Computergestützte Steganographie

Computergestützte Steganographie bezeichnet Verfahren, die mithilfe steganographischer Techniken Daten in durch einen Computer zugänglichen Trägerdaten verbergen. Es wird dabei das Ziel verfolgt, die Vertraulichkeit zu sichern.

Beispiele für Trägerdaten, die computergestützt steganographisch verändert werden, sind Bilddaten, Audiodaten und Textdaten.

By Teumteum (steganart.com), CC-BY-SA-3.0 - Wikimedia Commons

Abgrenzung

Das Funktionsprinzip der Steganographie beruht darauf, dass ein Aussenstehender die Existenz der steganographierten Information nicht erkennt. Dadurch unterscheidet Steganographie sich von der Kryptographie, bei der ein Aussenstehender zwar um die Existenz von Informationen weiss, aber aufgrund der Verschlüsselung nicht in der Lage ist, den Inhalt zu verstehen.

Sicherheit

Ein steganographisches Verfahren gilt genau dann als sicher, wenn nach Anwendung des Verfahrens auf ein Medium dritte Personen keinerlei Rückschlüsse ziehen können, ob in einem vorliegenden Medium nicht offensichtliche Informationen verborgen sind. Ein weiteres, aber nachrangiges Sicherheitsmerkmal ist, dass eingebettete Informationen selbst bei Kenntnis von deren Existenz von Dritten nicht auslesbar sind.

Beispiel: Bilder verstecken

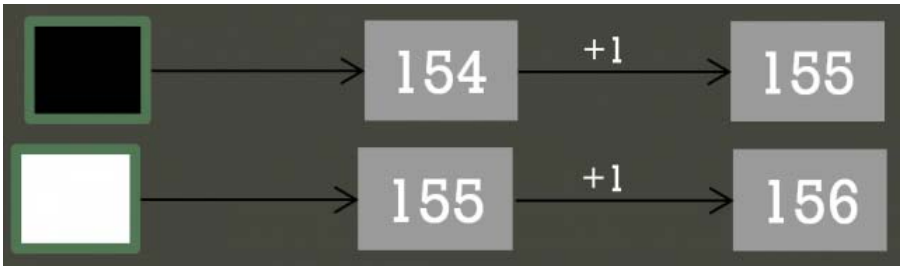
Wir verstecken Bilder in anderen Bildern, indem wir die Graustufenwerte leicht verändern. Hierbei nutzen wir aus, dass kleine Veränderungen der Grauwerte für das menschliche Auge nicht erkennbar sind.

Um einen schwarzen Pixel zu verstecken, muss der Wert im Originalbild ungerade sein. Ist dies noch nicht der Fall, erhöht man den Wert um 1.

Zum Verstecken eines weissen Pixel, muss der Wert im Originalbild gerade sein. Ist dies noch nicht der Fall, erhöht man den Wert um 1.

Achtung: Bei 255 muss der wird um 1 verringert werden.

Zum Herauslesen des geheimen Bildes markiert man alle ungeraden Grauwerte. Die ungeraden Werte ergeben die schwarzen Pixel, die geraden Werte die weissen Pixel.



OpenPuff - Steganographie Tool

OpenPuff ist ein Steganographie Tool mit hochsicherer Mehrfach-Verschlüsselung, welches sensible Daten erst sicher verschlüsselt und dann in anderen Dateien versteckt.

OpenPuff schützt Ihre Daten in einem mehrstufigen Verfahren, in welchem Daten zunächst mit einen doppelt passwortgeschützten Multikryptografie Verfahren, welches 16 hochsichere 256-Bit Verschlüsselungs-Algorithmen verwendet, verschlüsselt werden.

OpenPuff kann sensible Dateien auf mehrere Trägerdateien verteilen (sofern Sie genug Trägerdateien zur Verfügung haben) und die letzte Trägerdatei mit Zufallszahlen auffüllen, so dass diese sich nicht von anderen Trägerdateien unterscheidet.

