プライバシーを保護する特許検索

中川研究室 修士 2 年 胡 瀚林
指導教員： 中川 裕志 教授

2016 年 7 月 1 日

概要

企業が特許を取る前に，類似な特許が既に存在するかを確かめるために特許データベースを検索する必要がある．しかし，検索の質問から企業秘密が漏洩する可能性がある．ウェブテキスト検索の質問からユーザーの興味を守る手法が多数存在している．その中真の質問と同時にダミー質問を提出する手法が一番効率的、現実的である．一般的なウェブテキスト検索と違い，特許データベース検索は長い検索質問を用い，検索の精度と再現率を重視しているため、既存手法を直接特許検索に適用することはできない．本発表では既存手法を破られる攻手法を提案し、その攻撃手法に対応できるダミー質問生成システムを提案する．

1 INTRODUCTION

1.1 Patent Search

特許文章の特徴
特許検索の目的と方法
ーー新規性調査 (Novelty Search)

1.2 Patent Versus Non-patent Literature

特許文章と普通の文章の区別

2 PRIVATE INFORMATION RETRIEVAL

PIR の背景紹介

2.1 Private Information Retrieval

2.2 Obfuscation-Based Private Search

既存手法とその手法が特許検索に適用できない理由

3 LATENT SEMANTIC MODELS

ユーザーが質問に使った具体的な単語だけではなくユーザーが興味ある分野も隠すため、質問の意味を分析する必要がある．本稿では，分野あるいは単語の意味のカテゴリをトピックという．質問が一連のトピックと関係があると仮定し，質問 q とトピック t の関係を関数 $rscore(q,t)$ で評価する．

定義 1 (ユニバーサル質問集合:Q)**.** W を全ての単語の集合とする．ユニバーサル質問集合 Q とは W の冪集合である，つまり

$$Q = P(W) = X|X \subset W \tag{1}$$

定義 2 (質問-トピックスコア関数:$rscore$)**.** T を全ての可能なトピックの集合とする．質問 q とトピックの関係を表す関数とは

$$rscore : Q \times T \to \mathbb{R} \tag{2}$$

3.1 tf-idf

3.2 Latent Semantic Indexing

長所:計算簡単
短所:トピックベクトルが直交である単語 w の LSI トピックベクトル $LSI_w = (s_1, s_2, \ldots, s_{K_{LSI}})$
LSI トピック t の単語集合 $W' \subset W = \{w_1, w_2, \ldots, w_m\}$ の LSI トピックベクトル

$$LSI_q = \sum_{w_i \in q} LSI_{w_i} \tag{3}$$

3.3 Probabilistic Latent Semantic Indexing

長所:確率的モデル
短所:トレーニングセットに含まれていない文章 (質問) の分析が困難である

3.4 Latent Dirichlet Allocation

長所:確率的モデルトレーニングセットに含まれていない文章 (質問) の分析が簡単
短所:学習するときは単語数 x トピック数の行列を用いて反復するので学習するには時間がかかる (30 トピック、1000 反復は 3 日かかる) 各クラスに属する単語の tfidf 値の上位 10000 個を用いて LDA を行い全ての単語とトピックに対して $Pr[w|t]$ と $Pr[t]$ を計算する．
単語 w の LDA トピックベクトル $LDA_w = (Pr[w|t=1], Pr[w|t=2], \ldots, Pr[w|t=K_{LDA}])$
単語集合 $W' \subset W = \{w_1, w_2, \ldots, w_m\}$ の LDA トピックベクトル

$$Pr[t|W'] = \frac{\prod_{w \in W'} Pr[w|t])Pr[t]}{\prod_{w \in W'} Pr[w]} \tag{4}$$

