Vol.2022-UBI-74 No.4
2022/6/6

写真のプライバシー保護加工を対話的に行うインタフェース

徐 安然[1,a)]　周 中一[1,b)]　吉川 諒[1,c)]　矢谷 浩司[1,d)]

概要：写真は SNS で共有され，ユビキタス・コンピューティングで活用される重要なメディアとなっている．そのため，写真のプライバシー保護は，多くのユーザーにとって重要であるが，プライバシー保護のための写真編集支援は必ずしも十分でない．本研究ではプライバシー保護のための写真編集を対話的に行う HideTight を提案する．HideTight は，プライバシーを脅かす可能性のある 8 種類のオブジェクトを我々独自の物体認識モデルによりユーザから与えられた写真の中から検出し，プライバシー保護を行う領域を提案する．ユーザは，ボタンを押すことで提案された場所に保護編集を行えるほか，必要に応じて修正を行うことができる．本稿では，HideTight の実装について報告し，および今後の研究の方向性について議論する．

キーワード：写真のプライバシー保護，ユーザブルセキュリティ，対話型システム

1. はじめに

写真はメディアの重要な要素であり，さまざまな場面でさまざまな目的で使用されている．人々は，自己表現のために SNS で写真を頻繁に共有する．また，参加型センシングやアーバンコンピューティングなどのユビキタスコンピューティングの研究においても，写真は重要な情報資源となっている．しかし，このようなメディアで得られる豊富なコンテンツは，プライバシーをおびやかす可能性のある内容を迅速に特定し，それを保護することを困難にすることがしばしばある．また，写真のプライバシー保護加工のためには手動で修正を行う必要があり，多くの場合，大きな負担となっている．また，SNS で写真を共有する主な目的は，カジュアルなコミュニケーションや娯楽であることが多いため，写真の加工のための労力は必ずしも必要ではない．このような状況から，プライバシー保護の重要性に対する人々の理解と，必要な写真編集を行う意欲との間にギャップが生じるという，意識と行動のプライバシーパラドックス [9] が発生している．

先行研究では，人工知能を活用することでこの問題に対処することが試みられている．その多くは，オブジェクトの認識結果に基づいてプライバシー保護加工された写真を自動的に生成することに焦点を当てているが，ユーザがその決定に関与する機会を提供することはなかった [5], [7], [22], [23], [25], [27]．また，他のプロジェクトでは，ユーザが独自のプライバシールールを定義し，異なる受信者に応じて写真にきめ細かいプライバシー保護加工を適用することができた [13], [26]. しかし，これらの方法では，ユーザが手動でポリシーを定義する必要があり，その負担を軽減するためにはさらなる検討が必要である．コンピュータビジョン技術によって写真のプライバシー保護加工技術が進歩している一方で，加工のプロセスにユーザが関わる機会は十分とは言えない．

我々は，写真のプライバシー保護加工の過程にユーザがインタラクティブに関与できることが，ユーザのプライバシーに対する意識を高められると考えている．そこで本研究では，コンピュータビジョン技術を応用して，写真中のプライバシーを脅かす可能性のあるオブジェクトを識別し，対話的に写真加工ができるシステムである HideTight を構築した（図 1）．オブジェクト認識モデルによって，8 つのカテゴリに分類されたオブジェクトを検出し，ユーザに写真のプライバシー保護加工を提案する（図 1 左）．また，加工を促す内容をナッジで表示する（図 1 中）．ボタンを 1 回タップするだけで，写真内の提案された領域に対して自動的にプライバシー保護加工（モザイクやステッカーを使用するなど）を適用する（図 1 右）．加工の結果が気に入らない場合は，ユーザが手動でプライバシー保護加工を追加したり削除することができる．このように，HideTight を利用することで，ユーザは面倒な手作業による写真のプライバシー保護加工から解放される一方で，加工内容を自

[1] 東京大学
[a)] anran@iis-lab.org
[b)] zhongyi@iis-lab.org
[c)] ryo@iis-lab.org
[d)] koji@iis-lab.org

