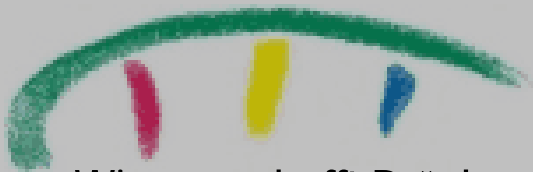


TECHNISCHE  
UNIVERSITÄT  
DRESDEN

## Verdeckte Kommunikation für den Amateurfunk und die Programmierungsumgebung

*Andreas Westfeld, DL1DSX*

*[westfeld@inf.tu-dresden.de](mailto:westfeld@inf.tu-dresden.de)*



»Wissen schafft Brücken.«

# Gliederung

- Programmierumgebung R
  - Demo
  - Beispielsitzung
- Ein Beispiel für den Einsatz von R
  - Verdeckte Kommunikation (Steganographie)
  - Motivation durch Amateurfunkrecht
  - Anforderungen für Funkübertragung
  - Schmalbandfernsehen (SSTV)
  - Umsetzung mit R
  - Sicherheitsbetrachtung

# Programmierumgebung R



- Interpretierte, objektorientierte Sprache und Programmierumgebung für Datenanalyse
- R ist GPL-Version von S (von den Bell-Labs)
- Für Linux, Windows, MacOS X usw. verfügbar unter [www.r-project.org](http://www.r-project.org) (Download/CRAN)
- An Introduction to R (Documentation/Manuals)
- Beispielsitzung (Vorführung)

# Demonstration von R

```
# R als Taschenrechner
```

```
1+2*3
```

```
5^2
```

```
4*sin(pi/2)
```

```
sqrt(-1)
```

```
?sqrt
```

```
sqrt(as.complex(-1))
```

```
sqrt(-1+0i)
```

```
0/0
```

```
x<-1:12
```

```
x
```

```
/* Summe von 100 Zahlen in C */
```

```
int s=0, i;
```

```
for (i=1; i<=100; i++) s+=i;
```

```
printf("%d\n", s);
```

```
# Summe von 100 Zahlen in R
```

```
sum(1:100)
```

```
cumsum(x) # kumulative Summe
```

```
(m<-matrix(1:12,3))
```

```
mean(m) # Mittelwert
```

```
max(m)
```

```
min(m)
```

# Demonstration von R (2)

```
apply(m,1,sum) # Zeilensummen
apply(m,2,sum) # Spaltensummen
m%%2          # Matrix modulo 2
m*2+1
m^2
m==4          # Matrix von Wahrheitswerten
# mit Wahrheitswerten indizieren
m[m%%2==0]
# gerade Werte in m ersetzen
m[m%%2==0]<-0
m
```

```
rnorm(9) # normalverteilte Zufallszahlen
# Histogramm von 1000 Zahlen
hist(rnorm(1000))
hist(rnorm(10000),50) # 50 Balken
hist(runif(10000),50) # gleichverteilt
plot(rnorm(1000))
```

```
demo() # listet verfügbare demos auf
demo(graphics)
demo(persp)
```

# Steganographie

Trägermedium



↓ *möglichst unverändert* ①

Steganogramm



Schlüssel

Schlüssel

einbetten

extrahieren

übertragen

M/uogOCSn210Tx0cB/kkb0  
jQrEje21ESJnyG8yN7+VzH  
empuxzFEUvQCC7T2xCTgyl  
IQHkrfW8YkWgxuGtTmb...

← *möglichst viel* ②

③ *möglichst fehlerfrei/robust* →

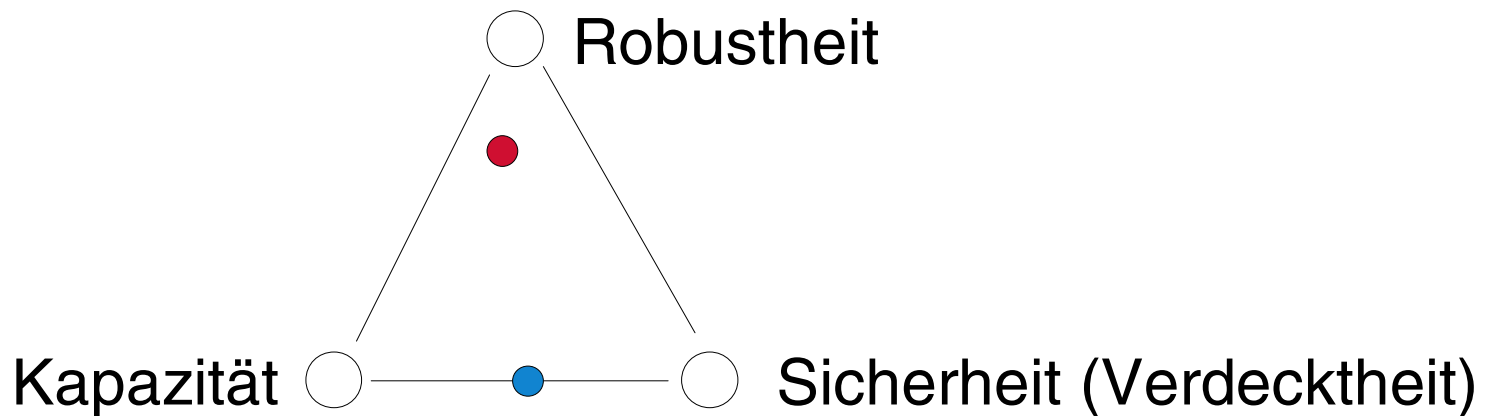
M/uogOCSn210Tx0cB/kkb0  
jQrEje21ESJnyG8yN7+VzH  
empuxzFEUvQCC7T2xCTgyl  
IQHkrfW8YkWgxuGtTmb...

