PURDUE INNOVATES | Office of Technology Commercialization

Privacy-Preserving Method and System for Generative AI Image Processing

Oracle-plus-generator pipeline masks and restores sensitive regions so generative edits preserve privacy without losing fidelity.

Researchers at Purdue University developed a privacy-preserving image processing framework for generative AI applications. The system uses a two-component architecture: a privacy-aware oracle model to detect and mask sensitive image regions (e.g., faces or identifiers) and a server-based generative model (e.g., Stable Diffusion) to perform image refinement without accessing the protected areas. The oracle then reintegrates the original masked content into the enhanced image using advanced blending algorithms. This method ensures sensitive data remains secure while preserving image quality and enabling high-performance AI editing. This technology could enable use of generative AI in privacy-sensitive contexts such as medical imaging, security applications

Technology Validation:

The technology was validated through internal testing using a pipeline that combined a convolutional neural network-based oracle model with a Stable Diffusion-based generative model. Sample images containing privacy-sensitive regions were processed to confirm accurate detection, masking, and reintegration of these regions without compromising image quality. The results demonstrated successful privacy preservation and seamless visual integration across various image editing scenarios.

Advantages:

-Privacy preservation

-High Fidelity Image Quality

-Easy Integration with existing AI platform

Applications:

-Medical Imaging and Diagnostics

Technology ID

2025-AGGA-71122

Category

Artificial Intelligence & Machine Learning/AI Model Optimization & Acceleration Tools

Artificial Intelligence & Machine Learning/Multimodal & Generative Visual AI

Authors

Vaneet Aggarwal

Vineet Punyamoorty

Dipesh Hemchandra Tamboli

Further information

Parag Vasekar

psvasekar@prf.org

View online

-AI headshot and portrait enhancement services

-Surveillance footage and analysis

TRL: 4

Intellectual Property:

Utility-Gov. Funding, N/A, United States

Provisional-Patent, 2025-05-03, United States

Keywords: Computer Technology, diffusion models, generative AI, privacy preservation, stable diffusion