PROVISIONAL APPLICATION FOR PATENT

Under 35 U.S.C. §111(b)

Title of Invention: SYSTEM AND METHOD FOR DETECTING AND DEFENDING AGAINST MASS-FILED, AI-GENERATED PATENT CLAIMS TARGETING INDEPENDENT INVENTORS

Inventor: Jonathan Wren

Filing Date: March 28th, 2026

Correspondence Address: [REDACTED]

SPECIFICATION

TITLE OF THE INVENTION

SYSTEM AND METHOD FOR DETECTING AND DEFENDING AGAINST MASS-FILED, AI-GENERATED PATENT CLAIMS TARGETING INDEPENDENT INVENTORS

FIELD OF THE INVENTION

The present invention relates generally to artificial intelligence systems for intellectual property defense. More specifically, the invention relates to a system and method for detecting, analyzing, and defending against mass-filed, AI-generated patent applications that target independent inventors and small entities through broadly worded, speculative claims filed by non-practicing entities (patent trolls).

BACKGROUND OF THE INVENTION

The United States Patent and Trademark Office (USPTO) confirmed in revised guidance issued November 2025 that artificial intelligence cannot be named as an inventor on a patent application. Under current law, AI is classified as a tool, and only the human who directed the AI's contribution may be listed as the inventor. While this guidance was intended to clarify inventorship standards, it has created an unintended consequence that fundamentally threatens the patent system's purpose of protecting genuine innovation.

Specifically, this guidance enables the following exploit: a human operator uses generative AI to produce thousands of broadly worded, thinly plausible patent claim variations across multiple technology domains. The human lists themselves as the sole inventor on each application. Because AI has reduced the cost of generating patent-quality language to near

zero, a single operator can file at scale what previously required teams of patent attorneys and months of effort. These filings are not accompanied by working prototypes, products, or any commercial activity. They exist solely as legal instruments designed to ensnare independent inventors who, working without knowledge of these filings, independently arrive at similar ideas through their own legitimate research and development.

This practice is commonly known as patent trolling when conducted by non-practicing entities (NPEs). Recent data indicates that NPEs account for more than half of all AI-related patent litigation, that one in five NPE lawsuits in the technology sector is now AI-related, and that startups are targeted at approximately twice the rate of established companies because trolls calculate that small entities cannot afford to mount a defense. The average cost of defending a patent infringement lawsuit through trial exceeds $2 million, creating an asymmetry that economically coerces settlements regardless of the merits of the claim.

Existing systems for patent analysis and invalidation are designed for enterprise use. They require substantial technical expertise, access to patent counsel, and budgets that are inaccessible to independent inventors and small entities—the very population most vulnerable to mass-filed AI-generated claims. There is no existing system that provides proactive, consumer-accessible defense against the specific pattern of AI-enabled mass patent filing.

The present invention addresses this gap.

SUMMARY OF THE INVENTION

The present invention provides a system and method for detecting, analyzing, and defending against mass-filed, AI-generated patent claims. The system is specifically designed to be accessible to independent inventors, small businesses, and individual entrepreneurs who lack the resources to retain patent counsel or subscribe to enterprise-grade patent analytics platforms.

The system comprises the following core functional components:

(a) A Troll Pattern Detection Engine that analyzes patent filings to identify characteristics associated with mass-filed, AI-generated, speculative claims. Detection criteria include but are not limited to: filing volume anomalies (single filers submitting abnormally high numbers of applications across unrelated technology domains); claim breadth analysis (identifying claims drafted with intentionally broad language designed to maximize future infringement surface area); entity classification (determining whether the filer is a practicing entity with products or services, or a non-practicing entity with no commercial activity); temporal patterns (detecting rapid sequential filings suggesting automated generation); linguistic fingerprinting (identifying stylistic markers consistent with AI-generated patent language rather than human-drafted claims); and absence of corresponding product, prototype, or commercial activity by the filer).

(b) An Independent Inventor Risk Assessment Module that accepts a natural language description of an invention, idea, or product concept from a user and performs real-time comparison against the database of flagged troll-pattern patents. The module returns a risk score indicating the probability that the user's concept overlaps with one or more existing mass-filed claims, identifies the specific claims that present risk, and provides a plain-language explanation accessible to non-patent-professionals.

(c) A Defensive Prior Art Package Generator that, upon detection of overlap between a user's concept and one or more flagged troll-pattern patents, automatically compiles a prior art package. This package includes identified prior art references that predate the flagged patent's filing date, analysis of the flagged claims' vulnerability to invalidity challenges (including obviousness under 35 U.S.C. §103 and lack of enablement under 35 U.S.C. §112), a summary report formatted for use in response to a demand letter or cease-and-desist communication, and template response language for pro se (self-represented) inventors.

