



NUEVO: etiqueta tus imágenes de IA
Reglamento europeo de IA, art. 50

Stego-Lab

Manual de Usuario & Documentación Técnica

iOS · iPadOS · macOS

Esteganografía · Marcas de agua · EXIF · Lotes · Etiquetado de IA

Propiedad	Valor
Producto	Stego-Lab
Plataformas	iOS 17+ · iPadOS 17+ · macOS 14+
Versión	1.1 · creado el 22/09/2026, 14:19
Idioma del manual	Español
Privacidad	100 % local: sin nube
GitLab	gitlab.com/RaithChr/stego-lab

Índice

1 Introducción	5
1.1 ¿Qué es Stego-Lab?	5
1.2 Ámbitos de uso	5
1.3 Puntos fuertes	5
2 Instalación y primeros pasos	7
2.1 Requisitos del sistema	7
2.2 Instalación	7
2.3 Primer inicio	8
3 Interfaz	9
3.1 Navegación principal	9
3.2 Área Codificar	9
3.3 Área Decodificar	10
4 Esteganografía	12
4.1 Fundamentos	12
4.2 Método LSB	12
4.3 Incrustar contenidos	12
4.4 Protección con contraseña	13
4.5 Decodificación y capacidad	13
5 Marcas de agua	15
5.1 Marcas de agua visibles	15
5.2 Marcas de agua invisibles y combinadas	15
5.3 Posicionamiento y lotes	15
6 Edición de EXIF y metadatos	17
6.1 Fundamentos de EXIF	17
6.2 Campos legibles	17
6.3 Campos editables	18
6.4 Datos GPS	18
6.5 Borrar todos los metadatos	19
7 Lotes y formatos	20
7 Procesamiento por lotes	20
8 Formatos admitidos	20
9 Etiquetar imágenes de IA	23
9.1 Marco legal	23
9.2 Etiquetar en Codificar y en lotes	23
9.3 Campos escritos	23
9.4 Detección al leer	24

9.5 Gratis frente a Pro	24
9.6 Límites	24
9.7 Aviso legal	24
10 Seguridad y privacidad	25
10.1 Procesamiento local	25
10.2 Detalles del cifrado	25
10.3 Seguridad esteganográfica	25
11 Especificaciones técnicas	27
11.1 Rendimiento	27
11.2 Necesidades de memoria	27
11.3 Algoritmos y normas	27
12 Ejemplos de uso	29
12.1 Protección de documentos privados (Pro)	29
12.2 Prueba de autoría (Pro)	29
12.3 Flujo del fotógrafo, 500 imágenes (Pro)	29
12.4 Contexto educativo (Pro)	30
13 Preguntas frecuentes	31
14 Anexo técnico	33
14.1 Proceso de codificación LSB	33
14.2 Formato de trama interno	33
14.3 Gestión de errores	34
15 Glosario	36
16 Posicionamiento	38
16.1 Comparativa de funciones	38
16.2 Públicos objetivo	38
17 Referencia de flujos de trabajo	39
17.1 Flujo de codificación (Pro)	39
17.2 Limpieza de EXIF	39
17.3 Lote para redes sociales (Pro)	40
17.4 Etiquetar una imagen de IA	40
18 Evaluación de seguridad	41
18.1 Modelo de amenazas	41
18.2 Recomendaciones para contraseñas	41
18.3 Revisión de seguridad interna previa a la publicación	41
19 Soporte y contacto	43
19.1 Canales de soporte	43
19.2 Limitaciones conocidas	43

20 Índice de tablas	44
21 Historial de versiones	46
Funciones previstas	47
22 Compra integrada Stego-Lab Pro	48
22.1 Free y Pro de un vistazo	48
22.2 Compra y restauración	48
23 Sobre el desarrollador / Aviso legal	50
23.1 Datos del desarrollador	50
23.2 Otros proyectos del desarrollador	50
23.3 Repositorio de GitLab	51
23.4 Sitio web	51
24 Aspectos legales y privacidad	52
24.1 Política de privacidad (resumen)	52
24.2 Licencia y condiciones de uso	52
24.3 Frameworks utilizados y componentes de terceros	53
24.4 Derechos de autor y marcas	54

Introducción

CAPÍTULO 1

1.1 ¿Qué es Stego-Lab?

Stego-Lab es una app nativa para iPhone, iPad y Mac que reúne cinco áreas de herramientas: esteganografía, marcas de agua, edición de EXIF y metadatos, etiquetado de imágenes generadas por IA y procesamiento de imágenes por lotes. Todos los datos de imagen se procesan exclusivamente en local: sin nube ni servidores externos. La app no establece por sí misma ninguna conexión de red; las únicas excepciones son la compra integrada a través de StoreKit de Apple y los enlaces que el usuario decide abrir en el navegador.

1.2 Ámbitos de uso

Ámbito	Descripción
Archivo privado	Incrustar documentos sensibles de forma invisible en fotos
Protección del derecho de autor	Incrustar de forma invisible una mención de autoría (texto, imagen o archivo): no es una firma criptográfica; no resiste una recompresión JPEG (Pro)
Fotografía	Limpiar EXIF, quitar GPS, fijar el copyright
Series de imágenes	Marcas de agua por lotes en colecciones enteras
Periodismo	Incrustar pruebas de forma cifrada
Docencia	Demostrar en la práctica los conceptos de esteganografía
Creadores de contenido	Marcas de agua de copyright para redes sociales
Seguridad informática	Estudiar canales de imagen encubiertos

1.3 Puntos fuertes

Característica	Descripción
Totalmente local	Sin nube, sin telemetría; la app no establece por sí misma ninguna conexión de red (excepción: compra integrada a través de StoreKit)
Multiplataforma	iPhone, iPad, Mac: mismo formato de datos (PV2) y mismo núcleo funcional; el manejo, la selección de archivos y algunas funciones adicionales varían según la plataforma
Herramientas reunidas	Estegano + marca de agua + EXIF + etiquetado de IA + lotes en una sola app

Característica	Descripción
Cifrado AES-256	Protección opcional con contraseña (AES-256-GCM, Pro) para texto, imágenes y archivos ocultos; la cabecera de formato y el etiquetado de IA invisible permanecen deliberadamente sin cifrar
Salida sin pérdidas	PNG + TIFF para la máxima integridad de los datos

Instalación y primeros pasos

CAPÍTULO 2

2.1 Requisitos del sistema

Plataforma	Mínimo	Recomendado	Arquitectura
iPhone	iOS 17.0	Versión de iOS más reciente mantenida por Apple	ARM64 (A12 o posterior)
iPad	iPadOS 17.0	Versión de iPadOS más reciente mantenida por Apple	ARM64 (A10 o posterior)
Mac	macOS 14.0	Versión de macOS más reciente mantenida por Apple	Apple Silicon + Intel
Almacenamiento	Espacio libre para los archivos de salida (PNG/TIFF ocupan más que JPEG)	—	—
Memoria RAM	Sin mínimo técnico	4 GB+ (iPhone/iPad) u 8 GB+ (Mac) para imágenes grandes	—
Red	No necesaria	Solo para la compra integrada	Sin conexión

▲ Ya no se admiten: iOS 16 / iPadOS 16 y macOS 13 (Ventura). A partir de la versión 1.1, Stego-Lab requiere como mínimo iOS 17 / iPadOS 17 o macOS 14. El motivo es el cambio del entorno de desarrollo a Xcode 27: desde entonces la app utiliza interfaces del sistema que solo existen a partir de esas versiones. Además, Apple ya no publica actualizaciones de seguridad para macOS 13. Los dispositivos que no pueden pasar de iOS 16 o macOS 13 pueden seguir usando la versión 1.0, pero ya no reciben actualizaciones de la app. Para proteger datos confidenciales se recomienda usar siempre la versión del sistema más reciente que admita el dispositivo, con todas las actualizaciones de seguridad disponibles.

2.2 Instalación

Paso	iOS / iPadOS	macOS
1	Abrir la App Store	Abrir la Mac App Store
2	Buscar «Stego-Lab»	Buscar «Stego-Lab»
3	Tocar «Obtener»	Hacer clic en «Obtener»
4	Confirmar con Face ID / Touch ID	Confirmar con la cuenta de Apple

Paso	iOS / iPadOS	macOS
5	Abrir la app desde la pantalla de inicio	Abrir la app desde la carpeta Aplicaciones (hasta macOS 15 también desde el Launchpad, a partir de macOS 26 desde «Apps»)

✓ Stego-Lab no necesita registro ni cuenta. Todas las funciones trabajan sin conexión; solo la compra y la restauración de Stego-Lab Pro requieren conexión con la App Store.

2.3 Primer inicio

Stego-Lab no solicita ningún permiso en el primer inicio. En iPhone y iPad, las imágenes se eligen con el selector de fotos del sistema, que no necesita acceso a toda la fototeca; solo al guardar por primera vez en Fotos pide iOS permiso para añadir fotos. También pueden cargarse imágenes desde la app Archivos. En el Mac, las imágenes se abren desde el Finder (diálogo Abrir o arrastrar y soltar). El acceso a la cámara se solicita solo en la primera toma directa (Pro). La interfaz de la app está en alemán; los nombres de pestañas y botones citados en este manual son los rótulos originales.

Interfaz

CAPÍTULO 3

3.1 Navegación principal

Área	Símbolo (iPhone/iPad · Mac)	Función
«Encode» (Mac: «Verstecken»)	arrow.up.square · eye.slash.fill	Incrustar contenidos en imágenes
«Decode» (Mac: «Entdecken»)	arrow.down.square · eye.fill	Extraer los contenidos incrustados
«EXIF»	info.square · tag	Ver y editar los metadatos
«Batch»	square.stack.3d.up.fill · wand.and.stars	Procesar varias imágenes (Pro)
«Info»	info.circle · info.circle	Ayuda, ventana Pro y detalles de la app. En el Mac, el orden de las pestañas es Verstecken, Entdecken, Batch, EXIF, Info

■ La interfaz de Stego-Lab 1.1 está en alemán; en iPhone y iPad las pestañas llevan nombres en inglés (Encode, Decode, EXIF, Batch, Info) y en el Mac nombres en alemán (Verstecken, Entdecken, Batch, EXIF, Info). Este manual cita la etiqueta original y da la traducción entre paréntesis.

3.2 Área Codificar

Elemento	Descripción
Imagen portadora	Cualquier imagen (PNG, TIFF, JPEG, HEIC, BMP, RAW); el resultado se guarda siempre sin pérdidas como PNG o TIFF
Tipo de contenido	Texto, imagen o archivo: imagen y archivo solo con Pro
Toma directa	Hacer la foto con la cámara e incrustarla en un solo paso; nunca se guarda en la fototeca (Pro)
Control de calidad	Control en vivo que equilibra la resolución de la toma con la capacidad de la portadora
Contraseña	Opcional: activa AES-256-GCM (Pro)
Formato de salida	PNG o TIFF (iPhone/iPad: PNG por defecto; Mac: una portadora TIFF sigue en TIFF, si no PNG)
Indicador de capacidad	Barra con porcentaje en tiempo real, más el tamaño del contenido en relación con la capacidad

Elemento	Descripción
Botón Codificar	El botón «Kodieren» (Mac: «Kodieren und Speichern») inicia la incrustación invisible (Pro); sin Pro solo puede guardarse la portadora con la etiqueta de IA

Tomar una foto directamente

En el área «Encode», la imagen que se va a incrustar también puede tomarse directamente con la cámara: hacer la foto y ocultarla en la imagen portadora en un solo paso, sin pasar por la fototeca. La toma nunca se guarda en la fototeca. En el Mac permanece exclusivamente en la memoria. En iPhone y iPad, la app deposita una copia temporal en su contenedor protegido para el procesamiento posterior; esa copia se elimina al restablecer o sustituir el contenido y, como muy tarde, en el siguiente inicio de la app. Un control de calidad en vivo equilibra la resolución con la capacidad libre de la imagen portadora; la orientación EXIF se graba directamente en los píxeles para que la imagen quede bien orientada al incrustarla. En el Mac, la app admite Continuity Camera: el iPhone actúa como cámara externa. La toma directa forma parte de Stego-Lab Pro.

