H. Langweg, M. Meier, B.C. Witt, D. Reinhardt (Hrsg.): Sicherheit 2018,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2018 83

Verbesserung der Syndrome-Trellis-Kodierung zur Erhöhung der Unvorhersagbarkeit von Einbettpositionen in steganographischen Systemen

Olaf Markus Köhler[1], Cecilia Pasquini[2,4] und Rainer Böhme[3,4]

Abstract: Beim Einbetten einer versteckten Nachricht in ein Trägermedium wählen adaptive steganographische Systeme die Einbettpositionen abhängig von der erwarteten Auffälligkeit der Änderungen. Die optimale Auswahl kann statistisch modelliert werden. Wir präsentieren Ergebnisse einer Reihe von Experimenten, in denen untersucht wird, inwiefern die Auswahl durch Syndrome-Trellis-Kodierung dem Modell unabhängiger Bernoulli-verteilter Zufallsvariablen entspricht. Wir beobachten im Allgemeinen kleine Näherungsfehler sowie Ausreißer an Randpositionen. Bivariate Abhängigkeiten zwischen Einbettpositionen ermöglichen zudem Rückschlüsse auf den verwendeten Kode und seine Parameter. In Anwendungen, welche die Ausreißer nicht mithilfe zufälliger Permutationen verstecken können, kann die hier vorgeschlagene „outlier corrected"-Variante verwendet werden um die steganographische Sicherheit zu verbessern. Die aggregierten bivariaten Statistiken sind dahingegen invariant unter Permutationen und stellen, unter der Annahme mächtiger Angreifer, ein bisher nicht erforschtes Sicherheitsrisiko dar.

Keywords: Steganographie, Syndrome-Trellis-Kodierung

1 Einleitung

Um steganographisch versteckte Nachrichten möglichst unentdeckbar zu halten, ist es von Nutzen, die Positionen von Änderungen am Trägermedium entsprechend ihrer erwarteten Auffälligkeit zu wählen. Damit der Empfänger zum Extrahieren der Nachricht die Positionen der Änderungen nicht rekonstruieren muss, oder ihm diese auf anderem Wege mitgeteilt werden müssen, setzen moderne steganographische Systeme auf Syndrom-Kodierung. Die populärste Form ist die Syndrom-Trellis-Kodierung (STC) [FJF11]. Sie erlaubt die Trennung der Entscheidungen *wo* und *wie* das Trägermedium geändert wird und zeichnet sich dabei durch ihre rechnerische Effizienz aus.

[1] Institut für Informatik, Universität Innsbruck, Österreich, olaf.koehler@uibk.ac.at
[2] Institut für Informatik, Universität Innsbruck, Österreich, cecilia.pasquini@uibk.ac.at
[3] Institut für Informatik, Universität Innsbruck, Österreich, rainer.boehme@uibk.ac.at
[4] ebenfalls Institut für Wirtschaftsinformatik, Universität Münster, Deutschland

[5] Die hier präsentierten Forschungsergebnisse wurden umfangreicher und in englischer Sprache im Rahmen der Konferenz IWDW 2017 in Magdeburg veröffentlicht. [KPB17]

doi:10.18420/sicherheit2018_06

Kurzgefasst erhält STC als Eingaben das Trägermedium, die zu versteckende Nachricht und einen Vektor von Änderungswahrscheinlichkeiten je Position des Trägermediums. Daraus erzeugt sie einen binären Vektor, der angibt, an welchen Positionen das Trägermedium geändert werden muss, um die Nachricht einzubetten. Üblicherweise wird diese Ausgabe als Realisation eines Vektors unabhängiger Bernoulli-Zufallsvariablen abstrahiert [BFP11, FJF11, SCF16]. Demgegenüber stehen die Struktur des Kodes und einhergehende Beschränkung der möglichen Lösungen, welche der vorherigen Abstraktion widersprechen. Unser Ziel ist es, diese Diskrepanz statistisch zu untersuchen, mit der Leitfrage: Wie dicht werden die vorgeschriebenen Änderungswahrscheinlichkeiten durch die STC angenähert?

Im Rahmen unserer empirischen Herangehensweise erzeugen wir 150 Millionen Steganogramme[6]. Die statistische Auswertung der experimentell gesammelten Daten gliedert sich in drei Schritte: Aggregierte Momente (Kapitel 2), univariate Statistiken (Kapitel 3) und bivariate Abhängigkeiten (Kapitel 5). Zu den neuen Erkenntnissen gehört unter anderem, dass die reguläre STC, wie sie in akademischen Veröffentlichungen und der Referenzimplementierung [FFJ] beschrieben ist, die geforderten Eigenschaften am Beginn des Kodes nicht erfüllt. Um die ermittelten Ausreißer zu vermeiden, schlagen wir eine modifizierte Kode-Konstruktion namens OC-STC vor (Kapitel 4).

1.1 Systemmodell

Steganographie durch Modifikation eines Trägermediums erzeugt aus einem Trägermedium $\boldsymbol{x} = (x_i)_{i=1,\ldots,n}$ der Länge n ein Steganogramm $\boldsymbol{y} = (y_i)_{i=1,\ldots,n}$. Das Steganogramm enthält die gewünschte Nachricht $\boldsymbol{m} = (m_j)_{j=1,\ldots,\alpha n}$, wobei α das Verhältnis zwischen den Längen von Nachricht und Trägermedium beschreibt. Die Änderungen am Trägermedium werden als binärer Vektor $\boldsymbol{c} = (c_i)_{i=1,\ldots,n} \in \{0,1\}^n$ formalisiert, wobei einzelne Elemente des Änderungsvektors $\boldsymbol{c}$ als Änderungspositionen c_i bezeichnet werden. Ein passendes Steganogramm zu finden, wird als Einbettprozess bezeichnet.

