

Update

Eine kurze Einführung

Wie ich erkennen kann, ist der Artikel auf Wikipedia angepasst worden. Insbesondere wird ein gewisser Spielraum in der Definitionen der Begriffe offengehalten. Das habe ich schon in einigen Wikipedia-Artikel erkennen dürfen.

Ich bin mir sicher, dass die Abgrenzungen wie auch die ganz genauen Beschreibungen in der Wissenschaft wie auch in der Rechtsprechung irgendwann zu einer Konklusion führen, wo die genauen Erkenntnisse und Bildung der Normen auch für den Internationalen oder Nationalen Bereich einfließen und festgehalten werden.

Ich werde hier immer noch meine eigene Worte verwenden, wie ich es damit genau meine.

Steganographie

Gemäss Wikipedia ist Steganographie die Kunst bzw. Wissenschaft der verborgenen Speicherung oder Übermittlung von Informationen in einem Trägermedium (Container). In diesen Artikel beziehe ich mich auf die kryptographische Steganographie.

Das Ziel der Steganographie ist die Geheimhaltung bzw. die Vertraulichkeit von Informationen. Der "Dritte" soll also bei Betrachtung des Trägermediums (Bilder, Dateien, etc.) kein Verdacht schöpfen können, dass es sich um ein Trägermedium handelt, dass ganz bewusst versteckte Informationen beinhaltet. Mit der Kryptographie meint man hier die Geheimhaltung die gewährleistet werden soll.

Es gibt unterschiedliche Verfahren. Einige haben sich bestens bewährt, andere hingegen lassen Manipulationen sofort erkennen, und gewährleisten in dem Sinne „vertrauliche Geheimhaltung durch Verbergen der Geheimhaltung“ kryptographisch nicht.

Es darf also gesagt werden, sobald unsere Wahrnehmung erkennen lassen, dass es sich um ein manipuliertes Trägermedium handelt, verliert die kryptographische Steganographie ihre Gewährleistung und ihren Zweck, und es darf streng genommen nicht mehr zu dieser Kunst gezählt werden.

© Steganography 2022

Ist ein Programm das als Trägermedium ein Bild voraussetzt. In dieses Bild kann Text oder wiederum ein Bild "versteckt" werden.

Voraussetzung von © Steganography 2022

Windows 10 / ideal ab I5 Prozessor

.Net Core-Framework muss eventuell installiert sein.

Seit neuerem besteht die Möglichkeit RunTimes-Dateien mitzuliefern, was das Ganze enorm erleichtert. Eine vorgängige Installation des .Net Core-Framework muss nicht mehr gemacht werden, da alle Dateien die die Lauffähigkeit sicherstellen, direkt beiliegend zur Exe-Datei vorhanden sind. Ein Doppelklick auf die exe-Datei reicht schon.

Verfahren von © Steganography 2022

Das entsprechende Verfahren für die Einbettung bzw. Extraktion von Informationen basiert auf Bit-Ebene mit Bit-Operationen, die gewährleisten sollen, dass die Umsetzung fehlerfrei abgeschlossen werden können.

Grenzen Speicherkapazität von © Steganography 2022

Trotzdem gibt es Grenzen die sich einfach erklären lassen. Stellen Sie sich vor, das Trägermedium (Basic Image) besitzt die Grösse von 100 x 100 Pixel. Es versteht sich von selbst, dass ein solches Bild eine gewisse "Speicherkapazität" besitzt, und sobald die aufgebraucht ist, können weitere Informationen nicht mehr eingearbeitet werden, nicht ohne bewusstes manipulieren der Trägermedien, sei es durch vergrössern oder durch andere Techniken.

