Ajeet Kumar Singh

Personal Data

Place and Date of Birth:	Jodhpur, Rajasthan | 13 July 1991
Phone:	+91 88972-65167
email:	ajeetsingh0712[at]gmail[dot]com
Webpage:	ajeetksingh.github.io

Areas of Interest

Computer Vision, Natural Language Processing, Adversarial Machine Learning

Work Experience

Jul 2016 - Current | Researcher at TCS Research, TRDDC, Pune

As a researcher, I am responsible to make machine learning and deep learning private and secure. Specifically, ensuring the model performance is up to par in adversarial situations and preventing any private information leakage.

Jan 2016 - Jul 2016 | Research Intern at Intel Labs, Bengaluru

Responsible for development of deep learning based algorithms for large scale object recognition, detection and localization in images.

Jun 2013 - Dec 2015 | Research Associate at International Institute of Information and Technology-Hyderabad

Responsible for development of interactive Optical Character Recognition platform for web using popular web technologies.

Education

Dec 2015 MS by Research in Computer Science and Engineering
International Institute of Information Technology, Hydearbad
CGPA: 9.0

Aug 2011 Bachelor of Technology in Computer Engineering
Rajasthan Technical University(Jodhpur Institute of Engineering and Technology)
First Class Honours
Percentage: 78.16%

May 2007 Senior Secondary
Central Academy(Board of Secondary Education, Rajasthan)
Percentage: 82.62%

May 2005 Secondary
Central Academy(Board of Secondary Education, Rajasthan)
Percentage: 89.50%

Projects & Patents

July 2017 - Current | **Secure & Private Deep Learning**

1. *ML Testing Tool:* Nowadays machine learning and deep learning models are deployed heavily to speed up the analysis of large amount of data. Hence, adversarial evaluation of these models becomes very necessary. This evaluation will be done to ascertain any privacy or security loopholes in the model and how to prevent these. To this end, we came up with a testing tool which will test the model against various adversarial attacks (security and privacy) and provide recommendations to make these models more robust against such attacks.
2. Due to high level penetration of Internet in various aspects of life, it has become easy for any adversary to fool a user using *phishing*, where she provides a malicious URL to the user instead of original one. To this end, we propose a URL-based phishing detection technique to distinguish malicious URLs from benign ones (CSCML 2019).
3. A privacy prediction algorithm to predict if user is sharing a private image on social media platforms. Since definition of privacy is very subjective, we also let user label the images as *private* or *public* making the predictions more personalized (PSTCI@CIKM 2021).
4. VQA models generally do not consider the external facts about the useful texts present in images. So, we propose a dataset (OCR-VQA) which contains facts about the texts in images (ICDAR 2019). We also propose a GNN-based method to answer question which can only be answered using external facts (ICCV 2019).
5. Fully homomorphic encryption can be used to make the models more private making them immune to privacy attacks such as membership inference attacks and such. But, most of the FHE schemes are very slow making them undesirable to be used. We propose a recommendation engine which takes users privacy requirements from the machine learning model and accordingly suggest them suitable FHE library (SEAL, Heaan, etc.) to use (CSCML 2020).

Jul 2016 - July 2017 | **Data Masking System for Security and Privacy (One Patent filed in India, US and Europe)**

We developed a data masking system which automatically masks the sensitive contents in a document. This document can be either text or an image.

Jan 2016 - Jul 2016 | **Large Scale Image Recognition**

As part of the PCL team at Intel, my task was to develop deep learning based algorithms for large scale image recognition using popular Residual Networks and its variants.

Jun 2013 - Dec 2015 | **A Web framework for Optical Character Recognition on Indic Scripts and Languages.**

Development of a web-based OCR to provide a state-of-the-art optical character recognition tool to the general public. This web tool contains preprocessing module, script identification module, word recognition module, and an post-processing module. The framework was adaptable to include and evaluate multiple OCRs.

