

libCandle - Ein Softwarewerkzeug für die Stegoanalyse

Lars Herrmann

21.05.2010

- 1 **Steganographie**
 - Ursprüngliche Methoden
 - Computergestützte Steganographie
- 2 **Stegoanalyse**
 - visuelle Analyse
 - χ^2
 - RS-Analyse
- 3 **libCandle**
 - Aufbau
 - Implementierte Funktionalitäten
 - Ruby-Schnittstelle
- 4 **Demonstration**
- 5 **Ausblick**

libCandle - Ein
Softwarewerk-
zeug für die
Stegoanalyse

Lars
Herrmann

Steganographie

Ursprüngliche
Methoden
Computergestüt-
zte
Steganographie

Stegoanalyse

visuelle Analyse
 χ^2
RS-Analyse

libCandle

Aufbau
Implementierte
Funktionalitäten
Ruby-
Schnittstelle

Demonstration

Ausblick

■ Verstecktes Schreiben

Steganographie

libCandle - Ein
Softwarewerk-
zeug für die
Stegoanalyse

Lars
Herrmann

Steganographie

Ursprüngliche
Methoden
Computergestützte
Steganographie

Stegoanalyse

visuelle Analyse
 χ^2
RS-Analyse

libCandle

Aufbau
Implementierte
Funktionalitäten
Ruby-
Schnittstelle

Demonstration

Ausblick

- Verstecktes Schreiben
- Unauffälliges Trägermedium

Steganographie

libCandle - Ein
Softwarewerk-
zeug für die
Steganalyse

Lars
Herrmann

Steganographie

Ursprüngliche
Methoden
Computergestützte
Steganographie

Steganalyse

visuelle Analyse
 χ^2
RS-Analyse

libCandle

Aufbau
Implementierte
Funktionalitäten
Ruby-
Schnittstelle

Demonstration

Ausblick

- Verstecktes Schreiben
- Unauffälliges Trägermedium
- Einsatzgebiet: Kryptographie nicht möglich

libCandle - Ein
Softwarewerk-
zeug für die
Stegoanalyse

Lars
Herrmann

Steganographie
Ursprüngliche
Methoden
Computergestüt-
zte
Steganographie

Stegoanalyse
visuelle Analyse
 χ^2
RS-Analyse

libCandle
Aufbau
Implementierte
Funktionalitäten
Ruby-
Schnittstelle

Demonstration

Ausblick

Historische Steganographiemethoden:

- Tätowierung unter Kopfhaar

libCandle - Ein
Softwarewerk-
zeug für die
Stegoanalyse

Lars
Herrmann

Steganographie
Ursprüngliche
Methoden
Computergestüt-
zte
Steganographie

Stegoanalyse
visuelle Analyse
 χ^2
RS-Analyse

libCandle
Aufbau
Implementierte
Funktionalitäten
Ruby-
Schnittstelle

Demonstration

Ausblick

Historische Steganographiemethoden:

- Tätowierung unter Kopfhaar
- Wachstafeln

libCandle - Ein
Softwarewerk-
zeug für die
Stegoanalyse

Lars
Herrmann

Steganographie
Ursprüngliche
Methoden
Computergestüt-
zte
Steganographie

Stegoanalyse
visuelle Analyse
 χ^2
RS-Analyse

libCandle
Aufbau
Implementierte
Funktionalitäten
Ruby-
Schnittstelle

Demonstration

Ausblick

Historische Steganographiemethoden:

- Tätowierung unter Kopfhaar
- Wachstafeln
- Geheimtinte (Zitronensaft)