Daneben muss der Einbettprozess, wie er in Abb. 1 dargestellt ist, das Schutzziel der Unerkennbarkeit erfüllen: Die statistische Unterscheidbarkeit zwischen Trägermedien und Steganogrammen ist zu minimieren. Aufbauend auf dem Modell additiver Störung, wird ausgehend vom Trägermedium ein Kostenvektor $\boldsymbol{\varrho} = (\varrho_i)_{i=1,\ldots,n}$ bestimmt. Mithilfe einer Heuristik wird jeder Position des Trägermediums ein positiver Wert ϱ_i zugewiesen, der den Einfluss einer dortigen Änderung auf die statistische Unterscheidbarkeit schätzt. Im Fall regulärer STC [FJF10] bedeutet die Anwendung des Modells additiver Störung: Der Anteil von Änderungsposition i an der gesamten Störung ist durch $c_i \varrho_i$ gegeben, sodass die gesamte Störung d als Summe $d = \sum_{i=1}^{n} c_i \varrho_i$ bestimmt wird.

[6] Als Trägermedien werden 1000 64×64 Bildausschnitte aus dem BOSSBase-Datensatz v1.01 [BFP11] verwendet. Die vollständigen Details des Experimentaufbaus sind [KPB17] zu entnehmen.

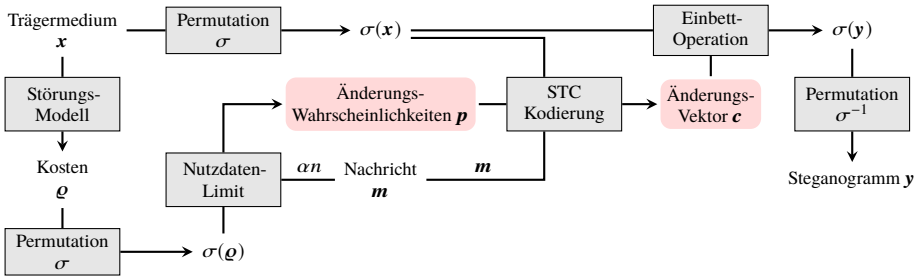

Abb. 1: Systemmodell des Einbettprozesses.

Die Permutation σ wird auf das Trägermedium und den Kostenvektor angewendet. Intuitiv ist die Permutation als Versatz zu begreifen, der die Nachricht in etwa gleichmäßig auf die Positionen des Trägermediums verteilt. Das erhöht die Chance einer erfolgreichen Einbettung, da Positionen mit hohen Kosten oft lokal konzentriert sind. Des Weiteren erhöht die Konvention Passwort-abhängiger pseudozufälliger Permutationen die Sicherheit, da es die Zuordnung von Positionen des Trägermediums zu Nachrichten-Bits erschwert.

Beim Kodierungs-Schritt werden aus dem permutierten Trägermedium $\sigma(\boldsymbol{x})$, der Nachricht $\boldsymbol{m}$ und dem permutierten Kostenvektor $\sigma(\boldsymbol{\varrho})$ die nötigen Änderungen $\boldsymbol{c}$ am Trägermedium bestimmt. Mithilfe der Einbettoperation wird der Änderungsvektor $\boldsymbol{c}$ auf das permutierte Trägermedium $\sigma(\boldsymbol{x})$ angewendet, wodurch das permutierte Steganogramm $\sigma(\boldsymbol{y})$ entsteht. Durch Rückpermutation wird das Steganogramm $\boldsymbol{y}$ erzeugt, was an den Empfänger geschickt wird. Dieser kann die Nachricht durch Permutation des Steganogramms mit σ und Multiplikation mit der Matrix der Syndrom-Kodierung extrahieren. (Das Extrahieren der Nachricht ist in Abb. 1 nicht dargestellt.)

Als Vereinfachung nehmen wir folgend an, dass α so gewählt sei, dass α^{-1} eine Ganzzahl ist. Desweiteren sei $\boldsymbol{x}$ beliebig, aber fest. Zur Vereinfachung der Notationen führen wir die Mehrdeutigkeit ein, dass $\boldsymbol{x}$ und $\boldsymbol{y}$ Ganzzahl-Vektoren im Kontext von Trägermedium und Steganogramm bezeichnen, aber binäre Vektoren im Kontext der Kodierung bezeichnen. Die implizite Annahme dabei ist, dass eine Abbildung von den Ganzzahl-Vektoren auf ihre binäre steganographische Semantik durch die Einbettoperation gegeben ist. In einfachen Fällen ist die Semantik durch das niedrigstwertige Bit gegeben, aber auch andere (sicherere) Einbettoperationen sind möglich.

