

# Vision Transformer を用いた顔なりすまし攻撃検知手法とその評価

## A Face Spoofing Detection Method Using Vision Transformer and its Evaluation

渡邊 浩太 \*      伊藤 康一 \*      青木 孝文 \*  
Kota Watanabe      Koichi Ito      Takafumi Aoki

キーワード バイオメトリクス, なりすまし検知, 顔認証, ディープラーニング

### あらまし

顔認証は、利便性と受容性の高さから生体認証の中でも特に実用化が進んでいる。一方で、顔画像はインターネットなどから容易に入手することができるため、顔認証システムに対するなりすまし攻撃の危険性がある。なりすまし攻撃とは、悪意のある第三者が認証システムのカメラに登録者の顔画像を提示して認証を不正に通過しようとする攻撃である。なりすまし攻撃には、登録者の顔写真を紙に印刷して提示する Print-Attack や、顔画像をディスプレイに表示して提示する Display-Attack がある。そのため、認証前に、入力された顔画像が本物であるかなりすまし攻撃であるかを判別する必要がある。なりすましを判別するためには、紙面の反射やディスプレイの干渉縞など、顔画像に局所的に存在するノイズを捉える必要がある。

本稿では、画像を小領域に分割して特徴量を抽出するパッチベースの手法である Vision Transformer [1] を用いたなりすまし攻撃検知手法を提案する。ViT は、自然言語の翻訳タスクに用いられている Transformer を画像分類に応用したネットワークモデルである。画像を  $16 \times 16$  のパッチに分割し、パッチ間の対応関係から特徴量表現を学習する。提案手法では、Transformer Encoder で得られた特徴ベクトルを 2 クラス分類器に入力し、本物 (Live) あるいはなりすまし攻撃 (Spoof) に分類する。

本手法の精度を評価するために、公開データセットである SiW [2] を用いる。検知手法の汎化性を評価するために以下に示す SiW の評価プロトコルに従う。プロト

表 1: 実験結果 [%]

Prot.	Method	APCER	BPCER	ACER
1	FAS-BAS	3.58	3.58	3.58
	Proposed	0.02	0.03	<b>0.03</b>
2	FAS-BAS	0.57±0.69	0.57±0.69	0.57±0.69
	Proposed	0.17±0.15	0.17±0.14	<b>0.17±0.15</b>
3	FAS-BAS	8.31±3.81	8.31±3.80	8.31±3.81
	Proposed	7.66±1.29	7.66±1.29	<b>7.66±1.29</b>

コル 1 は、顔の姿勢や表情の変化に対する検知精度を評価する。プロトコル 2 は、Display-Attack の検知精度を評価する。プロトコル 3 は、未知のなりすまし攻撃手法に対する検知精度を評価する。なりすまし攻撃の検知精度の評価には、なりすまし攻撃クラスの中で最大の誤受入率を示す APCER、本物クラスの誤拒否率を示す BPCER、APCER と BPCER の平均値である ACER を用いる。

実験結果を表 1 にまとめる。従来手法である FAS-BAS [2] に対して、提案手法はいずれの評価プロトコルにおいても高精度である。以上より、パッチベースの CNN である ViT を用いることで CNN に基づく従来手法よりも高精度になりすまし攻撃を検知できることを示した。

### 参考文献

- [1] A. Dosovitskiy et al., “An image is worth  $16 \times 16$  words: Transformers for image recognition at scale,” Proc. Int'l Conf. Learning Representations, May 2021.
- [2] Y. Liu et al., “Learning deep models for face anti-spoofing: Binary or auxiliary supervision,” Proc. IEEE Conf. Computer Vision and Pattern Recognition, pp. 389–398, June 2018.

\* 東北大学 大学院情報科学研究科, 〒 980-8579 仙台市青葉区荒巻字 青葉 6-6-05. Graduate School of Information Sciences, Tohoku University, 6-6-05, Aramaki Aza Aoba, Aoba-ku, Sendai-shi, Miyagi 980-8579, Japan.