

Ghost in the Transformer: Detecting Model Reuse with Invariant Spectral Signatures

Suqing Wang^{1*}, Ziyang Ma^{2*}, Li Xinyi², Zuchao Li^{1†}

¹School of Artificial Intelligence, Wuhan University

²School of Computer Science, Wuhan University

{wangsuqing, maziyang, xyli-lucia, zcli-charlie}@whu.edu.cn

Abstract

Large Language Models (LLMs) are widely adopted, but their high training cost leads many developers to fine-tune existing open-source models. While most adhere to open-source licenses, some falsely claim original training despite clear derivation from public models, raising pressing concerns about intellectual property protection and the need to verify model provenance. In this paper, we propose Ghost-Spec, a lightweight yet effective method for verifying LLM lineage without access to training data or modification of model behavior. Our approach constructs compact and robust fingerprints by applying singular value decomposition (SVD) to invariant products of internal attention weight matrices. Unlike watermarking or output-based methods, Ghost-Spec is fully data-free, non-invasive, and computationally efficient. Extensive experiments show it is robust to fine-tuning, pruning, expansion, and adversarial transformations, reliably tracing lineage with minimal overhead. By offering a practical solution for model verification, our method contributes to intellectual property protection and fosters a transparent, trustworthy LLM ecosystem.

Code — <https://github.com/DX0369/GhostSpec>

Extended version — <http://arxiv.org/abs/2511.06390>

1 Introduction

LLMs have quickly become essential for various applications in research and industry (Achiam et al. 2023; Yang et al. 2025a; Wang et al. 2025; Zhang et al. 2025; Poon et al. 2025). Due to the high cost of training LLMs from scratch (Workshop et al. 2022), many developers modify open-source LLMs via fine-tuning, continued pre-training, merging, and compression (Yang et al. 2024; Zhu et al. 2024; Tang et al. 2025; Yang et al. 2025b; Li et al. 2023; Hu et al. 2025). While most developers comply with open-source licenses, there have been instances of falsely claiming to have trained models “from scratch” when they are in fact repackaged or fine-tuned versions of public models (e.g., Llama3-V and MiniCPM-Llama3-V 2.5) (Yao et al. 2024). It is crucial to distinguish such intellectual property

violations, which often break attribution requirements, from legitimate, licensed fine-tuning. This raises concerns about plagiarism and intellectual property violations, emphasizing the need for tools to verify model lineage.

To address these concerns, researchers have proposed various model identification methods (Sun et al. 2023b), which can be broadly classified into black-box and white-box approaches. Black-box methods identify models without accessing their weights, using techniques like behavioral fingerprinting and watermarking. However, these approaches are often sensitive to randomness, adversarial changes, or require intrusive pipeline modifications. In contrast, white-box methods leverage internal parameters. While representation-based techniques analyze hidden states or gradients, they depend on data access and are computationally expensive. Direct weight comparisons are simpler but fragile under fine-tuning or pruning.

We propose GhostSpec, a simple, data-free, and robust white-box method for verifying LLM lineage. GhostSpec is, by design, a white-box method targeting the open-weight model ecosystem where weights are accessible. Our key insight is that the spectral structure of weight matrices encodes intrinsic information about a model’s origin, remaining stable under various modifications. Specifically, we apply singular value decomposition (SVD) to internal matrix products within the attention mechanism, including the query-key and value-output weight products. From the resulting spectra, we select the most significant singular values based on effective rank to compute similarity. To handle architectural variations in depth, such as those resulting from layer pruning or expansion, we develop the Penalty-based Optimal Spectral Alignment (POSA) algorithm that finds the best layer-wise correspondence between models. This yields a quantitative similarity score robust to differences in depth and architectural variations. Unlike black-box or representation-based white-box methods, GhostSpec is data-independent, requires no model modification, and has minimal computational cost.

Our contributions are summarized as follows:

- We propose GhostSpec, a lightweight white-box method for verifying LLM lineage from model weights, requiring no training data or architectural changes, offering a practical solution for provenance verification and IP protection in open-source LLMs.

*These authors contributed equally.

†Corresponding author.

Copyright © 2026, Association for the Advancement of Artificial Intelligence (www.aaai.org). All rights reserved.

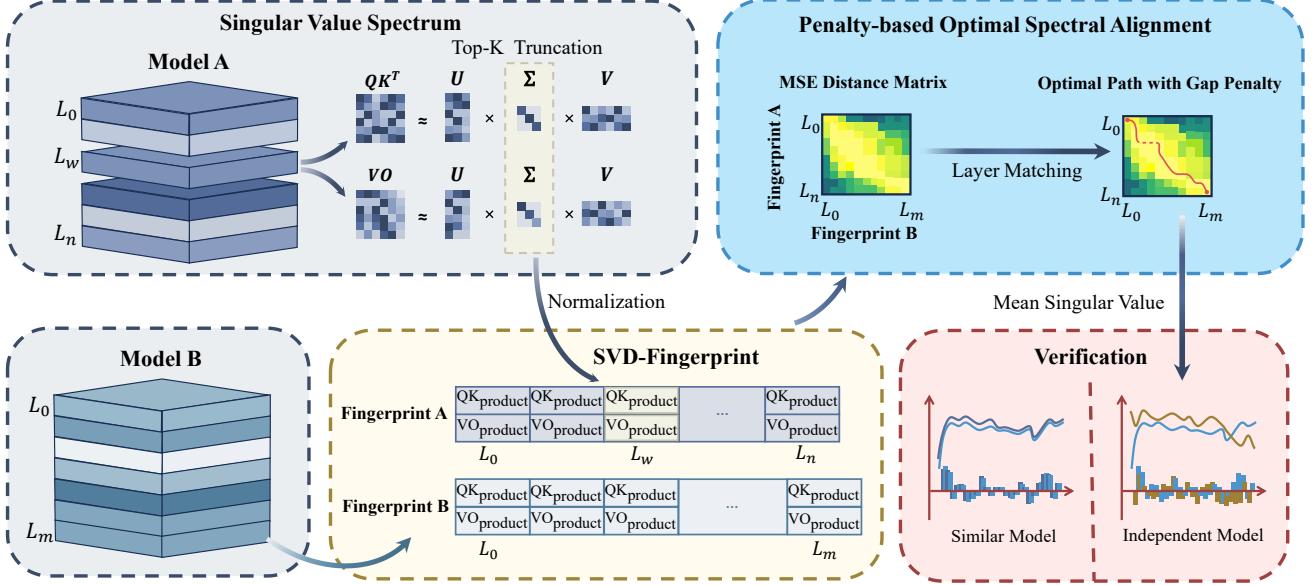


Figure 1: GhostSpec extracts singular value spectra from each layer’s attention products to form spectral fingerprints. A pairwise MSE distance matrix is computed, and a penalty-based alignment algorithm matches layers across models of different depths. The final similarity score distinguishes between related and independently trained models.

- We introduce spectral fingerprints based on invariant matrix products within the attention mechanism, robust to scaling and permutation transformations, and develop the POSA algorithm for comparing models with varying depths.
- We demonstrate through experiments that GhostSpec reliably distinguishes derivative models from independently trained ones, even under challenging modifications.

2 Related Work

Efforts to verify model lineage can be broadly classified into black-box and white-box approaches, depending on whether internal model access is required.

2.1 Black-Box Identification

Black-box methods operate without access to model weights and are suitable for closed-source, API-only models. They include behavioral fingerprinting and watermarking.

Behavioral Fingerprinting. These passive methods identify model signatures from natural outputs. Approaches analyze stylistic or statistical patterns in generated text, or use crafted prompts to probe responses (Pasquini, Kornaropoulos, and Ateniese 2024; McGovern et al. 2024; Sam, Finzi, and Kolter 2025). Some rely on output logits or top-k probabilities to define a unique model space (Yang and Wu 2024). However, such methods are sensitive to decoding randomness and vulnerable to adversarial paraphrasing.

Watermarking. Watermarking embeds a detectable signal in model outputs, either via instruction tuning (Xu et al. 2024) or token-level perturbation (Kirchenbauer et al. 2023; Nagatsuka, Morishita, and Sogawa 2025). These signals can be verified statistically, but require the model creator’s cooperation and can be invalidated by output editing or algorithm exposure.

2.2 White-Box Identification

White-box approaches leverage internal model weights or activations, typically by computing similarity between weights, intermediate representations, or gradients.

Representation-based Fingerprinting. These methods analyze hidden representations and generally require input data. Techniques such as CKA similarity or gradient statistics have been used to reveal shared training origins (Zhang et al. 2024; Wu, Zhao, and Wang 2025; Liang et al. 2025). While effective, these methods are computationally intensive, data-dependent, and may raise concerns regarding potential correlations with training data.

Weight-based Fingerprinting. This line of work focuses on static, data-free analysis of model weights. Prior methods include visualizing invariant structural features (Zeng et al. 2024) or analyzing layer-wise statistics (Yoon et al. 2025). Our proposed GhostSpec method falls into this category, capturing deeper structural information by leveraging the full singular value spectrum of invariant matrix products. The POSA algorithm is further introduced to robustly trace model ancestry under various transformations.

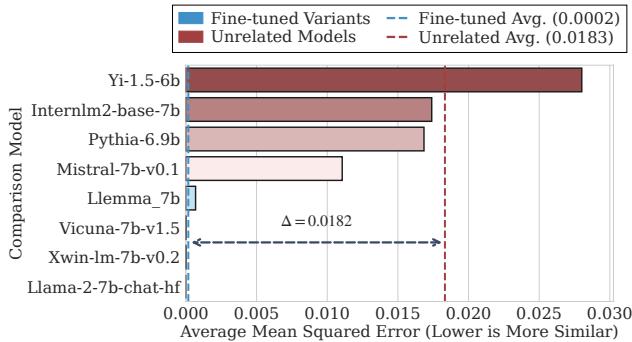


Figure 2: Average MSE of normalized singular values from Q/K/V/O projections. The spectral distance from Llama-2-7b to its fine-tuned variants (blue) is negligible, while the distance to unrelated models (red) is large, confirming the fingerprint’s robustness against fine-tuning.