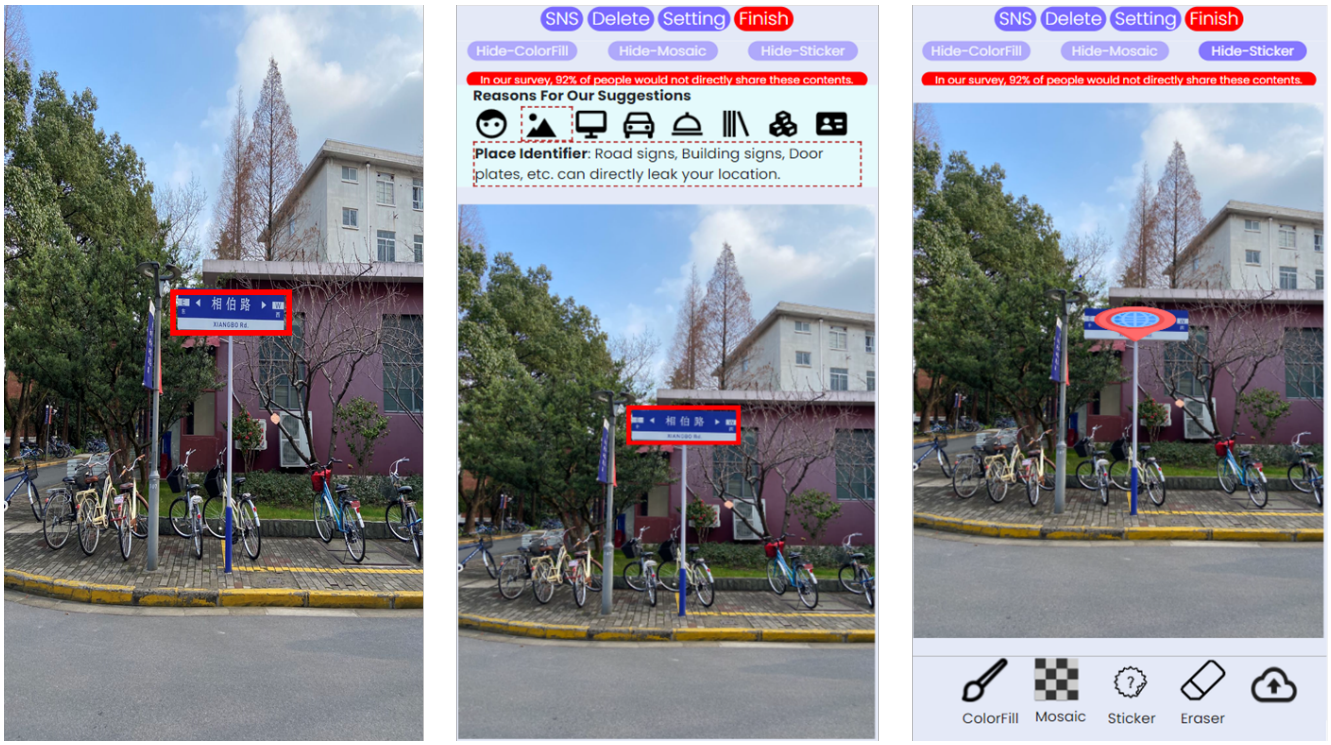

図 1: 左：写真の中で，プライバシーに配慮する必要があると思われる部分に枠囲みを配置する．この例では，道路標識がユーザの位置を特定する可能性があるため，加工を提案している．中：HideTight，指定されたコンテンツを保護する詳細な理由を提示するナッジを表示する．右：ボタンを 1 回タップするだけで，提案された部分に加工を施すことができる．この例では，道路標識の上に地図上のピンのステッカーを追加している．画面の下部にあるツールでは，必要に応じて加工内容を手動で調整することができる．

分の意思で選択することもできる．

本稿では，yolov5 [8] に基づくカスタムオブジェクト認識モデルによる写真プライバシー保護加工支援システム HideTight の設計について述べたのち，今後の研究の方向性について議論する．

2. 関連研究

2.1 プライバシーに配慮したコンテンツの検出

個人情報の含まれたコンテンツを検出するほとんどの手段は，人間の顔 [7]，人間の体 [3]，コンピュータ画面 [10] または重要文書 [23] などのよく定義されたコンテンツの検出に焦点を当てている．別の研究では，ウェアラブルカメラで撮影されたユビキタスビデオ撮影において，周囲の人のプライバシー保護 [2], [4] が実現されている．

プライバシーに配慮したコンテンツの自動検出により，プライバシーを維持した方法で写真を共有することが可能になる．ユーザが写真のプライバシーを管理できるようにするために，ピープルマッチング技術 [26] とルール定義 [13] を利用したシステムも開発されてきた．異なる認証レベルに属するユーザが写真を取得しようとする場合，これらのシステムは所有者の設定に基づいて異なる保護レベルの画像を返す．

