Aufgabenstellung SN-Labor Versuch 2: Steganographie

Jedes zu versteckende Dokument soll in einer Trägerdatei mit einem Passwort versteckt werden und per Email an eine Nachbargruppe gesendet werden.

Versuche mit Bildern als Träger

1. Erstellen Sie eine Textdatei und verstecken diese in einem Bild
2. Das Originalbild mit der Trägerdatei mit Hilfe von Paint Shop pro vergleichen. Dazusteht im Menü Image der Punkt Arithmetik zur Verfügung.
3. Erklären Sie, weshalb genau diese Einstellungen (aus Punkt 2) verwendet werden müssen.
4. Drucken Sie die Trägerdatei (Bild) aus und scannen Sie sie anschließend ein. Extrahieren Sie die versteckte Datei aus dem gescannten Bild. Ist dies möglich? Begründung?
5. Das Ergebnis von Aufgabe 2 auf ein weiteres Bild aufaddieren. Aus diesem Bild nun die Textdatei extrahieren.
6. Führen Sie die Punkte 1-2 mit verschiedenen Bildern durch (hell, dunkel, Portrait, Landschaft etc.). Wo werden die Daten versteckt?
7. Ein Trägerbild, welches versteckte Daten enthält, in verschiedene Formate konvertieren. Nach anschließender Rückkonvertierung die Daten wieder extrahieren. Bei welchen Formaten gelingt dies nicht? Warum?
8. Erstellen Sie eine Textdatei und verstecken sie diese in einem Bild. Nochmals eine Textdatei erstellen und diese in das gleiche Bild verstecken. Nun die erste Textdatei wieder extrahieren.

Versuche mit Klangdateien als Träger

9. Erstellen einer Textdatei und verstecken in einer WAV-Datei

Versuche mit Textdateien als Träger

10. Erstellen Sie eine Textdatei und verstecken sie in einer HTML-Datei (aus dem Internet). Diese Funktion ist nur mit Steganos 2 möglich! Wie werden die Daten in einer HTML-Datei versteckt?

Weitere Funktionen von Steganos nutzen

11. Kopieren Sie Dateien in den Safe. Schließen Sie ihn und öffnen die Safe-Datei im Steganos-Explorer.
12. Probieren Sie den Portablen Safe aus. Kopieren Sie Dateien hinein und öffnen diese am Nachbarrechner (Diskette).
13. Löschen Sie eine Datei von Diskette mit dem Windows Explorer. Vernichten Sie nun eine weitere Datei von Diskette mit dem Schredder. Benutzen Sie das Tool PCI Filerecorvery um die Daten zu retten. Was passiert? Welche Art des Schredderns würden Sie privat bevorzugen und warum?
14. Verschlüsseln Sie eine Email und senden diese an eine Nachbargruppe. Versuchen Sie, die verschlüsselte Email ohne Passwort zu öffnen. Öffnen Sie sie anschließend mit dem Passwort.
15. Nutzen Sie den Internet-Spurenvernichter und überprüfen Sie, was er alles löscht.
16. Diskutieren Sie die Vor- und Nachteile der Steganos Security Suite 6.
17. Testen Sie den Passwort-Manager. Beschreiben Sie wie er benutzt wird und wofür er von Vorteil ist.

Versuche mit anderen steganographischen Programmen

18. Erstellen Sie mit Paint Shop pro ein Wasserzeichen. Vergleichen Sie auch hier, wie in Punkt 2 das Originalbild mit dem veränderten Bild.
19. Versuchen Sie, ohne das Bild erheblich zu verschlechtern, das Wasserzeichen zu zerstören. Welche Möglichkeiten dafür gibt es?
20. Tun Sie das gleiche mit dem Programm „BS2“.
21. Verstecken einer Textdatei in einem Bild mit JPEG HIDE (auf \\Server01\SI-Software). Anschließend auch hier wieder die Veränderungen wie in Punkt 2 sichtbar machen. Gibt es Unterschiede zu Steganos?
22. Welche Auswirkungen könnte ein Kryptographieverbot haben?

Versuche mit Bildern als Träger

1. Erstellen Sie eine Textdatei und verstecken diese in einem Bild

Um eine Textdatei in einem Bild zu speichern, war zuerst die Installation von Steganos Security Suite 6 notwendig (siehe Abbildung 1). Nach der Installation haben wir eine .txt Datei mit dem Editor erstellt und in einem Beispiel Bild von Windows (.bmp) versteckt.

Abbildung 1 – Steganos Security Suite 6 - Zentrale

Will man nun die Datei in einem Bild verstecken, klicken wir auf den „Steganos Datei-Manager“ (siehe Abbildung 1). Im Datei-Manager (siehe Abbildung 2) fügen wir die gewünschte zu versteckende Datei hinzu (hier: „geheim.txt“).

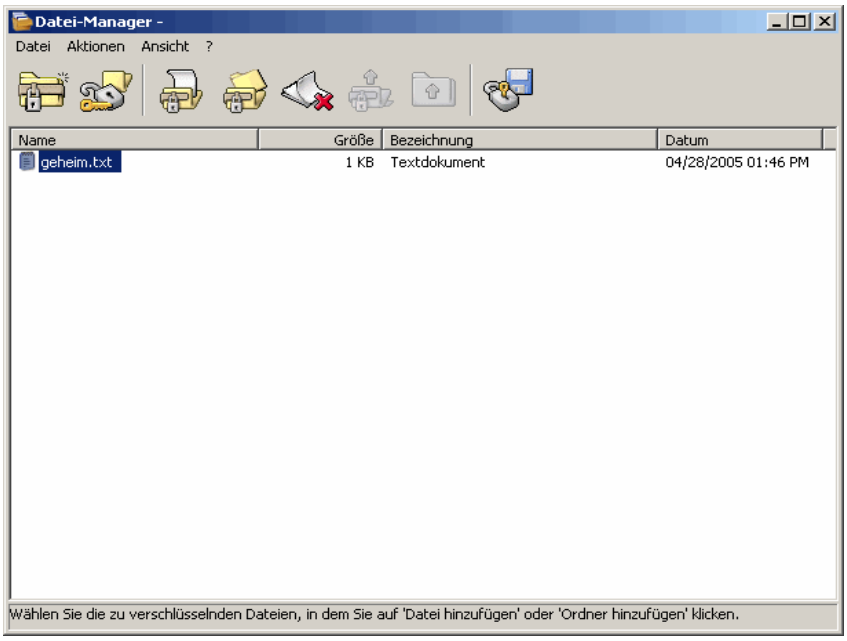


Abbildung 2 – Datei-Manager mit Datei „geheim.txt“

Nach einem Klick auf den Button rechts oben (siehe Abbildung 2), werden wir gefragt ob die Datei nun „verschlüsseln“ oder „verstecken“ wollen. Wir klicken auf „Verstecken…“ und wählen das von Windows mitgelieferte Bild „BlaueBerge.bmp“ aus. Nach der Auswahl der Trägerdatei, werden wir nach einem Passwort gefragt, mit dem die Informationen in der Trägerdatei gespeichert werden. Wir wählten hier das Passwort „2se0cu0ne5t“, was laut Steganos nicht von PC-Spezialisten geknackt werden kann.

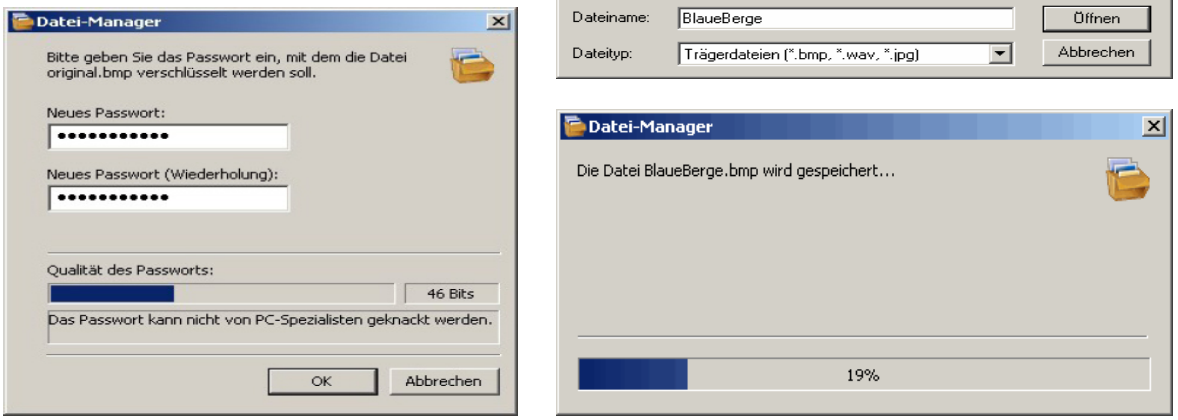


Abbildung 3 – Datei in .bmp verstecken.