Klartext Steganographie

libCandle - Ein
Softwarewerk-
zeug für die
Stegoanalyse

Lars
Herrmann

Steganographie

Ursprüngliche
Methoden

Computergestützte
Steganographie

Stegoanalyse

visuelle Analyse

χ^2
RS-Analyse

libCandle

Aufbau
Implementierte
Funktionalitäten

Ruby-
Schnittstelle

Demonstration

Ausblick

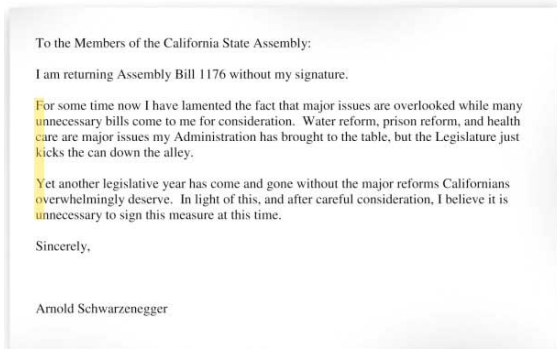


Abbildung: Einfaches Verfahren

Computergestützte Steganographie

libCandle - Ein
Softwarewerk-
zeug für die
Stegoanalyse

Lars
Herrmann

Steganographie
Ursprüngliche
Methoden
Computergestütz-
te
Steganographie

Stegoanalyse
visuelle Analyse
 χ^2
RS-Analyse

libCandle
Aufbau
Implementierte
Funktionalitäten
Ruby-
Schnittstelle

Demonstration

Ausblick

■ Einbettung von Datenströmen in Trägermedien

- Einbettung von Datenströmen in Trägermedien
 - Bilddateien
 - Tondateien
 - Videodateien
 - ...

Beispiel: LSB

libCandle - Ein
Softwarewerk-
zeug für die
Steganalyse

Lars
Herrmann

Steganographie

Ursprüngliche
Methoden

Computergestützte
Steganographie

Stegoanalyse

visuelle Analyse

χ^2
RS-Analyse

libCandle

Aufbau
Implementierte
Funktionalitäten

Ruby-
Schnittstelle

Demonstration

Ausblick

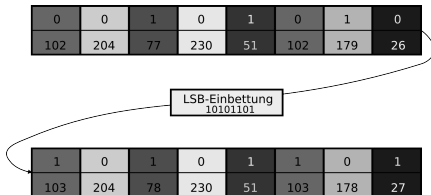


Abbildung: Schematische Darstellung der Einbettung mit dem LSB-Verfahren

Beispiel: BattleSteg

libCandle - Ein
Softwarewerk-
zeug für die
Stegoanalyse

Lars
Herrmann

Steganographie
Ursprüngliche
Methoden
Computergestützte
Steganographie

Stegoanalyse
visuelle Analyse
 χ^2
RS-Analyse

libCandle
Aufbau
Implementierte
Funktionalitäten
Ruby-
Schnittstelle

Demonstration

Ausblick

- LSB-Verfahren mit intelligenter Pixelauswahl
- Nachricht wird vorwiegend in Bildkanten eingebettet
- Auswahl der Pixel an das Spiel "Schiffeversenken" angelehnt

weitere Verfahren

libCandle - Ein
Softwarewerk-
zeug für die
Stegoanalyse

Lars
Herrmann

Steganographie

Ursprüngliche
Methoden

Computergestütz-
te
Steganographie

Stegoanalyse

visuelle Analyse

χ^2
RS-Analyse

libCandle

Aufbau
Implementierte
Funktionalitäten

Ruby-
Schnittstelle

Demonstration

Ausblick

- F5
- CPT
- PQ

libCandle - Ein
Softwarewerk-
zeug für die
Stegoanalyse

Lars
Herrmann

Steganographie
Ursprüngliche
Methoden
Computergestützte
Steganographie

Stegoanalyse

visuelle Analyse
 χ^2
RS-Analyse

libCandle

Aufbau
Implementierte
Funktionalitäten
Ruby-
Schnittstelle

Demonstration

Ausblick

- Analyse von Bildern mit dem Ziel, eingebettete Daten zu erkennen

Stegoanalyse

libCandle - Ein
Softwarewerk-
zeug für die
Stegoanalyse

Lars
Herrmann

Steganographie
Ursprüngliche
Methoden
Computergestüt-
zte
Steganographie

Stegoanalyse
visuelle Analyse
 χ^2
RS-Analyse

libCandle
Aufbau
Implementierte
Funktionalitäten
Ruby-
Schnittstelle

Demonstration

Ausblick

- Analyse von Bildern mit dem Ziel, eingebettete Daten zu erkennen
- Steganographie-Algorithmus gilt als gebrochen, wenn die Existenz von Daten erkannt werden kann

libCandle - Ein
Softwarewerk-
zeug für die
Stegoanalyse

Lars
Herrmann

Steganographie
Ursprüngliche
Methoden
Computergestüt-
zte
Steganographie

Stegoanalyse
visuelle Analyse
 χ^2
RS-Analyse

libCandle
Aufbau
Implementierte
Funktionalitäten
Ruby-
Schnittstelle

Demonstration

Ausblick

- Analyse von Bildern mit dem Ziel, eingebettete Daten zu erkennen
- Steganographie-Algorithmus gilt als gebrochen, wenn die Existenz von Daten erkannt werden kann
- Ausbetten der Daten nicht erforderlich