2.2 インタラクティブな写真プライバシー保護

既存の研究では，写真撮影システムに人間がどのように関与できるかが検討されている．この方法では，システムは，写真共有の前に通知し，共有の好みを照合することによって，すべての利害関係者（例えば，他人の写真に写る人）を考慮することができる [1], [12]. Shu らは，自動でプライバシー写真加工を行わせるためのジェスチャを提示できるカメラアプリケーションを開発した [18]．例えば，ユーザがカメラの前で拒否のジェスチャをすると，撮影された画像においてそのユーザの顔が自動的にぼかされる．Raval らは，特別なマーカを使用して，特定の領域を自動的に加工する指示を含んだカメラのキューを出す Marklt を開発した [17]．このように，これらのシステムは，写真編集ではなく，写真撮影時の保護に重点を置いている．

本研究では，写真のプライバシー保護に特化した写真編集のための提案型インタフェースを提供することで，このようなインタラクティブなプライバシー保護技術の研究を深めることに貢献する．HideTight は，最先端の Web ベースの機械学習技術を活用し [19]，ユーザのデバイス（スマートフォンなど）で実行可能な，プライバシーに関連しうるコンテンツをリアルタイムに認識することを実現している．

2.3 プライバシー保護加工がユーザ知覚に与える影響

実証研究により，人々が写真を共有する意欲と，彼らが好む写真のプライバシー保護加工のレベルには負の相関があることが確認されている [21]．また，先行研究では，人々はステッカーなどの新しい加工方法に満足する傾向があることが分かった [15]. 写真の縮小またはフェード効果は，古いコンテンツの崩壊を視覚的に伝えることができ，そのような古い写真に関連するプライバシーを保護するためにも役立つ [16]. また，モザイク，エッジ，マスキングと加工を組み合わせることで，ユーザの満足度の低下を緩和している [6]．Li らは，GAN に基づく顔再構成を利用し，人間の見た目の高い知覚品質を維持しながら，自動システムと悪意を持った人間の両方からの不正な顔認識を防止している [14].

本研究の主な貢献は，編集された写真の知覚的な美観を維持するために，異なるプライバシー保護のスタイルや方法を統合することではない．一方でより広い人々の好みや需要に対応するために，将来的には先行研究にあるような視覚効果を統合することができると考えられる．本研究では，写真のプライバシー保護のための手作業を減らすための HideTight の効果に焦点を当て，参加者が写真のプライバシー保護に意識的になるかどうかを調査した．

3. HideTight インタフェース

HideTight は，機械学習に基づいて，ユーザとインタラクティブに写真のプライバシー保護を行うことができる．このシステムは Web ベースのアプリとして実装されており，デスクトップパソコンやタブレットなど，様々なデバイスに対応させることができる．本稿では，スマートフォンが最も一般的な写真撮影デバイスの 1 つとなっていることから，HideTight のモバイルインタフェースを示す．図 2 は，スマートフォン上での HideTight の画面遷移である．

ユーザは，右下のボタンをタップして写真をアップロードする（図 2a）．その後，写真に含まれるプライバシーに配慮した内容を枠囲みで強調し（図 2b），その理由を説明する（図 2c）ことでナッジとして提案する．提案された修正対象のエリアが気に入らない場合，ユーザはこれらの境界ボックスを消去することができる．また，インタフェース上部にある 3 種類のプライバシー保護加工スタイル（“ColorFill”, “Mosaic”, “Sticker”）を選択することで，素早く保護を追加できる（図 2d）．HideTight は，1 回のタップ操作で，提案された領域に対してプライバシー保護加工を自動的に適用する．さらに，プライバシー保護加工を調整するために，好みのステッカーやスタイルを選択したり（図 2e），好みや必要に応じてプライバシー保護加工の程度を変更したり（図 2f）することが可能になる．以下では，HideTight の設計要件を説明する．