✓ La toma directa con la cámara nunca se escribe en la fototeca. En el Mac permanece exclusivamente en la memoria; en iPhone y iPad, solo como archivo temporal en el contenedor de la app hasta que se ha procesado, en coherencia con el principio de Stego-Lab de trabajar en el dispositivo y sin nube.

Recibir una foto desde el menú Compartir

Una imagen portadora también puede recibirse desde fuera de la app, directamente desde el menú Compartir del sistema. En iPhone y iPad, selecciona una imagen en Fotos o en Archivos, toca Compartir y después «Copiar en Stego-Lab»; la foto se carga de inmediato como imagen portadora en la pestaña «Encode», que se abre automáticamente. En el Mac, Stego-Lab aparece en el Finder bajo «Abrir con» (clic derecho sobre una imagen); también puedes arrastrar la imagen al icono de la app en el Dock, y entonces llega a la pestaña «Verstecken». Así una foto entra en el flujo de incrustación sin pasar por el selector de imágenes.

✓ Stego-Lab se registra en el sistema únicamente como receptor de imágenes: sin inicio de sesión y sin servicios adicionales. En iPhone y iPad, la copia recibida se elimina justo después de cargarla; la foto permanece solo en la memoria hasta que tú mismo guardas el resultado.

3.3 Área Decodificar

Elemento	Descripción
Cargar imagen	iPhone/iPad: desde Fotos o Archivos (PNG, JPG, TIFF, HEIC, RAW); Mac: «Bild öffnen...» (PNG, JPEG, TIFF, BMP) o arrastrar y soltar
Contraseña	Se introduce si el contenido está cifrado (Pro)
Decodificar	Extrae el contenido incrustado: formato Stego-Lab, PNG de Stegosuite (LSB), JPG antiguos de Stegosuite 0.8 (F5). Texto sin contraseña gratis; contenidos de imagen y archivo con Pro
Vista previa	El contenido decodificado se muestra directamente; un mensaje adicional (p. ej. en portadoras multibloque) aparece en el aviso superior

Elemento	Descripción
Exportar	Copiar o compartir texto (gratis); exportación de imágenes y archivos con Pro
Nota heredados	Con contenidos PV1 y Stegosuite aparece un aviso de seguridad: criptografía más débil, solo lectura (PV1 = formato de desarrollo anterior a la primera publicación, nunca distribuido)

3.4 – 3.6 EXIF · Lotes · Información

Área EXIF: mostrar todos los metadatos de forma estructurada y editar directamente los campos modificables.
Área Lotes: procesar varias imágenes a la vez con barra de progreso. Área Información: referencia rápida y detalles de la versión de la app.

Esteganografía

CAPÍTULO 4

4.1 Fundamentos

La esteganografía es la técnica de ocultar información dentro de un soporte discreto. A diferencia de la criptografía, la esteganografía encubre la propia existencia del mensaje.

Stego-Lab implementa la esteganografía de imagen mediante el método del bit menos significativo (LSB): los bits menos significativos de los canales de color R, G, B se sustituyen por bits de datos útiles. El efecto visual resulta imperceptible para el ojo humano.

4.2 Método LSB

Cada canal de color es un valor de 8 bits (0–255). Una modificación del LSB equivale a una diferencia de color de ± 1 , muy por debajo del umbral de percepción humana.

Canal	Bit original (LSB)	Bit de datos	Bit resultante	Diferencia de color
Rojo	1101 0110	1	1101 0111	+1
Verde	1010 0011	0	1010 0010	-1
Azul	0011 1001	1	0011 1001	0

Parámetro	Valor	Observación
Bits por canal	1 (fijo, no configurable)	3 canales: R, G, B
Capacidad de carga	3 bits por píxel	= 3/8 de byte por píxel, menos los datos de trama (véase 4.5)
PSNR (calidad)	≥ 51 dB	$\approx 51,1$ dB a plena carga; imperceptible a la vista, detectable estadísticamente
Canales usados	R, G, B	El canal alfa no se usa; la transparencia de la imagen portadora no se conserva
Formato de salida obligatorio	PNG o TIFF	¡El JPEG destruye los datos LSB!

▲ **IMPORTANTE:** la compresión JPEG destruye de forma irreversible los datos LSB incrustados. En las operaciones de esteganografía, Stego-Lab genera exclusivamente PNG o TIFF.

4.3 Incrustar contenidos

Incrustar texto

El texto se incrusta como secuencia de bytes UTF-8. Se admiten por completo todos los caracteres Unicode, los saltos de línea y los caracteres especiales.

Resolución	Capacidad (bytes)	Capacidad (caracteres)
1080 × 1920 (Full HD)	aprox. 777.600 B	aprox. 777.600 ASCII
2160 × 3840 (4 K)	aprox. 3.110.400 B	aprox. 3 millones ASCII
4000 × 6000 (24 MP)	aprox. 9.000.000 B	aprox. 9 millones ASCII

Imágenes y archivos

Las imágenes y los archivos de cualquier tipo (PDF, DOCX, ZIP...) se incrustan tal como la app los recibe: byte a byte, sin recodificación ni compresión adicional; un JPEG sigue siendo un JPEG. La única excepción es una foto tomada con la función de cámara: solo existe en memoria, por lo que se codifica sin pérdidas como PNG y, si hace falta, se reduce a la capacidad de la imagen portadora. El nombre de archivo original se antepone a la carga útil (2 bytes de longitud + nombre en UTF-8) y se cifra junto con el contenido si hay contraseña. La cabecera de 10 bytes solo contiene identificador, versión, longitud de la carga útil e indicadores; no se guarda ningún tipo MIME.

4.4 Protección con contraseña

Cifrado AES-256-GCM opcional (AEAD), incluido en Stego-Lab Pro. Sin contraseña, la carga útil se escribe en claro en la capa LSB. La clave se deriva de la contraseña mediante PBKDF2-HMAC-SHA256 (600.000 iteraciones, sal aleatoria de 16 bytes en cada cifrado). Sin la contraseña correcta, los bits incrustados pueden leerse, pero no descifrarse; con una contraseña suficientemente fuerte, adivinarla es computacionalmente inviable. Las contraseñas débiles pueden encontrarse mediante ataques de diccionario: Stego-Lab ofrece esa comprobación en el área Decodificar.

Parámetro	Valor
Algoritmo	AES-256-GCM (AEAD)
Derivación de clave	PBKDF2-HMAC-SHA256
Iteraciones	600.000 (recomendación OWASP 2023)
Sal	16 bytes, criptográficamente aleatoria, nueva en cada cifrado
Nonce	12 bytes, criptográficamente aleatorio (estándar GCM)
Integridad	Etiqueta de autenticación GCM de 16 bytes (integrada, sin HMAC aparte)

▲ No hay puerta trasera, ni clave maestra, ni función de recuperación: quien pierde la contraseña no puede recuperar el contenido, ni siquiera el desarrollador. Una contraseña fuerte protege el contenido de forma permanente; una débil puede encontrarse con un ataque de diccionario. Elige contraseñas suficientemente largas y guárdalas en lugar seguro.

4.5 Decodificación y capacidad

Decodificar: leer los primeros 80 bits LSB (cabecera de 10 bytes), comprobar el identificador (PV2; el formato de desarrollo PV1 se acepta solo en lectura), evaluar longitud e indicadores y, después, leer sal y nonce si los hay y la carga útil. Con contenidos cifrados, la clave se deriva mediante PBKDF2-HMAC-SHA256 (600.000 iteraciones) a partir de la contraseña y la sal guardada, y la carga útil se descifra con AES-256-GCM comprobando la etiqueta de autenticación de 16 bytes. Si la etiqueta no es válida (contraseña incorrecta o datos modificados), no se devuelve nada. Si no hay ningún identificador conocido, Stego-Lab prueba, solo en lectura, los formatos antiguos Stegosuite (PNG) y, con portadoras JPEG, F5.

Fórmula	Valor
Capacidad (bytes) = $\lceil \frac{An \times Al \times 3}{8} \rceil$ – datos de trama	An, Al = anchura y altura en píxeles; 3 canales $\times$ 1 bit; datos de trama véase abajo (10 bytes como mínimo)
Ejemplo: $3024 \times 4032 \times 3 \div 8$	= 4.572.288 bytes $\approx$ 4,57 MB (4,36 MiB); utilizables sin contraseña 4.572.278 bytes, con contraseña 4.572.234 bytes
Datos de trama (internos de Stego-Lab)	Cabecera de 10 bytes (identificador 4 + versión 1 + longitud 4 + indicadores 1); con contraseña, 44 bytes más (sal 16 + nonce 12 + etiqueta GCM 16), 54 bytes en total; con imágenes y archivos, 2 bytes + nombre de archivo en UTF-8 más (dentro del cifrado si hay contraseña); con etiquetado de IA (Pro, lote), 7 bytes de marco + datos de etiquetado más (2.048 bytes como máximo), sin cifrar

Marcas de agua

CAPÍTULO 5

5.1 Marcas de agua visibles

Parámetro	Marca de agua de texto	Marca de agua de imagen
Tipo de contenido	Cualquier texto UTF-8	PNG, JPEG, HEIC, TIFF
Opacidad	15 – 100 % (predeterminado 65 %)	15 – 100 % (predeterminado 65 %)
Posición	9 posiciones fijas en una cuadrícula 3×3; predeterminada: abajo a la derecha	9 posiciones fijas en una cuadrícula 3×3; predeterminada: abajo a la derecha
Tamaño	2 – 10 % del lado menor de la imagen (mínimo 24 px)	8 – 45 % del ancho de la imagen (mínimo 48 px)
Representación	Blanco, fuente del sistema en negrita, sombra negra: color, tipografía y rotación no seleccionables	Colores originales del logotipo, sin rotación
Disponibilidad	Área «Batch»: una imagen gratis, varias imágenes con Pro	Área «Batch»: una imagen gratis, varias imágenes con Pro

5.2 Marcas de agua invisibles y combinadas

Invisible: se oculta un identificador en la imagen mediante LSB. Visualmente idéntico al original y extraíble en cualquier momento con Stego-Lab. Combinado: aplicar a la vez una marca de agua visible y otra invisible sobre la misma imagen.