libCandle - Ein
Softwarewerk-
zeug für die
Stegoanalyse

Lars
Herrmann

Steganographie
Ursprüngliche
Methoden
Computergestüt-
zte
Steganographie

Stegoanalyse
visuelle Analyse
 χ^2
RS-Analyse

libCandle
Aufbau
Implementierte
Funktionalitäten
Ruby-
Schnittstelle

Demonstration

Ausblick

- durchsuchen eines Bildes nach erkennbaren Artefakten, die auf eingebettete Daten schließen lassen

visuelle Analyse

libCandle - Ein
Softwarewerk-
zeug für die
Stegoanalyse

Lars
Herrmann

Steganographie
Ursprüngliche
Methoden
Computergestüt-
zte
Steganographie

Stegoanalyse
visuelle Analyse
 χ^2
RS-Analyse

libCandle
Aufbau
Implementierte
Funktionalitäten
Ruby-
Schnittstelle

Demonstration

Ausblick

- durchsuchen eines Bildes nach erkennbaren Artefakten, die auf eingebettete Daten schließen lassen
- nur bei Bildern mit max. 256 Farben praktikabel

visuelle Analyse

libCandle - Ein
Softwarewerk-
zeug für die
Stegoanalyse

Lars
Herrmann

Steganographie
Ursprüngliche
Methoden
Computergestüt-
zte
Steganographie

Stegoanalyse
visuelle Analyse
 χ^2
RS-Analyse

libCandle
Aufbau
Implementierte
Funktionalitäten
Ruby-
Schnittstelle

Demonstration

Ausblick

- durchsuchen eines Bildes nach erkennbaren Artefakten, die auf eingebettete Daten schließen lassen
- nur bei Bildern mit max. 256 Farben praktikabel
- verbesserung des Verfahrens durch Vorbehandlung des Bildes

verbesserte visuelle Analyse

libCandle - Ein
Softwarewerk-
zeug für die
Stegoanalyse

Lars
Herrmann

Steganographie

Ursprüngliche
Methoden
Computergestützte
Steganographie

Stegoanalyse

visuelle Analyse
 χ^2
RS-Analyse

libCandle

Aufbau
Implementierte
Funktionalitäten
Ruby-
Schnittstelle

Demonstration

Ausblick

- Die LSB-Ebene enthält oft noch erkennbare Bildstrukturen
- Bei einer Einbettung werden diese zerstört

verbesserte visuelle Analyse

libCandle - Ein
Softwarewerk-
zeug für die
Steganalyse

Lars
Herrmann

Steganographie
Ursprüngliche
Methoden
Computergestützte
Steganographie

Stegoanalyse
visuelle Analyse
 χ^2
RS-Analyse

libCandle
Aufbau
Implementierte
Funktionalitäten
Ruby-
Schnittstelle

Demonstration

Ausblick

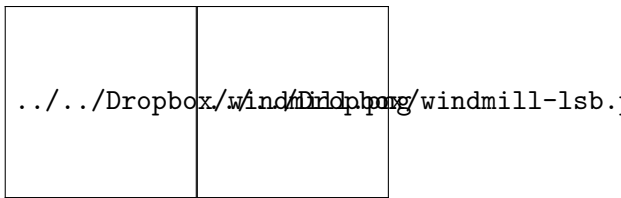


Abbildung: Bild und dessen LSB-Ebene

verbesserte visuelle Analyse

libCandle - Ein
Softwarewerk-
zeug für die
Steganalyse

Lars
Herrmann

Steganographie
Ursprüngliche
Methoden
Computergestütz-
te
Steganographie

Stegoanalyse
visuelle Analyse
 χ^2
RS-Analyse

libCandle
Aufbau
Implementierte
Funktionalitäten
Ruby-
Schnittstelle

Demonstration

Ausblick

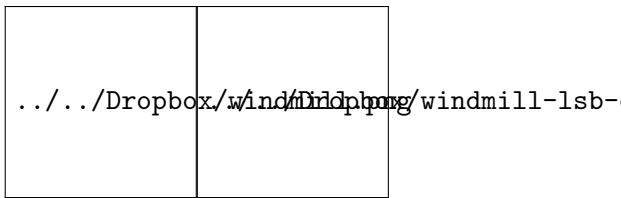


Abbildung: Bild mit Eingebetteten Daten und dessen LSB-Ebene

- Farbwerte des Bildes werden in Paare aufgeteilt
(0,1),(2,3),..., (254,255)
- Differenz der Häufigkeit der Werte eines Paares in einem Bild wird gemessen
- geht davon aus, dass in der Geheimnachricht 0-Bits und 1-Bits gleich häufig vorkommen

