Angriffe auf eine Spreizspektrummethode für Audio-Steganographie

Andreas Westfeld
Hochschule für Technik und Wirtschaft Dresden
01069 Dresden, Friedrich-List-Platz 1

Abstract: Steganographie ist eine Technik zur vertraulichen Kommunikation. Ihre Sicherheit definiert sich über das Unvermögen des Angreifers, die Existenz einer vertraulichen Kommunikation nachzuweisen.

Ziel dieses Beitrags ist es, einige Analysemuster für Schwachstellen am Beispiel einer veröffentlichten Spreizspektrummethode für Steganographie in Audiomedien (Nutzinger und Wurzer, ARES 2011) vorzustellen. Einige Schwächen werden gefunden und beseitigt.

1 Einführung

Steganographie ist die Kunst und Wissenschaft der verdeckten Kommunikation. Ihr Zweck ist die Übertragung von Informationen, die in einem Trägermedium sicher versteckt sind. Sichere *Wasserzeichen*verfahren betten zwar kurze Nachrichten robust ein. Denn diese sollen bis zu einem gewissen Grade gegen verändernde Angreifer, etwa Nutzer, die das Wasserzeichen entfernen wollen, geschützt werden. In der Regel hinterlassen Wasserzeichenverfahren jedoch leicht nachweisbare Spuren. Dagegen lässt sich zwar die Existenz sicherer *steganographischer* Nachrichten nicht nachweisen, üblicherweise sind diese jedoch selten robust eingebettet. Denn der Empfänger der steganographischen Nachricht hat selbst grundsätzlich kein Interesse, die Nachricht vor dem Empfang zu stören. Für hinreichenden Schutz auf dem Übertragungsweg kann die Netz-Sicherungsschicht sorgen – unabhängig davon, ob eine Nachricht eingebettet wurde und mit welcher Robustheit.

Bei Internet-Telefonie ist eine möglichst geringe Verzögerungszeit wichtiger als eine vollständige Fehlerkorrektur. Zugunsten einer niedrigen Latenz wird unbestätigt übertragen. Verlorene, verzögerte oder fehlerhaft übertragene Pakete werden nicht erneut gesendet und verlangsamen daher die Laufzeit nicht. Wegen der Redundanz des gesprochenen Wortes und durch die fehlermindernde Wirkung der Codierung ist ein Telefonat dennoch ohne nennenswerte Beeinträchtigung möglich. Auch bei einigen Funkbetriebsarten (z. B. analoger Sprechfunk, Schmalbandfernsehen) wird auf Fehlerkorrektur verzichtet, weil sich die entstehenden Fehler nur geringfügig auf das Trägermedium auswirken und toleriert werden können.

Überwiegend können wir bei digitaler steganographischer Kommunikation 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. Wenn jedes Bit des Trägermediums den Empfänger ungestört erreicht, dann lässt sich auch eine eventuell eingebettete steganographische Nachricht problemlos extrahieren.

Ohne Fehlerkorrektur (z. B. Internet-Telefonie, analoge Funkbetriebsarten) sind Störungen nur dort erträglich, wo sie die geringsten Auswirkungen auf das Trägermedium haben, also an den irrelevanten, für unsere Sinne 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 dort 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.

Dieser Beitrag beschäftigt sich mit einem steganographischen Verfahren, das dennoch robust ist, nicht gegen absichtliche Störungen eines Angreifers, aber gegen unbeabsichtigte, zufällige Kanalfehler, wie sie im Zusammenhang mit Telefonie auftreten.

Diese im Vergleich zu digitalen Wasserzeichen beschränkte Robustheit ermöglicht höhere Kapazität, z. B. verglichen mit dem Verfahren von Tachibana und Kollegen [TSNK01] eine viermal größere geheime Nachricht in einem Trägermedium, das nur ein Fünfzigstel der Bandbreite benötigt. Wie es um die Sicherheit bestellt ist, soll in diesem Papier näher untersucht werden.

Beispiele für robuste Steganographie sind eher selten und verwenden in den meisten Fällen digitale Bilder als Trägermedium. Marvel und Kollegen entwickelten ein robustes steganographisches Verfahren für Bilder [MBR99] auf der Basis von Spreizspektrum-Modulation [PSM82]. Damit lassen sich Informationen unterhalb des Störpegels übertragen. Weitere Beispiele sind Verfahren für Slow-Scan-Television-Signale (SSTV) [Wes06] oder in Audiosignalen.