1.2 Syndrom-Trellis-Kodierung

Bei der Syndrom-Kodierung ergibt sich das Steganogramm $\boldsymbol{y}$ als Syndrom aus dem linearen Gleichungssystem mit der Matrix $\mathbb{H}$ und der Nachricht $\boldsymbol{m}$, $\mathbb{H}\boldsymbol{y} = \boldsymbol{m}$. Die STC [FJF10] ist als Spezialfall der Syndrom-Kodierung zu verstehen, bei dem eine dünn besetzte Matrix $\mathbb{H}$, wie in (1), durch mehrfaches Konkatenieren und nach unten Rücken einer Submatrix

$\hat{\mathbb{H}} \in \{0,1\}^{h \times \alpha^{-1}}$ konstruiert wird. Die Höhe der Submatrix wird als Kodierungsparameter h bezeichnet. Diese Konstruktion erlaubt es mithilfe des Viterbi-Algorithmus [RC12] effizient einen Änderungsvektor $\boldsymbol{c}$ zu finden, der zugleich die gesamte Störung d minimiert und die Nachricht $\boldsymbol{m}$ als Syndrom bedingt, $\mathbb{H}(\boldsymbol{x} \oplus \boldsymbol{c}) = \boldsymbol{m}$.

$$\mathbb{H} = \begin{pmatrix} \hat{\mathbb{H}} & \begin{matrix}0\ldots0\\0\ldots0\end{matrix} & \begin{matrix}0\ldots0\\0\ldots0\end{matrix} & & & \\ \begin{matrix}0\ldots0\\0\ldots0\end{matrix} & \hat{\mathbb{H}} & \hat{\mathbb{H}} & \ddots & 0 & \\ & 0 & & \hat{\mathbb{H}} & \begin{matrix}0\ldots0\\\hat{\mathbb{H}}\end{matrix} & \begin{matrix}0\ldots0\\\vdots\\0\ldots0\end{matrix} \end{pmatrix} . \tag{1}$$

Aufgrund der strikten Minimieren der gesamten Störung d, hängt der Änderungsvektor $\boldsymbol{c}$ von den Kosten $\boldsymbol{\varrho}$ ab. So lassen sich unter dem Modell additiver Störung die Änderungswahrscheinlichkeiten für den Fall einer optimalen Kodierung bestimmen. Die optimale Änderungswahrscheinlichkeit p_i für jede Position i mit den Kosten ϱ_i ist $p_i = e^{-\lambda\varrho_i}\left(1 + e^{-\lambda\varrho_i}\right)^{-1}$ [FF10a, FF10b, FJF11]. Unter der Annahme, dass die Nachricht die volle Entropie erreicht, ist dabei λ so zu wählen, dass die gesamte Entropie der Länge der Nachricht entspricht, $\sum_{i=1\ldots n} H(p_i) = n\alpha$, wobei die binäre Entropie durch $H(p_i) = -p_i \log_2(p_i) - (1-p_i)\log_2(1-p_i)$ gegeben ist.

Der Zufallsvektor der Änderungen sei als $\boldsymbol{C} = (C_i)_{i=1\ldots n}$ mit dem Ergebnisraum $\{0,1\}^n$ gegeben. Aufgrund paarweiser Unabhängigkeit der Änderungspositionen c_i lässt sich die multivariaten Bernoulli-Verteilung von $\boldsymbol{C}$ zu einem Produkt univariater Bernoulli-Verteilungen vereinfachen. Dabei ergibt sich die Wahrscheinlichkeitsfunktion

$$P_{\boldsymbol{C}}(\boldsymbol{c}) = \prod_{i=1,\ldots,n} (p_i)^{c_i}\,(1-p_i)^{1-c_i} \quad . \tag{2}$$

Bei der Einbettung N verschiedener Nachrichten in ein Trägermedium $\boldsymbol{x}$ entstehen N Realisierungen $(\boldsymbol{c}^{(1)}, \ldots, \boldsymbol{c}^{(N)})$ des Zufallsvektors $\boldsymbol{C}$. Bei optimaler Kodierung folgt der Änderungsvektor $\boldsymbol{c}$ der Verteilung (2). Zur Untersuchung der Abweichung von STC zum optimalen Fall definieren wir die relative Häufigkeitsverteilung $\hat{P}_{\boldsymbol{C}} : \{0,1\}^n \to [0,1]$, wobei $\hat{P}_{\boldsymbol{C}}(\boldsymbol{c})$ die relative Häufigkeit der Erscheinung von $\boldsymbol{c}$ unter den beobachteten N Realisierungen angibt.

2 Analyse der Änderungshäufigkeit

Die Anzahl der Änderungen wird als Zufallsvariable $A = \sum_{i=1}^{n} C_i$ formalisiert, wobei die Realisationen von A mit a bezeichnet werden. Unter der Annahme optimaler Kodierung sollte A als Summe unabhängiger Bernoulli-Variablen einer verallgemeinerten Binomialverteilung folgen [Wa93]. Die Verteilung P_A ergibt sich also aus der Summe der Verteilungen der unabhängigen univariaten Bernoulli-Variablen mit Parameter p_i.

Je Trägermedium $\boldsymbol{x}$ wird ein asymmetrisches 95%-Konfidenzintervall $[a_{\min}, a_{\max}]$ bestimmt, sodass $\sum_{a<a_{\min}} P_A(a) \approx 0.025$ und $\sum_{a<a_{\max}} P_A(a) \approx 0.975$. Des Weiteren werden je Trägermedium $\boldsymbol{x}$ und Kodierungsparameter $h \in \{7, 10, 13\}$ unter einer fixen Permutation σ, $N = 50\,000$ zufällige Nachrichten eingebettet. Die sich dabei ergebenden Änderungsvektoren seien als $Z_h = \{\boldsymbol{c}^{(j)}\}_{j=1,\ldots,N}$ gegeben. Zu den Kodierungsparametern passend, werden dabei die Submatrizen der Referenzimplementierung [FFJ] verwendet:

$$\hat{\mathbb{H}}_7 = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}^T, \quad \hat{\mathbb{H}}_{10} = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}^T,$$

$$\hat{\mathbb{H}}_{13} = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}^T.$$

Daraufhin bestimmen wir je Trägermedium den Anteil der Änderungshäufigkeiten, die innerhalb des Konfidenzintervalls liegen. Die Anteile sind im Histogramm Abb. 2 aggregiert.

