



Download on the
App Store



Site web



NOUVEAU : étiquetez vos images IA
AI Act européen, art. 50

Stego-Lab

Manuel Utilisateur & Documentation Technique

iOS · iPadOS · macOS

Stéganographie · Filigranage · EXIF · Lot · Étiquetage IA

Propriété	Valeur
Produit	Stego-Lab
Plateformes	iOS 17+ · iPadOS 17+ · macOS 14+
Version	1.1 · créé le 22/09/2026 à 14:19
Langue du manuel	Français
Confidentialité	100 % local — aucun cloud
GitLab	gitlab.com/RaithChr/stego-lab

Table des matières

1 Introduction	5
1.1 Qu'est-ce que Stego-Lab ?	5
1.2 Domaines d'application	5
1.3 Points forts	5
2 Installation et premiers pas	7
2.1 Configuration requise	7
2.2 Installation	7
2.3 Premier lancement	8
3 Interface	9
3.1 Navigation principale	9
3.2 Zone Encoder	9
3.3 Zone Décodeur	10
4 Stéganographie	12
4.1 Principes	12
4.2 Méthode LSB	12
4.3 Intégrer des contenus	12
4.4 Protection par mot de passe	13
4.5 Décodage et capacité	14
5 Filigranage	15
5.1 Filigranes visibles	15
5.2 Filigranes invisibles et combinés	15
5.3 Positionnement et traitement par lot	15
6 Édition EXIF et métadonnées	17
6.1 Principes EXIF	17
6.2 Champs lisibles	17
6.3 Champs modifiables	18
6.4 Données GPS	18
6.5 Supprimer toutes les métadonnées	19
7 Lot et formats	20
7 Traitement par lot	20
8 Formats pris en charge	20
9 Étiqueter les images IA	23
9.1 Cadre juridique	23
9.2 Étiqueter dans Encoder et par lot	23
9.3 Champs écrits	23
9.4 Détection à la lecture	24

9.5 Gratuit ou Pro	24
9.6 Limites	24
9.7 Mention juridique	24
10 Sécurité et confidentialité	25
10.1 Traitement local	25
10.2 Détails du chiffrement	25
10.3 Sécurité stéganographique	25
11 Spécifications techniques	27
11.1 Performances	27
11.2 Besoins en mémoire	27
11.3 Algorithmes et normes	27
12 Exemples d'utilisation	29
12.1 Protection de documents privés (Pro)	29
12.2 Preuve de droit d'auteur (Pro)	29
12.3 Flux du photographe, 500 images (Pro)	30
12.4 Contexte pédagogique (Pro)	30
13 Questions fréquentes	31
14 Annexe technique	33
14.1 Processus d'encodage LSB	33
14.2 Format de trame interne	33
14.3 Gestion des erreurs	34
15 Glossaire	36
16 Positionnement	38
16.1 Comparatif des fonctions	38
16.2 Publics visés	38
17 Référence des flux de travail	39
17.1 Flux d'encodage (Pro)	39
17.2 Nettoyage EXIF	39
17.3 Lot pour les réseaux sociaux (Pro)	40
17.4 Étiqueter une image IA	40
18 Évaluation de la sécurité	42
18.1 Modèle de menaces	42
18.2 Recommandations pour les mots de passe	42
18.3 Revue de sécurité interne avant publication	42
19 Assistance et contact	44
19.1 Canaux d'assistance	44
19.2 Limitations connues	44

20 Table des tableaux	45
21 Historique des versions	47
Fonctions prévues	48
22 Achat intégré Stego-Lab Pro	49
22.1 Gratuit et Pro en un coup d'œil	49
22.2 Achat et restauration	49
23 À propos du développeur / Mentions légales	51
23.1 Coordonnées du développeur	51
23.2 Autres projets du développeur	51
23.3 Dépôt GitLab	52
23.4 Site web	52
24 Mentions légales et confidentialité	53
24.1 Politique de confidentialité (résumé)	53
24.2 Licence et conditions d'utilisation	53
24.3 Frameworks utilisés et éléments tiers	54
24.4 Droit d'auteur et marques	55

Introduction

CHAPITRE 1

1.1 Qu'est-ce que Stego-Lab ?

Stego-Lab est une application native pour iPhone, iPad et Mac qui réunit cinq domaines d'outils : stéganographie, filigranage, édition EXIF et des métadonnées, marquage des images générées par IA et traitement d'images par lot. Toutes les données d'image sont traitées exclusivement en local — sans cloud ni serveur externe. L'app n'établit elle-même aucune connexion réseau ; les seules exceptions sont l'achat intégré via StoreKit d'Apple et les liens que vous choisissez d'ouvrir dans le navigateur.

1.2 Domaines d'application

Domaine	Description
Archivage privé	Intégrer des documents sensibles de façon invisible dans des photos
Protection du droit d'auteur	Intégrer de façon invisible une mention d'auteur (texte, image ou fichier) — pas de signature cryptographique ; ne résiste pas à une recompression JPEG (Pro)
Photographie	Nettoyer l'EXIF, retirer le GPS, apposer un copyright
Séries d'images	Filigranes par lot sur des collections entières
Journalisme	Intégrer des preuves de façon chiffrée
Enseignement	Démontrer concrètement les concepts de stéganographie
Créateurs de contenu	Filigranes de copyright pour les réseaux sociaux
Sécurité informatique	Étudier les canaux d'image dissimulés

1.3 Points forts

Caractéristique	Description
Entièrement local	Pas de cloud, pas de télémétrie ; l'app n'établit elle-même aucune connexion réseau (exception : achat intégré via StoreKit)
Multiplateforme	iPhone, iPad, Mac — même format de données (PV2) et même noyau fonctionnel ; l'interface, la sélection des fichiers et quelques fonctions annexes diffèrent selon la plateforme
Outils réunis	Stégano + filigrane + EXIF + marquage IA + lot dans une seule app
Chiffrement AES-256	Protection facultative par mot de passe (AES-256-GCM, Pro) du texte, des images et des fichiers dissimulés ; l'en-tête de format et le marquage IA invisible restent volontairement non chiffrés

Caractéristique	Description
Sortie sans perte	PNG + TIFF pour une intégrité maximale des données

Installation et premiers pas

CHAPITRE 2

2.1 Configuration requise

Plateforme	Minimum	Recommandé	Architecture
iPhone	iOS 17.0	Version d'iOS la plus récente maintenue par Apple	ARM64 (A12 ou plus récent)
iPad	iPadOS 17.0	Version d'iPadOS la plus récente maintenue par Apple	ARM64 (A10 ou plus récent)
Mac	macOS 14.0	Version de macOS la plus récente maintenue par Apple	Apple Silicon + Intel
Stockage	Espace libre pour les fichiers de sortie (PNG/TIFF sont plus volumineux que JPEG)	—	—
Mémoire vive	Pas de minimum technique	4 Go+ (iPhone/iPad) ou 8 Go+ (Mac) pour les grandes images	—
Réseau	Non nécessaire	Uniquement pour l'achat intégré	Hors ligne

▲ **Ne sont plus pris en charge : iOS 16 / iPadOS 16 et macOS 13 (Ventura).** À partir de la version 1.1, Stego-Lab exige au minimum iOS 17 / iPadOS 17 ou macOS 14. La raison est le passage de l'environnement de développement à Xcode 27 : l'app utilise depuis lors des interfaces système qui n'existent qu'à partir de ces versions. En outre, Apple ne fournit plus de mises à jour de sécurité pour macOS 13. Les appareils qui ne dépassent pas iOS 16 ou macOS 13 peuvent continuer à utiliser la version 1.0, mais ne reçoivent plus de mises à jour de l'app. Pour protéger des données confidentielles, il est recommandé d'utiliser la version la plus récente du système prise en charge par l'appareil, avec toutes les mises à jour de sécurité disponibles.

2.2 Installation

Étape	iOS / iPadOS	macOS
1	Ouvrir l'App Store	Ouvrir le Mac App Store
2	Rechercher « Stego-Lab »	Rechercher « Stego-Lab »
3	Toucher « Obtenir »	Cliquer sur « Obtenir »
4	Confirmer avec Face ID / Touch ID	Confirmer avec le compte Apple

Étape	iOS / iPadOS	macOS
5	Lancer l'app depuis l'écran d'accueil	Lancer l'app depuis le dossier Applications (jusqu'à macOS 15 aussi via le Launchpad, à partir de macOS 26 via « Apps »)

✓ Stego-Lab ne demande ni inscription ni compte. Toutes les fonctions sont utilisables hors ligne ; seuls l'achat et la restauration de Stego-Lab Pro nécessitent une connexion à l'App Store.

2.3 Premier lancement

Stego-Lab ne demande aucune autorisation au premier lancement. Sur iPhone et iPad, les images sont choisies avec le sélecteur de photos du système, qui ne donne pas accès à l'ensemble de la photothèque ; iOS ne demande l'autorisation d'ajouter des photos qu'au premier enregistrement dans Photos. Les images peuvent aussi être chargées depuis l'app Fichiers. Sur Mac, elles sont ouvertes depuis le Finder (dialogue d'ouverture ou glisser-déposer). L'accès à l'appareil photo n'est demandé qu'à la première prise de vue directe (Pro). L'interface de l'app est en allemand ; les noms d'onglets et de boutons cités dans ce manuel sont les libellés d'origine.

Interface

CHAPITRE 3

3.1 Navigation principale

Zone	Symbole (iPhone/iPad · Mac)	Fonction
« Encode » (Mac : « Verstecken »)	arrow.up.square · eye.slash.fill	Intégrer des contenus dans des images
« Decode » (Mac : « Entdecken »)	arrow.down.square · eye.fill	Extraire les contenus intégrés
« EXIF »	info.square · tag	Afficher et modifier les métadonnées
« Batch »	square.stack.3d.up.fill · wand.and.stars	Traiter plusieurs images (Pro)
« Info »	info.circle · info.circle	Aide, fenêtre Pro et détails de l'app. Sur Mac, l'ordre des onglets est Verstecken, Entdecken, Batch, EXIF, Info

■ L'interface de Stego-Lab 1.1 est en allemand ; sur iPhone et iPad, les onglets portent des noms anglais (Encode, Decode, EXIF, Batch, Info), sur Mac des noms allemands (Verstecken, Entdecken, Batch, EXIF, Info). Ce manuel cite le libellé d'origine et donne sa traduction entre parenthèses.

3.2 Zone Encoder

Élément	Description
Image porteuse	Toute image (PNG, TIFF, JPEG, HEIC, BMP, RAW) ; le résultat est toujours enregistré sans perte en PNG ou TIFF
Type de contenu	Texte, image ou fichier — image et fichier avec Pro uniquement
Prise de vue directe	Photographier avec l'appareil photo et intégrer en une étape ; n'est jamais enregistrée dans la photothèque (Pro)
Curseur de qualité	Curseur en direct équilibrant la résolution de la prise de vue et la capacité de l'image porteuse
Mot de passe	Facultatif — active AES-256-GCM (Pro)
Format de sortie	PNG ou TIFF (iPhone/iPad : PNG par défaut ; sur Mac, une image porteuse TIFF reste en TIFF, sinon PNG)
Indicateur de capacité	Barre avec pourcentage en temps réel, plus la taille du contenu par rapport à la capacité

Élément	Description
Bouton Encoder	Le bouton « Kodieren » (Mac : « Kodieren und Speichern ») lance l'intégration invisible (Pro) ; sans Pro, seule l'image porteuse avec étiquette IA peut être enregistrée

Prendre une photo directement

Dans la zone « Encode », l'image à intégrer peut aussi être prise directement avec l'appareil photo : photographier et dissimuler dans l'image porteuse en une seule étape, sans passer par la photothèque. La prise de vue n'est jamais enregistrée dans la photothèque. Sur Mac, elle reste exclusivement en mémoire vive. Sur iPhone et iPad, l'app en dépose une copie temporaire dans son conteneur protégé pour la suite du traitement ; cette copie est supprimée lors de la réinitialisation ou du remplacement du contenu, au plus tard au lancement suivant de l'app. Un curseur de qualité en direct met en balance la résolution et la capacité disponible de l'image porteuse ; l'orientation EXIF est alors inscrite directement dans les pixels, afin que l'image soit intégrée dans le bon sens. Sur Mac, l'app prend en charge Continuity Camera — l'iPhone sert alors d'appareil photo externe. La prise de vue directe fait partie de Stego-Lab Pro.