Dieser Beitrag untersucht ein Spreizspektrumverfahren für Steganographie in Audiomedien, das von Nutzinger und Kollegen 2010 eingeführt [NFM10] und von Nutzinger und Wurzer 2011 implementiert wurde [NW11]. Dieses Verfahren überlebte verschiedene Robustheitstests seiner Entwickler wie additives Rauschen, variable Zeitverzögerung, variable Frequenzverschiebung, GSM-Kodierung, akustische Übertragung, Neuabtastung und Schnitt. Es verursachte auch keine nennenswerte Veränderung der wahrnehmbaren Störungen bei Hörtests im Vergleich zum Originalsignal [NW11].

Ziel dieses Beitrags ist, wie der Titel nahelegt, nicht die Beschreibung oder der Nachweis der Sicherheit eines neuen steganographischen Verfahrens, sondern die Demonstration häufig auftretender Schwächen am Beispiel einer bereits in der Literatur evaluierten Implementierung, wenngleich die vorgeschlagene Mängelbeseitigung unter bestimmten

Voraussetzungen zu einem brauchbaren Ergebnis führen kann. Einige dieser Voraussetzungen können wir als Angreifer bestimmen. Dennoch sagt das wenig über die Risiken bei einem ernsthaften Einsatz des Verfahrens. Es ist gut möglich, dass sich einige der hier beschriebenen Angriffe erfolgreich auf andere steganographische (Audio-)Methoden übertragen lassen. Dennoch waren die Entwickler sich dieser Angriffe bei ihrer eigenen, nicht minder aufwändigen Evaluation nicht bewusst. Zwar kann der Steganograph manche Schwäche ausräumen, indem er eine geeignete Trägermedien-Quelle wählt. Dennoch ist beim vorliegenden Sicherheitsniveau kein universeller Detektor nötig, der sämtliche Quellen unterscheiden kann. Es ist immer ratsam, die Ursache der Schwächen zu ermitteln und die dafür verantwortlichen Teile zu überarbeiten.

Im folgenden Abschnitt werfen wir zunächst einen Blick auf das Spreizspektrumverfahren und seine Motivation, stellen anschließend die gefundenen Schwächen vor, die in Abschnitt 4 beseitigt werden. Abschnitt 5 beschließt den Beitrag.

2 Spreizspektrumverfahren

Der steganographische Algorithmus nutzt das Audiosignal eines Telefongesprächs als Trägermedium. Es ist zunächst nicht wichtig, ob es ein VoIP-Telefonat ist oder eine mobile Konversation über GSM oder UMTS, und die Anwendung ist auch nicht auf solche Audiosignale beschränkt. Die Nachricht wird in die dekodierten Audiodaten eingebettet. Die ursprüngliche Idee war, direkt in die analoge Information einzugreifen, aus praktischen Gründen also so nah wie möglich an der Quelle anzusetzen. Damit verband man wohl die Hoffnung, dass Schwächen der Steganographie, die überwiegend durch unvollkommene digitale Einbettungsfunktionen verursacht werden, z. B. das Überschreiben niederwertigster Bits, vermieden werden.

Beim Spreizspektrumverfahren wird die einzubettende Information in ein möglichst breitbandiges, dafür sehr schwaches pseudozufälliges Signal (Pseudorauschen, pseudo noise, PN-Folge), über einen längeren Zeitraum gespreizt. Nun ist die Bandbreite in dem für Telefonate typischen Übertragungskanal stark beschränkt. Das „breitbandige“ Rauschen wird, da ein Informationsverlust nicht gewollt ist, entsprechend schmalbandig ausfallen und vor allem über die Zeit gespreizt. Die Beschreibung bleibt an dieser Stelle aus dramaturgischen Gründen offen, weil am Anfang der Untersuchung kaum Informationen – zumindest nicht die konkrete Implementierung [NW11] – zur Verfügung standen.

