

SRINIVASA RAO CHALAMALA

PERSONAL DATA

PLACE : Hyderabad, Telangana
PHONE: +91 9030325566
EMAIL: [srini.chalamala\[at\]gmail\[dot\]com](mailto:srini.chalamala[at]gmail[dot]com)
WEBPAGE: <https://srinivaschalamala.github.io/>

AREAS OF INTEREST

Computer Vision, Natural Language Processing, Deep learning, Image Processing, Adversarial Machine Learning, and Embedded digital signal processing.

WORK EXPERIENCE: [LINKEDIN](#)

2018 - CURRENT	Senior Scientist and Lead, Trustworthy AI project at TCS Research As a lead researcher, I am responsible for ensuring that deep learning applications are Trustworthy. Some of Trustworthy AI aspects comprise resiliency to adversarial attacks, explainability, and fairness and bias.
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 images. Also, responsible for the development of various algorithms for text detection, extraction, OCR, and text redaction algorithms
2009 - 2014	Researcher at TCS Innovation Labs Responsible for Research and development of various Face recognition algorithms, images, videos, and speech watermarking algorithms
2004 - 2009	DSP Engineer Responsible for porting and optimizing video and audio codecs onto TI DSP Boards, development of wireless signal processing algorithms, and implementing WLAN algorithms in SystemC

EDUCATION

MARCH 2023	Ph.D. in ELECTRONICS AND COMMUNICATION ENGINEERING SECURITY AND PROTECTION OF FACIAL BIOMETRICS SYSTEMS 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%

PATENTS

54 PATENT FILINGS
28 PATENT GRANTS

[PATENTS REFERENCE URL](#)

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 deep learning systems are highly dependent on the data and learning process, it is easy to manipulate and force them to provide wrong predictions. Other concerns related to the opaqueness of the models used in several applications especially when these models are affecting a large number of people. Unless these models are well explained, it is difficult to create trust among the end users. Bias and Fairness are the other important issues that are affecting the widespread usage of systems-based deep learning. In this project, we evaluate models for robustness, explainability, Bias to enhance 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 a user is sharing a private image on social media platforms. Since the definition of privacy is very subjective, we also let the 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) that contains facts about the texts in images. We also propose a GNN-based method to answer questions that 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. However, most of the FHE schemes are very slow making them undesirable to be used. We propose a recommendation engine that takes user 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 <p>The need for digital rights management (DRM) is increasing to prevent the unauthorized distribution of media whether it is video or audio. With the increase in web-based solutions and expertise in using computer, there is a great chance of illegal data distribution and usage. Watermarking is a technique of embedding a piece of 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</p>
2007 - 2008	CardioNet <p>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 Wide-band 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.</p>
2006 - 2007	PlaceShift Box <p>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 the newly emerging Codec Standard for high compression for bandwidth saving. TCP is mainly used for the transportation of media data.</p>
2005 - 2006	Porting and Optimization of H.264 Video Codec <p>The project is aimed at porting h.264 decoder reference code on TM3206416 platform, optimizing 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. Integration is done in such a way that the real-time needs of speech codec are taken care of. The speech quality was enhanced by using EDMA.</p>
2004 - 2005	Physical layer security for Wireless Networks <p>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 systems 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.</p>

PUBLICATIONS: [GOOGLE SCHOLAR LINK](#)