✓ La prise de vue directe n'est jamais écrite dans la photothèque. Sur Mac, elle reste exclusivement en mémoire vive ; sur iPhone et iPad, uniquement sous forme de fichier temporaire dans le conteneur de l'app jusqu'à la fin du traitement — conformément au principe « sur l'appareil, sans cloud » de Stego-Lab.

Reprendre une photo depuis le menu Partager

Une image porteuse peut aussi être reprise depuis l'extérieur de l'app, directement depuis le menu Partager du système. Sur iPhone et iPad, sélectionnez une image dans Photos ou Fichiers, touchez Partager puis « Copier vers Stego-Lab » ; la photo est aussitôt chargée comme image porteuse dans l'onglet « Encode », qui s'ouvre automatiquement. Sur Mac, Stego-Lab apparaît dans le Finder sous « Ouvrir avec » (clic droit sur une image) — vous pouvez également déposer l'image sur l'icône de l'app dans le Dock ; elle arrive alors dans l'onglet « Verstecken ». Une photo rejoint ainsi le flux d'intégration sans détour par le sélecteur d'images.

✓ Stego-Lab se déclare au système uniquement comme destinataire d'images — pas de connexion, pas de service supplémentaire. Sur iPhone et iPad, la copie transmise est supprimée aussitôt après le chargement ; la photo ne reste qu'en mémoire vive jusqu'à ce que vous enregistriez vous-même le résultat.

3.3 Zone Décoder

Élément	Description
Charger une image	iPhone/iPad : depuis Photos ou Fichiers (PNG, JPG, TIFF, HEIC, RAW) ; Mac : « Bild öffnen... » (PNG, JPEG, TIFF, BMP) ou glisser-déposer
Mot de passe	À saisir si le contenu est chiffré (Pro)
Décoder	Extrait le contenu intégré — format Stego-Lab, PNG Stegosuite (LSB), anciens JPG Stegosuite 0.8 (F5). Texte sans mot de passe gratuit, contenus image et fichier avec Pro
Aperçu	Contenu décodé affiché directement ; un message d'accompagnement (par ex. pour les porteurs multiblocs) apparaît dans le bandeau au-dessus

Élément	Description
Exporter	Copier ou partager le texte (gratuit) ; export d'images et de fichiers avec Pro
Note héritage	Pour les contenus PV1 et Stegosuite, un avertissement de sécurité s'affiche — chiffrement plus faible, lecture seule (PV1 = format de développement antérieur à la première publication, jamais distribué)

3.4 – 3.6 EXIF · Lot · Infos

Zone EXIF : afficher toutes les métadonnées de façon structurée et modifier directement les champs éditables.
Zone Lot : traiter plusieurs images à la fois avec une barre de progression. Zone Infos : aide-mémoire et détails de version de l'app.

Stéganographie

CHAPITRE 4

4.1 Principes

La stéganographie est la technique consistant à dissimuler des informations à l'intérieur d'un support anodin. Contrairement à la cryptographie, la stéganographie masque l'existence même du message.

Stego-Lab met en œuvre la stéganographie d'image par la méthode du bit de poids faible (LSB) : les bits de poids le plus faible des canaux de couleur R, V, B sont remplacés par des bits de données utiles. L'effet visuel est imperceptible pour l'œil humain.

4.2 Méthode LSB

Chaque canal de couleur est une valeur sur 8 bits (0–255). Une modification du LSB correspond à une différence de couleur de ± 1 — bien en dessous du seuil de perception humaine.

Canal	Bit d'origine (LSB)	Bit de données	Bit résultant	Écart de couleur
Rouge	1101 0110	1	1101 0111	+1
Vert	1010 0011	0	1010 0010	-1
Bleu	0011 1001	1	0011 1001	0

Paramètre	Valeur	Remarque
Bits par canal	1 (fixe, non réglable)	3 canaux : R, V, B
Capacité de charge	3 bits par pixel	= 3/8 octet par pixel, moins les données de trame (voir 4.5)
PSNR (qualité)	≥ 51 dB	$\approx 51,1$ dB à pleine charge ; imperceptible à l'œil, détectable statistiquement
Canaux utilisés	R, V, B	Canal alpha non utilisé ; la transparence de l'image porteuse n'est pas conservée
Format de sortie obligatoire	PNG ou TIFF	Le JPEG détruit les données LSB !

▲ IMPORTANT : la compression JPEG détruit irrémédiablement les données LSB intégrées. Pour les opérations de stéganographie, Stego-Lab produit exclusivement du PNG ou du TIFF.

4.3 Intégrer des contenus

Intégrer du texte

Le texte est intégré sous forme de suite d'octets UTF-8. Tous les caractères Unicode, les sauts de ligne et les caractères spéciaux sont pris en charge intégralement.

Résolution	Capacité (octets)	Capacité (caractères)
1080 × 1920 (Full HD)	env. 777 600 o	env. 777 600 ASCII
2160 × 3840 (4 K)	env. 3 110 400 o	env. 3 millions ASCII
4000 × 6000 (24 MP)	env. 9 000 000 o	env. 9 millions ASCII

Images et fichiers

Les images et les fichiers de tout type (PDF, DOCX, ZIP...) sont intégrés tels que l'app les reçoit : octet par octet, sans réencodage ni compression supplémentaire – un JPEG reste un JPEG. Seule exception : une prise de vue réalisée avec la fonction appareil photo n'existe qu'en mémoire vive ; elle est donc encodée sans perte en PNG et, si nécessaire, réduite à la capacité de l'image porteuse. Le nom de fichier d'origine est placé en tête de la charge utile (longueur sur 2 octets + nom en UTF-8) et chiffré avec le contenu lorsqu'un mot de passe est défini. L'en-tête de 10 octets ne contient que l'identifiant de format, la version, la longueur de la charge utile et les indicateurs ; aucun type MIME n'est enregistré.

4.4 Protection par mot de passe

Chiffrement AES-256-GCM facultatif (AEAD), inclus dans Stego-Lab Pro. Sans mot de passe, la charge utile est écrite en clair dans la couche LSB. La clé est dérivée du mot de passe par PBKDF2-HMAC-SHA256 (600 000 itérations, sel aléatoire de 16 octets pour chaque chiffrement). Sans le bon mot de passe, les bits insérés peuvent être lus, mais pas déchiffrés ; avec un mot de passe suffisamment robuste, le deviner est calculatoirement infaisable. Un mot de passe faible peut en revanche être retrouvé par une attaque par dictionnaire : Stego-Lab propose lui-même un tel test dans la zone Décoder.

Paramètre	Valeur
Algorithme	AES-256-GCM (AEAD)
Dérivation de clé	PBKDF2-HMAC-SHA256
Itérations	600 000 (recommandation OWASP 2023)
Sel	16 octets, cryptographiquement aléatoire, renouvelé à chaque chiffrement
Nonce	12 octets, cryptographiquement aléatoire (standard GCM)
Intégrité	Tag d'authentification GCM de 16 octets (intégré, pas de HMAC séparé)

▲ Il n'existe ni porte dérobée, ni clé maîtresse, ni fonction de récupération : un mot de passe perdu rend le contenu définitivement inaccessible, y compris pour le développeur. Un mot de passe robuste protège durablement le contenu ; un mot de passe faible peut être retrouvé par une attaque par dictionnaire. Choisissez des mots de passe suffisamment longs et conservez-les en lieu sûr.

4.5 Décodage et capacité

Décodage : lire les 80 premiers bits LSB (en-tête de 10 octets), vérifier l'identifiant de format (PV2 ; le format de développement PV1 est accepté en lecture seule), exploiter la longueur et les indicateurs, puis lire le sel et le nonce le cas échéant ainsi que la charge utile. Pour les contenus chiffrés, la clé est dérivée par PBKDF2-HMAC-SHA256 (600 000 itérations) du mot de passe et du sel enregistré, et la charge utile est déchiffrée en AES-256-GCM avec vérification du tag d'authentification GCM de 16 octets. Si le tag est invalide (mot de passe erroné ou données modifiées), aucune donnée n'est restituée. En l'absence d'identifiant connu, Stego-Lab essaie, en lecture seule, les formats hérités Stegosuite (PNG) et, pour les porteuses JPEG, F5.

Formule	Valeur
Capacité (octets) = $\lfloor L \times H \times 3 \div 8 \rfloor$ – données de trame	L, H = largeur et hauteur en pixels ; 3 canaux × 1 bit ; données de trame ci-dessous (10 octets au minimum)
Exemple : $3024 \times 4032 \times 3 \div 8$	= 4 572 288 octets ≈ 4,57 Mo (4,36 Mio) ; utilisables sans mot de passe 4 572 278 octets, avec mot de passe 4 572 234 octets
Données de trame (internes à Stego-Lab)	En-tête de 10 octets (identifiant 4 + version 1 + longueur 4 + indicateurs 1) ; avec mot de passe, 44 octets de plus (sel 16 + nonce 12 + tag GCM 16), soit 54 octets ; pour une image ou un fichier, 2 octets + nom de fichier en UTF-8 en plus (dans le chiffré si un mot de passe est défini) ; avec l'étiquetage IA (Pro, lot), 7 octets de cadre + données d'étiquetage en plus (2 048 octets au maximum), non chiffrées

Filigranage

CHAPITRE 5

5.1 Filigranes visibles

Paramètre	Filigrane texte	Filigrane image
Type de contenu	Tout texte UTF-8	PNG, JPEG, HEIC, TIFF
Opacité	15 – 100 % (par défaut 65 %)	15 – 100 % (par défaut 65 %)
Position	9 positions fixes sur une grille 3×3, par défaut : en bas à droite	9 positions fixes sur une grille 3×3, par défaut : en bas à droite
Taille	2 – 10 % du petit côté de l'image (minimum 24 px)	8 – 45 % de la largeur de l'image (minimum 48 px)
Rendu	Blanc, police système grasse, ombre portée noire — couleur, police et rotation non réglables	Couleurs d'origine du logo, pas de rotation
Disponibilité	Zone « Batch » : une image gratuite, plusieurs images avec Pro	Zone « Batch » : une image gratuite, plusieurs images avec Pro

5.2 Filigranes invisibles et combinés

Invisible : un identifiant est dissimulé dans l'image via le LSB. Visuellement identique à l'original — extractible à tout moment par Stego-Lab. Combiné : appliquer simultanément un filigrane visible et un filigrane invisible à une même image.