5.3 Posicionamiento y lotes

Posición	Nombre en la app	Descripción
Arriba a la izquierda	«Oben L»	Esquina superior izquierda
Arriba al centro	«Oben M»	Centro superior de la imagen
Arriba a la derecha	«Oben R»	Esquina superior derecha
En medio a la izquierda	«Links M»	Centrado en vertical, a la izquierda
Centrado	«Mitte»	Totalmente centrado
En medio a la derecha	«Rechts M»	Centrado en vertical, a la derecha
Abajo a la izquierda	«Unten L»	Esquina inferior izquierda

Posición	Nombre en la app	Descripción
Abajo al centro	«Unten M»	Centro inferior de la imagen
Abajo a la derecha	«Unten R»	Esquina inferior derecha: predeterminada

Marcas de agua por lotes: los mismos ajustes en una pasada en tantas imágenes como quieras (Pro; una sola imagen con marca de agua visible es gratis), visibles, invisibles o combinadas.

Edición de EXIF y metadatos

CAPÍTULO 6

6.1 Fundamentos de EXIF

EXIF (Exchangeable Image File Format) es la norma más extendida para almacenar metadatos en archivos de imagen. Contiene datos técnicos de la cámara, coordenadas GPS, marcas de tiempo e información de derechos. Stego-Lab lee y escribe estos campos mediante ImageIO de Apple, sin fijar una versión concreta de EXIF.

6.2 Campos legibles

Etiqueta EXIF	Campo (nombre en la app)	Valor de ejemplo
0x010F	«Kamera-Hersteller» (fabricante de la cámara)	Apple
0x0110	«Kamera-Modell» (modelo de la cámara)	iPhone 15 Pro
0xA434	«Objektiv» (objetivo)	iPhone 15 Pro back camera
0x9003	«Aufnahmedatum» (fecha de la toma, DateTimeOriginal)	2024:03:15 14:32:00
0x9004	«Digitalisiert» (fecha de digitalización, DateTimeDigitized)	2024:03:15 14:32:00
0x829A	«Belichtungszeit» (tiempo de exposición)	0.001 (= 1/1000 s)
0x829D	«Blende» (apertura)	1.8
0x8827	«ISO» (sensibilidad ISO)	64
0x920A	«Brennweite» (distancia focal)	6.765
0x013B	«Künstler» (autor, Artist)	Juan Pérez
0x8298	«Copyright»	© 2024 J. Pérez
0x010E	«Beschreibung» (descripción de la imagen)	Panorama de los Alpes
0x9286	«Kommentar» (comentario, UserComment)	Texto libre
0x0131	«Software»	Stego-Lab 1.1

6.3 Campos editables

Campo	Editable	Observación
«Beschreibung» (descripción)	Sí (gratis)	Texto libre
«Künstler» (autor, Artist)	Sí (gratis)	Nombre del fotógrafo
«Copyright»	Sí (gratis)	Mención de copyright
«Software»	Sí (gratis)	Software de edición
«Kamera-Hersteller», «Kamera-Modell» (fabricante, modelo)	Sí (Pro)	Texto libre (Mac: «Kamera (Marke)», «Kamera (Modell)»)
«Objektiv» (objetivo)	Sí (Pro)	Texto libre
«Aufnahmedatum» (fecha de la toma)	Sí (Pro)	Formato EXIF AAAA:MM:DD HH:MM:SS (Mac: «Datum (Original)»)
«Digitalisiert» (fecha de digitalización)	Sí (Pro)	Formato EXIF AAAA:MM:DD HH:MM:SS (Mac: «Datum (Digitalisiert)»)
«Belichtungszeit» (tiempo de exposición)	Sí (Pro)	Segundos, en decimal (p. ej. 0.001); una entrada no válida se descarta sin aviso
«Blende» (apertura)	Sí (Pro)	Número f (p. ej. 2.8); una entrada no válida se descarta sin aviso
«ISO»	Sí (Pro)	Número entero (p. ej. 800)
«Brennweite» (distancia focal)	Sí (Pro)	Milímetros, en decimal (p. ej. 50); una entrada no válida se descarta sin aviso
«Kommentar» (comentario)	Sí (Pro)	Texto libre (EXIF UserComment)
GPS: «Breitengrad», «Längengrad», «Höhe» (latitud, longitud, altitud)	Sí (Pro)	Número decimal; negativo = sur, oeste o bajo el nivel del mar. Borrar y/o volver a fijar: un campo vacío elimina solo ese valor
Todos los campos	—	Un campo vacío elimina el valor. Surte efecto con «Änderungen anwenden» (aplicar cambios; Mac: «Metadaten anwenden»)

6.4 Datos GPS

Etiqueta GPS	Descripción	Formato
GPSLatitude	Latitud	Archivo: grados, min., seg. + N/S — app: grados decimales, negativo = sur (Pro)
GPSLongitude	Longitud	Archivo: grados, min., seg. + E/W — app: grados decimales, negativo = oeste (Pro)

Etiqueta GPS	Descripción	Formato
GPSPAltitude	Altitud sobre el nivel del mar	Archivo: metros + referencia — app: metros, negativo = bajo el nivel del mar (Pro)
GPSTimeStamp	Hora GPS	UTC HH:MM:SS — no se muestra en la app
GPSTimestamp	Fecha GPS	AAAA:MM:DD — no se muestra en la app
GPSPimgDirection	Dirección de la cámara	0 – 360° — no se muestra en la app
Eliminación	Parcial o completa	Vaciar los campos de coordenadas elimina solo latitud, longitud y altitud; las demás etiquetas GPS permanecen en el archivo. Solo «Alle Metadaten löschen» (borrar todos los metadatos, gratis) las elimina por completo, junto con todos los demás metadatos

▲ Los datos GPS contienen el lugar exacto de la toma. ¡Compruébalos siempre antes de compartir imágenes y elimínalos si hace falta!

6.5 Borrar todos los metadatos

Esta función elimina de la imagen los metadatos EXIF, GPS, IPTC y XMP, así como los datos de cámara y objetivo y las miniaturas incrustadas: ideal antes de compartir o publicar.

En el área EXIF está disponible para ello el botón «Alle Metadaten löschen» (borrar todos los metadatos; gratis, con diálogo de confirmación). El borrado solo surte efecto con «Änderungen anwenden» (aplicar cambios; Mac: «Metadaten anwenden»); hasta entonces, compartir y guardar están bloqueados. En el área «Batch», la opción «Alle Metadaten löschen» (Pro) limpia toda una serie de imágenes en una sola pasada; si allí está activo a la vez el etiquetado de IA, se vuelve a escribir tras el borrado. Si la imagen lleva un etiquetado de IA (véase el capítulo 9), solo se elimina su parte en los metadatos. Una etiqueta visible y un marcado invisible en los datos de la imagen se conservan, porque forman parte de los píxeles; el diálogo de confirmación lo advierte.

■ Lo que se conserva: el contenido de la imagen, el perfil de color (ICC) y la orientación. Los archivos JPEG y HEIC se vuelven a codificar en el proceso: un paso adicional de compresión con pérdidas. PNG y TIFF siguen siendo sin pérdidas.

Lotes y formatos

CAPÍTULO 7

7 Procesamiento por lotes

Parámetro	Valor
N.º máx. de imágenes	Ilimitado (según la memoria RAM; máx. 250 MB o 300 megapíxeles por archivo)
Procesamiento	Secuencial, con barra de progreso («Bearbeite x / y»)
Gestión de errores	Los archivos que no se pueden cargar se notifican al importar y se descartan; un error durante el procesamiento interrumpe el lote. Sin registro.
Cancelación	No se puede cancelar durante la ejecución
Salida	Carpeta temporal; nombre de archivo = original + «_watermark» en todos los modos (con contador si hay nombres repetidos). Después, en iPhone/iPad: «Exportordner teilen...» o «Alle in Fotos speichern»; en Mac: «Im Finder zeigen» o «In Ordner kopieren...»
Formato de exportación	PNG, TIFF o JPG; JPG solo en el modo «Sichtbar» (visible) y no con la capa de IA robusta activa
Modos	«Sichtbar» (visible) · «Unsichtbar» (invisible) · «Beides» (ambos); además, etiquetado de IA y «Alle Metadaten löschen» (borrar todos los metadatos)
Disponibilidad	Una imagen con marca de agua visible gratis; varias imágenes, «Unsichtbar» (invisible), «Beides» (ambas), «Alle Metadaten löschen» (borrar todos los metadatos) y capa de IA robusta con Stego-Lab Pro

8 Formatos admitidos

Formatos de entrada

Formato	Nombre completo	Sin pérdidas	Cargable como imagen portadora
PNG	Portable Network Graphics	Sí	Sí: formato principal; el resultado se guarda como PNG o TIFF
TIFF	Tagged Image File Format	Sí	Sí: el resultado se guarda como PNG o TIFF

Formato	Nombre completo	Sin pérdidas	Cargable como imagen portadora
JPEG / JPG	Joint Photographic Experts Group	NO	Sí: el resultado se guarda siempre como PNG o TIFF; además, lectura de JPG antiguos de Stegosuite 0.8 (F5, desde la versión 1.1)
HEIC	Contenedor HEIF (ISO/IEC 23008-12) con codificación HEVC	NO	Sí: el resultado se guarda como PNG o TIFF (Mac: arrastrar y soltar o «Abrir con»)
DNG	Adobe Digital Negative (RAW)	normalmente	Sí, si el sistema reconoce el modelo RAW: el resultado se guarda como PNG o TIFF (Mac: arrastrar y soltar o «Abrir con»)
CR2 / CR3	Canon RAW	normalmente	Sí, si el sistema reconoce el modelo RAW: el resultado se guarda como PNG o TIFF (Mac: arrastrar y soltar o «Abrir con»)
NEF	Nikon RAW	normalmente	Sí, si el sistema reconoce el modelo RAW: el resultado se guarda como PNG o TIFF (Mac: arrastrar y soltar o «Abrir con»)
ARW	Sony RAW	normalmente	Sí, si el sistema reconoce el modelo RAW: el resultado se guarda como PNG o TIFF (Mac: arrastrar y soltar o «Abrir con»)
BMP	Bitmap	Sí	Sí: el resultado se guarda como PNG o TIFF

Formatos de salida

Formato	Esteganografía	Marca de agua	EXIF	Calidad
PNG	Sí (predeterminado)	Sí	Sí (si el origen es PNG)	Sin pérdidas
TIFF	Sí	Sí	Sí (si el origen es TIFF; formato de reserva si el tipo de origen es desconocido)	Sin pérdidas
JPEG	NO: solo lectura de JPG antiguos de Stegosuite 0.8 (F5)	Sí (solo en el modo por lotes «Sichtbar» (visible), sin la capa de IA robusta)	Sí (si el origen es JPEG)	Ajuste del sistema, no configurable
HEIC	NO	NO	Sí (si el origen es HEIC)	Ajuste del sistema, no configurable

Recomendaciones de formato

Caso de uso	Formato de entrada	Formato de salida
Esteganografía (texto)	Cualquier imagen (PNG, TIFF, JPEG, HEIC, BMP, RAW)	PNG o TIFF
Esteganografía (archivo)	Cualquier imagen (PNG, TIFF, JPEG, HEIC, BMP, RAW)	PNG o TIFF
Marca de agua visible (lotes; una imagen gratis)	Indiferente	JPG (redes sociales) / PNG o TIFF (archivo)
Marca de agua invisible (lotes, Pro)	Indiferente	PNG o TIFF
Edición EXIF	Indiferente	Mismo formato que el origen (TIFF si el tipo de origen es desconocido)
Quitar el GPS	JPEG, HEIC, PNG, TIFF	Mismo formato que el origen
Archivo a largo plazo	TIFF	TIFF (sin comprimir)

Etiquetar imágenes de IA

CAPÍTULO 9

9.1 Marco legal

Desde el 2 de agosto de 2026, el artículo 50 del Reglamento (UE) 2024/1689 de IA impone dos obligaciones distintas. Los proveedores de sistemas de IA que generan imágenes deben marcar su salida de forma legible por máquina (apdo. 2); los sistemas comercializados antes del 2 de agosto de 2026 disponen de un plazo transitorio hasta el 2 de diciembre de 2026. Los responsables del despliegue que utilicen un sistema de IA para generar o manipular imágenes que constituyan una ultrasuplantación (deep fake) en el sentido del artículo 3, punto 60, deben revelar que el contenido ha sido generado o manipulado artificialmente (apdo. 4). Se trata de imágenes que se asemejan a personas, objetos, lugares o acontecimientos reales y que podrían parecer falsamente auténticas. En obras manifiestamente artísticas, creativas o satíricas basta una indicación que no obstaculice su presentación; el uso puramente personal y no profesional no está comprendido. No existe una obligación general de etiquetar toda imagen editada con IA.