Anschließend wird uns noch empfohlen, die original Dateien mit dem Schredder zu vernicht (siehe Abbildung 4). So wird sichergestellt, dass 3. Personen die geheime Nachricht nicht finden können, bzw. sie überhaupt nicht bemerken.

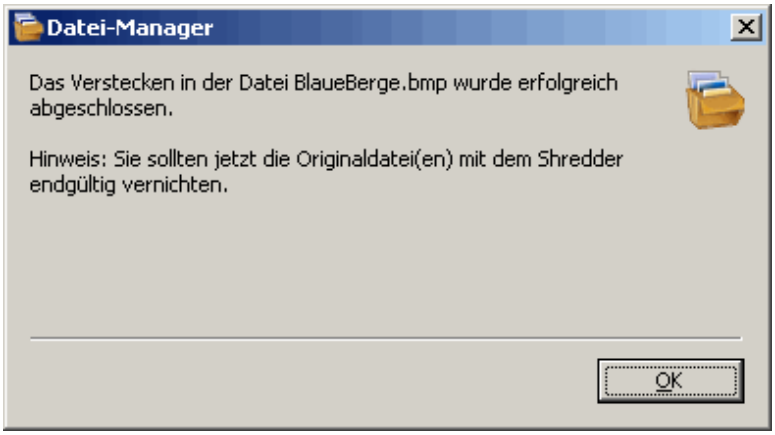


Abbildung 4 – Original Dateien mit dem Schredder vernichten.

2. Das Originalbild mit der Trägerdatei mit Hilfe von Paint Shop pro vergleichen. Dazu steht im Menü Image der Punkt Arithmetik zur Verfügung.
Um das Bild mit den „versteckten“ Informationen, mit dem originalen Bild zu vergleichen, öffnen wir das Bildbearbeitungsprogramm „Paint Shop Pro“.
Wir klicken im Menü auf „Bild “ und wählen dort den Punkt „Bildberechnung“ aus, um die beiden Bilder zu vergleichen (siehe Abbildung 5).

Abbildung 5 – Registerkarte „Bildberechnung“.

Das Bild ist größtenteils schwarz mit einigen roten Punkten im unteren Bereich des Bildes (siehe Abbildung 6).

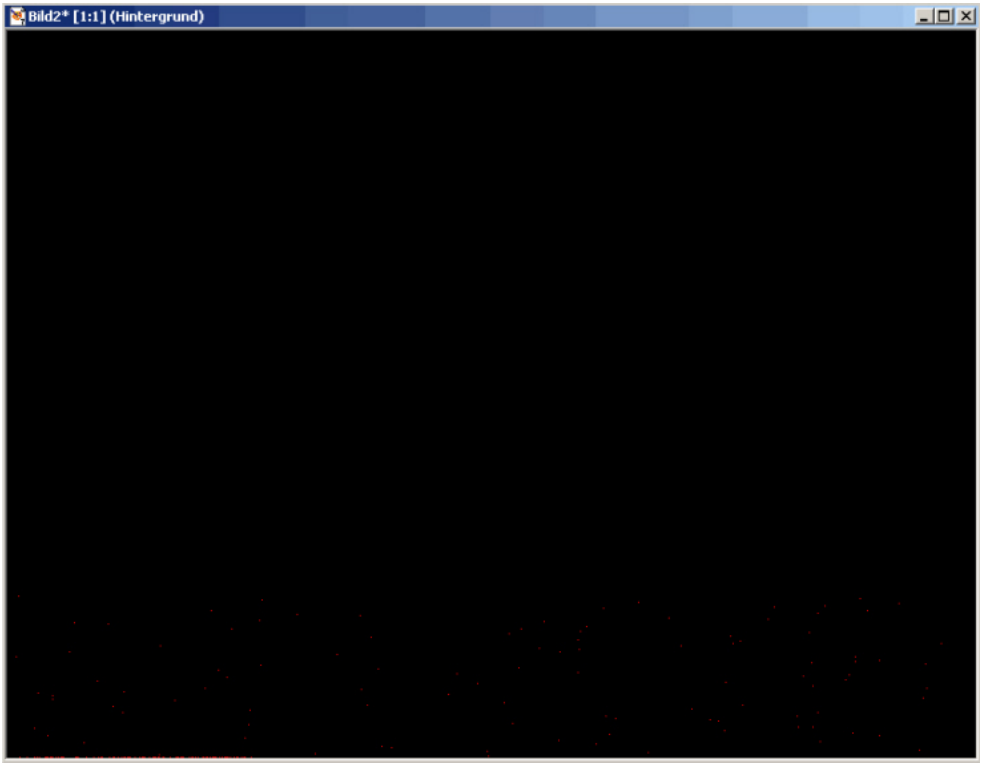


Abbildung 6 – Ergebnis Subtraktion

3. Erklären Sie, weshalb genau diese Einstellungen (aus Punkt 2) verwendet werden müssen.
Die zu versteckenden Informationen werden mit Hilfe von Farbmanipulationen im Bild gespeichert. Im Bild wird der dezimale Wert jedes Pixels um eins erhöht. Das „manipulierte Bild“ sieht für das menschliche Auge noch genauso aus, wenn man es mit dem Originalbild vergleicht.
Vergleicht man nun das Originalbild und das Trägerbild direkt miteinander, dann müsste man zumindest auf dem PC minimale Unterschiede erkennen.
Durch den Punkt „Subtraktion“ werden die Farbwerte aller Bildpunkte voneinander abgezogen. An Bildpunkten wo keine Information versteckt wurde, ist der Farbwert 0 (schwarz). An Bildpunkten wo Information versteckt wurde, ist der Farbwert ungleich 0 (rot) (siehe Abbildung 6).

4. Drucken Sie die Trägerdatei (Bild) aus und scannen Sie sie anschließend ein. Extrahieren Sie die versteckte Datei aus dem gescannten Bild. Ist dies möglich? Begründung?
Wie in der Aufgabenstellung beschrieben, haben wir das Bild ausgedruckt und anschließend eingescannt. Anschließend versuchten wir das Bild mit dem „Steganos Datei-Manger“ zu öffnen (siehe Abbildung 7).

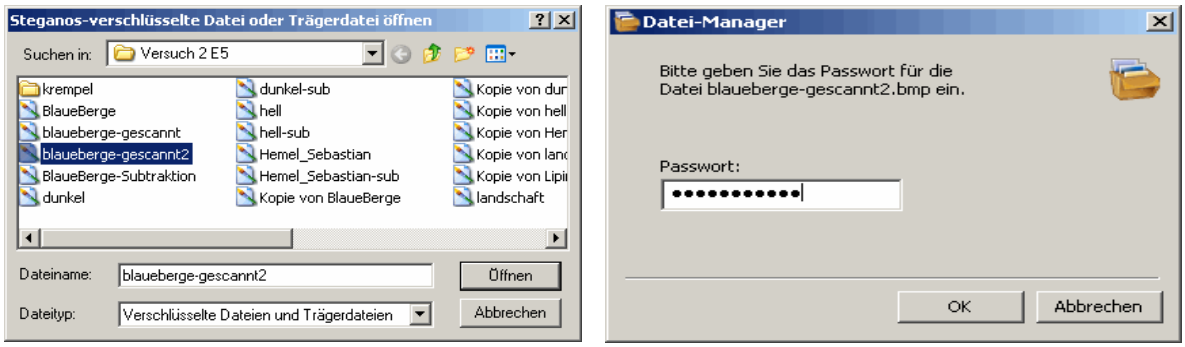


Abbildung 7 – Gescanntes Bild öffnen

Allerdings war jeder Versuch erfolglos, das Bild zu öffnen und die versteckten Informationen wieder auszulesen (siehe Abbildung 8).

Dies kann folgende Gründe haben:
Drucker und Scanner sind nicht genau kalibriert, so dass die Information im Bild einen Druck- und anschließenden Scanvorgang nicht übersteht.
Dies war gerade in unserem Bild sehr schwierig, da unser verwendetes Bild eine sehr große Farbtiefe aufwies.

