Functional invariants to watermark large transformers
Pierre Fernandez, Guillaume Couairon, Teddy Furon, Matthijs Douze

To cite this version:
Pierre Fernandez, Guillaume Couairon, Teddy Furon, Matthijs Douze. Functional invariants to watermark large transformers. IEEE International Conference on Acoustics, Speech and Signal Processing, Apr 2024, Seoul (Korea), South Korea. hal-04361026

HAL Id: hal-04361026
https://inria.hal.science/hal-04361026
Submitted on 22 Dec 2023

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L’archive ouverte pluridisciplinaire HAL, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d’enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Distributed under a Creative Commons Attribution 4.0 International License
FUNCTIONAL INVARIANTS TO WATERMARK LARGE TRANSFORMERS

Pierre Fernandez\textsuperscript{1,2*}, Guillaume Couairon\textsuperscript{1}, Teddy Furon\textsuperscript{21}, Matthijs Douze\textsuperscript{1}

\textsuperscript{1}FAIR, Meta \quad \textsuperscript{2}Centre Inria de l’Université de Rennes

ABSTRACT

The rapid growth of transformer-based models increases the concerns about their integrity and ownership insurance. Watermarking addresses this issue by embedding a unique identifier into the model, while preserving its performance. However, most existing approaches require to optimize the weights to imprint the watermark signal, which is not suitable at scale due to the computational cost. This paper explores watermarks with virtually no computational cost, applicable to a non-blind white-box setting (assuming access to both the original and watermarked networks). They generate functionally equivalent copies by leveraging the models’ invariance, via operations like dimension permutations or scaling/unscaling. This enables to watermark models without any change in their outputs and remains stealthy. Experiments demonstrate the effectiveness of the approach and its robustness against various model transformations (fine-tuning, quantization, pruning), making it a practical solution to protect the integrity of large models.

Index Terms— DNN watermarking, white-box, transformers

1. INTRODUCTION

Large-scale transformer models are a leap forward in the field of machine learning, with large language models like GPT-4 \cite{1}, LLaMA \cite{2} and others \cite{3,4,5}, or vision ones like ViT-22b \cite{6} or DINOv2 \cite{7}. As these models grow in complexity and size, protecting them is important due to investments in their development. Notably, this is raised by the US “Ensuring Safe, Secure, and Trustworthy AI” announcement, European AI Act and Chinese AI governance rules.

Watermarking deep neural networks \cite{8,9} presents a step towards ensuring their security, integrity and ownership. Embedding a unique identifier into the model enables tracing it to safeguard it from unauthorized usage and distribution. However, watermarking large transformer models poses new challenges. Current watermarking methods involve optimizing the weights to infuse the watermark, either during pre-training or by fine-tuning the weights with additional losses. While these techniques have shown success for smaller models, they become computationally infeasible for large-scale models and for the burgeoning number of potential users and applications.

To address these challenges, we introduce a new approach to watermarking large transformers, when access to both the original and watermarked model is granted, \textit{i.e.} in a non-blind white-box setting. Our method capitalizes on the inherent invariance of transformers. For a given model, it generates equivalent copies that serve as carriers for arbitrary signatures. By employing operations such as dimension permutation and coupled matrix multiplications, we create model replicas without changing the model’s outputs and without training. We conduct experiments on state-of-the-art transformer architectures to evaluate the applicability of our approach and its robustness against model processing (\textit{e.g.} fine-tuning, pruning, quantization, etc.). We also discuss the main drawbacks of this setting.

The paper is organized as follows: section 2 provides an overview of related works on DNN watermarking and background on transformers; section 3 details the transformer’s invariants and how to exploit them for watermarking; section 4 presents experimental results on large language models.