Häufigkeitsverteilung

libCandle - Ein
Softwarewerk-
zeug für die
Stegoanalyse

Lars
Herrmann


Steganographie
Ursprüngliche
Methoden
Computergestüt-
zte
Steganographie

Stegoanalyse
visuelle Analyse
 χ^2
RS-Analyse

libCandle
Aufbau
Implementierte
Funktionalitäten
Ruby-
Schnittstelle

Demonstration

Ausblick



```
./././Dropbox/dist.png
```

Abbildung: Häufigkeitsverteilung vor und nach Einbettung

Formeln

libCandle - Ein
Softwarewerk-
zeug für die
Steganalyse

Lars
Herrmann

Steganographie

Ursprüngliche
Methoden

Computergestütz-
te
Steganographie

Stegoanalyse

visuelle Analyse

χ^2
RS-Analyse

libCandle

Aufbau

Implementierte
Funktionalitäten

Ruby-
Schnittstelle

Demonstration

Ausblick

$$n_i = \frac{f_{2i} + f_{2i+1}}{2} \quad (1)$$

Formeln

libCandle - Ein
Softwarewerk-
zeug für die
Stegoanalyse

Lars
Herrmann

Steganographie

Ursprüngliche
Methoden
Computergestüt-
zte
Steganographie

Stegoanalyse

visuelle Analyse
 χ^2
RS-Analyse

libCandle

Aufbau
Implementierte
Funktionalitäten
Ruby-
Schnittstelle

Demonstration

Ausblick

$$n_i = \frac{f_{2i} + f_{2i+1}}{2} \quad (1)$$

$$\chi_{k-1}^2 = \sum_{i=1}^k \frac{(n_i - n_i^*)^2}{n_i^*} \quad (2)$$

Formeln

libCandle - Ein
Softwarewerk-
zeug für die
Steganalyse

Lars
Herrmann

Steganographie

Ursprüngliche
Methoden
Computergestüt-
zte
Steganographie

Steganalyse

visuelle Analyse
 χ^2
RS-Analyse

libCandle

Aufbau
Implementierte
Funktionalitäten
Ruby-
Schnittstelle

Demonstration

Ausblick

$$n_i = \frac{f_{2i} + f_{2i+1}}{2} \quad (1)$$

$$\chi_{k-1}^2 = \sum_{i=1}^k \frac{(n_i - n_i^*)^2}{n_i^*} \quad (2)$$

$$F_k(x) = \frac{1}{2^{\frac{k-1}{2}} \Gamma(\frac{k-1}{2})} \int_0^{\chi_{k-1}^2} e^{-\frac{x}{2}} x^{\frac{k-1}{2}-1} dx \quad (3)$$

Übersicht

libCandle - Ein
Softwarewerk-
zeug für die
Stegoanalyse

Lars
Herrmann

Steganographie
Ursprüngliche
Methoden
Computergestüt-
zte
Steganographie

Stegoanalyse
visuelle Analyse
 χ^2
RS-Analyse

libCandle
Aufbau
Implementierte
Funktionalitäten
Ruby-
Schnittstelle

Demonstration

Ausblick

- Betrachtet Gruppen von benachbarten Pixeln eines Bildes
- Berechnet die “Unregelmäßigkeit” der Gruppen

Übersicht

libCandle - Ein
Softwarewerk-
zeug für die
Stegoanalyse

Lars
Herrmann

Steganographie

Ursprüngliche
Methoden

Computergestütz-
te
Steganographie

Stegoanalyse

visuelle Analyse

χ^2
RS-Analyse

libCandle

Aufbau
Implementierte
Funktionalitäten

Ruby-
Schnittstelle

Demonstration

Ausblick

- Betrachtet Gruppen von benachbarten Pixeln eines Bildes
- Berechnet die “Unregelmäßigkeit” der Gruppen
- Kippt die LSBs des Bildes nach bestimmten Muster
- Teilt in Reguläre und Singulare Gruppen ein