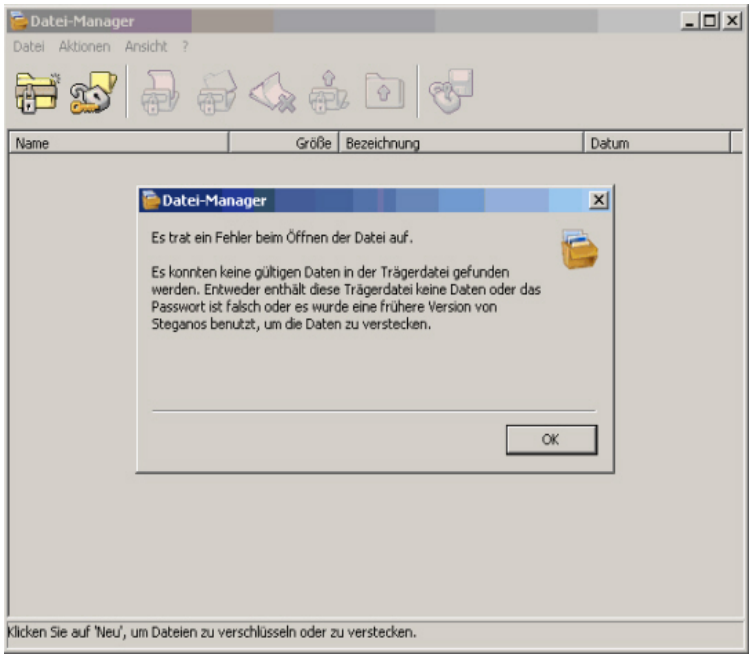


Abbildung 8 – Gescanntes Bild öffnen - Fehlermeldung

5. Das Ergebnis von Aufgabe 2 auf ein weiteres Bild aufaddieren. Aus diesem Bild nun die Textdatei extrahieren.

Nach einer ähnlichen Vorgehensweise wie in Aufgabe 2 gehen wir bei der Aufaddierung auf ein anderes Bild vor. Allerdings wählen wir unter „Bild“ > „Bildberechnung“ statt „Subtraktion“ „Addition“ aus (siehe Abbildung 9).

Danach versuchen wir das Ergebnis der Aufaddierung auf ein anderes Bild wieder in Steganos auszulesen, um an die geheimen Daten zu kommen (siehe Abbildung 10).

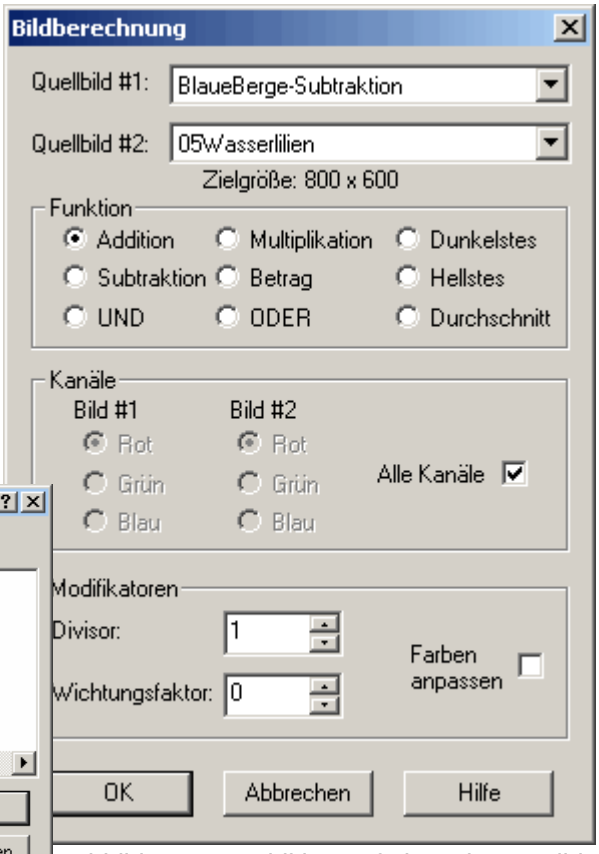


Abbildung 9 – Addition auf ein weiteres Bild

Abbildung 10 – Bild der Addition öffnen

Abbildung 11 – Eingabe des Passworts für die Additions-Datei

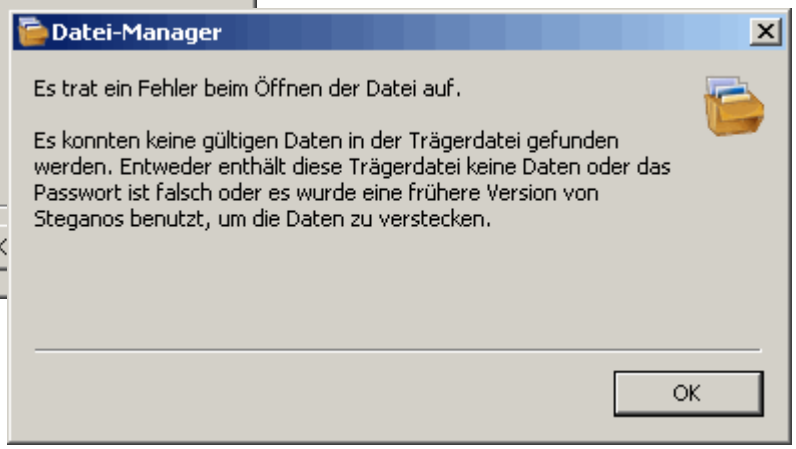


Abbildung 12 – Fehler beim Öffnen der Additions-Datei

Nach der Passwortabfrage gibt es allerdings kein Weiterkommen. Die Wiederherstellung der geheimen Informationen bleibt erfolglos (siehe Abbildung 12).

6. Führen Sie die Punkte 1-2 mit verschiedenen Bildern durch (hell, dunkel, Portrait, Landschaft etc.). Wo werden die Daten versteckt?

Abbildung 13 – Verschiedene Trägerbilder zum Verstecken der Informationen (Landschaft, dunkel, hell)

Die Bearbeitung der Bilder erfolgte nach den Anweisungen aus den Aufgaben 1 und 2 mit oben gezeigten Bildern. Das Ergebnis glich dabei bei allen Bildern sehr stark dem Ergebnis aus Aufgabe 2. Die Informationen waren ebenfalls gleichmäßig im unteren Teil des jeweiligen Bildes versteckt.

7. Ein Trägerbild, welches versteckte Daten enthält, in verschiedene Formate konvertieren. Nach anschließender Rückkonvertierung die Daten wieder extrahieren. Bei welchen Formaten gelingt dies nicht? Warum?

Zum Konvertieren unseres Originalbildes mit den enthaltenen Informationen aus Aufgabe 1 in die Dateiformate JPEG, GIF, TIFF und PNG benutzten wir PaintShop

Pro. Nach der Rückkonvertierung versuchten wir die Datei wieder mit Steganos zu öffnen. Dabei traten unterschiedliche Ergebnisse auf.

So gelang es uns bei dem in JPEG und dem in GIF konvertierten Bild nicht, die versteckten Informationen mit Steganos wieder zu extrahieren. Steganos zeigte uns dieselbe Fehlermeldung wie bei Abbildung 12.

Dies liegt vor allem daran, dass bei diesen Komprimierungsverfahren direkt auf die Farbwerte Einfluss genommen wird. Es sind sogenannte verlustbehaftete Kompressionsverfahren. Bei der JPEG Kompression werden nach Blockbildung im Laufe des Vorgangs diese quantisiert, das heisst, die Farbwerte werden auf- oder abgerundet und somit leicht verfälscht. Dadurch kann es zum Verlust der enthaltenen Informationen kommen. Bei der GIF Kompression wird nach unterchiedlichen Verfahren die Anzahl der Farben im Bild auf maximal 256 (8Byte) Farben reduziert. Da unser Bild aber vor der Kompression über 16Millionen (24Byte) Farben enthielt, gingen die enthaltenen Informationen durch die drastische Reduzierung verloren.

8. Erstellen Sie eine Textdatei und verstecken sie diese in einem Bild. Nochmals eine Textdatei erstellen und diese in das gleiche Bild verstecken. Nun die erste Textdatei wieder extrahieren.

Nach dem bekannten Verfahren aus Aufgabe 1 haben wir zunächst eine Textdatei im Bild versteckt. Daraufhin haben wir ebenfalls nach Aufgabe 1 eine zweite, zur Kenntlichmachung anderslautende, Textdatei in dieselbe Bild-Datei versteckt.
Es war uns jedoch unmöglich nach dem Verstecken der zweiten Textdatei noch die erste Textdatei aus dem Bild zu extrahieren. Die zweite dagegen konnte mühelos ausgelesen werden, die erste war verloren.
Beim Verstecken der zweiten Datei wurde offenbar die Information im Bild und somit der Inhalt der ersten Datei überschrieben.

9. Erstellen einer Textdatei und verstecken in einer WAV-Datei

Das Verstecken einer Textdatei funktioniert so ähnlich wie mit der .bmp Datei. Der einzige Unterschied ist, dass eine andere Trägerdatei ausgewählt wird (siehe Abbildung 14).

Nach dem Verstecken hörten sich beide Dateien gleich an. Auch die Dateigröße blieb gleich.