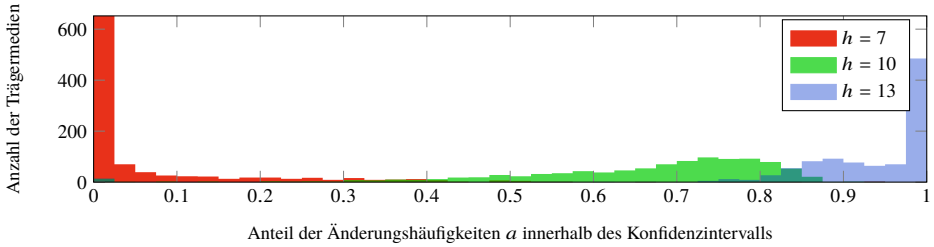

Abb. 2: Histogramm der Änderungsanzahl je Trägermedium innerhalb des 95%-Konfidenzintervalls.

Diskussion der Beobachtungen. Mit dem Kodierungsparameter $h = 13$ ist der mittlere Anteil der Einbettungen im Konfidenzintervall bei 92%. Für kleinere Kodierungsparameter sinkt der Anteil der Einbettungen, die in das Konfidenzintervall fallen. Der für diese Statistik im Falle optimaler Kodierung erwartete mittlere Anteil wäre 95%.

Dass die Zielverteilung nicht vollständig erreicht wird bedeutet, dass zumindest eine der zugrunde liegenden Annahmen nicht zutrifft. Zu diesen Annahmen zählt das Erzielen von Häufigkeiten entsprechend der optimalen Änderungswahrscheinlichkeiten p_i und die Unabhängigkeit der Änderungspositionen c_i. Folgend werden Statistiken untersucht, die es ermöglichen, die Erfüllung dieser beiden Annahmen differenziert zu betrachten.

3 Analyse der Änderungswahrscheinlichkeiten

Zur Untersuchung der individuellen Änderungswahrscheinlichkeiten werden die univariaten Zufallsvariablen C_i betrachtet, welche durch die i-te Komponente des Zufallvektors $\boldsymbol{C}$ gegeben sind. Entsprechend (2) müsste C_i unter der Annahme optimaler Kodierung einer univariaten Bernoulli-Verteilung mit der Wahrscheinlichkeit p_i und der Wahrscheinlichkeitsfunktion $P_{C_i}(c_i) = (p_i)^{c_i}(1-p_i)^{1-c_i}$ folgen.

Für ein beliebiges aber festes Trägermedium $\boldsymbol{x}$ ist die beobachtete Häufigkeit für eine Position i als $\hat{p}_i = \frac{1}{N}\,|\{c \in Z_h : c_i = 1\}|$ gegeben. Zum Vergleich der beobachteten relativen Häufigkeitsverteilung und der optimalen Wahrscheinlichkeitsverteilung von Änderungen genügt es, die Erfolgswahrscheinlichkeiten $\hat{p}_i$ und p_i zu vergleichen, da sie die Bernoulli-Verteilungen vollständig bestimmen.

Ein Vergleich der Änderungswahrscheinlichkeit p_i mit realisierten relativen Häufigkeit $\hat{p}_i$ für ein exemplarisch ausgewähltes Trägermedium, ist in Abbildung 3 (links) dargestellt. Zur Quantifizierung der Abweichung nutzen wir den Hellinger-Abstand $D_{\text{Hellinger}}(p_i,\ \hat{p}_i) = \sqrt{\sqrt{1-p_i}\sqrt{1-\hat{p}_i} + \sqrt{p_i}\sqrt{\hat{p}_i} + 1}$. Die 20 Positionen des Trägermediums mit der stärksten Abweichung sind mit ihrer Position im 4096-elementigen Änderungsvektor $\boldsymbol{c}$ annotiert.

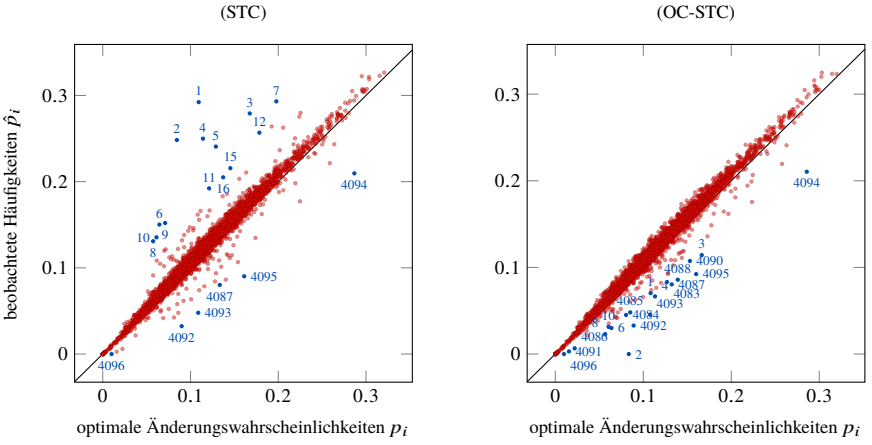

Abb. 3: Exemplarischer Vergleich der optimalen Änderungswahrscheinlichkeiten p_i und beobachteten Häufigkeiten $\hat{p}_i$ mit regulärer STC (links) und der hier vorgeschlagenen OC-STC (rechts). Das zugrundeliegende Trägermedium ist das Graustufenbild 5729 des BOSSBase Datensatzes, ausgeschnitten auf 64×64 Pixel an Position $(258, 53)$. Der verwendete Kodierungsparameter ist $h = 13$.

