Srinivasa Rao Chalamala

Personal Data

Place :	Hyderabad, Telangana
Phone:	+91 9030325566
email:	vaasuch[at]gmail[dot]com
Webpage:	https://srinivaschalamala.github.io/

Areas of Interest

Computer Vision, Natural Language Processing, Adversarial Machine Learning, Embedded digital signal processing.

Work Experience: LinkedIn

2018 - Current — Senior Scientist and Lead, Trustworthy AI project at TCS Research

As a researcher, I am responsible to ensure deep learning models are Trustworthy. Trustworthy AI comprises of models that are resilient to adversarial attacks, explainable, and fair.

2014 - 2018 — Scientist, Secure and Private AI project at TCS Innovation Labs

Responsible for research and development of deep learning based algorithms for large scale object recognition, detection and localization in image. Also, responsible for development of various algorithms for text detection, extraction, OCR, text redaction algorithms

2009 - 2014 — Researcher at TCS Innovation Labs

Responsible for Research and development of various Face recognition algorithms, image, video, and speech watermarking algorithms

2004 - 2009 — DSP Engineer

Responsible for porting and optimizing video and audio codecs on to TI DSP Boards, development of wireless signal processing algorithms, implement WLAN algorithms in SystemC

Education

JUN 2023 — Ph.D. in Electronics and Communication Engineering
International Institute of Information Technology, Hyderabad

May 2004 — Master of Technology in Electronics and Communications Engineering
IIT Kharagpur
Percentage:CGPA 8.8

May 2001 — Bachelor of Engineering in Electronics and Communication Engineering
Andhra University University(SRKR Engineering College, Bhimavaram)
First Class Honours
Percentage: 74%

March 1998 — Diploma in Engineering in Industrial Electronics
Govt. Institute of Electronics, Secunderabad
Percentage: 73%

Projects

2019 - Current

Trustworthy AI

Recent incidents related to real world deep learning systems prompt us to focus on the safety and security aspects. As the deep learning systems are highly dependent on the data and learning process, it is easy to manipulate and force them to provide wrong prediction. Other concerns related to the opaqueness of the models used in several applications especially when these models are affecting large number of people. Unless these models are well explained it is difficult to create trust among the end users. Bias and Fairness is another important issue that is affecting the widespread usage of systems based deep learning. In this project we evaluating models for robustness, explainability, Bias to enhance the trust in AI.

2016 - 2018

Secure & Private Deep Learning

1. Adversarial perturbation to the images could completely flip the model predictions. This could result in complete failure of the systems developed based on deep learning. Effective defenses are required to prevent these scenarios from occurring. We developed methods to detect adversarial input samples and prevent them from fooling the models.
2. 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).
3. 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. We also propose a GNN-based method to answer question which can only be answered using external facts
4. 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

2016 - 2017

Data Masking System for Security and Privacy

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

2013 - 2015

Face Recognition

Developed a face verification system for identifying car drivers entering office premises. The face verification systems shall work on faces having pose and light variations(ICCE 2015).

2009 - 2012

Digital watermarking

The need for digital rights management (DRM) is increasing to prevent the unauthorized distribution of media whether it is video or audio. With increase in web based solutions and expertise in using computer there is great chance of illegal data distribution and usage. Watermarking is a technique of embedding a secret information in the media and used for tracking the source of content. In addition the process must be reversible even if there are malicious attacks on the content in which it is embedded. This project aims at developing watermarking algorithms for video copyright protection

2007 - 2008

CardioNet

This project is aimed at developing a health monitoring system on TMS320DM642 EVM called Cardionet. The system is based on H.264 codec (baseline profile) and AMR Wideband codec. H.264 technology is newly emerging Codec Standard for high compression for bandwidth saving. AMR-WB speech codec is being used for better compression of speech signals with good quality. Along with audio, video data ECG data acquired from a ECG system using serial port is also sent.

2006 - 2007

PlaceShift Box

This project is aimed at developing TMS320DM642 based Place-shifting box using H.264 codec (baseline profile), AMR audio codec and TCP protocol for distribution of media data. H.264 technology is newly emerging Codec Standard for high compression for bandwidth saving. TCP is mainly used for transportation of media data.

2005 - 2006

Porting and Optimization of H.264 Video Codec

The project is aimed at porting h.264 decoder reference code on TM3206416 platform, optimize it for streaming applications. This decoder used in the subsequent projects. Also, this project aimed at integrating the AMR-WB encoder and decoder with the on-board audio device(AIC23) of TI's DM642. The integration is done in such a way that the real time needs of speech codec taken care of. The speech quality was enhanced by using EDMA.