einzubettende Nachricht

eingebettete Nachricht

# Robuste Steganographie

- Robustheit: Nachricht überlebt Störung
- **Steganographie**: nicht robust
- **Digitale Wasserzeichen**: nicht versteckt



# Motivation

Die Existenz steganographischer Methoden ist ein wesentliches Argument gegen ein Verbot von Kryptographie. Ein solches Verbot wurde im Jahre 2005 neu in die Amateurfunkverordnung aufgenommen.

Amateurfunkverordnung §16:

(8) **Amateurfunkverkehr darf nicht zur Verschleierung des Inhalts verschlüsselt werden;** Steuersignale für Erd- und Weltraumfunkstellen des Amateurfunkdienstes über Satelliten gelten nicht als verschlüsselte Aussendungen.

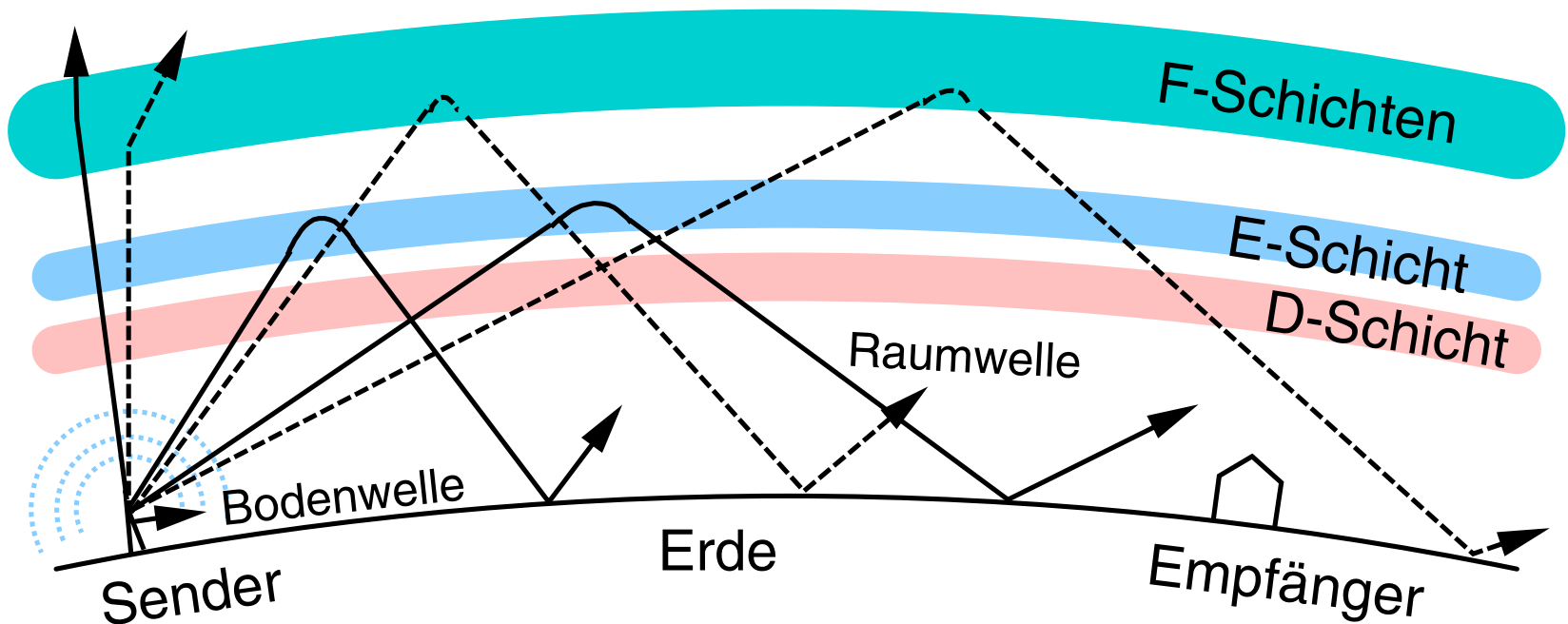
→ VOFunk82: offene Sprache im internationalen Funkverkehr,