Diskussion der Beobachtungen. Deutliche Abweichungen von den optimalen Änderungswahrscheinlichkeiten sind besonders am Anfang und Ende des Änderungsvektors $\boldsymbol{c}$ zu beobachten. Dabei fällt auf, dass die Ausreißer am Anfang des Änderungsvektors $\boldsymbol{c}$

im Diagramm über der Diagonale liegen und die Ausreißer am Ende unter der Diagonale. Beide Arten von Ausreißern lassen sich durch die spezifische Konstruktion der Matrix der STC erklären.

Die Ausreißer über der Diagonale lassen sich durch das geringe Hamming-Gewicht in den ersten Zeilen der Matrix $\mathbb{H}$ erklären. Im Fall von $\alpha = 0.5$ hängt das erste Bit der Nachricht, unabhängig vom Kodierungsparameter h, nur von den ersten zwei Bits des permutierten Steganogramms $\sigma(\boldsymbol{y})$ ab. In anderen Worten müssen die ersten zwei Bits des Steganogramms so angepasst werden, dass sie gemeinsam das korrekte erste Bit der Nachricht bilden. Unter der Annahme, dass die Bits des Steganogramms und der Nachricht gleichverteilt sind, ist die Wahrscheinlichkeit, eine Änderung an einer der ersten beiden Positionen vornehmen zu müssen, 50%, obwohl die Summe der optimalen Änderungswahrscheinlichkeiten $p_1 + p_2$ typischerweise deutlich darunter liegt. Ein ähnlicher Effekt trifft die Änderungspositionen $c_j : j < h\alpha^{-1}$, wenn auch weniger ausgeprägt als die ersten beiden Positionen.

Eine der Berechnung optimaler Änderungswahrscheinlichkeiten zugrundeliegende Annahme ist die Einbettung mit maximaler Entropie. Die STC kann dies nur in dem Maß realisieren, in dem die zugrundeliegende Matrix $\mathbb{H}$ dies zulässt. Das deckt sich mit der Beobachtung der im Mittel positiven Abweichung der Häufigkeiten $\hat{p}_i$ von den optimalen Wahrscheinlichkeiten p_i. Kleinere Kodierungsparameter h beschränken die Kodierung stärker und implizieren entsprechend höhere positive Abweichungen der Häufigkeiten.

Diese Beobachtungen lassen sich in der Darstellung Abbildung 3 (links) nachvollziehen. Vergleichbare Ergebnisse sind auch bei den anderen untersuchten Trägermedien zu beobachten. Für eine über alle untersuchten Trägermedien aggregierte Darstellung sei auf [KPB17] verwiesen.

4 OC-STC

Die Ausreißer über der Diagonale entsprechen ungewollt häufiger Änderungen an potentiell auffälligen Positionen und sind damit eine sicherheitsrelevante Abweichung von den optimalen Änderungswahrscheinlichkeiten.

Es ist nicht möglich, die Ausreißer durch eine Anpassung des Kostenvektors $\boldsymbol{\varrho}$ (z.B. mithilfe von einer Fensterfunktion) zu beheben, da die Ausreißer durch die Konstruktion des Kodes bedingt sind. Ein möglicher Ansatz wäre die Detektion derartiger Ausreißer nach der Einbettung und die Korrektur der effektiven Änderungswahrscheinlichkeiten durch die Wiederholung des gesamten Prozesses. Ein solches Vorgehen würde allerdings die Abschätzung des zeitlichen Aufwands der Einbettung erschweren und ähnelt dem unsicheren Verfahren der Steganographie durch Auswahl von Trägermedien.

Stattdessen schlagen wir eine Modifikation der Kode-Konstruktion vor, welche die sicherheitsrelevanten Ausreißer vermeidet. Der Verbesserungsvorschlag wird folgend als OC-STC bezeichnet, was für „Outlier-Corrected Syndrome Trellis Coding“ steht. Die

Kode-Konstruktion von OC-STC ergibt sich durch das Aussparen der ersten $h-1$ Zeilen von $\mathbb{H}$:

$$\mathbb{H}_{\mathrm{OC}} = \begin{pmatrix} \begin{matrix} \\ 0\ldots0 \\ \vdots \\ 0\ldots0 \\ 0\ldots0 \end{matrix} & \ddots & \begin{matrix} \hat{\mathbb{H}} \\ 0\ldots0 \\ 0\ldots0 \end{matrix} & \begin{matrix} \hat{\mathbb{H}} \\ 0\ldots0 \end{matrix} & \begin{matrix} 0\ldots0 \\ \hat{\mathbb{H}} \end{matrix} & & \\ & & & & \ddots & 0 & \\ 0 & & & & \begin{matrix} \hat{\mathbb{H}} \\ \hat{\mathbb{H}} \end{matrix} & \begin{matrix} 0\ldots0 \\ \ddots \end{matrix} & \begin{matrix} 0\ldots0 \\ \vdots \\ 0\ldots0 \end{matrix} \end{pmatrix} . \tag{3}$$