5.3 Positionnement et traitement par lot

Position	Libellé dans l'app	Description
En haut à gauche	« Oben L »	Coin supérieur gauche
En haut au centre	« Oben M »	Milieu supérieur de l'image
En haut à droite	« Oben R »	Coin supérieur droit
Au milieu à gauche	« Links M »	Centré verticalement, à gauche
Centré	« Mitte »	Entièrement centré
Au milieu à droite	« Rechts M »	Centré verticalement, à droite
En bas à gauche	« Unten L »	Coin inférieur gauche
En bas au centre	« Unten M »	Milieu inférieur de l'image

Position	Libellé dans l'app	Description
En bas à droite	« Unten R »	Coin inférieur droit — par défaut

Filigranage par lot : les mêmes réglages appliqués en une passe à autant d'images que vous voulez (Pro ; une image unique avec filigrane visible est gratuite) — visible, invisible ou combiné.

Édition EXIF et métadonnées

CHAPITRE 6

6.1 Principes EXIF

EXIF (Exchangeable Image File Format) est la norme la plus répandue pour stocker des métadonnées dans les fichiers image. Elle contient les données techniques de l'appareil photo, les coordonnées GPS, les horodatages et les informations de droits. Stego-Lab lit et écrit ces champs via ImageIO d'Apple, sans imposer une version particulière d'EXIF.

6.2 Champs lisibles

Balise EXIF	Champ (libellé dans l'app)	Exemple de valeur
0x010F	« Kamera-Hersteller » (fabricant de l'appareil)	Apple
0x0110	« Kamera-Modell » (modèle de l'appareil)	iPhone 15 Pro
0xA434	« Objektiv » (objectif)	iPhone 15 Pro back camera
0x9003	« Aufnahmedatum » (date de prise de vue, DateTimeOriginal)	2024:03:15 14:32:00
0x9004	« Digitalisiert » (date de numérisation, DateTimeDigitized)	2024:03:15 14:32:00
0x829A	« Belichtungszeit » (temps d'exposition)	0.001 (= 1/1000 s)
0x829D	« Blende » (ouverture)	1.8
0x8827	« ISO » (sensibilité ISO)	64
0x920A	« Brennweite » (distance focale)	6.765
0x013B	« Künstler » (auteur, Artist)	Jean Dupont
0x8298	« Copyright »	© 2024 J. Dupont
0x010E	« Beschreibung » (description de l'image)	Panorama des Alpes
0x9286	« Kommentar » (commentaire, UserComment)	Texte libre
0x0131	« Software » (logiciel)	Stego-Lab 1.1

6.3 Champs modifiables

Champ	Modifiable	Remarque
« Beschreibung » (description)	OUI (gratuit)	Texte libre
« Künstler » (auteur, Artist)	OUI (gratuit)	Nom du photographe
« Copyright »	OUI (gratuit)	Mention de copyright
« Software » (logiciel)	OUI (gratuit)	Logiciel de retouche
« Kamera-Hersteller », « Kamera-Modell » (fabricant, modèle)	OUI (Pro)	Texte libre (Mac : « Kamera (Marke) », « Kamera (Modell) »)
« Objektiv » (objectif)	OUI (Pro)	Texte libre
« Aufnahmedatum » (date de prise de vue)	OUI (Pro)	Format EXIF AAAA:MM:JJ HH:MM:SS (Mac : « Datum (Original) »)
« Digitalisiert » (date de numérisation)	OUI (Pro)	Format EXIF AAAA:MM:JJ HH:MM:SS (Mac : « Datum (Digitalisiert) »)
« Belichtungszeit » (temps d'exposition)	OUI (Pro)	Secondes, en décimal (p. ex. 0.001) ; une saisie invalide est ignorée sans message
« Blende » (ouverture)	OUI (Pro)	Nombre f (p. ex. 2.8) ; une saisie invalide est ignorée sans message
« ISO »	OUI (Pro)	Nombre entier (p. ex. 800)
« Brennweite » (distance focale)	OUI (Pro)	Millimètres, en décimal (p. ex. 50) ; une saisie invalide est ignorée sans message
« Kommentar » (commentaire)	OUI (Pro)	Texte libre (EXIF UserComment)
GPS : « Breitengrad », « Längengrad », « Höhe » (latitude, longitude, altitude)	OUI (Pro)	Valeur décimale ; négatif = sud, ouest ou sous le niveau de la mer. Supprimer et/ou redéfinir — un champ vide ne supprime que cette valeur
Tous les champs	—	Un champ vide supprime la valeur. Prend effet avec « Änderungen anwenden » (appliquer les modifications ; Mac : « Metadaten anwenden »)

6.4 Données GPS

Balise GPS	Description	Format
GPSLatitude	Latitude	Fichier : degrés, min., sec. + N/S — app : degrés décimaux, négatif = sud (Pro)
GPSLongitude	Longitude	Fichier : degrés, min., sec. + E/W — app : degrés décimaux, négatif = ouest (Pro)

Balise GPS	Description	Format
GPSPAltitude	Altitude au-dessus du niveau de la mer	Fichier : mètres + référence — app : mètres, négatif = sous le niveau de la mer (Pro)
GPSTimeStamp	Heure GPS	UTC HH:MM:SS — non affiché dans l'app
GPSTDateStamp	Date GPS	AAAA:MM:JJ — non affiché dans l'app
GPSPimgDirection	Direction de visée	0 – 360° — non affiché dans l'app
Suppression	Partielle ou complète	Vider les champs de coordonnées ne supprime que latitude, longitude et altitude ; les autres balises GPS restent dans le fichier. Seule la fonction « Alle Metadaten löschen » (supprimer toutes les métadonnées, gratuit) les supprime entièrement — avec toutes les autres métadonnées

▲ Les données GPS contiennent le lieu exact de la prise de vue. Vérifiez-les toujours avant de transmettre des images et supprimez-les au besoin !

6.5 Supprimer toutes les métadonnées

Cette fonction supprime de l'image les métadonnées EXIF, GPS, IPTC et XMP ainsi que les données d'appareil photo et d'objectif et les vignettes intégrées — idéal avant transmission ou publication.

Dans la zone EXIF, le bouton « Alle Metadaten löschen » (supprimer toutes les métadonnées) est prévu à cet effet (gratuit, avec boîte de dialogue de confirmation). La suppression ne prend effet qu'avec « Änderungen anwenden » (appliquer les modifications ; Mac : « Metadaten anwenden ») ; jusque-là, le partage et l'enregistrement sont bloqués. Dans la zone « Batch », l'option « Alle Metadaten löschen » (Pro) nettoie toute une série d'images en une seule passe ; si l'étiquetage IA y est actif en même temps, il est réécrit après la suppression. Si l'image porte un étiquetage IA (voir chapitre 9), seule sa partie dans les métadonnées est supprimée. Une étiquette visible et un marquage invisible dans les données de l'image sont conservés, car ils font partie des pixels — la boîte de dialogue de confirmation le signale.

■ Ce qui est conservé : le contenu de l'image, le profil colorimétrique (ICC) et l'orientation. Les fichiers JPEG et HEIC sont réencodés à cette occasion — une étape de compression avec perte supplémentaire. Le PNG et le TIFF restent sans perte.

Lot et formats

CHAPITRE 7

7 Traitement par lot

Paramètre	Valeur
Nombre max. d'images	Illimité (selon la mémoire vive ; max. 250 Mo ou 300 mégapixels par fichier)
Traitement	Séquentiel, avec barre de progression (« Bearbeite x / y »)
Gestion des erreurs	Les fichiers illisibles sont signalés à l'import et écartés ; une erreur pendant le traitement interrompt le lot. Aucun journal.
Interruption	Pas d'annulation possible pendant le traitement
Sortie	Dossier temporaire ; nom de fichier = nom d'origine + « _watermark » dans tous les modes (compteur en cas de doublon). Ensuite sur iPhone/iPad : « Exportordner teilen... » ou « Alle in Fotos speichern » ; sur Mac : « Im Finder zeigen » ou « In Ordner kopieren... »
Format d'export	PNG, TIFF ou JPG ; JPG uniquement en mode « Sichtbar » (visible) et pas lorsque la couche IA robuste est active
Modes	« Sichtbar » (visible) · « Unsichtbar » (invisible) · « Beides » (les deux) ; en plus, marquage IA et « Alle Metadaten löschen » (supprimer toutes les métadonnées)
Disponibilité	Une image avec filigrane visible gratuite ; plusieurs images, « Unsichtbar » (invisible), « Beides » (les deux), « Alle Metadaten löschen » (supprimer toutes les métadonnées) et couche IA robuste avec Stego-Lab Pro

8 Formats pris en charge

Formats d'entrée

Format	Nom complet	Sans perte	Utilisable comme image porteuse
PNG	Portable Network Graphics	OUI	OUI — format principal ; résultat enregistré en PNG ou TIFF
TIFF	Tagged Image File Format	OUI	OUI — résultat enregistré en PNG ou TIFF
JPEG / JPG	Joint Photographic Experts Group	NON	OUI — le résultat est toujours enregistré en PNG ou TIFF ; en outre, lecture des anciens JPG Stegosuite 0.8 (F5, depuis la version 1.1)

Format	Nom complet	Sans perte	Utilisable comme image porteuse
HEIC	Conteneur HEIF (ISO/IEC 23008-12) avec codage HEVC	NON	OUI — résultat enregistré en PNG ou TIFF (Mac : par glisser-déposer ou « Ouvrir avec »)
DNG	Adobe Digital Negative (RAW)	en général	OUI, si le système connaît le modèle RAW — résultat enregistré en PNG ou TIFF (Mac : par glisser-déposer ou « Ouvrir avec »)
CR2 / CR3	Canon RAW	en général	OUI, si le système connaît le modèle RAW — résultat enregistré en PNG ou TIFF (Mac : par glisser-déposer ou « Ouvrir avec »)
NEF	Nikon RAW	en général	OUI, si le système connaît le modèle RAW — résultat enregistré en PNG ou TIFF (Mac : par glisser-déposer ou « Ouvrir avec »)
ARW	Sony RAW	en général	OUI, si le système connaît le modèle RAW — résultat enregistré en PNG ou TIFF (Mac : par glisser-déposer ou « Ouvrir avec »)
BMP	Bitmap	OUI	OUI — résultat enregistré en PNG ou TIFF

Formats de sortie

Format	Stéganographie	Filigrane	EXIF	Qualité
PNG	OUI (par défaut)	OUI	OUI (si la source est en PNG)	Sans perte
TIFF	OUI	OUI	OUI (si la source est en TIFF ; format de repli si le type source est inconnu)	Sans perte
JPEG	NON — uniquement lecture des anciens JPG Stegosuite 0.8 (F5)	OUI (mode lot « Sichtbar » (visible) uniquement, sans la couche IA robuste)	OUI (si la source est en JPEG)	Réglage système, non modifiable
HEIC	NON	NON	OUI (si la source est en HEIC)	Réglage système, non modifiable

Recommandations de format

Cas d'usage	Format d'entrée	Format de sortie
Stéganographie (texte)	Toute image (PNG, TIFF, JPEG, HEIC, BMP, RAW)	PNG ou TIFF
Stéganographie (fichier)	Toute image (PNG, TIFF, JPEG, HEIC, BMP, RAW)	PNG ou TIFF
Filigrane visible (lot ; une image gratuite)	Indifférent	JPG (réseaux sociaux) / PNG ou TIFF (archive)
Filigrane invisible (lot, Pro)	Indifférent	PNG ou TIFF
Édition EXIF	Indifférent	Même format que la source (TIFF si le type source est inconnu)
Suppression du GPS	JPEG, HEIC, PNG, TIFF	Même format que la source
Archivage longue durée	TIFF	TIFF (non compressé)

Étiqueter les images IA

CHAPITRE 9

9.1 Cadre juridique

Depuis le 2 août 2026, l'article 50 du règlement (UE) 2024/1689 sur l'IA impose deux obligations distinctes. Les fournisseurs de systèmes d'IA qui génèrent des images doivent marquer leurs sorties dans un format lisible par machine (par. 2) ; les systèmes mis sur le marché avant le 2 août 2026 bénéficient d'un délai transitoire jusqu'au 2 décembre 2026. Les déployeurs qui utilisent un système d'IA pour générer ou manipuler des images constituant un hypertrucage (deep fake) au sens de l'article 3, point 60, doivent indiquer que le contenu a été généré ou manipulé artificiellement (par. 4). Sont visées les images qui ressemblent à des personnes, objets, lieux ou événements réels et pourraient être perçues à tort comme authentiques. Pour les œuvres manifestement artistiques, créatives ou satiriques, une mention qui ne gêne pas la présentation de l'œuvre suffit ; l'usage purement personnel, non professionnel, n'est pas visé. Il n'existe pas d'obligation générale d'étiquetage pour toute image retouchée par IA.