Aug 2015 | **Script and Language Identification using Recurrent Neural Networks (Accepted at ICDAR 2015)**

In this project, we investigate the utility of popular Recurrent Neural Networks for identification of script and language in document images at word and line level. We achieve the highest accuracy of 99.0% percent in script identification and 94.67% accuracy in language identification. Experiments were done on 12 Indic scripts and 3 Roman-script based languages on 55K document images.

Oct 2015 | **Script Identification in Multilingual Scene Texts (Accepted at DAS 2016)**

We present an approach for automatically identifying the script of the text localized on the scene images using computer vision. We represent the text images using mid-level strokes based features. We achieved an accuracy of 96.70% on CVSI dataset and benchmark on our own Indian language scene text dataset.

Nov 2014 | **Billion Word Imputation**

This project was done under Machine Learning course requirement under the guidance of Dr. Shailesh Kumar. In this NLP project, our task was to find the missing word in a given sentence as well as its position in the sentence. We found the missing words and their location by finding the co-occurrence consistency calculated from $n-$gram and *skip*-grams of the words available in training set.

Publications

PSTCI@CIKM 2021 | **Interpretable and Robust Face Verification.**
Preetam Prabhu Srikar Dammu, Srinivasa Rao Chalamala, *Ajeet Kumar Singh*.

PSTCI@CIKM 2021 | **Explainable and Personalized Privacy Prediction.**
Preetam Prabhu Srikar Dammu, Srinivasa Rao Chalamala, *Ajeet Kumar Singh*.

CSCML 2020 | **A Recommender System for Efficient Implementation of Privacy Preserving Machine Learning Primitives Based on FHE.**
Imtiyazuddin Shaik, *Ajeet Kumar Singh*, Harika Narumanchi, Nitesh Emmadi, Rajan Mindigal Alasingara Bhattachar.

ICCV 2019 | **From String to Things: Knowledge-enabled VQA Model that can Read and Reason.**
*Ajeet Kumar Singh (*TCS *Research)*, Anand Mishra (IIT Jodhpur), Shashank Shekhar (IISc), Anirban Chakraborty (IISc).

ICDAR 2019 | **OCR-VQA: Visual Question Answering by Reading Text in Images.**
Anand Mishra (IISc), Shashank Shekhar (IISc), *Ajeet Kumar Singh (*TCS *Research)*, Anirban Chakraborty (IISc).

CSCML 2019 | **Everything Is in the Name–A URL Based Approach for Phishing Detection.**
Harshal Tupsamudre (TCS Research), *Ajeet Kumar Singh (*TCS *Research)*, Sachin Lodha (TCS Research).

ACCV 2018 | **Deep Embedding using Bayesian Risk Minimization with Application to Sketch Recognition.**
*Ajeet Kumar Singh (*TCS *Research)*, Anand Mishra (IISc).

DAS 2016 | **A Simple and Effective Solution for Script Identification in Wild.**
*Ajeet Kumar Singh (*IIIT-H*)*, Anand Mishra (IIIT-H), Pranav Dabral (IIIT-H), C. V. Jawahar (IIIT-H).

DAS 2016 | **Multilingual ocr for Indic Scripts.**
Minesh Mathew (IIIT-H), *Ajeet Kumar Singh (*IIIT-H*)*, C. V. Jawahar (IIIT-H)

ICDAR 2015 | **Can RNNs Reliably Separate Script and Language at Word and Line Level?**
*Ajeet Kumar Singh (*IIIT-H*)*, C. V. Jawahar (IIIT-H).

DAS 2014 | **Towards Robust OCR System for Indic Scripts.**
Praveen Krishnan (IIIT-H), Naveen Sankaran (IIIT-H), *Ajeet Kumar Singh (*IIIT-H*)*, C. V. Jawahar (IIIT-H).

Tecnical Skills

Languages:	C, C++, Python, MATLAB
Frameworks and Technology:	PyTorch, TensorFlow, Caffe
Databases:	MySQL
Web Design:	HTML, PHP, JavaScript, AJAX, JQuery
Platforms:	Linux, Unix

Hobbies and Interests

Reading, Sports

References

Available on request.