Problem statement. A provider \textit{Alice}, distributes her model to various users \textit{Bob} (either individuals or organizations). She aims to trace the model back to a specific user, in case of unauthorized distribution or leaks. As a precautionary measure, Alice embeds a unique signature in the model’s weights for each user. In a white-box setting, Alice has access to the models’ weights and extracts the signature from it to identify Bob. Besides, Bob may evade detection intentionally (trying to remove the watermark) or unintentionally (fine-tuning, quantization, etc.).

This setting is quite common. Indeed few entities (“Alices”) have the necessary computation resources, data and expertise to generate the base model. For example, the training of the 65-B LLaMA model took around 1B GPU-hours. Therefore, there are few variants of such large models in the world. Besides, when Bob gains access to the base model, it is common that he transforms it and that it re-emerges in a public forum or through another channel, so that Alice can analyze it. This can be either because Bob re-distributed it or because Alice sought the model through legal channels, as suggested by Fan \textit{et al.} \cite{10}. For example, many variants of the LLaMA models have been fine-tuned on instruction datasets and been made available online.

\*Correspondance to pfz@meta.com
\textsuperscript{1}Work supported by ANR / AID under Chaire SAIDA ANR-20-CHIA-0011.
2. RELATED WORK & TECHNICAL BACKGROUND

2.1. Deep Neural Network (DNN) Watermarking

DNN watermarking robustly embeds a unique identifier into the model without affecting its performance, in order to later verify the model’s identity. Watermarking should satisfy three criteria: utility: the new model should have the same performance as the original one; security: it should be stealthy, hard to remove and to forge; robustness: the watermark should be detected even after the model has been modified. Modifications may be unintentional – models are fine-tuned, pruned and quantized – or intentional – adversaries may try to remove the watermark or embed their own [11, 12, 13]. For instance, some adversarial transforms employ invariance operations in neurons and ReLU layers to evade detection [14], in a similar fashion as the techniques of this work.

We distinguish between white-box and black-box settings, depending on whether the model weights are accessible at verification time, or only through a remote API. In white-box, the pioneering work [8] embeds watermarks into the DNN’s weights. A regularization loss term during training constrains the weights to carry a specific signal, while minimizing the impact on the model’s performance. The watermark is then retrieved directly by analyzing the model’s weights.

Transformer [24] neural networks have become the standard for many applications in the last few years. They can be trained efficiently on GPUs and scale well to large datasets and models, in both natural language processing [25, 26] and computer vision [6, 7]. In the following we describe the NLP architecture from [27].

The input string is first tokenized into a sequence of integers \(x_1, \ldots, x_n\) \(\in \mathbb{V}^n\). An embedding layer \(E \in \mathbb{R}^{|\mathbb{V}| \times d}\) maps each token \(x_i\) to a continuous vector \(z^d_i = E x_i \in \mathbb{R}^d\), where \(d\) is the embedding dimension. The transformer is a stack of attention and feed-forward layers, that we describe in the following.

**Attention layers.** The self-attention mechanism enables long-range dependencies between sequence elements. A self-attention transforms an input sequence \(z \in \mathbb{R}^{d \times n}\) into queries \(Q\), keys \(K\), and values \(V\):

\[
Q = z W^Q \in \mathbb{R}^{d \times n}; \quad K = z W^K \in \mathbb{R}^{d \times n}; \quad V = z W^V \in \mathbb{R}^{d \times n}.
\]

It then computes attention weights by taking a scaled dot product between the queries and keys:

\[
\text{Attention}(Q, K, V) = \text{softmax} \left( \frac{Q K^T}{\sqrt{d_k}} \right) V.
\]

This attention operator is applied \(h\) times in parallel, yielding \(h\) output heads. The results are concatenated and projected back to the original dimension:

\[
\text{MultiHead}(Q, K, V) = \text{Concat}(\text{head}_1, \ldots, \text{head}_h) W^O,
\]

where \(\text{head}_1 = \text{Attention}(Q W^Q, K W^K, V W^V)\). The projections \(W^Q, W^K, W^V \in \mathbb{R}^{d \times d}\) and \(W^O \in \mathbb{R}^{hd \times d}\) are learned parameters.