Stego-Lab ne génère pas lui-même de contenus IA et n'est donc pas un fournisseur au sens du par. 2. L'app est un outil pour les déployeurs qui veulent ou doivent mettre en œuvre une divulgation au titre du par. 4 : elle réunit l'étiquette visible et les métadonnées lisibles par machine ; dans la zone « Batch » (Pro) s'y ajoute la « Robuste unsichtbare Schicht » (couche invisible robuste) — robuste face à la suppression des métadonnées, mais pas face à une recompression avec perte (voir 9.6).

artificialintelligenceact.eu/fr/transparency-rules-article-50

9.2 Étiqueter dans Encoder et par lot

Un interrupteur suffit : dans la section « Étiquetage IA » d'Encoder et du mode Lot, « Étiqueter comme image IA » active le pré-réglage. Deux variantes sont proposées, « entièrement générée par IA » et « retouchée par IA » ; un champ libre facultatif « Générateur » accepte par exemple « Midjourney v7 » et n'apparaît que dans les métadonnées, jamais dans l'étiquette visible.

L'étiquette visible s'adapte automatiquement : un contraste minimal calculé par mesure de luminance (texte clair sur fond sombre ou l'inverse) et une taille minimale de 3 % du plus petit côté de l'image garantissent la lisibilité. La position se choisit librement dans une grille 3×3 (par défaut : en bas à gauche). Un voyant à trois niveaux placé à côté de l'interrupteur indique d'un coup d'œil si le réglage est conforme à l'article 50.

Encoder étiquette déjà complètement en version gratuite : étiquette visible et métadonnées, même sans contenu dissimulé. Le mode Lot ajoute, pour Stego-Lab Pro, la couche invisible robuste et étiquette autant d'images que vous voulez en une seule passe.

9.3 Champs écrits

Champ	Valeur / contenu	Format
IPTC Digital Source Type — entièrement générée par IA	http://cv.iptc.org/newscodes/digitalsourcetype/trainedAlgorithmicMedia	IPTC / XMP

Champ	Valeur / contenu	Format
IPTC Digital Source Type — retouchée par IA	http://cv.iptc.org/newscodes/digitalsourcetype/compositeWithTrainedAlgorithmicMedia	IPTC / XMP
XMP Iptc4xmpExt:DigitalSourceType	Même valeur que pour IPTC, en plus comme propriété XMP (PNG via iTXt)	XMP
EXIF UserComment + TIFF ImageDescription	AI-generated content · KI-generierter Inhalt (EU AI Act Art. 50)	Texte en clair
Couche invisible « AI-DISCLOSURE v1 »	JSON contenant la variante, le générateur, l'émetteur et l'horodatage ; préfixe « AIDISC1: »	Trailer PV2, bit 3 de FLAGS (Pro)

9.4 Détection à la lecture

Décoder et EXIF affichent un badge neutre « Étiquetage IA détecté » dès que l'une des trois sources est trouvée — sans jugement et sans affirmation sur l'origine. En cas de sources multiples, l'ordre de priorité est : couche invisible, puis métadonnées, puis mention en clair ; si les sources se contredisent, une indication neutre apparaît au lieu d'un avertissement.

9.5 Gratuit ou Pro

Composant	Formule
Étiquette IA visible	Gratuit
Étiquetage dans les métadonnées (IPTC/XMP/EXIF)	Gratuit
Couche invisible robuste	Pro
Étiquetage par lot de nombreuses images	Pro

9.6 Limites

▲ Limites : le Digital Source Type IPTC/XMP est écrit de façon fiable en PNG, TIFF et JPEG, et relu par Stego-Lab. La mention en clair dans TIFF ImageDescription est correctement écrite dans le fichier pour les trois formats, mais la fonction de lecture de Stego-Lab ne la relit que sur les images porteuses TIFF, pas en PNG ni en JPEG. Le point médian « · » de la mention en clair EXIF UserComment devient un point d'interrogation dans les trois formats — une véritable perte de données, indépendante du format. La couche invisible ne survit ni à une recompression JPEG ni à une mise en ligne sur les réseaux sociaux ; c'est une marque d'archivage et de preuve pour PNG/TIFF, pas un substitut à C2PA. La marque unifiée à l'échelle de l'UE ne viendra qu'après le code de conduite définitif de la Commission — d'ici là, l'étiquette textuelle reste de mise.

9.7 Mention juridique

■ Stego-Lab ne génère pas de contenus IA et ne se prononce pas sur l'origine d'une image. L'étiquetage repose sur les indications de l'utilisateur. L'app est une aide à l'accomplissement d'obligations de transparence, pas un conseil juridique. L'exactitude et l'exhaustivité de l'étiquetage restent de la responsabilité de l'utilisateur.

Sécurité et confidentialité

CHAPITRE 10

10.1 Traitement local

Catégorie de données	Traitement	Réseau
Images	Local uniquement	AUCUN
Contenus intégrés	Local uniquement	AUCUN
Mots de passe	En mémoire vive seulement, jamais conservés	AUCUN
Données EXIF	Local uniquement	AUCUN
Rapports de plantage	Aucun outil de rapport dans l'app (rapports système transmis à Apple uniquement avec l'accord de l'utilisateur)	AUCUN
Analyses / télémétrie	Inexistantes	AUCUN
Publicité	Inexistante	AUCUN

10.2 Détails du chiffrement

Étape	Méthode	Paramètres
1. Sel	SecRandomCopyBytes (Apple Security)	16 octets, cryptographiquement aléatoire, renouvelé à chaque chiffrement
2. Nonce	Apple CryptoKit (AES.GCM.seal)	12 octets, aléatoire, renouvelé à chaque chiffrement (standard GCM)
3. Clé	PBKDF2-HMAC-SHA256	600 000 itérations, clé de 32 octets
4. Chiffr.	AES-256-GCM (AEAD)	Tag d'authentification GCM de 16 octets ajouté au chiffré
5. Trame	En-tête sel nonce chiffré+tag bloc IA le cas échéant	Binaire, dans la couche LSB ; l'en-tête et le bloc IA restent en clair
6. Vérif.	Tag d'authentification GCM	Vérifié lors du décodage ; pas de HMAC séparé

10.3 Sécurité stéganographique

Attaque	Sans mot de passe	Avec AES-256
Recherche d'identifiant (format connu)	Détection immédiate : l'identifiant de format « PV2 » figure en clair dans la couche LSB	Détection immédiate ; contenu et nom de fichier protégés
Inspection visuelle	Sûr	Sûr
Analyse RS	Délectable	Canal visible, contenu protégé
Test du khi-deux	Délectable	Canal visible, contenu protégé
Force brute (contenu)	Contenu directement lisible	Calculatoirement infaisable (mot de passe robuste)
Attaque par dictionnaire	Sans objet	Possible avec un mot de passe faible
Conversion en JPEG	Contenu détruit	Contenu détruit

✓ **Recommandation** : combinez toujours la stéganographie LSB avec AES-256. Le contenu reste ainsi illisible même si le canal est détecté statistiquement.

Spécifications techniques

CHAPITRE 11

11.1 Performances

Opération	Taille d'image	iPhone 15 Pro	iPad Pro M4	MacBook Pro M3
Encoder texte 1 Ko	12 MP (4032×3024)	< 0,5 s	< 0,5 s	< 0,2 s
Encoder fichier 1 Mo	12 MP	~1,5 s	~1,2 s	~0,5 s
Encoder fichier 10 Mo	48 MP	~8 s	~6 s	~2,5 s
Décoder 1 Ko	12 MP	< 0,5 s	< 0,5 s	< 0,2 s
Décoder 1 Mo	12 MP	~1,5 s	~1,2 s	~0,5 s
Filigrane visible	12 MP	~0,8 s	~0,6 s	~0,3 s
Lecture EXIF	Indifférent	< 0,1 s	< 0,1 s	< 0,1 s
Lot filigrane, 100 images	8 MP en moyenne	~80 s	~60 s	~25 s

11.2 Besoins en mémoire

Taille d'image	RAM (RVBA)	RAM (RVB)	RAM conseillée
8 MP (3264×2448)	~32 Mo	~24 Mo	3 Go
12 MP (4032×3024)	~49 Mo	~37 Mo	4 Go
24 MP (6000×4000)	~96 Mo	~72 Mo	6 Go
48 MP (8064×6048)	~196 Mo	~147 Mo	8 Go
108 MP (12000×9000)	~432 Mo	~324 Mo	16 Go

11.3 Algorithmes et normes

Algorithme	Utilisation	Spécification
Stéganographie LSB	Méthode d'intégration principale (1 bit par canal, R/V/B, séquentielle)	Format de trame PV2 propre, code source publié sous licence MIT
AES-256-GCM	Chiffrement de la charge utile (AEAD) ; le nonce de 12 octets est généré par CryptoKit lors du scellement	FIPS 197, NIST SP 800-38D

Algorithme	Utilisation	Spécification
PBKDF2-HMAC-SHA256	Dérivation de clé, 600 000 itérations	RFC 8018 (anciennement RFC 2898), NIST SP 800-132
Tag d'authentification GCM	Contrôle d'intégrité (16 octets, pas de HMAC séparé)	NIST SP 800-38D
SecRandomCopyBytes	Génération du sel de 16 octets	Framework Apple Security
HKDF-SHA256	Dérivation de clé, format hérité PV1 (format de développement antérieur à la version 1.0, jamais publié) – lecture seule	RFC 5869
AES-128-CTR	Compatibilité Stegosuite – lecture seule	NIST SP 800-38A
PBKDF2-HMAC-SHA1	Dérivation de clé Stegosuite – lecture seule	RFC 8018
MD5	Graine du générateur de positions Stegosuite – sans fonction de sécurité, lecture seule	RFC 1321
SHA-1	Générateur pseudo-aléatoire de sélection des coefficients F5 – sans fonction de sécurité, lecture seule	FIPS 180-4
EXIF 2.32	Norme de métadonnées	CIPA DC-X008-Translation-2019
PNG	Format de sortie sans perte	ISO/IEC 15948:2004
TIFF 6.0	Format de sortie sans perte	Spécification Adobe TIFF
UTF-8	Codage du texte	RFC 3629, Unicode 15.0

Exemples d'utilisation

CHAPITRE 12

12.1 Protection de documents privés (Pro)

Étape	Action
1	Ouvrir la zone Encode
2	Charger une photo de vacances comme image porteuse (PNG/TIFF recommandé)
3	Type de contenu : Fichier → sélectionner Scan-passeport.pdf
4	Saisir un mot de passe fort (recommandé : 12 caractères minimum, de préférence une phrase secrète)
5	Lancer l'encodage → enregistrer en PNG
6	Supprimer le PDF d'origine après sauvegarde
Décod.	Charger le PNG → Decode → mot de passe → extraire le fichier

12.2 Preuve de droit d'auteur (Pro)

Étape	Action
1	Batch → apposer le filigrane visible : « @Nom © 2025 » → sortie PNG
2	EXIF → renseigner Copyright et « Künstler » (auteur) (gratuit), « Änderungen anwenden » (appliquer les modifications)
3	Encode : intégrer ensuite le filigrane textuel invisible dans l'image ainsi marquée
4	Produire un PNG, mot de passe facultatif
5	Publier
Preuve	Decode → le filigrane invisible atteste la paternité (uniquement si l'image est transmise sans perte, en PNG/TIFF)
Attention	Respecter l'ordre : un filigrane visible apposé après coup sur des données déjà dissimulées les détruit. Variante en une seule passe : mode lot « Beides » (les deux).

