Vishal Asnani

Phone: +1 (517) 505-4249
Email: asnanivi@msu.edu
Website: https://vishal3477.github.io/
LinkedIn: https://linkedin.com/in/vishal-asnani/
GitHub: https://github.com/vishal3477

OBJECTIVE

Innovative and dedicated media forensics professional seeking a dynamic role where my advanced skills in media provenance, analysis, detection, and verification can be utilized to counter misinformation and enhance the trustworthiness of visual information. I am committed to leveraging cutting-edge technologies and collaborating with multidisciplinary teams to develop impactful and reliable solutions.

EDUCATION

Ph.D. In Computer Science and Engineering | Aug. 2020-Dec. 2024|
Advisor: Dr. Xiaoming Liu
Michigan State University, East Lansing, USA
GPA: 3.75/4.0, Graduation: December 2024

B.E.(Hons.) Electronics and Instrumentation Engineering (Minor in Finance) | Aug. 2015- May 2019|
Birla Institute of Technology and Science, Pilani, India
CGPA: 8.01/10.0

PUBLICATIONS

- **Vishal Asnani**, John Collomosse, Tu Bui, Xiaoming Liu, and Shruti Agarwal. "ProMark: Proactive Diffusion Watermarking for Causal Attribution." In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, 2024.

- **Vishal Asnani**, Abhinav Kumar, Suya You, and Xiaoming Liu. "PrObeD: Proactive Object Detection Wrapper." *Advances in Neural Information Processing Systems (NeuRIPS)*, 2023.

- **Vishal Asnani**, Xi Yin, Tal Hassner, Xiaoming Liu, "Reverse Engineering of Generative Models: Inferring Model Hyperparameters from Generated Images", *In IEEE Transactions on Pattern Analysis and Machine Intelligence (T-PAMI)* 2023.

- **Vishal Asnani,** Xi Yin, Tal Hassner, Xiaoming Liu, "MaLP: Manipulation Localization Using a Proactive Scheme," In Proceeding of IEEE Computer Vision and Pattern Recognition (**CVPR**), 2023.

- **Vishal Asnani**, Xi Yin, Tal Hassner, Sijia Liu, Xiaoming Liu, "Proactive Image Manipulation Detection," In Proceeding of IEEE Computer Vision and Pattern Recognition (**CVPR**), 2022.

- Yuguang Yao, Xiao Guo, **Vishal Asnani**, Yifan Gong, Jiancheng Liu, Xue Lin, Xiaoming Liu, and Sijia Liu. "Reverse Engineering of Deceptions on Machine-and Human-Centric Attacks." Foundations and Trends® in Privacy and Security, 2024.

- Xiao Guo, **Vishal Asnani**, Sijia Liu, and Xiaoming Liu. "Tracing Hyperparameter Dependencies for Model Parsing via Learnable Graph Pooling Network, submitted for review.

WORK EXPERIENCE

1. **Adobe, San Jose, USA: Research Scientist Intern** | May. 2024- Present|
   - Research scientist intern in the Cross-representation learning (XRL) team.
   - Real-time practical scenario of Causal Training Concept attribution for the synthetic images generated by a generative model.
   - The concepts are watermarked in an online manner without any costly training.

2. **Adobe, San Jose, USA: Research Scientist Intern.** | May. 2023- Nov. 2023 |
   - Research scientist intern in the Cross-representation learning (XRL) team.
   - Working on the novel problem of Causal Training Concept attribution for the synthetic images generated by a generative model.
   - The problem involves attributing different artist's concept images which influenced the generation of the synthetic images.
   - We use a proactive scheme of embedding different watermarks into the images, to later recover these watermarks for attribution.

3. **Texas Instruments, Bengaluru, India: Analog design intern** | Jul. 2018- Dec. 2018 |
   - Analog design intern in Multiphase and Control solutions team.
   - Developed a Perl Script to create vector-based patterns for SWD and PMBus commands used in the test program.
   - Patterns were appended to the test program beforehand, thereby saving test time by approximately 74%.

PROJECTS

1. **Video Templates for video-based tasks (Collaboration with Meta)** |Jan. 2024- Present|
   - Working on developing a video-template, which would improve the performance of video-based tasks.
   - A video-based proactive technique leveraging large-language models (LLMs) and vision language models is being developed.
   - The performance for video-based tasks like action recognition, video-captioning, video classification, etc. would be improved.

2. **Concept watermarking using textual inversion (Collaboration with Adobe)** |May 2024- Present|
   - Developing a customization-based textual inversion approach for concept watermarking of diffusion models.
   - The stable diffusion model would be fixed, but the original artists IP would be integrated into the model for media provenance.

3. **Diffusion Watermarking for Causal Attribution (Collaboration with Adobe)** |May. 2023-Nov. 2023|
   - Developed ProMark, a causal attribution technique to credit training data concepts in images generated by GenAI models.
   - Embedded imperceptible watermarks into training images, which diffusion models retain in generated images.