→ AFuV98: offene Sprache auch nationalen Funkverkehr

Bundesgesetzblatt Jahrgang 2005 Teil I Nr. 10, ausgegeben zu Bonn am 18. Februar 2005, Seiten 242-250  
Verordnung zum Gesetz über den Amateurfunk (Amateurfunkverordnung - AFuV) vom 15. Februar 2005

# Störungen im Amateurfunk

- F1-Schicht senkt/hebt sich, wenn es Tag/Nacht wird → dynamische Änderung der Weglänge (Phasenlage)
- Mehrwegeempfang → Schwund (Fading, QSB)



# Simulationsparameter

- Acht Bedingungen: zwei Empfangswege mit Phasenverschiebung und Dopplereffekt

Ausbreitungsbedingung	Verzögerungszeit	Dopplerverschiebung
Noise	0 ms	0 Hz
Flat 1	0 ms	0,2 Hz
Flat 2	0 ms	1 Hz
CCIR good	0,5 ms	0,1 Hz
CCIR moderate	1 ms	0,5 Hz
CCIR poor	2 ms	1 Hz
CCIR flutter fading	0,5 ms	10 Hz
Extreme	2 ms	5 Hz

# HF-Kanalsimulation

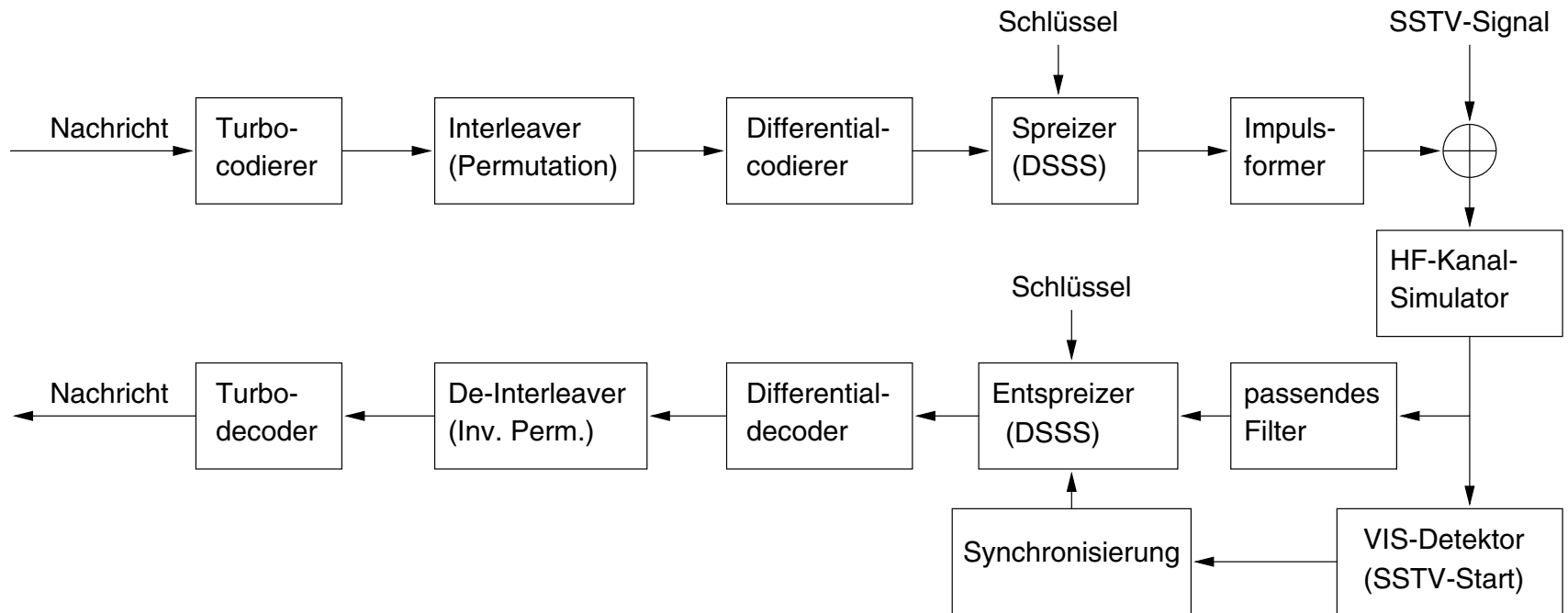
The screenshot shows the 'QSSTV Transmit' window. The title bar includes 'File Options Debug'. The menu bar contains 'File Options Debug'. The toolbar includes icons for file operations, a traffic light icon, a musical note, a pencil, a magnifying glass, a refresh icon, and a dropdown menu set to 'SSTV'. The main area displays a dropdown menu with 'Martin 1' selected, followed by 'CCIR POOR' and another dropdown. Below this, the SNR is shown as '26 dB (S4)' with a slider. A list of checkboxes includes 'Banner', 'Timestamp' (checked), 'CW' (checked), 'VOX', and 'Loopback' (checked). The status bar at the bottom shows 'Ready' and a green progress indicator.