3 Preliminaries

Staats, Thamm, and Rosenow (2024) use Random Matrix Theory (RMT) to analyze the singular value spectrum of pre-trained language models. Their analysis reveals deviations from the Marchenko–Pastur distribution, especially in large singular values. These outliers correspond to dominant directions in the weight space and are strongly associated with the model’s learned representations. Removing them significantly increases perplexity, showing they form a stable backbone of the model’s identity.

Fine-tuning, in contrast to training from scratch, refines rather than rebuilds the model’s internal structure. Staats, Thamm, and Rosenow (2024) demonstrates that fine-tuning primarily affects directions associated with small singular values. A key asymmetry is observed: pruning small singular values after fine-tuning leads to significantly greater performance degradation than pruning them before fine-tuning. This indicates that fine-tuning updates are concentrated in low-magnitude spectral components.

Together, these findings suggest spectral stability: large singular values, encoding foundational pre-trained knowledge, remain stable throughout adaptation and anchor the model’s global behavior. In contrast, fine-tuning introduces targeted, low-rank modifications reflected in small singular values. We hypothesize that the large singular value spectrum of attention matrices serves as a robust, fine-tuning-invariant fingerprint.

3.1 Experimental Design

To empirically test this hypothesis, we designed an experiment centered on Llama-2-7b-hf. We compared this primary model against two distinct groups:

- Fine-tuned Variants:** A group of known direct descendants of Llama-2-7b (Touvron et al. 2023), including Llama-2-7b-chat-hf, Vicuna-7b-v1.5, Llemma_7b (Azerbaiyev et al. 2023), and Xwin-LM-7B-V0.2 (Xwin-LM Team 2023).
- Unrelated Models:** A control group of architecturally distinct models, including Mistral-7B-v0.1 (Jiang et al.

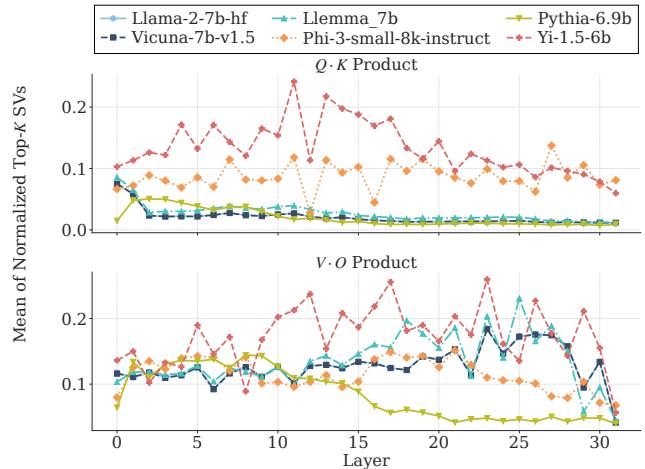


Figure 3: The layer-wise trend of the mean of normalized singular values for various models. Models with a shared lineage (e.g., Llama-2-7b-hf and its variants) exhibit highly correlated trends, while unrelated models show divergent patterns.

2023), Pythia-6.9b (Biderman et al. 2023), Yi-1.5-6B (Young et al. 2024), Internlm2-base-7b (Cai et al. 2024).

Our objective is to quantify the spectral distance between the base model and each model in these groups.

3.2 Quantifying Spectral Similarity

To quantify the similarity between the singular value spectra of two models A and B , we define a compact layer-wise distance metric.

For each projection type $p \in \{q, k, v, o\}$ and each layer $i \in \{1, \dots, L\}$, we extract the singular value vectors $\mathbf{s}_{p,A}^{(i)}$ and $\mathbf{s}_{p,B}^{(i)}$ from the corresponding weight matrices. We first truncate both vectors to their minimum effective rank $r_p^{(i)}$ and then apply min-max normalization to map them into $[0, 1]$. The spectral distance at layer i and projection p is then defined as the Mean Squared Error (MSE) between the normalized, truncated vectors:

$$d_p^{(i)}(A, B) = \frac{1}{r_p^{(i)}} \left\| \text{norm}(\text{trunc}(\mathbf{s}_{p,A}^{(i)})) - \text{norm}(\text{trunc}(\mathbf{s}_{p,B}^{(i)})) \right\|_2^2. \quad (1)$$

The overall spectral distance is computed by averaging over all layers and projection types:

$$D(A, B) = \frac{1}{4L} \sum_{p \in \{q, k, v, o\}} \sum_{i=1}^L d_p^{(i)}(A, B). \quad (2)$$

3.3 Empirical Validation

As shown in Figure 2, fine-tuned models have low spectral MSE with their base models, indicating similar structures.

Algorithm 1: Penalty-based Optimal Spectral Alignment

Input: Distance matrix $D \in \mathbb{R}^{N \times M}$ (assume $N \leq M$), gap penalty ρ .

Output: Average distance along the optimal path.

```

1: Initialize cost matrix  $C \in \mathbb{R}^{N \times M}$  and backtrack
   matrix  $B \in \mathbb{Z}^{N \times M}$ .
2: for  $j = 0$  to  $M - 1$  do
3:    $C[0, j] \leftarrow D[0, j]$  {Base case for the first layer.}
4: end for
5: for  $i = 1$  to  $N - 1$  do
6:   for  $j = i$  to  $M - 1$  do
7:      $k^* \leftarrow \arg \min_{i-1 \leq k < j} (C[i-1, k] + (j - k - 1)\rho)$ 
8:      $C[i, j] \leftarrow C[i-1, k^*] + (j - k^* - 1)\rho + D[i, j]$ 
9:      $B[i, j] \leftarrow k^*$ 
10:  end for
11: end for
12:  $j_{\text{end}} \leftarrow \arg \min_{N-1 \leq k < M} C[N-1, k]$ 
13: Reconstruct optimal path  $P$  by backtracking from
     $(N-1, j_{\text{end}})$  using  $B$ .
14: return  $\frac{1}{|P|} \sum_{(i,j) \in P} D[i, j]$  {Avg. MSE on path.}

```

In contrast, unrelated models show much higher distances, highlighting structural dissimilarity.

These results confirm that the singular value spectrum is a stable, intrinsic property, mostly preserved through fine-tuning, motivating the design of a robust fingerprinting framework for model lineage verification under transformations.

4 Methodology

In practice, model weights may undergo transformation attacks such as permutation or scaling, which preserve the model’s functionality while significantly altering the raw weight distribution (Zhang et al. 2024). Directly comparing the singular values of individual attention matrices W_q , W_k , W_v , and W_o is therefore highly vulnerable to such obfuscation techniques. To address this, we propose constructing an invariant fingerprint derived from composite matrix products, which are resistant to these transformation attacks. Additionally, we introduce two complementary similarity metrics, GhostSpec-mse and GhostSpec-corr, designed to capture both fine-grained variations and macroscopic structural properties. Together, these components form a robust spectral fingerprinting methodology, as shown in Figure 1.

4.1 The GhostSpec Fingerprint

To quantify and compare the structural properties of Transformer-based language models, we first define an invariant spectral fingerprint that is robust to permutation and scaling transformations. For a given model M with L layers, we focus on the attention-related weight matrices: $W_q^{(i)}$, $W_k^{(i)}$, $W_v^{(i)}$, and $W_o^{(i)}$ from each layer $i \in \{1, \dots, L\}$.

We define two invariant matrices per layer whose singular value spectra are resilient to functionality-preserving transformations like permutation or scaling:

$$M_{qk}^{(i)} = W_q^{(i)}(W_k^{(i)})^T \quad \text{and} \quad M_{vo}^{(i)} = W_v^{(i)}W_o^{(i)}. \quad (3)$$

These transformations alter the weight distribution without changing the model’s output by modifying the weights in pairs or scaling them uniformly. Since the relative relationships between the weights are preserved, the model’s core functionality and input-output behavior remain unchanged.

The fingerprint for each layer is composed of the two singular value vectors derived from these products. The layer fingerprint $S_M^{(i)}$ is defined as the tuple:

$$S_M^{(i)} = \left(\mathbf{s}_{qk,M}^{(i)}, \mathbf{s}_{vo,M}^{(i)} \right), \quad (4)$$

where $\mathbf{s}_{p,M}^{(i)} = \text{SVD}(M_{p,M}^{(i)})$ for $p \in \{qk, vo\}$. The complete model fingerprint \mathcal{F}_M is the sequence of these layer fingerprints across all layers.

4.2 Similarity Metrics

Given the GhostSpec fingerprints of two models, A (with N layers) and B (with M layers), we introduce two complementary metrics: GhostSpec-mse, which provides a fine-grained, layer-by-layer comparison to measure structural correspondence, and GhostSpec-corr, a lightweight metric that captures the overall trend of spectral properties across layers. Used together, these metrics offer a comprehensive and reliable assessment of model lineage.

Fine-grained Similarity: GhostSpec-mse. This metric performs a detailed, layer-by-layer comparison of the singular value vectors to populate an aggregate distance matrix $D_{\text{avg}} \in \mathbb{R}^{N \times M}$. Each entry $(D_{\text{avg}})_{ij}$ represents the average spectral distance between layer i of model A and layer j of model B, computed as the mean of MSE over the invariant components:

$$(D_{\text{avg}})_{ij} = \frac{1}{2} \sum_{p \in \{qk, vo\}} \frac{1}{r_{p,ij}} \left\| \hat{\mathbf{s}}_{p,A}^{(i)} - \hat{\mathbf{s}}_{p,B}^{(j)} \right\|_2^2 \quad (5)$$

where:

- p is the invariant product type (qk or vo).
- $r_{p,ij} = \min(\text{eff_rank}(\mathbf{s}_{p,A}^{(i)}), \text{eff_rank}(\mathbf{s}_{p,B}^{(j)}))$ is the minimum of the effective ranks of the two singular value vectors being compared.
- $\hat{\mathbf{s}}$ denotes a processed singular value vector. The processing involves first truncating the original vector \mathbf{s} to its top $r_{p,ij}$ values, and then applying min-max normalization to scale the result to the $[0, 1]$ range.

