見せ、その文字を答えさせる。文字の大部分を隠しても人間は文字を補完できるため、人間の正答率を保ちつつ、機械認識を阻害できる。本研究では意味の近い熟語を複数個並べて読み取らせる方法を取り、人間が読み取りやすくする工夫をしている。提案 CAPTCHA の実用性とセキュリティ性能の調査を行った結果，平均正答率 は 80 %で，SUS スコア は 85.4 を記録したため実用性があると分かった．また，テンプレートマッチングを用いた攻撃実験を実施した．

キーワード：文字型 CAPTCHA、視覚的補完機能、セキュリティ、テンプレートマッチング

Study on Text-based CAPTCHA Using Visual Completion Mechanism

Hidetaka Nishi[1]　Kamada taiki[1]　Shotaro Usuzaki[1]　Kentaro Aburada[1]　Hisaaki Yamaba[1]
Mirang Park[2]　Naonobu Okazaki[1]

Abstract: We propose a new text-based CAPTCHA using human visual completion to address traditional CAPTCHA issues. Characters are partially blacked out, requiring users to recognize them. Humans can complete missing parts, maintaining accuracy while blocking machine recognition. We use similar-word phrases to enhance readability. Tests showed 80% accuracy and an SUS score of 85.4, confirming usability. We also conducted an attack experiment using template matching.

Keywords: Text-based CAPTCHA, Visual Completion Function, Security, Template Matching

1. はじめに

近年，インターネットの普及とともに，Web サービスの利用が日常生活に欠かせないものとなっている．しかし，自動プログラム（以下，ボット）による不正行為も増加しており，アカウントの大量取得やスパム投稿といった問題が深刻化している．このような不正利用への対策として，CAPTCHA（Completely Automated Public Turing test to tell Computers and Humans Apart）[1] と呼ばれる，機械でなく人間であることを証明する逆チューリングテストが開発され，広く利用されている．

CAPTCHA には，歪んだ文字列を解読する文字型や，画像の中から指定された条件に合致するものを選択する画像型など，さまざまな形式が存在する．しかし近年，OCR（Optical Character Recognition）[2] 技術や機械学習技術の発展により，これらの CAPTCHA がコンピュータによって容易に突破される事例が増えている．特に画像型 CAPTCHA では，画像認識技術の進歩により，ボットが高い精度で突破可能となっているだけでなく，近年では AI 技術の進展により，チャットボット AI を用いて CAPTCHA が簡単に解かれてしまう事例も挙げられている [3].

[1] 宮崎大学
University of Miyazaki
[2] 神奈川工科大学
Kanagawa Institute of Technology

これらの背景を踏まえ，機械による突破が難しく，かつユーザにとって負担が少ない新たな文字型 CAPTCHA の開発が求められている．本研究では，この課題に対し新しい視点を取り入れた解決策を模索し，より高い機械攻撃耐性を持つ文字型 CAPTCHA を提案することを目指す．

以降，2 章では関連研究について説明する．3 章では提案手法について述べる．4 章では評価実験と考察について述べる．6 章ではまとめと今後の課題について述べる．

2. 関連研究

2.1 CAPTCHA

CAPTCHA（Completely Automated Public Turing test to tell Computers and Humans Apart）[1] は，人間にとっては比較的容易に解答可能だが，機械にとっては解答が困難な問題を web サービスを利用するユーザに出題し，その解答結果を基に人間と機械を区別する技術である．CAPTCHA は，人工知能（AI），ネットワークセキュリティ，自然言語処理，コンピュータービジョン，信号処理といった多岐にわたる研究分野に関連しており，これらの技術的発展が CAPTCHA の設計や運用に直接的な影響を与えている．また，オンライン投票や電子メールの登録，検索エンジンの利用など，さまざまなネットワークアプリケーションにおいて，不正なボットによる大量利用やスパム行為を防止する目的で広く利用されている．具体的には，CAPTCHA は人間の認識能力を利用することで，機械による自動化された不正操作を排除する役割を果たしており，web サービスのセキュリティ向上に貢献している．この技術は，インターネットが発展する中でますます重要性を増しており，AI の進化に伴う新たな課題に対応するため，進化を続けている．