Die dabei resultierende Matrix $\mathbb{H}_{\mathrm{OC}}$ unterscheidet sich in der zentralen Eigenschaft, dass jede Zeile jedes Element von $\hat{\mathbb{H}}$ exakt einmal enthält. Damit ist das Hamming-Gewicht der Zeilen von $\mathbb{H}_{\mathrm{OC}}$ konstant. Somit wird jedes Bit der Nachricht durch gleich viele Positionen des Steganogramms definiert. Auch mit der modifizierten Matrix $\mathbb{H}_{\mathrm{OC}}$ wird die Kodierung mit dem Viterbi-Algorithmus durchgeführt.

Durch das Aussparen der ersten $h-1$ Zeilen wird das Nutzdaten-Limit um $h-1$ Bits reduziert. Um den Einfluss von OC-STC korrekt beurteilen zu können, wird daher ein neuer Wert λ' bestimmt, der die optimalen Änderungswahrscheinlichkeiten entsprechend des reduzierten Nutzdaten-Limits korrekt skaliert. Ein Vergleich der so bestimmten optimalen Änderungswahrscheinlichkeiten und mit OC-STC beobachteten Häufigkeiten ist in Abb. 3 (rechts) dargestellt.

In der exemplarischen Gegenüberstellung zur regulären STC ist die erfolgreiche Vermeidung der Ausreißer über der Diagonale zu erkennen. Die verbleibenden positiven Abweichungen sind dann durch die Beschränkung der Kodierung durch den Kodierungsparameter h zu erklären. OC-STC erzeugt weiterhin Ausreißer unter der Diagonale, was Positionen entspricht, die seltener geändert werden als unter dem verwendeten Modell additiver Störung möglich. Aus diesen Ausreißern ergeben sich nicht unmittelbar Sicherheitsbedenken. Dennoch wäre es wünschenswert, die steganographische Kapazität aller Positionen im Trägermedium voll auszunutzen.

5 Analyse der Abhängigkeiten zwischen Änderungen

Zur Untersuchung paarweiser Abhängigkeiten definieren wir die bivariaten Zufallsvariablen $\boldsymbol{C}_{i,j} = (C_i, C_j)$, die sich aus Komponenten-Paaren von $\boldsymbol{C}$ zusammensetzen. Realisierungen von $\boldsymbol{C}_{i,j}$ werden mit $\boldsymbol{c}_{i,j} = (c_i, c_j)$ bezeichnet. Unter der Annahme optimaler Kodierung wären die Komponenten unabhängig.

Basierend auf Verteilung optimaler Änderungsvektoren (2), ergibt sich für die paarweisen Änderungen $\boldsymbol{C}_{i,j}$ die bivariate Bernoulli-Verteilung mit der Wahrscheinlichkeitsfunktion

$$P_{\boldsymbol{C}_{i,j}}(\boldsymbol{c}_{i,j}) = (p_i)^{c_i}\,(1-p_i)^{1-c_i}\,\left(p_j\right)^{c_j}\,\left(1-p_j\right)^{1-c_j} \quad . \tag{4}$$

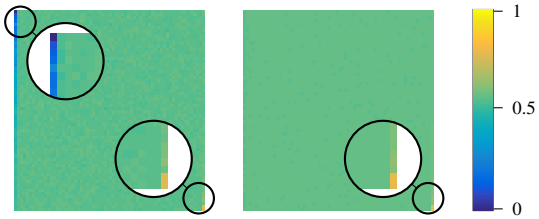

Abb. 4: Spaltenweise Darstellung der gemittelten p-Werte des χ^2-Unabhängigkeitstests über das erste Element im Vergleich zu allen anderen Pixeln j (links), und über jedes Elements j im Vergleich zu allen anderen Elementen (rechts). Die dargestellten Werte sind die über alle Trägermedien gemittelten p-Werte je Position in der Reihenfolge der Kodierung. Der Kodierungsparameter ist $h = 13$.

Wir bestimmen die relativen Häufigkeiten $\hat{p}_{i,j}^{(b'b'')}$, die durch die Rate der beobachteten Änderungsvektoren bestimmt wird. An den Positionen i und j haben diese die binären Werte b' und b''. Daraus lässt sich die empirische Häufigkeitsverteilung $\hat{P}_{\boldsymbol{C}_{i,j}}$ bestimmen. Als bivariate Bernoulli-Verteilung formuliert, ist die Wahrscheinlichkeitsfunktion gegeben als

$$\hat{P}_{\boldsymbol{C}_{i,j}}(\boldsymbol{c}_{i,j}) = \left(\hat{p}_{i,j}^{(00)}\right)^{(1-c_i)(1-c_j)} \left(\hat{p}_{i,j}^{(01)}\right)^{(1-c_i)c_j} \left(\hat{p}_{i,j}^{(10)}\right)^{c_i(1-c_j)} \left(\hat{p}_{i,j}^{(11)}\right)^{c_i c_j}. \tag{5}$$

Mithilfe des χ^2-Unabhängigkeitstests auf C_i und C_j untersuchen wir die Abhängigkeiten zwischen Positionen i und j unter der Häufigkeitsverteilung $\hat{P}_{\boldsymbol{C}_{i,j}}$. Zunächst wird die Abhängigkeit der ersten Position $i = 1$ von allen anderen Positionen $j \neq i$ getestet. Dies wird für alle Trägermedien wiederholt. Die dabei gesammelten p-Werte werden je Position j gemittelt und spaltenweise aufgereiht in Abb. 4 (links) dargestellt.