To handle models with different depths ($N \neq M$), we apply our POSA algorithm, as shown in Algorithm 1, to find the minimum-cost alignment path through D_{avg} . The raw similarity score, d_{path} , is the average MSE along this optimal path. Finally, we convert this distance into a normalized similarity score using an inverted Sigmoid transformation:

$$\text{Sim}_{\text{MSE}}(A, B) = 1 - \frac{1}{1 + e^{-k(d_{\text{path}} - \tau)}}, \quad (6)$$

Primary Model: Llama-2-7b							
Method	Data Dep.	Model Fine-tuning (\uparrow)		Adversarial Transforms (\uparrow)		Unstructured Pruning (\uparrow)	
		Vicuna-7b-v1.5	Llemma_7b	Llama-2-7b -scaled	Llama-2-7b -permuted	Pruned-50% -Retrained	Pruned-70% -Retrained
QueRE	Data-Aware	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000
Logits	Data-Aware	0.9767	0.8400	1.0000	1.0000	0.8567	0.8533
REEF	Data-Aware	0.9992	0.9979	1.0000	1.0000	0.9968	0.9948
PCS	Data-Free	0.9986	0.5052	0.5970	0.3863	0.9061	0.7829
GhostSpec-corr	Data-Free	0.9992	0.7595	1.0000	1.0000	0.8967	0.7045
GhostSpec-mse	Data-Free	0.9760	0.9532	0.9761	0.9761	0.9727	0.9653
Structured Pruning (\uparrow)		Merging & Expansion (\uparrow)			Unrelated Models (\downarrow)		
Method	Data Dep.	Sheared-Llama 1.3B	Sheared-Llama 2.7B	Llama2-7b-func -call-slerp	Camelidae-8x7B	Qwen2.5-7B	OPT-6.7b
QueRE	Data-Aware	1.0000	1.0000	0.0910	1.0000	0.3410	1.0000
Logits	Data-Aware	1.0000	1.0000	1.0000	0.9500	0.9967	0.2200
REEF	Data-Aware	0.9315	0.9487	0.9996	0.9991	0.2513	0.2692
PCS	Data-Free	0.0000	0.0000	0.9993	0.0204	0.0000	0.0000
GhostSpec-corr	Data-Free	0.9398	0.9414	0.9998	0.9999	0.2940	0.3423
GhostSpec-mse	Data-Free	0.8886	0.9045	0.9760	0.9761	0.0000	0.5025
Primary Model: Mistral-7B							
Method	Data Dep.	Fine-tuning (\uparrow)	Merging (\uparrow)	Expansion (\uparrow)	Pruning (\uparrow)	Unrelated Models (\downarrow)	
		OpenHermes-2.5 -Mistral-7B	Triunvirato-7b	Chunky-Lemon -Cookie-11B	OpenHermes-2.5 -Mistral-7B-pruned50	Qwen2.5-7B	Yi-1.5-6B
QueRE	Data-Aware	1.0000	1.0000	1.0000	1.0000	0.3410	0.0819
Logits	Data-Aware	0.9933	0.9967	1.0000	0.9867	0.9567	0.2067
REEF	Data-Aware	0.8949	0.8538	0.8495	0.8596	0.7473	0.8301
PCS	Data-Free	0.9999	0.9997	0.8987	0.9979	0.0000	0.0000
GhostSpec-corr	Data-Free	0.9999	0.9997	0.9981	0.9896	0.2708	0.4304
GhostSpec-mse	Data-Free	0.9760	0.9759	0.9758	0.9753	0.0083	0.0581

Table 1: Comprehensive comparison of fingerprinting methods against various derivative and unrelated models, with **Llama-2-7b** and **Mistral-7B** as primary models. The table evaluates robustness to fine-tuning, architectural dissimilarity, compression, merging, expansion, and adversarial transformations. Similarity scores are color-coded based on method-specific thresholds: a blue cell indicates a score above the threshold (positive classification), while a red cell indicates a score below it (negative classification).

where τ is an empirical discrimination threshold and k is a steepness factor. A score approaching 1.0 indicates high similarity.

Lightweight Similarity: GhostSpec-corr. As illustrated in Figure 3, models with shared lineage exhibit highly correlated spectral trends, while unrelated models show divergent patterns. Based on this observation, we propose the GhostSpec-corr metric, which quantifies model similarity by capturing the overall trend of spectral properties.

First, we generate the trend sequences. For each layer i and component p , we compute a scalar value, $\mu_{p,M}^{(i)}$, defined as the mean of the top- K normalized singular values. Here, K is dynamically determined based on the effective rank of each singular value spectrum, consistent with the truncation method used in GhostSpec-mse. This process produces two trend sequences for each model: $\mu_{qk,M}$ and $\mu_{vo,M}$.

Second, we align the sequences. Since these sequences may differ in length, direct comparison is not feasible. To address this, we apply a dynamic sequence alignment algorithm (similar to the POSA algorithm introduced previously) to match the sequence lengths. This step generates new sequences of equal length ($\mu'_{qk,A}$, $\mu'_{qk,B}$, etc.).

Finally, we compute the similarity. We concatenate the aligned sequences for each model and calculate the final similarity score using the distance correlation coefficient:

$$\text{Sim}_{\text{Corr}}(A, B) = \text{dCor}([\mu'_{qk,A}; \mu'_{vo,A}], [\mu'_{qk,B}; \mu'_{vo,B}]). \quad (7)$$

This score quantifies the correlation of the models' high-level spectral evolution, providing a computationally efficient indicator of shared lineage.

5 Experiments

To evaluate the effectiveness and robustness of our proposed GhostSpec, we conduct a comprehensive suite of experiments designed to emulate real-world scenarios of model reuse, modification, and transformation.

5.1 Experimental Setup

Dataset Construction. We constructed a comprehensive dataset consisting of 55 model pairs, using Llama-2-7b and Mistral-7B as the primary base models. This dataset covers a wide range of transformations, including fine-tuning, com-

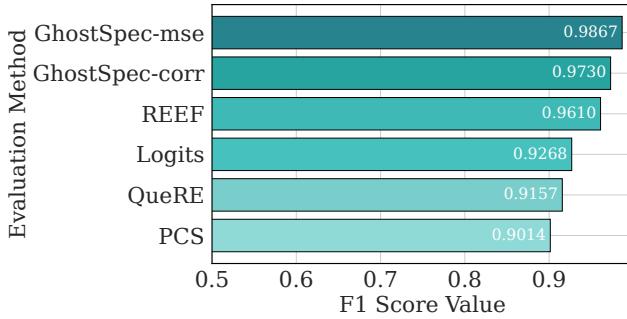


Figure 4: Maximum F1 scores for each method on our dataset. Both GhostSpec variants clearly outperform all baseline methods in accurately distinguishing related from unrelated models.

pression, merging, and expansion, with ground-truth labels indicating whether each pair is related or unrelated.

- **Fine-Tuning.** Fine-tuning is a common source of model derivation. We evaluate similarity between Llama-2-7B and several of its fine-tuned variants: Llama-2-7B-Chat-HF, Vicuna-7B-v1.5 and Llemma-7B, etc. Mistral-7B and several of its fine-tuned variants, including instruction-tuned models, DPO-optimized variants (Teknium et al. 2024).
- **Model Pruning.** For structured pruning, we consider methods that remove layers based on importance, such as ShortGPT (Men et al. 2024) and Sheared Llama (Xia et al. 2023). For unstructured pruning, we evaluate representative importance-based methods that prune weights according to their significance, including Wanda (Sun et al. 2023a) and SparseGPT (Frantar and Alistarh 2023). Ma et al. (2025) identifies critical sparsity thresholds near 35% (structured) and 60% (unstructured), beyond which model performance rapidly deteriorates. We thus evaluate sparsity levels at 30%, 50%, and 70%.
- **Model Merging.** Model merging combines weights from multiple source models to create a new model. We evaluate GhostSpec on various merging approaches, including direct weight averaging, methods that reduce parameter interference through pruning and sign conflict resolution (Yadav et al. 2023), as well as techniques that merge models by fusing weights or aligning output distributions (Goddard et al. 2024; Wan et al. 2024).
- **Model Upcycling.** Model upcycling expands model capacity by introducing new components, such as additional layers or sparsely activated expert modules, including techniques that convert dense LLMs into sparse MoEs through Parameter-Efficient Sparsity Crafting (PESC) (Wu, Zheng, and Yu 2024).
- **Permutation and Scaling Transformations.** To evaluate invariance under adversarial weight manipulations, we apply random permutations to the hidden dimensions of MLP weight matrices. For the attention layers, we apply functionality-preserving similarity transforms, which

combine both random rotation and scaling, to the attention projection matrices.

- **Unrelated Models.** We computed similarity scores between our base models (Llama-2-7b and Mistral-7B) and a diverse set of independently trained LLMs, including pythia-6.9b, opt-6.7b, among others (MosaicML NLP Team 2023; Guo et al. 2024; Zhang et al. 2022).

Evaluation Protocol. To ensure a fair and rigorous comparison with baseline methods, we establish a standardized evaluation protocol. For each method, a model pair is classified as ‘related’ if its similarity score exceeds a certain threshold. We determine the optimal threshold τ^* for each method by finding the value that maximizes the F1-score against the ground truth labels (1 for related, 0 for unrelated):

$$\tau^* = \operatorname{argmax}_{\tau \in \mathcal{S}} \text{F1}(\hat{y}_i(\tau), y_i). \quad (8)$$

where:

- y_i is the true label, which is 1 for related pairs (based on ground truth) and 0 for unrelated pairs.
- $\hat{y}_i(\tau)$ is the predicted label, which is 1 if the similarity score exceeds the threshold τ , and 0 otherwise.

This protocol allows us to evaluate each method at its peak performance, ensuring a fair comparison.

Baseline Methods. We compare GhostSpec against representative fingerprinting methods across multiple paradigms.

- **Data-Aware Baselines:** These methods require input data to generate outputs or internal representations for analysis. This category includes black-box approaches like **QueRE** (Sam, Finzi, and Kolter 2025) and **Logits** (Yang and Wu 2024), which analyze model outputs, as well as white-box methods like **REFE** (Zhang et al. 2024), which measures hidden representation similarity. A key characteristic of these methods is their reliance on data, which increases computational cost and necessitates curated datasets.
- **Data-Free Baselines:** These methods operate directly on static model weights without requiring any input data. This category includes methods like **PCS** (Zeng et al. 2024), which analyzes invariant submatrices within transformer layers.

