

Insurance Connect — 11 Giugno 2026

AI Fraud Detection nel ciclo assicurativo

AI deepfake detection per il settore assicurativo

Gianmarco di Campi — CEO, Claim Expert®

Marco Castaldo — CEO & Co-founder, identifAI



Chi è identifAI®

Deepfake detection di video, audio, immagini per proteggere le organizzazioni ed i business dai rischi e dalle frodi dell'era dell'IA Generativa

identifAI

Piattaforma tecnologica all'avanguardia che utilizza modelli avanzati di intelligenza artificiale "de-generativa" per distinguere tra contenuti creati dall'uomo e artefatti generati dall'IA.

Mission

Garantire trasparenza, affidabilità e responsabilità nel mondo dell'informazione digitale, fornendo strumenti scientificamente solidi per distinguere tra contenuti autentici e contenuti generati artificialmente.

In un ecosistema digitale in rapida evoluzione, identifAI adotta un modello dinamico e adattivo, perché le difese statiche non sono più sufficienti.

Competitive Edge

- Modelli proprietari, completamente sviluppati in-house
- Team di ricerca attivo che produce pubblicazioni scientifiche
- Tecnologia facile da integrare e adattabile allo specifico caso d'uso
- Cybersecurity approach



CYBERSECURITY APPROACH

Affrontiamo i rischi dell'IA generativa come un **problema di cybersecurity**, non come un compito statico di classificazione di Machine Learning.

Il nostro approccio si basa su una vera e propria **"prospettiva da hacker"** nella risoluzione del problema del riconoscimento dei contenuti generati dall'IA.

Questo si traduce nello sviluppo continuo di nuovi modelli di detection per rispondere velocemente al rilascio di nuovi generatori che potrebbero essere usati a fini di frode.

I modelli e le euristiche vengono adattati ai singoli use cases per ottenere sempre il **massimo livello di accuracy** raggiungibile ed offrire output affidabili, interpretabili e contestualizzati.

La frode digitale nell'era dell'AI

Il contesto in cui operiamo — 2024-2026



Il settore assicurativo è il secondo più colpito dalle frodi digitali in Europa. La diffusione e l'accessibilità (anche economica) degli strumenti AI generativa ha abbassato la barriera di ingresso per i frodatori, rendendo la detection un'infrastruttura critica — non più un'opzione.

92%

delle aziende ha subito almeno un caso di identity fraud negli ultimi 12 mesi
(Regula Deepfake Research Report, 2024)

+2.137%

tentativi di frode deepfake negli ultimi 3 anni
(Signicat AI Fraud Report, 2025)

10%

dei costi dei sinistri in Europa sono attribuibili a frodi (rilevate)
(Insurance Europe — The Impact of Insurance Fraud)

\$600.000

perdita media per incidente deepfake nel settore finanziario
(Regula Deepfake Research Report, 2024)

\$2.190.000.000

perdite globali da deepfake fraud nel 2026
(Digital Information World, apr. 2026)

«We used to get about one deepfake a month. Now we're seeing seven attacks per customer every day.» — Vijay Balasubramaniyan, CEO Pindrop

3 livelli di analisi — Claim Expert × identifAI

01 Core Analysis

- Deepfake detection
Rileva se il contenuto è generato o manipolato con AI
- Origin scoring 0–10
(Human / Artificial)
- Punteggio per ogni file
Score dedicato per foto, video e documenti

02 Metadata & Provenance

- Analisi EXIF e metadati
Data di creazione, dispositivo e software utilizzato
- Catena di custodia digitale
Storia digitale del file: modifiche, passaggi, trasmissioni
- Watermark e fingerprint
Tracce invisibili lasciate dal dispositivo originale

03 Media Forensics

- Tampering detection + heatmap
Individua l'area modificata e la evidenza visivamente
- Analisi video frame by frame
Per i video: analisi fotogramma per fotogramma
- Scoring per tipo di media
Score differenziato per foto, video e documenti

Web app — operatività immediata, score in secondi, zero integrazione

API — integrazione nel claims management system esistente

Chi è Claim Expert®

Outsourcing assicurativo d'eccellenza — dal 2009

+65.000 pratiche gestite

Anno 2024-2025. Gestione completa sinistri e antifrode assicurativa.

