Computer Security Symposium 2013
21 - 23 October 2013

文字認識攻撃に耐性をもつランダム妨害図形を用いた画像ベースCAPTCHA方式の検討

田村 拓己† 久保田 真一郎† 朴 美娘‡ 岡崎 直宣†

†宮崎大学
889-2192 宮崎県宮崎市学園木花台西 1-1
tf13005@student.miyazaki-u.ac.jp

‡神奈川工科大学
243-0292 神奈川県厚木市下荻野 1030

あらまし ボットによるWebサービスの不正利用に対抗するために，CAPTCHAと呼ばれる反転チューリングテストが広く利用されている．しかし，近年文字認識技術が発達し，高い確率でテストが突破されるなど，その脆弱性が指摘されている．さらに，高度化するボットの文字認識技術に対抗し解読難度を高くすることに伴って，利便性が極端に低下してしまう問題があった．本稿では，人間特有の画像認識能力を利用することで，高い利便性を実現することを目指した新たな画像ベースCAPTCHA方式を提案する．提案手法は，提示画像の中に答えとなる文字を表示しないことで文字認識機能を有するボットによる攻撃に耐性を持たせることを特長とする．

An Examination of an Image-based CAPTCHA Using Random Obstruction Figures to Resist OCR-based Bot-attack

Takumi Tamura† Shin-ichiro Kubota† Mirang Park‡ Naonobu Okazaki†

†University of Miyazaki
1-1 Gakuen-kibanadai-nishi, Miyazaki, Miyazaki 889-2192, JAPAN
tf13005@student.miyazaki-u.ac.jp

‡Kanagawa Institute of Technology
1030 Shimo-ogino, Atsugi, Kanagawa 243-0292, JAPAN

Abstract A reversal Turing test called CAPTCHA is used in many Web-sites in order to prevent from bot-attack. However, Optical Character Recognition technology and the automatically breaking technology against CAPTCHA has developed, and many researchers have pointed out the vulnerability of CAPTCHA. In this paper, we propose a new image-based CAPTCHA using random obstruction figures, to achieve high usability and high resistance against OCR-based bot-attack. The proposed method has a resistance against the bot-attack because of displaying an enhanced image which include images to indicate an answer object but not answer characters.

1 はじめに

近年，Webサービスの普及により，誰でも様々なサービスを利用することが可能となっている．しかし，それらの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使用し，不正にサービスを利用するという悪質な行為が問題視されている．このような問題を防止するためには，人間とボットを識別する反転チューリングテストが必要となり，現在，CAPTCHAと呼ばれる方式が広く利用されている [1]．CAPTCHA

とはチャレンジ/レスポンス型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．一般的に利用されている手法としては，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がある（**図 1**）．

しかし，CAPTCHA を自動的に突破する技術が発達し，その脆弱性が多くの研究者に指摘されている．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）機能を備えるボットが出現している [2][3]．その対策として，文字列に加える変形やノイズを大きくすることによってボットを排除する確率を向上させることはできるが，そのような文字は人間にとっても認識が困難になるため，人間の正答率まで低下させてしまう．この問題に対し，画像や音声をベースにした，人間のより高度な知識処理を利用する CAPTCHA [4] も提案されているものの，一部の手法ではボットによる突破が可能であるという指摘もされている [5]．さらに，ボットの能力（CAPCTHA 解読アルゴリズム，および PC の CPU パワー）は，日々強化されている．したがって，高度な機能を有するボットに対して耐性をもつ，新たな CAPTCHA の導入が強く望まれる．ただし，CAPTCHA は，安全性とユーザビリティがトレードオフの関係になっていることに留意しなければならない．

そこで本論文では，画像ベースの新たな CAPTCHA 方式を提案する．本提案手法では，人間の視覚補完を利用することと，画像を使用することでユーザビリティを確保しつつ，提示画像の中に答えとなる文字を全く用いないことで，OCR 機能を備えるボットの突破率を低下させる．また，ランダムで多数の種類の妨害図形を用いることと，使用画像を毎回インターネット上で検索し収集することでデータベースを用いた攻撃に対して耐性を持たせる．