The screenshot shows the 'QSSTV Receive' window. The title bar includes 'File Options Debug Help'. The menu bar contains 'File Options Debug Help'. The toolbar includes icons for file operations, a traffic light icon, a magnifying glass, a refresh icon, and a dropdown menu set to 'SSTV'. The main area displays 'Filters Main 1000 Hz Post NO Filter'. A list of checkboxes includes 'VIS', 'AutoSave' (checked), and 'DX'. Below this, a dropdown menu is set to 'Medium Sen', followed by 'AutoErase' and 'Repeater'. There are three colored squares (red, yellow, green) below the 'Repeater' checkbox. The main display area shows a distorted image of a building. The status bar at the bottom shows 'Receiving' and 'Martin 1'.

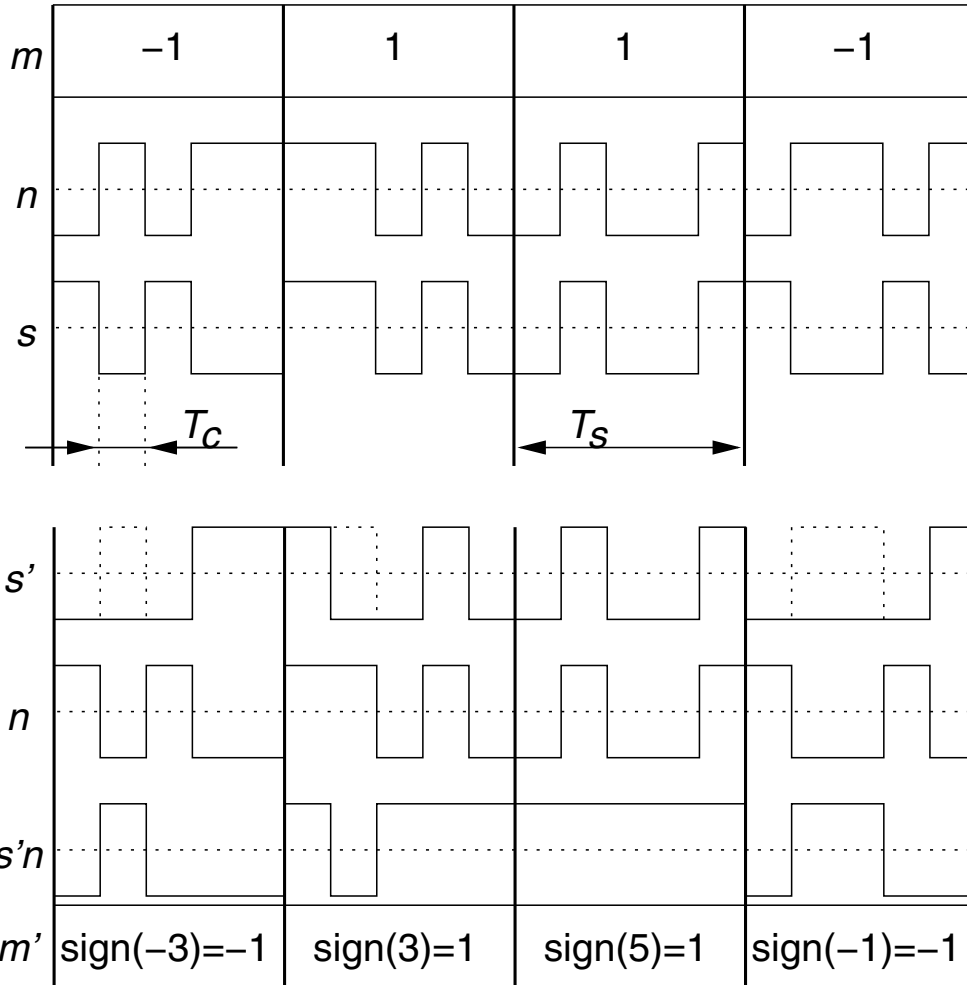
# Wahl der Betriebsart

- **Verbindungszeit** sollte möglichst lang sein  
→ geringerer Synchronisationsaufwand, höhere Kapazität
- **Synchronisationsinformation** sollte möglichst schon vorhanden sein  
→ muss dann nicht eingebettet und verschleiert werden
- Sprechfunk: keine Synchronisation vorhanden
- Telegraphie: zu geringe Bandbreite
- Schmalbandfernsehen (slow scan television, SSTV):
  - Synchronisiert
  - Lange Sendephase
  - Sehr verbreitet