(Beispiel: Totale Speicherkapazität für ein Bild mit 100 x 100 Pixel ergibt beachtliche 239'943 Bits oder 29'992 Bytes abzüglich den Header-Informationen)

Einteilung Speicherkapazität von © Steganography 2022

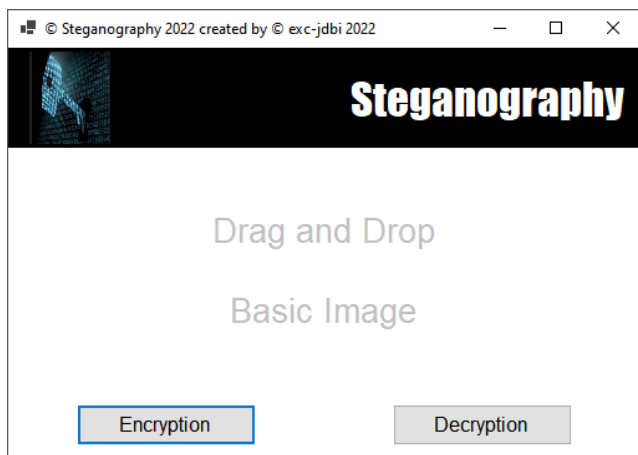
© Steganographie 2022 teilt die "Speicherkapazität" in 4 Kategorien ein.

- L1: Wahrnehmung auf keine Manipulationen, Geheimhaltung, sowie die Vertraulichkeit sind komplett gewährleistet.
- L2: Bedingte erkennbare Manipulationen durch Wahrnehmung können bestehen, wobei die Geheimhaltung (Kryptographie), sowie Vertraulichkeit immer noch gewährleistet sein können.
- L3: Veränderungen sind durch Wahrnehmung deutlich erkennbar, wobei Vertraulichkeit nicht mehr gewährleistet ist. Die Geheimhaltung (die Kryptographie) der Informationen kann jedoch immer noch bestehen.

Ist der letzte Bereich (L3) ausgeschöpft, so ist das Trägermedium zu klein für die gewünschten Informationen die eingearbeitet werden sollen. © Steganographie 2022 lässt das deutlich erkennen. (Farben: L1 = Grün, L2 = Gelb, L3 = Orange und L4 = Rot >> für zu wenig Speicherkapazität)

Starten von © Steganography 2022

© Steganography 2022 lässt sich auf dem Windows-Rechner mit einem Doppelklick auf die Exe-Datei starten. Seit .Net Core 6 werden die RunTimes-Dateien auch mitgeliefert. Eine vorgängige Core-Framework Installation ist nicht mehr notwendig.



Das Startbild lässt drei Möglichkeiten erkennen.

Encryption steht dafür, ein Bild oder Text in das Trägermedium (Basic Image) einzubetten.

Decryption steht dafür, ein Bild oder ein Text aus dem Trägermedium zu extrahieren.

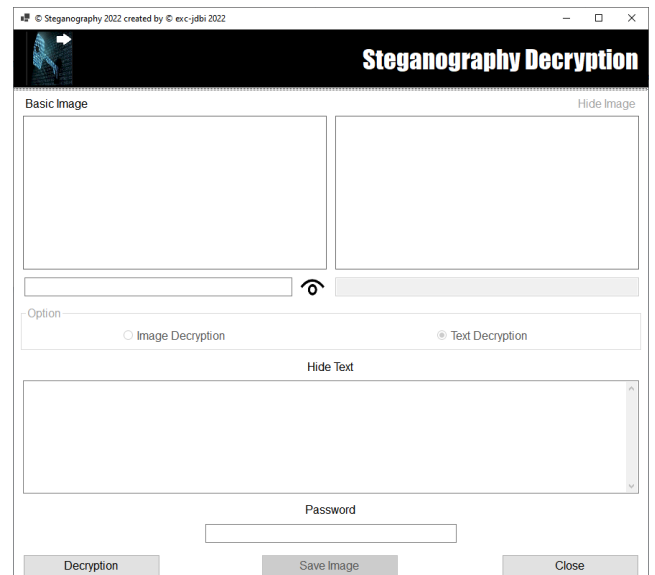
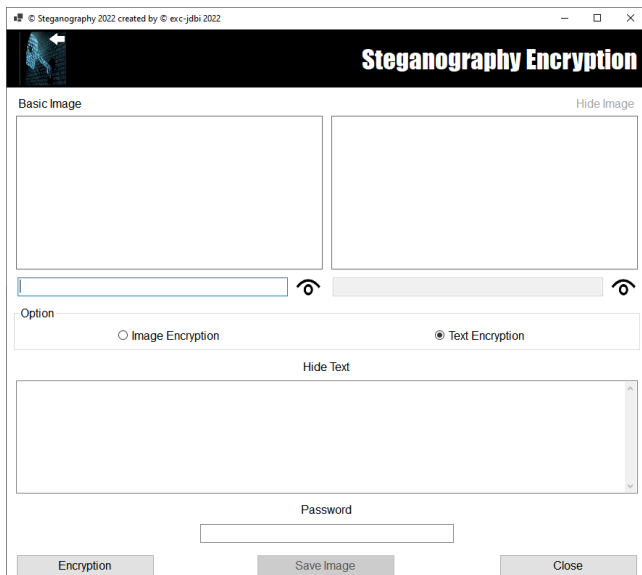
Die *dritte Möglichkeit* ist die einfachste Vorgehensweise, in dem einfach ein Bild als Trägermedium (Basic Image) auf die 'Drag and Drop' Oberfläche gezogen wird.

