CSC490 Assignment 1: Project Landscape

Sohee Goo / 1008065479 Akshaya Deepak Ramachandran / 1008806810
Maryam Taj / 1008990362 Kashish Mittal / 1009115315

1 Part One: Interest Statements

Our team is interested in art authentication, specifically detecting forged artworks. Presently, contemporary solutions are often expensive and lack interpretability and transparency. Our team seeks to address this challenge by developing a machine learning model that helps users efficiently discriminate between original artworks and imitations, in addition to providing clear justification behind its predictions.

- Akshaya: I'm excited to contribute to this project because I think that art is such an interesting domain, and I'm also interested in the process of deploying and turning our model into a product, especially using cloud tools I haven't had the chance to work with before.
- Kashish: I am excited about how art can be integrated with CS. From a technical POV, I am interested in the whole process of making this ML application deployable, as most of the models I've built so far have never left a Google Colab notebook.
- Maryam: I am excited to learn about and implement best practices for ML engineering, including data engineering, thorough testing, prompting, and evaluation, so we can build something robust and scalable.
- Sohee: I'm interested in diving into the ops side of machine learning and gaining hands-on skills on building infrastructure on the cloud. Additionally, I'm excited to apply transfer learning and fine-tuning to develop models tailored specifically for the art domain.

2 Part Two: Landscape Analysis

Relevant Item	Description	Commentary
Art Authentication with Vision Transformers	Compares Vision Transformers (ViTs) and CNNs on the art authentication task.	Using a standard contrast set containing imitations and proxies (works by painters with styles closely related to van Gogh), we find that EfficientNet achieves the best performance overall. With a contrast set that only consists of imitations, we find the Swin Transformer to be superior to EfficientNet by achieving an authentication accuracy of over 85%.
Art Forgery Detection using Kolmogorov Arnold and Convolutional Neural Networks	Flipping the approach of traditional methods, this paper seeks to tackle art authentication from the perspective of the forger, detecting forgeries made by a known art forger.	Preprocessing includes splitting paintings into center-cropped patches of 256x256 pixels, using a Gaussian blur, and an entropy measure to quantify the amount of information contained in each patch and filter out uninformative patches.
So-Fake: Benchmarking and Explaining Social Media Image Forgery Detection	A large-scale social media dataset and benchmark for AI-generated image forgery detection, comprising over 2 million synthetic images generated by diverse state-of-the-art models, alongside a novel and large-scale (100K) out-of-domain benchmark (So-Fake-OOD) featuring synthetic imagery from commercial models explicitly excluded from the training distribution. Also includes an explainable interface.	Advances forgery detection by combining detection, localization, and interpretable explanations within a unified, reinforcement-learning framework. It addresses dataset diversity and out-of-domain generalization for social media imagery, but its focus remains on digital content. It does not tackle physical artworks or artist-specific stylistic signatures, highlighting a gap for applications in fine-art authentication.

Synthetic images aid the recognition of human-made art forgeries	Synthetic art generated with AI models is used to augment training data, improving the detection of human-made art forgeries.	This paper shows that including AI-generated synthetic forgeries in training sets helps models learn stylistic boundaries more effectively, addressing the scarcity of labeled forgery examples.
On art authentication and the Rijksmuseum challenge: A residual neural network approach	Authenticate artists using ResNet 101 on Rijksmuseum dataset	Provides interesting future directions; the investigation of adversarial attacks on art authentication will be useful to understand; investigate the use of recommender systems with art authentication.
PhotoHolmes	PhotoHolmes is an open-source python library designed to easily run and benchmark forgery detection methods on digital images. The library includes an implementation of popular and SOTA methods, datasets and evaluation metrics, all of which easily integrate with their custom methods, datasets and metrics.	Focuses on digital image manipulation rather than physical-medium forgeries (e.g., brushstroke depth, material analysis).
Patch-Based Oil Painting Forgery Detection Based on Brushstroke Analysis Using Generative Adversarial Networks and Depth Visualization	Generative Adversarial Networks (GANs) trained on artists' unique brushstroke signature to distinguish original artworks from counterfeits.	This paper leverages 3D surface information of brushstrokes and trains GANs on small image patches to capture fine-grained patterns. The model can detect subtle differences between originals and forgeries, achieving up to 82% accuracy, highlighting the promise of combining texture analysis with adversarial learning for automated art authentication.
Art Recognition AG	A Swiss B2B leader using hybrid CNN + SWIN architectures for high-end art authentication.	Their reports are static and binary. They offer no pedagogical value or explanation of why the model made its decision. High fees gatekeep their services to the elite level of the art market.
Hephaestus Analytical	Authentication service that combines high-resolution AI brushstroke analysis (Pictology) with traditional connoisseurship, chemical material testing, and provenance research to offer a conclusive.	Positioned as a luxury service for banks, insurers, and elite galleries. Expensive and slow. Middle market gap. Pictures need to be taken on extremely expensive Hasselblad cameras. Claims that their model can ”learn” an artist's signature from very few images. Shows that using traditional techniques might still be needed to provide stronger guarantees.
Norval AI	Canadian company which uses robotic arms to physically replicate an artist's style (specifically Norval Morrisseau) to generate a training set of ”perfect” machine-made fakes.	Addresses the data scarcity problem by creating its own high-quality forgery data to test and train their detection model, Norval AI. Since the artist has to provide a live drawing session to help the robot learn initially, this tool is less effective for replicating deceased artists' work.