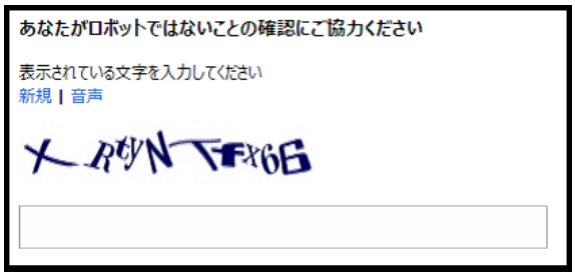

図 1: Microsoft 社のサイトで利用されている CAPTCHA（文字列 CAPTCHA）[6]

2 関連研究

2.1 CAPTCHA について

CAPTCHA は 2000 年にカーネギーメロン大学の Luis von Ahn， Manuel Blum， Nicholas Hopper， John Langford によって考案された．人間には容易に解くことが可能であるが，コンピュータには解くことが難しいものを出題し，正しい解答をした者を人間と判断する．

次節から既存の CAPTCHA について紹介する．

2.2 文字列 CAPTCHA

現在，最も広く利用されている CAPTCHA は文字列 CAPTCHA である．文字列 CAPTCHA には Gimpy [7]，EZ-Gimpy [7]，r-Gimpy [8]，reCAPTCHA [9] などがある．

文字列 CAPTCHA として頻繁に使用される EZ-Gimpy 及び r-Gimpy は，1 つの単語，あるいはアルファベットと数字をランダムに並べた文字列の画像を歪ませて表示し，その答えをテキストボックスに入力させ，解答が正しければ解答者を人間と判別する．

文字列 CAPTCHA のメリットとしては，システムとして単純であり，Web サイトに簡単に取り入れることが可能である点と，総当たり攻撃に高い耐性を持つ点が挙げられる．reCAPTCHA については，書籍電子化を同時に行うことができるというメリットもある．

これに対し，文字列 CAPTCHA のデメリットとしてはユーザビリティの低さや，近年の OCR（自動文字認識）の性能向上により，ボットでも

簡単に文字を認識できるようになっていることが挙げられる．文字列 CAPTCHA は平均して 10 文字以上の文字のひとつひとつを認識しながら入力を繰り返すため，ユーザビリティは低くなる．また近年は，文字列画像の難読化も行われており，ノイズや歪みが強化されているため，そのような文字を認識するのは煩雑さが増すと考えられる．さらに，近年の研究で，OCR 機能を用いた突破テストを実施した Mori らは，191 個の EZ-Gimpy に対して攻撃テストを行い，結果は 83 %の突破率であったと報告した [7]. reCAPTCHA も OCR に対しての耐性はないため，同様のデメリットがある．

2.3 画像 CAPTCHA

画像 CAPTCHA は文字列を使用せず，具体物の画像を用いることで人間と機械を判別する．多くの方式で，選択や分類といった手法が用いられている．主な画像 CAPTCHA には，Asirra [4]，4 コマ漫画 CAPTCHA [10] などがある．

ここでは例として Asirra を挙げる．Asirra は，人間とボットのイヌとネコを見分ける能力の違いに基づいている．利用者は提示された 12 枚のイヌまたはネコの画像のうち，ネコの画像を全て選択する．ネコの画像を正しく選択できれば，利用者を人間と判別する．

画像 CAPTCHA のメリットは，文字列 CAPTCHA と違い多くの場合文字より大きな画像を用いて人間の判断を促すことができる点，OCR 機能を用いたボットに対する耐性を考慮しなくても良い点が挙げられる．

デメリットとしては，文字列方式の CAPTCHA に比べて大きな表示スペースを使うことや総当り攻撃に対する脆弱性，データベース攻撃に対する脆弱性が挙げられる．画像 CAPTCHA では，画像の選択や分類を手法に取り入れている場合が多いため，総当り数を確保することが難しく総当たり攻撃に対する耐性が低くなってしまう．総当り攻撃に対する耐性をあげる場合，選択する画像を増やす，分類する種類を増やすなどの手法が考えられるが，それらの手法はユーザビリティが低下してしまう．また，近年，サポートベクターマシン（SVM）を用いた機械学習によって，10.3% の確率で Asirra が破られたことが報告されている [5].