Danach beobachten wir die Abhängigkeiten zwischen allen Positionspaaren $i \neq j$. Dazu wird der mittlere p-Wert für alle j und $i \neq j$ bestimmt, je Position j gemittelt, über alle Trägermedien gemittelt und spaltenweise in Abb. 4 (rechts) dargestellt. Abbildungsposition j stellt dann den gemittelten p-Wert der χ^2-Unabhängigkeitstests über die alle Positionen $i \neq j$ im Vergleich zu Position j dar.

Zum Verständnis der Verteilung der p-Werte, bestimmen wir den Anteil der p-Werte $\leq 5\%$ je Trägermedium. Die Anteile sind in Histogramm Abbildung 5 aggregiert.

Diskussion der Beobachtungen. In Abbildung 4 (links) sind niedrige p-Werte für die Nachbarschaft der ersten Position zu erkennen. Die beobachtete Abhängigkeit lässt sich aus der Konstruktion der Matrix $\mathbb{H}$ (1) erklären, die lineare Abhängigkeiten zwischen nahen Positionen impliziert. Die ersten $h\alpha^{-1}$ Positionen müssen gemeinsam so gewählt werden, dass deren Paritäten mit den ersten h Nachrichten-Bits übereinstimmen. Diese Abhängigkeiten setzen sich kaskadierend über den gesamten Änderungsvektor fort.

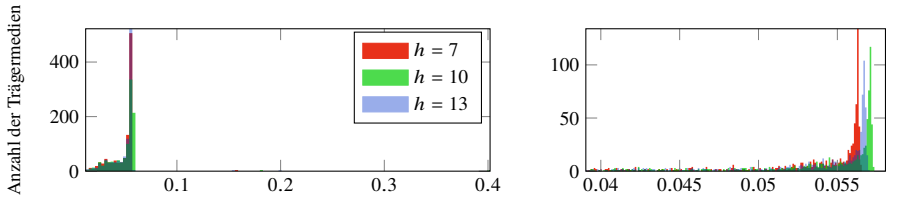

Abb. 5: Histogramme der Anteile von p-Werten $\leq 5\%$. Dabei fließt je Trägermedium der Anteil der p-Werte $\leq 5\%$ über alle Positionen ein. Dargestellt ist ein Histogramm über alle Anteile (links) und ein Histogramm über die Anteile in der Nachbarschaft der Höhepunkte um 0.05 (rechts).

Ein gegenteiliger Effekt ist zum Ende des Änderungsvektors zu beobachten, und das für beide aggregierten Abhängigkeiten in Abbildung 4 (links und rechts): Die letzten Positionen weisen hohe gemittelte p-Werte auf, was bedeutet, dass sie dazu tendieren unabhängig von den restlichen Positionen zu sein. Auch dies kann als Konsequenz der Konstruktion der Matrix $\mathbb{H}$ erklärt werden. Die letzten α^{-1} Positionen des Steganogramms beeinflussen lediglich das letzte Nachrichten-Bit. Die letzten α^{-1} Positionen sind lediglich implizit über die Parität des letzten Nachrichten-Bits mit den vorherigen $h\alpha^{-1}$ Positionen verbunden. Daher ist der kaskadierende Effekt der Auswahl bestimmter Änderungen an diesen Positionen und die damit verbundene Abhängigkeit verhältnismäßig klein.

Diese Untersuchung ist unter Kenntnis der Permutation durchgeführt, sodass die Positionen in der Reihenfolge der Kodierung betrachtet werden können. Im Fall einer unbekannten, aber für ausreichend viele Steganogramme fixen Permutation, würde eine solche Untersuchung potentiell das Rekonstruieren der Permutation ermöglichen und damit deren Beitrag zur steganographischen Sicherheit neutralisieren.

Des Weiteren kann ein ausreichend mächtiger Angreifer bei einer unbekannten aber festen Permutation ein Histogramm der p-Werte, wie in Abbildung 5, erstellen. Der erwartete Anteil von Positions-Paaren mit p-Werten $\leq 5\%$ ist für unabhängig gewählte Änderungen 5%. Aufgrund der Abhängigkeit des Anteils von dem gewählten Kodierungsparameter, ist die Beobachtung von mittleren Anteilen über 5% nicht nur für die Steganalyse relevant, sondern offenbart potenziell auch Informationen über die Permutation.

In unserem Experiment ist der mittlere Anteil der p-Werte $\leq 5\%$ für den Kodierungsparameter $h = 10$ höher als für $h = 13$. Dies bedeutet, dass bei $h = 10$ im Mittel weniger Positionspaare den Unabhängigkeitstest bestehen, als bei $h = 13$. Die Ursache dafür bilden die Werte der Submatrix $\hat{\mathbb{H}}$, da sie maßgeblich dafür sind, wie sich Abhängigkeiten über den Änderungsvektor hinweg bilden. Derartige Statistiken sollten die Wahl einer Submatrix in zukünftigen Forschungsarbeiten anleiten.