3 Part Three: Project Outline

3.1 Problem Statement

Today, art forgery represents a significant and persistent problem in the global art market. According to Yan Walter, Executive Director of the Fine Arts Expert Institute, the frequently cited estimate that nearly half the artworks in circulation are forged, may in fact be an understatement [1]. This is understandable, as verifying the authenticity of an artwork is costly, with professional authentication services, such as those at the Institute, charging up to $19,000 per piece. As a result, the art market remains highly uncertain, creating financial and information barriers for collectors, galleries, and institutions seeking to assess authenticity with confidence.

While recent advances in deep learning have led to automated approaches for art forgery, existing methods largely provide only a binary decision or a single confidence score indicating whether an artwork is authentic or forged [2]. Such outputs offer limited insight into why a work may be classified as a forgery, making it difficult for users to interpret or trust these assessments. This lack of transparency and interpretability poses a significant challenge in applying machine learning systems to domains such as art authentication.

3.2 Proposed Solution

We propose a full-stack ML application that uses vision transformer to authenticate artworks via upload, and an LLM-RAG system that provides written supporting evidence justifying an artwork's authenticity or inauthenticity.

3.3 High-level technical approach

- **Data/ETL Pipeline:** We will extract high-resolution ”authentic” ground-truth images, imitations and/or forgeries, and technical forensic reports. We will transform the data by applying random rotations and gaussian blurs to simulate a variety of photo upload conditions. We will load the data providing context for LLMs to Amazon Bedrock's Knowledge Base and the remaining visual data in AWS S3.
- **Vision Model:** We will use a vision transformer, SWIN, to extract feature embeddings for each patch in the painting, producing a tensor of shape (P, D), where P is the number of patches and D is the embedding dimension. We aggregate patch embeddings (i.e., mean pooling / attention pooling) to obtain a painting-level representation of shape (D,). We will pass the representation through a classification head (i.e., multi-layer perceptron) that outputs logits. We will use the sigmoid function to transform the logit to a probability representing p(authentic). We train the model using binary cross-entropy loss.
- **LLM + RAG:** We will use a RAG system to retrieve artist-specific and artwork-related information, which will be passed to the LLM alongside the model's feature embedding and logits. Using this combined output, the LLM will generate a clear explanation that contextualizes the prediction, highlighting why an artwork is likely authentic or forged.
- **App**: We will use FastAPI to serve responses to a simple interface (React) where users can upload their images, see forgery scores, and receive context-specific LLM generated explanations.

3.4 Milestones

- February 13: Consolidate our datasets, and implement ETL data pipeline (including our cloud environment setup).
- February 27: Fine tune baseline vision transformer, Swin, and evaluate and document performance using metrics such as accuracy, precision, recall and F1.
- March 13: Construct a knowledge base for RAG. We will integrate vision transformer, and LLM API with RAG into a full-stack application.
- March 27: Break our project with load testing, and document how our project breaks in different parts with corresponding test cases.

3.5 Unknowns to investigate

- How might we generate synthetic data to augment the dataset with true negatives?
- What kind of pooling should we apply after we extract feature embeddings from the Swin vision transformer?
- What specific information do we store in the knowledge base for RAG? Do we need to have cron jobs that pull data periodically?
- What evaluation metrics should we include or exclude (e.g. sensitivity, specificity, AUC, etc.) for our vision model?
- What evaluation metrics should we use to assess the LLM's outputs? Prompt engineering techniques so LLM outputs are geared towards art experts?

