Steganographie für den Amateurfunk

Andreas Westfeld*

Technische Universität Dresden
Institut für Systemarchitektur
mailto:dl1dsx@inf.tu-dresden.de

Zusammenfassung: Ziel dieses Beitrags ist es, Ideen auf mehreren Gebieten zur Verbesserung der Robustheit verdeckter Kommunikation gegenüber unbeabsichtigten, zufälligen Kanalfehlern zusammenzutragen und deren Wirksamkeit durch Simulation zu überprüfen. Am Szenario einer Funkverbindung werden praktikable Parameter für sechs verschiedene Kurzwellenbedingungen bei geringstmöglicher Nachweisbarkeit ermittelt. Konkret wird ein Verfahren entwickelt, mit dem sich Nachrichten einer Länge von bis zu 118 Bytes in einer Schmalbandfernsehverbindung im Modus Martin-M1 steganographisch übermitteln lassen.

1 Anforderungen für robuste Steganographie

Wasserzeichen und Steganographie haben unterschiedliche Ziele. Sicherheit bedeutet bei digitalen Wasserzeichen, dass die eingebetteten Nachrichten gegen verändernde Angreifer geschützt sind (Robustheit, Wasserzeichensicherheit), während es bei der Steganographie darauf ankommt, dass die Existenz der eingebetteten Information für Dritte nicht nachweisbar ist (Unerkennbarkeit, Transparenz, steganographische Sicherheit).

Dieser Beitrag verfolgt die steganographische Sichtweise, beschäftigt sich aber dennoch mit der Eigenschaft Robustheit, allerdings in erster Linie nicht gegen absichtliche Störungen eines Angreifers, sondern gegen unbeabsichtigte, zufällige Kanalfehler, wie sie bei Funkverbindungen auftreten. Robustheit gegenüber Störungen mit Zeit- und Frequenzschwankungen wird zwar auch von einigen Verfahren für digitale Wasserzeichen erreicht, z. B. dem von Tachibana u. a. [TSNK01]. Bislang gewährleistet jedoch kein bekanntes Verfahren gleichzeitig die Unerkennbarkeit der Existenz der eingebetteten Information [Bar05].

Das hier entwickelte Verfahren soll eine möglichst umfangreiche Nachricht unerkennbar und robust gegenüber dem zugrunde gelegten Störungsmodell einbetten, das durch die üblichen Kurzwellenbedingungen im Amateurfunk mit Rauschen, Schwund und geringer Bandbreite gekennzeichnet ist [EF87].

Die Existenz steganographischer Methoden ist ein wesentliches Argument gegen ein Verbot von Kryptographie, da Steganographie ebenfalls vertrauliche Kommunikation ermöglicht, aber nicht erkannt und somit nicht wirksam verfolgt werden kann. Dennoch wurde 1998 das Gebot der offenen Sprache im Amateurfunk auf das Inland ausgeweitet, das vorher nur im internationalen Funkverkehr galt[1]. Die neue Amateurfunkverordnung von 2005 [AFuV05] verbietet in den betrieblichen Rahmenbedingungen für Amateurfunkstellen den

*Der Autor dankt Oliver Prätor für nützliche Impulse und fruchtbare Diskussionen. Diese Arbeit wurde finanziell unterstützt durch das Air Force Research Laboratory, Rome (NY), USA, Bewilligung FA8655-04-1-3036.

[1] Vollzugsordnung für den Funkdienst zum Internationalen Fernmeldevertrag (VO Funk), Genf 1982

verschlüsselten Funkverkehr nun explizit. Dort heißt es in § 16: „Amateurfunkverkehr darf nicht zur Verschleierung des Inhalts verschlüsselt werden“.
Üblicherweise können wir bei digitaler steganographischer Kommunikation zunächst davon ausgehen, dass Nachrichten ungestört empfangen werden. So erreichen z. B. digitalisierte Bilder, die als E-Mail-Anhang versendet werden, praktisch immer fehlerfrei den Empfänger. Grundsätzlich sorgt die Sicherungsschicht für eine fehlerfreie Übertragung. Wenn jedes Bit des Trägermediums den Empfänger ungestört erreicht, dann lässt sich auch eine eventuell eingebettete steganographische Nachricht problemlos extrahieren. Bei einigen Funk-Betriebsarten (z. B. analoger Sprechfunk, Schmalbandfernsehen) wird jedoch auf die Sicherungsschicht verzichtet, weil sich die entstehenden Fehler nur geringfügig auf das Trägermedium auswirken und toleriert werden können.
Ohne Fehlerkorrektur sind Störungen nur dort erträglich, wo sie die geringsten Auswirkungen auf das Trägermedium haben, also an den irrelevanten, schlecht wahrnehmbaren Stellen eines Trägermediums. Typische steganographische Algorithmen betten jedoch mit Vorliebe in solche Stellen ein. Die eingebettete Nachricht wäre also in der Gegenwart von Störungen am meisten gefährdet. Deshalb müssen robuste Einbettungsfunktionen die Auswahl der änderbaren Stellen in Bezug auf das Verhältnis zwischen unauffälliger Änderbarkeit und Fehlergefahr optimieren sowie durch Hinzufügen von Redundanz möglichen Störungen vorbeugen. Beide Maßnahmen bewirken in ihrer Konsequenz geringere Kapazität und erhöhte Entdeckungsgefahr.
Robuste Einbettung wird oft durch Spreizspektrum-Modulation erreicht [CKLS96, MBR99]. Diese Modulation kann Informationen unterhalb des Rauschpegels zu übermitteln (Signal–Rausch-Abstand kleiner 0 dB). Es ist schwierig, das Signal zu stören, sofern die Synchronisation zwischen Sender und Empfänger erhalten bleibt. Gezielte Angriffe auf die Robustheit versuchen deshalb, das modulierte Signal zu desynchronisieren [PAK98]. Da es sich bei einer Funkübertragung um keinen gezielten Angriff zur Zerstörung des eingebetteten Inhalts handelt, können wir hoffen, einen Vorteil gegenüber den digitalen Wasserzeichen zu haben und die zusätzliche Anforderung der Steganographie, dass das Signal nicht nachweisbar sein darf, ohne Kapazitätsbeschränkung zu meistern.
Im folgenden Abschnitt 2 soll zunächst das Modell und die Simulation der Kurzwellenbedingungen beschrieben werden. In Abschnitt 3 wird ein bekanntes steganographisches Spreizspektrum-Verfahren schrittweise um Bausteine erweitert, die die Fehlerrate des steganographischen Signals verringern. Durch Simulation werden dabei sinnvolle Parameter bestimmt, die eine fehlerfreie Übertragung ermöglichen. Erste Gedanken zur Sicherheit des vorgeschlagenen Verfahrens werden in Abschnitt 4 erläutert. Dort wird auch ein kurzer Ausblick auf künftige Arbeiten gegeben.