+30 professionisti dedicati

Team dedicati e metodologie analitiche avanzate per efficienza operativa e SLA ottimizzati.

+6 Compagnie assicurative partner

Mission: trasformare le esigenze dei Clienti in obiettivi concreti e misurabili.



Fondata nel 2009, Claim Expert opera nel settore dell'**outsourcing assicurativo**, collaborando con primarie compagnie. Offre servizi di **gestione completa dei sinistri** e **antifrode assicurativa**, attraverso team dedicati e metodologie analitiche avanzate, garantendo **efficienza operativa** e **tempistiche ottimizzate** rispetto ai modelli organizzativi tradizionali.

MISSION

Servizi di eccellenza basati su **professionalità, precisione e proattività**, trasformando le esigenze dei Clienti in obiettivi concreti e misurabili.

ABOUT US

Il ciclo assicurativo si è digitalizzato.

L'affidabilità delle evidenze digitali non si è adeguata.

I documenti arrivano in formato digitale — ma nessuno ne verifica l'autenticità.



Foto del sinistro



Documento d'identità



Video dashcam

Perché l'analisi tradizionale non basta

01 L'occhio umano non basta

Le AI generative producono immagini con una coerenza visiva superiore alla soglia di percezione umana.

02 Nessuno strumento nativo per EXIF nei workflows liquidativi

Metadati, inconsistenze di compressione e catena di custodia: invisibili nelle attuali piattaforme per Compagnie.

03 Il voice cloning supera qualsiasi verifica telefonica

Un clone vocale chiama il call center. Nessun operatore lo identifica come falso. I sistemi di riconoscimento vocale tradizionali non sono progettati per questo.

04 La media forensics manuale non è scalabile

Analizzare ogni file ricevuto è operativamente impossibile. Il problema non è la competenza — è il volume.

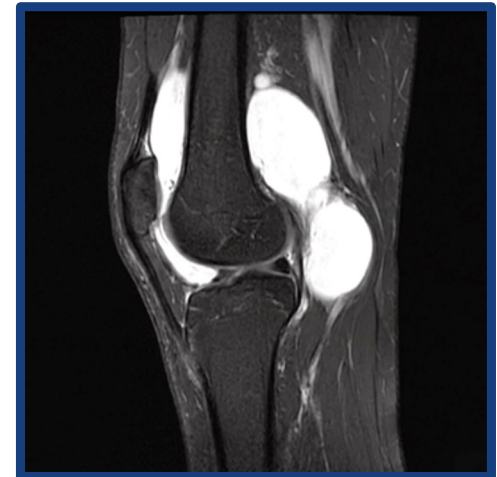
Quale di questi esempi è autentico?



A



B



C



Nessuno.

Tutti e tre gli esempi sono generati o manipolati con AI.

Veicolo — modificato con AI — 85% Tampering

Carta d'identità — sintetica — 99.83% Artificiale

Radiografia — manipolata — 95.71% Artificiale



Origin:
Artificial

Artificial score: 4/10

Full sample

Metadata

Intelligence

Media Forensic

Tampering Analysis

Ellen





CASO 1 — FOTO VEICOLO MANIPOLATA

4/10

Score medio — Rilevazione confermata

85%

Analisi *Tampering* artificiale (Ellen I)

Foto del sinistro reale, poi modificata con AI per rimuovere i danni visibili. L'immagine mostra lo stesso veicolo — stessa targa, stessa angolazione.

Paraurti, cofano, fanalino — tutto cancellato digitalmente. La vettura non è mai stata riparata.

Lo stesso veicolo. Due versioni. Un solo sistema che le distingue.



Originale — Umano 0/10



AI-modificata — Tampering 4/10

10/10

Artificiale

99.83%

probabilità artificiale (Revelio IV + Arde)

Carta d'identità italiana interamente generata con AI.
Vista isolata: indistinguibile da un documento autentico.

Nome, foto, ologramma, numero seriale — tutto sintetico.





Origin:
Artificial

Artificial score: **10/10**

Full sample

Metadata

Heatmap

Face detection

Intelligence

Full sample artificial score: **10/10**

Revelio IV stated that content is **99.83% artificial**

Revelio IV



ⓘ

Ardē



ⓘ



10/10

Artificiale

95.71%

probabilità artificiale (Revelio IV)

Radiografia autentica di ginocchio modificata con AI: strutture ossee e fluido sinoviale alterati per simulare una patologia inesistente.