2.2 代表的な CAPTCHA の種類

CAPTCHA で人間と機械を区別するために出題される問題は多岐にわたる．ここでは代表的な CAPTCHA を説明する．

2.2.1 文字型 CAPTCHA

文字型 CAPTCHA は, 最も広く普及している CAPTCHA の出題形式であり，その基本的な仕組みは，文字画像に歪みやノイズを付加してユーザに提示し，画像内の文字列を正確にテキストボックスに入力できるかどうかで人間とボットを区別するものである．この形式はシンプルかつ効果的で，多くの web サービスで採用されている．しかし近年，OCR 技術や機械学習技術の飛躍的な進歩により，機械によって容易に解読されることが問題となっている．そのため，提示する文字列の形状をより複雑に歪ませたり，ノイズや背景模様を増やしたりすることで機械攻撃への耐性を高めている．しかし，これらの対策は人間のユーザにとっても解読を困難にし，正答率が下がることでユーザ体験や利便性が著しく低下するという課題を抱えている [5].

2.2.2 画像型 CAPTCHA

画像型 CAPTCHA は，人間が持つ高度な画像認識能力を活用し，人間と機械を区別する CAPTCHA である．このタイプの CAPTCHA では，ユーザに画像の内容や画像間の共通点を解答させることで人間であるかどうかを判断する．代表的な例として，動物の画像を使用した Asirra [6] や，広く利用されている reCAPTCHA [7] などが挙げられる．画像内容を正確に理解し，特定の条件に合致する画像を選ぶことは，画像認識能力を必要とし，機械にとって困難な作業である．

しかし近年，ディープラーニングをはじめとする機械学習技術の飛躍的な発展により，画像型 CAPTCHA は機械によって高精度で解読されることが問題視されている [9]. 従って，このような技術の進歩により，画像型 CAPTCHA のセキュリティ効果が低下しつつあることが指摘されている．

2.3 人間の視覚補完機能を利用した CAPTCHA

上妻らの研究 [10] では，人間が持つ視覚の補完機能「アモーダル補完」を応用した CAPTCHA を提案した．当該手法では，文字の一部を隠した欠損画像（図 1a）と，その欠損部を隠すためのマスク画像（図 1b）の 2 枚を提示し，これらを図 2 のように適切に重ね合わせることで文字認識を可能にしている．アモーダル補完とは，人間が隠された部分を視覚的に補完して認識できる現象のことであり，この研究では静止画像形式でこれを利用している．

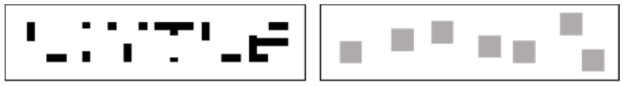
上妻らの提案手法では，反転ノイズ重畳や文字幅・間隔の不均一化といった認識困難化手法を組み合わせることで，自動文字認識技術に対する耐性を高めた．評価実験の結果，認識精度を従来手法の 94.6%から 78.8%に低減させることに成功し，機械攻撃耐性が向上したことが確認された．また，人間による認識実験では，アモーダル補完の効果によって，欠損画像とマスク画像を重ね合わせた場合に文字を容易に認識できることが示された．

一方で，画像の重ね合わせ操作において被験者が負担を感じる場合があることも明らかになり，操作負担の軽減や解答時間の短縮を可能にする改良の必要性が指摘された．この研究の提案手法は，文字認識に対する機械攻撃耐性を向上させる新たな可能性を示しており，人間にとっての負担を軽減しつつ，ボットによる突破を防ぐ技術として期待されている．

3. 提案手法

3.1 概要

本研究で提案する CAPTCHA は，X においてオゾン氏が投稿した「思ったより漢字って隠されてても読める人間の能力凄くない？？」[11] というコメントと共に掲載され



(a) 欠損画像の例　　(b) マスク画像の例

図 1: 重ね合わせる前の画像
(文献 [10] より引用)

図 2: 画像の重ね合わせを行った画像の例
(文献 [10] より引用)

た画像を参考にしている．この画像は，中央に太い横線が重なった 3 つの漢字二字熟語を提示するものであり，本研究ではこれを CAPTCHA として利用した．具体的には，提示されたすべての漢字の読み仮名を正確に入力させる文字型 CAPTCHA である．

また，本研究では問題の生成を効率化するために Google Fonts [12] を利用している．

文字サイズは 100 px，横線の太さは 60 px に設定している．

3.2 提案 CAPTCHA に利用するフォント

提案 CAPTCHA は，文字を太い線で隠す都合上，フォントの形によって認識結果に影響を与えることが考えられる．一般的なゴシック体フォントである”Noto-Sans.ttf” [13] と筆で書かれた文字を基に設計された”YujiSyuku-Regular.ttf” [14] と細い文字を特徴とする”HinaMincho-Regular.ttf” [15] について調査を行い，より人間が認識しやすいフォントの選定を行った．”Noto-Sans.ttf”を用いて画像を作成した例を図 3 に示す．本フォントでは，一部の見慣れていない書体や漢字における止めや跳ねが明確でないため，人間の視覚補完機能が十分に作用せず，解答困難な熟語が多く確認された．

