# Comparison with textbugger\_li\_2018.py

# Bert-base-uncased-yelp-polarity model:

#### Our Attack

### **TextBugger**

Attack Results	<u> </u>	Attack Results	
Number of successful attacks:   Number of failed attacks:   Number of skipped attacks:   Original accuracy:   Accuracy under attack:   Attack success rate:   Average perturbed word %:   Average num. words per input:   Avg num queries:	21	Number of successful attacks: Number of failed attacks: Number of skipped attacks: Original accuracy: Accuracy under attack: Attack success rate: Average perturbed word %: Average num. words per input: Avg num queries:	21

textattack: Attack time: 172.80336356163025s textattack: Attack time: 176.63516521453857s

#### Bert-base-uncased-imdb model:

# Our Attack

# <u>TextBugger</u>

Number of successful attacks:   21	Attack Results	ļ	Attack Kesults	
Avg num queries:   419.72   Avg num queries:   539.12	Number of failed attacks:	4	Number of failed attacks:	3
	Number of skipped attacks:	2	Number of skipped attacks:	2
	Original accuracy:	92.59%	Original accuracy:	92.59%
	Accuracy under attack:	14.81%	Accuracy under attack:	11.11%
	Attack success rate:	84.0%	Attack success rate:	88.0%
	Average perturbed word %:	5.29%	Average perturbed word %:	32.84%

textattack: Attack time: 266.0633933544159s textattack: Attack time: 278.07997155189514s

# Albert-Base-v2-yelp-polarity model:

## Our Attack <u>TextBugger</u>

Attack Results		Attack Results	ļ.	ļ
Original accuracy:   Accuracy under attack:   Attack success rate:	8	Attack success rate:   Average perturbed word %:	22 3 0 100.0% 12.0% 88.0% 25.53% 133.36 337.72	     

textattack: Attack time: 144.9083080291748s textattack: Attack time: 174.5719850063324s

#### Albert-Base-v2-imdb model:

#### Our Attack

### <u>TextBugger</u>

Attack Results	1	Attack Results	
	22	Number of successful attacks:    Number of failed attacks:    Number of skipped attacks:	
Original accuracy:	89.29%	Original accuracy:	89.29%
Accuracy under attack:	10.71%	Accuracy under attack:	3.57%
Attack success rate:	88.0%	Attack success rate:	96.0%
Average perturbed word %:	5.2%	Average perturbed word %:	27.25%
Average num. words per input:	244.71	Average num. words per input:	244.71
Avg num queries:		Avg num queries:	490.64

textattack: Attack time: 582.0640995502472s textattack: Attack time: 486.14418745040894s