3.1 修正の提案

HideTight の重要な目標の一つは，自動的に赤枠で囲まれた部分のコンテンツのプライバシー保護の重要性をユーザに認識させることである．後に説明するモデルの検出結果に従って，HideTight はプライバシー上の懸念があると考えられる箇所の周りに赤い枠囲みをつける．ユーザに心理的負荷ををを与えないために，写真編集スペースの上にナッジという形式で加工の提案を行う．このナッジの文面には，該当の部分を写真加工せずに共有することを避けると考えられる人の割合を含むことで説得力を持たせている．この割合は我々の調査で得られたものである．例えば図 2c では，「我々の調査では，92%の人がこのコンテンツを直接共有しないであろう」と通知している．さらに，ナッジの下に配置されたアイコン（本システムが定義している，プライバシー保護加工が必要である内容の 8 つの分類を表す）をクリックすると，枠囲みの中の物体をプライバシー保護加工すべき理由を一般的な説明として短く提示する．

3.2 プライバシー保護加工の適応

プライバシー保護加工する領域を確認したら，インタフェース上部にある 3 つの “Hide” ボタンをタップするだけで，プライバシー保護加工を追加することができる．ColorFill，Mosaic，Sticker は，それぞれ指定した色の矩形，モザイク，ステッカーを加工する領域に上書きする．Figure 2d に示す例では，ユーザが「Hide - Sticker」 ボタンをタップし，システムが道路標識にステッカーを追加している．なお，今回の実装では，利用できるステッカーの種類は猫などの一部のものに限定されている．ステッカーの種類を拡張したり，ぼかし加工など別の方法を含めることは本研究の範囲外である．我々の貢献は，より目立たない，またはより視覚的に訴える加工フィルタを検討することではなく，ユーザが容易に，必要な加工処理を行えるシステムを提案することである．

3.3 物体検出のパーソナライズ

個人差に対応するため，これらのオブジェクトをどの程度プライバシー保護加工するかをスライダーで制御することができる．現在のプロトタイプでは，認識のための最小信頼スコアを更新することで，対応するオブジェクト分類の認識感度を制御することができる（図 2f）．最も強い感度では最小信頼スコアが 20 であり，最も弱い感度では最小信頼スコアが 40 となる．例えば感度を上げると，より多くの候補が表示されるが，そのうちのいくつかは誤検出となる可能性がある．この設定は，ユーザが写真を共有する際に，特定の種類のオブジェクトに強く注意を払う必要がある場合に役立つことが期待される．さらに，ユーザは，ボトムメニューの “ColorFill”, “Mosaic”, “Sticker” のいずれかをクリックし，隠したい領域をドラッグして，プライ

図 2: HideTight の詳細な説明．(a) HideTight の初期状態． (b) ユーザが写真を読み込むと，システムはオブジェクト認識を行い，プライバシーを脅かす可能性のあるオブジェクトを枠囲みでユーザに知らせる． (c) HideTight は真上のナッジで修正を促す（例：“In our survey, 92% of people would not directly share these contents.” といった説明を提示する）．ユーザは，これらのコンテンツがプライバシー保護加工されるべき理由の詳細を読むことができる．(d) 3 つのボタン（“Hide-ColorFill”，“Hide-Mosaic”，“Hide-Sticker”）のいずれかをタップすると，提案された領域の上にプライバシー保護加工を追加することができる．(e) 必要に応じてプライバシー保護加工を手動で調整することができる．(f) ユーザは、各アイコンをタップしてスライダーを調整することで、8 つのオブジェクト分類ごとに検出感度を設定することができる．

バシー保護加工を手動で追加，変更することも可能である．

4. プライバシーコンテンツ検出モデル

4.1 プライバシーに配慮した共通のカテゴリの収集

HideTight の機能を十分に発揮させるためには，プライバシーに配慮したコンテンツに対する認識モデルを開発する必要がある．写真に含まれる情報で，プライバシーを脅かす可能性があるものについては，既に人の顔や，コンピュータに映り込むデータなどが指摘されている．先行研究では，そのようなコンテンツを検出するためのモデルを開発している [22], [23]．しかし，これらのモデルの主な対象は人体や顔に限定されており，本研究で使用するには十分ではない．そこで，プライバシー保護加工が必要と思われる物体を検出するモデルを独自に開発した．開発にあたってオンライン調査とデータ収集を行い，SNS 上の写真によく見られる，プライバシーを脅かしかねないコンテンツの主要なカテゴリを導出し，認識モデルを開発した．