”YujiSyuku-Regular.ttf”を用いて画像を作成した例を図 4 に示す．本フォントでは，止めや跳ねがはっきりしており，人間の視覚補完機能が効果的に働いた結果，隠された文字を認識できるケースが増加した．しかしながら，フォント自体が太いことに起因して，隠蔽されていない部分から得られる漢字の特徴が減少し，別の漢字と誤認されるケースが多く確認された．

”HinaMincho-Regular.ttf”を用いて画像作成した例を図 5 に示す．本フォントは手描き風ではないものの，文字の止めや跳ねが明確であり，かつ線が細いため，隠蔽されていない部分の特徴がより際立ち，人間の視覚補完機能を効果的に引き出すことが可能であることが確認された．

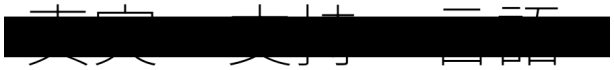


図 3: ゴシック体”真実支持言語”の例

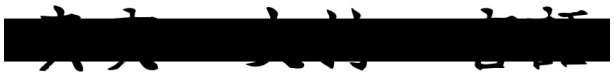


図 4: 手描きフォント”真実支持言語”の例

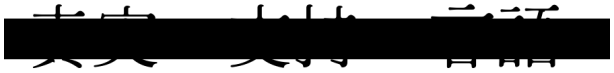


図 5: 明朝体”真実支持言語”の例

図 6: 不鮮明化した文字の例

図 7: アモーダル補完を利用した加工の例

従って，提案 CAPTCHA に使用するフォントには”HinaMincho-Regular.ttf”を用いる．

3.3 文字の加工方法

本研究では，テンプレートマッチングに対する耐性を持たせるために，2 つの加工方法の調査実験を行った．

(1) 文字の不鮮明化．

(2) アモーダル補完を利用した加工．

これらの加工方法について以下で紹介する．

3.4 文字の不鮮明化

図 6 は，文字の不鮮明化を適用した画像である．この加工方法は，文字の視認性を著しく低下させるものである．

3.5 アモーダル補完を利用した加工

図 7 は，アモーダル補完を利用した加工を適用した画像である．この加工方法は，参考文献 [10] で提案された手法である．

図 8: 提案 CAPTCHA1 問の画面例”自由遺伝判明”

3.6 提案する CAPTCHA

提案する CAPTCHA は，表示された画像に描かれた 3 つの漢字二字熟語の読み仮名をユーザが入力する形式である．提案 CAPTCHA の例を図 8 に示す．ユーザが入力した読み仮名が不正解であった場合，または再生成ボタンが押された場合には，新たに画像を生成して再表示する仕様となっている．

4. 評価実験と考察

本章では，提案手法に対する評価実験と考察を行う．以下，4.1 節では提案する CAPTCHA の実用性についての評価実験を行う．5 節ではテンプレートマッチングを利用した攻撃手法への耐性を調べる実験を行う．

4.1 実用性についての評価験

3.6 節で自動生成で作成された問題が，人間が正確に読み仮名を入力できるかどうかを調べる実験を行う．実験から取得した人間の正答率，平均解答時間と実験終了後に行った SUS（System Usability Scale Facts）[16] を用いたアンケートを評価指標として利用する．

4.2 実験方法

実験は，宮崎大学工学部の学生 10 名を対象に行った．本実験では提案した CAPTCHA を計 10 問出題した．提案 CAPTCHA に慣れるためのデモンストレーション 5 問と，実際に正答率や解答時間の計測を行う本番の 5 問である．出題する 10 問は固定しており，すべての被験者が同じ問題を解く．評価は，1 問当たりの正答率，解答時間，入力時間を調べる．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に答えてもらう．

