LABEL4.AI

La technologie au service de la confiance numérique

Deeptech française spécialisée dans l'authenticité et la traçabilité des contenus numériques



Deux expertises complémentaires

Détection forensique

Identifier les contenus générés ou manipulés par IA, même en l'absence de traces visibles.

Tatouage numérique

Insérer une empreinte invisible et robuste pour identifier et tracer les contenus.

Un ancrage scientifique et institutionnel

Inria / cnrs	Technologies issues de travaux de recherche Inria / CNRS.
Commission européenne	Participation aux travaux de la Commission européenne sur la transparence des contenus générés par IA (AI Act, article 50).
OCDE	Contribution aux travaux de l'OCDE sur l'authentification et la provenance des contenus (Processus d'Hiroshima).
Frontria	Participation au consortium international Frontria, coordonné par Fujitsu.

Détecter les manipulations. Protéger l'authenticité. Renforcer la confiance.

LABEL4.AI

L'IA générative bouleverse notre rapport à l'image

Des contenus de plus en plus réalistes, massifs et faciles à produire, qui fragilisent la confiance.



Un changement d'échelle

Des contenus très réalistes

Une production massive et à faible coût

Une diffusion instantanée et mondiale

Des risques majeurs

Désinformation

Manipuler l'opinion, semer le doute.

Deepfakes

Usurpation d'identité, atteinte à la réputation.

Falsifications

Images et vidéos truquées ou sorties de leur contexte.

Atteinte aux droits

Détournement de contenus, violation de la propriété intellectuelle.

Une crise de confiance qui touche les institutions, les médias et nos sociétés.

LABEL4.AI

Pourquoi il devient impossible de se fier à ce que l'on voit

Des images trompeuses de plus en plus crédibles et difficiles à vérifier avec les méthodes traditionnelles.



Les méthodes traditionnelles atteignent leurs limites

Œil humain

Inefficace face au réalisme de l'IA.

Recherche inversée

Ne détecte pas les images générées ou retouchées.

Détection algorithmique

Performante mais non infaillible, dépendante des modèles et des données.

Le problème de la preuve

Même lorsqu'un contenu est identifié comme faux, il reste difficile de prouver son origine, ses modifications et son parcours de diffusion.

La vérification a posteriori ne suffit plus : il faut aussi pouvoir authentifier et tracer l'origine.



LABEL4.AI

Deux approches complémentaires : détecter le faux, protéger le vrai

Une chaîne de confiance complète pour identifier les manipulations et garantir l'authenticité des contenus.

Décrypter et détecter

Analyse forensique

Identifier un contenu généré ou manipulé par IA
en analysant ses traces techniques.



Authentifier et tracer

Tatouage numérique (watermarking)

Insérer une empreinte invisible, robuste et persistante
pour identifier, attribuer et tracer le contenu.



Des technologies complémentaires

Une authentification fiable et durable

Une traçabilité sur tout le cycle de vie

Un atout pour les droits et la propriété intellectuelle

Détection et tatouage numérique se renforcent pour une information vérifiable et traçable.

LABEL4.AI

Le tatouage numérique : une empreinte invisible au cœur du contenu

Une technologie qui insère un signal robuste et discret pour identifier, authentifier et tracer une image ou une vidéo.



Comment ça fonctionne ?

Contenu (d'image, vidéo...) › **Insertion du tatouage** (invisible) › **Contenu tatoué** (inaltérable) › **Vérification et identification** (à tout moment)

Une empreinte robuste

Recadrage | Compression | Retouches | Capture d'écran | Impression / scan | Réencodage (vidéo)

