

招待論文 ScreenConcealer:

オンライン会議における画面共有時のプライバシー懸念調査と保護システム

石田 瑞季*† 池松 香*‡ 五十嵐 悠紀†

概要. オンライン会議で画面共有を行う際に、ユーザは誤って共有したくない情報を公開してしまうことがある。我々の調査からユーザは名前などの個人情報だけでなく、閲覧履歴などユーザの好みや過去の行動がわかる情報を共有したくないということがわかった。また、ユーザは会議前や会議中にプライバシー保護のための対策をしている一方で、誤って共有したくない情報を公開してしまった事例が多く報告された。本研究では画面上のユーザが共有したくないと感じる情報を自動で検出し、視覚的に保護するシステム ScreenConcealer を提案する。我々は画面上の他者と共有したくない情報を検出する深層学習モデルを作成するために、データ収集実験を行った。作成したモデルを使用して、画面共有をしている際にリアルタイムで個人情報やプライベートな情報を保護するシステムを開発した。

1 はじめに

Zoom や Teams, Google Meet などのオンライン会議ツールには、画面共有機能という発表者の画面を会議参加者全員と共有する機能が搭載されている。画面共有機能は、資料を視覚的に共有することで、参加者に対して理解を促せるため会議を円滑に進められる [7]。一方で、共有された画面には意図しない情報を含んでしまうことがある。例えば図 1 のような画面を共有した場合、会議の参加者からは発表者の名前や住所、検索履歴、閲覧履歴に基づくおすすめ商品などの情報がわかってしまう。

こうした画面上の情報を意図せず共有してしまった事例は多く報告されている [8, 5, 3, 4]。しかし共有された画面上のどのような情報を共有したくないと感じているか、またユーザ自身が画面を共有する際にどのような対策を行っているかについて基礎的な調査は行われていない。

我々は画面共有時にユーザがどのような情報を共有したくないと感じているか、また情報を誤って共有しないようにどのような対策をしているのか基礎的な調査を行った [1]。調査結果を元に、図 2 のように画面中の他者と共有したくない情報を自動で検出し、画像処理を用いて情報を視覚的に遮蔽するシステムを開発した [1, 2]。

2 データ収集実験と物体検出モデルの作成

システム実装にあたり、ユーザが隠したい情報を自動で検出するモデルを作成した。まず、データ収集

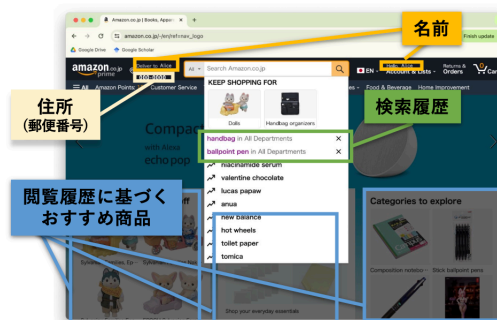


図 1. 画面共有時の画面の例

実験を行い物体検出モデルの学習を行うためのデータセットを作成した。実験には 10 名 (平均年齢 22.3 歳, SD = 1.3, 女性 6 名, 男性 4 名) が参加した。データセット用の画像の収集には、5 秒ごととクリックが行われた際に自動で Chrome の画面を撮影するアプリケーションを作成した。参加者らは自身のラップトップ PC で Google Chrome (以降, Chrome) を開き、配布されたアプリケーションを起動させ、指定された 5 つの Web サイトを閲覧し、それぞれの Web サイト上で指示されたタスクを行った。なお、指定された Web サイトは SimilarWeb の Top Websites Ranking¹ に基づき、日本国内において 2023 年 7 月に多く閲覧された Web サイトからカテゴリの重複がないように選んだ。画像収集後、参加者自身が撮影された画像に対してラベル付け作業を行った。ラベル付け作業には LabelImg² を使用し、ラベルは我々が行った Web サイト上の他者共有したくない情報の調査結果 [1] で一定割合以上のユー

Copyright is held by the author(s). This paper is nonrefereed and non-archival.

* Authors contributed equally.

† お茶の水女子大学

‡ LINE ヤフー株式会社

¹ <https://www.similarweb.com/top-websites/>

² <https://github.com/HumanSignal/labelImg>

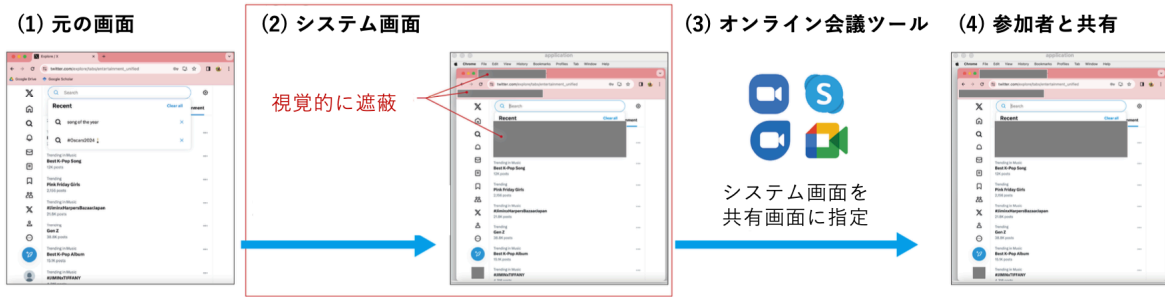


図 2. 提案システムの流れ

表 1. Leave-One-User-Out 分割の検証結果. 各評価項目の値 (Instance, Precision, Recall, mAP50, F1) は平均値.