3 Angriffe

Vor der Suche nach hinterlassenen Einbettungsspuren ist es sinnvoll, zunächst möglichst viele Informationen über das Verfahren zusammenzutragen. Der Verfasser musste je-

doch (unfreiwillig) den Angreifer in zwei unterschiedlichen Situationen spielen. Es war zunächst unklar, ob der Auftraggeber des Einbettungsprogramms der Untersuchung des Programms zustimmen würde. So war in der ersten Phase zunächst weder der C++-Quelltext noch die ausführbare Datei verfügbar. Lediglich eine kleine Anzahl aufgezeichneter Telefonate (WAV-Dateien) stand in verschiedenen Versionen zur Verfügung:

- ohne eingebettete Nachricht (Original) und
- mit eingebetteter Nachricht unter Verwendung verschiedener Konfigurationen (bezeichnet mit „amp“, „bpsk“ und „phase“) unter welchen die beste herausgefunden werden sollte.

Es war bekannt, dass die Nachrichten mit einer Art Spreizspektrumverfahren eingebettet wurden.

3.1 Zwillingsspitzen?

Soweit die genaue Implementierung unbekannt war, wurde ein einfacher DSSS-Algorithmus (direct sequence spread spectrum) unterstellt. Der Verfasser hoffte, dass wenigstens eine der drei Konfigurationen („amp“, „bpsk“ und „phase“) nahe genug an dieser sicherlich vereinfachenden Annahme liegt. Abbildung 1 zeigt ein konkretes Beispiel für

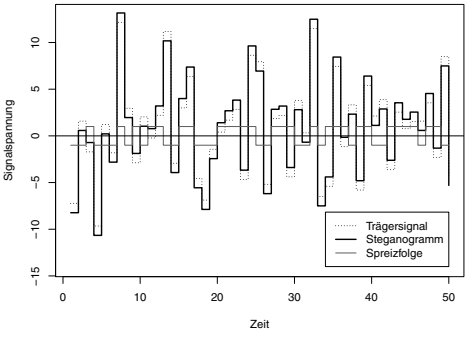

Abbildung 1: Eine pseudozufällige Spreizfolge wird mit dem Trägersignal (gepunktete Linie) überlagert und ergibt so das Steganogramm (fette Linie)

die unterstellte, einfache Spreizsprektrum-Einbettung mit einem normalverteilten Trägersignal. Eine pseudozufällige Spreizfolge, die ausschließlich aus den Werten -1 und 1 besteht, wird dabei verwendet, um ein einzubettendes Symbol (z. B. ein Bit) über einen längeren Zeitabschnitt zu spreizen. Obwohl diese Spreizfolge mit dem Trägersignal überlagert wird (bezogen auf die eingebettete Nachricht ein Störsignal), lässt sich das Symbol anschließend als Skalarprodukt der Spreizfolge mit dem Steganogramm extrahieren.

Passend zur einfachen Spreizspektrum-Einbettung gibt es einen einfachen Angriff in der Literatur, nämlich einen Histogramm-Angriff namens *Twin Peaks* [Mae98]. Wenn im Histogramm des Trägermediums eine Spitze vorhanden ist, könnte sich im Histogramm des Steganogramms eine verräterische Zwillingsspitze zeigen, woher der Name des Angriffs rührt. Wenn das Trägermedium eine Normalverteilung aufweist, dann ist das Steganogramm die Summe von zwei gegeneinander verschobenen Normalverteilungen, wobei der Abstand zwischen beiden durch die Spreizfolge bestimmt wird ($1 - (-1) = 2$). Wenn die Streuung des Signals groß ist (vgl. Abb. 2, links), z. B. an den lauteren Stellen des Tele-

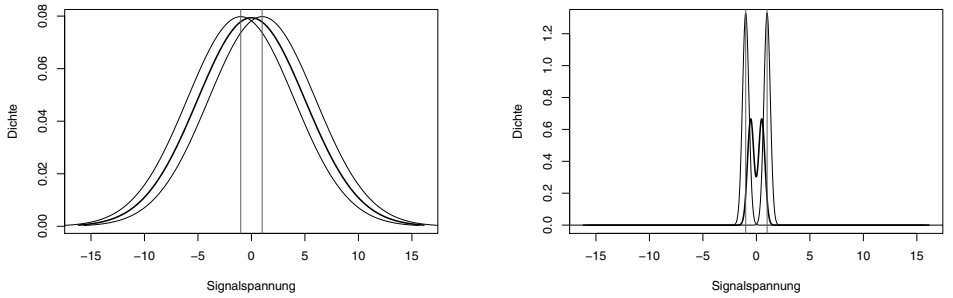

Abbildung 2: Wenn das Trägersignal lautstark genug ist, scheint die zusammengesetzte Verteilung (fette Linie) ebenfalls normalverteilt zu sein (links), leise Passagen des Steganogramms könnten jedoch eine Zwillingsspitze zeigen (rechts).