Stego-Lab no genera contenidos de IA y, por tanto, no es un proveedor en el sentido del apdo. 2. La app es una herramienta para los responsables del despliegue que quieran o deban aplicar una divulgación conforme al apdo. 4: reúne la etiqueta visible y los metadatos legibles por máquina; en el área «Batch» (Pro) se añade la «Robuste unsichtbare Schicht» (capa invisible robusta), robusta frente a la eliminación de los metadatos, pero no frente a una recompresión con pérdidas (véase 9.6).

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

9.2 Etiquetar en Codificar y en lotes

Basta un interruptor: en la sección «Etiquetado de IA» de Codificar y del modo por lotes, «Etiquetar como imagen de IA» activa el ajuste preestablecido. Hay dos variantes disponibles, «totalmente generada por IA» y «editada con IA»; un campo libre opcional «Generador» admite, por ejemplo, «Midjourney v7» y solo llega a los metadatos, nunca a la etiqueta visible.

La etiqueta visible se adapta automáticamente: un contraste mínimo calculado por medición de luminancia (texto claro sobre fondo oscuro o al revés) y un tamaño mínimo del 3 % del lado más corto de la imagen garantizan la legibilidad. La posición se elige libremente en una cuadrícula de 3×3 (por defecto: abajo a la izquierda). Un semáforo de tres niveles junto al interruptor muestra de un vistazo si el ajuste cumple el artículo 50.

Codificar ya etiqueta por completo en la versión gratuita: etiqueta visible y metadatos, incluso sin contenido oculto propio. El modo por lotes añade, con Stego-Lab Pro, la capa invisible robusta y etiqueta tantas imágenes como quieras en una sola pasada.

9.3 Campos escritos

Campo	Valor / contenido	Formato
IPTC Digital Source Type: totalmente generada por IA	http://cv.iptc.org/newscodes/digitalsourcetype/trainedAlgorithmicMedia	IPTC / XMP

Campo	Valor / contenido	Formato
IPTC Digital Source Type: editada con IA	http://cv.iptc.org/newscodes/digitalsourcetype/compositeWithTrainedAlgorithmicMedia	IPTC / XMP
XMP Iptc4xmpExt:DigitalSourceType	El mismo valor que en IPTC, además como propiedad XMP (PNG mediante iTXt)	XMP
EXIF UserComment + TIFF ImageDescription	AI-generated content · KI-generierter Inhalt (EU AI Act Art. 50)	Texto plano
Capa invisible «AI-DISCLOSURE v1»	JSON con la variante, el generador, el emisor y la marca de tiempo; prefijo «AIDISC1:»	Trailer PV2, bit 3 de FLAGS (Pro)

9.4 Detección al leer

Decodificar y EXIF muestran un distintivo neutro «Etiquetado de IA detectado» en cuanto se encuentra una de las tres fuentes, sin valoración y sin afirmar nada sobre el origen. Si hay varias fuentes, el orden de prioridad es: capa invisible, metadatos y, por último, la indicación en texto plano; si las fuentes se contradicen, aparece una nota neutra en lugar de una advertencia.

9.5 Gratis frente a Pro

Componente	Modalidad
Etiqueta de IA visible	Gratis
Etiquetado en los metadatos (IPTC/XMP/EXIF)	Gratis
Capa invisible robusta	Pro
Etiquetado por lotes de muchas imágenes	Pro

9.6 Límites

▲ Límites: el Digital Source Type de IPTC/XMP se escribe de forma fiable en PNG, TIFF y JPEG, y Stego-Lab lo vuelve a leer. La indicación en texto plano en TIFF ImageDescription se escribe correctamente en el archivo en los tres formatos, pero la función de lectura propia de Stego-Lab solo la recupera en imágenes portadoras TIFF, no en PNG ni en JPEG. El punto medio «-» del texto plano de EXIF UserComment se convierte en un signo de interrogación en los tres formatos: una pérdida de datos real e independiente del formato. La capa invisible no sobrevive a una recompresión JPEG ni a una subida a redes sociales; es una marca de archivo y de prueba para PNG/TIFF, no un sustituto de C2PA. El distintivo unificado a escala de la UE llegará tras el código de conducta definitivo de la Comisión; hasta entonces se mantiene la etiqueta de texto.

9.7 Aviso legal

■ Stego-Lab no genera contenidos de IA ni se pronuncia sobre el origen de una imagen. El etiquetado se basa en lo que indica el usuario. La app es una ayuda para cumplir obligaciones de transparencia, no asesoramiento jurídico. La exactitud y la integridad del etiquetado siguen siendo responsabilidad del usuario.

Seguridad y privacidad

CAPÍTULO 10

10.1 Procesamiento local

Categoría de datos	Procesamiento	Red
Imágenes	Solo en local	NINGUNA
Contenidos incrustados	Solo en local	NINGUNA
Contraseñas	Solo en memoria, nunca se guardan	NINGUNA
Datos EXIF	Solo en local	NINGUNA
Informes de fallos	Sin informes de fallos en la app (los informes del sistema van a Apple solo con consentimiento del usuario)	NINGUNA
Analíticas / telemetría	No existen	NINGUNA
Publicidad	No existe	NINGUNA

10.2 Detalles del cifrado

Paso	Método	Parámetros
1. Sal	SecRandomCopyBytes (Apple Security)	16 bytes, criptográficamente aleatoria, nueva en cada cifrado
2. Nonce	Apple CryptoKit (AES.GCM.seal)	12 bytes, aleatorio, nuevo en cada cifrado (estándar GCM)
3. Clave	PBKDF2-HMAC-SHA256	600.000 iteraciones, clave de 32 bytes
4. Cifrado	AES-256-GCM (AEAD)	Etiqueta de autenticación de 16 bytes añadida al cifrado
5. Trama	Cabecera sal nonce cifrado+etiqueta bloque de IA si lo hay	Binario, en la capa LSB; la cabecera y el bloque de IA quedan sin cifrar
6. Verif.	Etiqueta de autenticación GCM	Se comprueba al decodificar; sin HMAC aparte

10.3 Seguridad esteganográfica

Ataque	Sin contraseña	Con AES-256
Comprobación de identificador (formato conocido)	Detección inmediata: el identificador «PV2» está en claro en la capa LSB	Detección inmediata; contenido y nombre de archivo protegidos

Ataque	Sin contraseña	Con AES-256
Inspección visual	Seguro	Seguro
Análisis RS	Detectable	Canal visible, contenido protegido
Prueba de ji cuadrado	Detectable	Canal visible, contenido protegido
Fuerza bruta (contenido)	Contenido legible directamente	Computacionalmente inviable (contraseña fuerte)
Ataque por diccionario	No procede	Posible con una contraseña débil
Conversión a JPEG	Contenido destruido	Contenido destruido

✓ Recomendación: combina siempre la esteganografía LSB con AES-256. Así el contenido sigue siendo ilegible aunque se detecte el canal por medios estadísticos.

Especificaciones técnicas

CAPÍTULO 11

11.1 Rendimiento

Operación	Tamaño de imagen	iPhone 15 Pro	iPad Pro M4	MacBook Pro M3
Codificar texto 1 KB	12 MP (4032×3024)	< 0,5 s	< 0,5 s	< 0,2 s
Codificar archivo 1 MB	12 MP	~1,5 s	~1,2 s	~0,5 s
Codificar archivo 10 MB	48 MP	~8 s	~6 s	~2,5 s
Decodificar 1 KB	12 MP	< 0,5 s	< 0,5 s	< 0,2 s
Decodificar 1 MB	12 MP	~1,5 s	~1,2 s	~0,5 s
Marca de agua visible	12 MP	~0,8 s	~0,6 s	~0,3 s
Leer EXIF	Indiferente	< 0,1 s	< 0,1 s	< 0,1 s
Lote de marca de agua visible, 100 imágenes	8 MP de media	~80 s	~60 s	~25 s

11.2 Necesidades de memoria

Tamaño de imagen	RAM (RGBA)	RAM (RGB)	RAM recomendada
8 MP (3264×2448)	~32 MB	~24 MB	3 GB
12 MP (4032×3024)	~49 MB	~37 MB	4 GB
24 MP (6000×4000)	~96 MB	~72 MB	6 GB
48 MP (8064×6048)	~196 MB	~147 MB	8 GB
108 MP (12000×9000)	~432 MB	~324 MB	16 GB

11.3 Algoritmos y normas

Algoritmo	Uso	Especificación
Esteganografía LSB	Método principal de incrustación (1 bit por canal, R/G/B, secuencial)	Formato de trama propio PV2, código fuente publicado bajo licencia MIT

Algoritmo	Uso	Especificación
AES-256-GCM	Cifrado de la carga útil (AEAD); el nonce de 12 bytes lo genera CryptoKit al sellar	FIPS 197, NIST SP 800-38D
PBKDF2-HMAC-SHA256	Derivación de clave, 600.000 iteraciones	RFC 8018 (antes RFC 2898), NIST SP 800-132
Etiqueta de autenticación GCM	Comprobación de integridad (16 bytes, sin HMAC aparte)	NIST SP 800-38D
SecRandomCopyBytes	Generación de la sal de 16 bytes	Framework Apple Security
HKDF-SHA256	Derivación de clave del formato antiguo PV1 (formato de desarrollo anterior a 1.0, nunca publicado): solo lectura	RFC 5869
AES-128-CTR	Compatibilidad con Stegosuite: solo lectura	NIST SP 800-38A
PBKDF2-HMAC-SHA1	Derivación de clave de Stegosuite: solo lectura	RFC 8018
MD5	Semilla del generador de posiciones de Stegosuite: sin función de seguridad, solo lectura	RFC 1321
SHA-1	Generador pseudoaleatorio para la selección de coeficientes F5: sin función de seguridad, solo lectura	FIPS 180-4
EXIF 2.32	Norma de metadatos	CIPA DC-X008-Translation-2019
PNG	Formato de salida sin pérdidas	ISO/IEC 15948:2004
TIFF 6.0	Formato de salida sin pérdidas	Especificación Adobe TIFF
UTF-8	Codificación de texto	RFC 3629, Unicode 15.0

Ejemplos de uso

CAPÍTULO 12

12.1 Protección de documentos privados (Pro)

Paso	Acción
1	Abrir el área Encode
2	Cargar una foto de vacaciones como imagen portadora (se recomienda PNG/TIFF)
3	Tipo de contenido: Archivo → seleccionar Escaneo-pasaporte.pdf
4	Introducir una contraseña fuerte (recomendado: al menos 12 caracteres, mejor una frase de contraseña)
5	Iniciar la codificación → guardar como PNG
6	Borrar el PDF original tras la copia de seguridad
Decod.	Cargar el PNG → Decode → contraseña → extraer el archivo

12.2 Prueba de autoría (Pro)

Paso	Acción
1	Batch → aplicar la marca visible: «@Nombre © 2025» → salida PNG
2	EXIF → fijar Copyright y «Künstler» (autor) (gratis), «Änderungen anwenden» (aplicar cambios)
3	Encode: incrustar después la marca de agua de texto invisible en la imagen así marcada
4	Generar un PNG, contraseña opcional
5	Publicar
Prueba	Decode → la marca invisible acredita la autoría (solo si la imagen se transmite sin pérdidas, como PNG/TIFF)
Atención	Respetar el orden: una marca de agua visible aplicada después sobre datos ya ocultos los destruye. Alternativa en una sola pasada: modo por lotes «Beides» (ambos).