(d) A Crowdfunded Public Utility Model wherein the system operates as a publicly funded, non-exclusive resource. The system is designed to be funded through public crowdfunding mechanisms. The patent holder commits, as a condition of the public funding, to never enforce the patent offensively against any entity using similar technology for non-commercial defensive purposes. The patent exists solely to prevent any other entity from patenting the same defensive methodology and enforcing it in a manner that restricts access. Revenue generated through enforcement actions against entities that attempt to patent and offensively enforce similar defensive systems is recycled into the public fund to maintain operations and sustain the patent through its maintenance fee lifecycle. Any surplus funds are directed to a designated charitable organization.

DETAILED DESCRIPTION OF THE INVENTION

System Architecture

The system comprises a cloud-based or locally deployed software platform with the following interconnected modules:

Patent Filing Monitor: A continuous monitoring service that ingests newly published patent applications from the USPTO, EPO, WIPO, and other patent offices via their respective public APIs and bulk data feeds. The monitor indexes new filings in near-real-time and feeds them to the Troll Pattern Detection Engine for analysis.

Troll Pattern Detection Engine: A machine learning system trained on historical patent filing data, specifically on features that distinguish mass-filed speculative patents from legitimate innovation-backed filings. The engine assigns a Troll Probability Score (TPS) to each analyzed filing based on a weighted combination of the following features:

(i) Filing Volume: Number of applications filed by the same entity or associated entities within a rolling time window, normalized against industry baselines.

(ii) Domain Dispersion: The degree to which an entity's filings span unrelated CPC (Cooperative Patent Classification) codes, indicating breadth-for-breadth's-sake rather than focused R&D.

(iii) Claim Breadth Index: A natural language processing (NLP) metric that scores the specificity of independent claims, where broader and more abstract language receives a higher score.

(iv) Commercial Activity Correlation: Cross-referencing the filer against business registries, product databases, SEC filings, and web presence to determine whether the entity manufactures, sells, or develops products or services related to its filings.

(v) Linguistic Fingerprinting: Stylometric analysis comparing claim language against known AI-generation models to identify patterns consistent with automated drafting tools, including repetitive structural patterns, vocabulary distribution anomalies, and syntactic uniformity across filings.

(vi) Litigation History: Whether the filing entity or its related entities have a history of patent infringement lawsuits, demand letters, or licensing campaigns without corresponding product activity.

Risk Assessment Module: An interface through which a user inputs a plain-language description of their invention concept. The module uses semantic similarity analysis (employing transformer-based NLP models) to compare the user's description against all patents flagged with a TPS above a configurable threshold. The output includes a risk score (0–100), a list of flagged patents ranked by overlap probability, highlighted claim elements that present the greatest risk, and suggested modifications to the user's concept that could reduce overlap.

Defensive Prior Art Generator: Upon identification of risk, this module automatically searches prior art databases (including but not limited to USPTO, Google Patents, Google Scholar, arXiv, IEEE, ACM, GitHub public repositories, and the Internet Archive Wayback Machine) for publications, products, or disclosures that predate the flagged patent's effective filing date. The generator compiles a downloadable prior art package that includes bibliographic references, relevance explanations, claim-by-claim mapping, and template legal language suitable for responding to a demand letter without legal representation.

Automated Enforcement Module: In the event that a third party patents a substantially similar defensive system and attempts to enforce it against independent inventors or small entities in a manner inconsistent with the public utility purpose of the present invention, this

module provides automated detection of such enforcement actions through court filing monitors and patent assignment databases. Upon detection, the module generates a litigation assessment, identifies the present patent as prior art, and facilitates coordinated defense funded by the public utility fund.

Differentiation from Prior Art

The present invention is distinguished from existing patents and systems in the following ways:

From US6049811A and US8041739B2 (automated patent drafting): Those patents address the creation of patent applications. The present invention addresses the detection and defense against abusive patent filings. The systems operate in opposite directions—one generates patents, the other identifies and neutralizes exploitative ones.

From US11966688B1 (AI-based patent drafting): That patent uses AI to draft patent claims from inventive concepts. The present invention uses AI to analyze existing claims for patterns of abuse and generate defensive countermeasures. There is no functional overlap.

From commercial patent analytics platforms (Patlytics, XLSCOUT, etc.): Existing platforms are enterprise-grade, require patent expertise, operate reactively (after litigation begins), and are priced for corporate legal departments. The present invention is consumer-grade, operates proactively (before litigation), requires no patent expertise, and is funded as a public utility.

Public Utility and Non-Enforcement Covenant

The inventor intends, and by the filing of this application memorializes the intent, that this patent shall operate as a public utility. The patent shall not be enforced against any individual, small business, open-source project, academic institution, or nonprofit organization using similar methods for non-commercial defensive purposes. Enforcement shall be pursued only against entities that (a) patent substantially similar defensive systems and (b) attempt to enforce such patents in a manner that restricts access to defensive tools by independent inventors or small entities. All net proceeds from any such enforcement action shall be directed first to the maintenance and operation of the public utility system, and any surplus shall be donated to a designated charitable organization.

