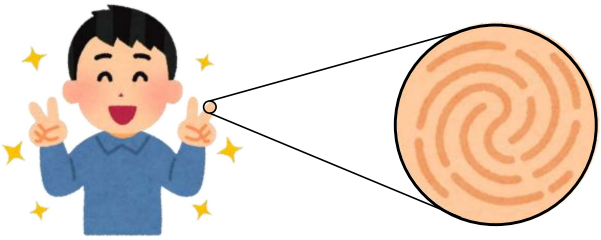
画像からの情報漏洩防止に関する研究

早稲田大学本庄高等学院　3年　工藤 蒔大

研究背景

ここ数年でスマートフォンが急速に普及し、SNSが若者を中心に普及している。SNSの利用者は、文字や画像、動画などの情報を受け取るだけでなく、不特定多数に発信することもできる。



画像センサの技術が発達し、投稿される画像や動画の高画素化が進んだ。スマートフォンのカメラで撮影された写真は綺麗になり、顔や指紋などの個人情報を多く含まれるようになってしまった。さらに建築物や書類などが写り込み、それらを手掛かりに住所などが特定されてしまう可能性もある。

これらの情報は変更することが難しい。そのため、画像からの情報漏洩を防止することはセキュリティの観点から極めて重要である。

提案手法

本研究では画像からの情報漏洩の対策技術として、画像に含まれる個人情報や特定につながる情報を検出し、それらを表示および処理する手法を提案する。画像を入力し、指紋や顔などの情報を含んでいる場合はそれら処理した画像を出力する。また、画像に含まれる建造物などの情報から場所が特定できる場合は、その情報も出力する。

本手法では、テキスト、ランドマーク、顔、指紋の4つの情報を検出および処理する。

図1: テキストの処理の例

テキスト及びランドマークの検出にはGoogle Cloud Vision APIを用いる。テキストが検出された場合、その領域に塗りつぶし処理を行う。ランドマークが検出された場合、その結果を出力する。

図2: 顔の処理の例

顔及び指の検出には、MediaPipeを用いる。顔が検出された場合、絵文字を顔の上に描写して隠す。指が検出された場合、検出された手のランドマークから指紋の範囲をから割り出し、指紋が読み取れない程度に平滑化処理を行う。

評価

それぞれの処理について評価を行う。テキスト、ランドマーク、顔、指紋の4つの情報それぞれが写り込んでいる画像20枚ずつとそれぞれが2つ以上写り込んでいる写真を10枚用意し、提案手法によって開発されたプログラムに入力した。結果は次の通りである。

情報	処理率
テキスト	80%
ランドマーク	55%
顔	60%
指紋	65%
複合	66%

表1: 評価結果

考察

テキストは概ね検出できていたが、手書き文字の検出率が低かった。ランドマークは誤検出が多かった。顔はマスクをしていると、検出率が大きく下がった。指紋は手の向きに関係なく平滑化処理を行うため、爪に平滑化処理されていることがあった。

課題と今後の展望

検出されないことが多々あるため、改善する必要がある。また、ユーザーが気付いたり、処理してほしくなったりすることもあるため、ユーザーが手動で処理及び選択できる機能の実装が望まれる。顔の検出に関しては、着用機会が増えているマスクへの対応が求められる。指の検出に関しては、姿勢推定を行い、指紋の範囲をより正確に割り出す必要がある。最後に提案手法によって開発されたプログラムはCUIのみでしか操作できないため、GUIの実装が強く望まれる。