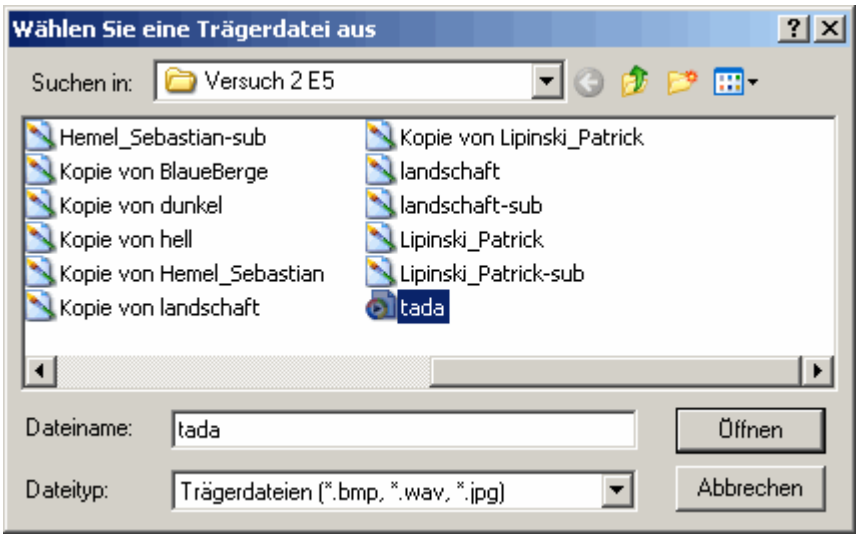


Abbildung 14 – Informationen in .wav Datei verstecken

10. Erstellen Sie eine Textdatei und verstecken sie in einer HTML-Datei (aus dem Internet). Diese Funktion ist nur mit Steganos 2 möglich! Wie werden die Daten in einer HTML-Datei versteckt?

Da diese Funktion nur mit Steganos 2 möglich ist, mussten wir erst dieses installieren. Als Trägerdatei wählten wir die Seite der FH-Friedberg.
HTML Dateien nehmen die zu versteckenden Informationen nicht durch Bits auf, wie bei Bild Dateien. Dies würde dazu führen das eine Nachricht nicht mehr versteckt wäre sondern für jeden offensichtlich, dass die Datei versteckte Informationen enthält.
Informationen in einer Textdatei werden über zusätzliche Leerzeichen siehe Abbildung 15a), Tabulatoren am Zeilenende, Wortsynonyme und Umbrüche gespeichert. Dies kann sehr eindeutig an der Größe der Datei erkennen (siehe Abbildung 15b).

Name	Größe	Typ
aufgabe10.html	13 KB	HTML Document
html_änderungen.doc	49 KB	Microsoft Word-Dok...
html_original.doc	46 KB	Microsoft Word-Dok...
html_versteckt.doc	48 KB	Microsoft Word-Dok...
Kopie von aufgabe10.html	12 KB	HTML Document

Abbildung 15a – Unterschiedliche Größe der HTML-Dateien

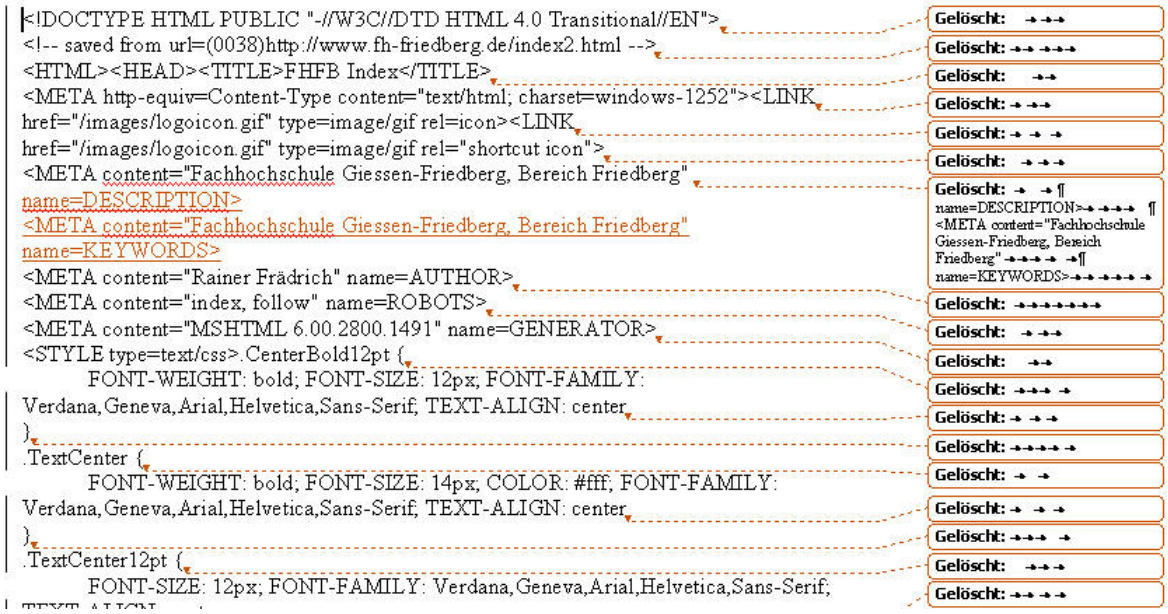


Abbildung 15b – Vergleich beider HTML-Dateien mit Word

11. Kopieren Sie Dateien in den Safe. Schließen Sie ihn und öffnen die Safe-Datei im Steganos-Explorer.

Der Safe funktioniert wie eine Festplatte am Rechner (siehe Abbildung 16). Steganos legt ein neues Laufwerk (z.B. G:) an. Mit dem Steganos-Explorer kopiert man die gewünschten Dateien einfach in das neue Laufwerk.
Anschließend werden alle Dateien in einer Datei gespeichert, welche mit einem Passwort versehen wird.

Abbildung 16 – Steganos Safe

Nach Eingabe des zuvor festgelegten Passwort, lassen sich die Dateien im Steganos-Explorer wieder öffnen (siehe Abbildung 17).

Abbildung 17 – Steganos-Explorer Passwort Eingabe

12. Probieren Sie den Portablen Safe aus. Kopieren Sie Dateien hinein und öffnen diese am Nachbarrechner (Diskette).
Mit dem Portablen Safe hat man die Möglichkeit, Daten zu verschlüsseln und sie an einem anderen Rechner zu öffnen. So können verschlüsselte Laufwerke auf jedem PC ohne Zusatzsoftware entschlüsselt werden - Passwort genügt.
Man erstellt einfach einen "tragbaren Datensafe", indem man aus den gewünschten Daten eine verschlüsselte Datei anlegt und diese auf eine CD oder eine Speicherkarte kopiert. Die Software zur Entschlüsselung des Datenträgers ist bereits im Steganos Portable Safe enthalten (siehe Abbildung 18).

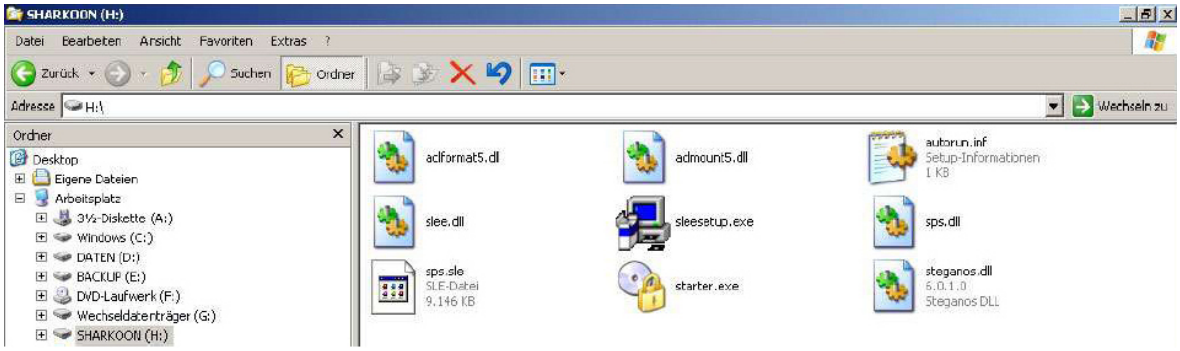


Abbildung 18 – Steganos Portable Safe

13. Löschen Sie eine Datei von Diskette mit dem Windows Explorer. Vernichten Sie nun eine weitere Datei von Diskette mit dem Schredder. Benutzen Sie das Tool PCI Filerecorvery um die Daten zu retten. Was passiert? Welche Art des Schredderns würden Sie privat bevorzugen und warum?

Wir kopieren 4 Dateien auf den USB-Stick. Anschließend wird eine Datei mit dem Windows-Explorer (image28.jpg) und eine Datei mit dem Steganos-Shredder (image29.jpg) gelöscht (siehe Abbildung 19 und 20).