CLAIMS

What is claimed is:

A computer-implemented method for detecting and defending against mass-filed, AI-generated patent claims targeting independent inventors, the method comprising:

receiving, by a processor, patent filing data from one or more patent office databases;

analyzing, by a troll pattern detection engine executing on the processor, each patent filing to compute a Troll Probability Score based on a plurality of detection criteria including filing volume anomalies, claim breadth analysis, entity commercial activity correlation, cross-domain filing dispersion, linguistic fingerprinting for AI-generated language patterns, and litigation history;

flagging patent filings that exceed a configurable Troll Probability Score threshold;

receiving, through a user interface, a natural language description of an inventive concept from an independent inventor or small entity;

performing, by a risk assessment module, semantic similarity analysis comparing the natural language description against flagged patent filings to generate a risk score and identify overlapping claims;

generating, by a defensive prior art generator, a prior art package comprising identified references predating the flagged patent filing date, claim-by-claim vulnerability analysis, and template response language for use by a non-legally-represented inventor; and

delivering the risk score, identified overlapping claims, and prior art package to the user through the user interface.

The method of claim 1, wherein the linguistic fingerprinting comprises stylometric analysis comparing claim language against known AI text generation patterns including repetitive structural patterns, vocabulary distribution anomalies, and syntactic uniformity across filings by a common entity.

The method of claim 1, wherein the claim breadth analysis comprises a natural language processing metric that scores the specificity of independent claims on a continuous scale, wherein broader and more abstract claim language receives a higher score.

The method of claim 1, wherein the entity commercial activity correlation comprises cross-referencing the filing entity against business registries, product databases, public financial filings, and web presence data to determine whether the entity produces goods or services related to its patent filings.

The method of claim 1, wherein the risk assessment module outputs one or more suggested modifications to the user’s inventive concept that would reduce overlap with flagged patent claims.

The method of claim 1, further comprising monitoring court filings and patent assignment databases to detect enforcement actions by third parties holding patents on substantially

similar defensive systems, and generating automated litigation assessments in response to detected enforcement actions.

A system for proactively defending independent inventors against mass-filed patent claims, the system comprising:

a patent filing monitor configured to continuously ingest newly published patent applications from one or more patent office databases;

a troll pattern detection engine comprising a machine learning model trained to assign a Troll Probability Score to each ingested filing based on filing volume, domain dispersion across classification codes, claim breadth, commercial activity correlation, linguistic fingerprinting, and litigation history;

a risk assessment module configured to receive a natural language invention description from a user and perform semantic similarity comparison against filings exceeding a Troll Probability Score threshold;

a defensive prior art generator configured to automatically compile prior art references, claim vulnerability analyses, and template response language; and

a user interface configured to present the risk score, overlapping claims, and defensive prior art package in plain language accessible to users without patent expertise.

The system of claim 7, wherein the system is deployed as a publicly funded utility and the patent holder commits to a non-enforcement covenant prohibiting offensive enforcement against individuals, small businesses, open-source projects, academic institutions, or nonprofit organizations using similar methods for non-commercial defensive purposes.

The system of claim 7, wherein the troll pattern detection engine is further configured to detect temporal filing patterns indicative of automated batch generation, including abnormally uniform filing intervals and clustered submission timestamps.

The system of claim 7, further comprising an automated enforcement module configured to monitor for third-party patents covering substantially similar defensive systems and to generate coordinated defense materials when such patents are enforced against independent inventors or small entities.

ABSTRACT

A system and method for detecting and defending against mass-filed, AI-generated patent claims that target independent inventors and small entities. The system monitors patent office filings in near-real-time, applies a machine-learning-based Troll Pattern Detection Engine to identify filings exhibiting characteristics of speculative mass-filing (including filing volume

anomalies, overbroad claim language, cross-domain dispersion, absence of commercial activity, AI linguistic fingerprints, and litigation history), and assigns a Troll Probability Score to each filing. Independent inventors input natural language descriptions of their inventive concepts through a consumer-accessible interface, and a Risk Assessment Module performs semantic similarity analysis against flagged filings to generate risk scores and identify overlapping claims. A Defensive Prior Art Generator automatically compiles prior art packages including references, claim vulnerability analyses, and template response language for use by non-legally-represented inventors. The system operates as a crowdfunded public utility with a non-enforcement covenant, wherein the patent is enforced only against entities that patent similar defensive systems and restrict access to defensive tools. Net enforcement proceeds sustain the public utility and fund a designated charitable organization.