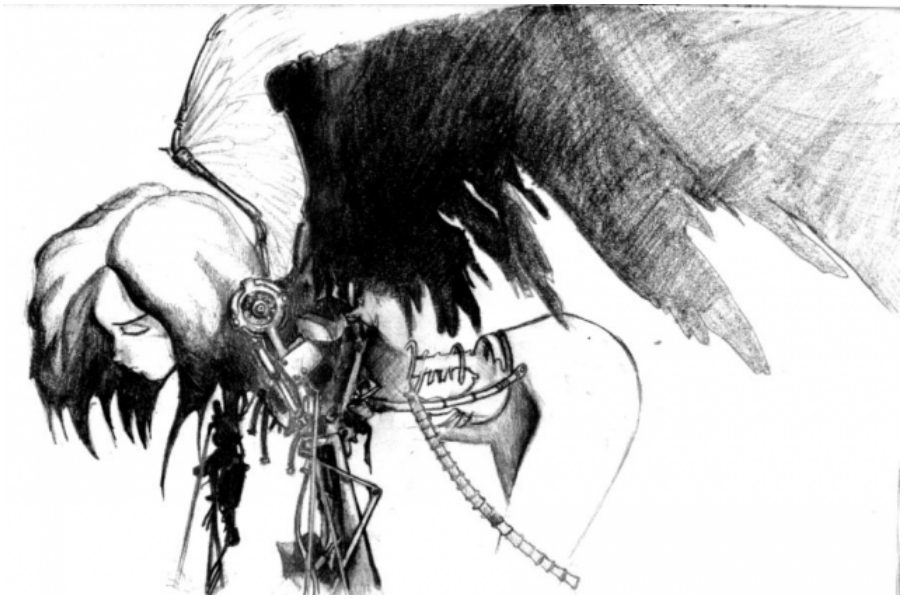
OpenPuff ist auch als installationsfreie Portable Anwendung erhältlich, die darüber hinaus auch im sogenannten "Stealth Modus" verdeckt arbeitet.

Aufgabenstellungen

Für diese Übungen sollten Sie ein Konto auf https://www.root-me.org/ eröffnen.

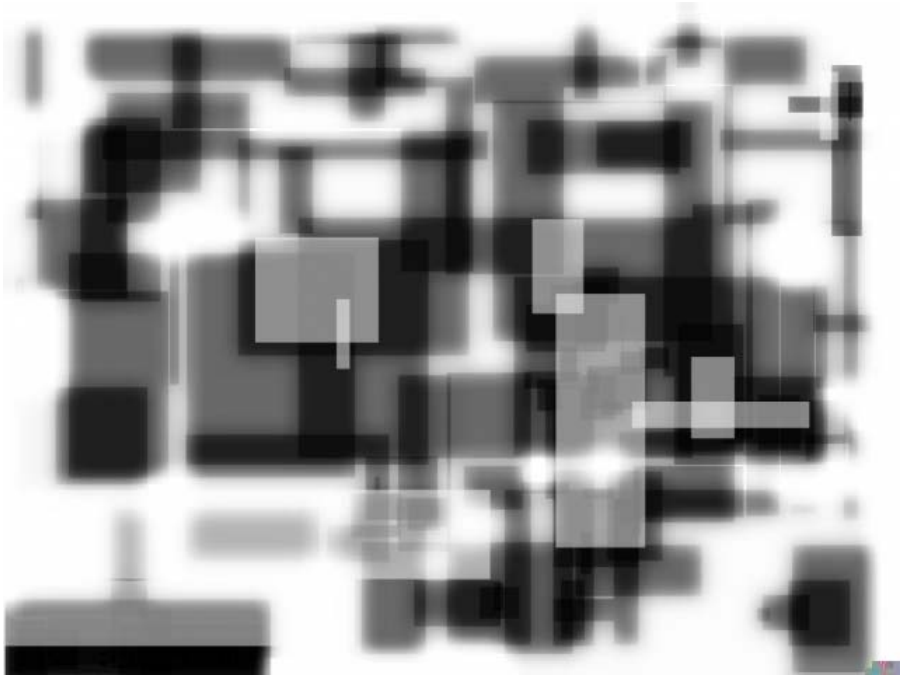
Welches Passwort ist in diesem Bild versteckt?

Hinweis: Zoomen Sie in das Bild hinein ...
Tragen Sie das Passwort bei For the beginning : an image ein.



Welches Passwort ist in diesem Bild versteckt?

Hinweis: Öffnen Sie die Datei mit einem HEX Editor.
Tragen Sie das Passwort bei Squared ein.



Welches Passwort ist in der Audio Datei versteckt?

Laden Sie die Datei unter Audio Stegano herunter und tragen Sie das Passwort bei Audio Stegano ein. Verwenden Sie Sonic Visualizer um die Audio Datei zu analysieren.

Audio in einem Bild mit OpenPuff verstecken

Machen Sie sich mit dem Tool OpenPuff vertraut. Versuchen Sie eine Audio Datei in einer Bild Datei zu verstecken.

Wo werden wir uns treffen?

Hinweis: Homoglyphen sind ähnlich oder gleich aussehende Schriftzeichen.

Choose a job you love, and you will never have to work a day in your life.

Tragen Sie das Passwort bei Twitter Secret Messages ein.

Zu schwierig? Lassen Sie sich helfen. Hide secret messages in your tweets (or any text) with steg-of-the-dump.js.