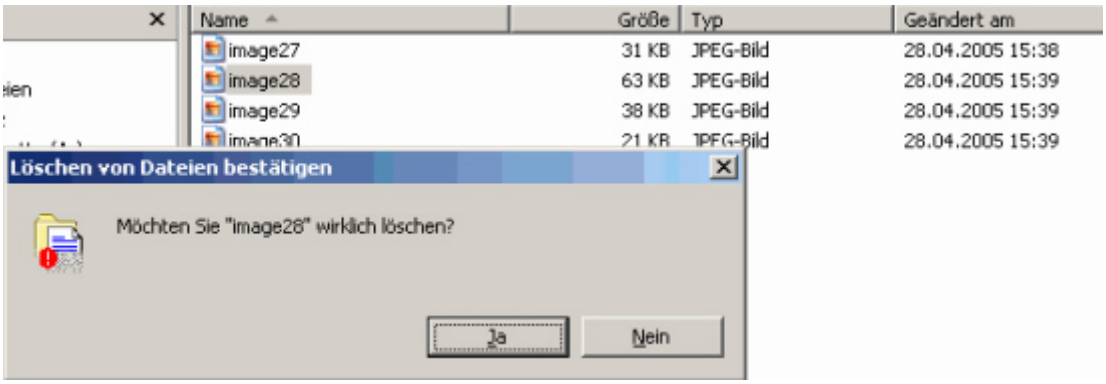


Abbildung 19 – Datei löschen mit Windows-Explorer

Abbildung 20 – Datei löschen mit Steganos-Shredder

Bei dem Versuch die Dateien mit dem Tool PCI Filerecorvery (siehe Abbildung 21) wiederherzustellen, konnten wir nur die Datei (image28.jpg) wiederherstellen, welche mit dem Windows-Explorer gelöscht wurde. Die Datei (image29.jpg), welche mit dem Steganos-Shredder gelöscht wurde, konnte nicht wiederhergestellt werden (siehe Abbildung 22). Der Shredder löscht somit Dateien unwiderruflich.

Abbildung 21 – PCI Filerecovery

Name	Größe	Typ	Geändert am
image27	31 KB	JPEG-Bild	28.04.2005 15:38
image30	21 KB	JPEG-Bild	28.04.2005 15:39
_MAGE28	63 KB	JPEG-Bild	28.04.2005 17:39
_MAGE29	0 KB	JPEG-Bild	28.04.2005 17:41

Abbildung 22 – Wiederhergestellte Dateien

Bei den alltäglichen Arbeiten am Rechner reicht in der Regel das Löschen mit dem Windows-Explorer. Daten die von der Sicherheitsstufe niedrig anzusetzen sind, müssen nicht vor einer Wiederherstellung geschützt werden. Auch besteht hierbei weiterhin die Möglichkeit, versehentlich gelöschte Dateien wiederherstellen zu können. Bei Daten die von der Sicherheitsstufe hoch anzusetzen sind (z.B.

Passwörter, Bankdaten), empfiehlt sich die Benutzung des Shredders. So ist eine Wiederherstellung der Dateien durch Dritte nicht mehr möglich.

14. Verschlüsseln Sie eine Email und senden diese an eine Nachbargruppe. Versuchen Sie, die verschlüsselte Email ohne Passwort zu öffnen. Öffnen Sie sie anschließend mit dem Passwort.

Zuvor müssten die Rechner für den E-Mail Versand eingerichtet werden.
Um die E-Mail verschlüsseln zu können, benutzen wir das Programm „Steganos E-Mail-Verschlüsselung“ (siehe Abbildung 23).
Der zu verschlüsselnde Text wird einfach in das Textfeld (siehe unten) eingegeben. Nach einem Klick auf „Verschlüsselt senden…“, wird die Nachricht verschlüsselt und das eingerichtete E-Mail Programm öffnet sich mit dem verschlüsselten Dateianhang (siehe Abbildung 24).

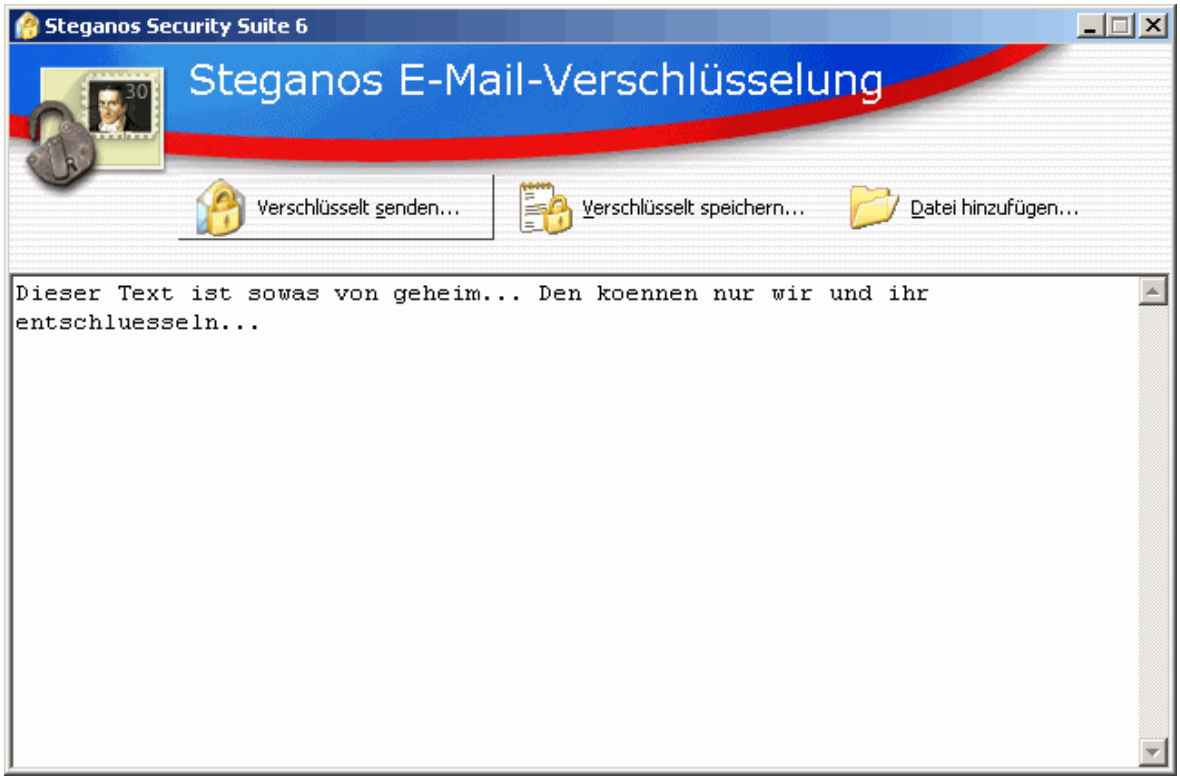


Abbildung 23 – Steganos E-Mail-Verschlüsselung

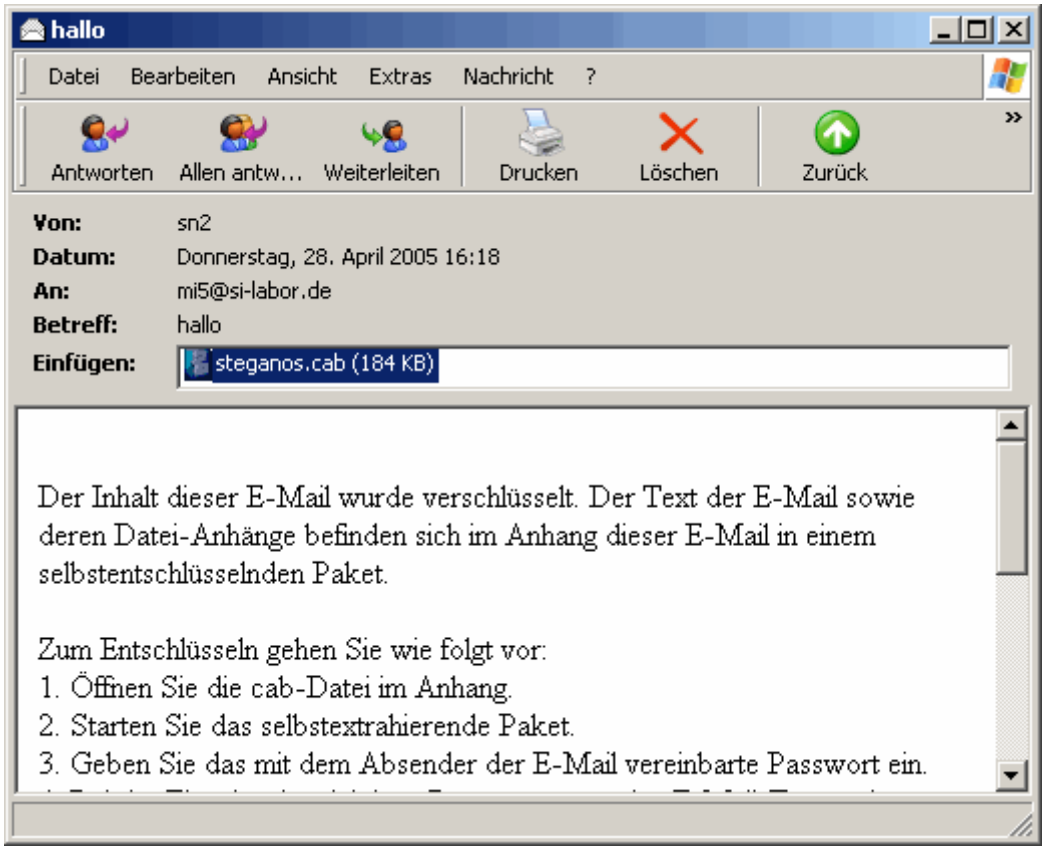


Abbildung 24 – E-Mail mit Dateianhang

Die verschlüsselte E-Mail wird auf dem Nachbarrechner mit einem Doppelklick auf die Datei (steganos.cab) geöffnet. Nach einem weiteren Doppelklick auf das selbstextrahierende Paket (steganos.exe) wird nur noch das vereinbarte Passwort eingegeben und die E-Mail wird wieder entschlüsselt (siehe Abbildung 25 und 26).