Origin:
Artificial

Artificial score: **10/10**

Core

Metadata & Provenance

Core artificial score: 10/10

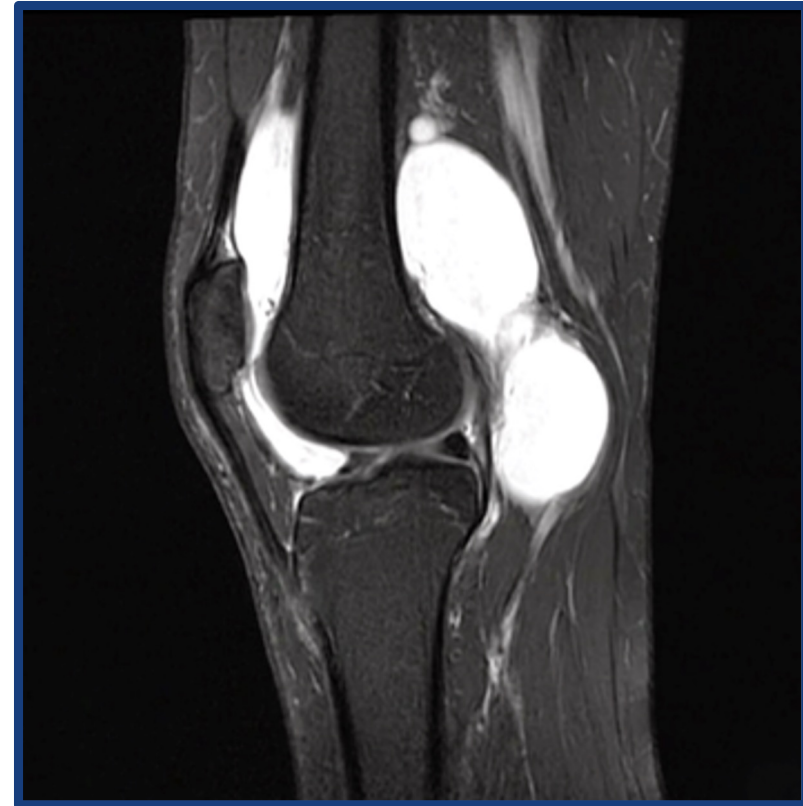
Revello IV stated that content is 95.71% **artificial**

Revello IV





Originale — Umano 0/10



AI-modificata — Artificial Score 10/10



10/10

Artificiale

95.71%

probabilità artificiale (Arde)

Piede reale: l'AI inserisce placche e viti chirurgiche mai impiantate.

Una mappa di calore individua esattamente l'area alterata.

Intervento mai eseguito.

sottocarico

R

Origine: Artificiale

Punteggio artificiale : 10/10

Campione completo Metadati Mappa di calore Intelligenza Anali

Punteggio artificiale della mappa di calore: 6/10

Ardo

Mappa di colore ✓ Immagine ✓



CASO 5 — VIDEO ANALIZZATO PER FOTOGRAMMI

4/10

Score medio — Rilevazione confermata

98.99%

artificiale (Revelio V)

Dashcam suddiviso in 5 fotogrammi, ciascuno analizzato singolarmente da Revelio V.



Rilevazione confermata nonostante score complessivo basso. Applicabile anche ad audio e voice cloning.



Origine: **Umano** Punteggio artificiale: **4 /10**

Campione completo Metadati Media forensic

Punteggio artificiale del campione completo: 4/10

Revelio V ha affermato che il contenuto è **artificiale al 98,99%**

Revelio V

98.99%

Come si implementa la detection senza rallentare i processi?

Web App

- Nessuna integrazione richiesta
- Operativo da subito per fraud team e uffici sinistri
- Carica il file → score in pochi secondi
- Ideale per avviare il presidio senza attese

API — Fasi strutturate

- 1. Enrichment automatico**
Score allegato all'apertura di ogni pratica
- 2. Trigger su soglie**
Escalation automatica sopra la soglia di rischio
- 3. Integrazione full**
Embedded nel claims management system esistente

I *Workflows* non cambiano. Vengono potenziati.

La AI detection
non è un'opzione.

È infrastruttura.

Claim Expert® e identifAI supportano le Imprese assicurative a costruire i processi di detection.