2 Simulation einer Kurzwellenübertragung

Eine Simulation der variablen Ausbreitungsbedingungen der Ionosphäre ermöglicht gegenüber wirklichen Übertragungen nicht nur eine schnellere Prüfung im Labor während der Entwicklungsphase, sondern auch den Vergleich unter reproduzierbaren, standardisierten Bedingungen. Für die Entwicklung des vorgeschlagenen Systems wurde daher ein Simulator verwendet, der auf Quelltexten von Johan Forrer, KC7WW[2], basiert. Er wurde vom Verfasser als ein Paket namens `chansim` für R [R05] implementiert und beherrscht

[2] Diese alphanumerischen Zeichenketten hinter Namen sind Rufzeichen von Funkamateuren.

eine breite Vielfalt simulierter Bedingungen einschließlich CCIR 520-1 (good, moderate, poor, flutter-fading), siehe Tabelle 1 [CCIR90].

Tabelle 1: Voreingestellte Parameter für die Kanalsimulation

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

Das verwendete Modell ist eine Umsetzung des normalverteilt streuenden HF Ionosphärenkanalmodells von Watterson [WJB70], das üblicherweise für diese Art von Simulationen eingesetzt wird [For99].
Aus physikalischer Sicht ist der HF-Kanal durch eine zeitlich variierende Mehrwegeumgebung gekennzeichnet, die Zeit- und Frequenzdispersion erzeugt [EF87]. Der Grund für die Vielzahl der Wege liegt in den Reflektionen des Funksignals an verschiedenen Schichten in der Ionosphäre. Außerdem können Mehrfachreflektionen zwischen der Erdoberfläche und der Ionosphäre auftreten, die zu sogenannter Multi-Hop-Ausbreitung führt. Deshalb kann das empfangene Signal mehrere Echos enthalten, die einen zeitlichen Abstand von mehreren Millisekunden haben (Verzögerungszeit). Die Dopplerverschiebung (Frequenzveränderung) entsteht, wenn sich die einzelnen Pfadlängen der Mehrwegeumgebung aufgrund von Höhenverlagerungen der Reflektionsschichten verändern.
Für Funkverbindungen in mittleren Breiten kann die relative Verzögerungszeit τ_i in der Mehrwegeumgebung bis zu 6 ms betragen und die Schwundrate (Dopplerverschiebung) bis zu 5 Hz [FN01]. Typischere Werte liegen jedoch bei 2 ms bzw. 1 Hz, die die standardisierten CCIR-HF-Kanalbedingungen „poor“ kennzeichnen.
Einer der Hauptbeiträge zum Thema HF-Kanalmodellierung war der von Watterson u. a. [WJB70] aus dem Jahre 1970. In diesem Beitrag wurde ein stationäres Modell für HF-Kanäle vorgeschlagen und experimentell durch Messungen auf Funkstrecken bestätigt. Obwohl HF-Kanäle gewöhnlich nicht-stationär sind, wurde die Gültigkeit des Modells für hinreichend kurze Zeiten ($\approx$ 10 Minuten) und für begrenzte Bandbreiten ($\approx$ 10 kHz) nachgewiesen. Das Watterson-Modell sieht den HF-Kanal als ein Transversalfilter, dessen Anzapfungen komplex sind und sich mit der Zeit verändern (siehe Abbildung 1) und erzeugt Phasen- und Amplitudenverzerrungen im Signal. Die zeitlich variierenden Anzapfungen (h_i) werden durch gefiltertes komplexes weißes Rauschen parametrisiert, dessen Spektrum im Frequenzraum normalverteilt ist. Die gewünschte Dopplerverschiebung wird durch die Standardabweichung des Spektrums gesteuert.

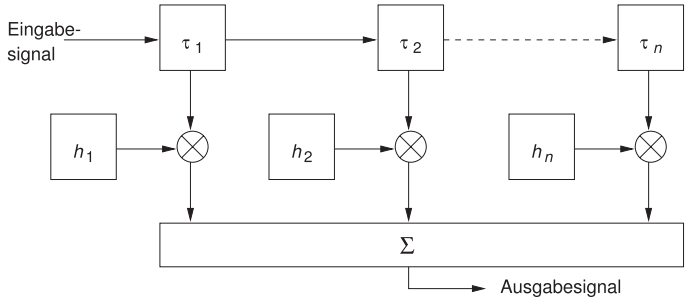

Abbildung 1: Watterson-Modell eines HF-Kanals [WJB70]

3 Systementwurf

3.1 Schmalbandfernsehen

Schmalbandfernsehen (Slow Scan Television, SSTV) hat eine gegenüber dem Sprechfunk vergleichsweise lange Sendephase. So kann trotz der geringen Bandbreite von nur 3 kHz eine angemessene steganographische Kapazität erreicht werden. Schmalbandfernsehen ist sehr verbreitet unter Funkamateuren.
Ein SSTV-Signal startet mit einem VIS-Kode[3], der eine Bildübertragung und die verwendete Betriebsart ankündigt. Sein Frequenz–Zeit-Diagramm ist in Abbildung 2 dargestellt.

