Privacy-Aware Tag Recommendation for Image Sharing

Kansas State University College of Engineering Department of Computer Science

Ashwini Tonge[1], Cornelia Caragea[1] and Anna Squicciarini[2]

[1]Kansas State University, [2]Pennsylvania State University

Image Privacy Prediction?

- Rapid increase in social media can cause threat to user's privacy
- Many users are quick to share private images without realizing the consequences of an unwanted disclosure of these images.
- Users rarely change default privacy settings, which could jeopardize their privacy [Zerr et al., 2012].
- Current social networking sites do not assist users in making privacy decisions for images that they share online.
- Image Privacy Prediction predicts privacy setting for images and avoid a possible loss of users' privacy.

Prior Works

- Recently, [Squicciarini et al., 2014] and [Zerr et al., 2012] found that user tags are informative for classifying images as *private* or *public*.
- [Tonge and Caragea, 2016, Tonge and Caragea, 2018, Tonge et al., 2018] automatically obtained image tags from the visual content using convolutional neural networks and also showed their performance for privacy prediction.

Motivation

(a) *Private*, Elegant Corporate, Style Fashion, Girl, Woman Skirt, Top, Bag, Pretty

(b) *Public*, Parisi, Sabrina News, Celebrity Famous, Girl Woman, Hollywood

Figure: Anecdotal evidence for visually similar images with privacy-aware user tags.

Our Contributions

- Present a privacy-aware approach to image tagging.
  - Improve the quality of user tags.
  - Preserving the images original privacy sharing patterns.
- Recommends potential tags for a target image by mining privacy-aware tags from the most similar images.
- Although the user-input tags comprise noise or even some images do not have any tags at all, our approach is able to recommend accurate tags.
- Results show that the predicted tags can exhibit relevant cues for specific privacy settings.

Datasets

- We evaluated our approach on Flickr images sampled from the PiCalert dataset [Zerr et al., 2012].
- PiCalert consists of Flickr images on various subjects, which are manually labeled as *public* or *private* by external viewers.
- The public and private images are in the ratio of 3:1.
- *Private*: Private image discloses sensitive information about a user. E.g., images with self-portraits, family, friends, someone's home, etc.
- *Public*: Remaining images are labeled as public.

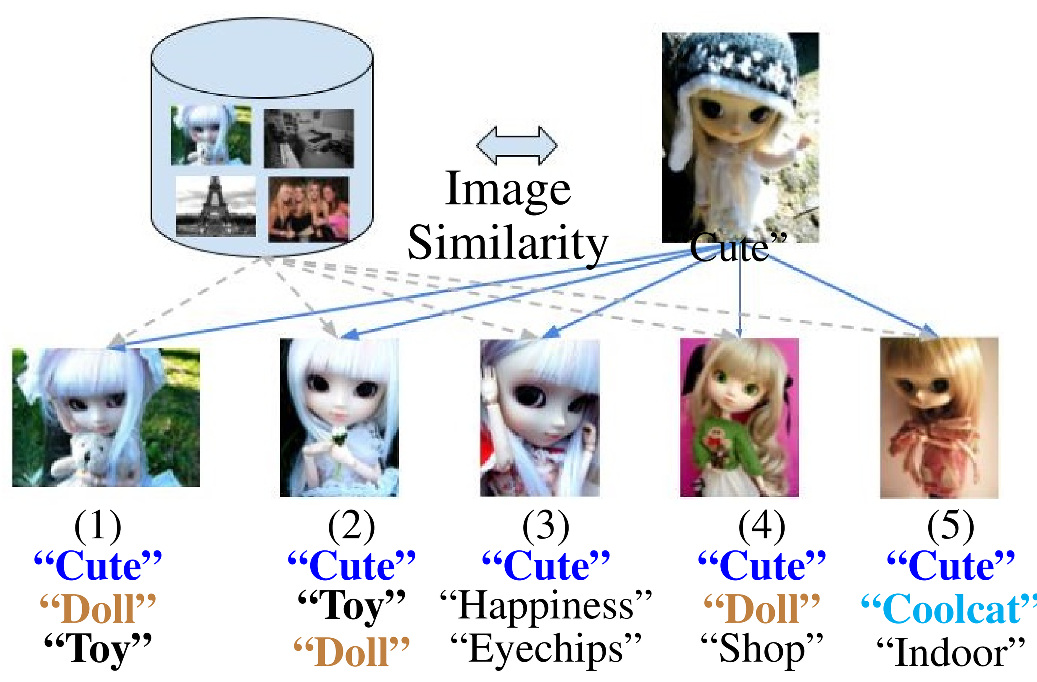
Dataset	#Total Images	#Avg. Tags	#min. Tags	#max. Tags	#Pr.	#Pu.
$(\mathfrak{D})$	8000	9.73	1	71	2000	6000
DS_1	3689	16.60	11	78	922	2767
DS_2	500	20.70	11	69	125	375