Unregelmäßigkeit

libCandle - Ein
Softwarewerk-
zeug für die
Steganalyse

Lars
Herrmann

Steganographie

Ursprüngliche
Methoden
Computergestützte
Steganographie

Steganalyse

visuelle Analyse
 χ^2
RS-Analyse

libCandle

Aufbau
Implementierte
Funktionalitäten
Ruby-
Schnittstelle

Demonstration

Ausblick

$$f(x_1, x_2, \dots, x_n) = \sum_{i=1}^{n-1} x_{i+1} - x_i \quad (4)$$

Kippen - 1

libCandle - Ein
Softwarewerk-
zeug für die
Stegoanalyse

Lars
Herrmann

Steganographie
Ursprüngliche
Methoden
Computergestüt-
zte
Steganographie

Stegoanalyse
visuelle Analyse
 χ^2
RS-Analyse

libCandle
Aufbau
Implementierte
Funktionalitäten
Ruby-
Schnittstelle

Demonstration

Ausblick

$$F_1(x) = \begin{cases} x + 1 & \text{wenn } x \text{ gerade} \\ x - 1 & \text{sonst} \end{cases} \quad (5)$$

Kippen - 1

libCandle - Ein
Softwarewerk-
zeug für die
Steganalyse

Lars
Herrmann

Steganographie
Ursprüngliche
Methoden
Computergestütz-
te
Steganographie

Stegoanalyse
visuelle Analyse
 χ^2
RS-Analyse

libCandle
Aufbau
Implementierte
Funktionalitäten
Ruby-
Schnittstelle

Demonstration

Ausblick

$$F_1(x) = \begin{cases} x + 1 & \text{wenn } x \text{ gerade} \\ x - 1 & \text{sonst} \end{cases} \quad (5)$$

$$F_{-1}(x) = \begin{cases} x - 1 & \text{wenn } x \text{ gerade} \\ x + 1 & \text{sonst} \end{cases} \quad (6)$$

$$F_0(x) = x$$

Kippen - 2

libCandle - Ein
Softwarewerk-
zeug für die
Stegoanalyse

Lars
Herrmann

Steganographie
Ursprüngliche
Methoden
Computergestüt-
zte
Steganographie

Stegoanalyse
visuelle Analyse
 χ^2
RS-Analyse

libCandle
Aufbau
Implementierte
Funktionalitäten
Ruby-
Schnittstelle

Demonstration

Ausblick

Gruppen von Pixeln werden anhand einer Maske gekippt:

$$M_n \in [-1, 0, 1]^n$$

$$F(G_n, M_n) = (F_{M_1}(G_1), \dots, F_{M_n}(G_n)) \quad (7)$$

Einteilung in Gruppen

libCandle - Ein
Softwarewerk-
zeug für die
Stegoanalyse

Lars
Herrmann

Steganographie

Ursprüngliche
Methoden
Computergestüt-
zte
Steganographie

Stegoanalyse

visuelle Analyse
 χ^2
RS-Analyse

libCandle

Aufbau
Implementierte
Funktionalitäten
Ruby-
Schnittstelle

Demonstration

Ausblick

regulär , wenn gilt: $f(G) < f(F(G))$
singular , wenn gilt: $f(G) > f(F(G))$
unverändert , wenn gilt: $f(G) = f(F(G))$

Beobachtungen

libCandle - Ein
Softwarewerk-
zeug für die
Stegoanalyse

Lars
Herrmann

Steganographie

Ursprüngliche
Methoden

Computergestüt-
zte
Steganographie

Stegoanalyse

visuelle Analyse

χ^2
RS-Analyse

libCandle

Aufbau
Implementierte
Funktionalitäten

Ruby-
Schnittstelle

Demonstration

Ausblick

- in typischen Bildern erhöht sich der Wert f einer Gruppe durch anwendung der Kippfunktion
- daher mehr R- als S-Gruppen

Beobachtungen

libCandle - Ein
Softwarewerk-
zeug für die
Stegoanalyse

Lars
Herrmann

Steganographie

Ursprüngliche
Methoden

Computergestüt-
zte
Steganographie

Stegoanalyse

visuelle Analyse

χ^2
RS-Analyse

libCandle

Aufbau
Implementierte
Funktionalitäten

Ruby-
Schnittstelle

Demonstration

Ausblick

- in typischen Bildern erhöht sich der Wert f einer Gruppe durch anwendung der Kippfunktion
- daher mehr R- als S-Gruppen
- die Anteile von R- und S-Gruppen verändern sich in typischen Bildern durch Umkehren der Maske kaum
- wird die LSB-Ebene zur Hälfte durch Zufallswerte überschrieben, enthält das Bild etwa gleich viele R- und S-Gruppen