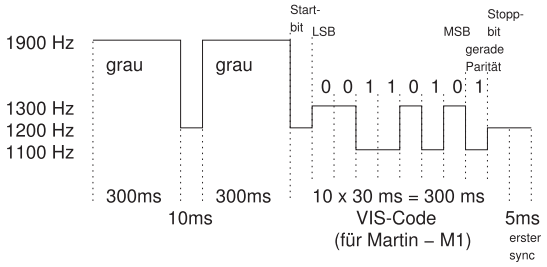

Abbildung 2: VIS-Kode zur Ankündigung einer SSTV-Übertragung und der Betriebsart [Wum97]

Es gibt ungefähr 30 verschiedene SSTV-Modi. Martin-M1 wurde von Martin H. Emmerson, G3OQD, entwickelt und ist eine der am häufigsten verwendeten.
Die Betriebsart Martin-M1 kodiert Farbbilder mit einer Auflösung von 320×256 Bildpunkten. Das Bild wird zeilenweise, von oben beginnend, übertragen. Für jede Zeile gibt es einen Synchronisationsimpuls, gefolgt von der Intensitätsinformation des grünen, blauen und roten Farbkanals. Die Intensitäten werden als Töne übertragen im Bereich von $1400 \ldots 2400$ Hz (siehe Abbildung 3). Ein 1200-Hz-Ton dient als Synchronimpuls. Insgesamt dauert das SSTV-Signal 1 Minute und 55 Sekunden, eventuell erweitert um das Rufzeichen des Senders in CW (Morsezeichen, continuous wave).
Die Suche nach der geeignetsten Open-Source-SSTV-Software als Grundlage für die Implementierung des steganographischen Systems führte zu QSSTV [Mae05] von Johan

[3] Diese Bezeichnung wurde vom Wetterfax übernommen: VIS=visible, IR=infrared

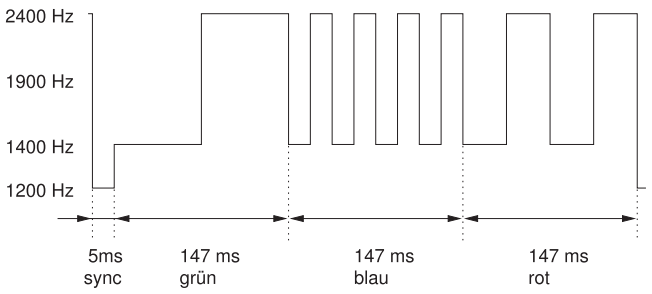

Abbildung 3: Eine von 256 Zeilen im Martin-M1-Modus [Wum97]

Maes, ON4QZ. Viele Alternativen gibt es nicht, denn die Mehrzahl der SSTV-Programme wird ohne Quelltext angeboten oder setzt die SSTV-Spezifikation nur rudimentär um.
Im Rahmen der hier beschriebenen Experimente wurde QSSTV um den bereits erwähnten Kanalsimulator von Johan Forrer, KC7WW, erweitert. Eine simulierte Übertragung dauert nur etwa eine Sekunde und ist damit viel schneller als eine echte (zweiminütige) Übertragung. Das von QSSTV generierte SSTV-Signal hat eine Abtastrate von 8000 Werten pro Sekunde. Das ist ausreichend, da ein Funkkanal nur das Band von $200 \ldots 3000$ Hz überträgt.

3.2 Steganographisches SSTV-System

Dieser Abschnitt beschreibt den Signalfluss im Gesamtsystem (siehe Abbildung 4). Zuerst wird die Nachricht durch einen fehlerkorrigierenden Kode mit Redundanz versehen, um die Verluste durch Schwund und atmosphärische Störungen auszugleichen, die wir anders nicht verhindern können. Der Interleaver, der die Nachricht permutiert, beugt Bündelfehlern vor. Der differenzielle Kodierer ermöglicht auch wenn das Signal aufgrund von Phasenstörungen mit falschem Vorzeichen empfangen wird eine korrekte Demodulation. Die entstehenden Symbole werden gespreizt und ihre Energie wird über einen längeren Zeitraum verstreut. Impulsformung mit einem RRC-Filter (root raised cosine) begrenzt die Bandbreite des gespreizten Signals, das mit relativ kleinem Pegel ($-27 \ldots -11$ dB) zum SSTV-Signal addiert wird und deshalb schwer nachzuweisen ist. Die Summe beider Signale wird zum Empfänger übertragen. In der hier verwendeten Experimentalumgebung wurden die Funkbedingungen in reproduzierbarer Weise simuliert. Im wirklichen Einsatz würde das Signal mit seiner Abtastrate von 8000 Hz durch die Soundkarte des Rechners in ein analoges Audiosignal gewandelt werden und anschließend mit einem SSB-Kurzwellensender (single side band) ausgestrahlt. Der Kurzwellenempfänger der Gegenstelle würde ebenfalls mit einer Soundkarte im Empfangsrechner verbunden sein, wo das Signal digitalisiert und weiterverarbeitet wird. Das digitalisierte Signal kann auch von der Ausgabe des Kanalsimulators der Experimentalumgebung abgegriffen werden. Es ist ein gewöhnliches SSTV-Signal und sein Bildinhalt kann auf übliche Weise demoduliert werden. Die Synchronisationsinformation des SSTV-Signals stellt sicher, dass der Empfänger auch den Start des potenziellen steganographischen Inhalts ermitteln kann. Bevor das steganographische Signal empfängerseitig demoduliert wird, muss ein passendes RRC-Filter angewendet werden, um die Interferenz zwischen den Elementen der Spreizfolge