モデルの開発のために，18 名（女性 11 名，男性 7 名）の参加者を募集した．参加者は，同意書に署名した後，この研究のために自分で撮影した少なくとも 10 種類の写真を提供するよう求められた．そして，これらの写真がインターネット上で誰でも見ることができる場合，プライバシーを脅かすと思われる場所をすべて，プライバシー保護のために処理するよう指示した．プライバシー保護加工のために，簡単なオンライン写真編集インタフェースを参加者に提供した．次に，参加者にプライバシー保護加工の理由についての説明文を提供してもらった．編集したすべての写真と説明はオンラインツールにより収集した．調査終了時に参加者に対して謝金 2080 円を提供した．このデータ収集手順は，所属機関の研究倫理委員会によって承認されている．

4.2 データセットと認識モデルの作成

今回の調査で判明したプライバシーに配慮したコンテンツのうち，上位 8 つのカテゴリを選んだ．その結果を表 1 に示す．そして，OpenImage データセット [11] を利用して，プライバシーを侵害しかねない 8 つの被写体のカテゴリを構築し，モデル学習を行った．COCO で事前学習した yolov5m に対して，このデータセットを用いて 300 エポックの学習を行い，微調整を行った．そして，このモデルを TensorFlow.js [19] を用いて Web ベースの環境に実装した．

Table 2 は，各カテゴリにおける我々のモデルの平均再現率（Mean Average Precision，mAP），精度（Precision），再現率（Recall）をまとめたものである．OpenImages データセットにおける他の最先端モデルと比較して，我々のモデルは同等の性能を達成し [20]，我々のターゲットシナリオの要件を満たすことができる．

また，Google Pixel5 (オペレーションシステム: Android 11, プロセッサ: Snapdragon 765g, RAM: 8GB, ブラウザ: Chrome) と iPhone 13 Pro (オペレーションシステム: IOS 15, プロセッサ: A15 Bionic, ブラウザ: Safari) の両方で Web ベースの実装 (TensorFlow.js [19]) を 100 回実行し，レイテンシを測定している．1 枚の写真（入力解像度：640 画素 × 640 画素）を推論する際の平均待ち時間は，Google Pixel 5 で 86.02 ms（SD=3.66 ms），iPhone 13 Pro で 20.19 ms（SD=1.61 ms）であった．この結果は，我々の認識モデルがスマートフォンでもリアルタイム処理できることを示唆している．

5. 今後の課題

本研究には，今後改善すべきいくつかの課題がある．我々は，写真においてプライバシーを脅かす可能性のあるコンテンツのカテゴリを 8 つ設定したが，これらは決定的なものではなく，検証のためにさらなる研究を実行する必要がある．また，現在のプロトタイプには，ユーザとのやりとりを通じたパーソナライゼーションは含まれていない．Vishwamitra ら [24] はごく最近，固定されたカテゴリにおけるプライバシーの配慮が必要な内容について，ユーザの判断基準を自動的に学習するための検出機能を導入した．我々は，このような技術によって，事前にデータがないような，新しい形態のプライバシーコンテンツについても素早く学習することができるのではないかと考えている．さらに，将来のシステムでは，プライバシー保護のための加工の方法について，ユーザがどのような方法やステッカーを使用する傾向があるか調べることで，ユーザの好みを学習できる可能性が期待される．これらの機能は，HideTight のユーザ満足度の向上につながると考えられる．

6. おわりに

写真の修正は，プライバシー保護のための重要な手法の一つである．しかし，写真の難読化は，ユーザが手作業で写真を編集する必要があり，面倒な作業である．さらに，プライバシーに関する意識や知識が乏しいため，処理を行うことができないユーザも少なくない．本研究では，写真のプライバシー保護に特化した対話的な写真編集インタフェース HideTight を提案した．HideTight は，写真に含まれる 8 種類のプライバシーに配慮したコンテンツを検出し，プライバシー保護加工の提案を行う．今後の研究では，プライバシー保護加工手法の改良を検討するとともに，より広範なユーザスタディを通じて HideTight の効果をさらに調査する予定である．

謝辞

本研究の一部は，セコム科学技術振興財団の挑戦的研究助成によって行われました．また，本論文に対してアドバ

表 1: プライバシーを脅かす可能性のあるものを 8 つにの分類名.

HideTight の分類名	**OpenImages に含まれるクラス**
Human face	Human face
Place identifier	Office Building; Traffic sign
Screen	Computer monitor; Tablet computer; Laptop; Television
Identity & Ticket	Identity; Ticket
Food	Food; Fruit; Drink
Book	Book
Items on table	Kitchen & dining room tables; Table
Vehicle plate	Vehicle registration plate

表 2: yolov5m モデルを我々のデータセットに適用した結果（検証セット）.