The **feed-forward network.** The output is fed to a feed-forward network (FFN), e.g. two linear layers with a ReLU activation:

\[
\text{FFN}(h) = \text{ReLU}(h W_1 + b_1) W_2 + b_2,
\]

where \(W_1 \in \mathbb{R}^{d \times d_l}, b_1 \in \mathbb{R}^{d_l}\), \(W_2 \in \mathbb{R}^{d_l \times d}\) and \(b_2 \in \mathbb{R}^d\) are learned parameters (SwiGLU [28] and other variants also frequently replace ReLU). The **output** is fed to a normalization layer \(L_{out}\) and a linear layer \(W_{out} \in \mathbb{R}^{d \times |\mathbb{V}|}\) to generate logits, and a softmax outputs the probability distribution of the next token.

**Positional embeddings.** For many tasks, it is useful to encode the position of tokens in the input sequence. Positional embeddings are what allows to encode this information. They were originally sinusoidal functions of the position [24] added to the input embeddings. There are now several variants [25, 31, 32, 33], that may change Eq. (2). For instance, rotary embeddings [31] multiply queries and keys depending on their relative position in the sequence. If \(n\) is the position of the query \((Q_m = z_m W^K)\) and \(n\) the position of the key, then it rewrites the product of Eq. (2) as:

\[
Q_m K_n^T = z_m W^Q R_{\theta,n-m} (z_n W^K)^T.
\]

\(R_{\theta,n}\) is a block diagonal matrix with \(2 \times 2\) rotation matrix entries:

\[
(R_{\theta,n})_i = \begin{pmatrix}
\cos n \theta_i & \sin n \theta_i \\
\sin n \theta_i & \cos n \theta_i
\end{pmatrix},
\]

with rotation frequencies chosen as \(\theta_i = 10,000^{-2i/d}\).
**Permutation invariance** appears in (at least) four levels of the transformer. We note \( \Pi^d \) the set of permutations of \([1, \ldots, d]\). For a matrix \( M \in \mathbb{R}^{d \times d} \) and \( \pi \in \Pi^d \), we denote by \( M_{\pi} \) (resp. \( M_{\pi}^- \)) the matrix where columns (resp. rows) are permuted according to \( \pi \).

**Embedding dimension.** The embedding matrix \( E \) can be permuted along its second dimension without changing the output of the model, as long as the permutation is propagated to other matrices in the model. More formally, for \( \pi \in \Pi^d \), if \( E = E_{\pi} \), then matrices \( \{W^1, W^K, W^V, W_1, W_{\text{out}}, \text{Lformer}, \text{Lformer}_b, b_2\} \subset \theta \) need to be permuted along their first dimension by \( \pi \) and all matrices \( \{W^O, W_2\} \) along their second one: \((W^O)^\pi = W_{\pi}^O, (W^O)^{\pi^{-}} = W_{\pi^-}^O, \) etc.

**FFN layer dimension.** All neurons making up matrices \( W_1 \) and \( W_2 \) of feed-forward networks can be permuted: for \( \pi \in \Pi^d \), if \( W_1 = (W_1)_{\pi} \) and \( W_2 = (W_2)_{\pi} \), then \( f_{\theta'}(\cdot) = f_{\theta}(\cdot) \).

**Attention heads.** Because of Eq. 3, heads are interchangeable, provided that \( W^O \) is permuted in blocks of \( d_k \) rows, according to its first dimension. In practice, the \((W^Q)_{i,\pi(1, \ldots, i)}\) are stored as a unique matrix, so permuting the heads is equivalent to permuting the columns of this matrix in blocks of \( d_k \) (same for \( W^K \) and \( W^V \)).

**Inside the head.** Depending on the type of positional embeddings, the previous permutations can be extended. For instance if they do not impact Eq. 2 (this is not the case for rotary embeddings) then \( W^O \) and \( W^K \) can be permuted along their second dimension.