(Chips) zu reduzieren. Der Entspreizer gewinnt die Energie der einzelnen binären Zeichen der steganographischen Nachricht zurück. Er benötigt dazu die Schlüsselinformation, die beim Sender verwendet wurde. Die differenzielle Dekodierung korrigiert die Nachricht, wenn das Signal negativ empfangen wird, und der De-Interleaver gepaart mit dem Turbodekoder versucht die übrigen Fehler im Signal zu beseitigen. Dieser nutzt den Pegel der empfangenen Symbole als Maß für die Zuverlässigkeit (Soft-Decision-Dekodierung, siehe Abschnitt 3.7).

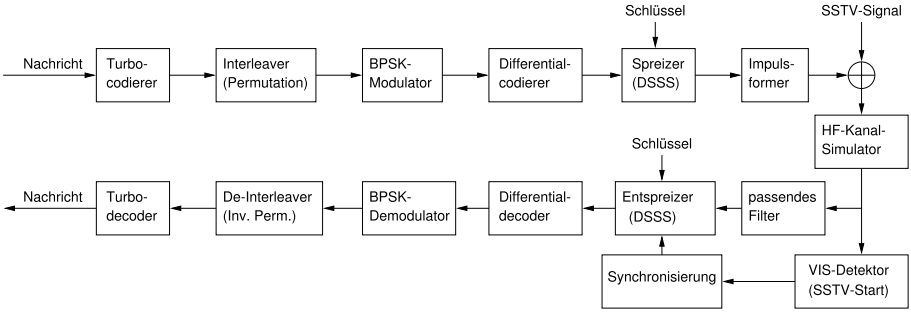

Abbildung 4: Signalweg im steganographischen SSTV-System

3.3 Reines Direct Sequence Spread Spectrum (DSSS)

DSSS wandelt die einzubettende Nachricht m durch Multiplikation mit einer Spreizfolge n in die Einbettungsfolge $s = mn$ um (siehe Abbildung 5). Hier wird eine lange Spreiz-

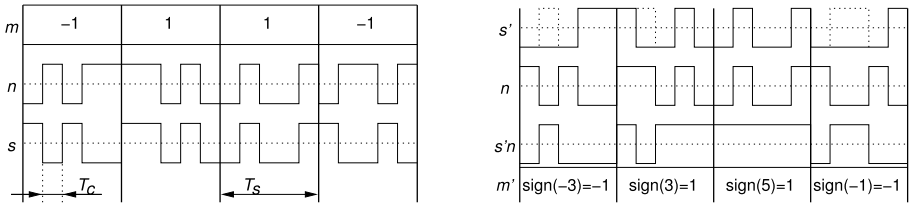

Abbildung 5: DSSS-Modulation (links) und -Demodulation nach Störung (rechts)

folge n verwendet, die für alle Symbole pseudozufällig vom Schlüssel abgeleitet wird. Die einzelnen Elemente der Spreizfolge heißen *Chips* und haben eine Dauer T_c. Die Symboldauer T_s ist ein ganzzahliges Vielfaches von T_c. Die Einbettungsfolge s wird mit einer gewissen Wichtung g (Modulationsgrad) zum Trägersignal c addiert, wodurch sich das Steganogramm $c_s = c + gs$ ergibt. Beim Empfänger wird die Nachricht aus dem gestörten Signal c'_s extrahiert, indem $c'_s n$ stückweise über die Symboldauer T_s integriert wird.[4]
In der folgenden ersten Untersuchung werden die Länge der Spreizfolge und der steganographische Rauschabstand variiert und dabei die Bitfehlerrate (bit error rate, BER) gemessen. Dieses Experiment wurde für verschiedene Funkbedingungen wiederholt. Abbildung 6 zeigt die Bitfehlerrate als eine physische Landkarte. Horizontal ist der Spreizfaktor

[4] In Abbildung 5 wird vereinfachend aus der gestörten Einbettungsfolge demoduliert.

(logarithmisch fallend) abgetragen, und vertikal der steganographische Rauschabstand (in Dezibel). In den Diagrammen ist also rechts die Kapazität am größten und oben die Nachweisbarkeit am geringsten. Durch Fehler dominierte Gebiete (BER $\approx 50\,\%$) sind weiß, hohe Bitfehlerraten sind braun, geringe grün und fehlerfreie Bereiche blau dargestellt.

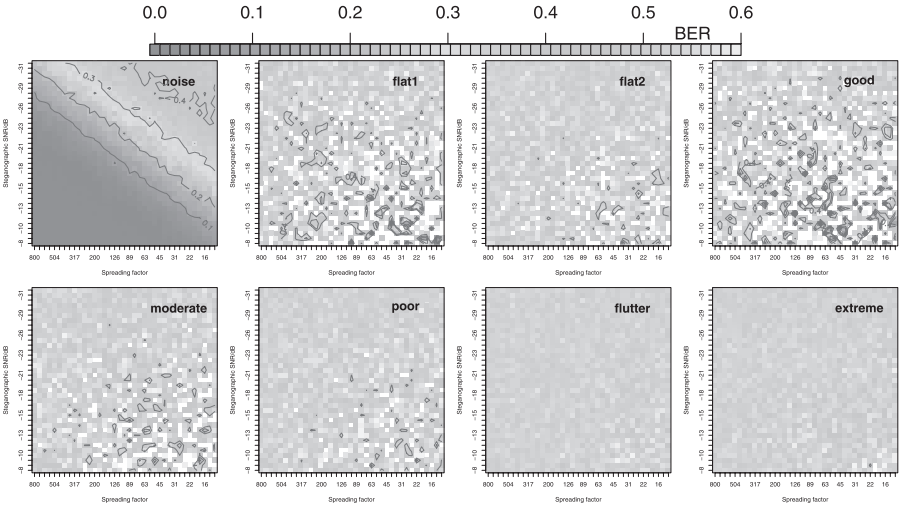

Abbildung 6: Direct Sequence Spread Spectrum (DSSS)