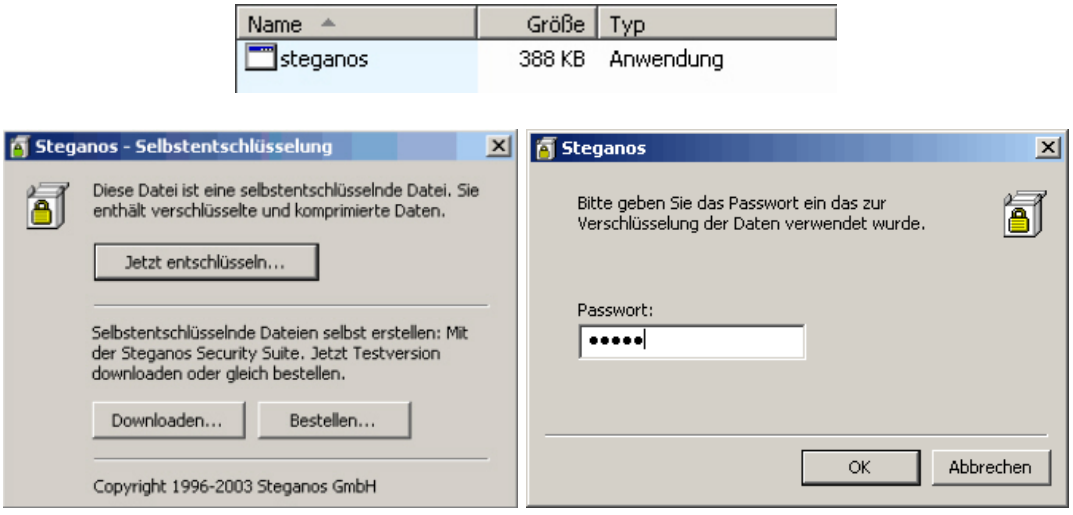


Abbildung 25 – Selbstextrahierendes Paket

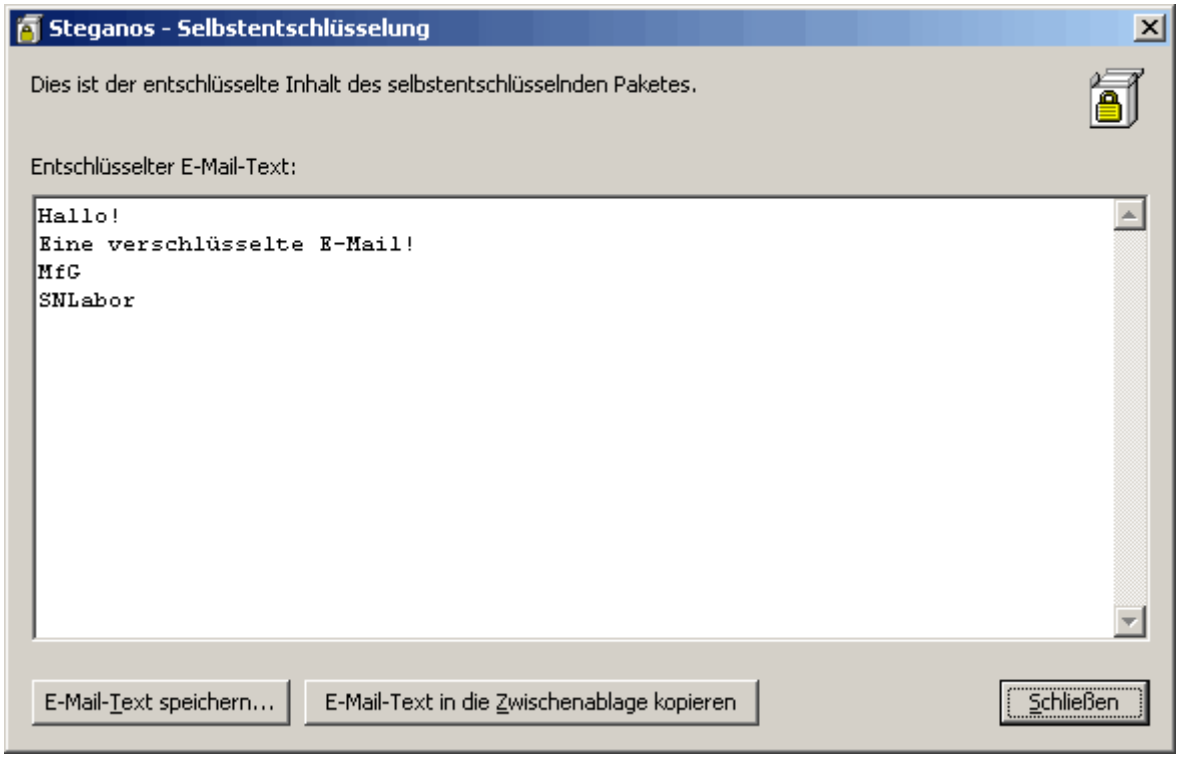
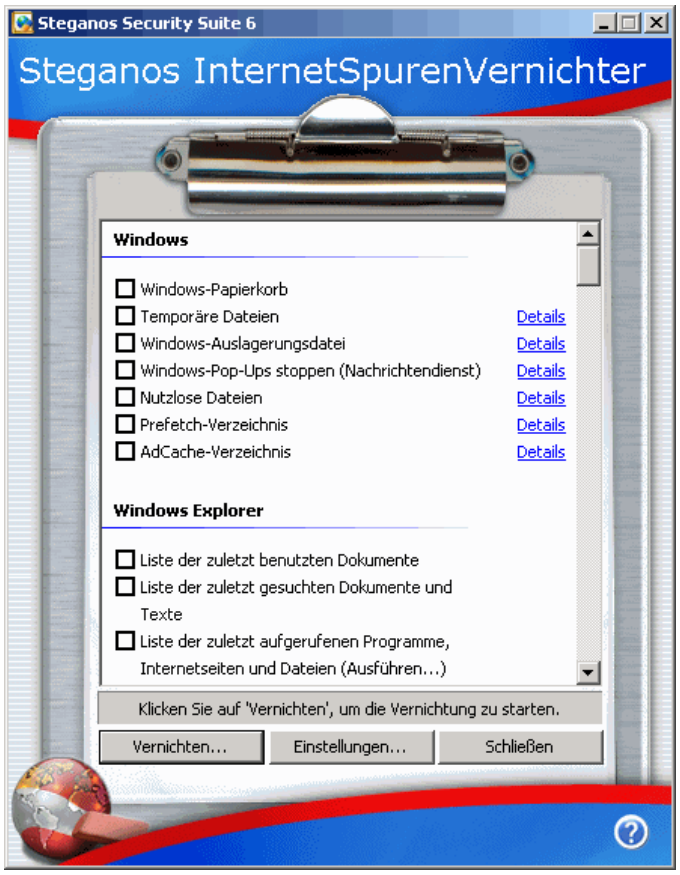


Abbildung 26 – Entschlüsselte E-Mail

15. Nutzen Sie den Internet-Spurenvernichter und überprüfen Sie, was er alles löscht.



Mit dem Internet-Spurenvernichter (siehe Abbildung 27) von Steganos ist es möglich, sämtliche Spuren lokal auf dem Rechner zu löschen, die ein das Internet nutzendes Programm hinterlässt. Hierbei werden unter anderem von den Programmen protokollierte Daten über den Aufenthalt im Internet, die angeforderten Daten und gespeicherten Nutzungsinformationen, wie zum Beispiel die „History“, der Cache oder die Cookies im Browser, gelöscht. Aber auch bei Programmen wie Word löscht der Internet-Spurenvernichter zum Beispiel die Liste der zuletzt geöffneten Dateien.

Abbildung 27 – Auswahlmenü SpurenVernichter

16. Diskutieren Sie die Vor- und Nachteile der Steganos Security Suite 6.
Die Steganos Security Suite ist ein Komplettpaket, um mit relativ einfachen Mitteln, eMail-Nachrichten zu verschlüsseln, Daten versteckt zu sichern und auch zu versenden und somit einige Datenschutzaspekte sehr einfach zu realisieren.