12.3 Flujo del fotógrafo, 500 imágenes (Pro)

Paso	Acción
1	Batch → seleccionar 500 imágenes
2	Marca visible: «© 2025 Nombre» — posición «Unten M» (abajo al centro), opacidad 25–40 %
3	Activar la opción «Alle Metadaten löschen» (borrar todos los metadatos): elimina EXIF, GPS, IPTC y XMP de todas las imágenes de salida
4	La mención de autor va en la marca de agua visible; no existe una edición masiva de EXIF campo por campo (autor/copyright); si hace falta, imagen por imagen en el área EXIF
5	Formato de exportación: JPG para la entrega (calidad no configurable, valor del sistema); para un archivo PNG, iniciar una segunda pasada
6	Iniciar el lote
Resultado	500 imágenes en ~10 minutos (valor orientativo)

12.4 Contexto educativo (Pro)

Objetivo de aprendizaje	Demostración con Stego-Lab
Comprender la esteganografía LSB	Incrustar texto; comparar el original y el resultado con una herramienta externa (histograma): Stego-Lab no muestra histogramas
Experimentar el cifrado AES	Activar la protección con contraseña; decodificar sin ella → error
Comprender PBKDF2 y la sal	Incrustar dos veces la misma contraseña → resultado distinto cada vez por la sal aleatoria
Analizar la norma EXIF	Analizar por completo una foto de cámara
Privacidad del GPS	Ver el GPS → eliminarlo («Alle Metadaten löschen» es gratis, los campos GPS son Pro) → comprobar el resultado
Sin pérdidas frente a con pérdidas	Codificar en PNG, guardar como JPEG con una herramienta externa → la decodificación falla
Cálculo de capacidad	Dimensiones de la imagen → fórmula → comparar con la app

Preguntas frecuentes

CAPÍTULO 13

P1: ¿Se puede usar JPEG para la esteganografía?

R: Para incrustar, no: la compresión JPEG destruye de forma irreversible los datos LSB, por lo que Stego-Lab solo genera PNG o TIFF. En lectura, la app admite además los antiguos JPG de Stegosuite 0.8 con el procedimiento F5 (solo decodificación).

P2: ¿Qué tamaño puede tener el contenido que se incrusta?

R: Capacidad (bytes) = $(An \times Al \times 3) \div 8$ – datos de trama (10 bytes, 54 bytes con contraseña, más el nombre de archivo). Una imagen de 12 MP (3024×4032) ofrece $\approx 4,57$ MB (4,36 MiB). Stego-Lab muestra la capacidad restante en tiempo real.

P3: ¿Qué ocurre si olvido la contraseña?

R: La contraseña nunca se guarda; no hay puerta trasera, ni clave maestra, ni recuperación. Solo el ataque opcional por lista de palabras del área Decodificar (Pro) puede encontrar una contraseña débil incluida en la lista; con una contraseña fuerte, el contenido queda inaccesible de forma permanente.

P4: ¿Se pueden detectar los datos esteganográficos?

R: Visualmente: no. Estadísticamente (análisis RS, ji cuadrado) sí son detectables. Con AES-256 el contenido sigue siendo ilegible.

P5: ¿Funciona completamente sin conexión?

R: Sí. No hay ninguna conexión de red. Todas las funciones están disponibles sin conexión.

P6: ¿Se guardan las imágenes en la nube?

R: No. Stego-Lab no transmite ningún dato. Todos los pasos se ejecutan exclusivamente en local.

P7: ¿Se puede decodificar en el iPhone lo codificado en el Mac?

R: Sí. El formato interno es compatible entre plataformas.

P8: ¿Qué formato da la máxima calidad?

R: TIFF (sin comprimir) para archivo. PNG para un almacenamiento sin pérdidas con archivos más ligeros.

P9: ¿Se admiten los formatos RAW?

R: Como entrada: DNG, CR2, CR3, NEF, ARW, ORF... En esteganografía, la salida es siempre PNG o TIFF. Para marcas de agua solo visibles en el modo Lotes también es posible JPG (no con la capa invisible robusta activa); el área EXIF exporta en el formato del archivo de origen.

P10: ¿Se puede usar una contraseña distinta por imagen?

R: Sí. Cada imagen puede llevar su propia contraseña.

P11: ¿Se admite la app Atajos?

R: Está previsto para una versión futura.

P12: ¿Qué diferencia hay entre marca de agua visible e invisible?

R: Visible: dibujada directamente en la imagen. Invisible: oculta mediante LSB, extraíble solo con la app.

P13: ¿Debo etiquetar las imágenes de IA?

R: Depende. Desde el 2 de agosto de 2026, el art. 50, apdo. 4 del Reglamento de IA obliga a los responsables del despliegue a revelar, en las ultrasuplantaciones (deep fakes) publicadas, que el contenido ha sido generado o editado con IA; en obras manifiestamente artísticas o satíricas basta una indicación atenuada, y el uso puramente privado no está comprendido. Los proveedores de sistemas de IA están sujetos a la obligación de marcado legible por máquina del apdo. 2. Stego-Lab ofrece la herramienta, no asesoramiento jurídico (véase 9.7).

P14: ¿El etiquetado sobrevive a las redes sociales o a la compresión JPEG?

R: La etiqueta visible sí (forma parte de los píxeles). Los metadatos dependen de la plataforma: muchas los eliminan al subir. La capa invisible (LSB), no.

P15: ¿Cómo borro todos los metadatos de una vez?

R: Área EXIF: botón «Alle Metadaten löschen» (borrar todos los metadatos, gratis) y después «Änderungen anwenden» (aplicar cambios; Mac: «Metadaten anwenden»). Para toda una serie: área «Batch», opción «Alle Metadaten löschen» (Pro).

Anexo técnico

CAPÍTULO 14

14.1 Proceso de codificación LSB

Paso	Descripción
1. Preparar la carga útil	Texto como bytes UTF-8; imágenes y archivos como bytes originales sin modificar, sin recodificación ni compresión (solo las fotos de la cámara se guardan antes como PNG). Con imágenes y archivos se antepone el nombre de archivo: 2 bytes de longitud (big-endian) + nombre en UTF-8.
2. Cifrar (opcional, Pro)	Con contraseña: sal aleatoria de 16 bytes (SecRandomCopyBytes), clave de 256 bits mediante PBKDF2-HMAC-SHA256 (600.000 iteraciones), AES-256-GCM con nonce aleatorio de 12 bytes (CryptoKit). La etiqueta de autenticación de 16 bytes se añade al cifrado; el nombre de archivo se cifra también.
3. Formar la trama	Cabecera de 10 bytes (identificador «PV2», versión, longitud, indicadores), seguida de sal y nonce si hay cifrado, después la carga útil o el cifrado con su etiqueta y, si procede, el bloque de etiquetado de IA sin cifrar. Si la trama no cabe en la imagen, Stego-Lab se detiene antes de modificar ningún píxel.
4. Sustituir los LSB	La trama se escribe bit a bit, empezando por el bit más significativo de cada byte: en cada píxel, sucesivamente en el bit menos significativo de R, G y B, línea a línea desde el primer píxel (row-major order). Exactamente 1 bit por canal; el canal alfa no se usa.
5. Salida	Se guarda como PNG o TIFF (sin pérdidas, 8 bits por canal); la transparencia de la imagen portadora no se conserva. Los datos LSB se mantienen.

14.2 Formato de trama interno

La cabecera de trama interna de Stego-Lab se escribe en primer lugar en la capa LSB de la imagen portadora, seguida de los datos útiles. Este formato es compatible entre plataformas (iOS, iPadOS, macOS).

Zona	Tamaño	Contenido
MAGIC	4 bytes	0x50 0x56 0x32 0x00 («PV2» + byte nulo): identifica los datos de Stego-Lab en la capa LSB; «PV1» (formato de desarrollo) también se acepta solo en lectura
VERSION	1 byte	Versión del formato, actualmente 0x02 (no se evalúa al leer)
PAYLOAD_LENGTH	4 bytes	uint32, big-endian: longitud de la carga útil en bytes; con cifrado, longitud del cifrado incluida la etiqueta de 16 bytes (sin sal ni nonce); si no, longitud de la carga útil en claro incluido el prefijo de nombre

Zona	Tamaño	Contenido
FLAGS	1 byte	Bit 0 = tipo de contenido (1 = texto, 0 = imagen/archivo) · bit 1 = cifrado · bit 2 = prefijo de nombre de archivo al inicio de la carga útil · bit 3 = sigue un bloque de etiquetado de IA (desde 1.1, solo lote con capa robusta, Pro) · bits 4–7 = 0. Sin campo de tipo/MIME, sin compresión.
SALT	16 bytes	Solo si el bit 1 está activo: sal aleatoria para PBKDF2 (SecRandomCopyBytes)
NONCE	12 bytes	Solo si el bit 1 está activo: nonce AES-GCM aleatorio (CryptoKit)
CARGA ÚTIL	= PAYLOAD_LENGTH	Sin contraseña: [prefijo de nombre] + contenido en claro. Con contraseña: cifrado AES-256-GCM de [prefijo de nombre] + contenido, terminado por la etiqueta de autenticación de 16 bytes
– Prefijo de nombre	2 + n bytes	Solo si el bit 2 está activo, parte de la carga útil (incluido en PAYLOAD_LENGTH): longitud n (uint16, big-endian) + nombre de archivo en UTF-8; cifrado con el contenido si hay contraseña
BLOQUE DE IA	7 + n bytes	Solo si el bit 3 está activo, tras la carga útil, no incluido en PAYLOAD_LENGTH: «AIDT» + versión 0x01 + longitud n (uint16, big-endian) + «AIDISC1:» seguido del JSON (n ≤ 2.048); siempre sin cifrar, solo con salida PNG/TIFF

