# Privacy Attributes-aware Message Passing Neural Network for Visual Privacy Attributes Classification

Hanbin Hong[1], Wentao Bao[1], Yuan Hong[2] and Yu Kong[1]

[1]Rochester Institute of Technology

[2]Illinois Institute of Technology

**Task**: Visual Privacy Attributes Classification

**Labels:**
Partial Face
Race
Skin Color
Approximate Age
Approximate Weight
Occupation
Gender
Eye Color
Social Circle
Professional Circle
Hair Color
Complete Face

**Challenges**:

| Tasks | Input | Output (10 classes) | Output Space |
|---|---|---|---|
| Single-label Classification | Image | $[0, 0, 0, 0, 0, \mathbf{1}, 0, 0, 0, 0]$ | $\mathbf{10}$ |
| Multi-label Classification | Image | $[\mathbf{1}, 0, \mathbf{1}, 0, 0, \mathbf{1}, 0, 0, \mathbf{1}, \mathbf{1}]$ | $\mathbf{2^{10}}$ |

**Solutions**: Reduce the output space

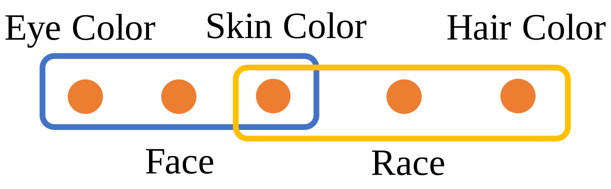
$$[\mathbf{1}, 0, \mathbf{1}, 0, 0, \mathbf{1}, 0, 0, \mathbf{1}, \mathbf{1}] \longrightarrow 2^{10}$$

$$[\mathbf{1}, 0, \mathbf{1}, 0, 0, \mathbf{1}, 0, 0, \mathbf{1}, \mathbf{1}] \longrightarrow 2^{6}$$

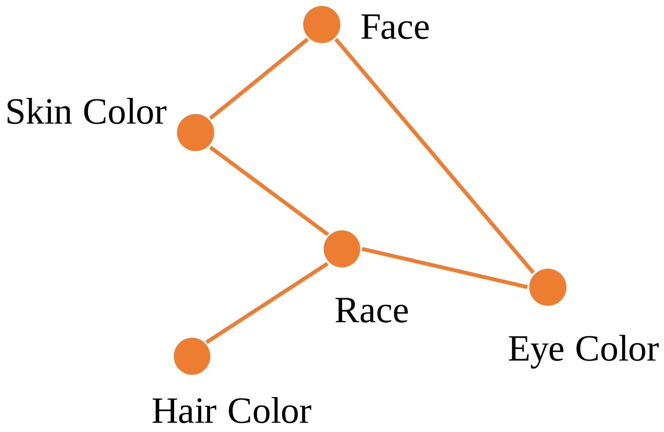
**Related Works**:

- Combining a set of labels [5]
- Class hierarchy [6]
- Embedding high dimension label vector to low dimension label vector [7]

**Dependencies between privacy attributes**




Group Dependency




Structural Dependency

**How to capture the structural dependency**?

**Message Passing Neural Network [8] (MPNN):**

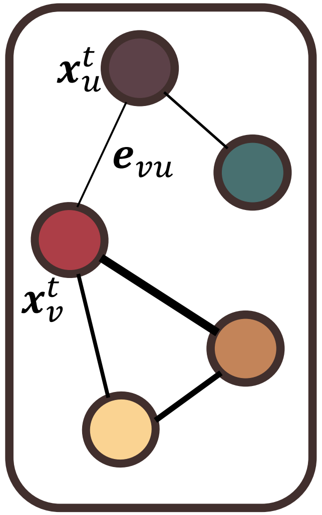
**Main Idea**: Privacy Attributes → Nodes on Graph

MPNN: Use adjacent node features to update node features.