$$LDA'_W = (Pr[W'|t=1], Pr[W'|t=2], \ldots, Pr[q|t=K_{LDA}]) \tag{5}$$

3.5 トピック間の距離

定義 3 (トピック間の cos 距離)**.**

4 privacy-protecting patent search

提案手法

評価 (攻撃) 方法

5 EXPERIMENT

実験

1 質問者:tfidf 攻撃者 LSA

2 質問者:LSA 攻撃者 LSA

3 質問者:LDA 攻撃者 LSA

4 質問者:LSA 攻撃者 LDA

6 CONCLUSIONS

7 FUTURE WORKS

符号	意味
N	辞書中の単語の数
$W = 1, 2, 3, \ldots, N$	単語集合
M	コーパス中の文書の数
$D = 1, 2, 3, \ldots, M$	文章集合
K	トピック数
$T = 1, 2, 3, \ldots, K$	トピック集合
$\ell_i = t_1, t_2, \ldots, K$	単語 i のトピックベクトル
ℓ	質問のトピックベクトル

表 1　表記法

Algorithm 1 潜在意味解析

Input: 単語文集行列 A

1: 特異値分解 $A = U\Sigma V$

2: 特異値の上位 T 個だけ用い、行列の階数を低減する:$A' = U_T\Sigma_T V_T$

3: U **return** R

Algorithm 2

Input: ユーザー質問集合:$U = \{u^r | r \in 1, 2, \ldots, R\}$, 単語のトピックベクトル集合 $L = \{\ell_i\}$ **return** R

Algorithm 3

Input: ユーザー質問集合:$U = \{u^r | r \in 1, 2, \ldots, R\}$, 単語のトピックベクトル集合 $L = \{\ell_i\}$ **return** R

Algorithm 4 デミー質問生成

Input: ユーザー質問集合:$U = \{u^r | r \in 1, 2, \ldots, R\}$, 単語のトピックベクトル集合 $L = \{\ell_i\}$ **return** R

Algorithm 5 HDGA(On Masking Topical Intent in Keyword Search)

Input: 質問:q_1

$Q = \{q_1\}\delta_{q_1} = \underset{t \in T}{\operatorname{argmax}} Pr[t|q_1]$
for all $t \in T \setminus \{\delta_{q_1}\}$ **do**
    $e_t = h(\delta_{q_1}||t||s)$
end for
$T_D = \{t^1_{q1}, t^2_{q1}, \ldots, t^2_{q1} | \forall t_1 \ \in T_D, \forall t_2 \ \in T \setminus T_D, e_{t_1} > e_{t_2}\}$
for all $t \in T_D$ **do**
    while $\underset{t \in T}{\operatorname{argmax}} Pr[t|q'] \neq t$ **do**
        randomly select $|q_1|$ keywords for t based on $Pr[w|t]$, to form a dummy query q'
    end while
    $Q = Q \cup \{q'\}$
end for
Shuffle queries in Q **return** Q

Algorithm 6 メイントピック攻撃

Input: 質問:$q = \{t_i\}$, 単語のトピックベクトル集合 $L = \{\ell_i\}$

$R = \phi$, $\ell = 0$
$\ell = \sum_{t_i \in Q} \ell_{t_i}$
$maintopic = \underset{j}{\operatorname{argmax}}\, \ell[j]$
for all $bk_k \in q$ **do**
    $R = R \cup \{\max_{t_i} l_{t_i}[maintopic]\}$
end for
return R

Algorithm 7 類似攻撃

Input: 質問集合:$Q = \{q_i^r \,|i \in \{1,2,3,4\}, r \in \{1,2,\ldots,R\}\}$, 単語のトピックベクトル集合 $L = \{\ell_i\}$

$p_i = q_i^1 \;\; i \in \{1,2,3,4\}, result = \phi$
for $r = 2, 3 \ldots, R$ **do**
  for $i = 1,2,3,4$ **do**
    $j = \underset{j}{\text{argmax}} \frac{p_i \cdot q_j^r}{|p_i||q_j^r|}$
    $d_i = \frac{p_i \cdot q_j^r}{|p_i||q_j^r|}$
    $temp_i = \frac{1}{r}(p_i(r-1) + q_j)$
  end for
  for $i = 1,2,3,4$ **do**
    $p_i = temp_i$
  end for
  $result = result \cup \{\underset{i}{\text{argmax}}\, d_i\}$
end for
return $result$