FLAIRS 2022	A ROBUST METHOD TO PROTECT TEXT CLASSIFICATION MODELS AGAINST ADVERSARIAL ATTACKS Bala Mallikarjunarao G, <i>Srinivasa Rao Chalamala</i> , Ajeet Kumar Singh.
CSI TRANSACTIONS 2022	FEDERATED LEARNING TO COMPLY WITH DATA PROTECTION REGULATIONS. <i>Srinivasa Rao Chalamala</i> , Naveen Ajeet Kumar Singh.
PSTCI@CIKM 2021	INTERPRETABLE AND ROBUST FACE VERIFICATION. Preetam Prabhu Srikar Dammu, <i>Srinivasa Rao Chalamala</i> , Ajeet Kumar Singh.
PSTCI@CIKM 2021	EXPLAINABLE AND PERSONALIZED PRIVACY PREDICTION. Preetam Prabhu Srikar Dammu, <i>Srinivasa Rao Chalamala</i> , Ajeet Kumar Singh.
TRUSTCOM 2020	SECURE AND PRIVACY PRESERVING METHOD FOR BIOMETRIC TEMPLATE PROTECTION USING FULLY HOMOMORPHIC ENCRYPTION. Arun Kumar Jindal, Imtiyazuddin Shaik, <i>Srinivasa Rao Chalamala</i> , Rajan MA, Sachin Lodha.
ICCE 2019	SECURING FACE TEMPLATES USING DEEP CONVOLUTIONAL NEURAL NETWORK AND RANDOM PROJECTION. Arun Kumar Jindal, <i>Srinivasa Rao Chalamala</i> , Santosh Kumar Jami.
ACL 2019	A FUZZY APPROACH TO MUTE SENSITIVE INFORMATION IN NOISY AUDIO CONVERSATIONS. Imran Shaik, Bala Mallikarjunarao G, <i>Srinivasa Rao Chalamala</i> , Sunil Kumar Koppurpu.
ICCE 2019	BIOMETRIC TEMPLATE PROTECTION THROUGH ADVERSARIAL LEARNING. Santosh Kumar Jami, <i>Srinivasa Rao Chalamala</i> , Arun Kumar Jindal.
CVPRW 2018	FACE TEMPLATE PROTECTION USING DEEP CONVOLUTIONAL NEURAL NETWORK. Arun Kumar Jindal, <i>Srinivasa Rao Chalamala</i> , Santosh Kumar Jami.
ISMS 2016	A PROBABILISTIC APPROACH FOR HUMAN ACTION RECOGNITION USING MOTION TRAJECTORIES. <i>Srinivasa Rao Chalamala</i> , Prasanna Kumar.
ISMS 2016	A SYMBOL BASED WATERMARKING APPROACH FOR SPREAD SPECTRUM AUDIO WATERMARKING METHODS. Bala Mallikarjunarao, <i>Srinivasa Rao Chalamala</i> , Prasanna Kumar.
AIMS 2015	LOCAL BINARY PATTERNS FOR DIGITAL IMAGE WATERMARKING. <i>Srinivasa Rao Chalamala</i> , Krishna Rao Kakkirala.
ICCE 2015	ENHANCED FACE RECOGNITION USING CROSS LOCAL RADON BINARY PATTERNS. <i>Srinivasa Rao Chalamala</i> , Santosh Kumar, Yegananarayana B.
IACC 2015	ANALYSIS OF WAVELET AND CONTOURLET TRANSFORM BASED IMAGE WATERMARKING TECHNIQUES . <i>Srinivasa Rao Chalamala</i> , Krishna Rao Kakkirala, Bala Mallikarjunarao .
ICALIP 2014	DWT-SVD BASED BLIND AUDIO WATERMARKING SCHEME FOR COPYRIGHT PROTECTION . Krishna Rao Kakkirala, <i>Srinivasa Rao Chalamala</i> , Bala Mallikarjuna Rao .

PUBLICATIONS

ICALIP 2014	A ROBUST VIDEO SYNCHRONIZATION METHOD BASED ON HIERARCHICAL SHOT DETECTION . <i>Srinivasa Rao Chalamala, Krishna Rao Kakkirala, Jyoti Dhillon .</i>
CSPA 2014	BLOCK BASED ROBUST BLIND IMAGE WATERMARKING USING DISCRETE WAVELET TRANSFORM . <i>Krishna Rao Kakkirala, Srinivasa Rao Chalamala, .</i>
CSPA 2014	FACE RECOGNITION USING SPATIAL PYRAMID MATCHING AND LRBP . <i>Srinivasa Rao Chalamala, Krishna Rao Kakkirala, Santosh Kumar Jami .</i>
CYBERNETICSCOM 2013	A ROBUST IMAGE WATERMARKING USING DWT, SVD AND TORUS AUTOMORPHISM . <i>Krishna Rao Kakkirala, Srinivasa Rao Chalamala, Jyoti Dhillon .</i>
ICGIP 2011	A ROBUST HIERARCHICAL VIDEO SHOT DETECTION METHOD . <i>Jyoti Dhillon, Krishna Rao Kakkirala, Srinivasa Rao Chalamala, .</i>
IWS 2005	ENHANCEMENT OF SECURITY OF WIRELESS NETWORKS USING PHYSICAL LAYER PROTECTION. <i>Arpan Pal, Srinivasa Rao Chalamala, Suvra Sekhar Das, Balamuralidhar Purushothaman .</i>
SPIE-OC 2005	A COMPARISON OF DISPERSION COMPENSATING SCHEMES IN 40 GB/S OPTICAL TRANSMISSION WITH DIFFERENT MODULATION FORMATS. <i>Ranjan Gangopadhyay, Vishnu Vardhanan, Srinivasa Rao Chalamala.</i>

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.