RS-Diagramm

libCandle - Ein
Softwarewerk-
zeug für die
Stegoanalyse

Lars
Herrmann

Steganographie

Ursprüngliche
Methoden
Computergestützte
Steganographie

Stegoanalyse

visuelle Analyse
 χ^2
RS-Analyse

libCandle

Aufbau
Implementierte
Funktionalitäten
Ruby-
Schnittstelle

Demonstration

Ausblick

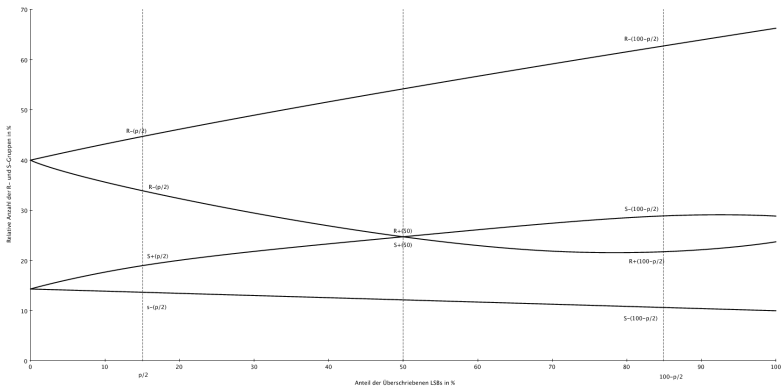


Abbildung: RS-Diagramm eines typischen Bildes

Verwendete Software

libCandle - Ein
Softwarewerk-
zeug für die
Stegoanalyse

Lars
Herrmann

Steganographie
Ursprüngliche
Methoden
Computergestüt-
zte
Steganographie

Stegoanalyse
visuelle Analyse
 χ^2
RS-Analyse

libCandle

Aufbau
Implementierte
Funktionalitäten
Ruby-
Schnittstelle

Demonstration

Ausblick

- C++
- ImageMagick
- Boost
 - Boost::test
 - Boost::math
 - Boost::any
- SWIG
- Ruby

Datenstrukturen

libCandle - Ein
Softwarewerk-
zeug für die
Stegoanalyse

Lars
Herrmann

Steganographie

Ursprüngliche
Methoden

Computergestützte
Steganographie

Stegoanalyse

visuelle Analyse

χ^2
RS-Analyse

libCandle

Aufbau

Implementierte
Funktionalitäten

Ruby-
Schnittstelle

Demonstration

Ausblick

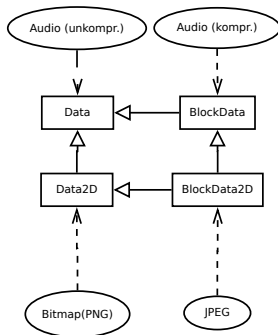


Abbildung: Datenstrukturen in libCandle

libCandle - Ein
Softwarewerk-
zeug für die
Stegoanalyse

Lars
Herrmann

Steganographie

Ursprüngliche
Methoden
Computergestützte
Steganographie

Stegoanalyse

visuelle Analyse
 χ^2
RS-Analyse

libCandle

Aufbau
Implementierte
Funktionalitäten
Ruby-
Schnittstelle

Demonstration

Ausblick

- Funktionen, die einen Datenstrom auf bestimmte Weise Transformieren
- Parametergesteuert

Analyzer

libCandle - Ein
Softwarewerk-
zeug für die
Stegoanalyse

Lars
Herrmann

Steganographie

Ursprüngliche
Methoden
Computergestüt-
zte
Steganographie

Stegoanalyse

visuelle Analyse
 χ^2
RS-Analyse

libCandle

Aufbau
Implementierte
Funktionalitäten
Ruby-
Schnittstelle

Demonstration

Ausblick

- Funktionen, die einem gegebenen Datenstrom eine reelle Zahl zwischen 0 und 1 zuweisen
→ Einbettungswahrscheinlichkeit
- Parametergesteuert

Parametersteuerung

libCandle - Ein
Softwarewerk-
zeug für die
Steganalyse

Lars
Herrmann

Steganographie

Ursprüngliche
Methoden
Computergestützte
Steganographie

Stegoanalyse

visuelle Analyse
 χ^2
RS-Analyse

libCandle

Aufbau
Implementierte
Funktionalitäten
Ruby-
Schnittstelle

Demonstration

Ausblick

- Funktionsobjekte enthalten ein Dictionary (`string Name => any value`)
- `typ any` entspricht einem bestimmten Datentyp (`string`, `int`, `double`, `bool`)
- zweites Dictionary enthält die benötigten Typen
- alle Parameter mit Standardwerten Initialisiert