14.3 Gestión de errores

Mensaje de error	Causa	Solución
Nota	La interfaz de Stego-Lab 1.1 está en alemán; los mensajes se citan literalmente, con traducción entre paréntesis. Las cifras de los mensajes dependen de la imagen.	—
«Zu groß: 5.2 MB (max 4.4 MB)» (demasiado grande: 5,2 MB, máx. 4,4 MB); en iOS al cargar: «Die Datei ist 5,2 MB groß, das Trägerbild fasst 4,4 MB. Bitte ein größeres Trägerbild oder eine kleinere Datei wählen.» (el archivo ocupa 5,2 MB, la portadora admite 4,4 MB; elegir una portadora mayor o un archivo menor)	Contenido más datos de trama (cabecera, sal, nonce, etiqueta, nombre de archivo, bloque de IA) mayores que la capacidad de la imagen portadora	Elegir una imagen portadora más grande o un contenido más pequeño
«Falsches Passwort oder beschädigte Daten» (contraseña incorrecta o datos dañados)	Falló la comprobación de la etiqueta de autenticación GCM: contraseña incorrecta o datos modificados	Comprobar la contraseña; usar el original sin modificar

Mensaje de error	Causa	Solución
«Kein erkanntes Steganographie-Format (PV1 oder StegSuite) in diesem Bild.» (ningún formato esteganográfico reconocido en esta imagen)	Ningún identificador de Stego-Lab en la capa LSB: imagen no codificada, o guardada con pérdidas (JPEG, HEIC), redimensionada o editada tras la incrustación	Usar el original PNG/TIFF sin modificar
«Header beschädigt — möglicherweise kein kodiertes Bild.» / «Payload abgeschnitten — Bild möglicherweise bearbeitet.» (cabecera dañada / carga trunca; solo macOS)	Longitud inverosímil en la cabecera, o imagen recortada o editada tras la incrustación	Usar el original sin modificar
«Bild konnte nicht geladen werden.» / «Datei konnte nicht gelesen werden oder ist kein gültiges Bild.» (no se pudo cargar la imagen / archivo ilegible o imagen no válida)	El archivo no es una imagen legible	Usar PNG, JPEG, TIFF o 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.» (archivo demasiado grande, máx. 250 MB / demasiados píxeles, máx. 300 MP, posible archivo manipulado)	Superados los límites de protección frente a archivos manipulados	Usar un archivo más pequeño
«PNG-Export fehlgeschlagen» o «TIFF-Export fehlgeschlagen» (error al exportar PNG/TIFF; iOS); en macOS, un mensaje del sistema	No se pudo escribir la imagen en el destino	Comprobar la ubicación y los permisos de acceso

Glosario

CAPÍTULO 15

Término	Descripción
AES-256-GCM	Advanced Encryption Standard, clave de 256 bits, modo GCM (AEAD). FIPS 197, NIST SP 800-38D.
Análisis RS	Análisis Regular-Singular: detector estadístico de LSB.
Canal alfa	Cuarto canal de la imagen (R,G,B+A) para la transparencia (0–255).
Digital Source Type	Campo de los NewsCodes de IPTC que indica el origen de una imagen de forma legible por máquina, p. ej. «totalmente generada por IA» o «editada con IA»; pieza central del etiquetado del artículo 50.
DNG	Formato RAW abierto (Adobe) para datos de sensor: sin comprimir, con compresión sin pérdidas o (desde DNG 1.4) con pérdidas.
Esteganografía	Ocultación de información dentro de un soporte.
EXIF 2.32	Norma de metadatos en archivos de imagen (CIPA DC-X008).
GCM	Modo de operación de AES (Galois/Counter Mode): cifra y autentica en un solo paso (AEAD). En Stego-Lab, la etiqueta de autenticación de 16 bytes garantiza la integridad del cifrado; no hace falta un HMAC aparte.
HEIC	Archivo de imagen en el contenedor HEIF (ISO/IEC 23008-12) con codificación HEVC, adoptado por Apple como formato predeterminado. Normalmente con pérdidas.
HMAC-SHA256	Código de autenticación de mensajes con clave basado en SHA-256 (RFC 2104). Stego-Lab lo usa únicamente como función pseudoaleatoria dentro de PBKDF2, no para comprobar la integridad; de eso se encarga la etiqueta de autenticación GCM.
Ji cuadrado	Método estadístico de estegoanálisis para detectar el LSB.
LSB	Bit menos significativo de un byte. Diferencia de color de ± 1 : invisible.
Marca de agua	Señal de autoría, visible o invisible, incorporada a un medio.
Nonce	Valor inicial aleatorio de 12 bytes para AES-GCM; garantiza la unicidad del texto cifrado.
PBKDF2-HMAC-SHA256	Derivación de clave a partir de la contraseña y la sal con 600.000 iteraciones (OWASP 2023).
PNG	Formato ráster sin pérdidas. ISO/IEC 15948. Formato principal de Stego-Lab.
PSNR	Medida de calidad de imagen en dB. > 51 dB = modificación invisible.
PV1	Formato de desarrollo de Stego-Lab (del 31 de marzo al 2 de abril de 2026, derivación de clave HKDF-SHA256 con sal fija), nunca publicado. La app solo lo lee; los contenidos nuevos se escriben exclusivamente en PV2.

Término	Descripción
PV2	Formato de trama de Stego-Lab desde la versión 1.0: cabecera de 10 bytes (identificador «PV2», versión, longitud, indicadores), con cifrado sal, nonce y cifrado AES-256-GCM con etiqueta, y opcionalmente un bloque de IA sin cifrar (véase 14.2).
RAW	Formato de datos brutos del sensor. Sin pérdidas y propio de cada fabricante.
Reglamento de IA, art. 50	Obligaciones de transparencia del Reglamento europeo de IA: los proveedores deben marcar las salidas de IA de forma legible por máquina (apdo. 2); los responsables del despliegue deben revelar, en las ultrasuplantaciones, que el contenido ha sido generado o manipulado artificialmente (apdo. 4). Aplicable desde el 2 de agosto de 2026.
Sal	Valor aleatorio para PBKDF2. Impide los ataques con tablas arcoíris.
TIFF 6.0	Formato de imagen sin pérdidas. Compresión LZW/ZIP/RAW. Especificación de Adobe.
Trailer AI-DISCLOSURE (bloque final PV2)	Datos PV2 adicionales, opcionales y sin cifrar (prefijo «AIDISC1:»), situados tras la carga útil: llevan el etiquetado de IA de forma invisible en los píxeles (Pro, lote). Sobreviven al borrado de los metadatos, pero no a una recompresión con pérdidas (véase 9.6).
UTF-8	Codificación universal de caracteres. De 1 a 4 bytes. Compatible con ASCII.

Posicionamiento

CAPÍTULO 16

16.1 Comparativa de funciones

Función	Stego-Lab	Servicio en línea	Programa de escritorio	App móvil
Esteganografía LSB	SÍ	En parte	SÍ	Rara vez
AES-256	SÍ	Rara vez	En parte	No
Marca de agua visible	SÍ	SÍ	SÍ	SÍ
Marca de agua invisible	SÍ	Rara vez	En parte	No
Edición EXIF	SÍ	En parte	SÍ	En parte
Quitar el GPS	SÍ	En parte	SÍ	En parte
Procesamiento por lotes	SÍ	Rara vez	SÍ	Rara vez
Totalmente sin conexión	SÍ	NO	SÍ	En parte
Nativa en iOS/iPadOS	SÍ	Navegador	NO	SÍ
Nativa en macOS	SÍ	Navegador	SÍ	NO
Sin cuenta	SÍ	A menudo NO	SÍ	A menudo NO

16.2 Públicos objetivo

Público objetivo	Beneficio principal
Fotógrafos	Gestión de EXIF, protección del GPS, marcas de agua por lotes
Creadores de contenido	Marcas de agua de copyright, en local y con rapidez
Usuarios preocupados por la privacidad	Procesamiento local, eliminación del GPS
Especialistas en seguridad informática	Demostraciones de estegano, ejercicios de estegoanálisis
Periodistas	Incrustación cifrada de pruebas
Archiveros	Edición masiva de EXIF, mantenimiento de metadatos
Docentes y estudiantes	Demostraciones prácticas de los conceptos
Usuarios particulares	Archivo discreto de documentos sensibles

Referencia de flujos de trabajo

CAPÍTULO 17

17.1 Flujo de codificación (Pro)

Paso	Acción	Observación
1	Cargar una imagen portadora ≥ 8 MP (se recomienda PNG/TIFF; JPEG, HEIC y RAW también se cargan)	Comprobar la capacidad
2	Elegir el tipo de contenido: texto / imagen / archivo	Indicador de capacidad
3	Introducir una contraseña (al menos 12 caracteres, mejor una frase de contraseña)	Recomendado; la app avisa por debajo de 8 caracteres
4	Salida: PNG o TIFF	PNG = más ligero
5	Iniciar la codificación	Progreso
6	Probar en el área Decode	Control de calidad
7	Guardar o compartir	¡Conserva el original!

17.2 Limpieza de EXIF

Paso	Acción
1	Cargar la imagen en el área EXIF
2	Comprobar los campos GPS («Breitengrad», «Längengrad», «Höhe»: latitud, longitud, altitud)
3	Eliminar las coordenadas GPS: vaciar los tres campos (Pro); las demás etiquetas GPS permanecen; eliminación completa solo con «Alle Metadaten löschen» (borrar todos los metadatos, gratis)
4	Copyright: fijar «© 2025 Nombre» (gratis)
5	Rellenar el campo «Künstler» (autor) (gratis)
6	«Änderungen anwenden» (aplicar cambios; Mac: «Metadaten anwenden») y después exportar
7	Verificar el EXIF
o bien	«Alle Metadaten löschen» (gratis) y después «Änderungen anwenden»

17.3 Lote para redes sociales (Pro)

Paso	Ajuste
1	Seleccionar todas las fotos en el área «Batch»
2	Marca visible: «@Usuario © 2025»
3	Posición: «Unten M» (abajo al centro) o «Unten R» (abajo a la derecha)
4	Opacidad: 25–40 % (regulador «Deckkraft», rango 15–100 %)
5	Formato de exportación: JPG (solo en el modo «Sichtbar» (visible); calidad no configurable)
6	Activar la opción «Alle Metadaten löschen» (borrar todos los metadatos): el GPS se elimina con ella
7	Iniciar el lote → comprobar

17.4 Etiquetar una imagen de IA

Paso	Acción	Observación
1	Cargar la imagen en Encode o en el área «Batch»	Se recomienda PNG/TIFF
2	Abrir la sección «KI-Kennzeichnung» (etiquetado de IA) y activar el interruptor «Als KI-Bild kennzeichnen» (etiquetar como imagen de IA)	Comprobar el semáforo
3	Elegir la variante: «vollständig KI-generiert» (totalmente generada por IA) / «KI-bearbeitet» (editada con IA)	Texto de etiqueta predefinido
4	Indicar el generador si se desea (p. ej. «Midjourney v7»)	Solo aparece en los metadatos
5	Comprobar la posición de la etiqueta visible en la cuadrícula 3×3	Por defecto: abajo a la izquierda
6	Batch/Pro: activar si se desea «Robuste unsichtbare Schicht (Pro)» (capa invisible robusta)	Obliga a usar PNG/TIFF
7	Iniciar la codificación o el lote y comprobar que el semáforo está verde	Verde = todos los componentes fijados

Evaluación de seguridad

CAPÍTULO 18

18.1 Modelo de amenazas

Amenaza	Sin contraseña	Con AES-256	Valoración
Inspección visual	Seguro	Seguro	OK
Análisis RS	Detectable	Canal visible, contenido no	Aceptable con contraseña
Ji cuadrado	Detectable	Canal visible, contenido no	Aceptable con contraseña
Fuerza bruta (contenido)	Legible	Prácticamente imposible	Seguro con contraseña
Conversión a JPEG	Destruído	Destruído	¡Conserva el PNG/TIFF!
Interceptación en la nube	No procede	No procede	Sin nube

18.2 Recomendaciones para contraseñas

Requisito	Recomendación	Motivo
Longitud mínima	12 caracteres	Por debajo de 8 caracteres es atacable incluso con PBKDF2
Conjunto de caracteres	Mayúsculas + minúsculas + cifras + símbolos	Espacio de búsqueda exponencialmente mayor
Palabras del diccionario	Evitarlas	Los ataques por diccionario son eficaces
Reutilización	Nunca	Una contraseña comprometida pone en riesgo todo
Custodia	Gestor de contraseñas	Almacenamiento cifrado y seguro

18.3 Revisión de seguridad interna previa a la publicación

Entre abril y septiembre de 2026, el código fuente de Stego-Lab se revisó internamente varias veces en busca de vulnerabilidades de seguridad, la última antes del envío de la versión 1.1. Las revisiones se realizaron con ayuda de IA; el desarrollador evaluó y aplicó los resultados. Se trata de revisiones técnicas internas, no de una auditoría independiente ni de una certificación. El informe de la primera revisión, del 10 de abril de 2026, puede consultarse en el repositorio público como SECURITY-AUDIT.md. En ninguno de los informes se detectó un hallazgo crítico; los hallazgos clasificados como altos se corrigieron antes del envío. Las limitaciones conocidas figuran en la tabla; algunos puntos de gravedad baja están documentados y siguen abiertos.