Vorteil der Suite ist, dass man viele unterschiedliche Sicherheitseinrichtungen für den täglichen Gebrauch in einem leicht zu bedienenden Programm vereint hat. Allerdings gibt es beispielsweise bei der Versteckfunktion über den Steganos Dateimanager den Nachteil, dass die zu versteckenden Daten nur wenig verteilt im unteren Bereich der Bilder (Trägerdateien) versteckt werden und somit leichter erkennbar sind.

17. Testen Sie den Passwort-Manager. Beschreiben Sie wie er benutzt wird und wofür er von Vorteil ist.

Abbildung 28 – Einrichten des Masterpassworts

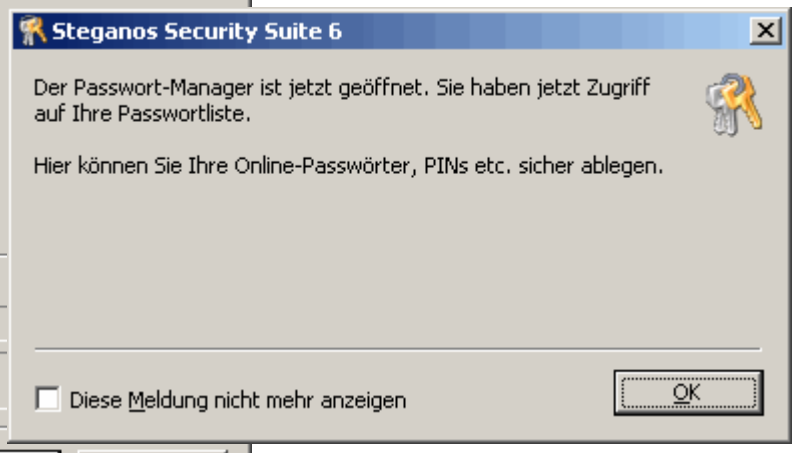


Abbildung 29 – PasswortManager

Mit Hilfe des Passwort-Managers (siehe Abbildung 30) ist es möglich, seine diversen Passwörter für z.B. Webmail, Internetforen, PINs in einer Datenbank und somit mit nur einem zu merkenden Passwort abzusichern. Dafür gibt man zunächst seine Daten und Passwörter ein. Es ist unter anderem möglich Kommentare zu den Daten einzugeben, um eine Art beschreibenden Schlüsselanhänger zu haben (siehe Abbildung 31). Das Programm speichert die gesamten Daten und verschlüsselt den Zugang dazu mit einem vom Benutzer angegebenen Passwort.
Somit ist es möglich mit nur einem Masterpasswort (siehe Abbildung 28), welches man dementsprechend sicher auswählen kann, seine gesamten eingegebenen Passwörter einzusehen und zu schützen. Dies bietet natürlich dem Nutzer die Möglichkeit mehr als nur komfortabel zu merkende 1 – 3 Standardpasswörter zu nutzen.

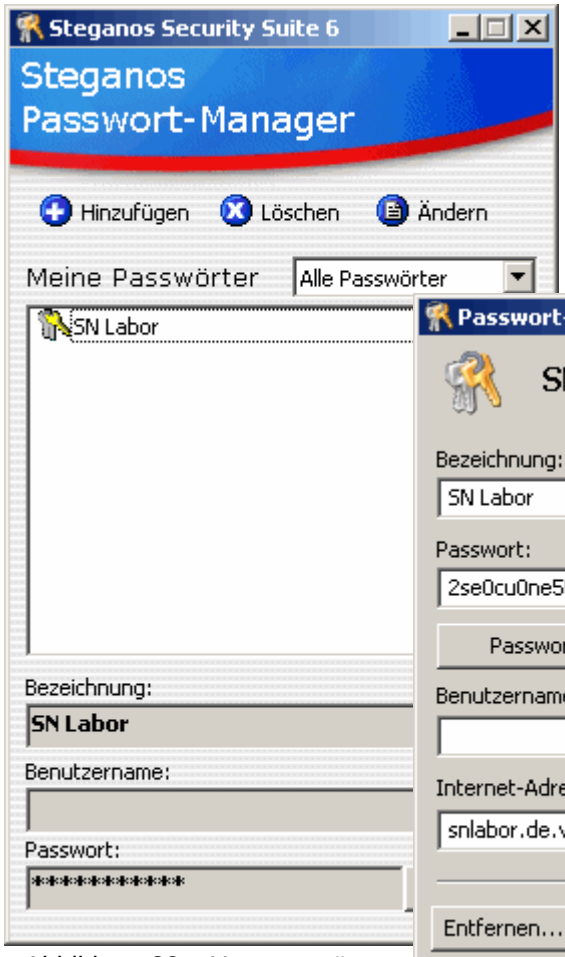


Abbildung 30 – Hauptmenü

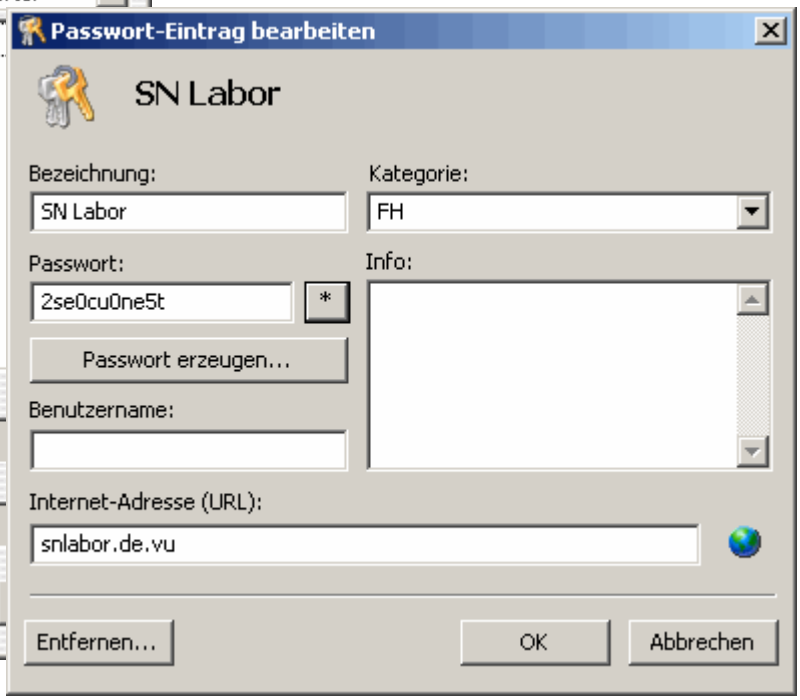


Abbildung 31 – Einzelne Passwörter bearbeiten

Versuche mit anderen steganographischen Programmen

18. Erstellen Sie mit Paint Shop pro ein Wasserzeichen. Vergleichen Sie auch hier, wie in Punkt 2 das Originalbild mit dem veränderten Bild.
Über den Befehl „Bild“ > „Wasserzeichen“ > „Wasserzeichen einfügen“ in PaintShop Pro ist es mit wenigen Klicks möglich, eine Bild-Datei mit einem unsichtbaren Wasserzeichen zu versehen. Für unseren Versuch benutzten wir die Standardeinstellungen des Programms ohne jegliche Anpassung der „Urheber-ID“. Somit wurde eine Nachricht mit dem Inhalt „Jasc Wasserzeichen Demo“ im Bild versteckt.
Nach Ausführen der Subtraktion nach Aufgabe 2, um die veränderte Information sichtbar zu machen, fällt auf, dass sich das Wasserzeichen stark an den Bildinhalt anpasst, da die Konturen des Originalbildes noch deutlich sichtbar waren.