4 Part Four: Project Press Release

Artisync Unveils First Affordable, ”Explainable” Detection Tool to Combat Art Forgery

TORONTO, ON — January 20, 2026 — Artisync today announced the launch of ArtGuard AI, an authentication platform designed to protect collectors, historians, and galleries from increasingly sophisticated forgeries. By combining cutting-edge computer vision with a specialized Digital Auditor assistant, ArtGuard AI makes professional-grade forgery analysis accessible to the broader art market for the first time.

Traditional forensic services often demand five-figure fees and weeks of lab time, leaving independent collectors and small galleries vulnerable to high-quality forgeries. ArtGuard AI democratizes this process, providing a high-performance digital screening tool that offers instant analysis at a fraction of the cost of traditional methods.

”High-end art authentication has long been a luxury that many simply can’t afford, creating a trust gap in the market,” said Akshaya Deepak, CTO of ArtGuard AI. ”We built ArtGuard to give the power back to the people who love and trade art. Our system doesn’t just give you a ’Genuine’ or ’Forgery’ verdict; it acts as a digital advisor that actually talks to you and explains the specific stylistic and structural inconsistencies it finds.”

ArtGuard AI utilizes a powerful hybrid of vision models, to analyze images for microscopic discrepancies in texture and style. It also cross-references a comprehensive database of art history to create a Forensic Audit Report, providing a Fraud Percentage Score and a detailed breakdown of where the work deviates from known authentic patterns. Furthermore, ArtGuard AI’s training regimen incorporated a meticulously curated dataset encompassing diverse art periods, styles, and forgery types, crucially including a significant proportion of AI-generated forgeries, ensuring robust performance.

“The level of detail is startling,” says Sarah Jenkins, an independent gallery owner and early beta tester. “Before ArtGuard, I had to wait weeks for a $10,000 expert consultation. Now, ArtGuard AI has completely changed my workflow. It acts like a second set of expert eyes on my team, screening artworks in real time. ” ArtGuard AI is available starting today, offering a tiered subscription model designed to fit the budgets of individual collectors and mid-sized galleries alike.

About Artisync
Artisync is an AI research lab dedicated to creating transparent, high-performance tools for the creative community. By leveraging scalable infrastructure and explainable machine learning, they aim to foster a more honest and accessible global art market.

5 Appendix

5.1 Iterations

Iteration 1:

- Too much focus on architecture (ex: SWIN, RAG enhanced LLM). Non-technical audiences care about accuracy but don't need to understand technical jargon to trust the product.
- Emphasizes technical metrics like scalability, robustness, cost-effectiveness. The voice of the statement is too much of an engineer/technical person.
- Need more focus on the paint points and impact, making the users feel confident that this would improve their work, rather than reliability of the tech.

Iteration 2:

- Language is heavily weighted toward business metrics (ex: B2B SaaS, gross margins, ROI, liquidity). Appeals to stakeholders who care about profitability of the company rather than art.
- Focuses on market positioning and competitive advantage of company, by providing financial scope more than emphasizing features (ex: 6B forgery market, mid-market segment)
- Outlines how the project makes money, which is unnecessary for a press release, where focus should be on how the product helps customers.
- Points about scalability are less relevant for smaller, independent gallery owners.

Final Iteration:

- Strategic positioning of the middle market gap, which places ArtGuard as an affordable middle option that didn't exist before.
- Highlights lack of accessibility and transparency in existing products.
- Uses convincing language without technical jargon (ex: vision model instead of SWIN), to be accessible to the target audience who work in the art domain. Words like 'cutting edge', emotionally convince readers of novel technology.
- Focus on user gaps and how their workflow will be improved. The quote mentions impact to the target user's life. Highlights price and explainability benefits, which is our competitive advantage. Assumes the audience already understands forgery is a problem, so focus is less on market sizing and more on what the tool will deliver.

5.2 PR Statement Iteration 1

Artisync Unveils ArtGuard AI: A ML Solution for Art Forgery Detection

TORONTO, ON — January 20, 2026 — Artisync today announced the launch of ArtGuard AI, an enterprise-grade machine learning pipeline designed to detect sophisticated human forgeries with forensic precision. By combining cutting-edge computer vision with a specialized Digital Auditor assistant, ArtGuard AI delivers comprehensive Static Forensic Audit Reports that provide a quantitative Fraud Probability Index at a fraction of the cost of manual laboratory analysis. This solution addresses the growing need for robust, cost-effective, and transparent authentication in the art market.

