先端科学技術研究科　修士論文要旨

所属研究室 (主指導教員)	サイバーレジリエンス構成学 (門林　雄基　(教授))		
学籍番号	2011127	提出日	令和 3年 7月 27日
学生氏名	笹田　大翔		
論文題目	Differentially-Private Text Transformation to Prevent Private Attribute Inference プライベート属性推定の阻止に向けた差分プライベートテキスト変換		

要旨

To build prediction and classification models, fine-tuning, and transfer learning, various text data is provided to third parties. Since there is a risk that the adversary can infer the author's private attributes such as gender, age, location from text data, privacy preserving technologies are necessary. The text has a privacy problem in that the author's private attributes can be inferred even from unique expressions and abbreviations. To promote text sharing, we need to provide privacy preservation for both words and documents. Moreover, excessive privacy preservation impairs text utility. Therefore, it is necessary to prevent private attribute inference by privacy preservation while maintaining text utility. In this study, we propose a method to prevent from text privacy leakage by combining word-based anonymization using knowledge graph and document-based differentially-private transformation. We create duplicates in the text set while anonymizing words that lead to identification, and reduced the amount of noise required by the differential private transformation. As a result of evaluation experiments, we succeeded in maintaining the effectiveness of privacy preservation while suppressing the maximum loss of text utility to within 0.1 compared to the original text.