

Visual spoofing in content-based spam detection

Mark Sokolov, Kehinde Olufowobi, and Nic Herndon
East Carolina University

13th International Conference on Security of Information and Networks
November 4 – 7, 2020
Istanbul, Turkey

Overview

- 1 Introduction
 - Unchanged vs. changed email
- 2 Experimental design
 - Data source and format
 - Workflow
- 3 Results
 - Accuracy
 - Microsoft mail
 - Google mail
 - Other domains
- 4 Summary

Introduction

Subject: Please send money

Body: I am so distraught. I thought i could reach out to you to help me out. I came down to United Kingdom for a short vacation unfortunately i was mugged at the part of the hotel i stayed, all cash, credit card and cell phone was stolen from me but luckily for me i still have my passport with me. I've been to the embassy and to the police here but they're not helping issues at all end, my flight leaves in few hours time from now but. I am having problems settling the hotel bills and the hotel manager won't let me leave until i settle my hotel bills. I am freaked out at the moment.

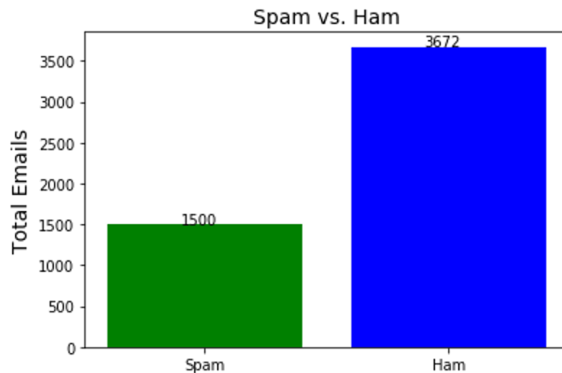
Unchanged vs. changed email

I am so distraught. I thought
 that I could reach out to you
 to help me out. I came down
 to United Kingdom for a short
 vacation unfortunately
 I was mugged at the park
 off the hotel I stayed, all cash,
 credit card and cell phone
 was stolen from me but
 luckily for me I still have
 my passport with me. I've
 been to the embassy and to
 the police here but they're
 not helping with issues at all
 and, my flight leaves in a few
 hours time from now but.
 I am having problems settling
 the hotel bills and the
 hotel manager won't let me
 leave until I settle my hotel
 bills. I am freaked out
 at the moment.

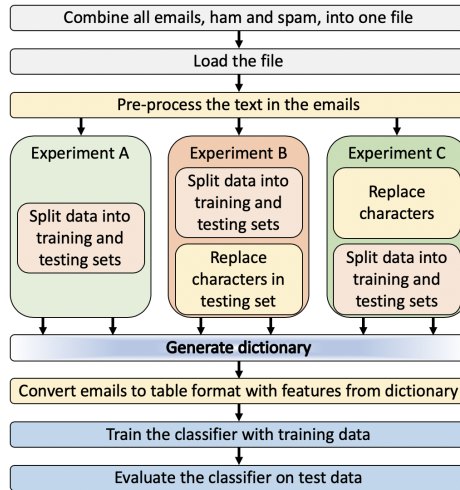
I am so distraught. I thought
 that I could reach out to you
 to help me out. I came down
 to United Kingdom for a short
 vacation unfortunately
 I was mugged at the park
 off the hotel I stayed, all cash,
 credit card and cell phone
 was stolen from me but
 luckily for me I still have
 my passport with me. I've
 been to the embassy and to
 the police here but they're
 not helping with issues at all
 and, my flight leaves in a few
 hours time from now but.
 I am having problems settling
 the hotel bills and the
 hotel manager won't let me
 leave until I settle my hotel
 bills. I am freaked out
 at the moment.

Data source

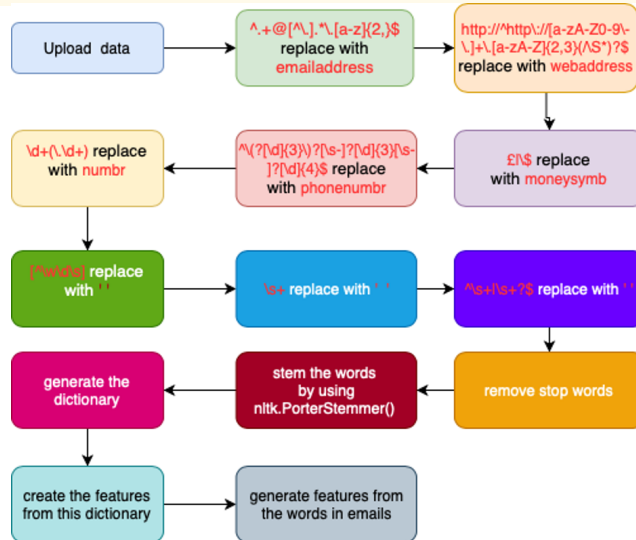
- Emails from the [Enron1 dataset](#)