# Steganographisches SSTV



# Spreadspektrum(de)modulation

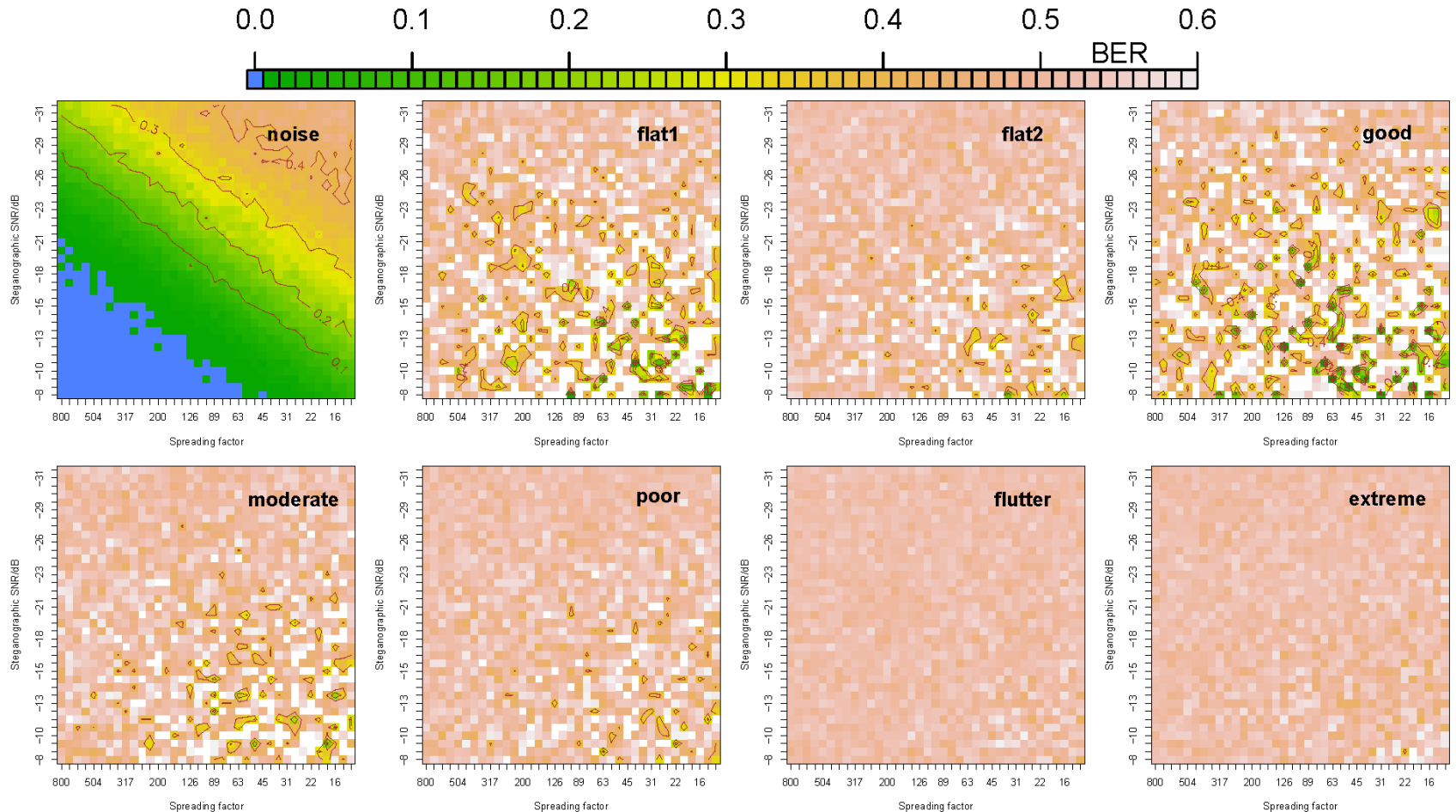


- Nachricht  $m$  wird mit Spreizfolge  $n$  (Rauschen) moduliert  $\rightarrow$  Einbettungsfolge  $s = mn$
- Gestörtes Signal  $s'$  wird empfangen
- $s'n$  wird stückweise integriert  $\rightarrow m'$

# Problem mit Spreizspektrum

- Kann nur demoduliert werden, wenn Sender und Empfänger synchron
- Wird für digitale Wasserzeichen zum Copyrightschutz verwendet
  - ➡ digitale Wasserzeichen werden durch **Desynchronisation** zerstört
- Zum Bsp. Stirmark: geometrische Verzerrung von Bildern

# Ergebnisse für Spreizspektrum



# Streckenweise Phasenumkehr

- Originalnachricht:

1 -1 -1 -1 -1 1 1 1 -1 -1 1 1 -1 -1 1 1 -1 -1

- Empfangene Nachricht:

1 -1 -1 -1 -1 -1 -1 -1 1 1 -1 -1 -1 -1 1 1 -1 -1 (7 Fehler)

- Originalnachricht:

1 -1 -1 -1 -1 1 1 1 -1 -1 1 1 -1 -1 1 1 -1 -1

- Differenziell codiert:

1 -1 1 -1 1 1 1 1 -1 1 1 1 -1 1 1 1 -1 1

- Gestört:

1 -1 1 -1 1 -1 -1 -1 1 -1 -1 -1 -1 1 1 1 -1 1 (7 Fehler)