4.3 ユーザビリティに関するアンケート調査

被験者には本実験の後に，SUS（System Usability Scale Facts）[16] によるアンケートを実施した．このアンケートの結果により提案 CAPTCHA の実用性を確認する．SUS は 1986 年に John Brooke により開発されたユーザビリティの評価のために多く利用されている 10 項目の質問票である．偶数項目はネガティブな質問，奇数項目はポジティブな質問となっている．文献 [17] より SUS の平均点数は 68 である．また，ユーザビリティの等級スケールは以下表 1 のようになっている．よって本実験で得られた SUS の得点が 68 以上であった場合，最低限のユーザビリティが確保できたと考えられる．

表 1: SUS スコアの等級スケール
(文献 [18] より引用)

SUS スコア	グレード	評価
>80.3	A	非常に良い
68 - 80.3	B	良い
68	C	平均
51 - 68	D	悪い
<51	F	非常に悪い

回答項目は，1（全くそう思わない）から 5（強くそう思う）の 5 段階評価から成り立つ．SUS の評価値の集計方法は奇数項目は回答番号から 1 を引く，偶数項目は 5 から回答項目を引く．その後にすべてを足し合わせた合計値を 2.5 倍した値が SUS の評価値となる．評価値 S は式 (1) で表すことができる．

$$S = (\sum_{i=1}^{10} N_i) \times 2.5 \quad (1)$$

(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) たいていの人は，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．

4.4 実験結果

問題ごとの平均正答率，平均解答時間，および平均入力時間を表 2 に示す．平均正答率は，被験者ごとに出題された問題に正しく解答できた割合の平均を指す．平均解答時間は，画像が表示されてから被験者が解答を理解するまで

表 2: 1 問あたりの正答率および所要時間

	問題 1	問題 2	問題 3	問題 4	問題 5
平均正答率	20%	100%	70%	80%	90%
正解時平均解答時間	3.94 秒	4.19 秒	4.50 秒	5.00 秒	3.18 秒
不正解時平均解答時間	12.25 秒	-	9.06 秒	20.57 秒	6.71 秒
平均入力時間	15.46 秒	12.27 秒	10.15 秒	16.39 秒	9.03 秒

表 3: 全 5 問の実験結果のまとめ

平均正答率（%）	72
正解時平均解答時間（秒）	4.15
平均入力時間（秒）	12.66
正解時最大解答時間（秒）	18.16
正解時最小解答時間（秒）	0.95
SUS スコア	86.75

図 9: 評価実験問題 1 の画像”条約経験福音”

の 1 問当たりの平均時間を示し，平均入力時間は，被験者が解答を理解してからその答えをタイピングし終えるまでの 1 問当たりの平均時間を表す．

提案手法における全 5 問の平均正答率は表 3 より 72%であり，人間による認識が可能であることが示された．これらの結果から，問題ごとに正答率に偏りがあることが確認された．さらに，提案手法の平均 SUS スコアは 86.75 であり，表 1 からグレード A に該当する．このことから，本手法の CAPTCHA はユーザビリティが十分に確保されていると評価できる．

また，本研究では，正解時の平均解答時間 4.15 秒であり，平均入力時間 12.66 秒で合計すると 16.81 秒であった．関連研究 [10] では，CAPTCHA の平均解答時間が 20.44 秒以上であると報告されており，提案 CAPTCHA の方が 3.63 秒短いことがわかった．

今回の評価実験では，被験者にとって難易度の高い問題であった場合でも解答してもらったため，問題の正答率は低いもので 20%となってしまった．しかし，それ以外の問題における正答率は 70%を超えており，再生成機能を活用することにより，人間にとって使いやすい CAPTCHA となることが期待される．

5. 機械耐性についての評価実験

3.6 節で自動生成で作成された問題が，テンプレートマッチングを利用した攻撃手法への耐性を持つことを確認する実験を行う。

5.1 実験方法

テンプレートマッチングによる攻撃方法の概要は，以下の手順で行われる．

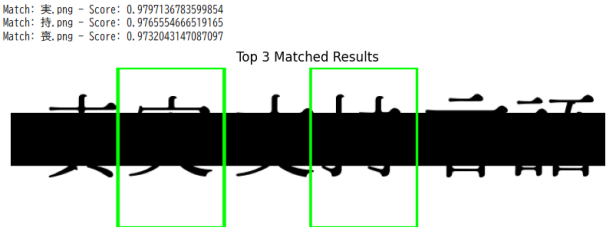


図 10: 3.3 節の加工なし CAPTCHA 画像

(1) 常用漢字 2136 文字のデータセットを準備する．

(2) データセット内の漢字画像を，本研究の CAPTCHA 画像と同様に横線付き画像へと加工する．

(3) 加工した漢字画像を用いて，CAPTCHA 画像とテンプレートマッチングを行う．

(4) 相関値が最も高い漢字を特定し，出力する．

5.2 実験結果

図 10 は，3.3 節で説明した加工を施した CAPTCHA 画像である．この例では，テンプレートマッチングによって相関値が最も高い漢字として「真実」の「実」が出力されている．さらに，相関値が二番目に高い漢字として「支持」の「持」が出力されていることから，加工を行わない場合にはテンプレートマッチングに対する耐性がないことが明らかとなった．