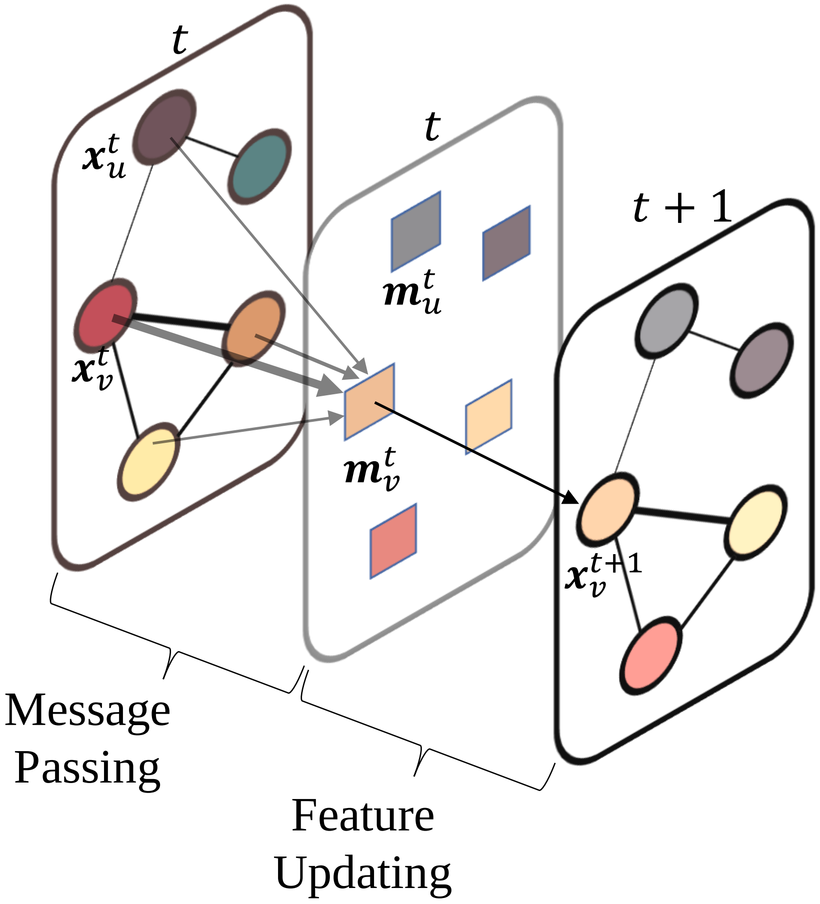
In layer $t$:

- Message Passing $\boldsymbol{m}_v^t = \sum_{u \in N(v)} M_t(\boldsymbol{x}_v^t, \boldsymbol{x}_u^t, \boldsymbol{e}_{vu})$
- Feature Updating $\boldsymbol{x}_v^{t+1} = U_t(\boldsymbol{x}_v^t, \boldsymbol{m}_v^t)$

$\boldsymbol{x}_v^t$: Feature of node $v$ in layer t
$\boldsymbol{e}_{\mathrm{vu}}$: Feature between node $v$ and $u$
$\boldsymbol{m}_v^t$: Hidden State of node $v$ in layer t