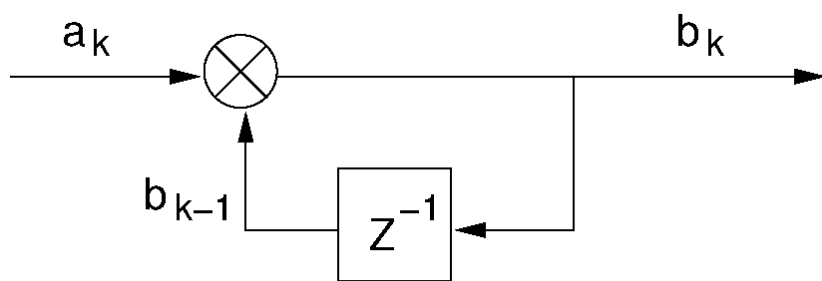
- Differentiell decodiert:

1 -1 -1 -1 -1 -1 1 1 -1 -1 1 1 1 -1 1 1 -1 -1 (2 Fehler)

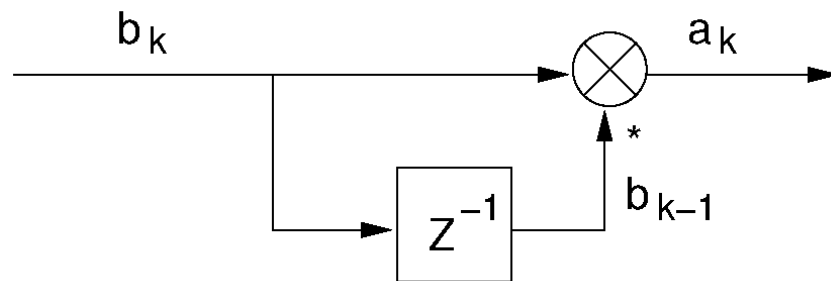
# Differenzielle Codierung

- Codierung in R:  $dx \leftarrow \text{cumprod}(x)$
- Decodierung in R:  $x \leftarrow x * c(1, x[-\text{length}(x)])$