2004 - 2005

Physical layer security for Wireless Networks

The main objective of the work is to develop a physical layer encryption scheme to ensure the security of wireless networks. MATLAB simulink is used for the required simulations. The scheme is implemented both in conventional wireless communication system and in MC-CDMA system under MAGNET group. Also developed a demonstrable model for 802.11g physical layer. The implementation of each block is done in MATLAB based Simulink.

Patents

17 Unique Patent filings (17 in India, 17 in USA)
Multiple Patent Grants

Patents Reference URL

Publications: Google Scholar link

FLAIRS 2022	A Robust Method to Protect Text Classification Models against Adversarial Attacks Bala Mallikarjunarao G, *Srinivasa Rao Chalamala*, Ajeet Kumar Singh.
CSI Transactions 2022	Federated learning to comply with data protection regulations. *Srinivasa Rao Chalamala*, Naveen Ajeet Kumar Singh.
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.
Trustcom 2020	Secure and Privacy Preserving Method for Biometric Template Protection using Fully Homomorphic Encryption. Arun Kumar Jindal, Imtiyazuddin Shaik, *Srinivasa Rao Chalamala*, Rajan MA, Sachin Lodha.
ICCE 2019	Securing Face Templates using Deep Convolutional Neural Network and Random Projection. Arun Kumar Jindal, *Srinivasa Rao Chalamala*, Santosh Kumar Jami.
ACL 2019	A Fuzzy Approach to Mute Sensitive Information in Noisy Audio Conversations. Imran Shaik, Bala Mallikarjunarao G, *Srinivasa Rao Chalamala*, Sunil Kumar Kopparpu.
ICCE 2019	Biometric Template Protection Through Adversarial Learning. Santosh Kumar Jami, *Srinivasa Rao Chalamala*, Arun Kumar Jindal.
CVPRW 2018	Face Template Protection Using Deep Convolutional Neural Network. Arun Kumar Jindal, *Srinivasa Rao Chalamala*, Santosh Kumar Jami.
ISMS 2016	A Probabilistic Approach for Human Action Recognition Using Motion Trajectories. *Srinivasa Rao Chalamala*, Prasanna Kumar.
ISMS 2016	A Symbol Based Watermarking Approach for Spread Spectrum Audio Watermarking Methods. Bala Malliarjunarao, *Srinivasa Rao Chalamala*, Prasanna Kumar.
AIMS 2015	Local Binary Patterns for Digital Image Watermarking. *Srinivasa Rao Chalamala*,Krishna Rao Kakkirala.
ICCE 2015	Enhanced face recognition using Cross Local Radon Binary Patterns. *Srinivasa Rao Chalamala*, Santosh Kumar, Yegananarayana B.
IACC 2015	Analysis of wavelet and contourlet transform based image watermarking techniques . *Srinivasa Rao Chalamala*, Krishna Rao Kakkirala, Bala Mallikarjunarao .
ICALIP 2014	DWT-SVD based blind audio watermarking scheme for copyright protection . Krishna Rao Kakkirala, *Srinivasa Rao Chalamala*, Bala Mallikarjuna Rao .

Publications

ICALIP 2014 | A robust video synchronization method based on hierarchical shot detection .
Srinivasa Rao Chalamala, Krishna Rao Kakkirala, Jyoti Dhillon .

CSPA 2014 | Block based robust blind image watermarking using discrete wavelet transform .
Krishna Rao Kakkirala, *Srinivasa Rao Chalamala*, .

CSPA 2014 | Face recognition using spatial pyramid matching and LRBP .
Srinivasa Rao Chalamala, Krishna Rao Kakkirala, Santosh Kumar Jami .

CYBERNETICSCOM 2013 | A robust image watermarking using DWT, SVD and Torus automorphism .
Krishna Rao Kakkirala, *Srinivasa Rao Chalamala*, Jyoti Dhillon .

ICGIP 2011 | A robust hierarchical video shot detection method .
Jyoti Dhillon, Krishna Rao Kakkirala, *Srinivasa Rao Chalamala*, .

IWS 2005 | Enhancement of Security of Wireless Networks using Physical Layer Protection.
Arpan Pal, *Srinivasa Rao Chalamala*, Suvra Sekhar Das, Balamuralidhar Purushothaman .

SPIE-OC 2005 | A comparison of dispersion compensating schemes in 40 Gb/s optical transmission with different modulation formats.
Ranjan Gangopadhyay, Vishnu Vardhanan, *Srinivasa Rao Chalamala*.

Technical Skills

Languages:	C, Python, MATLAB, VHDL
Frameworks and Technology:	PyTorch
Platforms:	Linux, Unix
DSP:	TMS320DM642, TM3206416
Embedded:	Beagle, ARM9, MSP430, DMA, I2C, RS232
Assembly Language:	Intel 8085, TM3206416

Hobbies and Interests

Reading, Gardening

References

Available on request.