"Our objective was to develop an end-to-end ML pipeline that not only outperforms existing unimodal visual systems but also delivers critical interpretability," said Akshaya Deepak, CTO of ArtGuard AI. "We built ArtGuard to give the power back to the people who love and trade art. We are providing the technical maturity usually reserved for big-tech platforms to the world of art forensics"

ArtGuard AI's detection engine utilizes a sophisticated ensemble of Swin Transformers (SWIN). This dual-architecture approach allows the system to capture both global stylistic patterns and microscopic texture anomalies. To ensure the results are interpretable for professional use, the system utilizes a RAG-enhanced Large Language Model to generate data-backed reports. ArtGuard AI's training regimen incorporated a meticulously curated dataset encompassing diverse art periods, styles, and forgery types, crucially including a significant proportion of AI-generated forgeries, ensuring robust generalization.

"The engineering behind ArtGuard AI is what sets it apart," says Sarah Jenkins, an independent gallery owner. "In my workflow, I need reliability and speed. ArtGuard AI functions like an additional team member, providing a forensic-level audit report that gives me a clear fraud percentage. It has turned a $10,000, month-long process into a scalable, near-instant screening protocol."

ArtGuard AI is available starting today, offering a tiered subscription model designed to fit the budgets of individual collectors and mid-sized galleries alike.

5.3 PR Statement Iteration 2

Artisync Targets $6B Art Forgery Market with Scalable, High-Margin Detection Infrastructure

TORONTO, ON — January 20, 2026 — Artisync, a pioneer in forensic-grade computer vision, today announced the launch of ArtGuard AI, a B2B SaaS platform poised to capture a significant share of the $6 billion annual global art forgery market. As the Art Market moves toward a $940B valuation by 2033, the demand for transparent, instant, and affordable authentication is the industry's most critical infrastructure need.

By replacing cost-prohibitive manual appraisals with a scalable, high-throughput machine learning pipeline, ArtGuard AI offers a disruptive solution for galleries, auction houses, and insurers seeking to mitigate risk and unlock liquidity in the mid-market art segment. With traditional forensic fees often exceeding $10,000 per piece and requiring weeks of lab time, millions of mid-market assets remain unverified and illiquid.

ArtGuard AI's automated Static Forensic Audit Reports provide verification for a fraction of the cost, creating a massive ROI for high-volume users. Utilizing Retrieval-Augmented Generation (RAG), our system generates reports that cite specific historical datasets, providing a defensible paper trail for insurance and resale purposes. Our cloud-native architecture allows for a pay-per-report or subscription model with gross margins exceeding 70%, far outperforming traditional lab-based forensic services.

"Our proprietary multi-modal engine analyzes both micro-textures and global styles," said Sohee Goo, Lead Engineer. "Our partners can process entire estates or seasonal auction catalogs in hours rather than months, transforming a traditional cost center into a high-speed value driver."

"ArtGuard AI has completely de-risked my acquisition pipeline," says Julian Reed, Managing Director of an independent art fund. "In a market where trust is expensive, ArtGuard provides a scalable peer-review that functions as a high-performance team member. It's the first time we've seen big-tech technical maturity applied to art asset management."

5.4 Sources

[1] Larson, N. (2014). *Fine arts experts institute: Lab sleuths in Geneva help art world uncover fakes.* ArtDaily.
https://artdaily.com/index.asp?int_sec=11&int_new=73562

[2] Zanardelli, M., Guerrini, F., Leonardi, R., & Adami, N. (2023). Image forgery detection: A survey of recent deep-learning approaches. *Multimedia Tools and Applications, 82*, 17521–17566.
https://doi.org/10.1007/s11042-022-13797-w

[3] Azimi, E., Ashtari, A., & Ahn, J. (2025). Patch-based oil painting forgery detection based on brushstroke analysis using generative adversarial networks and depth visualization. *Applied Sciences, 15*(1), 75.
https://doi.org/10.3390/app15010075

[4] Ostmeyer, J., Schaerf, L., Buividovich, P., Charles, T., Postma, E., & Popovici, C. (2023). Synthetic images aid the recognition of human-made art forgeries. *arXiv.*
https://doi.org/10.48550/arXiv.2312.14998

[5] Boccuzzo, S., Meyer, D. D., & Schaerf, L. (2024). Art forgery detection using Kolmogorov Arnold and convolutional neural networks. *arXiv.*
https://doi.org/10.48550/arXiv.2410.04866

[6] Dobbs, T., & Ras, Z. (2022). On art authentication and the Rijksmuseum challenge: A residual neural network approach. *Expert Systems with Applications, 200*, 116933.
https://doi.org/10.1016/j.eswa.2022.116933

[7] Schaerf, L., Popovici, C., & Postma, E. (2023). Art authentication with Vision Transformers. *arXiv.*
https://doi.org/10.48550/arXiv.2307.03039