Parametersteuerung

libCandle - Ein
Softwarewerk-
zeug für die
Steganalyse

Lars
Herrmann

Steganographie

Ursprüngliche
Methoden
Computergestüt-
zte
Steganographie

Stegoanalyse

visuelle Analyse
 χ^2
RS-Analyse

libCandle

Aufbau
Implementierte
Funktionalitäten
Ruby-
Schnittstelle

Demonstration

Ausblick

- Funktionsobjekte enthalten ein Dictionary (`string Name => any value`)
- `typ any` entspricht einem bestimmten Datentyp (`string`, `int`, `double`, `bool`)
- zweites Dictionary enthält die benötigten Typen
- alle Parameter mit Standardwerten Initialisiert

Programme, die libCandle verwenden, müssen die Parameter und deren Typen nicht unbedingt kennen, um Funktionen zu benutzen.

Trägerformate

libCandle - Ein
Softwarewerk-
zeug für die
Stegoanalyse

Lars
Herrmann

Steganographie
Ursprüngliche
Methoden
Computergestüt-
zte
Steganographie

Stegoanalyse
visuelle Analyse
 χ^2
RS-Analyse

libCandle
Aufbau
Implementierte
Funktionalitäten
Ruby-
Schnittstelle

Demonstration

Ausblick

Implementiert

- PNG,BMP,TGA,GIF,... (ImageMagick)
- JPEG als Bitmapgrafik

ToDo

- JPEG mit Zugriff auf DCT-Koeffizienten
- Audiodateien

libCandle - Ein
Softwarewerk-
zeug für die
Stegoanalyse

Lars
Herrmann

Steganographie
Ursprüngliche
Methoden
Computergestüt-
zte
Steganographie

Stegoanalyse
visuelle Analyse
 χ^2
RS-Analyse

libCandle
Aufbau
Implementierte
Funktionalitäten
Ruby-
Schnittstelle

Demonstration

Ausblick

NoiseFilter fügt dem Bild rauschen hinzu

ConvolutionFilter 2-D Faltung

BitremapFilter ordnet die Bitebenen eines Bildes neu an

FlipMapFilter kippt die LSBs eines Bildes anhand einer Matrix
(RS-Analyse)

libCandle - Ein
Softwarewerk-
zeug für die
Stegoanalyse

Lars
Herrmann

Steganographie

Ursprüngliche
Methoden
Computergestüt-
zte
Steganographie

Stegoanalyse

visuelle Analyse
 χ^2
RS-Analyse

libCandle

Aufbau
Implementierte
Funktionalitäten
Ruby-
Schnittstelle

Demonstration

Ausblick

- χ^2 -Analyse
- RS-Analyse
- Unterstützung für visuelle Analyse

libCandle - Ein
Softwarewerk-
zeug für die
Stegoanalyse

Lars
Herrmann

Steganographie

Ursprüngliche
Methoden

Computergestütz-
te
Steganographie

Stegoanalyse

visuelle Analyse

χ^2
RS-Analyse

libCandle

Aufbau
Implementierte
Funktionalitäten

Ruby-
Schnittstelle

Demonstration

Ausblick

■ zweistufige Implementierung

Übersicht

libCandle - Ein
Softwarewerk-
zeug für die
Steganalyse

Lars
Herrmann

Steganographie
Ursprüngliche
Methoden
Computergestüt-
zte
Steganographie

Stegoanalyse
visuelle Analyse
 χ^2
RS-Analyse

libCandle
Aufbau
Implementierte
Funktionalitäten
Ruby-
Schnittstelle

Demonstration

Ausblick

- zweistufige Implementierung
- zunächst Erstellung der eigentlichen Schnittstelle mit SWIG
- Anpassung der generierten Schnittstelle an Ruby Stil

Übersicht

libCandle - Ein
Softwarewerk-
zeug für die
Steganalyse

Lars
Herrmann

Steganographie
Ursprüngliche
Methoden
Computergestüt-
zte
Steganographie

Steganalyse
visuelle Analyse
 χ^2
RS-Analyse

libCandle
Aufbau
Implementierte
Funktionalitäten
Ruby-
Schnittstelle

Demonstration

Ausblick

- zweistufige Implementierung
- zunächst Erstellung der eigentlichen Schnittstelle mit SWIG
- Anpassung der generierten Schnittstelle an Ruby Stil
- Ermöglicht in Verbindung mit `irb` interaktive Benutzung der Funktionen