**Scaling/Unscaling.** Whenever layer norms or variants are directly followed (or preceded) by linear layers, e.g. at every attention or FFN block, we can rescale component-wise the parameters \( g, b \) of Eq. 5 by a vector \( \alpha \in \mathbb{R}^d \). Invariance is obtained by dividing the rows of the following (or preceding) linear layers by the same vector.

**Invertible matrices in QK products.** We hereby assume the positional embeddings do not impact Eq. 2. If \( P \in \mathbb{R}^{d_k \times d_k} \) is invertible, then choosing \((W^Q)^P = W^O P \) and \((W^K)^P = W^K (P^{-1}) \) is invariant in Eq. 2. This also applies to the case of rotary embeddings by restricting \( P \) to be block diagonal of \( 2 \times 2 \) matrices that apply a 2D rotations and scaling by a factor \( \lambda \) (thanks to the commutativity of 2D rotations).

**Combining invariants.** All previous parameter transformations may be seen as invertible right or left matrix multiplications applied to the model parameters. For instance, \( \pi \) is associated to a permutation matrix \( P \) such that \( P_{\pi(i)} = 1 \) and \( P_{\pi(j)} = 0 \) otherwise, scalings are diagonal matrix, etc. They do not interfere and may be combined in a sequence of arbitrary order, yielding \( \theta \rightarrow \theta' \rightarrow \theta'' \rightarrow \cdots \).

Combining transformations at all levels improves robustness to intentional removal attacks and to collusion (i.e. when several Bobs share their weights to evade detection). Indeed, if Bob tries to remove the watermark by re-applying one invariant, it will still be present in the other invariants. In the same way, if several Bobs compare their models, it will be hard for them to identify which operations were applied to their models, since the order in which they were applied is unknown, and since the weights will differ a lot between them.

### 3.2 From invariants to watermarks

**Insertion.** Before starting the watermark process, for each invariant and each level of the network, we restrict the set of transformations to \( 2^d \). For example, we randomly sample \( 2^d \) possible permutations in \( \Pi^d \) for the Embedding dimension (out of the total \( d \)!). This is to simplify the detection procedure.

Therefore, we can encode \( k \) bits for each combination of an invariant and a level. Thus, we encode a model’s identifier as the concatenation of \( m \) chunks of \( k \) bits (\( 2^{mk} \) possibilities). For instance, let \( k = 4 \) and the model have 32 layers. We choose to embed two permutations per layer, one for the attention block and one for the FFN block. The total number of bits is \( 2 \times 32 \times 4 = 256 \), representing \( 10^{77} \) possible models (approximately the number of atoms in the universe, an upper bound of the number of Bobs). This embedding process provides robustness and efficiency when extracting the watermarks.

**Extraction.** The brute-force way to extract the \( k \)-bits message from a weight matrix is to re-apply all \( 2^k \) possible invariants to the original matrix. Then we compute the Frobenius norm of the difference between the observed weight and the possible watermarked ones. We choose the one with lowest among the \( 2^k \) and this choice is encoded as a \( k \)-bit integer. Doing that on every blocks of the network and every invariant, we end up with a full message made of \( m \) chunks of \( k \) bits. In the case of intertwined invariants, we do the same in the order in which we inserted the invariants, reverting them as we go.

To speed up extraction, we may select a subset of the matrices’ rows before extraction. This speeds up the extraction (in the order of \( 10^2 \times \)), but makes the detection slightly less robust. For instance, in the case of scaling/unscaling we may select the first 100 components of \( \alpha \) from \( \mathbb{R}^d \) to \( \mathbb{R}^{100} \) and \( W \) from \( \mathbb{R}^{d \times d'} \) to \( \mathbb{R}^{100 \times 100} \).