2.4 動画 CAPTCHA

動画ベースの CAPTCHA は，基本的には文字列方式や画像方式の拡張方式と言える．NuCAPTCHA [11] やワンモア CAPTCHA [12] などがある．文字列 CAPTCHA を拡張した方式である NuCAPTCHA では，複数のフォントを用いたランダムな文字列が動画で表示され，ユーザは動画上部に表示される色指定などを読み取り，動画中に流れる文字列の中から該当文字列をテキストボックスに入力する．

動画 CAPTCHA のメリットとしては，動画を用いることによって，例えば従来の文字列 CAPTCHA より問題の文字数を少なくすることができるため，認識という面において高いユーザビリティを実現できることが挙げられる．

デメリットとしては，文字列 CAPTCHA の拡張方式である場合，OCR を用いたボットに対する脆弱性や，動画再生時間がユーザビリティに影響する点が挙げられる．動画があまりにも長い場合，ユーザはその動画の再生時間と回答を入力する時間をその CAPTCHA に拘束されるため，時間という面においてユーザビリティが低下すると考えられる．

3 提案手法

本章では，3.1 で提案手法に至る経緯を説明し，3.2 で提案手法の目的を述べ，3.3 で満たすべき要件について説明し，3.4 で実際に提案手法を用いて CAPTCHA 画像を生成する手順を紹介する．

以降，提案する CAPTCHA 方式を IC-CAPTCHA（Image-based Character input type CAPTCHA）と呼ぶ．

3.1 基本方針

既存の CAPTCHA の問題点を克服する新たな CAPTCHA の作成を考えた結果，できるだ

け実用的であり，認証する際に時間がかからないものを目指した．CAPTCHA には文字ベースと画像ベースの大きく分けて 2 つの方式が存在するが，提案手法では画像ベースを選択した．CAPTCHA には動画ベースも存在するが，これは，基本的に文字列方式か画像方式の拡張方式であるとの考えから基本となる手法からは除外して考えた．画像ベースを選択した理由としては，OCR 機能を搭載したボットの能力は日々強力になっており，OCR ソフトの本来の使い道から考えても，これからもさらなる発展をすることが予想されるため，文字列を用いた CAPTCHA には，たとえ，時間制限などを用いたとしても限界があると考えたためである．

実用的な画像 CAPTCHA を目指す中で，人間の視覚補完能力を生かすことはできないかと考えた．人間であれば，画像を見たときに少々欠損した画像であっても，その画像がなんの画像であるか判別が可能である．そこで，ある名詞の画像に妨害図形を上書きすることで，総当り攻撃や OCR ボットによる攻撃に耐性をもたせつつ，名詞の単語を入力するだけ，という実用的な CAPTCHA ができるのではないかと考えた．ただし，画像ベース CAPTCHA であるので，システム内の画像になるべく限界を持たせないようにするため，CAPTCHA で提示する元画像は Web 上より，画像検索を用いて取得することとした．

3.2 目的

3.1 より，提案手法には画像 CAPTCHA を採用したが，既存の画像 CAPTCHA には，総当り攻撃に対する脆弱性とデータベース攻撃に対する脆弱性という問題があった．従って提案手法では，画像 CAPTCHA におけるデータベース攻撃に対する耐性と総当たり攻撃に対する耐性に重点をおき，文字列画像を使用しないことで OCR 機能を持つボットに対する耐性をもたせ，ユーザビリティに配慮した CAPTCHA を作成することを目的とする．

3.3 満たすべき要件

3.2 より，提案手法の満たすべき要件を 2 つ挙げる．

（1）データベース攻撃に対する耐性

画像 CAPTCHA における脆弱性にデータベース攻撃がある．データベース攻撃には，攻撃者がデータベースを構築し，そのデータベースを利用して攻撃を行うものと，画像検索エンジンなどの Web 上のデータベースを用いて攻撃を行うものの 2 つの種類がある．そこで，本論文では，前者をデータベース攻撃，後者を画像検索攻撃と呼ぶ．