12.3 Flux du photographe, 500 images (Pro)

Étape	Action
1	Batch → sélectionner 500 images
2	Filigrane visible : « © 2025 Nom » — position « Unten M » (en bas au centre), opacité 25–40 %
3	Activer l'option « Alle Metadaten löschen » (supprimer toutes les métadonnées) — supprime EXIF, GPS, IPTC et XMP de toutes les images produites
4	La mention d'auteur figure dans le filigrane visible ; l'édition EXIF en masse champ par champ (auteur/copyright) n'existe pas — au besoin, image par image dans la zone EXIF
5	Format d'export : JPG pour la livraison (qualité non réglable, valeur système) ; pour une archive PNG, lancer une seconde passe
6	Lancer le lot
Résultat	500 images en ~10 minutes (valeur indicative)

12.4 Contexte pédagogique (Pro)

Objectif pédagogique	Démonstration avec Stego-Lab
Comprendre la stéganographie LSB	Intégrer du texte ; comparer l'original et le résultat avec un outil externe (histogramme) — Stego-Lab n'affiche pas d'histogramme
Éprouver le chiffrement AES	Activer la protection par mot de passe, décoder sans mot de passe → erreur
Comprendre PBKDF2 et le sel	Intégrer deux fois le même mot de passe → résultat différent à chaque fois à cause du sel aléatoire
Analyser la norme EXIF	Analyser entièrement une photo d'appareil
Confidentialité du GPS	Voir le GPS → le supprimer (« Alle Metadaten löschen » est gratuit, les champs GPS sont Pro) → vérifier le résultat
Sans perte ou avec perte	Encoder en PNG, enregistrer en JPEG avec un outil externe → le décodage échoue
Calcul de capacité	Dimensions de l'image → formule → comparer avec l'app

Questions fréquentes

CHAPITRE 13

Q1: Peut-on utiliser le JPEG pour la stéganographie ?

R : Pour l'intégration, non : la compression JPEG détruit irrémédiablement les données LSB, Stego-Lab n'exporte donc qu'en PNG ou TIFF. En lecture, l'app sait en revanche décoder les anciens JPG Stegosuite 0.8 (procédé F5, décodage seul).

Q2: Quelle peut être la taille du contenu à intégrer ?

R : Capacité (octets) = $(L \times H \times 3) \div 8$ – données de trame (10 octets, 54 octets avec mot de passe, plus le nom de fichier). Une image de 12 MP (3024×4032) offre $\approx 4,57$ Mo (4,36 Mio). Stego-Lab affiche la capacité restante en temps réel.

Q3: Que se passe-t-il si j'oublie le mot de passe ?

R : Le mot de passe n'est jamais enregistré ; il n'existe ni porte dérobée, ni clé maîtresse, ni récupération. Seule l'attaque par liste de mots, proposée en option dans la zone Décodeur (Pro), peut retrouver un mot de passe faible figurant dans la liste ; avec un mot de passe robuste, le contenu reste définitivement inaccessible.

Q4: Peut-on détecter des données stéganographiques ?

R : Visuellement : non. Statistiquement (analyse RS, khi-deux) : c'est détectable. Avec AES-256, le contenu reste malgré tout illisible.

Q5: L'app fonctionne-t-elle entièrement hors ligne ?

R : Oui. Aucune connexion réseau. Toutes les fonctions sont disponibles hors ligne.

Q6: Les images sont-elles enregistrées dans le cloud ?

R : Non. Stego-Lab ne transmet aucune donnée. Toutes les étapes se déroulent exclusivement en local.

Q7: Peut-on décoder sur iPhone ce qui a été encodé sur Mac ?

R : Oui. Le format interne est compatible d'une plateforme à l'autre.

Q8: Quel format donne la meilleure qualité ?

R : Le TIFF (non compressé) pour l'archivage. Le PNG pour un stockage sans perte avec des fichiers plus légers.

Q9: Les formats RAW sont-ils pris en charge ?

R : En entrée : DNG, CR2, CR3, NEF, ARW, ORF... Pour la stéganographie, la sortie est toujours en PNG ou TIFF. Pour un filigrane uniquement visible en mode Lot, le JPG est également possible (pas lorsque la couche invisible robuste est active) ; la zone EXIF exporte dans le format du fichier source.

Q10: Peut-on utiliser un mot de passe différent par image ?

R : Oui. Chaque image peut recevoir son propre mot de passe.

Q11: L'app Raccourcis est-elle prise en charge ?

R : C'est prévu pour une version future.

Q12: Quelle différence entre filigrane visible et invisible ?

R : Visible : dessiné directement dans l'image. Invisible : dissimulé via le LSB, extractible uniquement avec l'app.

Q13: Dois-je étiqueter les images produites par IA ?

R : Cela dépend. Depuis le 2 août 2026, l'article 50, par. 4 de l'AI Act oblige les déployeurs à indiquer, pour un hypertrucage (deep fake) publié, que le contenu a été généré ou manipulé par une IA ; pour une œuvre manifestement artistique ou satirique, une mention allégée suffit, et l'usage purement personnel n'est pas visé. Les fournisseurs de systèmes d'IA sont soumis au marquage lisible par machine du par. 2. Stego-Lab fournit l'outil, pas le conseil juridique (voir 9.7).

Q14: L'étiquetage survit-il aux réseaux sociaux ou à une compression JPEG ?

R : L'étiquette visible oui (elle fait partie des pixels). Les métadonnées dépendent de la plateforme — beaucoup les suppriment au téléversement. La couche invisible (LSB), non.

Q15: Comment supprimer toutes les métadonnées d'un coup ?

R : Zone EXIF : bouton « Alle Metadaten löschen » (supprimer toutes les métadonnées, gratuit), puis « Änderungen anwenden » (appliquer les modifications ; Mac : « Metadaten anwenden »). Pour toute une série : zone « Batch », option « Alle Metadaten löschen » (Pro).

Annexe technique

CHAPITRE 14

14.1 Processus d'encodage LSB

Étape	Description
1. Préparer la charge utile	Texte en octets UTF-8 ; images et fichiers repris tels quels, octet par octet, sans réencodage ni compression (seules les photos prises avec l'appareil photo sont d'abord enregistrées en PNG). Pour les images et les fichiers, le nom du fichier est placé en tête : 2 octets de longueur (big-endian) + nom en UTF-8.
2. Chiffrer (facultatif, Pro)	Avec mot de passe : sel aléatoire de 16 octets (SecRandomCopyBytes), clé de 256 bits dérivée par PBKDF2-HMAC-SHA256 (600 000 itérations), chiffrement AES-256-GCM avec un nonce aléatoire de 12 octets (CryptoKit). Le tag d'authentification GCM de 16 octets est ajouté au chiffré ; le nom du fichier est chiffré avec le contenu.
3. Assembler la trame	En-tête de 10 octets (identifiant de format « PV2 », version, longueur, indicateurs), suivi du sel et du nonce en cas de chiffrement, puis de la charge utile ou du chiffré avec son tag et, le cas échéant, du bloc d'étiquetage IA non chiffré. Si la trame dépasse la capacité de l'image, Stego-Lab s'arrête avant de modifier le moindre pixel.
4. Remplacer les LSB	La trame est écrite bit par bit, en commençant par le bit de poids fort de chaque octet : pour chaque pixel, successivement dans le bit de poids faible de R, V et B, ligne par ligne à partir du premier pixel (row-major order). Exactement 1 bit par canal ; le canal alpha n'est pas utilisé.
5. Sortie	Enregistrement en PNG ou TIFF (sans perte, 8 bits par canal) ; la transparence éventuelle de l'image porteuse n'est pas conservée. Les données LSB sont préservées.

14.2 Format de trame interne

L'en-tête de trame interne de Stego-Lab est écrit en premier dans la couche LSB de l'image porteuse, suivi des données utiles. Ce format est compatible d'une plateforme à l'autre (iOS, iPadOS, macOS).

Zone	Taille	Contenu
MAGIC	4 octets	0x50 0x56 0x32 0x00 (« PV2 » + octet nul) – identifie les données Stego-Lab dans la couche LSB ; « PV1 » (format de développement) est également accepté en lecture seule
VERSION	1 octet	Version du format, actuellement 0x02 (non évaluée à la lecture)
PAYLOAD_LENGTH	4 octets	Entier non signé de 32 bits, big-endian : longueur de la charge utile en octets – en cas de chiffrement, longueur du chiffré tag de 16 octets compris (sel et nonce exclus) ; sinon, longueur de la charge utile en clair, préfixe de nom compris

Zone	Taille	Contenu
FLAGS	1 octet	Bit 0 = nature du contenu (1 = texte, 0 = image ou fichier) · bit 1 = chiffré · bit 2 = préfixe de nom de fichier en tête de la charge utile · bit 3 = bloc d'étiquetage IA en fin de trame (depuis la version 1.1, traitement par lot avec couche robuste uniquement, Pro) · bits 4 à 7 = 0. Aucun champ de type ou MIME, aucune compression.
SALT	16 octets	Uniquement si bit 1 : sel aléatoire pour PBKDF2 (SecRandomCopyBytes)
NONCE	12 octets	Uniquement si bit 1 : nonce AES-GCM aléatoire (CryptoKit)
CHARGE UTILE	= PAYLOAD_LENGTH	Sans mot de passe : [préfixe de nom] + contenu en clair. Avec mot de passe : chiffré AES-256-GCM de [préfixe de nom] + contenu, terminé par le tag d'authentification GCM de 16 octets
– Préfixe de nom	2 + n octets	Uniquement si bit 2, partie intégrante de la charge utile (comprise dans PAYLOAD_LENGTH) : longueur n (entier de 16 bits, big-endian) + nom du fichier en UTF-8 ; chiffré avec le contenu si un mot de passe est défini
BLOC IA	7 + n octets	Uniquement si bit 3, après la charge utile, non compris dans PAYLOAD_LENGTH : « AIDT » + version 0x01 + longueur n (16 bits, big-endian) + « AIDISC1: » suivi du JSON ($n \leq 2\,048$) ; toujours en clair, uniquement avec une sortie PNG/TIFF

