L-017

CAPTCHA リレーアタックのパフォーマンス低減手法の提案
Mitigating Third-Party Human Attacks on CAPTCHA with Video-based Method

小宮山 哲俊† 梅澤 猛† 大澤 範高†
Tetsutoshi Komiyama Takeshi Umezawa Noritaka Osawa

1. はじめに

これまで，悪意のあるユーザによる CAPTCHA の回避手法としては，光学文字認識(OCR)プログラムによる解読が主流であった．しかし，近年ではインターネット上の一般ユーザや低賃金労働者を利用して解読をさせる，リレーアタックとよばれる攻撃手法が用いられている．

リレーアタックでは，人間が画像の解読を行うため，機械を想定した難読化を行う従来の対策では効果がなく，新たな対策が求められている．

そこで本稿では，1 回あたりの CAPTCHA 解読に掛かる時間を長くすることで，低賃金労働者を利用したリレーアタックのパフォーマンスを低減させる手法を提案する．提案手法においては，動画像中に複数の CAPTCHA を挿入することで単位時間あたりに解読できる数を抑制し，悪意のあるユーザによる大量アクセスの防止を図る．

2. CAPTCHA リレーアタック

典型的な CAPTCHA リレーアタックでは，攻撃者が正規サイトから画像を取得し，予め登録された低賃金労働者へ転送する（図 1）．低賃金労働者は，受け取った画像を解読して返答することで金銭を得る．画像の解読を人間が行うため，OCR を困難にするための難読化では効果がない．

図1 CAPTCHA リレーアタックの一例

リレーアタック対策の先行研究としては，画像をリレーすることで生じる遅延時間によりリレーアタックを検出しようという手法[1]が提案されている．しかし，インターネットトラフィックの特性を考えると，リレーによる遅延はネットワークの遅延ジッタに比べて小さく，応答時間の差異からリレーアタックと正規アクセスを区別することは現実的でない．

3. 提案手法

本稿では，動画像を用いて低賃金労働者が単位時間あたりに解読可能な CAPTCHA の数を大幅に減らす手法を提案する．本手法はリレーアタックのパフォーマンスを実行不可能な程度まで低下させることが狙いである．

提案手法は，複数の CAPTCHA 画像を埋め込んだ動画像を用いて認証を行う．提案手法による実装例を図 2 に示す．ユーザは，動画像を再生し（①），画面に表示された CAPTCHA 画像を解読して入力を行う（②）．時間経過と共に表示される CAPTCHA 画像が変化し，ユーザはその都度解読した内容を追加入力する（③，④）．動画像の再生終了後に入力した文字列を送信することで，認証を行う（⑤）．正しく解答するためには，動画像を最初から最後まで確認する必要があるため，動画像の再生時間を調整することで低賃金労働者の解読パフォーマンスを低下させることが可能である．

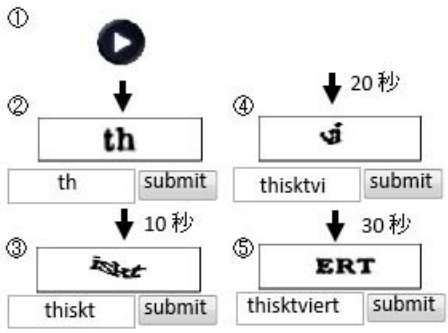

図2 提案手法の一例

3.1 正規ユーザへの影響

提案手法による認証には，動画像の再生分の時間が掛かるため，リレーアタックとは無関係の正規ユーザにとっても負担増が懸念される．しかし，正規ユーザは提案手法による認証を短時間で繰り返して行う必要はなく，メールアカウントの作成時など通常の利用においては，1 回認証に成功すれば十分である．従って，動画像を数十秒程度の長さに留めれば，正規ユーザへの影響は限定的であると考えられる．また，メールアカウントの作成手順を説明する動画像を利用して提案手法を適用することで，正規ユーザの負担とならない運用も可能である．

3.2 自動解析への耐性

動画像を用いた場合でもソフトウェアプログラムによる自動解析の恐れがあるが，動画像中に挿入する CAPTCHA 画像の表示時間間隔をランダムにしたり，CAPTCHA 画像を無関係な画像中に埋め込んだりすることで，画像の抽出や解析を困難にすることができる．

4. 評価実験

提案手法による認証を受ける際，実際にユーザが感じる負担を調べるために被験者による解読実験を行った．

4.1 実験方法

まず，提案手法による認証手続きとして，Google アカウントを作成する際の操作手順を説明する動画像を用意し，CAPTCHA 画像を 2 つ埋め込んで 60 秒間の動画像を作成した．つぎに，比較のために 2 種類の CAPTCHA 画像を用意した．ひとつは英字 10 字を解読する一般的な画

† 千葉大学大学院融合科学研究科 Graduate School of Advanced Integration Science, Chiba University

像、もうひとつは英字 40 字分の読解負荷が高いと思われる画像である．CAPTCHA の解読時間に関する既存研究[2]によると，1 文字あたりの入力時間は約 1.5 秒であることから，動画像の再生時間と同程度の読解時間を要する CAPTCHA 画像として，40 字のものを用意した．

被験者 4 人に対し，提案手法による動画像および比較用の 2 つの CAPTCHA 画像を提示して，それぞれの解読に掛かる時間を計測した．また，解読に感じた負担について 1（強く不同意）～5（強く同意）の 5 段階評価の質問紙調査を行った．なお，動画像に埋め込んだ CAPTCHA 画像 2 つに含まれる文字は合計で 8 文字であった．