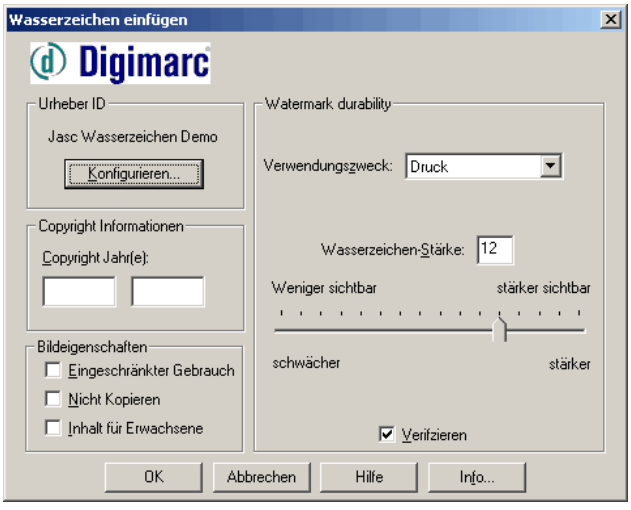


Abbildung 32a – Optionen bearbeiten

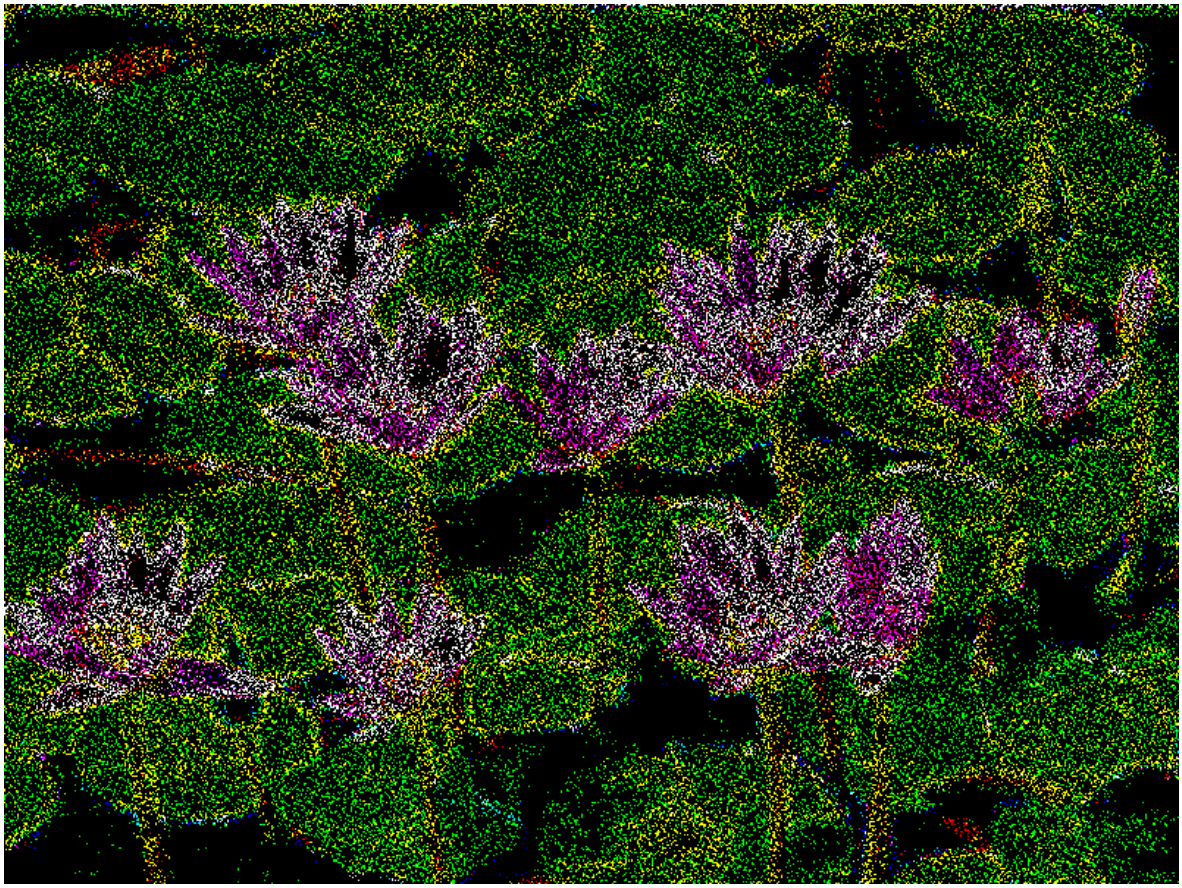


Abbildung 32b – Ergebnis der Subtraktion

19. Versuchen Sie, ohne das Bild erheblich zu verschlechtern, das Wasserzeichen zu zerstören. Welche Möglichkeiten gibt es dafür?

Das unsichtbare Wasserzeichen lässt sich nur durch das Verändern der Farbinformationen, in welchen die Informationen versteckt werden, zerstören. Dazu reicht schon ein einfaches leichtes Weichzeichnen des Bildes. Die Schärfe des Bildes wird dadurch nur leicht verringert und es sind somit kaum Unterschiede zum Original erkennbar.

Abbildung 32c – Fehlermeldung

20. Tun Sie das gleiche mit dem Programm „BS2“.

Im Gegensatz zum versteckten Wasserzeichen aus PaintShop Pro schreibt das Programm „BildSchutz 2“ ein sichtbares Wasserzeichen in die Datei. Dies kann z.B. ein eingegebener Text oder ein ausgewähltes Bild sein. Es ist möglich, den Ausgabeort und die Erscheinung des eingebundenen Elements zu beeinflussen.

Abbildung 34 – Wasserzeichen im Bild

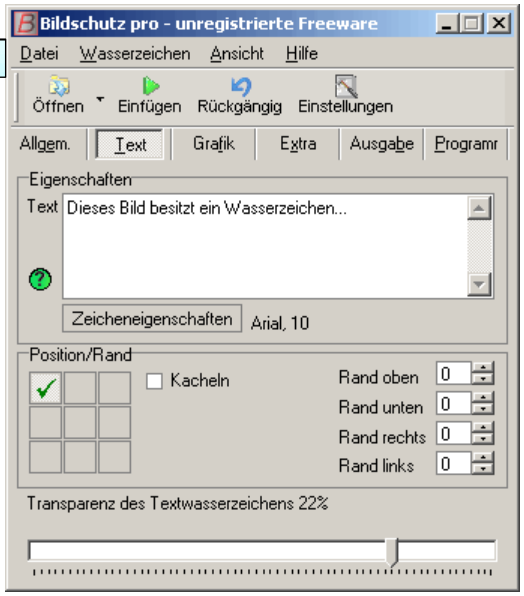


Abbildung 33 – Einstellungsoptionen

21. Verstecken einer Textdatei in einem Bild mit JPEG HIDE (auf \\Server01\SI-Software). Anschließend auch hier wieder die Veränderungen wie in Punkt 2 sichtbar machen. Gibt es Unterschiede zu Steganos?

Das Vorgehen des Versteckens ist gleich dem aus Steganos bekannten. Es wird zunächst eine Trägerdatei ausgewählt (diesmal explizit ein durch JPEG komprimiertes Bild) und danach die zu versteckende Datei.
JPEG Hide versteckt die Informationen im Gegensatz zu Steganos jedoch verteilt über das ganze Bild in den vom JPEG-Verfahren her bekannten Blöcken.
Zum Vergleich siehe Abbildung 6 (Steganos) und Abbildung 35 (JPEG Hide).

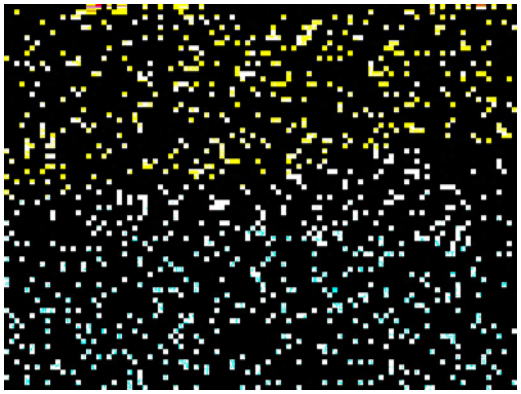


Abbildung 35 – Ergebnis Subtraktion

22. Welche Auswirkungen könnte ein Kryptographieverbot haben?

Die Diskussion um das Kryptographieverbot war ein brisantes Thema in den Jahren 1996 und 1997 und erlebte weltweit eine Wiedergeburt nach den Terroranschlägen vom 11. September 2001. Es wurde proklamiert, dass ein Kryptographieverbot automatisch zu mehr Sicherheit führen würde.
Ein Kryptographieverbot wäre allerdings ein verheerender Einschnitt in das Bürgerrecht, wie z.B. das Grundrecht auf Vertraulichkeit der Kommunikation sowie das Fernmeldegeheimnis, und somit ein weiterer Schritt zum „gläsernen Menschen“. Schliesslich könnten Regierungen somit ungehindert durch Verschlüsselung den Datenverkehr überwachen, sofern dies nicht sowieso schon geschieht. Der Datenschutz in der Informationstechnik würde nahezu komplett verloren gehen. Selbst sensible Daten wie z.B. Unternehmensdaten müssten dann ungeschützt verschickt werden und könnten somit um einiges leichter ausgelesen werden als bisher die verschlüsselten.

Ferner ist es fraglich, ob wir, um die Bekämpfung des organisierten Verbrechens vielleicht an einigen Stellen zu erleichtern, dem Staat und seinen Organen volles Vertrauen entgegenbringen können.
Denn wieso sollten sich Verbrecher, die sowieso schon gesetzesuntreu waren/sind, sich an ein solches Verbot halten? Wenn Kryptographie zum Verbrechen wird, werden nur noch Verbrecher Kryptographie verwenden.
Ein Kryptographieverbot hätte noch dazu keinen Sinn, da man auf die Steganographie ausweichen könnte, um brisante Informationen z.B. in Bildern zu verstecken. Diesem Trend wäre nur schwer beizukommen und es würde sich ein ständiges Katz- und Mausspiel entwickeln.