14.3 Gestion des erreurs

Message d'erreur	Cause	Solution
Remarque	L'interface de Stego-Lab 1.1 est en allemand ; les messages sont cités dans leur libellé d'origine, avec une traduction entre parenthèses. Les nombres qui y figurent dépendent de l'image.	—
« Zu groß: 5.2 MB (max 4.4 MB) » (trop volumineux : 5,2 Mo, max. 4,4 Mo) ; sur iOS au chargement : « Die Datei ist 5,2 MB groß, das Trägerbild fasst 4,4 MB. Bitte ein größeres Trägerbild oder eine kleinere Datei wählen. » (le fichier fait 5,2 Mo, l'image porteuse en contient 4,4 ; choisir une porteuse plus grande ou un fichier plus petit)	Contenu et données de trame (en-tête, sel, nonce, tag, nom de fichier, bloc IA) supérieurs à la capacité de l'image porteuse	Choisir une image porteuse plus grande ou un contenu plus petit
« Falsches Passwort oder beschädigte Daten » (mot de passe erroné ou données endommagées)	Échec de la vérification du tag d'authentification GCM : mot de passe erroné ou données modifiées	Vérifier le mot de passe ; utiliser l'original non modifié

Message d'erreur	Cause	Solution
« Kein erkanntes Steganographie-Format (PV1 oder StegSuite) in diesem Bild. » (aucun format stéganographique reconnu dans cette image)	Aucun identifiant Stego-Lab dans la couche LSB : image non encodée, ou image réenregistrée avec perte (JPEG, HEIC), redimensionnée ou retouchée après l'intégration	Utiliser l'original PNG/TIFF non modifié
« Header beschädigt — möglicherweise kein kodiertes Bild. » / « Payload abgeschnitten — Bild möglicherweise bearbeitet. » (en-tête endommagé / charge utile tronquée ; macOS uniquement)	Longueur invraisemblable dans l'en-tête, ou image recadrée ou retouchée après l'intégration	Utiliser l'original non modifié
« Bild konnte nicht geladen werden. » / « Datei konnte nicht gelesen werden oder ist kein gültiges Bild. » (image illisible / fichier illisible ou image non valide)	Le fichier n'est pas une image lisible	Utiliser PNG, JPEG, TIFF ou HEIC
« Datei ist zu groß (312.0 MB). Maximal 250 MB erlaubt. » / « Bild hat zu viele Pixel (340 MP). Maximal 300 MP erlaubt — möglicherweise eine präparierte Datei. » (fichier trop volumineux, max. 250 Mo / trop de pixels, max. 300 MP, fichier peut-être piégé)	Limites de protection contre les fichiers piégés dépassées	Utiliser un fichier plus petit
« PNG-Export fehlgeschlagen » ou « TIFF-Export fehlgeschlagen » (échec de l'exportation PNG/TIFF ; iOS) ; message système sur macOS	L'image n'a pas pu être écrite à l'emplacement choisi	Vérifier l'emplacement et les droits d'accès

Glossaire

CHAPITRE 15

Terme	Description
AES-256-GCM	Advanced Encryption Standard, clé de 256 bits, mode GCM (AEAD). FIPS 197, NIST SP 800-38D.
AI Act européen, art. 50	Obligations de transparence du règlement européen sur l'IA : les fournisseurs doivent marquer les sorties d'IA dans un format lisible par machine (par. 2) ; les déployeurs doivent indiquer, pour un hypertrucage, que le contenu a été généré ou manipulé artificiellement (par. 4). Applicable depuis le 2 août 2026.
Analyse RS	Analyse Regular-Singular — détecteur statistique de LSB.
Canal alpha	Quatrième canal de l'image (R,V,B+A) pour la transparence (0–255).
Digital Source Type	Champ des NewsCodes IPTC indiquant l'origine d'une image de façon lisible par machine, par ex. « entièrement générée par IA » ou « retouchée par IA » ; élément central de l'étiquetage au titre de l'article 50.
DNG	Format RAW ouvert (Adobe) pour les données de capteur – non compressées, compressées sans perte ou (depuis DNG 1.4) avec perte.
EXIF 2.32	Norme des métadonnées dans les fichiers image (CIPA DC-X008).
Filigrane	Marque de paternité, visible ou invisible, apposée sur un média.
GCM	Mode d'opération AES (Galois/Counter Mode) : chiffre et authentifie en une seule opération (AEAD). Dans Stego-Lab, le tag d'authentification GCM de 16 octets garantit l'intégrité du chiffré ; aucun HMAC séparé n'est nécessaire.
HEIC	Fichier image au format conteneur HEIF (ISO/IEC 23008-12) avec codage HEVC, adopté par Apple comme format par défaut. Généralement avec perte.
HMAC-SHA256	Code d'authentification de message à clé fondé sur SHA-256 (RFC 2104). Dans Stego-Lab, il sert uniquement de fonction pseudo-aléatoire au sein de PBKDF2, et non au contrôle d'intégrité, assuré par le tag d'authentification GCM.
Khi-deux	Méthode statistique de stéganalyse pour détecter le LSB.
LSB	Bit de poids le plus faible d'un octet. Écart de couleur de ± 1 — invisible.
Nonce	Valeur initiale aléatoire de 12 octets pour AES-GCM ; garantit l'unicité du chiffré.
PBKDF2-HMAC-SHA256	Dérivation de clé à partir du mot de passe et du sel, avec 600 000 itérations (OWASP 2023).
PNG	Format matriciel sans perte. ISO/IEC 15948. Format principal de Stego-Lab.
PSNR	Mesure de qualité d'image en dB. > 51 dB = modification invisible.

Terme	Description
PV1	Format de développement de Stego-Lab (du 31 mars au 2 avril 2026, dérivation de clé HKDF-SHA256 avec sel fixe), jamais publié. L'app ne fait plus que le lire ; les nouveaux contenus sont écrits exclusivement en PV2.
PV2	Format de trame de Stego-Lab depuis la version 1.0 : en-tête de 10 octets (identifiant de format « PV2 », version, longueur, indicateurs), en cas de chiffrement sel, nonce et chiffré AES-256-GCM avec tag, et en option un bloc IA non chiffré (voir 14.2).
RAW	Format brut de capteur. Sans perte, propre à chaque fabricant.
Sel	Valeur aléatoire utilisée par PBKDF2. Empêche les attaques par table arc-en-ciel.
Stéganographie	Dissimulation d'informations dans un support.
TIFF 6.0	Format d'image sans perte. Compression LZW/ZIP/RAW. Spécification Adobe.
Trailer AI-DISCLOSURE (bloc de fin PV2)	Données PV2 facultatives et non chiffrées (préfixe « AIDISC1: ») placées après la charge utile – elles portent l'étiquetage IA de façon invisible, dans les pixels (Pro, lot). Elles survivent à la suppression des métadonnées, mais pas à une recompression avec perte (voir 9.6).
UTF-8	Codage universel des caractères. 1 à 4 octets. Compatible ASCII.

Positionnement

CHAPITRE 16

16.1 Comparatif des fonctions

Fonction	Stego-Lab	Service en ligne	Outil de bureau	App mobile
Stéganographie LSB	OUI	En partie	OUI	Rarement
AES-256	OUI	Rarement	En partie	Non
Filigrane visible	OUI	OUI	OUI	OUI
Filigrane invisible	OUI	Rarement	En partie	Non
Édition EXIF	OUI	En partie	OUI	En partie
Suppression du GPS	OUI	En partie	OUI	En partie
Traitement par lot	OUI	Rarement	OUI	Rarement
Entièrement hors ligne	OUI	NON	OUI	En partie
Natif sur iOS/iPadOS	OUI	Navigateur	NON	OUI
Natif sur macOS	OUI	Navigateur	OUI	NON
Sans compte	OUI	Souvent NON	OUI	Souvent NON

16.2 Publics visés

Public visé	Bénéfice principal
Photographes	Gestion EXIF, protection GPS, filigranage par lot
Créateurs de contenu	Filigranes de copyright, en local et rapidement
Utilisateurs soucieux de leur vie privée	Traitement local, suppression du GPS
Experts en sécurité informatique	Démonstrations de stégano, exercices de stéganalyse
Journalistes	Intégration chiffrée de preuves
Archivistes	Édition EXIF en masse, entretien des métadonnées
Enseignants et étudiants	Démonstrations concrètes des concepts
Particuliers	Archivage discret de documents sensibles

Référence des flux de travail

CHAPITRE 17

17.1 Flux d'encodage (Pro)

Étape	Action	Remarque
1	Charger une image porteuse ≥ 8 MP (PNG/TIFF recommandé ; JPEG, HEIC et RAW sont également chargés)	Vérifier la capacité
2	Choisir le type de contenu : texte / image / fichier	Indicateur de capacité
3	Saisir un mot de passe (12 caractères minimum, de préférence une phrase secrète)	Recommandé ; l'app avertit en dessous de 8 caractères
4	Sortie : PNG ou TIFF	PNG = plus léger
5	Lancer l'encodage	Progression
6	Tester dans la zone Decode	Contrôle qualité
7	Enregistrer ou partager	Conservez l'original !

17.2 Nettoyage EXIF

Étape	Action
1	Charger l'image dans la zone EXIF
2	Vérifier les champs GPS (« Breitengrad », « Längengrad », « Höhe » — latitude, longitude, altitude)
3	Supprimer les coordonnées GPS : vider les trois champs (Pro) — les autres balises GPS restent ; suppression complète uniquement avec « Alle Metadaten löschen » (supprimer toutes les métadonnées, gratuit)
4	Copyright : saisir « © 2025 Nom » (gratuit)
5	Renseigner le champ « Künstler » (auteur) (gratuit)
6	« Änderungen anwenden » (appliquer les modifications ; Mac : « Metadaten anwenden »), puis exporter
7	Vérifier l'EXIF

Étape	Action
ou	« Alle Metadaten löschen » (gratuit), puis « Änderungen anwenden »

17.3 Lot pour les réseaux sociaux (Pro)

Étape	Réglage
1	Sélectionner toutes les photos dans la zone « Batch »
2	Filigrane visible : « @Pseudo © 2025 »
3	Position : « Unten M » (en bas au centre) ou « Unten R » (en bas à droite)
4	Opacité : 25–40 % (curseur « Deckkraft », plage 15–100 %)
5	Format d'export : JPG (mode « Sichtbar » (visible) uniquement ; qualité non réglable)
6	Activer l'option « Alle Metadaten löschen » (supprimer toutes les métadonnées) — le GPS disparaît avec le reste
7	Lancer le lot → vérifier

17.4 Étiqueter une image IA

Étape	Action	Remarque
1	Charger l'image dans Encode ou dans la zone « Batch »	PNG/TIFF recommandé
2	Ouvrir la section « KI-Kennzeichnung » (étiquetage IA), activer l'interrupteur « Als KI-Bild kennzeichnen » (étiqueter comme image IA)	Vérifier le voyant
3	Choisir la variante : « vollständig KI-generiert » (entièrement générée par IA) / « KI-bearbeitet » (retouchée par IA)	Texte d'étiquette prérempli
4	Renseigner le générateur si besoin (par ex. « Midjourney v7 »)	N'apparaît que dans les métadonnées
5	Vérifier la position de l'étiquette visible dans la grille 3×3	Par défaut : en bas à gauche
6	Batch/Pro : activer au besoin « Robuste unsichtbare Schicht (Pro) » (couche invisible robuste)	Impose PNG/TIFF

Étape	Action	Remarque
7	Lancer l'encodage ou le lot, vérifier que le voyant est vert	Vert = tous les éléments sont en place

Évaluation de la sécurité

CHAPITRE 18

18.1 Modèle de menaces

Menace	Sans mot de passe	Avec AES-256	Évaluation
Inspection visuelle	Sûr	Sûr	OK
Analyse RS	DéTECTABLE	Canal visible, contenu non	Acceptable avec mot de passe
Khi-deux	DéTECTABLE	Canal visible, contenu non	Acceptable avec mot de passe
Force brute (contenu)	Lisible	Pratiquement impossible	Sûr avec mot de passe
Conversion en JPEG	Détruit	Détruit	Conservez le PNG/TIFF !
Interception cloud	Sans objet	Sans objet	Aucun cloud

18.2 Recommandations pour les mots de passe

Exigence	Recommandation	Justification
Longueur minimale	12 caractères	En dessous de 8 caractères, attaquable même avec PBKDF2
Jeu de caractères	Majuscules + minuscules + chiffres + symboles	Espace de recherche exponentiellement plus grand
Mots du dictionnaire	À éviter	Les attaques par dictionnaire sont efficaces
Réutilisation	Jamais	Un mot de passe compromis met tout en danger
Conservation	Gestionnaire de mots de passe	Stockage chiffré et sûr

18.3 Revue de sécurité interne avant publication

Entre avril et septembre 2026, le code source de Stego-Lab a fait l'objet, à plusieurs reprises, de revues de sécurité internes, la dernière avant la soumission de la version 1.1. Ces revues ont été réalisées avec l'assistance de l'IA ; le développeur en a évalué et mis en œuvre les résultats. Il s'agit de revues techniques internes, et non d'un audit indépendant ni d'une certification. Le rapport de la première revue, du 10 avril 2026, est consultable dans le dépôt public sous le nom SECURITY-AUDIT.md. Aucun des rapports n'a relevé de constat critique ; les constats classés « élevés » ont été corrigés avant la soumission. Les limites connues figurent dans le tableau ; quelques points de gravité faible sont documentés et restent ouverts.