6. おわりに

本研究では，人間の視覚補完機能を活用した文字型 CAPTCHA を提案した．評価実験の結果，提案した CAPTCHA の SUS スコアは 86.75 と非常に高い評価を得ており，ユーザが操作しやすく，利用しやすい仕組みであることが示された．また，関連研究 [10] において CAPTCHA の平均解答時間が 20.44 秒以上であると報告されているのに対し，提案 CAPTCHA の正解時の平均解答時間と平均入力時間の合計は 16.81 秒であり，およそ 3.63 秒の短縮を達成することができた．

一方で，テンプレートマッチングに対する耐性が低いという課題が残された．文字の認識耐性を調べる際，文字を不鮮明化する方法や，アモーダル補完を用いる方法を試したが両者ともテンプレートマッチングによって認識された．テンプレートマッチングに耐性を持つような，文字の加工が必要である．

謝辞 本研究は JSPS 科研費 JP24K14917 の助成を受けたものです．

参考文献

[1] Luis von Ahn, Manuel Blum, and John Langford: Telling humans and computers apart automatically, Commun. ACM, Vol. 47, No. 2, p. 56–60, feb 2004.
[2] captchas.net, http://captchas.net/, (Accessed on 01/21/2025).
[3] 「死んだ祖母の形見」とウソをつくことで bing チャットに captcha の画像認識を解かせることに成功, https://gigazine.net/news/20231003-bing-chat-dead-grandma-tricks-solving-captcha/, (Accessed on 01/30/2024).
[4] Free captcha-service, https://captchas.net/, (Accessed on 01/21/2025).
[5] K. Popat H.S. Baird: Human interactive proofs and document image analysis, Proceedings of the International Workshop on Document Analysis Systems, pp. 507–518, 2002.
[6] Jeremy Elson, John R. Douceur, Jon Howell, and Jared Saul: Asirra: A captcha that exploits interest-aligned manual image categorization, Vol. 92, pp. 366–374, 2007.
[7] Luis Von Ahn, Benjamin Maurer, Colin McMillen, David Abraham, and Manuel Blum: recaptcha: Human-based character recognition via web security measures, Science, Vol. 321, No. 5895, pp. 1465–1468, 2008.
[8] recaptcha, https://www.google.com/recaptcha/about/, (Accessed on 01/21/2024).
[9] Fatmah H.Alqahtani and Fawaz A.Alsulaiman: Is image-based captcha secure against attacks based on machine learning? an experimental study, Computers&Security, Vol. 88, No. 101635, Jan 2020.
[10] 上妻拓也, 梅澤猛, 大澤範高: アモーダル補完を応用した文字型 CAPTCHA, 情報処理学会論文誌, Vol. 62, No. 6, pp. 1358–1367, June 2021.
[11] 「思ったより漢字って隠されてても読める人間の能力凄くない？？」, https://x.com/Ozone_Nazo0803/status/1849032747911696798, (Accessed on 10/29/2024).
[12] Googlefonts, https://fonts.google.com/, (Accessed on 11/21/2024).
[13] Googlefonts"notosans", https://fonts.google.com/noto/specimen/Noto+Sans+JP, (Accessed on 11/21/2024).
[14] Googlefonts"yujisyuku", https://fonts.google.com/specimen/Yuji+Syuku, (Accessed on 12/06/2024).
[15] Googlefonts"hina mincho", https://fonts.google.com/specimen/Hina+Mincho, (Accessed on 12/13/2024).
[16] System usability scale (sus) — usability.gov, https://www.usability.gov/how-to-and-tools/methods/system-usability-scale.html, (Accessed on 01/23/2024).
[17] Jeff Sauro and James R Lewis: Quantifying the user experience: Practical statistics for user research, Morgan Kaufmann, 2016.
[18] Medium, https://uxplanet.org/how-to-measure-product-usability-with-the-system-usability-scale-sus-score-69f3875b858f, (Accessed on 02/14/2025).