Wie erwartet, überlebt reines DSSS nur den AWGN-Kanal (additive white Gaussian noise, „noise“) teilweise fehlerfrei [MBR99], der als Bedingung für Kurzwellenübertragungen eher unwahrscheinlich ist. Der Rauschabstand im Kanal wurde auf $26\,\mathrm{dB}$ gesetzt. Die anderen simulierten Bedingungen verursachen Bitfehlerraten um den Mittelwert $0{,}5$ mit unterschiedlicher Streuung. Das ist auf die Phasenverschiebung zurückzuführen, die bei einem schwundbehafteten Mehrwegekanal entsteht.

3.4 Differenzielle Kodierung

Das übertragene Signal wird komplex gestört, d. h. seine Phase wandert und seine Amplitude ist Rayleigh-verteilt [Rap96]. Da die Amateurfunktechnologie nur den reellen Teil empfängt und die Phasenlage somit nicht abschätzbar ist, lässt sich keine Kanalentzerrung vornehmen. Es wird die BPSK-Modulation (binary phase shift keying) angewendet, da andere wie QPSK (quadrature phase shift keying) und n-QAM (quadrature amplitude modulation) ein komplexes Signal voraussetzen. Absolut kann die Phase jeden beliebigen Wert von 0 bis 360° annehmen. Deshalb ist die Bitfehlerrate ungefähr $0{,}5$. Die relative Änderung der Phase je Symbol ist jedoch nur gering. Der Schlüssel zu einer fehlerfreien Übertragung über einen Kanal mit (langsam) drehender Phasenlage ist differenzielle Demodulation [Cou01]. Abbildung 7 zeigt die demodulierte Folge von 4000 bei schlechten Bedingungen („CCIR poor“) übertragenen Impulsen (korrekter Empfang positiv und fehlerhafter Empfang negativ dargestellt). Die graue Kurve stellt die analoge Signalintensität dar, die schwarze deren Vorzeichen.
Man kann die durchgängig falschen Signalteile mittels differenzieller Kodierung in ein

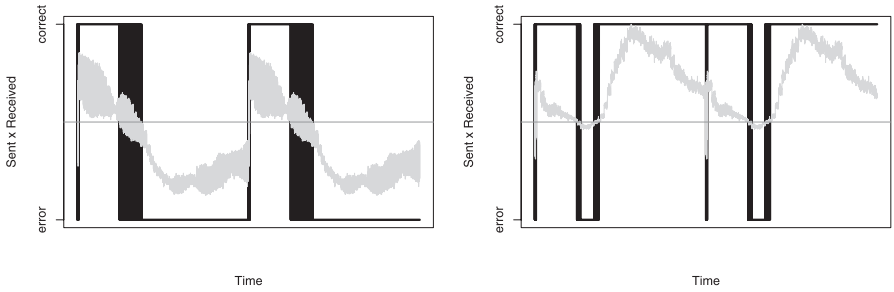

Abbildung 7: Bündelfehler durch Phasenverschiebung (links) und Verbesserung durch differenzielle Demodulation (rechts)

korrektes Signal wandeln. Diese Kodierung stellt sicher, dass das Signal zu einem bestimmten Zeitpunkt nicht absolut interpretiert wird, sondern in Abhängigkeit vom vorhergehenden Zeitpunkt. Das Signal wird also relativ interpretiert und ist, abgesehen von Abtastwerten bei Auslöschung, korrekt. Eine Folge $\vec{a}$ logischer Werte (*wahr* kodiert als -1 und *falsch* als 1) wird durch folgende Regeln in eine differenziell kodierte Folge $\vec{b}$ umgewandelt und wieder dekodiert:

$$b_k = \prod_{i=1}^{k} a_i = \begin{cases} k = 1: & a_1 \\ k > 1: & a_k \cdot b_{k-1} \end{cases} \qquad a_k = \begin{cases} k = 1: & b_1 \\ k > 1: & b_k \cdot b_{k-1} \end{cases}$$

Durch die differenzielle Kodierung haben sämtliche Bedingungen mit Dopplerverschiebung eine verringerte Fehlerrate. Nur beim reinen AWGN-Kanal (noise) erhöht die differenzielle Kodierung die Fehlerwahrscheinlichkeit, da einzelne Bitfehler sich nach der Dekodierung doppelt auswirken. Fehlerfreie Übertragungen werden durch die differenzielle Kodierung nicht beeinflusst.