© Steganography 2022 erkennt bei 'Drag and Drop' selber was gemacht werden muss. Sofern das Trägermedium schon eingebettete Informationen besitzt wird automatisch die 'Decryption-Maske' ausgeführt. Sind keine eingebettete Informationen vorhanden wird automatisch 'Encryption-Maske' ausgeführt. Das entsprechende Trägermedium wird in die neue Maske übernommen.

Wichtig: © Steganography 2022 erkennt nur eigene Verkryptungen. Ein anderes Steganographie Programm würde es nicht erkennen.


Bemerkung: Es soll ja nur eine Möglichkeit zeigen wie Steganographie funktionieren kann.

Die leeren Encryption- und Decryption Masken

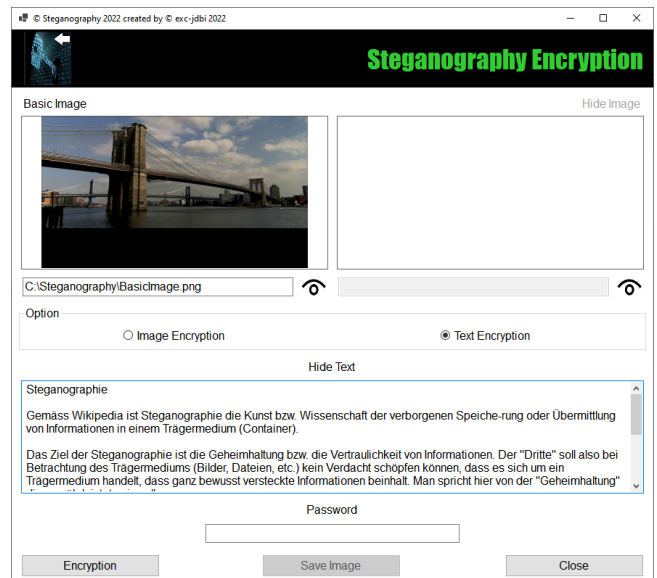
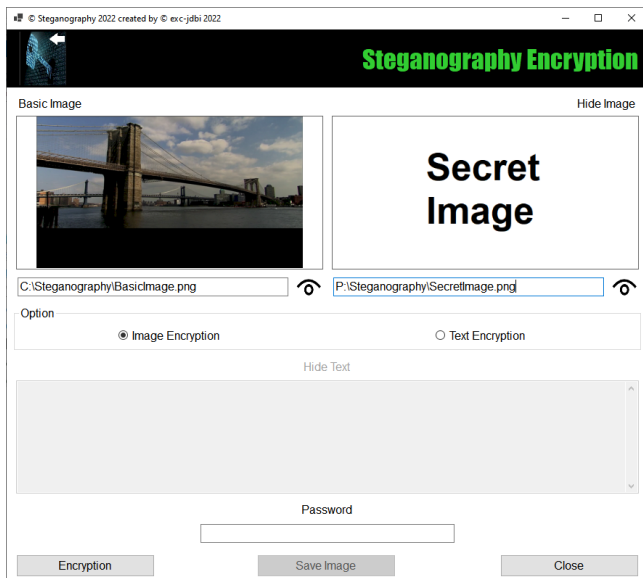


Abgesehen von den Funktionen der beiden leeren Masken sehen sie sehr ähnlich aus.