- Successfully embedded up to 2^{16} unique watermarks, with each training image containing multiple watermarks.
- ProMark significantly outperforms the prior passive correlation-based works. **(Patent Pending)**

4. **Proactive Object Detection Wrapper. (Collaboration with DEVCOM Army Research)**   **|Dec. 2022-May. 2023|**
   - Focused on enhancing 2D object detection, particularly for generic and camouflaged images.
   - Addressed the suboptimal convergence of neural networks in object detection by proposing PrObeD, a proactive scheme.
   - Developed an encoder-decoder architecture in PrObeD where the encoder generates image-dependent templates, and the decoder recovers these templates from encrypted images.
   - Demonstrated that learning templates improves object detection performance on MS-COCO, CAMO, COD10K, and NC4K datasets.

5. **Image manipulation Localization using proactive schemes. (Collaboration with Meta)**   **|May. 2022-Nov. 2022|**
   - A novel proactive scheme for image manipulation localization, MaLP, applicable to both face and generic images is proposed.
   - MaLP has a two-branch architecture to use both local and global features to learn templates in an unsupervised manner.
   - MaLP can be used as a plug-and-play discriminator module to fine-tune GMs to improve the quality of the generated images.
   - MaLP outperforms State-of-The-Art (SoTA) methods in manipulation localization and detection.

6. **Proactive scheme for image manipulation detection (Collaboration with Meta)**   **|May. 2021-Apr. 2022|**
   - A novel proactive scheme is proposed which encrypts a real image by adding a template from a learnable template set.
   - The added template is later recovered to perform image manipulation detection.
   - The template set is learned using defined constraints which incorporate properties including small magnitude, more high-frequency content, orthogonality, and classification ability.
   - Near-perfect average precision is obtained for unseen Generative Models (GMs) compared to prior works.
   - The proposed framework is more generalizable to different GMs, showing an improvement of 10% average precision averaged across 12 GMs compared to prior works.

7. **Reverse engineering of hyperparameters of GenAI models (Collaboration with Meta)**   **|Jul. 2020-Apr. 2022|**
   - A novel problem of Model Parsing is defined to develop a framework for predicting the network architecture and loss functions given a generated image.
   - We estimate the mean and deviation for each GM using two different parsers: cluster parser and instance parser which are then combined as the final predictions.
   - A network architecture super-set with 15 features and a loss function type set with 10 features were selected for every GM.
   - 1000 images each for 116 generative models were collected to create a new dataset.
   - The method generalizes well to tasks of deepfake detection on the Celeb-DF benchmark and image attribution.

8. **Deepfake video detection model**   **|Feb. 2020-Apr. 2020|**
   - Implemented a ML model consisting of CNN followed by a RNN for deepfake detection.
   - The CNN-RNN model would be able to detect whether a video is fake or real.

TECHNICAL PROFICIENCY

Tools, Simulation, and Software Platforms
- TensorFlow, PyTorch, Pytorch Lightning, Keras, NumPy, Scikit-learn, Jupyter, OpenCV, CUDA, MATLAB and Simulink, GCS, Amazon Web Services (AWS), LabVIEW, Linux, CST Microwave studio, Cadence virtuoso, Microsoft-Visual Studio, Excel, Word and PowerPoint, OrCAD PSpice, Labcentre Proteus, Eagle- PCB Design and Schematic Software, Xilinx Vivado Suite and SDK, FluidSim

Languages / Scripts
- Python, MATLAB, R, SQL, Perl, C, C++, Cascading Style Sheets (CSS), JavaScript, HTML, Verilog, VHDL, x86 Assembly Language, Arduino Programming

---

PROFESSIONAL TALKS & TUTORIALS

Tutorials Organized
Organized a tutorial in CVPR 2023 which aims to provide a comprehensive understanding of the emerging reverse engineering of deceptions (RED) techniques in adversarial machine learning (ML) for trustworthy computer vision (CV).

Talks Given
1. In-person talk given at Scale-AI headquarters in San Francisco. The talk was focused on our work on reverse engineering of generative models.
2. Virtual talk given at Scale-AI. The talk was focused on our work on proactive image manipulation detection.

RELEVANT COURSES PURSUED

- Computer Vision: Detectors and Descriptors, Optical Flow, Image segmentation, Tracking and object detection, Epipolar geometry.
- Machine learning: Regression, Classification, Dimensionality reduction, Sparse learning, Ensemble methods, multi-task learning
- Pattern recognition and analysis: Bayesian classification, Estimating gaussian MLE parameters, non-parametric density estimation.
- Deep Learning: Deep Neural Networks, Convolution Neural Networks, Recurrent Neural Networks, Sequence Models.
- Deep Learning specialization- deepleraning.ai by Andrew Ng (Coursera).

HOBBIES AND EXTRA-CURRICULAR ACTIVITIES

- I like going for long drives.
- When having small breaks from work, I like solving jigsaw puzzles or reading a book.
- Football, badminton, and table tennis are some of the outdoor sports I like.