分類名	Human face	Place identifier	Screen	Identity & Ticket	Food	Book	Items on table	Vehicle plate
$\boldsymbol{mAP_{.5}}$	0.76	0.50	0.67	0.78	0.36	0.31	0.51	0.80
$\boldsymbol{mAP_{.95}}$	0.45	0.37	0.50	0.49	0.22	0.17	0.29	0.47
Precision	0.91	0.45	0.55	0.71	0.53	0.33	0.65	0.84
Recall	0.47	0.73	0.72	0.88	0.30	0.52	0.43	0.80

イスを下さった研究室のメンバーに感謝申し上げます.

参考文献

[1] Aditya, P., Sen, R., Druschel, P., Joon Oh, S., Benenson, R., Fritz, M., Schiele, B., Bhattacharjee, B. and Wu, T. T.: I-pic: A platform for privacy-compliant image capture, *Proceedings of the 14th annual international conference on mobile systems, applications, and services (MobiSys '16)*, pp. 235–248 (2016).

[2] Alharbi, R., Tolba, M., Petito, L. C., Hester, J. and Alshurafa, N.: To mask or not to mask? balancing privacy with visual confirmation utility in activity-oriented wearable cameras, *Proceedings of the ACM on interactive, mobile, wearable and ubiquitous technologies (IMWUT '19)*, Vol. 3, No. 3, pp. 1–29 (2019).

[3] Cheung, S.-c., Venkatesh, M. V., Paruchuri, J. K., Zhao, J. and Nguyen, T.: Protecting and managing privacy information in video surveillance systems, *Protecting Privacy in Video Surveillance*, Springer, pp. 11–33 (2009).

[4] Dimiccoli, M., Marín, J. and Thomaz, E.: Mitigating bystander privacy concerns in egocentric activity recognition with deep learning and intentional image degradation, *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies (IMWUT '18)*, Vol. 1, No. 4, pp. 1–18 (2018).

[5] Hasan, R., Crandall, D., Fritz, M. and Kapadia, A.: Automatically detecting bystanders in photos to reduce privacy risks, *2020 IEEE Symposium on Security and Privacy (SP '20)*, IEEE, pp. 318–335 (2020).

[6] Hasan, R., Li, Y., Hassan, E., Caine, K., Crandall, D. J., Hoyle, R. and Kapadia, A.: Can privacy be satisfying? On improving viewer satisfaction for privacy-enhanced photos using aesthetic transforms, *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems (CHI '19)*, pp. 1–13 (2019).

[7] He, J., Liu, B., Kong, D., Bao, X., Wang, N., Jin, H. and Kesidis, G.: Puppies: Transformation-supported personalized privacy preserving partial image sharing, *46th annual IEEE/IFIP international conference on dependable systems and networks (DSN '16)*, IEEE, pp. 359–370 (2016).

[8] Jocher, G., Stoken, A., Borovec, J., NanoCode012, ChristopherSTAN, Changyu, L., Laughing, tkianai, Hogan, A., lorenzomammana, yxNONG, AlexWang1900, Diaconu, L., Marc, wanghaoyang0106, ml5ah, Doug, Ingham, F., Frederik, Guilhen, Hatovix, Poznanski, J., Fang, J., Yu, L., changyu98, Wang, M., Gupta, N., Akhtar, O., PetrDvoracek and Rai, P.: yolov5: v3.1 (2020).

[9] Kokolakis, S.: Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon, *Computers & security*, Vol. 64, pp. 122–134 (2017).

[10] Korayem, M., Templeman, R., Chen, D., Crandall, D. and Kapadia, A.: Enhancing lifelogging privacy by detecting screens, *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems (CHI '16)*, pp. 4309–4314 (2016).

[11] Kuznetsova, A., Rom, H., Alldrin, N., Uijlings, J., Krasin, I., Pont-Tuset, J., Kamali, S., Popov, S., Malloci, M., Kolesnikov, A. et al.: The open images dataset v4, *International Journal of Computer Vision*, Vol. 128, No. 7, pp. 1956–1981 (2020).

[12] Li, A., Li, Q. and Gao, W.: Privacycamera:

Cooperative privacy-aware photographing with mobile phones, *13th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON '16)*, IEEE, pp. 1–9 (2016).