In der Mitte der Masken erkennt man unter Option die zwei RadioButton die kennzeichnen, ob ein Image oder ein Text verkryptet bzw. entkryptet werden soll. In der Encryption-Maske können die RadioButton ausgewählt werden. In der Decryption-Maske hingegen nicht, da das grundlegende Trägermedium (ImageCryption oder TextCryption) entscheidet, was denn nun genau extrahiert werden soll.

In beiden oben gezeigten Bilder ist das Trägermedium (BasicImage) noch nicht eingepflegt. Auch hier besteht die Möglichkeit von 'Drag and Drop'. Man kann das Bild aber auch über den Schalter  einfließen lassen.

Die Encryption-Maske



Hier erkennt man auf einen Blick beide Möglichkeiten der Verkryptung. Im linken Bild soll ein Bild (RadioButton Image Encryption) und im rechten Bild soll ein Text (RadioButton Text Encryption) in das Trägermedium eingebettet werden.

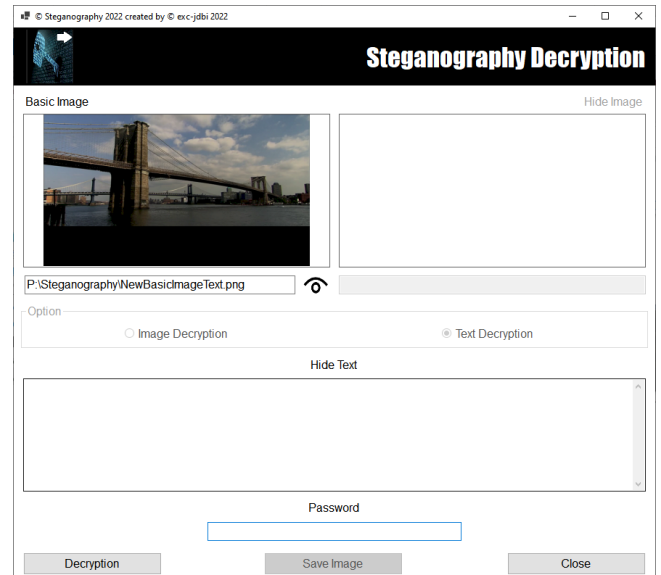
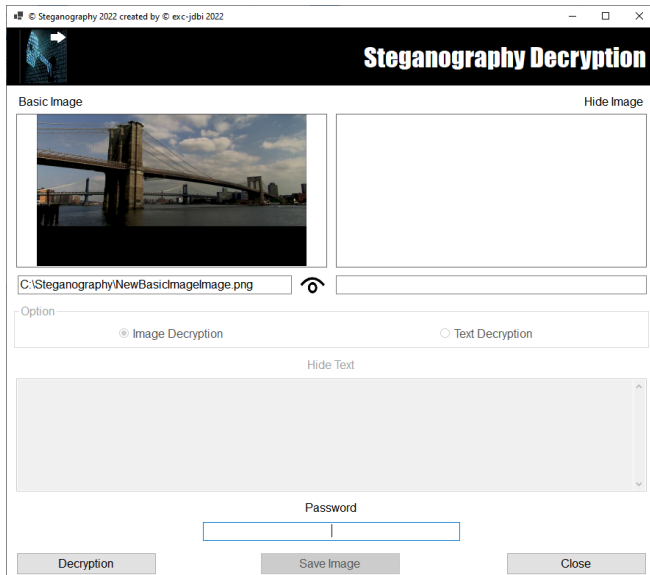
Die farbliche Schrift im Titelbereich oben zeigt hier, dass genug Speicherkapazität vorhanden ist. Die Farbe Grün kennzeichnet, dass die erforderliche Speicherkapazität im L1-Bereich ist, und dass nach der Verkryptung das neue 'BasicImage' scheinbar genau wieder so aussehen wird, wie das Originalbild.