5.2 Main Results

The overall classification performance of each method, measured by its maximum F1-score on our dataset, is summarized in Figure 4. Our two proposed variants, **GhostSpec-corr** ($F1 = 0.9730$) and **GhostSpec-mse** ($F1 = 0.9867$), achieve a clear lead, outperforming all data-aware and data-free baselines. Table 1 presents a selection of illustrative examples from our dataset, showing their detailed similarity scores. These scores are color-coded using the method-specific optimal thresholds, providing an intuitive visualization of the final classification results

GhostSpec demonstrated robust performance across various model transformations. It consistently produces high

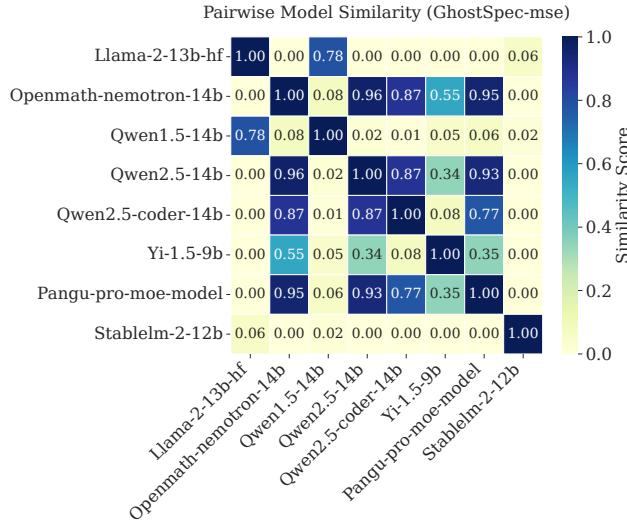


Figure 5: Pairwise structural similarity matrix of prominent open-source models computed using GhostSpec-mse. The heatmap visualizes the genealogical relationships between prominent open-source models. Higher scores indicate greater similarity.

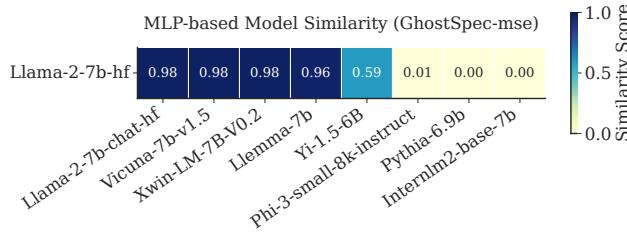


Figure 6: MLP-based spectral fingerprint similarity between Llama-2-7b and various models using GhostSpec-mse, computed from singular values of MLP up-proj and down-proj weights. Higher scores indicate greater similarity.

similarity scores for fine-tuned variants, regardless of training data or objectives. This robustness extends to structural modifications, including aggressive pruning (up to 70% sparsity), where it accurately recovers source models. It also detects strong similarity in merged and upcycled models, and remains resilient to adversarial transformations like permutation and scaling. Overall, GhostSpec reliably distinguishes true derivatives from unrelated models, showcasing strong discriminative power.

5.3 Further Discussion

Resilience to Evasion Attacks. We investigate an evasion strategy wherein an adversary fine-tunes a model with a custom loss to obscure its structural fingerprint. The objective is to maximize spectral distance from a victim model while preserving task performance.

To simulate this, we define a total loss combining task loss

and a spectral divergence term:

$$\mathcal{L}_{\text{total}}(\theta) = \mathcal{L}_{\text{task}}(\theta) - \lambda \cdot D_{\text{SVD}}(\mathcal{M}_\theta, \mathcal{M}_{\text{victim}}) \quad (9)$$

where D_{SVD} denotes the MSE between singular value spectra. The hyperparameter λ balances task fidelity and spectral divergence.

We apply this method to adversarially fine-tune a Llama-3.2-1B-instruct model. Results show that it is difficult to significantly alter the singular value spectrum without hurting model performance.

These findings indicate that spectral features are intrinsically tied to model functionality, limiting the practicality of evasion via spectral manipulation.

Case Study: A High-Profile Lineage Dispute We apply **GhostSpec** using GhostSpec-mse similarity to investigate the recently debated lineage of Pangu-Pro-MoE by comparing it with several open-source models, including the Qwen series and Llama variants.

As shown in Figure 5, GhostSpec finds that Pangu-Pro-MoE has the highest similarity with OpenMath-Nemotron-14B (a fine-tuned variant of Qwen2.5-14B) and Qwen2.5-14B, while showing negligible similarity to unrelated models such as Yi-1.5-9b and Llama-2-13b-hf.

These results indicate a potential lineage connection between Pangu-Pro-MoE and the Qwen2.5-14B family, though further evidence is needed for confirmation.

Analysis of MLP Module Spectra. To examine whether spectral fingerprinting extends beyond attention layers, we analyze singular values of the MLP up-proj and down-proj weight matrices in each Transformer layer. We compute GhostSpec-mse similarity between Llama-2-7b-hf, its fine-tuned variants, and unrelated models.

As shown in Figure 6, MLP-based fingerprints effectively distinguish fine-tuned models with similarity above 0.96 from unrelated models showing near-zero similarity.

However, this approach incurs higher computational cost due to the larger size of MLP weight matrices and is less robust to common dense-to-MoE expansions where MLP layers are replaced by experts. Therefore, attention-based fingerprints remain more efficient and structurally stable for reliable lineage verification.

6 Conclusion

This paper tackles LLM lineage verification amid widespread reuse and potential plagiarism. We propose GhostSpec, a robust, data-independent, and efficient white-box method that constructs stable fingerprints from the singular value spectra of invariant attention matrix products. Resilient to common modifications and adversarial attacks, it employs a penalty-based optimal path alignment algorithm to handle architectural differences. Extensive experiments demonstrate GhostSpec reliably identifies model ancestry across diverse transformations, including fine-tuning, pruning, merging, and expansion. GhostSpec offers a practical, trustworthy tool to protect intellectual property and improve transparency in open-source AI ecosystems.

Acknowledgements

This work was supported by the National Natural Science Foundation of China under Grant No. 62306216, the Fundamental Research Funds for the Central Universities under Grant No. 2042025kf0026, and the Technology Innovation Program of Hubei Province under Grant No. 2024BAB043.

References

- Achiam, J.; Adler, S.; Agarwal, S.; Ahmad, L.; Akkaya, I.; Aleman, F. L.; Almeida, D.; Altenschmidt, J.; Altman, S.; Anadkat, S.; et al. 2023. Gpt-4 technical report. *arXiv preprint arXiv:2303.08774*.
- Azerbayev, Z.; Schoelkopf, H.; Paster, K.; Santos, M. D.; McAleer, S.; Jiang, A. Q.; Deng, J.; Biderman, S.; and Welleck, S. 2023. Lemma: An open language model for mathematics. *arXiv preprint arXiv:2310.10631*.
- Bidberman, S.; Schoelkopf, H.; Anthony, Q. G.; Bradley, H.; O'Brien, K.; Hallahan, E.; Khan, M. A.; Purohit, S.; Prashanth, U. S.; Raff, E.; et al. 2023. Pythia: A suite for analyzing large language models across training and scaling. In *International Conference on Machine Learning*, 2397–2430. PMLR.
- Cai, Z.; Cao, M.; Chen, H.; Chen, K.; Chen, K.; Chen, X.; Chen, X.; Chen, Z.; Chen, Z.; Chu, P.; et al. 2024. Internlm2 technical report. *arXiv preprint arXiv:2403.17297*.
- Frantar, E.; and Alistarh, D. 2023. Sparsegpt: Massive language models can be accurately pruned in one-shot. In *International conference on machine learning*, 10323–10337. PMLR.
- Goddard, C.; Siriwardhana, S.; Ehghaghi, M.; Meyers, L.; Karpukhin, V.; Benedict, B.; McQuade, M.; and Solawetz, J. 2024. Arcee's MergeKit: A Toolkit for Merging Large Language Models. In Dernoncourt, F.; Preoțiu-Pietro, D.; and Shimorina, A., eds., *Proceedings of the 2024 Conference on Empirical Methods in Natural Language Processing: Industry Track*, 477–485. Miami, Florida, US: Association for Computational Linguistics.
- Guo, D.; Zhu, Q.; Yang, D.; Xie, Z.; Dong, K.; Zhang, W.; Chen, G.; Bi, X.; Wu, Y.; Li, Y.; et al. 2024. DeepSeek-Coder: When the Large Language Model Meets Programming—The Rise of Code Intelligence. *arXiv preprint arXiv:2401.14196*.
- Hu, J.; Li, J.; Pan, Z.; Chen, C.; Li, Z.; Wang, P.; and Zhang, L. 2025. SongSong: A Time Phonograph for Chinese SongCi Music from Thousand of Years Away. In *Proceedings of the AAAI Conference on Artificial Intelligence*, volume 39(25), 26229–26237.
- Jiang, A. Q.; Sablayrolles, A.; Mensch, A.; Bamford, C.; Chaplot, D. S.; de Las Casas, D.; Bressand, F.; Lengyel, G.; Lample, G.; Saulnier, L.; Lavaud, L. R.; Lachaux, M.; Stock, P.; Scao, T. L.; Lavril, T.; Wang, T.; Lacroix, T.; and Sayed, W. E. 2023. Mistral 7B. *CoRR*, abs/2310.06825.
- Kirchenbauer, J.; Geiping, J.; Wen, Y.; Katz, J.; Miers, I.; and Goldstein, T. 2023. A watermark for large language models. In *International Conference on Machine Learning*, 17061–17084. PMLR.
- Li, Q.; Li, Z.; Cai, X.; Du, B.; and Zhao, H. 2023. Enhancing visually-rich document understanding via layout structure modeling. In *Proceedings of the 31st ACM international conference on multimedia*, 4513–4523.
- Liang, H.; Zheng, Y.; Li, Y.; Zhang, Y.; and Liang, S. 2025. Origin Tracer: A Method for Detecting LoRA Fine-Tuning Origins in LLMs. *arXiv preprint arXiv:2505.19466*.
- Ma, Z.; Li, Z.; Zhang, L.; Xia, G.-S.; Du, B.; Zhang, L.; and Tao, D. 2025. Model Hemorrhage and the Robustness Limits of Large Language Models.
- McGovern, H.; Stureborg, R.; Suhara, Y.; and Alikaniotis, D. 2024. Your large language models are leaving fingerprints. *arXiv preprint arXiv:2405.14057*.
- Men, X.; Xu, M.; Zhang, Q.; Wang, B.; Lin, H.; Lu, Y.; Han, X.; and Chen, W. 2024. Shortgpt: Layers in large language models are more redundant than you expect. *arXiv preprint arXiv:2403.03853*.
- MosaicML NLP Team. 2023. Introducing MPT-7B: A New Standard for Open-Source, Commercially Usable LLMs. www.mosaicml.com/blog/mpt-7b. Accessed: 2023-05-05.
- Nagatsuka, K.; Morishita, T.; and Sogawa, Y. 2025. A Nested Watermark for Large Language Models. *arXiv preprint arXiv:2506.17308*.
- Pasquini, D.; Kornaropoulos, E. M.; and Ateniese, G. 2024. Llmmmap: Fingerprinting for large language models. *arXiv preprint arXiv:2407.15847*.
- Poon, M.; Dai, X.; Liu, X.; Kong, F.; Lui, J.; and Zuo, J. 2025. Online Multi-LLM Selection via Contextual Bandits under Unstructured Context Evolution. *arXiv preprint arXiv:2506.17670*.
- Sam, D.; Finzi, M.; and Kolter, J. Z. 2025. Predicting the performance of black-box llms through self-queries. *arXiv preprint arXiv:2501.01558*.
- Staats, M.; Thamm, M.; and Rosenow, B. 2024. Small Singular Values Matter: A Random Matrix Analysis of Transformer Models. *arXiv preprint arXiv:2410.17770*.
- Sun, M.; Liu, Z.; Bair, A.; and Kolter, J. Z. 2023a. A simple and effective pruning approach for large language models. *arXiv preprint arXiv:2306.11695*.
- Sun, Y.; Liu, T.; Hu, P.; Liao, Q.; Fu, S.; Yu, N.; Guo, D.; Liu, Y.; and Liu, L. 2023b. Deep intellectual property protection: A survey. *arXiv preprint arXiv:2304.14613*.
- Tang, Z.; Ma, Z.; Wang, S.; Li, Z.; Zhang, L.; Zhao, H.; Li, Y.; and Wang, Q. 2025. CoViPAL: Layer-wise Contextualized Visual Token Pruning for Large Vision-Language Models. In *Findings of the Association for Computational Linguistics: EMNLP 2025*, 20701–20714.
- Teknium; theemozilla; karan4d; and huemin art. 2024. Nous Hermes 2 Mistral 7B DPO. <https://huggingface.co/NousResearch/Nous-Hermes-2-Mistral-7B-DPO>.
- Touvron, H.; Martin, L.; Stone, K.; Albert, P.; Almahairi, A.; Babaei, Y.; Bashlykov, N.; Batra, S.; Bhargava, P.; Bhosale, S.; et al. 2023. Llama 2: Open foundation and fine-tuned chat models. *arXiv preprint arXiv:2307.09288*.