4.2 結果

10 字，40 字の CAPTCHA 画像および提案手法による動画の解読に要した時間は，平均でそれぞれ 14 秒，45 秒，90 秒であった．また，英字 40 字の CAPTCHA 画像に対する正解率が 50%であったのに対し，提案手法の動画については正解率 100%であった．

質問紙調査の結果，Q1「提案手法の解読の負担は小さいか」，Q2「10 字の CAPTCHA 画像と比較した提案手法の負担は小さいか」，Q3「40 字の CAPTCHA 画像と比較した提案手法の負担は小さいか」の 3 つの設問に対して，図 3 に示す回答を得た． また，図 3 に提案手法，10 字，40 字の CAPTCHA の回答の正誤と解答時間を示す．

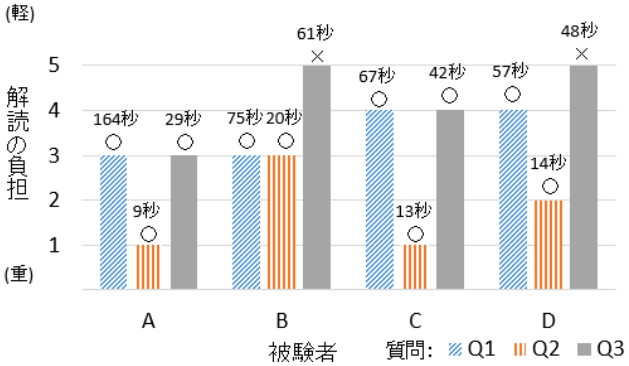

図3　提案手法の負担についての質問紙調査結果

5. 考察

5.1 正規ユーザへの影響

図 3 の Q1 において 1，2 と評価した回答がないため，提案手法の解読に大きな負担を感じた被験者はおらず，正規ユーザに対する負担増は小さいと考えられる．また，図 3 の Q2 では，3，4 と評価した回答がなく，Q3 では 1，2 と評価した回答がないため，従来型の CAPTCHA 画像 10 文字分よりは負担を感じるものの，40 文字分のものよりは負担が軽いと考えられる．従って，同じ 60 秒程度の解読時間が要求される場合，CAPTCHA の文字数を増やすよりも，提案手法を用いる方がユーザに掛かる負荷は小さいと考えられる．

5.2 リレーアタックへの効果

低賃金労働者を雇用する企業の Web ページによると，労働者によるテキストベースの CAPTCHA 解読時間は平均 9 秒である．提案手法の動画像の再生時間を 60 秒すると，解読 1 回あたりの所要時間は約 6.7 倍に増加し，低賃金労働者が単位時間あたりに解読可能な数は現在の 15%に減少すると試算できる．

つぎに，低賃金労働者が 1 日あたりに得られる賃金からリレーアタックへの効果を検討する．低賃金労働者が受け取る賃金は，解読 1,000 個あたり US$0.5～US$3 程度であるという報告[3]がある．1 日の労働時間を 8 時間としたときの，1 回当たりの解読時間と労働者が得る日給を試算した結果を図 4 に示す．図 4 より，解読時間を 40 秒にすると，解読 1,000 個あたりの賃金を US$3 としても日給は US$2.16 となる．これは，CAPTCHA 解読を行う低賃金労働者の存在が確認されているインドにおける全国最低賃金水準，日額 115 ルピー（US$2.3）を下回る．また，労働者の日給を固定とした場合，1 件あたりの解読コストが上昇するため，低賃金労働者を雇用する企業の負担となる．従って，提案手法により低賃金労働者を利用した CAPTCHA リレーアタックを実行の金銭コストの面から抑止できると考えられる．

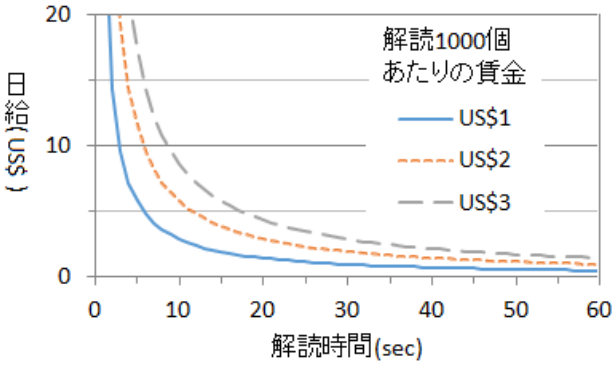

図4　1 回あたりの解読時間と労働者の日給の関係

6. おわりに

本稿では，CAPTCHA 画像を埋め込んだ動画像を用いた認証手法を提案した．提案手法は，解読 1 回あたりに掛かる時間を長くすることで，低賃金労働者を使ったリレーアタックを抑制できると考えられる．また，被験者実験の結果，リレーアタックとは無関係な正規ユーザにとって解読の負担が実用的な範囲内となることが示唆された．

今後は，多様な CAPTCHA 画像を使い文字列の違いによる影響について検討するとともに，被験者数を増やした実験を行うことで統計的な有意性について検証していきたい．

参考文献

[1] Truong, H. D., Turner, C. F. and Zou, C. C., “iCAPTCHA: The Next Generation of CAPTCHA Designed to Defend against 3rd Party Human Attacks”, IEEE ICC, Japan, pp. 1-6 (2011).
[2] Bursztein, E., Bethard, S., Fabry, C., Mitchell, J. C. and Jurafsky, D., “How Good Are Humans at Solving CAPTCHAs? A Large Scale Evaluation”, IEEE SP, pp. 399-413 (2010).
[3] Motoyama, M., Levchenko, K., Kanich, C., McCoy, D., Voelker, M. G. and Savage, S., “Re:CAPTCHAs-Understanding CATPCHA-Solving Services in an Economic Context”, USENIX Security Symposium, Washington, pp. 1-18 (2010).