3.5 Fehlerkorrigierende Kodierung

Um den schwundbedingten Verlust auszugleichen, wird hier eine fehlerkorrigierende Kodierung angewendet, die auf einer Implementierung von Turbokodes für ein OFDM-Soundmodem (orthogonal frequency division multiplexing) basiert [Wal98]. Diese Implementierung gestattet Koderaten[5] im Bereich $\frac{1}{3} \ldots 1$. In den folgenden Experimenten wird die kleinstmögliche Koderate von $\frac{1}{3}$ verwendet. Leider konnte bei dieser Rate keine Konfiguration für fehlerfreie Übertragung unter den Bedingungen „flutter“ und „extreme“ gefunden werden; offensichtlich müsste die Koderate noch geringer sein. Aus Abbildung 8 lassen sich die optimalen Parameter für geringste Nachweisbarkeit abschätzen. Diese sind in Tabelle 2 aufgelistet. Die angegebenen steganographischen Rauschabstände wurden am ungestörten Signal ermittelt, auf das der Angreifer keinen Zugriff hat.
Wir können sehen, dass die geringste Fehlerrate nicht immer für den größten Spreizfaktor erwartet wird. Der Grund dafür ist die erhöhte Wahrscheinlichkeit eines Vorzeichenwechsels aufgrund von Phasenstörungen in langen Symbolen (die bei großen Spreizfaktoren entstehen). Andererseits verringert sich der beim Entspreizen erwartete Gewinn bei kürze-

[5] Verhältnis der Anzahl der Informationsbits zur Anzahl der Bits im Kodewort

ren Symbolen (kleineren Spreizfaktoren) und der Einfluss des SSTV-Signals (Trägermedium) auf das eingebettete Signal nimmt zu.

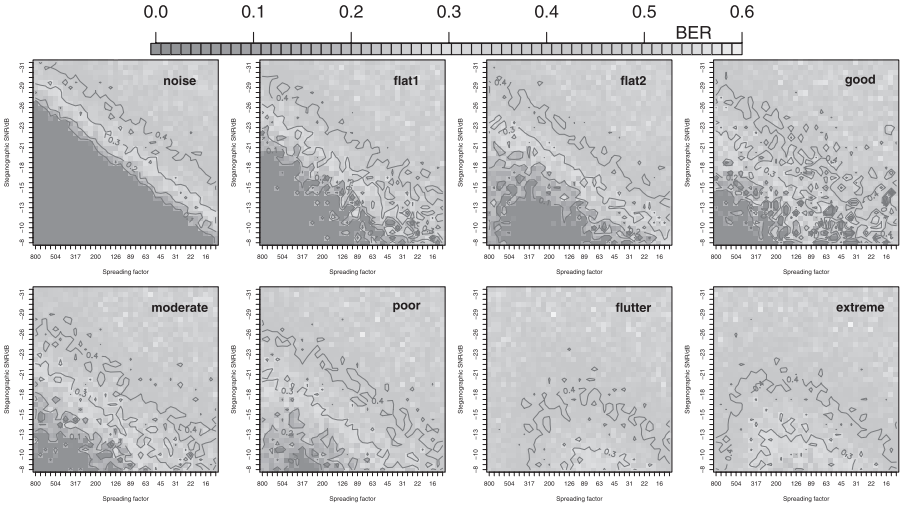

Abbildung 8: Direct sequence spread spectrum (DSSS) mit differenzieller Kodierung und Turbokode

Tabelle 2: Optimale Parameter für SSTV-Steganographie

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

3.6 Senderseitige Impulsformung und passendes Empfangsfilter

Die Spreizfolge besteht aus einer Folge von Rechteckimpulsen mit vertikalen Flanken, die unendliche Bandbreite belegen. Das Nyquist-Kriterium besagt, dass Rechteckimpulse nicht verlustfrei über einen Bandbreiten-beschränkten Kanal übertragen werden können [SS68]. Eine SSTV-Übertragung ist auf das Band von 200 Hz . . . 3000 Hz begrenzt. Um Verluste zu vermindern, wird ein RRC-Filter (root raised cosine) zur Impulsformung angewendet, das das Spektrum begrenzt [LM94]. Die Symbole sind Elemente der Spreizfolge und haben eine Dauer T, die in unserem Fall gleich der Chipdauer T_c ist. Der RRC hat

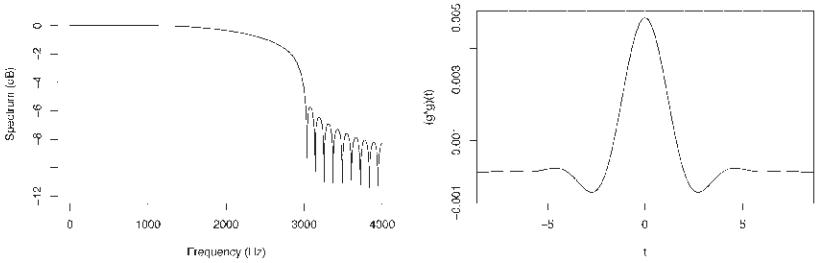

Abbildung 9: Spektrum eines beschnittenen RRC-Filters mit $\alpha = \frac{1}{2}$ und $T = 2$ (links) und Impulsantwort eines passenden Paares von RRC-Filtern (rechts)

einen Parameter $\alpha = 2f_{\mathrm{og}}T_c - 1$, genannt Roll-Off-Faktor. Dieser kann die obere Grenzfrequenz f_{og} für die Chipdauer T_c in bestimmten Grenzen verschieben. Da sich die Amplitude des RRC nach beiden Seiten verringert, kann ein Schwellwert ε festgelegt werden, ab welchem der RRC abgeschnitten und damit auf eine endliche Dauer begrenzt wird.
Für ein RRC-Filter (Roll-Off-Faktor $\alpha = \frac{1}{2}$, Chipdauer $T_c = 2$ Abtastwerte) zeigt Abbildung 9 (links) das Spektrum. Das Signal wird vor der Übertragung durch dieses Filter geformt und durch dessen obere Grenzfrequenz $f_{\mathrm{og}} = 3000\,\mathrm{Hz}$ in der Bandbreite beschränkt.
Um die erste Nyquist-Bedingung zu erfüllen (keine Intersymbolinterferenz), muss die Symboldauer T die erste Nullstelle der Impulsantwort des Filters sein. Zugleich soll der Rauschabstand maximiert werden, was für reelle Signale identische Sende- und Empfangsfilter erfordert. Die Kombination aus zwei RRC-Filtern bildet ein RC-Filter (raised cosine). Abbildung 9 (rechts) zeigt, dass die Impulsantwort der Kombination die Bedingung $t/T = 0$ für alle Zeitpunkte $t \neq 0$ erfüllt. Folglich stört ein Symbol nicht seine Nachbarn zu deren Abtastzeitpunkten.