**Matching.** To match an extracted message (made of \( m \) chunks of \( k \) bits) with a model’s identifier, we compute the number \( s \) of chunk-wise errors with respect to all possible identifiers. We return a match if \( s \) is bellow a fixed threshold \( \tau \) to ensure resilience to corruption and to provide a confidence score. A theoretical \( p \)-value, i.e. the probability of obtaining a number of errors lower than \( s \) for a random model, is given by the regularized incomplete beta function \( I \):

\[
p\text{-value}(s) = 1 - \left(1 - I_{1/2^k}(m - s, s + 1)^N\right),
\]

where \( N \) is the number of distributed models. \( N \) accounts for the fact that when multiple models are distributed, the risk of finding a match by chance is higher.

**Robustness and security.** Watermarking models through invariance is stealthy, because it does not change their outputs and does not leave artifacts in the weights. However, a distortion-free watermark is also a weakness. On the one hand, Alice can hide the watermark without impacting the model’s utility, on the other hand, an adversarial Bob may do the same at no cost. In short, most of these watermarks are very robust against classical model manipulations (fine-tuning, quantization, etc.) but not against a malicious user who knows the method. In this case we would only know that the model is an unauthorized copy, without knowing the leaker.

### 4. EXPERIMENTS

The purpose of the experiments is to evaluate the effectiveness and the robustness of the watermarks to transformations on transformers, in the context of large language models.

#### 4.1 Setup

**Model.** We use LLaMA [2] models as main benchmark. The architectural differences with regards to the original transformer architecture are pre-normalization [27] with RMSnorm [30], SwiGLU activation [28] and rotary embeddings [31]. Unless stated otherwise, we use the 7B-parameter model. To evaluate that the utility of the model is not degraded, we show results on a next-token prediction task. This is done on random sequences of text taken from Wikipedia, then tokenized using the default tokenizer of LLaMA.
4.2. Results.

Robustness. We evaluate the robustness of the watermark using the byte accuracy, i.e. the percentage of bytes correctly recovered. Results are averaged over N=100 watermarked models except for fine-tuning where we only fine-tune one model. The model has L=32 layers so the watermark is 64 bytes long except for the QK products invariant where it is 32. In the case of combined invariants, the total number of bytes is 160. We speed-up the extraction by selecting a subset of 100 rows of the matrices (see Sect. 3.2); time needed for extraction is around 20 minutes when using the full matrix instead.

Table 1 reports the byte accuracy for different processing applied before extraction. We observe that the watermark is robust to all attacks with byte accuracy >50%. Errors mainly come from the speed-up of the extraction process. We also consider the p-value of the associated statistical test (see Eq. 9). A byte accuracy of 50% on 64-bytes messages is more than enough to reliably identify a model: the p-values are always bellows 10^{-60}, due to the very low probability of simultaneously observing a match between tens of pairs of random bytes. As an illustration, 8 matching bytes on 64-bytes messages already gives a p-value of 10^{-8}.

<table>
<thead>
<tr>
<th>Method</th>
<th>Distortion</th>
<th>Byte accuracy (%) on:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Noise 1.0</td>
<td>Quant. 3b</td>
</tr>
<tr>
<td>Perm.</td>
<td>0.20%</td>
<td>51.4 (99.6)</td>
</tr>
<tr>
<td>QK</td>
<td>0.18%</td>
<td>100.0</td>
</tr>
<tr>
<td>Scaling</td>
<td>0.24%</td>
<td>100.0</td>
</tr>
<tr>
<td>All</td>
<td>1.77%</td>
<td>60.8 (99.8)</td>
</tr>
</tbody>
</table>

Table 1: Distortion induced on generation (measured as the proportion of generated tokens that differ between the original and the watermarked model); and robustness of watermark extraction under various processes. Each line stands for a different invariant, “all” is the combination of the three invariants in the following order: perm, QK and scaling. We present results of the speed-up extraction, the ones for no speed-up are given as (acc).