fonats, ist die sich ergebende Verteilung kaum von der ursprünglichen Normalverteilung zu unterscheiden. In leiseren Passagen könnte sich jedoch eine bimodale Verteilung ergeben (vgl. Abb. 2, rechts) oder zumindest eine nennenswerte Veränderung der Verteilung, an der die steganographische Einbettung erkennbar ist. Natürlich können wir erwarten, dass eine zeitgemäße Einbettungsmethode mit einer automatischen Pegelregelung für die Spreizsequenz aufwartet, die deren Amplitude in Abhängigkeit vom Trägersignal dynamisch verringert. Andererseits soll die Einbettungsmethode auch für Telefonate geeignet sein und muss sich zugunsten der Echtzeitfähigkeit einschränken. Die Regelung kann z. B. keinen allzu langen Abschnitt des Signals betrachten, ohne störende Verzögerungen bei der Übermittlung des Sprachsignal zu verursachen oder selbst verzögert zu reagieren.

Überraschenderweise ließen sich bei dieser ersten Untersuchung selbst kurze Ausschnitte der Telefonate (ca. 2–10 Sekunden) perfekt auseinanderhalten. Der Detektor arbeitet in zwei Schritten. Im ersten wurden leise Stellen des Signals ausgewählt, denn an den lauten erwarten wir ja gerade keine Zwillingsspitzen. Später stellte sich heraus, dass dieser Schritt verzichtbar ist. Im zweiten wurde das Histogramm gebildet, das eine „Solospitze“ für den Signalwert 0 zeigte, jedoch nur im Steganogramm. Das Trägersignal enthielt ungefähr die gleiche Anzahl Nullen und Einsen (ggf. bis zu 30 % mehr), in Steganogrammen gab es doppelt so viele. Der Angriff funktionierte in allen Konfigurationen („amp“, „bpsk“ und „phase“) mit dem gleichen Schwellwert: Wenn es mehr als 1,5 Mal so viele Nullen wie Einsen gab, dann wurde das Signal als „steganographisch verändert“ bewertet.

Warum das so war, blieb verborgen, bis letztlich der Quelltext des Verfahrens verfügbar war (vgl. Abschnitt 4.1).

3.2 „Stufen“

Dank der verfügbaren Testdaten jeweils mit und ohne eingebettete Nachricht, ist hier eine Analyse durch synchrone Gegenüberstellung der abgetasteten Werte c_i bzw. s_i des Trägermediums bzw. des Steganogramms möglich. Je näher die abgetasteten Werte an der Diagonale $s_i = c_i$ liegen, desto geringfügiger war die steganographische Veränderung des Signals. Abbildung 3 stellt Abtastwerte von Trägermedium und zugehörigem Stega-

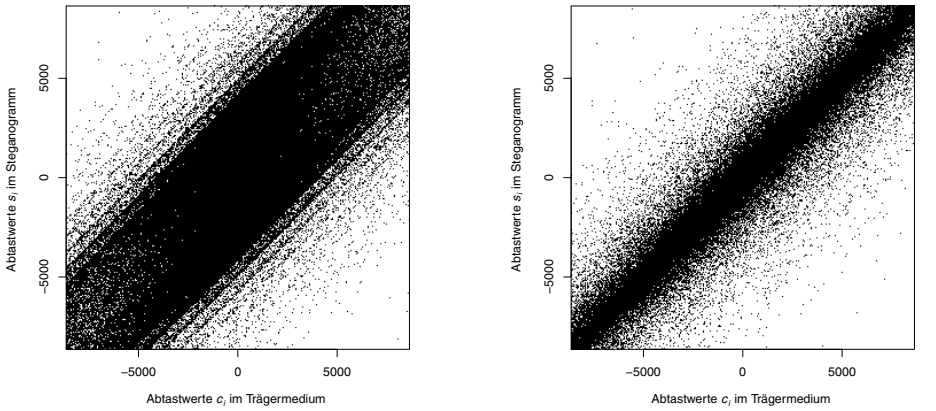

Abbildung 3: Die synchrone Gegenüberstellung der Abtastwerte im Trägermedium und im Steganogramm zeigt Steuerstufen (links), jedoch nicht mehr nach Korrektur des Algorithmus (rechts)

nogramm gegenüber, wobei eine Überlagerung diagonaler Streifen sichtbar wird. Offensichtlich gibt es eine Regelung, die die Einbettungsintensität in diskreten Schritten steuert. Unter realistischen Bedingungen ist dieser direkte Vergleich jedoch kaum möglich, da das Trägersignal nicht mit übertragen wird. Das fehlende Trägersignal kann dann nur aus dem steganographischen geschätzt werden. Dieser Prozess wird „Entrauschen“ genannt.