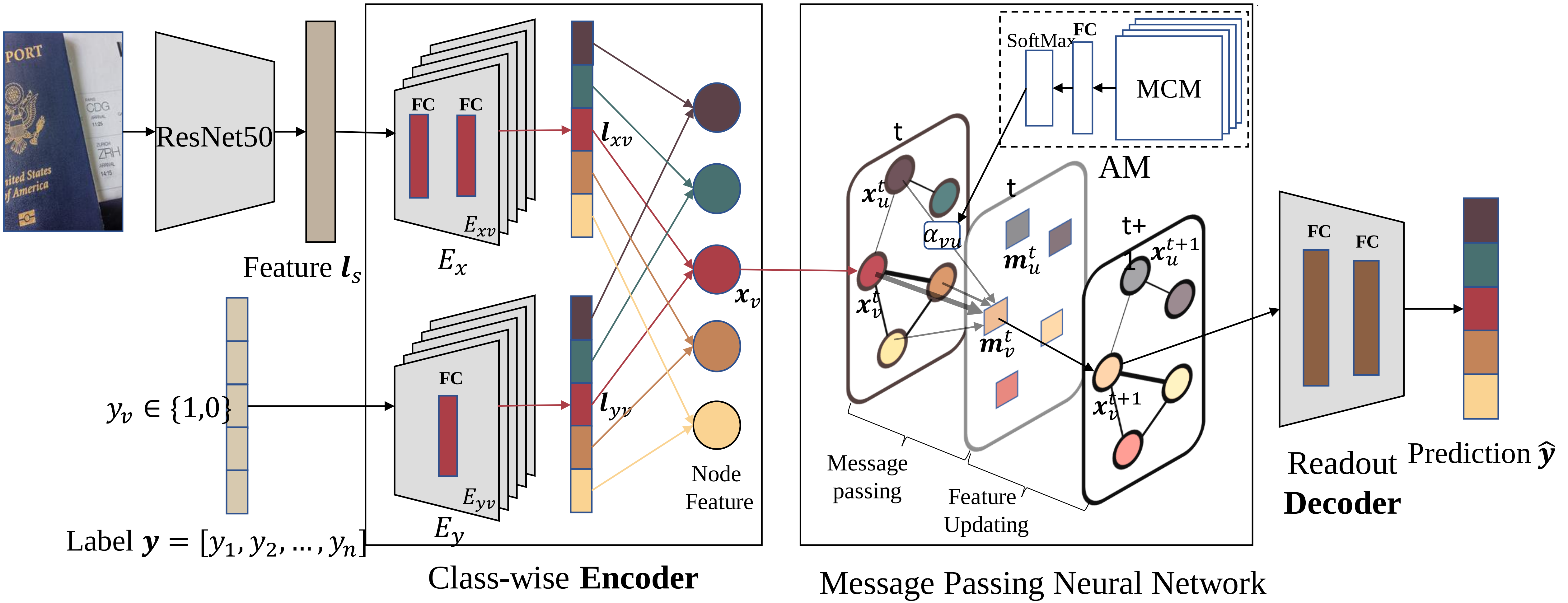



Graph




MPNN Mechanism

## Privacy Attributes-aware Message Passing Neural Network (PA-MPNN):



## Experiments:

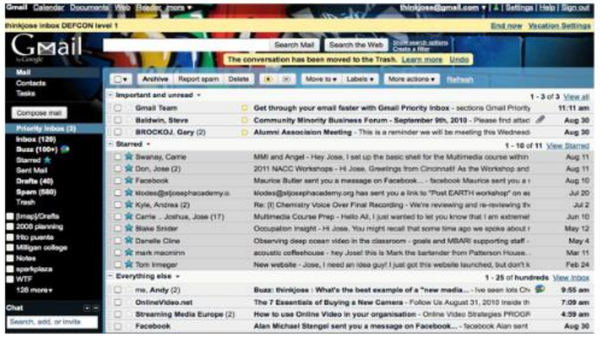
- Dataset:

  Privacy Attributes Dataset[1] with **22,167** images and **68** visual privacy attributes

- Comparison Results:

| Methods | CaffeNet [1] | GoogleNet [1] | ResNet-50 [1] | ours |
|---|---|---|---|---|
| mAP | 42.99 | 43.29 | 47.45 | **49.93** |

- Prediction Examples:




Full Name, Email Content, Email Address

Full Name, Email Content

Full Name, Email Content, **Email Address**

Race, Skin Color, Age, Occupation, Gender, Professional Circle, Hair Color, Complete Face, Partial Face, Weight, Height, Eye Color

Race, Skin Color, Age, Occupation, Gender, Professional Circle, Hair Color, Complete Face, Partial Face, Weight

Race, Skin Color, Age, Occupation, Gender, Professional Circle, Hair Color, Complete Face, Partial Face, Weight, **Height, Eye Color**