データベース攻撃というのは，問題画像とその解を記録したデータベースを構築し，このデータベースを用いて問題を解く方法である．これは，画像 CAPTCHA のシステムに使用される画像枚数が有限であることが原因となる．従って，データベース攻撃に対する耐性を持つ CAPTCHA を生成するためには，画像 CAPTCHA システム内で使用する画像枚数に，なるべく制限が無いようなシステムであることが望ましい．

画像検索攻撃とは，CAPTCHA の問題として提示された画像を Web 上の検索エンジンで検索することで，正答または正答に直結するキーワードを取得し，CAPTCHA を自動的に解くものである．画像検索攻撃に対する耐性については，問題として提示する画像を画像検索した際に，答えとなる名詞，または類似画像が判明しなければ良い．

（2）総当たり攻撃に対する耐性

総当たり攻撃というのは，暗号や暗証番号などで理論的にありうる全てのパターンを入力し解読する暗号解読法である．画像ベース CAPTCHA においては，方式自体が並べ替え方式，クリック方式，種類の分別方式，など解答の組み合わせの最大数が少ないものが多く，総当たり攻撃に対して脆弱であるといえる．画像ベースの CAPTCHA の場合，総当たり攻撃に対して，解答誤入力に回数制限をかける，解答時間に制限を設ける，などの対策を講じることを考慮しても，銀行 ATM に用いられている認証方式 PIN（1/10000）程度の強度を保つことが望

ましいと考える.

3.4 IC-CAPTCHA システム

本論文で提案するIC-CAPTCHAシステムは画像から容易に名詞を対応付けられる名詞群からなる名詞辞書と加工後画像のハッシュ値を登録したブルームフィルタを持つものとする．以下にIC-CAPTCHAシステムの画像生成手順を示す.

【IC-CAPTCHA システム画像生成手順】

Step1（名詞選択）: IC-CAPTCHA システムの持っている名詞辞書からランダムに1つの名詞を選ぶ.

Step2（画像取得）: その名詞，あるいは名詞に結びついている画像を検索エンジンを用いて検索し，その名詞に基づく画像を1枚取得する.

Step3（画像処理）: Step2の画像に，妨害図形の上書きをし，範囲処理（回転，モザイク，ぼかし，色反転等）の画像処理を施す.

Step4（妨害面積比率チェック）: Step3の後の画像の妨害図形の妨害領域の面積比率を計算し，その値が設定する閾値の範囲以内であるかを確認する．もし妨害領域の面積比率が設定する閾値の範囲に収まらない場合は，Step3に戻り，妨害図形を上書きし直す.

Step5（画像検索チェック）: 画像検索サイトを用い，Step3で生成される図形を入力値として画像検索を行った結果，その検索結果と正解名詞が一致しないかをチェックする.

Step6（ブルームフィルタチェック）: 画像のハッシュ値をとり，そのハッシュ値でブルームフィルタを検索し，まだ登録されていなければブルームフィルタに登録する．もし登録されている場合は，Step3に戻り，妨害図形を上書きし直す.

Step7（画像ストック）: Step4，5，6のチェックを通過した画像をStep1で選んだ名詞と結びつけて，画像ストックへ保存する.

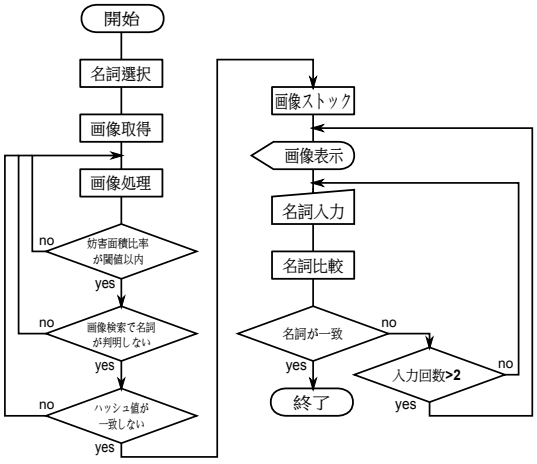

図 2: IC-CAPTCHA のフローチャート

Step8（画像提示）: アクセス・認証が必要なとき，画像ストックから画像をランダムに選択し，ユーザに画像を提示する.

