画像認識AIで個人情報流出対策

～つまり自己防衛だよね～

富山県立高岡高等学校 情報1班　岸本　正保　福岡　藤牧

動機

2019年10月にあるアイドルがファンの男に住所を特定されストーカー行為をされる事件が起きた。加害者はアイドルが載せた画像の瞳の反射から特定したと述べた。
最近もSNSに載せた画像や動画から、個人情報を特定される事例がある。
そこで、SNSの投稿が炎上して個人情報が特定されることをAIを駆使して防げないかと考えた。

目標

SNSに載せようとしている画像に映りこんでいるものを、画像認識AIを使って認識し、警告文などを出し、個人情報が流出する対策をする

前提

個人情報を流失させないためにはタバコやお酒、危険区域の映り込みや歴史的背景といった世間的によくないとされている事柄を、個人が特定できる映り込みと同時に載せないことが必要である。僕たちは、その中のお酒の映り込みについて調べる。

実験内容

1. AIに学習させる画像のデータセットをつくる

この実験で認識させたいお酒の画像をroboflowでタグ付けして Google colab上でYOLOv9に学習させる

2.画像認識AIに画像を認識させる

画像認識AIにその画像にお酒が写っているか認識させ、自分たちで撮った写真でもAIが高い精度で読み込めるようにする

3.お酒だと認識する精度を上げる

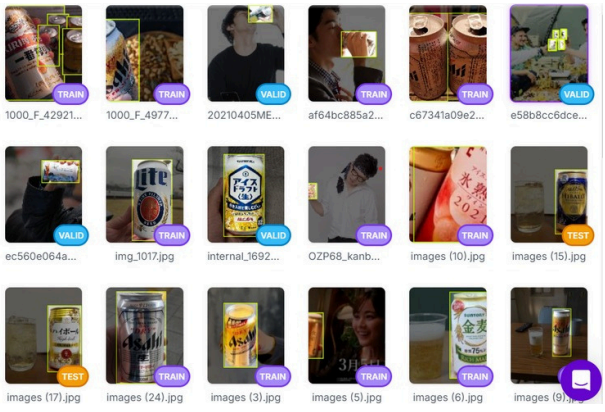
お酒の缶なのかそれ以外の缶なのか、などを判別する方法を探り、お酒だと認識できる精度を上げるにはどのように工夫すればいいのかを考える

結果

実際にお酒の部分は高い精度で認識できているが、顔など関係ない部分がお酒として認識されてしまっている。

展望

この研究は、認識する内容をお酒のみに絞ったが、たばこや暴力、危険な状況なども認識できるようにしたい。
また、小さい画像でも認識できるようにするために、一度画像を分割してそれぞれを認識させるなどの工夫を試してみたい。



使用サイト　Roboflow:Computer vision tools for developers and enterprises.https://roboflow.com/
Google colab.https://colab.google/