- Wan, F.; Huang, X.; Cai, D.; Quan, X.; Bi, W.; and Shi, S. 2024. Knowledge fusion of large language models. *arXiv preprint arXiv:2401.10491*.
- Wang, S.; Li, Z.; Luohe, S.; Du, B.; Zhao, H.; Li, Y.; and Wang, Q. 2025. From Parameters to Performance: A Data-Driven Study on LLM Structure and Development. In *Proceedings of the 2025 Conference on Empirical Methods in Natural Language Processing*, 26095–26112.
- Workshop, B.; Scao, T. L.; Fan, A.; Akiki, C.; Pavlick, E.; Ilić, S.; Hesslow, D.; Castagné, R.; Lucioni, A. S.; Yvon, F.; et al. 2022. Bloom: A 176b-parameter open-access multilingual language model. *arXiv preprint arXiv:2211.05100*.
- Wu, H.; Zheng, H.; and Yu, B. 2024. Parameter-Efficient Sparsity Crafting from Dense to Mixture-of-Experts for Instruction Tuning on General Tasks. *arXiv preprint arXiv:2401.02731*.
- Wu, Z.; Zhao, Y.; and Wang, H. 2025. Gradient-Based Model Fingerprinting for LLM Similarity Detection and Family Classification. *arXiv preprint arXiv:2506.01631*.
- Xia, M.; Gao, T.; Zeng, Z.; and Chen, D. 2023. Sheared llama: Accelerating language model pre-training via structured pruning. *arXiv preprint arXiv:2310.06694*.
- Xu, J.; Wang, F.; Ma, M. D.; Koh, P. W.; Xiao, C.; and Chen, M. 2024. Instructional fingerprinting of large language models. *arXiv preprint arXiv:2401.12255*.
- Xwin-LM Team. 2023. Xwin-LM. <https://github.com/Xwin-LM/Xwin-LM>. Accessed: 2023-09.
- Yadav, P.; Tam, D.; Choshen, L.; Raffel, C. A.; and Bansal, M. 2023. Ties-merging: Resolving interference when merging models. *Advances in Neural Information Processing Systems*, 36: 7093–7115.
- Yang, A.; Li, A.; Yang, B.; Zhang, B.; Hui, B.; Zheng, B.; Yu, B.; Gao, C.; Huang, C.; Lv, C.; et al. 2025a. Qwen3 technical report. *arXiv preprint arXiv:2505.09388*.
- Yang, E.; Shen, L.; Guo, G.; Wang, X.; Cao, X.; Zhang, J.; and Tao, D. 2024. Model merging in llms, mllms, and beyond: Methods, theories, applications and opportunities. *arXiv preprint arXiv:2408.07666*.
- Yang, H.; Yao, Y.; Li, Z.; Qi, B.; Guoming, L.; and Zhao, H. 2025b. XQuant: Achieving Ultra-Low Bit KV Cache Quantization with Cross-Layer Compression. In *Proceedings of the 2025 Conference on Empirical Methods in Natural Language Processing*, 9796–9811.
- Yang, Z.; and Wu, H. 2024. A fingerprint for large language models. *arXiv preprint arXiv:2407.01235*.
- Yao, Y.; Yu, T.; Zhang, A.; Wang, C.; Cui, J.; Zhu, H.; Cai, T.; Li, H.; Zhao, W.; He, Z.; et al. 2024. Minicpmv: A gpt-4v level mllm on your phone. *arXiv preprint arXiv:2408.01800*.
- Yoon, D.-h.; Chun, M.; Allen, T.; Müller, H.; Wang, M.; and Sharma, R. 2025. Intrinsic Fingerprint of LLMs: Continue Training is NOT All You Need to Steal A Model! *arXiv preprint arXiv:2507.03014*.
- Young, A.; Chen, B.; Li, C.; Huang, C.; Zhang, G.; Zhang, G.; Wang, G.; Li, H.; Zhu, J.; Chen, J.; et al. 2024. Yi: Open foundation models by 01. ai. *arXiv preprint arXiv:2403.04652*.
- Zeng, B.; Wang, L.; Hu, Y.; Xu, Y.; Zhou, C.; Wang, X.; Yu, Y.; and Lin, Z. 2024. Huref: Human-readable fingerprint for large language models. *Advances in Neural Information Processing Systems*, 37: 126332–126362.
- Zhang, J.; Liu, D.; Qian, C.; Zhang, L.; Liu, Y.; Qiao, Y.; and Shao, J. 2024. Reef: Representation encoding fingerprints for large language models. *arXiv preprint arXiv:2410.14273*.
- Zhang, S.; Roller, S.; Goyal, N.; Artetxe, M.; Chen, M.; Chen, S.; Dewan, C.; Diab, M.; Li, X.; Lin, X. V.; et al. 2022. Opt: Open pre-trained transformer language models. *arXiv preprint arXiv:2205.01068*.
- Zhang, Z.; He, L.; Li, Z.; Zhang, L.; Zhao, H.; and Du, B. 2025. Segment First or Comprehend First? Explore the Limit of Unsupervised Word Segmentation with Large Language Models. *arXiv preprint arXiv:2505.19631*.
- Zhu, X.; Li, J.; Liu, Y.; Ma, C.; and Wang, W. 2024. A survey on model compression for large language models. *Transactions of the Association for Computational Linguistics*, 12: 1556–1577.

A Theoretical Foundation of the GhostSpec Fingerprint

We first characterize the class of potential functionality-preserving weight transformation attacks that can significantly alter model parameters without changing the input-output mapping. To counter these attacks, we identify specific matrix products that remain strictly unaffected. We then provide a formal proof of this invariance, taking into account the practical convention of storing transposed weight matrices.

Throughout this section, we denote the conceptual weight matrices as W_q, W_k, W_v, W_o . For computational efficiency (e.g., using row-major input vectors x), models typically store their transposed counterparts: $W_q^\top, W_k^\top, W_v^\top, W_o^\top$. A projection is thus calculated as $x \cdot W^\top$. Our derivations will explicitly use this convention.

A.1 Functionality-Preserving Transformation Attack

V-O Per-Head Transformation. The context vector c from a single attention head is computed by projecting the value vectors v with the output weight matrix W_o . The value vectors themselves are projections of the input x , i.e., $v = x \cdot W_v^\top$. Thus, the final output y of the head is:

$$y = (\text{AttentionScores} \cdot (x \cdot W_v^\top)) \cdot W_o^\top.$$

The transformation involves a block-diagonal invertible matrix C applied to the conceptual weights as:

$$\tilde{W}_v = CW_v, \quad \tilde{W}_o = W_oC^{-1}.$$

The corresponding stored weights are:

$$\tilde{W}_v^\top = W_v^\top C^\top, \quad \tilde{W}_o^\top = (C^{-1})^\top W_o^\top.$$

The output becomes:

$$\begin{aligned}\tilde{y} &= (\text{AttentionScores} \cdot (x \cdot \tilde{W}_v^\top)) \cdot \tilde{W}_o^\top \\ &= (\text{AttentionScores} \cdot (x \cdot W_v^\top C^\top)) \cdot ((C^{-1})^\top W_o^\top) \\ &= (\text{AttentionScores} \cdot x \cdot W_v^\top) \cdot (C^\top (C^{-1})^\top) \cdot W_o^\top \\ &= (\text{AttentionScores} \cdot x \cdot W_v^\top) \cdot I^\top \cdot W_o^\top = y.\end{aligned}$$

Q-K RoPE-Compatible Transformation. Self-attention output is computed as:

$$\text{Attention}(Q, K, V) = \text{softmax} \left(\frac{QK^\top}{\sqrt{d_k}} \right) V, \quad (10)$$

where $Q = xW_q^\top$ and $K = xW_k^\top$.