Passport, Nationality

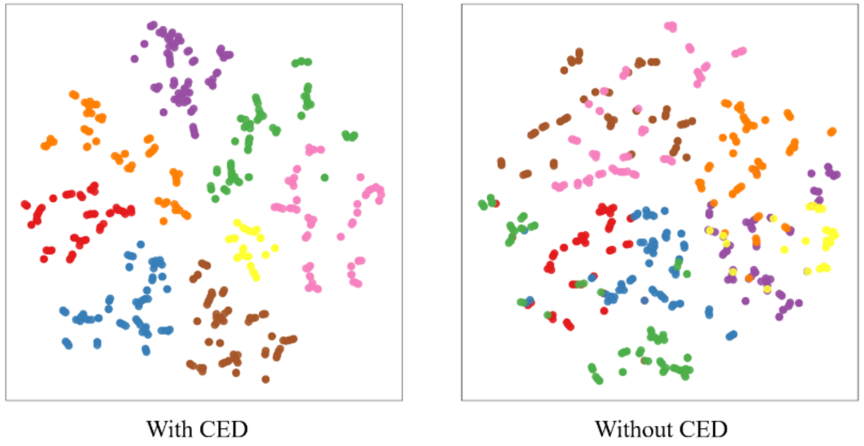
Passport

Passport, **Nationality**

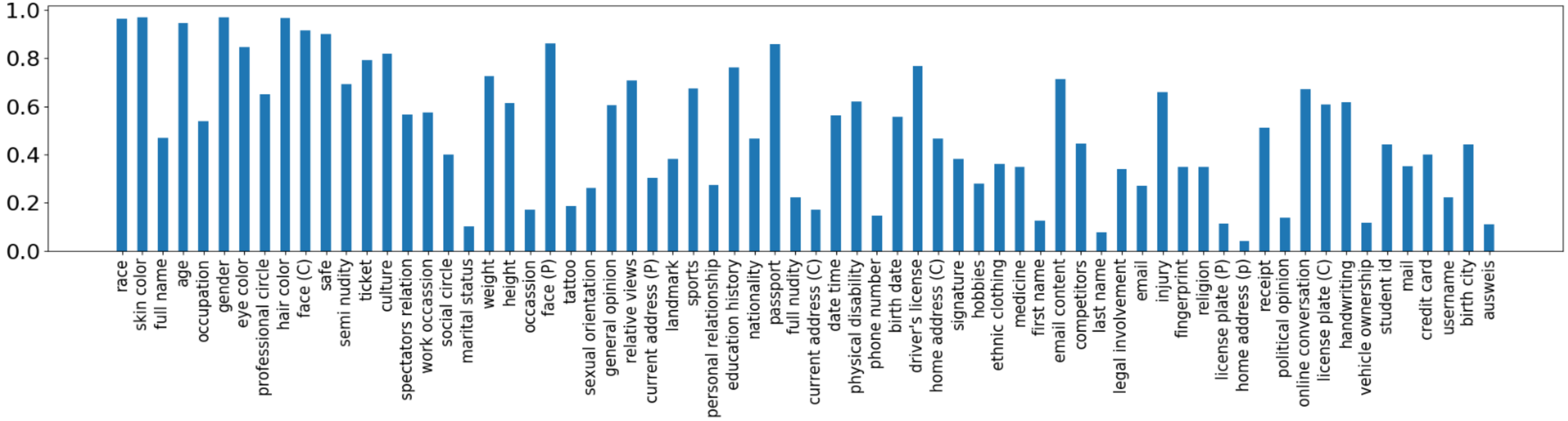
# Ablation Study:

| CED | Att. | MCM | mAP | miF1 | maF1 |
|---|---|---|---|---|---|
| | √ | √ | 49.83 | 0.7725 | 0.4428 |
| √ | | √ | 49.78 | 0.7645 | 0.4384 |
| √ | √ | | 49.78 | 0.7683 | 0.4284 |
| √ | √ | √ | **49.93** | **0.7751** | **0.4456** |

Comparison of our methods




t-SNE visualization




Average Precision scores on all visual privacy attributes. (C) represents ’complete’. (P) represents ’partial’.

## Reference:


[1] Gao J, Sun L, Cai M. Quantifying privacy vulnerability of individual mobility traces: A case study of license plate recognition data[J]. Transportation research part C: emerging technologies, 2019, 104: 78-94.

[2] Chen S, Zhang C, Dong M, et al. Using ranking-cnn for age estimation[C]//Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition. 2017: 5183-5192.

[3] Hu P, Ning H, Qiu T, et al. Security and privacy preservation scheme of face identification and resolution framework using fog computing in internet of things[J]. IEEE Internet of Things Journal, 2017, 4(5): 1143-1155.

[4] Orekondy T, Schiele B, Fritz M. Towards a visual privacy advisor: Understanding and predicting privacy risks in images[C]//Proceedings of the IEEE International Conference on Computer Vision. 2017: 3686-3695.

[5] Read J, Pfahringer B, Holmes G. Multi-label classification using ensembles of pruned sets[C]//2008 eighth IEEE international conference on data mining. IEEE, 2008: 995-1000.

[6] Barros R C, Cerri R, Freitas A A, et al. Probabilistic clustering for hierarchical multi-label classification of protein functions[C]//Joint European Conference on Machine Learning and Knowledge Discovery in Databases. Springer, Berlin, Heidelberg, 2013: 385-400.

[7] Bhatia K, Jain H, Kar P, et al. Sparse local embeddings for extreme multi-label classification[C]//Advances in neural information processing systems. 2015: 730-738.

[8] Gilmer J, Schoenholz S S, Riley P F, et al. Neural message passing for quantum chemistry[J]. arXiv preprint arXiv:1704.01212, 2017.

Thank you

&

Please email me if you have any questions.

Contact: Hanbin Hong (hhong4@hawk.iit.edu)