libCandle - Ein
Softwarewerk-
zeug für die
Stegoanalyse

Lars
Herrmann

Steganographie

Ursprüngliche
Methoden

Computergestüt-
zte
Steganographie

Stegoanalyse

visuelle Analyse

χ^2
RS-Analyse

libCandle

Aufbau
Implementierte
Funktionalitäten

Ruby-
Schnittstelle

Demonstration

Ausblick

Demonstration

libCandle - Ein
Softwarewerk-
zeug für die
Steganalyse

Lars
Herrmann

Steganographie

Ursprüngliche
Methoden

Computergestütz-
te
Steganographie

Stegoanalyse

visuelle Analyse

χ^2
RS-Analyse

libCandle

Aufbau
Implementierte
Funktionalitäten

Ruby-
Schnittstelle

Demonstration

Ausblick

■ GUI Entwickeln

weitere Möglichkeiten

libCandle - Ein
Softwarewerk-
zeug für die
Stegoanalyse

Lars
Herrmann

Steganographie
Ursprüngliche
Methoden
Computergestüt-
zte
Steganographie

Stegoanalyse
visuelle Analyse
 χ^2
RS-Analyse

libCandle
Aufbau
Implementierte
Funktionalitäten
Ruby-
Schnittstelle

Demonstration

Ausblick

- GUI Entwickeln
- Plug-Ins

weitere Möglichkeiten

libCandle - Ein
Softwarewerk-
zeug für die
Steganalyse

Lars
Herrmann

Steganographie
Ursprüngliche
Methoden
Computergestützte
Steganographie

Stegoanalyse
visuelle Analyse
 χ^2
RS-Analyse

libCandle
Aufbau
Implementierte
Funktionalitäten
Ruby-
Schnittstelle

Demonstration

Ausblick

- GUI Entwickeln
- Plug-Ins
- Mehr Boost

Boost::GIL besserer Zugriff auf Bilddaten
Boost::functional mehr Aspekte der Funktionalen
Programmierung

weitere Möglichkeiten

libCandle - Ein
Softwarewerk-
zeug für die
Steganalyse

Lars
Herrmann

Steganographie
Ursprüngliche
Methoden
Computergestüt-
zte
Steganographie

Stegoanalyse
visuelle Analyse
 χ^2
RS-Analyse

libCandle
Aufbau
Implementierte
Funktionalitäten
Ruby-
Schnittstelle

Demonstration

Ausblick

- GUI Entwickeln
- Plug-Ins
- Mehr Boost
 - Boost::[GIL](#) besserer Zugriff auf Bilddaten
 - Boost::[functional](#) mehr Aspekte der Funktionalen Programmierung
- Rewrite in Haskell ;)

libCandle - Ein
Softwarewerk-
zeug für die
Stegoanalyse

Lars
Herrmann

Steganographie

Ursprüngliche
Methoden
Computergestützte
Steganographie

Stegoanalyse

visuelle Analyse
 χ^2
RS-Analyse

libCandle

Aufbau
Implementierte
Funktionalitäten
Ruby-
Schnittstelle

Demonstration

Ausblick

- Viel über C++ und OOP gelernt

libCandle - Ein
Softwarewerk-
zeug für die
Stegoanalyse

Lars
Herrmann

Steganographie

Ursprüngliche
Methoden
Computergestützte
Steganographie

Stegoanalyse

visuelle Analyse
 χ^2
RS-Analyse

libCandle

Aufbau
Implementierte
Funktionalitäten
Ruby-
Schnittstelle

Demonstration

Ausblick

- Viel über C++ und OOP gelernt
- Funktionale Programmiersprache eventuell besser geeignet

libCandle - Ein
Softwarewerk-
zeug für die
Stegoanalyse

Lars
Herrmann

Steganographie

Ursprüngliche
Methoden
Computergestüt-
zte
Steganographie

Stegoanalyse

visuelle Analyse
 χ^2
RS-Analyse

libCandle

Aufbau
Implementierte
Funktionalitäten
Ruby-
Schnittstelle

Demonstration

Ausblick

- Viel über C++ und OOP gelernt
- Funktionale Programmiersprache eventuell besser geeignet
- Konzepte der Stegoanalyse nur schwierig zu abstrahieren

libCandle - Ein
Softwarewerk-
zeug für die
Stegoanalyse

Lars
Herrmann

Steganographie

Ursprüngliche
Methoden

Computergestützte
Steganographie

Stegoanalyse

visuelle Analyse

χ^2
RS-Analyse

libCandle

Aufbau
Implementierte
Funktionalitäten

Ruby-
Schnittstelle

Demonstration

Ausblick

Vielen Dank für die Aufmerksamkeit