Workflow



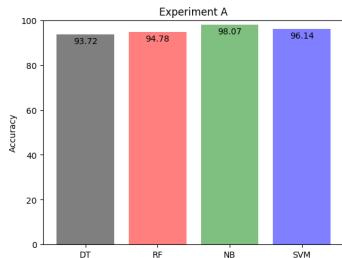
Pre-processing



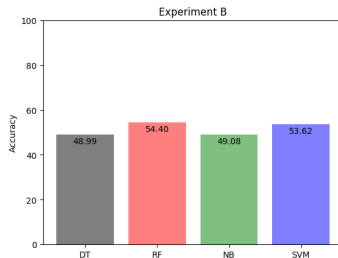
Analysis details

- Machine learning algorithms used
 - Naïve Bayes (NB)
 - Support vector machine (SVM)
 - Decision tree (DT)
 - Random forest (RF)
- Evaluation metrics
 - **Accuracy**
 - Precision
 - Recall
 - F-1 score
 - Confusion matrix
 - Production testing (Microsoft)

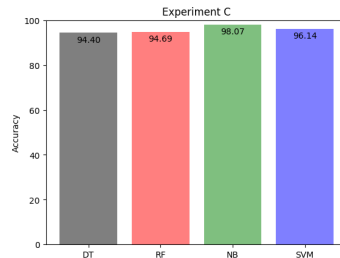
Results and discussion



Control experiment involving entirely unmodified datasets – the default encoding of characters in both the training and testing sets is preserved

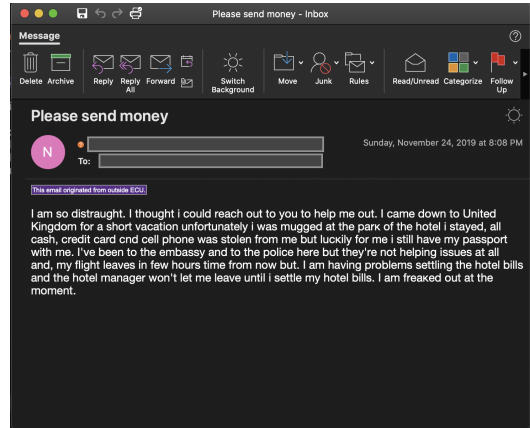
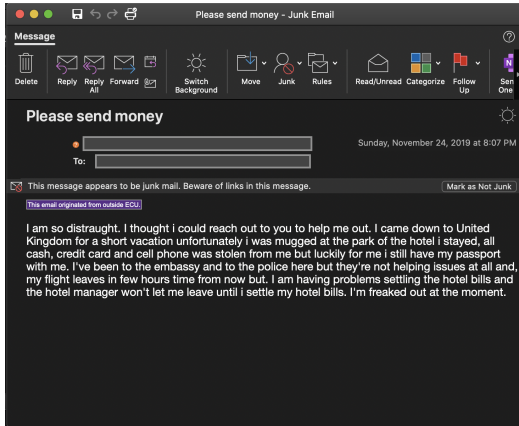


Encoding of the training set is preserved and the encoding of certain characters in the testing set uses corresponding confusables from the Cyrillic alphabet



Confusables introduced in training and testing sets so that each model is trained and evaluated with data from a single, mixed-script that contains confusables

Junk mail vs. inbox – Microsoft mail



Junk mail vs. inbox – Gmail

Money for Viagra ➤ Inbox x



Sokolov, Mark

to me ▾

Fri, Oct 30, 1:30 PM (1 day ago)



I

am so distraught. I thought i could reach out to you to help me out. I came down to United Kingdom for a short vacation unfortunately i was mugged at the part of the hotel i stayed, all cash, credit card and cell phone was stolen from me but luckily for me i still have my passport with me. I've been to the embassy and to the police here but they're not helping issues at all end, my flight leaves in few hours time from now but. I am having problems settling the hotel bills and the hotel manager won't let me leave until i settle my hotel bills. I am freaked out at the moment

Who are you?

Thanks, I'll check them out.

Very nice!

Money for Viagra ➤ Spam x



Sokolov, Mark

to me ▾

Oct 30, 2020, 1:31 PM (1 day ago)



Why is this message in spam? It is similar to messages that were identified as spam in the past.

Report not spam

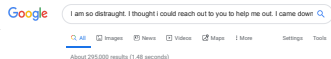


I

am so distraught. I thought i could reach out to you to help me out. I came down to United Kingdom for a short vacation unfortunately i was mugged at the part of the hotel i stayed, all cash, credit card and cell phone was stolen from me but luckily for me i still have my passport with me. I've been to the embassy and to the police here but they're not helping issues at all end, my flight leaves in few hours time from now but. I am having problems settling the hotel bills and the hotel manager won't let me leave until i settle my hotel bills. I am freaked out at the moment

Google search

11/30/2019 I am so distraught. I thought i could reach out to you to help me out. I came down to United Kingdom for a short vacation unfortunately i was mu...