[13] Li, F., Sun, Z., Li, A., Niu, B., Li, H. and Cao, G.: Hideme: Privacy-preserving photo sharing on social networks, *IEEE Conference on Computer Communications (IEEE INFOCOM '19)*, IEEE, pp. 154–162 (2019).

[14] Li, T. and Choi, M. S.: DeepBlur: A simple and effective method for natural image obfuscation, *arXiv preprint arXiv:2104.02655*, Vol. 1 (2021).

[15] Li, Y., Vishwamitra, N., Knijnenburg, B. P., Hu, H. and Caine, K.: Effectiveness and users' experience of obfuscation as a privacy-enhancing technology for sharing photos, *Proceedings of the ACM on Human-Computer Interaction (CHI '17)*, Vol. 1, No. CSCW, pp. 1–24 (2017).

[16] Mohamed, R. E. and Chiasson, S.: Online privacy and aging of digital artifacts, *Fourteenth Symposium on Usable Privacy and Security (SOUPS '18)*, pp. 177–195 (2018).

[17] Raval, N., Srivastava, A., Lebeck, K., Cox, L. and Machanavajjhala, A.: Markit: Privacy markers for protecting visual secrets, *Proceedings of the 2014 ACM international joint conference on pervasive and ubiquitous computing: Adjunct publication (UbiComp '14 Adjunct)*, pp. 1289–1295 (2014).

[18] Shu, J., Zheng, R. and Hui, P.: Cardea: Context-aware visual privacy protection for photo taking and sharing, *Proceedings of the 9th ACM Multimedia Systems Conference*, pp. 304–315 (2018).

[19] Smilkov, D., Thorat, N., Assogba, Y., Yuan, A., Kreeger, N., Yu, P., Zhang, K., Cai, S., Nielsen, E., Soergel, D., Bileschi, S., Terry, M., Nicholson, C., Gupta, S. N., Sirajuddin, S., Sculley, D., Monga, R., Corrado, G., Viégas, F. B. and Wattenberg, M.: TensorFlow.js: Machine Learning for the Web and Beyond, *CoRR*, Vol. abs/1901.05350 (online), available from ⟨http://arxiv.org/abs/1901.05350⟩ (2019).

[20] Song, G., Liu, Y. and Wang, X.: Revisiting the sibling head in object detector, *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR '20)*, pp. 11563–11572 (2020).

[21] Tanaka, Y., Kodate, A., Ichifuji, Y. and Sonehara, N.: Relationship between willingness to share photos and preferred level of photo blurring for privacy protection, *Proceedings of the ASE BigData & SocialInformatics (ASE BDSI '15)*, pp. 1–5 (2015).

[22] Tonge, A. and Caragea, C.: Image privacy prediction using deep neural networks, *ACM Transactions on the Web (TWEB '20)*, Vol. 14, No. 2, pp. 1–32 (2020).

[23] Tran, L., Kong, D., Jin, H. and Liu, J.: Privacy-cnh: A framework to detect photo privacy with convolutional neural network using hierarchical features, *Proceedings of the AAAI Conference on Artificial Intelligence*, Vol. 30, No. 1 (2016).

[24] Vishwamitra, N., Li, Y., Hu, H., Caine, K., Cheng, L., Zhao, Z. and Ahn, G.-J.: Towards Automated Content-based Photo Privacy Control in User-Centered Social Networks, *Proceedings of the Twelveth ACM Conference on Data and Application Security and Privacy (CODASPY '22)*, pp. 65–76 (2022).

[25] Yu, J., Kuang, Z., Zhang, B., Zhang, W., Lin, D. and Fan, J.: Leveraging content sensitiveness and user trustworthiness to recommend fine-grained privacy settings for social image sharing, *IEEE transactions on information forensics and security (IEEE TIFS '18)*, Vol. 13, No. 5, pp. 1317–1332 (2018).

[26] Zhang, L., Liu, K., Li, X.-Y., Liu, C., Ding, X. and Liu, Y.: Privacy-friendly photo capturing and sharing system, *Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing (UbiComp '16)*, pp. 524–534 (2016).

[27] Zhong, H., Squicciarini, A. C., Miller, D. J. and Caragea, C.: A Group-Based Personalized Model for Image Privacy Classification and Labeling., *International Joint Conference on Artificial Intelligence (IJCAI '17)*, Vol. 17, pp. 3952–3958 (2017).