Área	Aspectos revisados	Estado
Criptografía	AES-256-GCM; PBKDF2-HMAC-SHA256 con 600.000 iteraciones; sal aleatoria de 16 bytes; nonce de 12 bytes; las claves nunca se guardan ni se transmiten	revisado
Contraseñas en memoria	La app no sobrescribe de forma explícita en memoria las contraseñas ni las claves derivadas (límite de Swift/SwiftUI; hallazgo S-01/N-02, gravedad baja)	limitación conocida
Formatos antiguos (solo lectura)	PV1 (formato de desarrollo, nunca publicado), Stegosuite y F5: procedimientos más débiles u obsoletos, solo lectura, aviso en la app	limitación conocida
EXIF / metadatos	Saneamiento de metadatos; sin traspaso involuntario de datos GPS ni de cámara	revisado
Acceso a archivos	Protección frente a travesía de rutas, saneamiento de nombres de archivo externos, límites de tamaño y píxeles, App Sandbox (versión de la App Store)	revisado
Desbloqueo Pro	Bloqueo en la interfaz y, para ocultar y para el procesamiento por lotes, también en la lógica de la aplicación; verificación de las transacciones de StoreKit	revisado
Privacidad	Sin conexiones de red propias, sin telemetría, sin nube (excepciones: gestión de compras mediante StoreKit de Apple, enlaces abiertos en el navegador)	revisado
Marcas de agua	Modo combinado: primero visible, después invisible; los datos ocultos se conservan	revisado
Plataformas	Capa de seguridad común (StegoEngine) para iOS, iPadOS y macOS	revisado

■ El informe de la revisión del 10 de abril de 2026 puede consultarse en el repositorio público como [SECURITY-AUDIT.md](#); un resumen de las revisiones posteriores figura en [CHANGELOG.md](#). Los informes detallados de las revisiones posteriores se conservan internamente en el archivo del proyecto y no forman parte de la documentación publicada. Para cuestiones de seguridad, escribe al correo de soporte.

Soporte y contacto

CAPÍTULO 19

19.1 Canales de soporte

Canal	Descripción
Valoraciones en la App Store	Comentarios públicos
Enlace de soporte en la App Store	Enlace directo de soporte
Información en la app	Referencia rápida integrada
Actualizaciones	Actualizaciones periódicas con correcciones

19.2 Limitaciones conocidas

Limitación	Detalle
JPEG en esteganografía	No admitido: usar PNG/TIFF
GIF animados	Solo el primer fotograma
Salida RAW	Solo como entrada; la salida es PNG/TIFF
Estegano por lotes	El mismo contenido para todas las imágenes
App Atajos	Previsto
Recuperación de contraseña	No es posible

Índice de tablas

CAPÍTULO 20

N.º	Denominación	Capítulo
T-01	Ficha de la app	Portada
T-02	Requisitos del sistema	2.1
T-03	Pasos de instalación	2.2
T-04	Navegación principal	3.1
T-05	Área Codificar	3.2
T-06	Área Decodificar	3.3
T-07	Especificación LSB	4.2
T-08	Capacidades de texto	4.3
T-09	Cifrado	4.4
T-10	Parámetros de la marca de agua	5.1
T-11	Opciones de posicionamiento	5.3
T-12	Campos EXIF (legibles)	6.2
T-13	Campos EXIF editables	6.3
T-14	Campos GPS	6.4
T-15	Parámetros del modo por lotes	7
T-16	Formatos de entrada	8
T-17	Formatos de salida	8
T-18	Recomendaciones de formato	8
T-19	Campos de etiquetado de IA escritos	9.3
T-20	Resumen de privacidad	10.1
T-21	Pasos del cifrado	10.2
T-22	Seguridad esteganográfica	10.3
T-23	Rendimiento	11.1
T-24	Necesidades de memoria RAM	11.2

N.º	Denominación	Capítulo
T-25	Algoritmos y normas	11.3
T-26	Ejemplo de uso 12.1	12
T-27	Ejemplo de uso 12.2	12
T-28	Ejemplo de uso 12.3	12
T-29	Objetivos de aprendizaje	12.4
T-30	Preguntas frecuentes (15 entradas)	13
T-31	Gestión de errores	14.3
T-32	Glosario (25 entradas)	15
T-33	Comparativa de funciones	16.1
T-34	Públicos objetivo	16.2
T-35	Flujos de trabajo (4×)	17
T-36	Modelo de amenazas	18.1
T-37	Recomendaciones para contraseñas	18.2
T-38	Limitaciones	19.2

Historial de versiones

CAPÍTULO 21

Versión	Fecha	Cambios
1.0	16/04/2026	Primera publicación para iPhone y iPad (App Store): Encode, Decode, EXIF, Batch, Info
1.0	20/04/2026	Primera publicación para Mac (Mac App Store): Verstecken, Entdecken, Batch, EXIF, Info
1.0	04/2026	Versiones mínimas: iOS 16 / iPadOS 16 / macOS 13 (Mac: Apple Silicon e Intel)
1.0	04/2026	Cifrado por contraseña AES-256-GCM (autenticado, etiqueta de 16 bytes); derivación de clave PBKDF2-HMAC-SHA256 con 600 000 iteraciones y sal aleatoria de 16 bytes (formato PV2)
1.0	04/2026	Ruta de lectura para imágenes de versiones de desarrollo anteriores a la publicación (formato PV1, HKDF-SHA256): solo descifrado, nunca distribuido para cifrar
1.0	04/2026	Mac: lectura de imágenes PNG de Stegosuite (solo descifrado: AES-128-CTR, PBKDF2-HMAC-SHA1, generador de posiciones MD5)
1.0	04/2026	Mac: ataque por diccionario de contraseñas en el área Decodificar con una lista propia
1.0	04/2026	Lotes (Pro): marcas de agua visibles e invisibles, contenidos ocultos con cifrado opcional
1.0	04/2026	Imágenes portadoras: PNG, TIFF, JPEG, HEIC y varios formatos RAW
1.0	04/2026	Totalmente local: sin nube
1.1	2026	Versiones mínimas elevadas: iOS 17 / iPadOS 17 / macOS 14 (antes iOS 16 / iPadOS 16 / macOS 13) con el cambio a Xcode 27; la versión 1.0 sigue siendo utilizable en dispositivos más antiguos
1.1	2026	Cifrado de los contenidos nuevos sin cambios respecto a 1.0 (AES-256-GCM, PBKDF2-HMAC-SHA256, 600 000 iteraciones, formato PV2)
1.1	2026	Selector de modo oscuro (sistema/claro/oscuro) en iOS/iPadOS
1.1	2026	iPhone/iPad: ataque por diccionario de contraseñas en el área Decodificar; en ambas plataformas ahora con la lista Nmap incluida (Mac: ataque disponible desde 1.0)
1.1	2026	Selector de archivos unificado (iOS) con coordinador de hojas
1.1	2026	Refuerzo de la seguridad: paridad AES, saneamiento EXIF, bloqueo Pro
1.1	2026	iPhone/iPad: enlaces de donación externos eliminados; Mac: sigue el modo claro/oscuro del sistema

Versión	Fecha	Cambios
1.1	2026	iPhone/iPad: lectura de imágenes PNG de Stegosuite (solo descifrado); en Mac desde 1.0
1.1	2026	Decodificador F5/JPG: se pueden abrir los JPG antiguos de Stegosuite 0.8 (esteganografía en el dominio DCT), con mensaje Y archivo adjunto oculto en una misma imagen
1.1	2026	Indicador de progreso al decodificar rutas heredadas costosas (Stegosuite/F5)
1.1	2026	Aviso de detección en formatos criptográficos heredados más débiles (PV1 / Stegosuite): se permite leer, no escribir
1.1	2026	Ocultar directamente una foto de la cámara: incrustación en un solo paso, sin pasar por la fototeca (Mac: solo en memoria; iPhone/iPad: archivo temporal en el contenedor de la app), con control de calidad; en macOS con Continuity Camera
1.1	2026	Cámara de iOS: la orientación EXIF se graba en los píxeles al incrustar, de modo que las tomas quedan bien orientadas
1.1	2026	Recibir una foto como imagen portadora desde el menú Compartir / «Abrir con» (iPhone/iPad: «Copiar en Stego-Lab»; Mac: «Abrir con Stego-Lab»)
1.1	2026	Área Encode: botones más compactos, solo con icono, para una interfaz más despejada
1.1	2026	Etiquetado de IA según el art. 50 del Reglamento europeo de IA: ajuste preestablecido en Encode/Batch, distintivo en Decode/EXIF, capítulo del manual
1.1	2026	Borrar todos los metadatos con un clic (pestaña EXIF, gratis) y por lotes (Pro)

Funciones previstas

Función	Estado
Integración con la app Atajos	Previsto
Extensión de compartir	Descartada deliberadamente (seguridad: requeriría un grupo de apps)
Modo de 2 LSB	Idea
Detector de estegoanálisis	Previsto
Metadatos IPTC	Implementado (1.1)
Metadatos XMP	Implementado (1.1)

Compra integrada Stego-Lab Pro

CAPÍTULO 22

Stego-Lab está disponible gratis en la App Store. Existe exactamente una compra integrada: «Stego-Lab Pro». Se paga una sola vez, no tiene suscripción ni fecha de caducidad y desbloquea de forma permanente las funciones indicadas más abajo. No hay más paquetes ni extensiones. El precio vigente se muestra en la App Store.

22.1 Free y Pro de un vistazo

El desbloqueo se realiza exclusivamente a través de la App Store: sin clave de licencia, sin número de serie y sin intervención del desarrollador. El cifrado no se vende por separado: la protección con contraseña forma parte de Stego-Lab Pro. La tabla siguiente refleja el comportamiento real de la app.