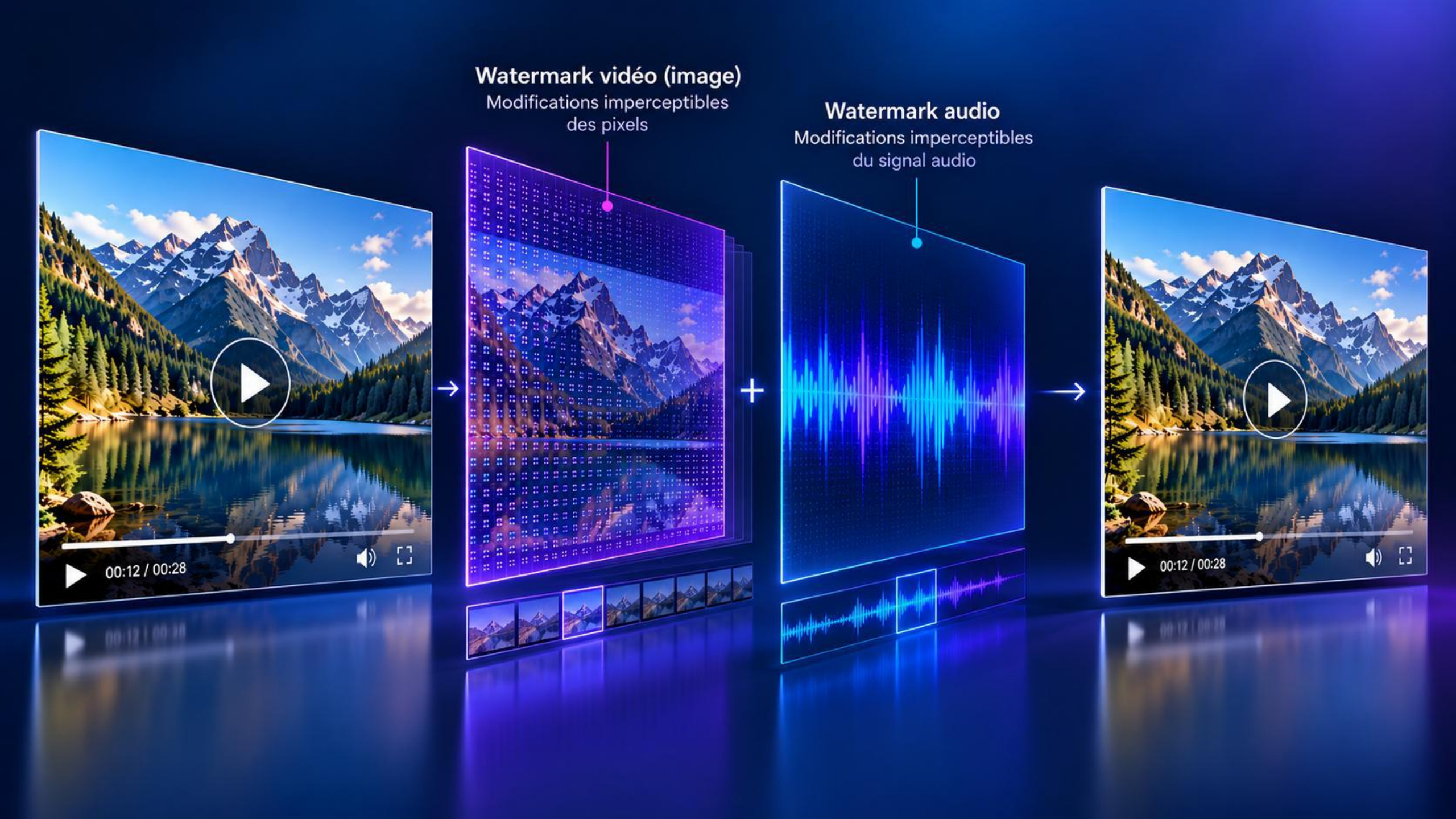
En complément, la provenance

Compatibilité avec les standards de provenance (ex. C2PA) pour documenter l'origine, l'auteur, la date et les modifications.

Une couche technique qui s'ajoute aux métadonnées et signatures cryptographiques.

Une identité durable, qui reste présente même lorsque l'image circule, se transforme ou se copie.




Watermark vidéo (image)
Modifications imperceptibles des pixels
Watermark audio
Modifications imperceptibles du signal audio
00:12 / 00:28
00:12 / 00:28

LABEL4.AI

La robustesse : une identité qui résiste à la vie réelle

Le tatouage numérique reste détectable même après les traitements courants et les tentatives de manipulation.



Le tatouage reste détectable après...



Recadrage



Compression
(faible ou forte)



Retouches
(couleur, contraste...)



Capture d'écran



Impression / scan



Réencodage
(vidéo)

Une résistance testée et mesurée

Robustesse
aux transformations courantes

Efficacité mesurée
(TPR / FPR)

Fiable
et reproductible

Interopérable
(avec les standards de provenance, ex. C2PA)

Un tatouage conçu pour durer, de la capture à la diffusion, y compris en cas de manipulation.

LABEL4.AI

Un mouvement mondial vers la transparence des contenus

L'identification des contenus d'origine IA s'impose dans les réglementations, avec des approches qui s'élargissent.



Union européenne – AI Act

Marquage des contenus générés ou manipulés par IA

Chine (2025)

Marquage des contenus générés par IA

Californie – SB 942

Marquage des contenus générés par IA
et des contenus réels (authentiques)

ONU

Charte de Paris
pour la confiance dans l'IA

Une recommandation commune :
marquer aussi les contenus réels pour
renforcer la confiance dans l'écosystème informationnel.

Une convergence internationale vers un marquage généralisé, IA et réel, pour plus de confiance.

LABEL4.AI

Demain, comment protéger les archives de l'ECPAD ?

Une image authentique peut être détournée à des fins de désinformation, à partir du contenu d'origine.



1. Image originale

Archive ECPAD authentique
Tatouée (watermark invisible) et associée à des métadonnées C2PA

C2PA



2. Image détournée

Ajout d'une explosion à partir de l'image d'origine (manipulation ou IA)



3. Vérification

Détection du tatouage, contrôle C2PA et comparaison avec l'archive source

Identifier l'origine
Retrouver l'archive source grâce au tatouage.

Vérifier la provenance
Contrôler les informations d'origine et l'historique C2PA.

Démontrer la manipulation
Établir les différences avec le contenu authentique et objectiver sa modification.

L'ECPAD dispose ainsi d'éléments techniques robustes pour identifier ses contenus, contrer les détournements et objectiver la désinformation.

LABEL4.AI

Protéger les archives, c'est préserver notre souveraineté informationnelle

Une chaîne de confiance pour garantir l'authenticité, la provenance et l'intégrité des contenus de l'ECPAD.



Authentifier les contenus d'origine

Tatouage invisible et métadonnées C2PA pour attester la source ECPAD.

Détecter les détournements

Identifier les contenus modifiés, falsifiés ou décontextualisés, même largement diffusés.

Tracer les réutilisations

Conserver l'historique des opérations et l'intégrité tout au long du cycle de vie.

Valoriser et sécuriser le patrimoine audiovisuel

Permettre une diffusion durable et fiable des archives auprès des publics et des partenaires.

Grâce au tatouage et à C2PA, l'ECPAD peut prouver qu'un contenu provient de son fonds d'origine et objectiver toute modification ultérieure.