ラベルセット	ラベル名	Instance	Precision	Recall	mAP50	F1
Sites-and-Items	amazon_address	151	0.725	0.752	0.752	0.734
	amazon_name	238	0.678	0.724	0.621	0.694
	amazon_recommend	167	0.616	0.626	0.584	0.578
	amazon_searchlog	12	0.814	0.795	0.800	0.743
	chrome_bookmark	758	0.625	0.078	0.203	0.095
	chrome_tab	902	0.990	0.993	0.988	0.991
	google_searchlog	28	0.886	0.708	0.781	0.775
	twitter_icon	209	0.747	0.618	0.668	0.661
	twitter_timeline	86	0.804	0.813	0.852	0.749
	twitter_recommend	120	0.928	0.798	0.928	0.810
	twitter_searchlog	17	0.834	0.841	0.865	0.821
	yahoo_advertisement	156	0.778	0.823	0.826	0.787
youtube_searchlog	20	0.708	0.827	0.785	0.742	
youtube_recommend	134	0.873	0.765	0.809	0.780	
Private-or-Not	private	2709	0.847	0.762	0.832	0.799

ザが他者と共有したくないと回答したものの 14 種類を使用した (表 1)。

本実験を通して 9041 枚の画像を収集し, 適切な箇所にラベル付けがされているかどうかを著者のうちの一名が確認した. 本研究では物体検出で広く使用されている YOLO [6] のバージョンの一つである YOLOv5³ のうち, YOLOv5s モデルを使用して学習を行った. 収集したデータセットに対し, 2 種類のラベルセットを定義し学習を行った. Sites-and-Items ラベルセットはラベルを対象の Web サイト名と項目名を繋いで表現したもの (例: amazon_address) であり, Private-or-Not ラベルセットは各ラベルを区別せず全てのラベルを private として扱ったものである. Leave One User Out 交差検証によるモデル性能を表 1 に示す.

3 システム実装

提案システムは前章で作成された物体検出モデルを用いて実装された. システムの概要を図 2 に示す. システムはまず, Web ブラウザの画面を画像として取得する. 取得された画像に対し, ユーザの PC 上で動作する物体検出モデルが, 隠す対象の情報が出現している領域を検出する. そして検出した領域に対し矩形を重ね, 情報を隠した状態の画像を新しい画面として出力する. システムは一連の操作を自動的かつ継続的に行う. 実際の画面共有で使用するには, システム適用画面を元の画面の代わりに指定することで, ユーザはプライバシーを保護しながら画面共有を行うことができる.

参考文献

- [1] M. Ishida, K. Ikematsu, and Y. Igarashi. Designing Privacy-protecting System with Visual Mask-

³ <https://github.com/ultralytics/yolov5>

- ing based on Investigation of Privacy Concerns in Virtual Screen Sharing Environments. *Proceedings of the ACM on Human-Computer Interaction*, (ISS), 2024.
- [2] M. Ishida, K. Ikematsu, and Y. Igarashi. Screen-Concealer: Privacy-protection System with Obfuscations for Screen Sharing. *The 37th Annual ACM Symposium on User Interface Software and Technology (UIST Adjunct '24)*, 2024.
- [3] L. Mannering. The Sometimes Catastrophic, but Mostly Just Embarrassing Consequences of Screen Sharing at Work (accessed 2023-01-07), 2019.
- [4] A. Mertes. 23. Google Search History on Display (accessed 2023-01-30), 2022.
- [5] S. Prange, S. D. Rodriguez, L. Mecke, and F. Alt. “I saw your partner naked”: Exploring Privacy Challenges During Video-based Online Meetings. In *Proceedings of the 21st International Conference on Mobile and Ubiquitous Multimedia, MUM '22*, p. 71–82, New York, NY, USA, 2022. Association for Computing Machinery.
- [6] J. Redmon, S. Divvala, R. Girshick, and A. Farhadi. You Only Look Once: Unified, Real-Time Object Detection. In *2016 IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, pp. 779–788, 2016.
- [7] W. Standaert, S. Muylle, and A. Basu. How shall we meet? Understanding the importance of meeting mode capabilities for different meeting objectives. *Information & Management*, 58(1):103393, 2021.
- [8] Y. Wu, Y. Li, and X. Gui. “I Am Concerned, But...”: Streamers’ Privacy Concerns and Strategies In Live Streaming Information Disclosure. *Proc. ACM Hum.-Comput. Interact.*, 6(CSCW2), nov 2022.