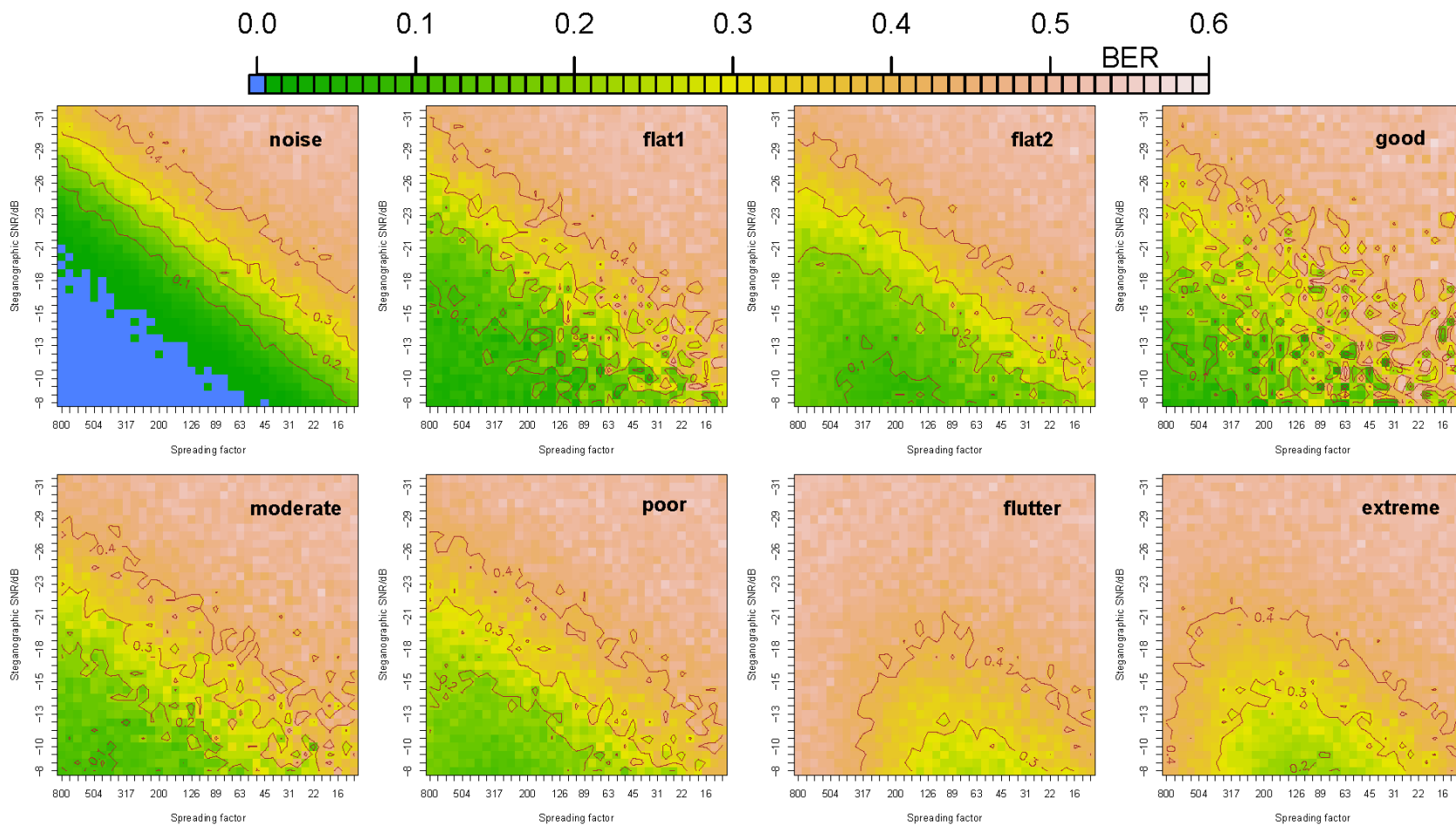
## Codierung



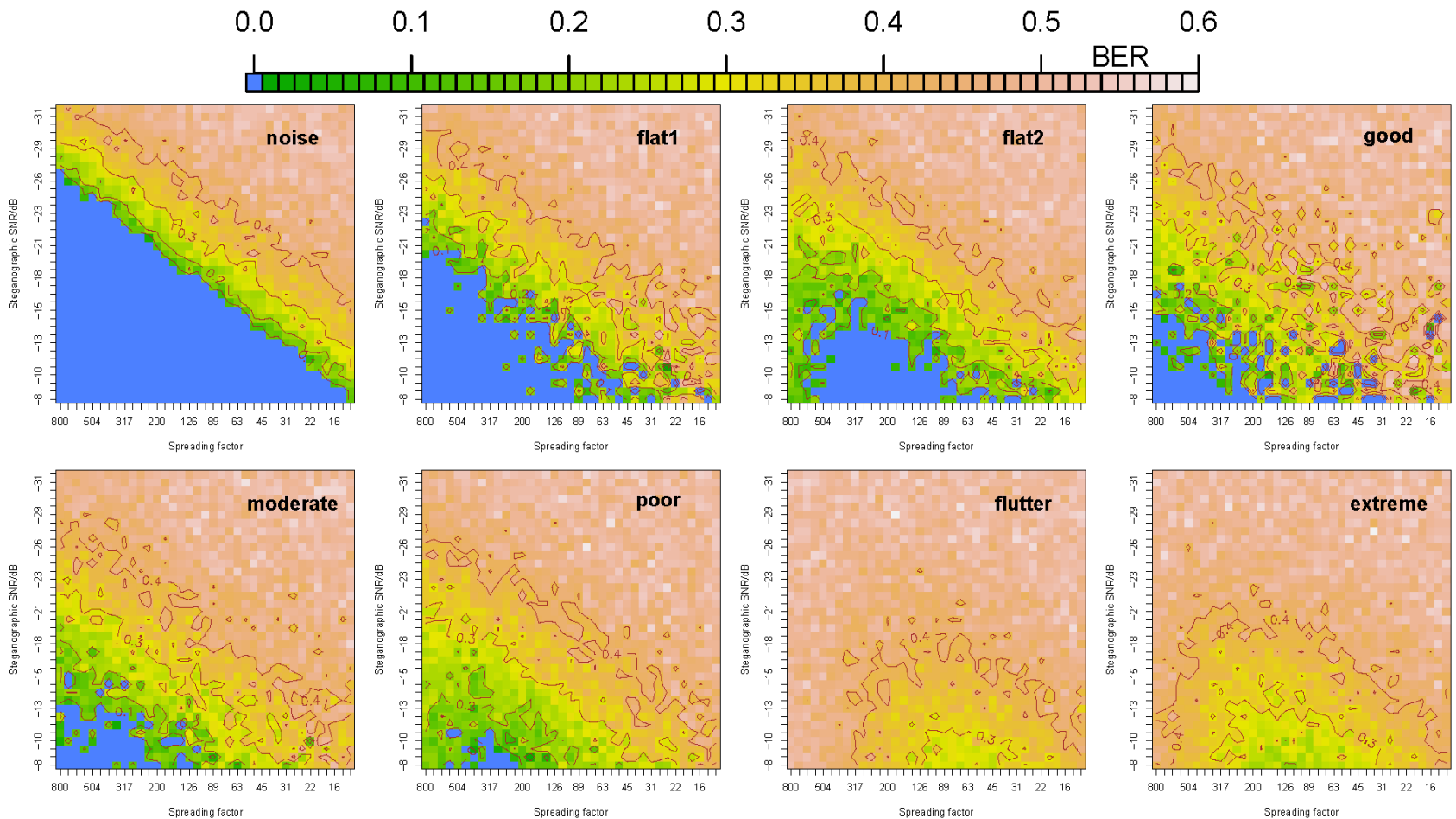
## Decodierung



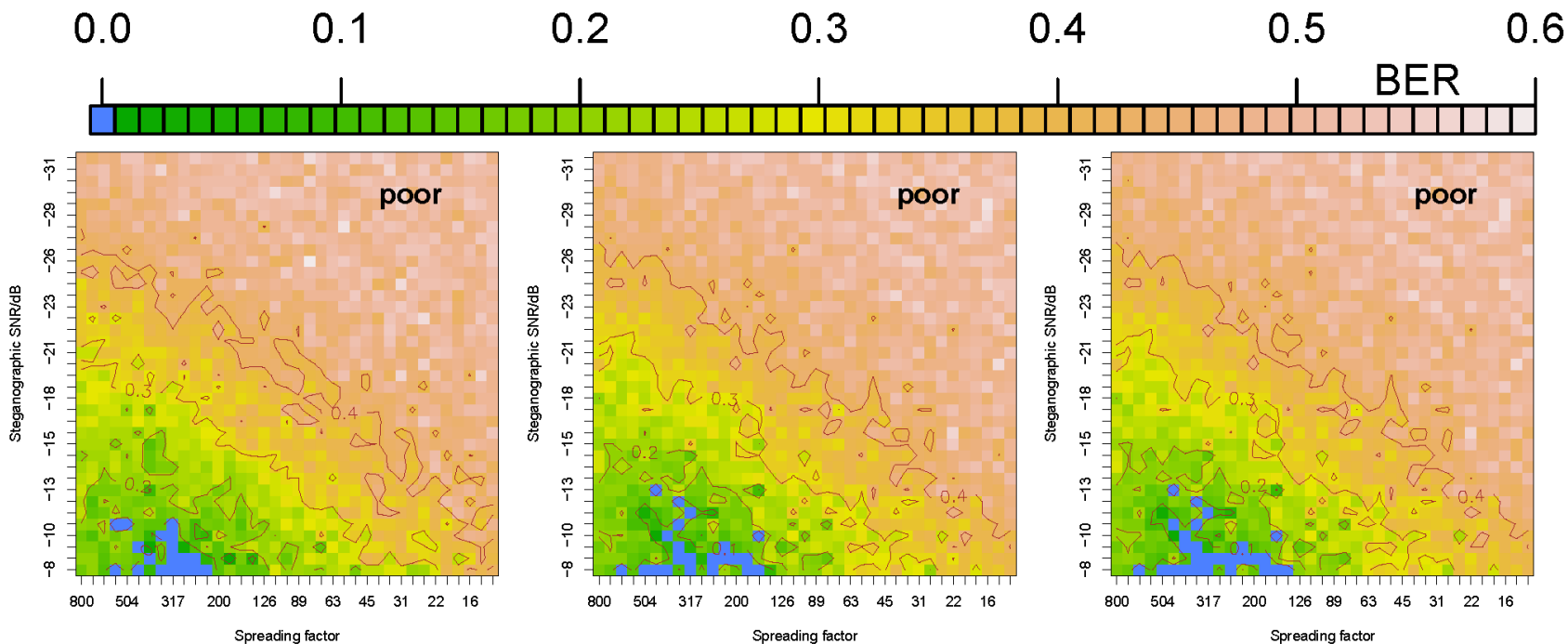
# Differenziell demoduliert



# Mit fehlerkorrigierendem Code



# Feineinstellung



Hard-Decision/Impulsformung/Soft-Decision  
fehlerfrei: 18/22/27

# Optimale Parameter

Ausbreitungsbedingung	Spreizfaktor	Steganogr. Rauschabstand	Kapazität
Noise	800	−27 dB	46 bytes
Flat 1	800	−21 dB	46 bytes
Flat 2	320	−16 dB	118 bytes
CCIR good	640	−15 dB	58 bytes
CCIR moderate	450	−13 dB	83 bytes
CCIR poor	320	−11 dB	118 bytes
CCIR flutter fading	—	—	0
Extreme	—	—	0

# Sicherheit

- Ziel des Angreifers: Nachrichten mit und ohne Steganographie unterscheiden
- Steganographischer Rauschanteil als Unterscheidungsmerkmal
- Problem: Rauschquellen lassen sich nur schwer trennen:
  - **steganographisches Rauschen**
  - Rauschen der Bildvorlage
  - Rauschen der Sendeanlage
  - atmosphärisches Grundrauschen
  - sonstige Störungen, denen das Signal ausgesetzt ist

# Sicherheit (2)

- Angreifer kann seine Situation verbessern
  - durch Wahl einer günstigen geographischen Position
  - durch einen empfindlicheren Empfänger
  - durch eine Antenne mit höherem Gewinn und besserer Richtcharakteristik
- Vorteil des Empfängers: Symbolenergie wird über einen längeren Zeitraum mit geheimer Spreizfolge verteilt.
- Wiegt das die Vorteile eines Angreifers auf?
  - Optimum für Spreizfaktor
  - Sichtkontakt → AWGN-Kanal?

# Zusammenfassung

- R ist eine kostenlose, leistungsfähige Programmierumgebung
- Spart viel Zeit bei Analyse und Verarbeitung von großen Datenmengen
- Inzwischen wichtigste Programmiersprache an meinem Arbeitsplatz
- Anwendungsbeispiel
  - Steganographie
  - Signalverarbeitung
  - Statistische Auswertung