Domaine	Aspects examinés	Statut
Cryptographie	AES-256-GCM ; PBKDF2-HMAC-SHA256, 600 000 itérations ; sel aléatoire de 16 octets ; nonce de 12 octets ; les clés ne sont jamais enregistrées ni transmises	examiné
Mots de passe en mémoire vive	Les mots de passe et les clés dérivées ne sont pas effacés explicitement de la mémoire vive par l'app (limite de Swift/SwiftUI ; constat S-01/N-02, gravité faible)	limite connue
Formats hérités (lecture seule)	PV1 (format de développement, jamais publié), Stegosuite et F5 : procédés plus faibles ou obsolètes, lecture uniquement, avertissement affiché dans l'app	limite connue
EXIF / métadonnées	Nettoyage des métadonnées ; aucune reprise involontaire des données GPS et de l'appareil photo	examiné
Accès aux fichiers	Protection contre la traversée de répertoires, nettoyage des noms de fichiers externes, limites de taille et de pixels, bac à sable (version App Store)	examiné
Déverrouillage Pro	Blocage dans l'interface et, pour la dissimulation et le traitement par lot, dans la logique applicative ; vérification des transactions StoreKit	examiné
Confidentialité	Aucune connexion réseau propre, aucune télémétrie, aucun cloud (exceptions : traitement des achats via StoreKit d'Apple, liens ouverts dans le navigateur)	examiné
Filigranes	Mode combiné : visible d'abord, puis invisible ; les données cachées sont préservées	examiné
Plateformes	Couche de sécurité commune (StegoEngine) pour iOS, iPadOS et macOS	examiné

■ Le rapport de la revue du 10 avril 2026 est consultable dans le dépôt public sous le nom SECURITY-AUDIT.md ; un résumé des revues ultérieures figure dans CHANGELOG.md. Les rapports détaillés des revues ultérieures sont conservés en interne dans les archives du projet et ne font pas partie de la documentation publiée. Pour toute question de sécurité, contactez l'assistance par e-mail.

Assistance et contact

CHAPITRE 19

19.1 Canaux d'assistance

Canal	Description
Avis sur l'App Store	Retours publics
Lien d'assistance App Store	Lien d'assistance direct
Infos dans l'app	Aide-mémoire intégré
Mises à jour	Mises à jour régulières avec corrections

19.2 Limitations connues

Limitation	Détail
JPEG en stéganographie	Non pris en charge — utiliser PNG/TIFF
GIF animés	Première image seulement
Sortie RAW	En entrée seulement ; sortie en PNG/TIFF
Stégano par lot	Même contenu pour toutes les images
App Raccourcis	Prévu
Récupération de mot de passe	Impossible

Table des tableaux

CHAPITRE 20

N°	Intitulé	Chapitre
T-01	Fiche signalétique de l'app	Couverture
T-02	Configuration requise	2.1
T-03	Étapes d'installation	2.2
T-04	Navigation principale	3.1
T-05	Zone Encoder	3.2
T-06	Zone Décoder	3.3
T-07	Spécification LSB	4.2
T-08	Capacités de texte	4.3
T-09	Chiffrement	4.4
T-10	Paramètres de filigrane	5.1
T-11	Options de positionnement	5.3
T-12	Champs EXIF (lisibles)	6.2
T-13	Champs EXIF modifiables	6.3
T-14	Champs GPS	6.4
T-15	Paramètres du mode lot	7
T-16	Formats d'entrée	8
T-17	Formats de sortie	8
T-18	Recommandations de format	8
T-19	Champs d'étiquetage IA écrits	9.3
T-20	Vue d'ensemble de la confidentialité	10.1
T-21	Étapes du chiffrement	10.2
T-22	Sécurité stéganographique	10.3
T-23	Performances	11.1
T-24	Besoins en mémoire vive	11.2

N°	Intitulé	Chapitre
T-25	Algorithmes et normes	11.3
T-26	Exemple d'utilisation 12.1	12
T-27	Exemple d'utilisation 12.2	12
T-28	Exemple d'utilisation 12.3	12
T-29	Objectifs pédagogiques	12.4
T-30	FAQ (15 entrées)	13
T-31	Gestion des erreurs	14.3
T-32	Glossaire (25 entrées)	15
T-33	Comparatif des fonctions	16.1
T-34	Publics visés	16.2
T-35	Flux de travail (4×)	17
T-36	Modèle de menaces	18.1
T-37	Recommandations pour les mots de passe	18.2
T-38	Limitations	19.2

Historique des versions

CHAPITRE 21

Version	Date	Modifications
1.0	16/04/2026	Première publication pour iPhone et iPad (App Store) : Encode, Decode, EXIF, Batch, Info
1.0	20/04/2026	Première publication pour Mac (Mac App Store) : Verstecken, Entdecken, Batch, EXIF, Info
1.0	04/2026	Versions minimales : iOS 16 / iPadOS 16 / macOS 13 (Mac : Apple Silicon et Intel)
1.0	04/2026	Chiffrement par mot de passe AES-256-GCM (authentifié, tag de 16 octets) ; dérivation de clé PBKDF2-HMAC-SHA256, 600 000 itérations, sel aléatoire de 16 octets (format PV2)
1.0	04/2026	Chemin de lecture pour les images issues des versions de développement antérieures à la publication (format PV1, HKDF-SHA256) — déchiffrement uniquement, jamais distribué pour chiffrer
1.0	04/2026	Mac : lecture des images PNG Stegosuite (déchiffrement uniquement : AES-128-CTR, PBKDF2-HMAC-SHA1, générateur de positions MD5)
1.0	04/2026	Mac : attaque par dictionnaire de mots de passe dans la zone Décoder, avec une liste fournie par l'utilisateur
1.0	04/2026	Lot (Pro) : filigranes visibles et invisibles, contenus dissimulés avec chiffrement facultatif
1.0	04/2026	Images porteuses : PNG, TIFF, JPEG, HEIC, divers formats RAW
1.0	04/2026	Entièrement local — pas de cloud
1.1	2026	Versions minimales relevées : iOS 17 / iPadOS 17 / macOS 14 (auparavant iOS 16 / iPadOS 16 / macOS 13) lors du passage à Xcode 27 ; la version 1.0 reste utilisable sur les appareils plus anciens
1.1	2026	Chiffrement des nouveaux contenus inchangé depuis la version 1.0 (AES-256-GCM, PBKDF2-HMAC-SHA256, 600 000 itérations, format PV2)
1.1	2026	Sélecteur de mode sombre (système/clair/sombre) sur iOS/iPadOS
1.1	2026	iPhone/iPad : attaque par dictionnaire de mots de passe dans la zone Décoder ; sur les deux plateformes désormais avec la liste Nmap fournie (Mac : attaque disponible depuis la version 1.0)
1.1	2026	Sélecteur de fichiers unifié (iOS) avec coordinateur de feuilles
1.1	2026	Durcissement de la sécurité : parité AES, nettoyage EXIF, verrouillage Pro
1.1	2026	iPhone/iPad : liens de don externes supprimés ; Mac : suit le mode clair/sombre du système

Version	Date	Modifications
1.1	2026	iPhone/iPad : lecture des images PNG Stegosuite (déchiffrement uniquement) — sur Mac depuis la version 1.0
1.1	2026	Décodeur F5/JPG : les anciens JPG Stegosuite 0.8 (stéganographie dans le domaine DCT) peuvent être ouverts — avec message ET fichier joint dissimulé dans une même image
1.1	2026	Indicateur de progression du décodage pour les chemins hérités coûteux (Stegosuite/F5)
1.1	2026	Avertissement de détection pour les formats cryptographiques hérités plus faibles (PV1 / Stegosuite) — lecture autorisée, écriture non
1.1	2026	Dissimuler directement une photo prise par l'appareil : intégration en une étape, sans passer par la photothèque (Mac : mémoire vive uniquement ; iPhone/iPad : fichier temporaire dans le conteneur de l'app), avec curseur de qualité ; sur macOS avec Continuity Camera
1.1	2026	Appareil photo iOS : l'orientation EXIF est inscrite dans les pixels lors de l'intégration — les prises de vue sont intégrées dans le bon sens
1.1	2026	Reprendre une photo comme image porteuse depuis le menu Partager / « Ouvrir avec » (iPhone/iPad : « Copier vers Stego-Lab », Mac : « Ouvrir avec Stego-Lab »)
1.1	2026	Zone Encode : boutons plus compacts, à icône seule, pour une interface plus claire
1.1	2026	Étiquetage IA selon l'art. 50 de l'AI Act : pré-réglage dans Encode/Batch, badge dans Decode/EXIF, chapitre du manuel
1.1	2026	Supprimer toutes les métadonnées en un clic (onglet EXIF, gratuit) et par lot (Pro)

Fonctions prévues

Fonction	Statut
Intégration à l'app Raccourcis	Prévu
Extension de partage	Écartée volontairement (sécurité : nécessiterait un groupe d'apps)
Mode 2 LSB	Piste envisagée
Détecteur de stéganalyse	Prévu
Métadonnées IPTC	Réalisé (1.1)
Métadonnées XMP	Réalisé (1.1)

Achat intégré Stego-Lab Pro

CHAPITRE 22

Stego-Lab est disponible gratuitement sur l'App Store. Il n'existe qu'un seul achat intégré : « Stego-Lab Pro ». Il se règle une seule fois, sans abonnement ni date d'expiration, et débloque définitivement les fonctions indiquées ci-dessous. Il n'existe aucun autre pack ni aucune autre extension. Le prix en vigueur est affiché sur l'App Store.

22.1 Gratuit et Pro en un coup d'œil

Le déblocage passe exclusivement par l'App Store — sans clé de licence, sans numéro de série et sans intervention du développeur. Le chiffrement n'est pas vendu séparément : la protection par mot de passe fait partie de Stego-Lab Pro. Le tableau suivant reflète le comportement réel de l'app.