Table: Datasets summary.

Privacy-Aware Image Tag Recommendation

- Our approach draws ideas from collaborative filtering (CF).
- The analogy with conventional CF methods is that images correspond to users and tags correspond to items.
- Base our models on the assumption that privacy-aware similar images possess similar tags Online Image Privacy.
- Images can be represented using two different views or feature types: (1) image visual content and (2) image tags.

Algorithm Illustration - I



Recommended Tags - "Doll," "Toy," "Coolcat"

Figure: Illustration of the privacy-aware tag recommendation algorithm using an example.

Algorithm Illustration - II

Candidate Tags	Count	$P(t\|pr = private)$	$P(t\|pr = public)$	w_t $s_j = 1$
Doll	**3**	**0.1**	**0.9**	**3 × 0.9 = 2.7**
Toy	**2**	**0.15**	**0.85**	**2 × 0.85 = 1.7**
Cute	**5**	**0.7**	**0.3**	**5 × 0.3 = 1.5**
Coolcat	**1**	**0.0**	**1.0**	**1 × 1.0 = 1.0**
Shop	1	0.0	1.0	1 × 1.0 = 1.0
Eyechips	1	0.3	0.7	1 × 0.7 = 0.7
Indoor	1	0.6	0.4	1 × 0.4 = 0.4
Happiness	1	0.6	0.4	1 × 0.4 = 0.4

Table: Privacy-aware weighted sum of tag occurrences ($K = 5$, $r = 3$).

Experiments and Results

Evaluation by Privacy Prediction

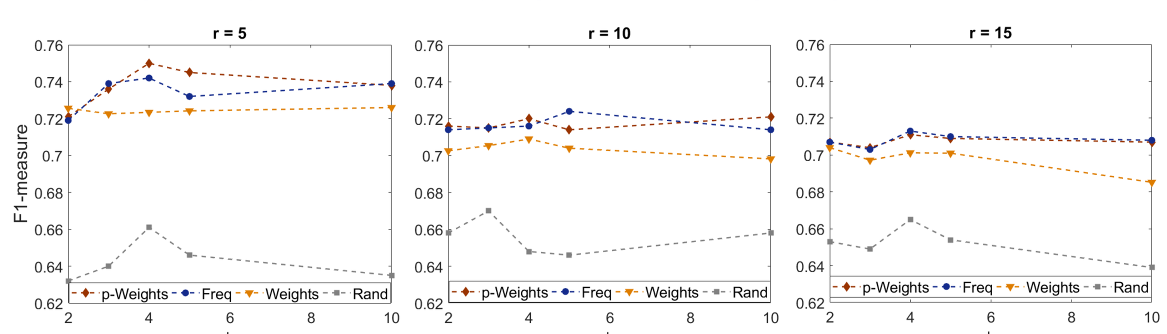


Figure: F1-measure obtained for various parameter values of scoring methods, k and r.

Features	Acc. %	F1	Precision	Recall
vt	74.83	0.743	0.739	0.748
		$k = 4$		
vt & $rt(5)$	**77.84**	**0.766**	**0.755**	**0.778**
vt & $rt(10)$	77.47	0.763	0.752	0.776
vt & $rt(15)$	77.31	0.757	0.744	0.771
vt & $rt(20)$	76.83	0.754	0.741	0.769
		$k = 5$		
vt & $rt(5)$	**77.96**	**0.769**	**0.758**	**0.781**
vt & $rt(10)$	77.80	0.766	0.755	0.778
vt & $rt(15)$	77.60	0.764	0.752	0.776
vt & $rt(20)$	77.27	0.760	0.747	0.773
		$k = 10$		
vt & $rt(5)$	**78.20**	**0.772**	**0.762**	**0.783**
vt & $rt(10)$	77.80	0.765	0.754	0.777
vt & $rt(15)$	77.92	0.767	0.758	0.778
vt & $rt(20)$	77.43	0.758	0.745	0.771

Table: Performance for privacy prediction after adding recommended tags.