Step9（名詞入力）: ユーザは，画像から名詞を推測し，テキストボックスに名詞を入力する.

Step10（名詞比較）: IC-CAPTCHA システムは，画像に結び付けられている名詞とユーザの入力した名詞を比較し，マッチしたならば，ユーザを人間と認識し，認証する．マッチしなかった場合，2回目まではStep9へ戻る．3回目は，Step8へ戻り，画像を変更する.

□

IC-CAPTCHAの画像生成手順のフローチャートを**図** 2に示す.

3.5 実装

（1）開発環境

開発言語はC++を，画像処理ライブラリはOpen CVを用い仮想PC上のUbuntu11.10にて画像生成プログラムを実装した.

（2）実装プログラム

IC-CAPTCHAシステムにおいては，どのようなCAPTCHA画像が生成されるかが，その安全性と利便性を決定付ける．そこで，本論文ではIC-CAPTCHA生成手順のうち，CAPTCHA

画像生成に必要なStep1（名詞選択），Step3（画像処理），Step8（画像提示），Step9（名詞入力），Step10（名詞比較）の部分を実装し，評価を行った．

Step2のWeb検索を用いた画像収集では，検討していたGoogle画像検索において自動プログラムを用いた使用に制限があったため，予め，素材となる複数の画像をそれぞれの名詞ごとに収集した．

Step3の実装プログラムの画像処理として，範囲処理では，モザイク，ぼかし，色反転，画像回転を用い，上書きする妨害図形には，円，楕円・扇型，ポリゴン（多角形），文字を用いた．実際に実装したプログラムによるIC-CAPTCHAシステムの生成画像は**図3**のようになる．

図 3: 生成画像の例（りんご）

4　評価と考察

この章では，まず静的な評価を行ったうえで，調査項目を整理し，必要な動的評価を行った．動的評価では，提案手法が既存手法のユーザビリティを改善していることを確認するため，実装したCAPTCHA生成プログラムで生成した画像を用いてユーザビリティ評価を行った．また，ユーザビリティ評価を行うにあたって，生成画像のパラメータを調整する必要があったため，生成画像の妨害図形の個数に関する事前調査も同時に行った．

4.1　各攻撃に対する耐性

この節では，提案手法においての各攻撃に対する耐性について説明する．

総当り攻撃に対する耐性については，Step1で使用する名詞辞書の単語登録数がそのまま総当たり攻撃に対する耐性となる．名詞辞書の単語登録数が少ないと総当たり攻撃に脆弱となってしまうが，他の方式と違い，画像の選択方式や分類方式を本提案手法は用いていないため，名詞辞書の登録数を増やすことは比較的容易である．また，登録単語数を増加させてもユーザの負担が増えることはないため，ユーザビリティが低下する心配はない．さらに，Step10において，1つの提示画像に対する名詞入力を3回までとすることで，総当り攻撃に対する耐性を強化する．ただし，実用レベルでの使用を考えるならば，名詞辞書の登録数は，10000語程度まで増やす必要がある．

また，Step2では検索エンジンを用いて画像を毎回検索し，収集することでデータベース攻撃に耐性を持たせる．もし，同じ画像を加工することになったとしても，ランダムな妨害図形と背景処理を施すため，加工後に全く同じ画像になることは実用上ない．そのため，一度問題として提示された画像を用いて行うデータベース攻撃は成り立ちにくい．

Step6では，ブルームフィルタチェックを行い，全く同一な画像をユーザに提示しないようにする機能を強化している．

Step4で，上書きする妨害図形について閾値の範囲を設け，妨害領域の面積比率が閾値の範囲を上回る場合を排除することで，妨害図形が多すぎて人間であっても名詞が何であるか判らない，という確率を下げる．

さらに，画像検索攻撃に関しては，Step5で画像検索チェックをすることで，妨害図形が上書きされている提示画像を攻撃者が再度画像検索にかけたとしても正解名詞が判明しないようにしている．