Zone	Gratuit	En plus avec Stego-Lab Pro
Encode	Charger une image porteuse ; apposer l'étiquette IA visible et les métadonnées IA, puis enregistrer l'image	Intégrer de manière invisible un texte, une image ou un fichier (LSB) ; protection facultative par mot de passe (AES-256-GCM, PBKDF2-HMAC-SHA256, 600 000 itérations) ; prise de vue directe avec l'appareil photo (Mac : Continuity Camera)
Decode	Afficher, copier et partager un texte intégré sans chiffrement	Images et fichiers intégrés ; contenus protégés par mot de passe, y compris les images PNG Stegosuite et JPG F5 (lecture seule) ; attaque par dictionnaire avec la liste Nmap fournie ou une liste personnelle
EXIF	Afficher toutes les métadonnées ; modifier description, auteur, copyright et logiciel ; supprimer toutes les métadonnées en un clic	Modifier les champs appareil, objectif, date, exposition, commentaire et GPS
Batch	Charger des images, vérifier les réglages et l'aperçu ; exporter une image unique avec un filigrane visible (texte ou logo)	Exporter plusieurs images en une passe et des séries entières (traitées l'une après l'autre) : filigranes visibles, invisibles et combinés, étiquetage IA avec couche invisible robuste, suppression de toutes les métadonnées
Info	Aide-mémoire, informations de version, fenêtre Pro	—

22.2 Achat et restauration

L'achat s'effectue dans la fenêtre Pro de l'app (accessible depuis la zone Info ou depuis toute mention Pro) avec le bouton « Stego-Lab Pro freischalten » (débloquer Stego-Lab Pro) ; le paiement et la transaction sont gérés par l'App Store. Au démarrage, l'app vérifie elle-même le statut de l'achat ; sur un autre appareil utilisant le même identifiant Apple, l'achat est donc en général repris automatiquement. Sinon, le bouton « Käufe wiederherstellen » (restaurer les achats) de la fenêtre Pro rétablit l'achat.

✓ Stego-Lab Pro est un achat unique — pas d'abonnement, pas de date d'expiration, pas de clé de licence. L'achat et le paiement sont traités exclusivement par Apple ; la restauration se fait dans l'app via « Käufe wiederherstellen » (restaurer les achats) dans la fenêtre Pro.

À propos du développeur / Mentions légales

CHAPITRE 23



Stego-Lab
Développé par
Ing. Christian Raith, BEd
OE3LCR · Wiener Neustadt, Autriche



Stego-Lab a été développé par Ing. Christian Raith (BEd). Il enseigne l'atelier informatique, l'électrotechnique et l'électronique à la HTL Mödling. Ses domaines de prédilection sont la sécurité informatique, les analyses et audits de sécurité, la programmation (surtout Arduino et Raspberry Pi), le développement d'applications de sécurité, de filigranage, de protection du droit d'auteur et de traitement photo, ainsi que la documentation technique et les supports pédagogiques. Il est par ailleurs radioamateur licencié (indicatif OE3LCR, locator JN87ct) et président du club de radioamateurs de Triestingtal à Berndorf.

23.1 Coordonnées du développeur

Propriété	Valeur
Nom	Ing. Christian Raith, BEd
Lieu	Wiener Neustadt, Basse-Autriche, Autriche
Radioamateur	OE3LCR · Locator JN87ct
Courriel d'assistance	stego-lab@proton.me
Site web / projet	www.craith.cloud/stego-lab
GitLab	gitlab.com/RaithChr/stego-lab
Profession	Enseignant à la HTL Mödling — atelier informatique, électrotechnique, électronique
Spécialisations	Sécurité informatique · audits de sécurité · Arduino/Raspberry Pi · développement d'apps · documentation technique

23.2 Autres projets du développeur

Projet	Description	Lien
OE3LCR Ham Radio Dashboard	Application web en direct : données solaires, conditions de propagation, cluster DX, suivi de satellites et météo spatiale.	www.craith.cloud

Projet	Description	Lien
Mesure de fréquence (RP2350)	Fréquencemètre secteur à base de Raspberry Pi Pico 2, écran TFT ST7735 et isolation galvanique par optocoupleur PC817.	gitlab.com/RaithChr/Frequenzmessung-PICO2-50HZ
Stego-Lab (cette app)	Stéganographie, filigranage, EXIF et traitement d'images par lot pour iPhone, iPad et Mac.	gitlab.com/RaithChr/stego-lab

23.3 Dépôt GitLab

Le code source de Stego-Lab est publié sur GitLab (gitlab.com/RaithChr/stego-lab). L'historique des versions figure dans CHANGELOG.md et docs/VERSION-HISTORY.de-en.md ; la procédure de signalement des vulnérabilités est décrite dans SECURITY.md.

Dépôt GitLab

gitlab.com/RaithChr/stego-lab

23.4 Site web

Site du projet

www.craith.cloud/stego-lab

Mentions légales et confidentialité

CHAPITRE 24

24.1 Politique de confidentialité (résumé)

Stego-Lab traite toutes les données de l'utilisateur exclusivement en local, sur son appareil. L'app ne collecte, ne stocke, ne transmet ni ne traite aucune donnée personnelle sur des serveurs externes.

Catégorie de données	Traitement	Transmission externe
Images	Local uniquement	NON
Contenus intégrés	Local uniquement	NON
Mots de passe	En mémoire vive seulement, jamais conservés	NON
Métadonnées EXIF	Local uniquement	NON
Statistiques d'usage	Non collectées	NON
Rapports de plantage	Désactivés	NON
Données publicitaires	Inexistantes	NON
Données de localisation	Jamais demandées	NON

24.2 Licence et conditions d'utilisation

Le code source de Stego-Lab est publié sous licence MIT (gitlab.com/RaithChr/stego-lab, fichier LICENSE). L'app obtenue sur l'App Store est en outre régie par les Conditions générales des Apple Media Services et par le contrat de licence utilisateur final standard d'Apple.

Disposition	Détails
Licence	Le code source de Stego-Lab est placé sous licence MIT (© 2026 Christian Raith ; fichier LICENSE du dépôt). Les éléments tiers (voir 24.3) restent soumis à leurs propres licences. Le nom et la marque verbale « Stego-Lab », le logo, l'icône de l'app et le texte du manuel ne relèvent pas de la licence MIT ; tous droits réservés.
Version App Store	L'app obtenue sur l'App Store est régie par les Conditions générales des Apple Media Services et par le contrat de licence utilisateur final standard d'Apple. Les fonctions Pro sont débloquentées par un achat intégré, sans clé de licence (voir chapitre 22).
Usage autorisé	Stego-Lab est destiné à des usages licites. L'utilisateur est responsable du respect de la législation applicable, notamment des droits d'auteur de tiers.

Disposition	Détails
Limitation de responsabilité	Le logiciel est fourni « en l'état », sans garantie (voir licence MIT). Un mot de passe oublié ne peut pas être récupéré ; une sauvegarde est expressément recommandée.
Modifications	Font foi le fichier LICENSE du dépôt dans sa version en vigueur et le contrat de licence d'Apple ; les exceptions relatives à la marque, au logo, à l'icône de l'app, au texte du manuel et aux éléments tiers demeurent inchangées.

24.3 Frameworks utilisés et éléments tiers

Stego-Lab n'intègre aucune bibliothèque logicielle tierce. La cryptographie, le traitement d'image et l'interface reposent sur les frameworks d'Apple, qui font partie du système d'exploitation et ne sont pas livrés avec l'app. Un seul élément tiers est fourni avec l'app : la liste de mots de passe du projet Nmap. Les fonctions de lecture des anciennes images Stegosuite et F5 ont été transposées en Swift à partir du code source Java de Stegosuite 0.8 (GPL).

Composant	Utilisation dans Stego-Lab	Origine / licence
CryptoKit	AES-256-GCM (chiffrement et déchiffrement) ; HKDF-SHA256 uniquement pour lire les images PV1 ; MD5 et SHA-1 uniquement pour lire les images Stegosuite et F5	Apple, composant du système d'exploitation
CommonCrypto	PBKDF2-HMAC-SHA256 (600 000 itérations) ; PBKDF2-HMAC-SHA1 et AES-128-CTR uniquement pour déchiffrer les images Stegosuite	Apple, composant du système d'exploitation
SecRandomCopyBytes (framework Security)	Sel aléatoire de 16 octets à chaque chiffrement ; le nonce de 12 octets est généré par CryptoKit	Apple, composant du système d'exploitation
Compression	Décompression zlib lors de la lecture des images Stegosuite et F5	Apple, composant du système d'exploitation
ImageIO, CoreGraphics, CoreText	Lecture et écriture des images, accès aux pixels pour le LSB, métadonnées EXIF, IPTC et XMP, police de l'étiquette IA	Apple, composant du système d'exploitation
CoreImage	iPhone/iPad uniquement : orientation des prises de vue	Apple, composant du système d'exploitation
AVFoundation	Prise de vue directe avec l'appareil photo, sur Mac via Continuity Camera	Apple, composant du système d'exploitation
Photos, PhotosUI	iPhone/iPad uniquement : import depuis la photothèque et enregistrement dans celle-ci	Apple, composant du système d'exploitation
StoreKit	Achat intégré « Stego-Lab Pro »	Apple, composant du système d'exploitation

Composant	Utilisation dans Stego-Lab	Origine / licence
SwiftUI, UIKit, AppKit, Foundation, Combine, UniformTypIdentifiers, CoreTransferable	Interface, sélection de fichiers, reconnaissance des types de fichiers	Apple, composant du système d'exploitation
Liste de mots de passe Nmap (passwords.lst)	Liste fournie d'environ 5 000 entrées pour l'attaque par dictionnaire dans la zone Décoder	© 1996–2022 Nmap Software LLC ; Nmap Public Source License (nmap.org/npsl)
Compatibilité de lecture Stegosuite / F5	Lecture seule : extraction et déchiffrement d'images créées avec Stegosuite 0.8 (PNG et JPEG avec F5), y compris le générateur pseudo-aléatoire Java SHA1PRNG transposé en Swift (SHA-1 de CryptoKit)	Transposé en Swift à partir du code source Java de Stegosuite 0.8 (GPL-3.0) ; procédé F5 d'après A. Westfeld, décodeur de Huffman d'après Westfeld/Breslin

24.4 Droit d'auteur et marques

Stego-Lab, le logo Stego-Lab et tous les graphismes associés sont la propriété d'Ing. Christian Raith. Apple, iPhone, iPad, Mac, iOS, iPadOS, macOS, App Store et le logo Apple sont des marques déposées d'Apple Inc.

Ressource	URL
Dépôt GitLab	gitlab.com/RaithChr/stego-lab
Page du projet	www.craith.cloud/stego-lab/fr/
Politique de confidentialité	www.craith.cloud/stego-lab/fr/privacy-policy.html
Assistance	www.craith.cloud/stego-lab/fr/support.html
Courriel d'assistance	stego-lab@proton.me
Politique de confidentialité Apple	apple.com/legal/privacy

Stego-Lab · Version 1.1 · © 2026 Ing. Christian Raith, BEd
 Logiciel : licence MIT · Texte du manuel, marque & logo : tous droits réservés
 iOS · iPadOS · macOS · Apple Silicon & Intel x86_64



Stego-Lab

Version 1.1 · iOS · iPadOS · macOS

© 2026 Christian Raith

Ing. Christian Raith, BEd · OE3LCR

Logiciel : licence MIT · Manuel & marque : tous droits réservés

gitlab.com/RaithChr/stego-lab · www.craith.cloud/stego-lab

stego-lab@proton.me