To construct a transformation that preserves this output while remaining compatible with RoPE, we introduce a doubly block-diagonal matrix P and define:

$$\tilde{W}_q = PW_q, \quad \tilde{W}_k = (P^\top)^{-1}W_k. \quad (11)$$

The corresponding transformed query and key matrices become:

$$\tilde{Q} = QP^\top, \quad \tilde{K} = KP^{-1}. \quad (12)$$

Then,

$$\tilde{Q}\tilde{K}^\top = (QP^\top)(KP^{-1})^\top = QP^\top(P^{-1})^\top K^\top \quad (13)$$

$$= Q(P^{-1}P)^\top K^\top = QK^\top. \quad (14)$$

Thus, attention logits and softmax remain unchanged. Since V is untouched, the overall attention output is exactly preserved:

$$\text{Attention}(\tilde{Q}, \tilde{K}, V) = \text{Attention}(Q, K, V). \quad (15)$$

This proves the transformation modifies W_q and W_k without altering the functionality of the attention layer.

A.2 Formal Proof of Invariance

This section provides the formal proof that our spectral fingerprints remain invariant when subjected to the functionality-preserving transformation attacks defined above. This resistance is a cornerstone of the method's robustness. We demonstrate that the singular value spectra of our selected matrix products are strictly immune to these adversarial manipulations.

Invariance of the V-O Product ($M_{ov} = W_o W_v$). The transformation is defined on the conceptual weights as $\tilde{W}_v = CW_v$ and $\tilde{W}_o = W_o C^{-1}$. The transformed product is:

$$\begin{aligned}\tilde{M}_{ov} &= \tilde{W}_o \cdot \tilde{W}_v \\ &= (W_o C^{-1}) \cdot (CW_v) \\ &= W_o \cdot (C^{-1}C) \cdot W_v \\ &= W_o \cdot I \cdot W_v = W_o W_v = M_{ov}.\end{aligned}$$

The product matrix M_{ov} is strictly invariant. Consequently, its Singular Value Decomposition (SVD), and therefore its singular value spectrum, is also invariant, regardless of the storage convention of the weights.

Invariance of the Q-K Product ($M_{q^\top k} = W_q^\top W_k$). The transformation is $\tilde{W}_q = PW_q$ and $\tilde{W}_k = (P^\top)^{-1}W_k$. The transformed product is:

$$\begin{aligned}\tilde{M}_{q^\top k} &= \tilde{W}_q^\top \cdot \tilde{W}_k \\ &= (W_q^\top P^\top) \cdot (P^\top)^{-1}W_k \\ &= W_q^\top \cdot I \cdot W_k = W_q^\top W_k = M_{q^\top k}.\end{aligned}$$

B Methodology and Implementation Details

This appendix provides specific implementation details for the algorithms and metrics described in Section 4, as well as the hyperparameter values used in our experiments (Section 5), to ensure full reproducibility.

B.1 Core Function Definitions

Effective Rank. The effective rank, used in Section 4.2 to determine the number of singular values to compare, is a continuous measure of a matrix's intrinsic dimensionality, defined via the entropy of its normalized singular values. Given a singular value vector $s = (s_1, s_2, \dots, s_n)$, we define its effective rank as:

$$\text{eff_rank}(s) = \exp \left(- \sum_{j=1}^n \frac{s_j}{\sum_{i=1}^n s_i} \log \frac{s_j}{\sum_{i=1}^n s_i} \right) \quad (16)$$

Distance Correlation (dCor). Distance correlation is used to compute the GhostSpec-corr similarity score (Section 4.2, Equation 7). It is a measure of statistical dependence between two random vectors of arbitrary, not necessarily equal, dimension. Unlike Pearson correlation, distance correlation is zero if and only if the vectors are statistically independent, making it a robust metric for comparing the complex, non-linear trends of our layer-wise spectral mean sequences.

Formally, for two sequences $\mathbf{X} \in \mathbb{R}^{n \times d_1}$ and $\mathbf{Y} \in \mathbb{R}^{n \times d_2}$ with n samples, the empirical distance correlation is computed as follows. First, the Euclidean distance matrices $a, b \in \mathbb{R}^{n \times n}$ are constructed, where $a_{ij} = \|x_i - x_j\|$ and $b_{ij} = \|y_i - y_j\|$. These matrices are then doubly centered:

$$A_{ij} = a_{ij} - \bar{a}_{..} - \bar{a}_{..} + \bar{a}_{..}, \quad (17)$$

where $\bar{a}_{..}$ is the row mean, $\bar{a}_{..}$ is the column mean, and $\bar{a}_{..}$ is the grand mean of matrix a . The same transformation is applied to b to obtain B . The sample distance correlation $\mathcal{R}_n(X, Y)$ is then defined based on the sample distance covariance $\mathcal{V}_n(X, Y)$ and variances $\mathcal{V}_n(X), \mathcal{V}_n(Y)$.

B.2 Hyperparameter Settings

POSA Gap Penalty (ρ). The gap penalty ρ for the Penalty-based Optimal Spectral Alignment (POSA) algorithm (Algorithm 1), which is central to comparing models of varying depth, was set empirically. We observed that a value corresponding to the average single-layer MSE distance between moderately similar models provided a good balance between matching corresponding layers and allowing for necessary skips in pruned or expanded models. Across all experiments, a fixed value of $\rho = 0.002$ was used.

Sigmoid Transformation Parameters (τ, k). The parameters for the final inverted Sigmoid transformation (Equation 6), used to convert the raw path distance from POSA into the final GhostSpec-mse similarity score, were determined empirically. The goal was to select values that best separate the distance distributions of related and unrelated model pairs, thereby maximizing the F1-score on a validation set. Based on this analysis, we use a fixed threshold $\tau = 0.00371$ and a steepness factor $k = 1000$.

Method-Specific Thresholds (τ^*). As described in the Evaluation Protocol (Section 5.1), we determine an optimal classification threshold τ^* for each fingerprinting method to ensure a fair and rigorous comparison. This threshold is found by searching for the value that maximizes the F1-score for each method on our ground-truth dataset, ensuring that every method is evaluated at its peak performance. The final, empirically determined thresholds used for all experiments are presented in Table 2.

Table 2: Optimal classification thresholds for all methods.

Method	Optimal Threshold (τ^*)
QueRE	0.18
Logits	0.83
REEF	0.83
PCS	0.12
GhostSpec-corr	0.61
GhostSpec-mse	0.85

C Detailed Experimental Setup

This appendix provides supplementary details for the experimental setup described in Section 5.

C.1 Model Dataset

Our comprehensive dataset is constructed using Llama-2-7B and Mistral-7B as the primary base models. This dataset covers a wide range of transformations, including finetuning, compression, merging, and expansion, with ground-truth labels indicating whether each pair is related or unrelated. A complete list of all model pairs and their corresponding modification type is provided in Table 2.

C.2 Computing Infrastructure

All experiments were conducted on a server equipped with four NVIDIA GeForce RTX 4090 GPUs (24GB VRAM). The software environment was based on CUDA Version 12.2, with Python 3.10 and PyTorch 2.1.

C.3 Computational Efficiency Analysis

We analyze the computational efficiency of GhostSpec in two distinct stages: the one-time fingerprint extraction and the pairwise similarity comparison.

Theoretical Complexity.

- **Stage 1: Fingerprint Extraction.** For a model with L layers and hidden dimension d , we compute two invariant products per layer (M_{qk} and M_{vo}) and perform Singular Value Decomposition (SVD). While the worst-case complexity for full SVD is $O(d^3)$, our practical implementation employs randomized truncated SVD to extract only the top- K singular values, where $K \ll d$ (typically determined by effective rank). This reduces the practical complexity to $O(L \cdot d^2 K)$. Importantly, this is a one-time cost per model checkpoint.
- **Stage 2: Similarity Comparison.** To compare two models with N and M layers, the POSA algorithm computes a pairwise distance matrix and executes dynamic programming to find the optimal alignment. The complexity is $O(N \cdot M \cdot K)$. Crucially, this step is independent of the model’s large hidden dimension d , making the retrieval and verification process extremely fast.

Empirical Runtime. We measured execution times on a server equipped with a single NVIDIA GeForce RTX 4090 GPU (24GB VRAM) for extraction and standard Intel Xeon CPUs for comparison. Table 3 details the fingerprint extraction times for models of varying sizes.

Model	Parameters	Extraction Time (s)
Qwen3-1.7B	1.7B	30.7
Qwen3-4B	4B	46.6
Qwen3-8B	8B	132.0

Table 3: One-time fingerprint extraction times measured on a single RTX 4090 GPU. The process is efficient, taking approximately 2 minutes for an 8B parameter model.

The pairwise comparison stage is near-instantaneous. For example, computing the similarity between Llama-2-7B and Qwen2.5-7B takes approximately 0.24 seconds, and comparing Llama-2-7B with the significantly deeper Qwen2.5-32B takes only 0.62 seconds. This efficiency demonstrates that GhostSpec is highly scalable for checking a query model against a large repository of existing fingerprints.

D Additional Experiments and Visualizations

This section provides additional experimental results that empirically justify key design choices of the GhostSpec method (Section 4) and offers further visual evidence of its effectiveness.

D.1 Out-of-Sample Threshold Generalization

To evaluate the generalizability of our method and the robustness of the optimal thresholds derived in Section 5.1 ($\tau_{\text{mse}} = 0.85$ and $\tau_{\text{corr}} = 0.61$), we conducted out-of-sample evaluations on two additional model families with significantly different parameter scales: the Qwen2.5-3B family and the Qwen2.5-32B family.

We applied the fixed thresholds determined solely from the initial Llama-2/Mistral-7B dataset.

Results on 3B Scale. Table 4 presents the results for the 3B parameter scale. GhostSpec correctly identifies all fine-tuned variants as related, with scores well above the thresholds. Conversely, unrelated models like MiniMA-3B and bloom-3b are correctly rejected.

