CS486C – Senior Capstone Design in Computer Science

Project Description

Project Title: ArtGuard: Integrated AI Protection Platform for Digital Artists

Sponsor Information:

Andres Sepulveda Morales, Founder / Creative Technologist
Red Mage Creative Technologies
andres@redmage.cc | https://redmage.cc

BIO: Andres Sepulveda Morales is a recovering corporate software engineer after navigating 3 layoffs in 2 years with over 8+ YOE and dedicated to community through technology. He graduated from Northern Arizona University in 2021 with a B.S. in Computer Science, and minors in Mathematics and Aerospace Studies.

Recognized 2x as one of Contra's Best Software Consultants to Hire in 2025, he found his terra firma for the time being through human-focused technology implementation and strategy for primarily non-profits, creative professionals, and what he calls "impact makers and barrier breakers" via his company, Red Mage. Andres founded the Fort Collins AI for Everyone chapter and sits on the Board of Directors for Rocky Mountain AI, a 501(c)(3) pending Colorado nonprofit organization dedicated to educating the community around AI with 3000+ members in Boulder and 12 distinctive subgroups covering industry specific topics and geographic areas in Fort Collins, Denver, and Boulder.

Project Overview:

Why This Matters

The digital art world is experiencing an unprecedented disruption. With AI models like Midjourney, DALL-E, and Stable Diffusion capable of generating artwork in any style within seconds, artists are witnessing their life's work being replicated without consent or compensation. Recent studies indicate that major AI training datasets contain millions of copyrighted artworks scraped from the internet, effectively allowing AI systems to mimic artistic styles that took years to develop. This represents both an existential threat to artistic livelihoods and a fundamental challenge to intellectual property rights in the digital age.

The Current Landscape and Problem

While researchers have developed promising defensive tools like Nightshade (which introduces "concept poisoning" to disrupt AI training) and Glaze (which applies adversarial perturbations to protect artistic style), these remain largely inaccessible to working artists. Current solutions require technical expertise in machine learning, command-line interfaces, and complex parameter tuning that puts them out of reach for most creative professionals.

The consequences of this accessibility gap are significant:

- Artists continue to have their work exploited without recourse
- Only technically sophisticated artists can protect their digital portfolios
- Existing tools require separate workflows, making protection cumbersome and time-consuming
- There's no integrated solution for managing protection across large portfolios or multiple platforms

Solution Overview

I envision ArtGuard (working title, subject to change) as an integrated application that democratizes AI adversarial protection through an intuitive, accessible workflow. The solution would bridge the gap between sophisticated research tools and practical artist needs, making protection as approachable as applying a filter in professional creative software. The specific platform, architecture, and integration approach present compelling design challenges that the team will explore and determine based on user needs, technical feasibility, and performance requirements.

From a personal perspective, this application would also be a love letter to the countless artists and creatives who are struggling in this new age of AI adoption.

Key Features

Minimum Viable Product:

- Intuitive user interface designed for artists without technical ML background
- Integration with existing adversarial protection algorithms (specific tools to be evaluated)
- Single-image processing with configurable protection settings
- Visual comparison system showing protection effects and quality impact
- Standard export formats with metadata preservation
- Progress tracking and error handling for reliable user experience

A Useful System:

- Batch processing capabilities for portfolio-scale protection
- Multiple protection strategy options (layered or selective approaches)
- Performance optimization to minimize processing time and visual artifacts

- User preference system with processing history
- Integration readiness for common art sharing platforms
- Cross-platform compatibility considerations

Stretch Goals:

- AI-driven protection recommendations based on image analysis and use case
- Community platform for sharing protection strategies and effectiveness insights
- Advanced analytics dashboard for tracking protection performance
- Mobile companion application for convenient protection workflows
- Extensible plugin architecture for future integration with digital art software
- Cloud processing infrastructure for computationally intensive operations

Impact of Successful Product

ArtGuard would serve the global community of digital artists, from independent freelancers to studio professionals, providing them with accessible tools to protect their creative work in an AI-dominated landscape. By lowering the technical barriers to adversarial protection, the platform would enable artists to maintain control over their intellectual property while continuing to share their work online. The impact extends beyond individual protection—widespread adoption could fundamentally shift the dynamics between AI companies and the creative community, establishing new norms for consent and compensation in AI training data.

Knowledge, Skills, and Expertise Required:

- **User Interface/User Experience Design:** Creating intuitive interfaces for complex technical processes
- **Python Programming:** Integration with existing ML libraries and frameworks
- **Machine Learning Integration:** Working with PyTorch/TensorFlow models and adversarial techniques
- **Software Engineering Best Practices:** Version control, testing, documentation, and deployment
- **Desktop Application Development:** Cross-platform GUI development (likely Electron or Qt)
- **Image Processing:** Optimization algorithms and format handling
- **Performance Optimization:** Managing computationally intensive operations
- **Cloud Computing:** Optional cloud processing infrastructure

Equipment Requirements:

- Development workstations with adequate GPU capabilities for ML model testing

- There should be no specialized equipment required beyond standard development platforms
- All software tools and libraries needed are freely available online
- Optional: Cloud computing credits for testing cloud processing features (can be provided through educational programs, sponsored by Red Mage within reason)

Software and Other Deliverables:

- **Complete Desktop Application:** Fully functional ArtGuard application with installer packages for major operating systems
- **Comprehensive Technical Documentation:** Including architecture decisions, API documentation, and user guides suitable for both end-users and future developers
- **Strong As-Built Report:** Detailed documentation of design and implementation decisions, performance analysis, and recommendations for future development
- **Professional Codebase:** Complete, well-documented source code delivered via GitHub repository with proper version control history
- **User Testing Results:** Documentation of user studies and feedback from actual digital artists
- **Deployment Package:** Installation guides and any necessary deployment scripts or configuration files