In Wirklichkeit ist es natürlich nicht ganz so, denn das menschliche Auge erkennt die Verzerrung (durch Wahrnehmung) der Farben nicht. Es darf sogar gesagt werden, dass es auf dieser Welt wahrscheinlich kein Lebewesen gibt, die die Unterschiede zwischen Original und dem neuen BasicImage im L1-Bereich gesamthaft deutlich zu erkennen vermag.

Damit das Bild oder der Text verkryptet werden kann, ist ein 10-stelliges Passwort notwendig. Erst wenn alle Mussfelder ausgefüllt sind, wird nach Klick auf das Button 'Encryption' eine Verkryptung bzw. Einbettung in das Trägermedium eingeleitet.

Das neue 'BasicImage' kann mit dem Button 'Save Image' an einen gewünschten Speicherort abgespeichert werden. Wird das Bild nicht abgespeichert, steht es nachher auch nicht mehr zur Verfügung!

Die Decryption-Maske



Damit irgendwas in der Decryption-Maske gemacht werden kann, muss vorgängig das verkryptete 'BasicImage' geladen werden. Ist das entsprechende 'BasicImage' nicht verkryptet, so meldet sich © Steganography 2022 automatisch.

Im linken Bild erkennt man, dass die Decryption-Maske das 'BasicImage' als ImageCryption erkannt hat. Genauso auch im rechten Bild, hier hat die Maske TextCryption erkannt.

Damit das 'BasicImage' entkryptet werden kann, ist das entsprechende Passwort erforderlich. Auch hier gilt, erst wenn alle Mussfelder ausgefüllt sind, wird nach Klick auf das Button 'Decryption' eine Entkryptung bzw. Extraktion aus dem Trägermedium eingeleitet.

Sofern es sich um das ImageCryption handelt, kann das extrahierte Bild mit dem Button 'Save Image' irgendwo auf der Hardware neu abgespeichert werden. Text (TextCryption) kann hingegen nicht abgespeichert werden.

Das extrahierte Bild bzw. der extrahierte Text entspricht wieder genau dem, was ursprünglich in das Trägermedium eingebettet worden ist.

Startmaske

Die einfachste Vorgehensweise ist das Trägermedium (Basic Image) direkt mit der Maus auf die 'Drag and Drop' Oberfläche ziehen. Sofern das Trägermedium keine Informationen besitzt, wird die Encryption-Maske gestartet. Besitzt das Trägermedium erkennbare Informationen, so wird die Decryption-Maske gestartet.

Encryption-Button

In einem Trägermedium (BasicImage) sollen Informationen gespeichert werden. Das kann ein Text, oder ein Bild sein. Damit das funktioniert, darf das BasicImage keine entsprechend eingebettete Informationen besitzen.

Decryption-Button

Aus einem Trägermedium (BasicImage) sollen Informationen extrahiert werden. Das kann ein Text, oder ein Bild sein. Damit das funktioniert, muss das BasicImage erkennbare, eingebettete Informationen besitzen.

Encryption-Maske

- Unverkryptetes Trägermedium (BasicImage) laden, sofern es nicht schon geladen ist.
- RadioButton auswählen (ImageCryption bzw. TextCryption)
- Text das versteckt werden soll schreiben, bzw. Bild das versteckt werden soll laden.
- Passwort angeben (min. 10 Buchstaben)
- Sicherstellen, durch die farbliche Kennzeichnung, das genug Speicherplatz vorhanden ist.
- Encryption-Button drücken.
- Das neue Trägermedium (BasicImage) abspeichern.

Decryption-Maske

- Verkryptetes Trägermedium (BasicImage) laden, sofern es noch nicht geladen ist.
- Erkennung ImageDecryption bzw. TextDecryption sicherstellen
- Passwort angeben.
- Decryption-Button drücken.
- Sofern eine ImageDecryption gemacht worden ist, kann das extrahierte Bild abgespeichert werden. Extrahierter Text hingegen nicht.