Experiments and Results

Cold Start Problem

Features	Acc.%	F1	Precision	Recall
$pool_5(rt)$	**75.74**	0.743	0.729	**0.757**
DT(rt)	74.19	0.731	0.725	0.742
vt	74.83	0.743	0.739	0.748
DT	68.54	0.645	0.619	0.685

Table: Visual content-based similarity ($k = 10$).

Proposed Approach vs. Prior Works

Features	Acc.%	F1	Precision	Recall
	#1 Original User Tags (Visible Tags)			
vt	74.83	0.743	0.739	0.748
	#2 FastTag (Prior work)			
vt & rt	74.55	0.741	0.738	0.745
	#3 Visual Content Similarity ($T = \phi$)			
vt & $rt(5)$	75.23	0.741	0.730	0.752
vt & $rt(10)$	75.63	0.742	0.727	0.757
vt & $rt(15)$	***76.71***	***0.752***	***0.737***	***0.768***
vt & $rt(20)$	76.27	0.747	0.732	0.763
	#4 Tag Similarity ($T \neq \phi$)			
vt & $rt(5)$	**78.20**	**0.772**	**0.762**	**0.783**

Table: Privacy-aware Tag recommendation vs. FastTag.

Quality Assessment of Recommended Tags

#Tags (r)	Gold-standard P@r	User-Study P@r
1	0.177	**0.855**
2	**0.181**	0.761
3	**0.181**	0.755
4	0.172	0.703
5	0.174	0.691
10	0.155	0.633

Table: Gold-standard and User evaluation of recommended tags.

Visible	Hidden	Recommended Tags	
Beauty	Geisha	**People**	*Culture*
Light	Kyoto	**Japan**	*Street*
Travel	Japan	**Asia**	*Walking*
Couple	Kimono	**Geisha**	
Woman	Traditional	**Kimono**	
Vintage	Asia	**Kyoto**	
	People	**Traditional**	

Figure: Image with recommended tags, r=10.

Conclusions

- Improve the original set of user tags and preserve images privacy.
- Draw ideas from collaborative filtering (CF).
- Although the user-input tags are prone to noise, we were able to integrate them in our approach and recommend accurate tags.
- Simulated the recommendation strategy for newly-posted images, which had no tags attached.
  - Simulated the recommendation strategy for newly-posted images, which had no tags attached.
- Achieved better performance for privacy prediction with recommended tags than user tags.
  - Indicate that the suggested tags comply to the images privacy.
- Conducted a user evaluation of recommended tags to inspect the quality of the recommended tags.
  - Results show that the proposed approach is able to recommend highly relevant tags.
- Future directions
  - Multiple sharing needs of the user.
  - Computing images similarity by combining both tags and visual content.

References

Squicciarini, A. C., Caragea, C., and Balakavi, R. (2014). Analyzing images' privacy for the modern web. HT '14, pages 136–147, New York, NY, USA. ACM.

Tonge, A. and Caragea, C. (2018). On the use of "deep" features for online image sharing. In *Companion Proceedings of The Web Conf.*, pages 1317–1321.

Tonge, A., Caragea, C., and Squicciarini, A. (2018). Uncovering scene context for predicting privacy of online shared images. In *AAAI '18*.

Tonge, A. K. and Caragea, C. (2016). Image privacy prediction using deep features. In *AAAI*.

Zerr, S., Siersdorfer, S., Hare, J., and Demidova, E. (2012). Privacy-aware image classification and search. In *ACM SIGIR*, NY, USA. ACM.

Acknowledgements: This research is supported by a grant from NSF to Cornelia Caragea and Anna Squicciarini. https://ashwinitonge.github.io/