Pulse CAPTCHA

脈拍の真正性を検証するCAPTCHA手法

研究駆動コース
31R 福原陸翔

背景

- ウェアラブル端末の普及による脈拍データ活用の拡大
  - 「Vitality [1]」に代表される健康増進型サービスの広がり
- サービス管理者の目の届かない範囲での利用
- **生成AIによる脈拍データ偽造の新たな脅威**
- 公平性・信頼性を揺るがす生体情報の真正性課題

既存研究・課題

液晶で脈拍を偽装する攻撃の研究 [2]

- 脈拍センサーにモニター上の脈拍を注入できる

センサーで取得した信号を機械学習の入力として用いた「**敵対的信号注入攻撃**」の研究・**防御の研究**は未だない

Pulse CAPTCHAとは

CAPTCHAとは

(Completely Automated Public Turing Test to tell computers and humans apart)

ウェブサイトにアクセスしているのが人間なのかコンピュータなのかを見分けるための仕組み [3]

[3]

[4]

Pulse CAPTCHA : 脈拍版CAPTCHA

通知への生体反応を利用して、脈拍が本物か生成AIによる偽物かを判別する技術

着想

人は通知を受けると脈拍が変化する(瞬間的にドキッとする)
この「反応」は、安静な脈拍のみを学習した生成AIは学習していない特徴
→ 偽脈拍を検出可能！

想定する攻撃

[5]

攻撃者の流れ

1. 生成モデルの学習
   脈拍を生成できるモデルを構築
2. 偽脈拍の生成
   学習したモデルでターゲットの機械学習モデルを騙す脈拍データを作成
3. 攻撃対象のシステムへの入力
   生成した脈拍をセンサーを介して対象のシステムに送信

iPad上に脈拍センサーを置き、生成した偽脈拍を読み込ませている様子

4. 不正な判定
   攻撃者に有利な結果を出力させる

Pulse CAPTCHAの仕組み

なぜ通知を使うのか？

- 毎日自然に届く
  - ➢ **ユーザーに追加の負担なし**
- タイミングがランダムな通知が多い
  - ➢ **予測不可能**
- 通知直後に脈拍間隔(PPI)が短くなることが確認できた
  - ➢ 検証：K-EmoPhoneデータセット[6]
  - ➢ 76名×7日間のスマートウォッチデータ

脈拍生成AIの弱点

生成AIは「統計的に安定した脈拍」を作るのは得意。
しかし、**急な反応（ドキドキ）には対応できない**！

実験設計

検証したいこと：通知への生体反応を見ることで、本人かAIの偽装かを見抜けるか？

データセット

- K-EmoPhone[6] : 76名×7日間のスマートウォッチデータ
- 300拍の脈拍間隔(PPI)を抽出し、それぞれの実験に利用
- 攻撃モデル：Transformer Diffusion Model
  - ➢ Transformerのエンコーダ・デコーダ構造を持つ拡散モデル
  - ➢ 最初の50拍を条件として入力し、残り250拍を生成（条件付き補完）

3つの実験条件

実験A	脈拍全体を見て判別。通知なし時の脈拍 (ベースライン)
実験B	通知後の脈拍変化で判別。通知ありの脈拍 (**提案手法**)
実験C	賢い攻撃AIを想定。通知を反映した高度な偽脈拍

識別器 : Naive Bayes (シンプルで高速な機械学習モデル)
評価指標 : Precision (偽脈拍と判定した中で、正しく識別した割合)

実験結果

実験	条件	Precision	改善率
実験A	ベースライン	76.5%	ー
実験B	提案手法	91.5%	+ 15.0%
実験C	高度な偽脈拍	71.8%	- 4.7%

実験A

それぞれの識別ステップの結果はバラバラで上手に判別することはできていない

実験B (提案手法)

全ての識別ステップで正しく判別出来ている

実験C

それぞれの識別ステップの確率は不安定で、確信を持った判別は出来ていない

赤線が上、**緑線**が下にある時は
正しく判別できている

赤＝偽脈拍

50%より上＝偽脈拍と判定

緑＝人間の脈拍

社会実装

生体情報の活用を研究開発する慶應発スタートアップに技術を継承

- ➢ 自身も引き続き研究を継続

今後の展望

確実に偽脈拍を識別するため、複数の生体信号と予測不可能な検証を組み合わせた多層防御を目指す

[1] 住友生命保険相互会社. "未来を変えていく、健康増進型保険 Vitality". 住友生命. https://vitality.sumitomolife.co.jp/, (参照 2026-02-15).
[2] J. Wang, L. Lu, H. Kong, F. Lin, Z. Ba and K. Ren, "Liquid Crystal Mimics Your Heart: A Physical Spoofing Attack Against PPG-Based Systems," in IEEE Transactions on Information Forensics and Security, vol. 20, pp. 8628-8642, 2025, doi: 10.1109/TIFS.2025.3598472.
[3] Cloudflare. "CAPTCHAとは？ | CAPTCHAの仕組み". Cloudflare. https://www.cloudflare.com/ja-jp/learning/bots/how-captchas-work/, (参照 2026-02-15).
[4] Google. "reCAPTCHA" [画像]. Google Developers. https://developers.google.com/static/recaptcha/images/newCaptchaAnchor.gif?hl=ja, (参照 2026-02-15).
[5] Freepik. "Ai" [アイコン]. Flaticon. https://www.flaticon.com/free-icon/ai_8131880, (参照 2026-02-15).
[6] Kang, S., Choi, W., Park, C.Y. et al. K-EmoPhone: A Mobile and Wearable Dataset with In-Situ Emotion, Stress, and Attention Labels. Sci Data 10, 351 (2023). https://doi.org/10.1038/s41597-023-02248-2