4Z-6

スマートフォンの利用に適したCAPTCHA

鶴田裕輔† 高谷眞弓‡ 山村明弘††
秋田大学

1. はじめに

スマートフォンの普及とともにスマートフォンからの web へのアクセスが増加している. web セキュリティの一種に CAPTCHA が存在するが, これは既存のパソコンで利用することを前提として作成されており, スマートフォンで利用する際, 画面の大きさ, 文字の入力方式などの違いから利用しにくいものとなっている.

本論文では, スマートフォンの機能の一つであるタッチパネルに着目し, より利便性の高い CAPTCHA 手法の概要と, 評価テストを行った結果を報告する.

2. 提案手法概要

提案手法は, 人間とプログラムの文字入力の仕方の違いに着目した CAPTCHA 手法である. 提案手法はタッチパネル上に表示された画像をなぞることによって取得した座標データを利用して認証を行う. 認証手順は以下の通りである.

1. サーバはクライアントからテスト要請を受け取る.
2. サーバはクライアントに画像データを送信する.
3. クライアントに表示された画像をなぞり入力を行う.
4. 入力されたデータをサーバに送信する.
5. サーバはテスト結果の判定を行い, 結果を通知する.

本章の冒頭で述べたように提案手法は人間とプログラムの文字入力の仕方の違いに着目している. 人間の入力であれば, 連続した入力となることが予想される. 一方プログラムの入力の場合, 不連続な入力や同時入力となることが予想される. この違いを判定するために提案手法は, 表示する画像を一定の範囲ごとに格子状に区切り, どの範囲をどのような順番で通過したかを調べることで認証の可否を決定する.

CAPTCHA suitable for smartphone
† Yusuke Tsuruta, Akita University
‡ Mayumi Takaya, Akita University
††Akihiro Yamamura, Akita University

漢数字「一」の入力を行う場合を例として認証を受理する場合, されない場合の説明を行う. 座標データを取得順にどの小領域にあたるのか調査していき, 9, 9, 10, 10, 10, 11, …, 13 というような書き順に沿った入力順ならば認証を受理する. 一方, 9, 9, 10, 10, 9, 8, 9, …のように前の小領域に戻る場合や, 9, 9, 3, 3, 4, …, 13 のように表示された文字からそれた座標データの場合認証を非受理とする. また, 9, 4, 18, …といったように取得座標に連続性のないものや, 複数の小領域の座標が同時入力されるといったような人間の文字入力として矛盾するものも認証を非受理となる.

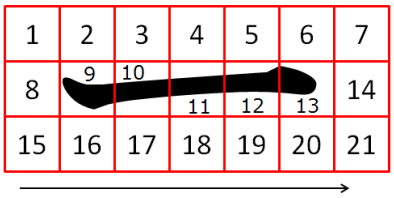

図 1 漢数字「一」

3 ライントレース

提案手法に対する攻撃手法の一例としてライントレースを用いた攻撃が考えられる. そのため提案手法ではライントレースを行えない画像を利用する必要がある. そこで, どのような画像ならばトレースを行えないか調査するために図 2～5 の画像にライントレースシミュレータ ver1.1 を利用してライントレースを行った. 始点を図 6 における小領域番号 1 と定め、書き順通りのトレースが行われた場合をトレース可とし、それ以外の場合をトレース不可とする. 図 2 アルファ, 図 3 アルファ(手書き)では, 同じ文字をトレースした際の結果の違いを調査する. ライントレース対策の一つとして, 図 4 アルファ(間隔)では人間ならば文字を判断できる程度に間隔を施した画像の、図 5 アルファ(格子)ではライントレーサの誤トレースを引き起こさせるために格子付の画像のトレースを行うことで対策の有用性を調査する. トレース結果は表 1 の通りである.

図 2 アルファ

図 3 アルファ(手書き)

図 4 アルファ(間隔)

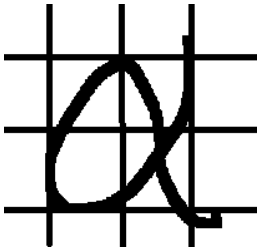

図 5 アルファ(格子)

	図1	図2	図3	図 4
トレース結果	不可	可	不可	格子の位置による

表 1 トレース結果

4. 評価テスト

提案手法を用いて,正しい入力を行った場合に正しい動作をするか(正答率),誤った入力を行った場合に正しく動作するか(誤検知率)を調べるために学生 21 人に対し,「α(図 2)」という文字を用いて次のような実験を行った.また,図 2 に対する正解となるデータは,画像を格子状に区切り,小領域 1 を始点とし 2,3,…,10,…20,…,と隣接する小領域上を通過し,最終的に 30 の小領域の範囲にあたる入力を一筆かつ重複せずに入力されたものである(図 6).また,同じ数を持つ小領域が複数ある場合はどれか 1 つの小領域を通過すればよい.

実験環境

プラットホーム:Android 2.2　メモリ:512MB
プロセッサ:NVIDIA Tegra 250 モバイルプロセッサ　内臓ディスプレイ:タッチパネル付き 7 型 WVGA 液晶　タッチパネル方式:抵抗膜方式

実験 1:始点を指定せず,任意の速度で入力を行い,正答率を調べる.
実験 2:同様に,30 秒程度かけ文字の中心をなぞるという条件の下,実験 1 との正答率の違いを調べる.
実験 3:表示された文字に関わらない間違った入力を行い,間違った入力を誤検知しないか調べる.
実験結果は表 2 の通りである.

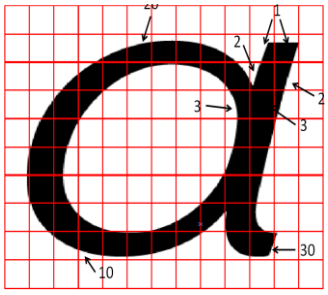

図 6 解答例

	実験1	実験2	実験3
正答数	13	20	0
誤検知数	8	1	21
正答率	61.9	95.24	0
誤検知率	38.1	4.76	100
テスト者数	21	21	21

表 2 実験結果

※実験 1,2 誤答数の内,各 1 は小領域 1(図 6)から書き始めるのではなく別所から書き始めたことによる誤答である.

5. まとめ

3 節ライントレースにおいて行った実験結果から,図 4 のように人間が文字を認識できる範囲内で文字に間隔を施すことでライントレースを利用した攻撃に対する一定の安全性を確保できると考えられる.一方,図 5 のように格子を利用した誤トレースの誘因は,格子と文字の入力方向が直線上に重なったときのみ誘因可能であり必ずしも有用とは言えないことが判明した.

4 節で行った実験の結果から,任意の速度での入力に対して提案手法は対応できていないことが判明した.この問題は,実験 2 の結果から時間を指定することによって丁寧な入力を意識させることで対応できると考えている.また,文字の書き方の間違いを防止するために随所に通過する順を示す番号を表示する等の工夫を施す必要がある.誤検知については実験 3 の結果から,提案手法は誤った入力を誤検知する可能性は非常に小さいと考えられる.

参考文献

[1]L. von Ahn, M. Blum, N. Hopper and J. Langford, CAPTCH:Using Hard Ai Problem for Security, Advances in Cryptology Eurocrypt 2003, LNCS Vol2656, 294-311(2003)
[2]鶴田裕輔,高谷眞弓,山村明弘,タッチパネルを利用した反転チューリングテストと CAPTCHA 平成 24 年度暗号と情報セキュリティシンポジウム 2012 年 1 月