3.7 Soft-Decision Dekodierung

Abbildung 10 zeigt den Gewinn durch die Impulsformung (Mitte) verglichen mit der Modulation von Rechteckimpulsen (links). Es kann eine kleine Zunahme von 18 auf 22 fehlerfreie Übertragungen unter schlechten Funkbedingungen (poor) registriert werden. Wenn nicht nur das Vorzeichen des Signals, sondern auch sein Pegel als Maß für seine Zuverlässigkeit ausgewertet wird, dann nimmt die Zahl der fehlerfreien Übertragungen wiederum von 22 auf 27 leicht zu.

4 Sicherheitsbetrachtung und Ausblick

Die Simulationen haben gezeigt, dass schmalbandige Verbindungen, wie sie Funkamateure auf Kurzwelle nutzen, die nicht nur additivem Rauschen, sondern auch dynamischen Phasen- und Frequenzgangverzerrungen ausgesetzt sind, für die Übermittlung spreizspektrummodulierter eingebetteter Nachrichten genutzt werden können. Die Experimente wurden mit dem Ziel durchgeführt, die physikalischen Grenzen für dieses Szenario zu bestimmen. Dabei wurden einige Zehntausend Funkverbindungen simuliert, die mit verschiedenen Parameterkombinationen von steganographischem Rauschabstand und steganogra-

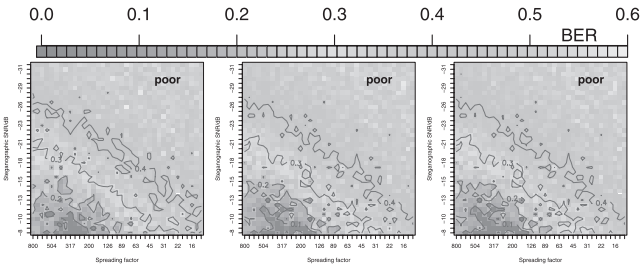

Abbildung 10: Direct sequence spread spectrum (DSSS) mit differenzieller Kodierung und Turbokode bei schlechter Funkbedingung (CCIR-poor) mit Hard-Decision-Dekodierung (links), zusätzlicher Impulsformung und passender emfängerseitiger Filterung (Mitte) und Soft-Decision-Dekodierung (rechts)

phischer Kapazität miteinander unter reproduzierbaren, standardisierten Kurzwellenbedingungen verglichen wurden.

Ein Angreifer steht vor der Aufgabe, die Existenz einer steganographischen Nachricht nachzuweisen, d. h. Nachrichten mit und ohne Steganographie voneinander zu unterscheiden. Die Unterscheidung muss anhand des steganographischen Rauschens erfolgen, das entweder vorhanden ist oder nicht. Dieses Rauschen müsste getrennt werden von anderen vorhandenen Rauschquellen: dem Rauschen in der Bildvorlage, dem Rauschen der Sendeanlage, dem atmosphärischen Grundrauschen und dem Kanalrauschen, also den Störungen, denen das Signal auf dem Weg ausgesetzt wird.

Ein Angreifer kann durch die Wahl einer günstigen geographischen Position, einen empfindlicheren Empfänger oder eine Antenne mit höherem Gewinn und besserer Richtcharakteristik einen relativen Vorteil gegenüber dem Empfänger erlangen. Letztlich wird die Frage der Sicherheit dadurch entschieden, ob der Vorteil des Empfängers, der darin besteht, dass die Symbolenergie über einen längeren Zeitraum mit einer geheimen Spreizfolge verteilt wird, ausreichend ist, um sich vor einem Angreifer in bestmöglicher Situation zu schützen. Wie die Messungen gezeigt haben (vgl. Abschnitt 3.5, gibt es für den Spreizfaktor ein Optimum. Deshalb lässt sich die Kapazität nicht ohne weiteres zugunsten eines größeren steganographischen Rauschabstands verringern. Ein Vorteil ist, dass zur Synchronisation zwischen Sender und Empfänger keine zusätzliche Redundanz zum eingebetteten Signal hinzugefügt werden musste, da im Trägersignal bereits genügend Synchronisationsimpulse vorhanden sind. Die Zeit vor dem ersten Zeilensynchronsignal und nach Ende der eingebetteten Nachricht sollte für ein sanftes Abklingen des steganographischen Rauschpegels genutzt werden, da abrupte Änderungen leichter nachweisbar sind.