3.3 Saturn gesichtet

Die Abtastwerte des Trägermediums könnten aus anderen, jedoch zeitlich naheliegenden steganographisch veränderten Werten geschätzt werden:

$$c_i \sim s_{i-2} + s_{i-1} + s_{i+1} + s_{i+2}. \tag{1}$$

Ein ähnlicher Ansatz wurde während des BOWS-2-Wettbewerbs erfolgreich genutzt, um die Größenordnung von Wavelet-Koeffizienten ohne Wasserzeichen aus der Umgebung zu schätzen [BW09]. Dies war möglich, da der Teil des Wasserzeichens in s_i *unabhängig* vom Wasserzeichen in den Werten der Umgebung war. Leider können wir bezüglich der Unabhängigkeit im Falle des angegriffenen Audiosignals nicht sicher sein oder diese Eigenschaft gar erwarten, da eine Chipzeit – das ist die zeitliche Länge der Spreizfolge eines Symbols – in der Regel länger ist als die Abtastperiode. Dennoch können wir einfach mal den nächsten unveränderten Abtastwert aus dessen steganographischem Vorgänger schätzen

$$\hat{c}_{i+1} = s_i, \tag{2}$$

was uns zu einer eindrucksvollen, „astronomischen“ Konstellation in Abb. 4 (links) führt.

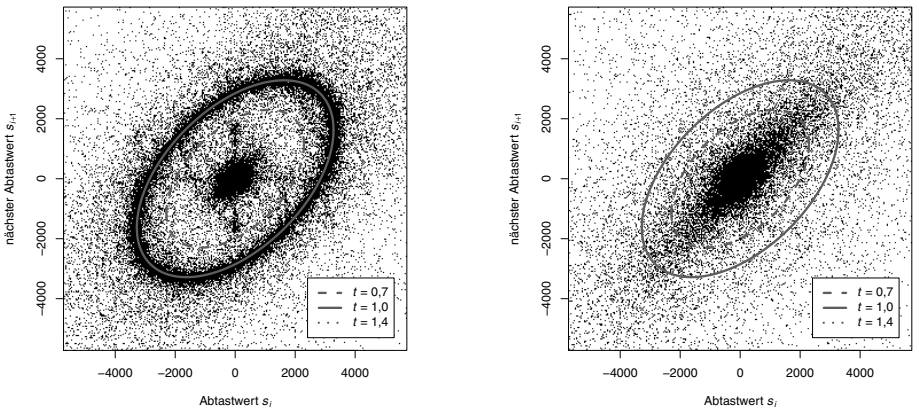

Abbildung 4: Die Gegenüberstellung aufeinanderfolgender Abtastwerte im Steganogramm (nächster Abtastwert als eine Schätzung des Trägersignals) zeigt eine Lissajous-Figur (links), nicht jedoch nach Reparatur des Algorithmus (rechts)

Obwohl die Ähnlichkeit mit einem Gestirn unseres Sonnensystems nicht abzustreiten ist, handelt es sich – technisch gesehen – um eine Lissajous-Figur, die durch folgende Ellipse

abgeschätzt werden kann:

$$\begin{aligned} t^2 &= \left(\frac{y - mx}{b}\right)^2 - \frac{x^2}{a^2}, \quad \text{mit} \\ a &= 3280, \\ b &= 2850 \quad \text{und} \\ m &= 0{,}496, \end{aligned} \tag{3}$$

wobei t ein Schwellwert ist, der bei geeigneter Wahl eine Unterscheidung zwischen Ring und Zentrum ermöglicht. Lissajous-Kurven erscheinen auf einem Oszilloskop im X–Y-Betrieb, also bei abgeschalteter Zeitablenkung, wenn an beide Eingänge je ein sinusförmiges Signal angelegt wird. In unserem Fall stammen beide Signale aus der selben Quelle. Sie haben also die gleiche Frequenz, sind aber untereinander zeitverzögert. Die Zeitverzögerung oder Phasenverschiebung wird im vorliegenden Fall durch die Abtastperiode festgelegt. Ein möglicher Detektor könnte den fragwürdigen Anteil von Abtastwerten ermitteln, der zwischen der gestrichelten Ellipse ($t = 0{,}7$) und der gepunkteten ($t = 1{,}4$) auftritt, und ihn mit der Gesamtzahl aller Werte vergleichen.