Base Model	Comparison Model	GhostSpec-mse	GhostSpec-corr	Ground Truth
Qwen2.5-3B	Qwen2.5-3B-Instruct	0.9761	0.9999	Related
Qwen2.5-3B	Qwen2.5-Coder-3B	0.9618	0.9407	Related
Qwen2.5-3B	SDLM-3B-D4	0.9760	0.9990	Related
Qwen2.5-3B	calme-3.1-instruct-3b	0.9761	0.9999	Related
Qwen2.5-3B	MiniMA-3B	0.0000	0.6097	Unrelated
Qwen2.5-3B	bloom-3b	0.0000	0.2765	Unrelated

Table 4: Out-of-sample evaluation on the Qwen2.5-3B family using fixed thresholds ($\tau_{\text{mse}} > 0.85$, $\tau_{\text{corr}} > 0.61$). Scores in **bold** indicate a positive classification (Related) consistent with Ground Truth.

Results on 32B Scale. Table 5 extends this validation to the larger 32B parameter scale. Despite the significant increase in model depth and width compared to the 7B base models used for calibration, GhostSpec maintains its discriminative power. All derivative models are identified with high confidence (MSE > 0.97), while unrelated large models show negligible similarity.

Base Model	Comparison Model	GhostSpec-mse	GhostSpec-corr	Ground Truth
Qwen2.5-32B	BFS-Prover-V2-32B	0.9761	0.9999	Related
Qwen2.5-32B	K2-Think	0.9761	0.9996	Related
Qwen2.5-32B	Qwen2.5-32B-Instruct	0.9761	0.9999	Related
Qwen2.5-32B	SDLM-32B-D4	0.9761	0.9965	Related
Qwen2.5-32B	Yi-34B	0.0003	0.2999	Unrelated
Qwen2.5-32B	opus-v1-34B	0.0003	0.2934	Unrelated

Table 5: Out-of-sample evaluation on the Qwen2.5-32B family using fixed thresholds ($\tau_{\text{mse}} > 0.85$, $\tau_{\text{corr}} > 0.61$). The method remains robust at larger scales.

These results confirm that the structural fingerprints captured by GhostSpec are scale-invariant and that the decision thresholds established on 7B models generalize effectively to both smaller (3B) and larger (32B) architectures without the need for recalibration.

D.2 Ablation Studies

On the Necessity of Invariant Products To demonstrate the critical role of our invariant product construction (Section 4.1), we performed an ablation study. We compared the performance of the full GhostSpec method against a naive variant that computes fingerprints directly from the singular values of the raw attention weights (W_q , W_k , W_v , W_o). The specific computational difference between the two methods is as follows:

- **Full GhostSpec (Invariant Method):** This is the standard method proposed in our paper. For each layer i , it first constructs two invariant product matrices whose singular value spectra are robust to functionality-preserving transformations:

$$M_{\text{ov}}^{(i)} = W_o^{(i)} W_v^{(i)} \quad \text{and} \quad M_{q^{\top}k}^{(i)} = (W_q^{(i)})^{\top} W_k^{(i)} \quad (18)$$

The final fingerprint for the layer, $\mathcal{F}^{(i)}$, is then derived from the singular value vectors of these two product matrices:

$$\mathcal{F}^{(i)} = \left(\text{SVD}(M_{\text{ov}}^{(i)}), \text{SVD}(M_{q^{\top}k}^{(i)}) \right) \quad (19)$$

- **Naive Variant (Vulnerable Method):** For the ablation study, we created a naive version that bypasses the invariant product construction. Instead, it directly computes the SVD of the four individual attention weight matrices for each layer i :

$$W_q^{(i)}, \quad W_k^{(i)}, \quad W_v^{(i)}, \quad W_o^{(i)} \quad (20)$$

The fingerprint in this case is composed of the singular value vectors from these four raw matrices:

$$\begin{aligned} \mathcal{F}_{\text{naive}}^{(i)} = & (\text{SVD}(W_q^{(i)}), \text{SVD}(W_k^{(i)}), \\ & \text{SVD}(W_v^{(i)}), \text{SVD}(W_o^{(i)})) \end{aligned} \quad (21)$$

We tested both methods on the task of identifying a transformed version of Llama-2-7b-chat-hf that had undergone both scaling and permutation attacks. The results are shown in Table 6. The naive method fails completely, with similarity scores dropping significantly. In contrast, GhostSpec maintains near-perfect similarity, proving that the invariant product construction is essential for robustness against these attacks.

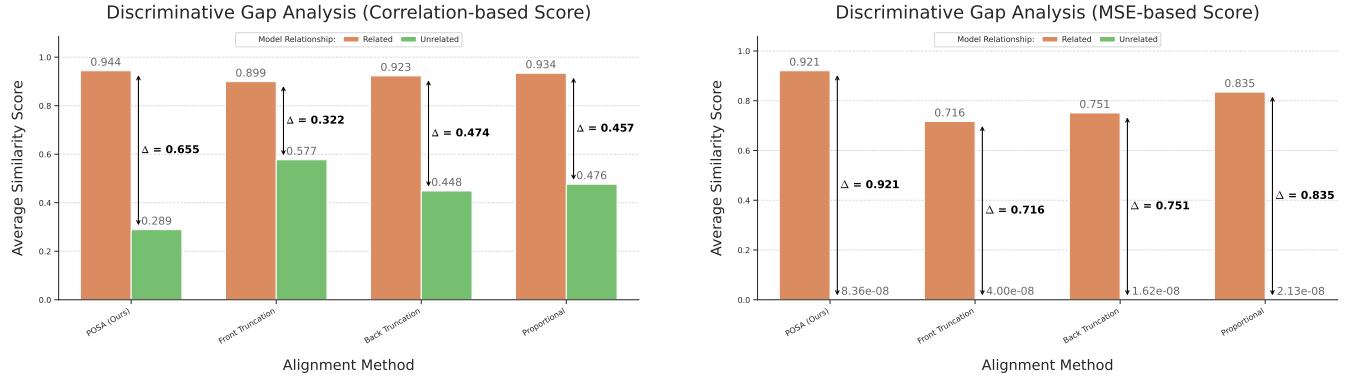
Table 6: Comparison between the naive direct SVD method and the invariant GhostSpec method when faced with an adversarial transformation. Scores are similarity to the original model.

Method	GhostSpec-mse	GhostSpec-corr
Direct SVD (Vulnerable)	0.2585	0.5684
GhostSpec (Invariant)	0.9761	1.0000

Ablation on Invariant Product Components To justify the design choice of using two invariant products ($M_{qk} = W_q W_k^{\top}$ and $M_{vo} = W_v W_o$) rather than a single one, we performed an ablation study on 28 model pairs (20 related, 8 unrelated). We evaluated the discriminative power of fingerprints derived from:

1. **QK Product Only:** Using only the singular values of M_{qk} .
2. **VO Product Only:** Using only the singular values of M_{vo} .
3. **Both (Proposed):** Using the concatenated fingerprints from both products.

As shown in Table 7, while each product independently captures meaningful structural information, combining them yields the highest discriminative gap for both metrics. This confirms that the Q - K and V - O interactions encode complementary information about the attention mechanism’s identity, and using both provides the most robust fingerprint.



(a) Discriminative gap for Correlation-based scores.

(b) Discriminative gap for MSE-based scores.

Figure 7: Comparison of the discriminative gaps for two scoring methods. POSA achieves the largest gaps, demonstrating superior discriminative power.

Fingerprint Configuration	Δ_{mse}	Δ_{corr}
QK Product Only (M_{qk})	0.7099	0.3962
VO Product Only (M_{vo})	0.5739	0.4568
Both (Proposed)	0.7370	0.4672

Table 7: Ablation study on the contribution of invariant matrix products. Combining both QK and VO products consistently yields the highest discriminative gap (Δ).

On the Necessity of the POSA Algorithm. To demonstrate the necessity of our *Penalty-based Optimal Spectral Alignment (POSA)* algorithm for comparing models of different depths, we conducted a targeted ablation study. The core challenge when comparing models A and B with different layer counts ($N_A \neq N_B$) is establishing a meaningful correspondence between their layer-wise feature sequences, $\mathcal{F}_A = (f_A^{(1)}, \dots, f_A^{(N_A)})$ and $\mathcal{F}_B = (f_B^{(1)}, \dots, f_B^{(N_B)})$. Our experiment was specifically designed to test this scenario.

We selected Llama-2-7b (32 layers) as the base model and compared it against a curated set of seven models, all of which have different layer counts, making a sophisticated alignment strategy essential. These models were categorized as:

- Related Models:** Five models derived from Llama-2 but with varying depths, including LLaMA-Pro-8B (40 layers), Llama-2-7b-chat-hf-30-sparsity (23 layers), and the Sheared-LLaMA-1.3B series (24 layers).
- Unrelated Models:** Two architecturally distinct models, Qwen2-7B (28 layers) and Qwen2.5-7B (28 layers).

Our experiment compared the performance of POSA against three naive baseline alignment strategies:

- POSA (Our Method):** Employs dynamic programming with a gap penalty (ρ) to find the optimal, potentially non-contiguous, layer alignment that minimizes global distance, as defined by the cost function:

$$\text{Cost}(P) = \sum_{(i_k, j_k) \in P} D_{i_k, j_k} + \sum_{k > 1} \rho \cdot (|j_k - j_{k-1}| - 1)$$

- Baseline 1: Front Truncation:** Compares only the first n layers of each model, where $n = \min(N_A, N_B)$.
- Baseline 2: Back Truncation:** Compares only the last n layers of each model.
- Baseline 3: Proportional Subsampling:** Downsamples the layer sequence of the larger model to match the length of the smaller one.

To quantitatively evaluate the discriminative power of each alignment strategy, we aggregated the results. For each method, we calculated the average similarity score for the Related group and the Unrelated group. The key metric for our evaluation is the Discriminative Gap (Δ), which we define as the difference between these two average scores:

$$\Delta = \text{AvgScore(Related)} - \text{AvgScore(Unrelated)}$$

A larger gap indicates a superior ability to clearly and reliably distinguish genuine derivatives from unrelated models. The results of this analysis are presented in Figure 7a and Figure 7b.