Es könnte versucht werden, eine steganalytische Methode vom Doppelspitzen-Histogrammangriff (Twin Peaks) auf digitale Wasserzeichen [Mae98] abzuleiten. Dieser beruht darauf, dass sich im Histogramm auftretende Spitzen nach Addition einer Spreizfolge $\{-d, +d\}^n$ verdoppeln. Der Angriff ist stark vom Bild abhängig, da der Effekt nur bei Histogrammen mit Spitzen erkannt wird. Im Unterschied zum SSTV-Szenario kann der Angreifer auf ein ungestörtes markiertes Bild zugreifen. Spitzen im Histogramm können in SSTV-Signalen zwar nicht ausgeschlossen werden, sie werden jedoch durch die Übertragungsstrecke „breitgeschliffen“. Da das SSTV-Signal den Angriff stört, wurde mit reinen

Spreizfolgen experimentiert, deren Histogramm genau zwei Spitzen bei $-d$ und $+d$ hat. Nach simulierter Übertragung war die Verteilung – abgesehen vom AWGN-Kanal (noise) – stets unimodal. Eine Übertragung bei Sichtkontakt ähnelt zwar einem AWGN-Kanal, unterliegt aber dennoch Schwund (Rice-Fading) [Rap96]. Ob ein Angriff bei Sichtkontakt tatsächlich erfolgreich ist, muss in der Praxis untersucht werden.
Die Sicherheit des entwickelten Systems lässt sich nur schwer vergleichen, da robuste Steganographie für Funksignale noch Neuland ist und auch keine Angriffe als Benchmark existieren, die die steganographische Sicherheit in der Simulationsumgebung bewerten könnten. Das Laborszenario muss im Rahmen künftiger Arbeiten in die Realität umgesetzt und an echten Sende- und Empfangsanlagen validiert werden.

Literatur

[AFuV05] Bundesministerium für Wirtschaft und Arbeit. Verordnung zum Gesetz über den Amateurfunk, 2005. Online verfügbar unter `http://bundesrecht.juris.de/bundesrecht/afuv_2005/gesamt.pdf`.

[Bar05] Mauro Barni. E-Mail-Kommunikation, November 2005.

[CCIR90] CCIR. Recommendation 520-1, Use of High Frequency Ionospheric Channel Simulators. *Recommendations of the CCIR*, III:57–58, 1990.

[CKLS96] Ingemar J. Cox, Joe Kilian, Tom Leighton und Talal Shamoon. A Secure, Robust Watermark for Multimedia. In Ross J. Anderson (Hrsg.), *Information Hiding (1st International Workshop)*, LNCS 1174, S. 185–206, Berlin Heidelberg, 1996. Springer Verlag.

[Cou01] Leon W. Couch II. *Digital and Analog Communication Systems*. Prentice Hall, Upper Saddle River, NJ, 2001.

[EF87] Evangelos Eleftheriou und David D. Falconer. Adaptive Equalization Techniques for HF Channels. *IEEE Journal on Selected Areas in Communications*, 5:238–247, 1987.

[FN01] William N. Furman und John W. Nieto. Understanding HF Channel Simulator Requirements in Order to Reduce HF Modem Performance Measurement Variability. In *Proceedings of HF01, the Nordic HF Conference*, Fårö, Sweden, 2001. Online verfügbar unter `http://www.nordichf.org/index.htm?forms/cdrom.htm&2`.

[For99] Johan B. Forrer. A Low-Cost HF Channel Simulator for Testing and Evaluating HF Digital Systems. In *Proceedings of the 18th ARRL and TAPR Digital Communications Conference*, Phoenix, Arizona, 1999. Online verfügbar unter `http://www.tapr.org/pub_dcc18.html`.

[LM94] Edward A. Lee und David G. Messerschmitt. *Digital Communications*. Kluwer Academic Publishers, Boston, 1994.

[Mae98] Maurice Maes. Twin Peaks: The Histogram Attack to Fixed Depth Image Watermarks. In David Aucsmith (Hrsg.), *Information Hiding (2nd International Workshop)*, LNCS 1525, S. 290–305, Berlin Heidelberg, 1998. Springer Verlag.

[Mae05] Johan Maes. QSSTV, 2005. Online verfügbar unter `http://users.telenet.be/on4qz/qsstv/`.

[MBR99] Lisa M. Marvel, Charles G. Boncelet und Charles T. Retter. Spread Spectrum Image Steganography. *IEEE Transactions on Image Processing*, 8:1075–1083, 1999.

[PAK98] Fabien A. P. Petitcolas, Ross J. Anderson und Markus G. Kuhn. Attacks on copyright marking systems. In David Aucsmith (Hrsg.), *Information Hiding (2nd International Workshop)*, LNCS 1525, S. 219–239, Berlin Heidelberg, 1998. Springer Verlag.

[R05] R Development Core Team. *R: A language and environment for statistical computing*. R Foundation for Statistical Computing, Vienna, Austria, 2005. ISBN 3-900051-07-0, Online verfügbar unter `http://www.R-project.org`.

[Rap96] Theodore S. Rappaport. *Wireless Communications: Principles and Practice*. IEEE Press, Piscataway, NJ, USA, 1996.

[SS68] Roberto Saucedo und Earl E. Schiring. *Introduction to Continuous and Digital Control Systems*. Macmillan, New York, 1968.

[TSNK01] Ryuki Tachibana, Shuichi Shimizu, Taiga Nakamura und Seiji Kobayashi. An Audio Watermarking Method Robust Against Time- and Frequency-Fluctuation. In Edward J. Delp und Ping W. Wong (Hrsg.), *Security, Steganography and Watermarking of Multimedia Contents III (Proc. of SPIE)*, S. 104–115, San Jose, CA, January 2001.

[Wal98] Mathys Walma. BCJR turbo code encoder/decoder, 1998. Online verfügbar unter `http://cvs.berlios.de/cgi-bin/viewcvs.cgi/ofdm/soundmodem/newqpsk/turbo.c?rev=HEAD`.

[WJB70] Clark C. Watterson, John R. Juroshek und William D. Bensema. Experimental Confirmation of an HF Channel Model. *IEEE Transactions on Communication Technology*, 18:792–803, 1970.

[Wum97] Wumpus. Einige SSTV-Modi, 1997. Online verfügbar unter `http://home.snafu.de/wumpus/sstvmod.htm`.