HĽADANIE ANOMÁLIÍ V TEXTOCH POMOCOU NEURÓNOVÝCH SIETÍ

Autor: Bc. Olha Koliesnikova
Vedúci práce: doc. RNDr. Gabriela Andrejková, CSc

Motivácia

- Odhaliť plagiátorstvo
- Zabezpečenie kvality textových údajov - identifikovať chyby, nezrovnalosti alebo odľahlé hodnoty vo veľkých súboroch textových údajov

Ciele

1. Spracovať prehľad známych výsledkov a použitých metód v oblasti hľadania anomálií v textoch.

2. Vytvoriť metódu (systém algoritmov) pre detekciu anomálií v textoch používajúci neurónovej siete.

3. Navrhnutú metódu aplikovať na textových dátach (vlastných alebo verejne dostupných) a výsledky vyhodnotiť porovnaním s inými metódami.

Článok

1. Kódovanie obsahu viet
   - ➔ Priemerovanie slovných vektorov do vety
   - ➔ Vektory relevancie značiek častí reči (POS)
   - ➔ Vloženie inverznej frekvencie dokumentov (IDF)
   - ➔ Sémantická podobnosť TF-IDF vektorov
2. Nájdenie posunov anomálnych častí
   - ➔ Bidirectional recurrent neural network, BI-LSTM, predikcia vloženia ďalšej vety.
3. Určenie anomálnych častí pomocou nájdených posunov.
   - ➔ Vety pod určitým prahom úspešnosti predikcie budú označené ako anomálne.
4. Evaluacia 4 metod vlozenia viet

Kľúčové pojmy:

1. **Detekcia anomálií** - identifikácia textov ktoré sa odchyľujú od bežných alebo očakávaných vzorcov v datasete.
2. **Vetné embeddingy** sú vektorové reprezentácie viet. Embeddingy umožňujú preniesť vety do vysoko dimenzionálneho priestoru, kde vety s podobným významom sú umiestnené blízko seba.
3. **Použitie vetných embeddingov na detekciu anomálií** - model transformuje vety na embeddingy a meria ich vzdialenosti od seba.

Anomálne texty sú tie, ktoré sú vzdialené (z hľadiska vektorovej vzdialenosti) od väčšiny ostatných viet v datasete.

Table 1

Results of pooling methods applied on Dataset 1

Dataset 1	Accu-racy	Preci-sion	Recall	*F1 Score*
Average pooling	96.13	0.72	0.75	0.74
POS-Tag pooling	96.94	0.77	0.81	0.79
IDF pooling	97.74	0.84	0.85	0.84
TF-IDF pooling	99.23	0.96	0.93	0.95

Dataset v článku vs Dataset v DP

Počet textov:	500	Planujeme 500
Veľkosť súboru:	5 kB - 3736 kB	Zatial neznama
Počet viet:	20 - 12728, priemerne 62	Zatial neznama
Anomalie:	Umelo vlozene	Umelo vlozene
Jazyk:	Arabsky	Slovensky

Aktualny stav

- Priprava datasetu (ziskanie dat, uprava textov - odstranit: mena, podakovanie, obsah, zoznamy, odkazy, cisla, znaky (okrem . a pismen)
- Model SlovakBERT, ktorý sme integrovali pomocou knižnice SentenceTransformer
- Programovanie metod na kódovanie obsahu viet
- Programovanie NS (2 vrstvova) na predikciu dalsiej vety – vstup 1 veta, vystup dalsia

Priklad upravenoho textu

"Analýza a návrh riešenia Kryptoanalýza šifier v mobilných sieťach Ciele práce."
"Analyzovať a porovnať publikované útoky na šifry používané v mobilných sieťach."
"Preskúmať praktické implementácie analyzovaných útokov."
"Navrhnúť nové metódy kryptoanalýzy týchto šifier."
"Úvod Práca je venovaná kryptoanalýze šifier ktoré sú používane v mobilných sieťach."
"Prioritne ide o šifry ako A A A alebo aj KASUMI a taktiež šifru SNOW G."
"V súčasnosti sú šifry A a A prelomené a je možná kryptoanalýza v reálnom respektíve skoro reálnom čase do niekoľko minút až hodín."
"Šifra KASUMI je taktiež šifra ktorá sa považuje sa prelomenú ale jej kryptoanalýza nie je možná v reálnom čase a v spôsobe použitia ako je v súčasnosti použitá v mobilných zariadeniach."
"Totižto šifra KASUMI sa používa v counting mode kde sa výsledok výstupu zašifrovaného počítadla pomocou xor funkciu pripojí k šifrovanej správe."
"Útoky ako related key rectangle attack je možný iba za znalosti veľkého počtu otvorených nešifrovaných textov kde je potrebná aj pomerne vysoká výpočtová sila."
"Poslednou spomínanou šifrou je šifra SNOW G."
"Práve táto šifra je časťou najnovšieho G štandardu v ktorom sa okrem šifry SNOW G taktiež využíva aj šifra AES."
"V našej práci sa budeme venovať predovšetkým kryptoanalýze šifier A a A respektíve budeme simulovať útoky na tieto šifry a povieme si aj niečo o reálnych možnostiach útokov na tieto šifry v súčasných mobilných sieťach."
"Následne sa budeme venovať kryptoanalýze predovšetkým diferenčnej kryptoanalýze šifre KASUMI a možnosti využití tejto kryptoanalýzy v praxi."
"Ako už bolo spomenuté v reálnych podmienkach súčasné útoky nedokážu prelomiť šifru KASUMI tak ako je používaná v mobilných sieťach a práve z tohto dôvodu budeme hľadať alternatívne útoky skúmať aktuálne prístupy s možnosťou využitie týchto útokov v praxi."
"Poslednú spomínanú šifru SNOW G si necháme ako alternatívnu časť záverečnej práce kde by sme taktiež chceli poukázať na možnosti útokov na túto šifru prípadne jej slabiny."
"Popis protokolov v mobilných sieťach a historické pozadie Počiatok komunikácie prostredníctvom mobilných telefónov sa datuje približne v rokoch."
"Vznikali rôzne dohody na štandardoch prvé telefónne zariadenia a začiatkom rokov prišiel druhý štandard ktorý už nevyužíval analógový ale digitálny prenos dát a zvuku."

Ďakujem za pozornosť!