Die Stärke des Effekts ist sicherlich überraschend. Im Telefonat ist diese Einbettungsintensität auch deutlich als Pfeifen hörbar. Das Signal wurde ursprünglich zum Test der steganographischen Übertragungseigenschaften in GSM-Kanälen erzeugt und fand so seinen Weg zu den Testdaten. Der Effekt ist jedoch auch beim Betrieb mit realistischeren Parametern als kleiner Ring ($a \approx b \approx 30$: ;-) in einigen leisen Passagen vorhanden (jedoch sonst von dem in Abb. 4 sichtbaren dunklen Zentrum überdeckt). Wahrscheinlich wären wir ohne dieses Versehen gar nicht darauf aufmerksam geworden.

4 Reparatur

4.1 Solospitze

Das Trägersignal wird aus einer Audioquelle gelesen, gewöhnlich ein Telefon, eine Soundkarte oder eine WAV-Datei (z. B. 8000 PCM 16-Bit-Abtastwerte pro Sekunde, Mono). Die Werte sind vorzeichenbehaftete ganze Zahlen. Der Einbettungsalgorithmus unterstützt verschiedene Abtastraten und Genauigkeiten. Er wandelt daher anfänglich die Rohdaten in eine Folge normalisierter `double`-Gleitkommawerte im Bereich $-1 \ldots 1$ um.

Implementiert ist das durch Typumwandlung von `double` nach `int` (Ganzzahl), gefolgt von einer Skalierung in das Interval $[-1, 1]$. Am Ende werden die `double`-Werte wieder in den ursprünglichen Bereich hochskaliert (und, falls nötig, beschnitten) sowie nach `int` zurückgewandelt. Solange die Werte dazwischen nicht durch den Einbettungsschritt

verändert werden, ist die Rückwandlung von `double` eine $1:1$-Abbildung, da neben dem ganzzahligen Teil kein Bruchteil bleibt.

Wenn jedoch etwas eingebettet wird, dann sind die entstehenden `double`-Werte in der Regel nicht ganzzahlig. Hier rächt sich der naheliegende, aber sorglose Einsatz der Typumwandlung. Der Typumwandlungs-Operator (`y = (int)x;`) erwartet einen numerischen Parameter $x \in \mathbb{R}$ und gibt eine Ganzzahl $y \in \mathbb{Z}$ zurück, die durch Abschneiden des Bruchteils gebildet wird (vgl. Abb. 5). Mögliche Reparatur:

```
y = (int)(x + ((x < 0) ? -0.5 : 0.5));
```

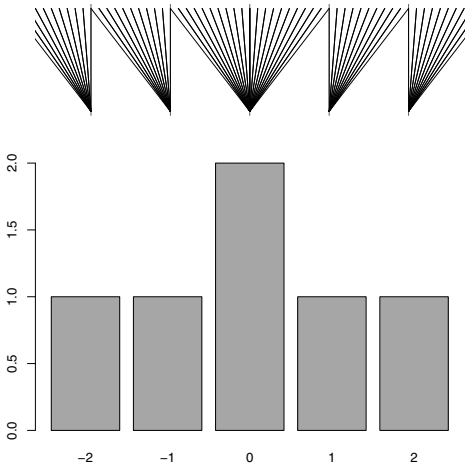

Abbildung 5: Im Korb für die 0 sammeln sich wegen des Abschneidens des Bruchteils die Werte aus einem doppelt so breiten Interval, wodurch die Spitze im Histogramm entsteht