As shown in the figures, our proposed POSA method consistently achieves the largest discriminative gap across both metrics. For the Correlation-based Score (Figure 7a), POSA achieves a gap of $\Delta = 0.655$, significantly outperforming Front Truncation ($\Delta = 0.322$), Back Truncation ($\Delta = 0.474$), and Proportional Subsampling ($\Delta = 0.457$). Similarly, for the MSE-based Score (Figure 7b), POSA's gap of $\Delta = 0.921$ is substantially larger than that of any other baseline.

These results empirically validate the superiority of the POSA algorithm. While naive methods can show some distinction, their separation between related and unrelated models is less pronounced and less reliable. By finding an optimal layer-wise correspondence that accounts for structural modifications, POSA maximizes the similarity signal from true derivatives while robustly rejecting unrelated models, thereby providing the most effective method for verifying model lineage when architectures differ.

Sensitivity Analysis of POSA Penalty (ρ) The Penalty-based Optimal Spectral Alignment (POSA) algorithm relies

on a gap penalty parameter, ρ , to balance the cost of matching dissimilar layers against the cost of skipping layers (introducing gaps). To validate our choice of $\rho = 0.002$ and analyze the method’s sensitivity to this hyperparameter, we conducted an experiment using the identical curated dataset of 7 model pairs described in the ablation study above. This dataset consists of the base Llama-2-7b model compared against the same group of 5 related variants with differing depths and 2 architecturally distinct unrelated models.

We measured the Discriminative Gap (Δ), defined as the difference between the average similarity score of related models and unrelated models:

$$\Delta = \text{AvgScore(Related)} - \text{AvgScore(Unrelated)}. \quad (22)$$

A higher Δ indicates better separation capability.

Table 8 presents the results for $\rho \in [0.0, 0.01]$. The results reveal a stable high-performance plateau for $\rho \in [0.0, 0.002]$, where the discriminative gap remains maximal. Beyond this range (e.g., $\rho \geq 0.005$), the penalty becomes too severe, forcing suboptimal alignments and reducing the gap, particularly for the MSE-based metric. Our default choice of $\rho = 0.002$ sits at the edge of this stable region, providing an optimal balance between alignment flexibility and structural constraint.

Gap Penalty (ρ)	Δ_{mse}	Δ_{corr}	Observation
0.000	0.9206	0.6385	Stable Plateau
0.001	0.9194	0.6385	Stable Plateau
0.002 (Default)	0.9194	0.6386	Optimal Choice
0.005	0.8447	0.6381	Onset of Decline
0.010	0.8074	0.6340	Significant Decline

Table 8: Sensitivity analysis of the POSA gap penalty ρ . The Discriminative Gap (Δ) remains stable for small penalties but degrades as ρ increases, justifying our selection of 0.002.

D.3 Visualization of the Fingerprint Space

To visualize the global structure of the fingerprint space and the discriminative power of our method, we perform dimensionality reduction using the t-SNE algorithm. Instead of constructing explicit high-dimensional feature vectors for each model, we leverage the final similarity scores to build a comprehensive pairwise distance matrix, which directly captures the relationships between all models in our dataset. This process is executed as follows:

1. Pairwise Distance Matrix Construction: For a set of N models in our dataset, we first compute an $N \times N$ similarity matrix S . Each element S_{ij} in this matrix represents the similarity score between model i and model j , calculated using either the GhostSpec-mse or GhostSpec-corr method. This similarity matrix is then converted into a distance matrix D , where each element is defined as:

$$D_{ij} = 1 - S_{ij}$$

The matrix D , where $D_{ii} = 0$ and $D_{ij} = D_{ji}$, serves as the direct input for the t-SNE algorithm.

2. t-SNE Dimensionality Reduction: We use the t-SNE algorithm with the `metric='precomputed'` setting, which operates directly on our distance matrix D . The algorithm seeks to find a low-dimensional embedding (in our case, 2D points $Y = \{y_1, y_2, \dots, y_N\}$) that preserves the local neighborhood structure of the original data. It achieves this by minimizing the Kullback–Leibler (KL) divergence between the joint probability distribution P , derived from the pairwise distances in D , and the joint probability distribution Q of the low-dimensional points in Y :

$$\text{KL}(P\|Q) = \sum_{i \neq j} p_{ij} \log \frac{p_{ij}}{q_{ij}}$$

The resulting 2D coordinates Y are then plotted, with each point representing a model.

We applied this visualization technique to a diverse dataset comprising models from the Llama family, the Mistral family, and several architecturally distinct unrelated models. The t-SNE embedding based on the GhostSpec-mse metric is shown in Figure 8. The visualization clearly demonstrates the effectiveness of our fingerprinting method. Models belonging to the Llama family form a distinct and tight cluster, while models from the Mistral family converge to a separate region in the embedded space. Critically, the unrelated models remain scattered and do not intrude upon these well-defined family clusters.

This clustering provides strong, intuitive evidence that our GhostSpec similarity scores effectively capture the underlying genealogical relationships between models. The clear separation of model families in the 2D space visually confirms that our method can robustly identify and differentiate model lineages, complementing the quantitative results presented earlier. For reproducibility, the t-SNE parameters were fixed with a perplexity of 20 and a random state of 42.

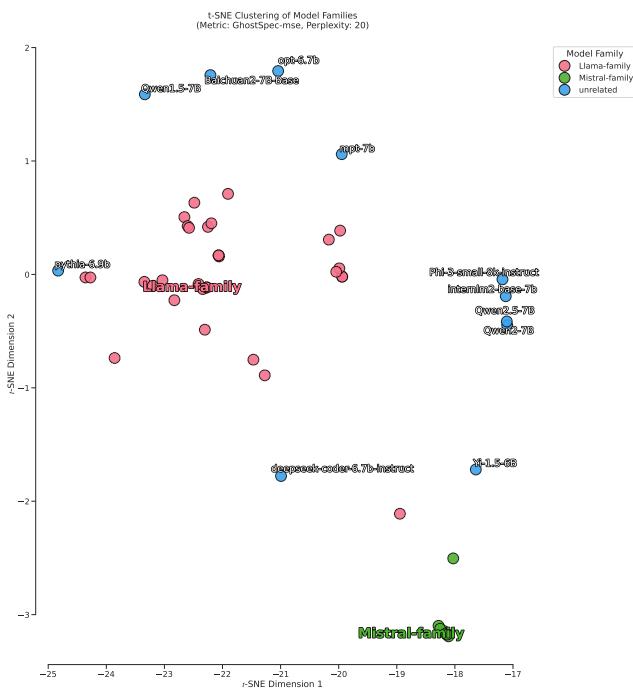


Figure 8: t-SNE visualization of the model fingerprint space using the GhostSpec-mse distance metric. Each point represents a model, colored by its family. The clear separation between the Llama family (red), Mistral family (green), and unrelated models (blue) demonstrates that our fingerprint effectively captures genealogical relationships, causing related models to cluster together.

Table 9: Complete list of the model pairs used in our dataset for evaluation, supplementing Section 5.1.

Primary Model: Llama-2-7b Comparison Model	Modification Type	Primary Model: Mistral-7B Comparison Model	Modification Type
Llama-2-7b-chat-hf	Fine-tuning	OpenHermes-2.5-Mistral-7B	Fine-tuning
Xwin-LM-7B-V0.2	Fine-tuning	Nous-Hermes-2-Mistral-7B	Fine-tuning
llemma_7b	Fine-tuning	dolphin-2.2.1-mistral-7b	Fine-tuning
CodeLlama-7b-hf	Fine-tuning		
chinese-llama-2-7b	Fine-tuning		
coma-7B-v0.1	Fine-tuning		
vicuna-7b-v1.5	Fine-tuning		
Sheared-LLaMA-1.3B	Structured Pruning	OpenHermes-pruned50	Pruning
Sheared-LLaMA-2.7B	Structured Pruning	OpenHermes-pruned2.4	Pruning
Sheared-LLaMA-1.3B-Pruned	Structured Pruning		
Sheared-LLaMA-1.3B-	Structured Pruning		
ShareGPT			
Sheared-LLaMA-2.7B-Pruned	Structured Pruning		
Sheared-LLaMA-2.7B-	Structured Pruning		
ShareGPT			
Llama-2-chat-shortgpt-30	Structured Pruning		
Llama-2-pruned50-retrained	Unstructured Pruning		
Llama-2-pruned70-retrained	Unstructured Pruning		
GBLM-Pruner-LLaMA-2-7B	Unstructured Pruning		
Llama-2-7b-chat-hf-30-sparsity	Unstructured Pruning		
Llama-2-7b-gsm8k-pruned_50	Unstructured Pruning		
Llama-2-7b-gsm8k-pruned_70	Unstructured Pruning		
Llama-2-7b-ultrachat200k-pruned_50	Unstructured Pruning		
Llama-2-7b-ultrachat200k-pruned_70	Unstructured Pruning		
CodeLlaMa-7B-dare-ties	Merging & Expansion	Chunky-Lemon-Cookie-11B	Merging & Expansion
llama2-7b-func-calling-slerp	Merging & Expansion	Triunvirato-7b	Merging & Expansion
FuseLLM-7B	Merging & Expansion	Daredevil-7B	Merging & Expansion
LLaMA-Pro-8B	Merging & Expansion	BioMistral-merged-instruct	Merging & Expansion
Camelidae-8x7B	Merging & Expansion		
Patent-Base-Llama-2-Chat-7B-Slerp	Merging & Expansion		
Llama-2-7b-chat-scaled	Adversarial Transforms		
Llama-2-7b-chat-permuted	Adversarial Transforms		
Qwen2.5-7B	Unrelated Models	pythia-6.9b	Unrelated Models
Yi-1.5-6B	Unrelated Models	mpt-7b	Unrelated Models
internlm2-base-7b	Unrelated Models	opt-6.7b	Unrelated Models
pythia-6.9b	Unrelated Models	Phi-3-small-8k-instruct	Unrelated Models
opt-6.7b	Unrelated Models	Yi-1.5-6B	Unrelated Models
Phi-3-small-8k-instruct	Unrelated Models	Qwen2-7B	Unrelated Models
		Baichuan2-7B-Base	Unrelated Models
		Qwen2.5-7B	Unrelated Models
		deepseek-coder-6.7b	Unrelated Models
		internlm2-base-7b	Unrelated Models