6 Abschließende Bemerkungen

Es ist weitere Forschung nötig um den tatsächlichen Verlust an steganographischer Sicherheit zu quantifizieren, der durch die Abhängigkeitsstrukturen in der Kodierung entsteht. Dazu könnte bei der Steganalyse das Wissen naher paarweiser Abhängigkeiten direkt genutzt werden, oder indirekt durch den Versuch, die Permutation wiederherzustellen. Auch eine gründliche Untersuchung von OC-STC und der Vermeidung von negativen Ausreißern der Änderungshäufigkeiten verbleibt im Rahmen künftiger Forschung zu erbringen.

Zusammenfassend hat diese Forschungsarbeit gezeigt, dass die Kodierung als Teil eines steganographischen Systems relevante Fragen offen lässt. Dabei widersprechen die hier präsentierten Ergebnisse nicht unmittelbar den bisherigen Erkenntnissen bezüglich steganographischer Sicherheit, die auf der Simulation von Einbettungen durch die zufällige Wahl optimaler Änderungsvektoren aufbauen. Vielmehr können die Ergebnisse als obere Grenze der Sicherheit von Systemen betrachtet werden, welche die Simulation durch Einbettung echter Nachrichten mit STC ersetzen.

Für weitere Statistiken, Details zu der Durchführung der Experimente, Erklärungen im Kontext von Bildern als Trägermedien und eine Performance-Untersuchung sei auf die englischsprachige Ursprungsfassung [KPB17] verwiesen.

Danksagung

Wir danken Alexander Schlögl für die Hilfe bei der Implementierung der STC auf dem HPC, Pascal Schöttle und den anonymen Reviewern der IWDW und GI Sicherheit für die wertvollen Kommentare.

Die präsentierten empirischen Ergebnisse wurden mithilfe der HPC Infrastruktur “LEO” der Universität Innsbruck erzielt. Diese Forschung wurde von der Archimedes Privatstiftung, Innsbruck und der Deutschen Forschungsgemeinschaft (DFG) unter “Informationstheoretische Schranken digitaler Bildforensik” gefördert.

Literaturverzeichnis

[BFP11] Bas, Patrick; Filler, Tomáš; Pevnỳ, Tomáš: “Break Our Steganographic System”: The Ins and Outs of Organizing BOSS. In (Filler, Tomáš; Pevný, Tomáš; Craver, Scott; Ker, Andrew, Hrsg.): Information Hiding (13th International Conference). Jgg. 6958 in Lecture Notes in Computer Science, Springer, Berlin, Heidelberg, S. 59–70, 2011.

[CSB14] Carnein, Matthias; Schöttle, Pascal; Böhme, Rainer: Predictable Rain? Steganalysis of Public-Key Steganography using Wet Paper Codes. In: ACM Information Hiding and Multimedia Security Workshop. Salzburg, Austria, S. 97–108, 2014.

[FF10a] Filler, Tomáš; Fridrich, Jessica: Gibbs construction in steganography. IEEE Transactions on Information Forensics and Security, 5(4):705–720, 2010.

[FF10b] Filler, Tomáš; Fridrich, Jessica: Minimizing additive distortion functions with non-binary embedding operation in steganography. In: IEEE International Workshop on Information Forensics and Security (WIFS). Tenerife, Spain, S. 1–6, 2010.

[FFJ] Filler, T.; Fridrich, J.; Judas, J.: , Syndrome Trellis Coding, Binghamton reference implementation. http://dde.binghamton.edu/download/syndrome/ (letzter Zugriff: Juni 2017).

[FJF10] Filler, Tomáš; Judas, Jan; Fridrich, Jessica: Minimizing embedding impact in steganography using trellis-coded quantization. In: Proceedings of SPIE-IS&T Electronic Imaging: Security, Forensics, Steganography and Watermarking of Multimedia Contents X. San Jose, CA, S. 754105–754105, 2010.

[FJF11] Filler, Tomáš; Judas, Jan; Fridrich, Jessica: Minimizing additive distortion in steganography using syndrome-trellis codes. IEEE Transactions on Information Forensics and Security, 6(3):920–935, 2011.

[Ke08] Ker, Andrew D: Locating steganographic payload via WS residuals. In: ACM Multimedia and Security Workshop. Oxford, UK, S. 27–32, 2008.

[KPB17] Köhler, Olaf Markus; Pasquini, Cecilia; Böhme, Rainer: On the Statistical Properties of Syndrome Trellis Coding. In (Krätzer, Christian; Shi, Yun-Qing; Dittmann, Jana; Kim, Hyoung-Joong, Hrsg.): Digital Forensics and Watermarking, 16th International Workshop, IWDW 2017. Jgg. 10431 in Lecture Notes in Computer Science, Springer, Berlin Heidelberg, S. 331–346, 2017.

[PK14] Pevnỳ, Tomäš; Ker, Andrew D: Steganographic key leakage through payload metadata. In: ACM Information Hiding and Multimedia Security Workshop. Salzburg, Austria, S. 109–114, 2014.

[RC12] Reed, Irving S; Chen, Xuemin: Error-control coding for data networks. Springer Science & Business Media, New York, US, 2012.

[SCF16] Sedighi, Vahid; Cogranne, Rémi; Fridrich, Jessica: Content-adaptive steganography by minimizing statistical detectability. IEEE Transactions on Information Forensics and Security, 11(2):221–234, 2016.

[Wa93] Wang, Yuan H: On the number of successes in independent trials. Statistica Sinica, 3(2):295–312, 1993.