"fer" (and any subsequent words) was ignored because we limit queries to 32 words.

For the Love of Viagra Spam and the 419 Email Scam | HuffPost
https://www.huffpost.com/entry/for-the-love-of-viagra-an_b_766530

Oct 19, 2010 - I am so distraught. I thought i could reach out to you to help me out. I came down to United Kingdom for a short vacation unfortunately i was mugged at the park of the hotel i stayed, all cash, credit card and cell phone was stolen from me but luckily for me i still have my passport with me. I've been to the ...

People also ask

What to do if you get robbed in a foreign country?

What should I do if I get robbed?

Does travel insurance cover being robbed?

Feedback

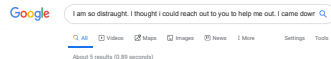
My Mom Got Robbed In Our Hotel! One Mile at a Time

<https://onemileatatime.com/my-mom-got-robbed-in-our-hotel>

The story of how my mom got robbed in our hotel, the W Barcelona. ... It's a safe city (in the sense that you don't have to fear for your life), but you do. ... "Told me that he likes me very much and wants to go out with me to find out more about him! ... I'm about to board a flight to get out of Spain so we can get to a consulate and ...

https://www.google.com/search?q=ACyBONR3TBVdJ_krim3N12c26NBR5aEQ%3A1575144769316&ci=Qc3Xf_cEILn5gL4w41Q&q=I+am+so+distr... 1/4

11/30/2019 I am so distraught. I thought i could reach out to you to help me out. I came down to United Kingdom for a short vacation unfortunately i was mu...



"all" (and any subsequent words) was ignored because we limit queries to 32 words.

Did you mean: I am so distraught. I thought i could reach out to you to help me out. I came down to United Kingdom for a short vacation unfortunately i was mugged at the park of the hotel i stayed, all cash, credit card and cell phone was stolen from me but luckily for me i still have my passport with me. I've been to the embassy and to the police here but they're not helping issues at all and, my flight leaves in few hours time from now but. I am having problems settling the hotel bills and the hotel manager won't let me leave until i settle my hotel bills. I am freaked out at the moment.

Trump lashes out at Iran for shutting down internet - KEYT ...

<https://keyt.com/news/national-world/2019/11/21/trump-lashes-out-...>
 Published November 21, 2019 10:21 am. Trump lashes out at Iran for shutting down internet. WASHINGTON (AP) — President Donald Trump says Iran is so "unstable" that the Iranian government has shut down the internet so Iranians cannot ...

Trump lashes out at Iran for shutting down internet - KTVZ

<https://kvz.com/news/national-world/2019/11/21/trump-lashes-out-...>
 Published November 21, 2019 10:21 am. Trump lashes out at Iran for shutting down internet. WASHINGTON (AP) — President Donald Trump says Iran is so "unstable" that the Iranian government has shut down the internet so Iranians cannot ...

Time Exception Sheet

<https://www.bcswan.net/cms/lib/Centricity/Domain>

https://www.google.com/search?q=ACyBONR3TBVdJ_krim3N12c26NBR5aEQ%3A1575144769316&ci=Qc3Xf_cEILn5gL4w41Q&q=I+am+so+distr... 1/3

Google translate

11/30/2019

Google Translate

ENGLISH - DETECTED



ENGLISH

I am so distraught. I thought i could reach out to you to help me out. I came down to United Kingdom for a short vacation unfortunately i was mugged at the park of the hotel i stayed, all cash, credit card cnd cell phone was stolen from me but luckily for me i still have my passport with me. I've been to the embassy and to the police here but they're not helping issues at all and, my flight leaves in few hours time from now but. I am having problems settling the hotel bills and the hotel manager won't let me leave until i settle my hotel bills. I am freaked out at the moment.

I am so distraught. I thought i could reach out to you to help me out. I came down to United Kingdom for a short vacation unfortunately i was mugged at the park of the hotel i stayed, all cash, credit card cnd cell phone was stolen from me but luckily for me i still have my passport with me. I've been to the embassy and to the police here but they're not helping issues at all and, my flight leaves in few hours time from now but. I am having problems settling the hotel bills and the hotel manager won't let me leave until i settle my hotel bills. I am freaked out at the moment.

<https://translate.google.com/#view=home&op=translate&sl=auto&tl=en&text=I am so distraught. I thought i could reach out to you to help me out. I came down...> 1/1

Summary

- 1 Introduction
 - Unchanged vs. changed email
- 2 Experimental design
 - Data source and format
 - Workflow
- 3 Results
 - Accuracy
 - Microsoft mail
 - Google mail
 - Other domains
- 4 Summary

Questions

Mark Sokolov

sokolovm19@students.ecu.edu

https://github.com/sokolovm19/Visual_Spoofing