Nachdem das eine Problem der auffälligen Solospitze behoben war, fiel bei einigen Medien noch ein weiteres im Sättigungsbereich auf. Es gibt eine gerade Anzahl von (vorzeichenbehafteten) 16-Bit-Ganzzahlen. Eine ist neutral (0), 32767 sind positiv und 32768 haben einen negativen Wert. Bei der Vorzeichenumkehr von -32768 (`0x8000`) kommt es zu einem Vorzeichenüberlauf: Es entsteht derselbe negative Wert. Die implementierte Normalisierung teilte alle Werte durch 32767 und beschnitt bei -32768 auf $-1{,}0$. Wenn das Signal nun hinreichend gesättigt ist, entstehen im Histogramm jeweils Spitzen für die gesättigten Werte $(-32768, 32767)$. Die Umwandlung in den internen Gleitkommabereich und zurück verschiebt dann die Spitze von -32768 nach -32767. Eine Spitze bei -32767 ist zwar ein zuverlässiger Indikator für steganographische Einbettung, tritt jedoch nur bei gesättigtem Ausgangsmaterial auf. Der Mangel lässt sich offensichtlich reparieren, indem der Divisor auf 32768 geändert wird und positive Werte bei nach der Rückumwandlung auf 32767 begrenzt werden.

5 Zusammenfassung

Wir haben mehrere Schwächen in einem Spreizspektrumverfahren für Audiosteganographie gefunden. Einige davon sind nicht auf die Einbettung selbst zurückzuführen, sondern die Umwandlung zwischen einem externen Format und einem internen Arbeitsformat. Es scheint also besonders wichtig zu sein, Umwandlungs- und Normalisierungsfunktionen auf Homogenität um besondere Werte wie 0 und ihre Eigenschaften bei Sättigung zu überprüfen.

Aber auch das Einbettungsverfahren selbst zeigte Schwächen. Es ist offenbar ratsam, die Differenz zwischen dem unveränderten und dem erzeugten Signal beim Entwurf genau zu analysieren. Zwar hat ein typischer Angreifer keinen Zugriff auf diese Differenz, auffällige Eigenschaften können dennoch über die abschirmende Wirkung der Unbestimmtheit aufgrund des zum Vergleich fehlenden Trägermediums hinausleuchten. Auch ist es ratsam, pathologische Signale wie rhythmische Audio-Impulse z. B. beim Test von Steuerungen einzusetzen.

Ferner ist es unerlässlich, Korrelationen innerhalb der Elemente des Trägermediums zu berücksichtigen. Solche Korrelationen treten natürlich auch im Steganogramm auf. Sie können häufig ausgenutzt werden, um das Signal zu „entrauschen“ oder entscheidende Statistiken zu „kalibrieren“ [FGH03, KF09], selbst in Audioströmen.

Literatur

[BW09] Patric Bas und Andreas Westfeld. Two Key Estimation Techniques for the Broken Arrows Watermarking Scheme. In *Proc. of ACM Multimedia and Security Workshop*, Seiten 1–8, Princeton, NJ, USA, September, 7–8 2009.

[FGH03] Jessica Fridrich, Miroslav Goljan und Dorin Hogea. Steganalysis of JPEG Images: Breaking the F5 Algorithm. In Fabien A. P. Petitcolas, Hrsg., *Information Hiding (5th International Workshop)*, Jgg. 2578 of *LNCS*, Seiten 310–323, Berlin Heidelberg, 2003. Springer-Verlag.

[KF09] Jan Kodovský und Jessica Fridrich. Calibration Revisited. In *Proc. of ACM Multimedia and Security Workshop*, Seiten 63–73, Princeton, NJ, USA, September, 7–8 2009.

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

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

[NFM10] Marcus Nutzinger, Christian Fabian und Marion Marschalek. Secure Hybrid Spread Spectrum System for Stegnanography in Auditive Media. *6th International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP)*, Seiten 78–81, October 2010.

[NW11] Marcus Nutzinger und Jürgen Wurzer. A Novel Phase Coding Technique for Steganography in Auditive Media. *6th International Conference on Availability, Reliability and Security (ARES)*, Seiten 91–98, August 2011.

[PSM82] Raymond L. Pickholtz, Donald L. Schilling und Laurence B. Milstein. Theory of Spread-Spectrum Communications—A Tutorial. *IEEE Transactions on Communications*, 30:855–884, 1982.

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

[Wes06] Andreas Westfeld. Steganographie für den Amateurfunk. In Jana Dittmann, Hrsg., *Sicherheit 2006, Sicherheit – Schutz und Zuverlässigkeit, Beiträge der 3. Jahrestagung des Fachbereichs Sicherheit der Gesellschaft für Informatik e. V. (GI), 20.–22. Februar 2006 in Magdeburg*, Jgg. P-77 of *LNI*, Seiten 119–130, Bonn, 2006.