IC-CAPTCHAシステムでは，画像内に答えと結びつく文字列は全く表示されないため，OCR機能を持つボットに対しての耐性は考慮する必要はない．

表 1: 妨害図形数アンケート結果

妨害図形数	4-7	8	9	10	11	12	13	14	15-20
人数	0	1	2	2	4	0	0	1	0

4.2 ユーザビリティ

提案手法について，以下の動的評価を行った．

（1）妨害図形数に関する事前調査

人間が画像から名詞を判別するには，画像の妨害面積が関係しているが，今回，画像の面積比率チェックを実装していない．このため，ユーザビリティ評価を実施する際，適切な妨害図形数について調査を行う必要がある．そこで事前調査では，宮崎大学工学部情報システム工学科の大学生 10 名に，IC-CAPTCHA システムの生成画像の妨害図形数に関してアンケートを行った．具体的には，ある名詞の画像について妨害図形の個数を 4 から 20 までに変えた画像をそれぞれ 10 枚ずつ作成し，名詞を判別可能である妨害図形の最大の個数について聞いた．その結果を表 1 に示す．

同表の結果より，人間が名詞判別をする際に許容できる妨害図形数の最大値の平均は 10.4 となる．そこで，以下では，妨害図形数を 10 として評価を行った．

（2）ユーザビリティ評価

ユーザビリティ評価では，提案手法 IC-CAPTCHA が，既存 CAPTCHA と比べて使いやすいものとなっているかを調査することをその目的とする．具体的な評価方法としては，情報システム工学科の大学生 14 名に，文字列 CAPTCHA [6] と画像 CAPTCHA（Asirra [4]），提案手法の IC-CAPTCHA を各手法 10 回ずつ回答してもらい，その後，アンケート調査を実施した．アンケート項目とその評価点を表 2 に示す．ここで，各項目において，肯定的であるほどその評価点が高くなる．アンケートの結果を表 3 に示す．同表は，各項目の評価点の平均値を評価値として表している．また，CAPTCHA を解いてもらう際に，CAPTCHA の解答までに要する時間とその正否を調査した．その結果は表 4 のようになった．

表 3 より，5 つの質問事項全てでその評価値が IC-CAPTCHA，画像 CAPTCHA，文字列 CAPTCHA の順に良かった．また，表 4 より，IC-CAPTCHA は 2 つの既存手法より正答率が高く，平均所要時間が短いことがわかる．したがって，IC-CAPTCHA は実際に使用する際のユーザビリティにおいて他の 2 つの手法に比べて優れているといえる．

表 2: ユーザビリティ評価の評価項目

質問事項	印象語と評価点
解いていて楽しかったか？	楽しくない 1 点← →5 点 楽しい
解くことは面倒だったか？	面倒だ 1 点← →5 点 面倒ではない
解くことは簡単だったか？	難しい 1 点← →5 点 簡単だ
CAPTCHA が使いやすかったか？	使いにくい 1 点← →5 点 使いやすい
Web サービス上で使いたいか？	使いたくない 1 点← →5 点 使いたい

表 3: ユーザビリティ評価の結果（評価値）

質問事項	IC-CAPTCHA（提案手法）	文字列 CAPTCHA	Asirra（画像 CAPTCHA）
解いていて楽しかったか？	4.21	1.93	4.00
解くことは面倒だったか？	4.86	1.43	3.43
解くことは簡単だったか？	4.50	2.36	4.36
CAPTCHA が使いやすかったか？	4.57	2.00	3.79
Web サービス上で使いたいか？	4.29	2.29	3.43

表 4: 所要時間と正答率

	正答率（%）	平均所要時間（sec）
IC-CAPTCHA 提案手法:妨害図形数 10	97.85	6.34
文字列 CAPTCHA	72.14	15.45
Asirra	95.71	14.19

4.3 考察

ユーザビリティ評価から，既存の文字列 CAPTCHA，画像 CAPTCHA（Asirra）と比べて，提案手法の IC-CAPTCHA のほうが回答に要する所要時間が短く，正答率が高いという結果と提案手法が高いユーザビリティを有しているという結果を確認することができた．特に，回答所要時間では比較実験で用いた CAPTCHA の回答所要時間の平均値の半分以下の値となっており，実用的な CAPTCHA という要件は達成できていると考えられる．しかし，提案手法にも CAPTCHA テストに不合格であった場合が存在する．この中には，留学生による回答で，「みかん」の画像を提示した際,「lemon」という

