GLITCH-SHIELD: Reclaiming the Digital Face of Equality

Proactive Adversarial Defence against Non-Consensual AI Content.

In 2026, a woman's face should not be a liability. We are making it unhackable.

GLITCH-SHIELD

Adversrial AI Defense for Digital Identity Sovertginty

The New Frontier of Gender-Based Violence.

01

The Statistic: 90% of deepfake content online is non-consensual and targets women.

02

The Impact: It is used to silence journalists, harass students, and blackmail professionals.

03

The Gap: Current laws are reactive; they only help *after* the video is viral and the damage is done.

Safety-by-Design: Moving from Reaction to Prevention.

Concept: Instead of chasing deepfakes, we poison the data they are built from.

The Glitch: Invisible mathematical noise (Adversarial Perturbations) that breaks AI facial mapping without changing the photo's look for humans.

The Motto: "Your eyes see a portrait; the AI sees a brick wall."

The Three-Layer Defence Protocol.

Layer 1 (The Cloak): Adversarial noise injection at the pixel level.

Layer 2 (The Vault): On-device encryption ensures no raw (vulnerable) images are accidentally leaked.

Layer 3 (The Ledger): Blockchain-hashed Proof of Origin for instant copyright and takedown validation.

Impact & The 2025/2030 Agenda

SDG 5: Achieving gender equality by removing digital barriers.

SDG 9: Innovative infrastructure that meets the specific needs of women.

Vision: Enabling women to lead in politics, media, and tech without fear of digital character assassination.

The Roadmap & Implementation

PHASE 1: MOBILE APP FOR INDIVIDUAL PROTECTION (JOURNALISTS/ACTIVISTS).

PHASE 2: API INTEGRATION FOR SOCIAL MEDIA PLATFORMS TO "AUTO-SHIELD" FEMALE USERS.

PHASE 3: GLOBAL STANDARD FOR "PROTECTED IDENTITY" METADATA.

Timeline

Phase	Milestone	Duration	Key Activities
Phase 1	**Research & Feasibility**	1 Month	Analyze current adversarial AI models and finalize legal compliance frameworks.
Phase 2	**Core Algorithm Dev**	3 Months	Develop the Adversarial Perturbation Engine to "cloak" images.
Phase 3	**Prototype (PoC)**	2 Months	Build the "Identity Vault" interface and conduct initial stress tests.
Phase 4	**Testing & Hashing**	3 Months	Integrate blockchain-based "Proof of Origin" and perform security audits.
Phase 5	**User Testing & Beta**	2 Months	Run pilot programs with at-risk female journalists to refine UX.
Phase 6	**Global Launch**	1 Month	Deploy to app stores and release the public API for platform integration

Budget

- **Total Estimated Budget: $85,000 – $120,000**
- **Engineering & R&D ($40k – $60k):** Covers the salaries of specialized data scientists and backend engineers to build the "AI-poisoning" logic.
- **Infrastructure & Cloud ($15k – $25k):** High-performance GPUs for training the adversarial models and secure database storage.
- **Data Acquisition & Cleaning ($10k – $15k):** Curating diverse datasets to ensure the "shield" works for all ethnicities and lighting conditions.
- **Security & Compliance Audits ($10k – $15k):** Essential third-party validation to ensure the "Proof of Origin" ledger is unhackable.
- **Design & UX ($5k – $10k):** Creating a "Zero-Trace" interface that is intuitive and discreet for users in high-risk zones.

Thank you