Área	Free	Adicionalmente con Stego-Lab Pro
Encode	Cargar una imagen portadora; aplicar la etiqueta de IA visible y los metadatos de IA, y guardar la imagen	Incrustar de forma invisible texto, imagen o archivo (LSB); protección opcional con contraseña (AES-256-GCM, PBKDF2-HMAC-SHA256, 600 000 iteraciones); toma directa con la cámara (Mac: Continuity Camera)
Decode	Mostrar, copiar y compartir texto incrustado sin cifrar	Imágenes y archivos incrustados; contenidos protegidos con contraseña, incluidas las imágenes PNG de Stegosuite y JPG F5 (solo lectura); ataque por diccionario con la lista Nmap incluida o una lista propia
EXIF	Ver todos los metadatos; editar descripción, autor, copyright y software; borrar todos los metadatos con un clic	Editar los campos de cámara, objetivo, fecha, exposición, comentario y GPS
Batch	Cargar imágenes, comprobar ajustes y vista previa; exportar una sola imagen con marca de agua visible de texto o logotipo	Exportar varias imágenes en una pasada y series enteras (procesadas una tras otra): marcas de agua visibles, invisibles y combinadas, etiquetado de IA con capa invisible robusta, borrado de todos los metadatos
Info	Referencia rápida, datos de versión, ventana Pro	—

22.2 Compra y restauración

La compra se realiza en la ventana Pro de la app (accesible desde el área Info o desde cualquier aviso Pro) con el botón «Stego-Lab Pro freischalten» (desbloquear Stego-Lab Pro); el pago y la tramitación corren a cargo de la App Store. Al iniciarse, la app comprueba por sí misma el estado de la compra, por lo que en otros dispositivos con el mismo ID de Apple la compra suele reconocerse automáticamente. Si no es así, el botón «Käufe wiederherstellen» (restaurar compras) de la ventana Pro la restablece.

✓ Stego-Lab Pro es una compra única: sin suscripción, sin fecha de caducidad y sin clave de licencia. La compra y el pago los gestiona exclusivamente Apple; la restauración se hace en la app mediante «Käufe wiederherstellen» (restaurar compras) en la ventana Pro.

Sobre el desarrollador / Aviso legal

CAPÍTULO 23



Stego-Lab

Desarrollado por

Ing. Christian Raith, BEd

OE3LCR · Wiener Neustadt, Austria



Stego-Lab ha sido desarrollado por Ing. Christian Raith (BEd). Imparte taller de informática, electrotecnia y electrónica en la HTL Mödling. Sus áreas principales son la seguridad informática, los análisis y auditorías de seguridad, la programación (sobre todo Arduino y Raspberry Pi), el desarrollo de apps de seguridad, marcas de agua, protección del derecho de autor y procesamiento fotográfico, así como la documentación técnica y los materiales didácticos. Además es radioaficionado con licencia (indicativo OE3LCR, locator JN87ct) y presidente del club de radioaficionados de Triestingtal en Berndorf.

23.1 Datos del desarrollador

Propiedad	Valor
Nombre	Ing. Christian Raith, BEd
Ubicación	Wiener Neustadt, Baja Austria, Austria
Radioafición	OE3LCR · Locator JN87ct
Correo de soporte	stego-lab@proton.me
Sitio web / proyecto	www.craith.cloud/stego-lab
GitLab	gitlab.com/RaithChr/stego-lab
Profesión	Docente en la HTL Mödling: taller de informática, electrotecnia, electrónica
Especialidades	Seguridad informática · auditorías de seguridad · Arduino/Raspberry Pi · desarrollo de apps · documentación técnica

23.2 Otros proyectos del desarrollador

Proyecto	Descripción	Enlace
OE3LCR Ham Radio Dashboard	Aplicación web en directo con datos solares, condiciones de las bandas, clúster DX, seguimiento de satélites y meteorología espacial.	www.craith.cloud

Proyecto	Descripción	Enlace
Medición de frecuencia (RP2350)	Frecuencímetro de red con Raspberry Pi Pico 2, pantalla TFT ST7735 y aislamiento galvánico por optoacoplador PC817.	gitlab.com/RaithChr/Frequen zmessung-PICO2-50HZ
Stego-Lab (esta app)	Esteganografía, marcas de agua, EXIF y procesamiento de imágenes por lotes para iPhone, iPad y Mac.	gitlab.com/RaithChr/stego-l ab

23.3 Repositorio de GitLab

El código fuente de Stego-Lab está disponible públicamente en GitLab (gitlab.com/RaithChr/stego-lab). El historial de versiones se encuentra en CHANGELOG.md y docs/VERSION-HISTORY.de-en.md; el procedimiento para notificar vulnerabilidades se describe en SECURITY.md.

Repositorio de GitLab

gitlab.com/RaithChr/stego-lab

23.4 Sitio web

Sitio del proyecto

www.craith.cloud/stego-lab

Aspectos legales y privacidad

CAPÍTULO 24

24.1 Política de privacidad (resumen)

Stego-Lab procesa todos los datos del usuario exclusivamente en local, en su dispositivo. La app no recopila, almacena, transmite ni procesa ningún dato personal en servidores externos.

Categoría de datos	Procesamiento	Transmisión externa
Imágenes	Solo en local	NO
Contenidos incrustados	Solo en local	NO
Contraseñas	Solo en memoria, nunca se guardan	NO
Metadatos EXIF	Solo en local	NO
Estadísticas de uso	No se recopilan	NO
Informes de fallos	Desactivados	NO
Datos publicitarios	No existen	NO
Datos de ubicación	Nunca se solicitan	NO

24.2 Licencia y condiciones de uso

El código fuente de Stego-Lab está publicado bajo la licencia MIT (gitlab.com/RaithChr/stego-lab, archivo LICENSE). La app obtenida en la App Store se rige además por los Términos y Condiciones de Apple Media Services y por el contrato de licencia de usuario final estándar de Apple.

Disposición	Detalles
Licencia	El código fuente de Stego-Lab está bajo la licencia MIT (© 2026 Christian Raith; archivo LICENSE del repositorio). Los componentes de terceros (véase 24.3) están sujetos a sus propias licencias. El nombre y la marca denominativa «Stego-Lab», el logotipo, el icono de la app y el texto del manual no están cubiertos por la licencia MIT; todos los derechos reservados.
Versión de la App Store	La app obtenida en la App Store se rige por los Términos y Condiciones de Apple Media Services y por el contrato de licencia de usuario final estándar de Apple. Las funciones Pro se desbloquean mediante compra integrada, sin clave de licencia (véase el capítulo 22).
Uso permitido	Stego-Lab está destinado a fines lícitos. El usuario es responsable del cumplimiento de la legislación aplicable, en particular de los derechos de autor de terceros.

Disposición	Detalles
Exención de responsabilidad	El software se proporciona sin garantía (véase la licencia MIT). Una contraseña olvidada no puede recuperarse; se recomienda expresamente hacer copias de seguridad.
Modificaciones	Son determinantes el archivo LICENSE del repositorio en su versión vigente y el contrato de licencia de Apple; las excepciones relativas a la marca, el logotipo, el icono de la app, el texto del manual y los componentes de terceros no se ven afectadas.

24.3 Frameworks utilizados y componentes de terceros

Stego-Lab no incorpora bibliotecas de programas de terceros. La criptografía, el procesamiento de imágenes y la interfaz proceden de los frameworks de Apple; forman parte del sistema operativo y no se distribuyen con la app. Se incluye un componente de terceros: la lista de contraseñas del proyecto Nmap. Las funciones de lectura de imágenes antiguas de Stegosuite y F5 se portaron a Swift desde el código fuente Java de Stegosuite 0.8 (GPL).

Componente	Uso en Stego-Lab	Origen / licencia
CryptoKit	AES-256-GCM (cifrado y descifrado); HKDF-SHA256 solo para leer imágenes PV1; MD5 y SHA-1 solo para leer imágenes de Stegosuite y F5	Apple, parte del sistema operativo
CommonCrypto	PBKDF2-HMAC-SHA256 (600 000 iteraciones); PBKDF2-HMAC-SHA1 y AES-128-CTR solo para descifrar imágenes de Stegosuite	Apple, parte del sistema operativo
SecRandomCopyBytes (framework Security)	Sal aleatoria de 16 bytes por cada cifrado; el nonce de 12 bytes lo genera CryptoKit	Apple, parte del sistema operativo
Compression	Descompresión zlib al leer imágenes de Stegosuite y F5	Apple, parte del sistema operativo
ImageIO, CoreGraphics, CoreText	Lectura y escritura de imágenes, acceso a píxeles para LSB, metadatos EXIF, IPTC y XMP, tipografía de la etiqueta de IA	Apple, parte del sistema operativo
CoreImage	Solo iPhone/iPad: orientación de las tomas de la cámara	Apple, parte del sistema operativo
AVFoundation	Toma directa con la cámara, en el Mac mediante Continuity Camera	Apple, parte del sistema operativo
Photos, PhotosUI	Solo iPhone/iPad: importación desde la fototeca y guardado en ella	Apple, parte del sistema operativo
StoreKit	Compra integrada «Stego-Lab Pro»	Apple, parte del sistema operativo

Componente	Uso en Stego-Lab	Origen / licencia
SwiftUI, UIKit, AppKit, Foundation, Combine, UniformTypeldentifiers, CoreTransferable	Interfaz, selección de archivos, detección de tipos de archivo	Apple, parte del sistema operativo
Lista de contraseñas de Nmap (passwords.lst)	Lista incluida con unas 5 000 entradas para el ataque por diccionario en el área Decodificar	© 1996–2022 Nmap Software LLC; Nmap Public Source License (nmap.org/npsl)
Compatibilidad de lectura Stegosuite / F5	Solo lectura: extracción y descifrado de imágenes creadas con Stegosuite 0.8 (PNG y JPEG con F5), incluido el generador pseudoaleatorio Java SHA1PRNG portado a Swift (SHA-1 de CryptoKit)	Portado a Swift desde el código fuente Java de Stegosuite 0.8 (GPL-3.0); método F5 según A. Westfeld, decodificador Huffman según Westfeld/Breslin

24.4 Derechos de autor y marcas

Stego-Lab, el logotipo de Stego-Lab y todos los gráficos asociados son propiedad de Ing. Christian Raith. Apple, iPhone, iPad, Mac, iOS, iPadOS, macOS, App Store y el logotipo de Apple son marcas registradas de Apple Inc.

Recurso	URL
Repositorio de GitLab	gitlab.com/RaithChr/stego-lab
Página del proyecto	www.craith.cloud/stego-lab/es/
Política de privacidad	www.craith.cloud/stego-lab/es/privacy-policy.html
Soporte	www.craith.cloud/stego-lab/es/support.html
Correo de soporte	stego-lab@proton.me
Política de privacidad de Apple	apple.com/legal/privacy

Stego-Lab · Versión 1.1 · © 2026 Ing. Christian Raith, BEd
 Software: licencia MIT · Texto del manual, marca & logotipo: todos los derechos reservados
 iOS · iPadOS · macOS · Apple Silicon & Intel x86_64



Stego-Lab

Versión 1.1 · iOS · iPadOS · macOS

© 2026 Christian Raith

Ing. Christian Raith, BEd · OE3LCR

Software: licencia MIT · Manual & marca: todos los derechos reservados

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

stego-lab@proton.me