回答がなされた例などがある．このように，国や地域など個人の育ってきた環境により同じ画像に対応付ける名詞に違いがあるため，考慮が必要である．

提案手法では，画像を Web 上から取得するため，取得された画像が，適切な名詞の画像であるかどうかは検索システムの精度に依存する．また，画像内に人物が写りこんでいる場合も想定され肖像権などの問題も存在する．しかし，この問題については，顔やナンバープレートに自動的にモザイクをいれる技術を用いることで回避できると考えている．

5 まとめ

本論文では，既存の CAPTCHA 手法のデータベース攻撃に対する脆弱性，総当り攻撃に対する脆弱性，OCR ボットに対する脆弱性，ユーザビリティの低さという問題点を改善する新たな手法である IC-CAPTCHA の提案を行った．提案手法では，Web 上から画像を毎回取得することで画像枚数になるべく制限をつけないようにすることと，色・形が毎回ランダムな妨害図形を上書きすること，文字入力方式にすることで総当り数を確保することによって，上記の問題の改善を目指した．また，ユーザビリティ評価と考察を行い，IC-CAPTCHA システムの有効性を示した．

今後は，名詞辞書の登録単語に階層的概念を用いてタグ付けを行うことで，正解名詞を判定する方法について検討したい．

参考文献

[1] L. von Ahn, M. Blum, N. Hopper, and J. Langford, “CAPTCHA: Telling humans and computers apart,” Advances in Cryptology, Eurocrypt’03, vol.2656 of Lect. Notes Comput. Sci.,pp.294-311, 2003.

[2] J. Yan and A.S.E. Ahmad, “Breaking visual CAPTCHAs with native pattern recognition algotithms,” 2007 Computer Security Applications Conference, pp.279-291, 2007.

[3] K. Chellapilla and P.Y. Simard, “Using machine learning to break visual human interaction proofs（HIPs）,” Advances in Neural Infomation Processing Systems, vol.17, pp.265-272, 2005.

[4] Jeremy Elson, John Douceur, Jon Howell and Jared Saul, “Asirra: a CAPTCHA that exploits interest-aligned manual image categorization,” Proceedings of the 14th ACM conference on Computer and Communications Security, pp. 366-374, October 2007.

[5] P.Golle, “Machine learning attacks against the asirra CAPTCHA,” Proc. 15th ACM conference on Computer and Communications Security, pp.535-542, 2008.

[6] “Microsoft”アカウント
`https://signup.live.com`

[7] Greg Mori, Jitendra Malik,“Recognizing Objects in Adversarial Clutter:Breaking a Visual CAPTCHA,” cvpr,pp.134, 2003 IEEE Computer Society Conference on Computer Vision and Pattern Recognition（CVPR ’03）- Volume 1, 2003.

[8] Gabriel Moy, Nathan Jones, Curt Harkless, and Randall Potter, “Distorition Estimation Techniques in Solving Visual CAPTCHAs,” proceedings of the 2004 IEEE Computer Society Conference on Computer Vision and Pattern Recognition（CVPR’04）, 2004.

[9] L. von Ahn, B. Maurer, C.McMillen, D. Abraham, and M. Blum, “reCAPTCHA:Humen-based character recognition via Web security measures,” Sience, vol.321, no.5895, pp.1465-1468, 2008.

[10] 鈴木 徳一郎，山本 匠，西垣 正勝，“4 コマ漫画 CAPTCHA の検討”，情報処理学会研究報告，IPSJ SIG Technical Report，Vol.2011-DPS-146 No.13，Vol.2011-CSEC-52 No.13，2011-03-10.

[11] “NuCAPTCHA”
`http://www.nucaptcha.com/`

[12] 可児 潤也，上松 晴信，西垣 正勝，“ワンモア CAPTCHA の提案”，The Institute of Electronics，Information and Communication Engineers，The 29th Symposium on Cryptography and Information Security Kanazawa，Japan，Jan. 30-Feb. 2，2012.