Technische Hochschule Brandenburg
University of Applied Sciences

Technische Hochschule Brandenburg

Faculty of Computer Science

Fingerprinting-Merkmale für Bilddaten unter Einfluss von Information Hiding

Submitted in partial fulfillment of the requirements for the degree of
Master of Science (M.Sc.)

by
Fabian Loewe
Matrikelnummer: 20202415

First Examiner

Prof. Dr. Claus Vielhauer

Second Examiner

Benedict Michaelis, M.Sc.

Abstract

In dieser Masterarbeit wird zunächst ein Überblick zum Information Hiding mit Hilfe von Bilddateien verschafft. Der Fokus wird auf die Verwendung der beschriebenen Techniken im öffentlichen Raum durch Einbettungswerkzeuge und Malware gesetzt. Eine Untersuchung aktueller Malware-Vorkommnisse zeigt die Relevanz der Thematik und verschafft einen kategorisierte Übersicht für weitere Untersuchungen. Anhand der Funde werden Einbettungswerkzeug, die algorithmisch verwandte Verfahren zu den untersuchten Malwares anwenden, und Forschungsdaten mit Cover- und Stego-Bild-Paaren ausgewählt. Die Bildpaaren werden daraufhin mit einem Werkzeug verglichen und aus den Ergebnissen steganografische Merkmale extrahiert, welche Hinweise auf die Anwendung bestimmter Algorithmen, Bildverarbeitungsbibliotheken und weitere Informationen liefern. Schließlich werden im Ausblick weitere Forschungsrichtungen im Bereich des Information Hiding vorgestellt.

Declaration

Suppose you are writing a thesis; you probably need this bit to confirm that you wrote it all by yourself. This template adds the `signature-required` CSS class, which adds a nice line where you can write your name.

If you are not writing a thesis, just delete this whole section.

Potsdam, 1.1.2024_

Fabian Loewe

Chapter 1. Einleitung

Informationen versteckt in Schrift, Bild oder, allgemeiner, einem anderen Objekt zu übermitteln ist eine Jahrhunderte alte Technik, welche als Steganografie bereits seit 2500 Jahren bekannt ist. Der Begriff *Steganografie* leitet sich vom griechischen *steganós (στεγανός)* und -graphia (γραφή) ab, was grob übersetzt für *verborgen* und *Schrift* steht. [1]

So nutzte beispielsweise Griechen im Krieg mit Persien im fünften Jahrhundert versteckte Nachrichten, um nicht von den Persern eingenommen zu werden. Die schottische Königin Mary griff im 16. Jahrundert auf Kryptografie und Steganografie zurück, um ihre Briefe vor ungewünschten Lesern zu schützen. Im Jahr 1499 veröffentlichte der deutsche Abt Johannes Trithemius sein Werk *Steganographia*, welches erstmals, soweit bekannt, Methoden zum Verstecken von Nachrichten in Schrift beschäftigt. [2]

Insbesondere mit der Entwicklung von Computern nahm Steganografie als Forschungsbereich final Einzug in die Wissenschaft, wobei großes Interesse besonders bei der Einbettung von Informationen in Medien wie Bild- und Audiodaten aufgekommen. Die Grundlagen der noch heute relevanten Methoden wurden bereits in den 1990er bis 2000er Jahren entwickelt und werden in den kommenden Kapiteln dieser Arbeit genauer vorgestellt.

1.1. Motivation

Für Entwickler von Schadsoftware, auch bekannt als Malware, ist stets wichtig, im Wettstreit mit den Gesetzeshütern einen Schritt voraus zu sein. Dazu wird inzwischen die Technik der Steganografie immer öfter aufgegriffen, um Daten wie weiteren Schadcode für Multi-Layer- oder Befehle für sogenannte Command-and-Control-Malware (kurz C&C) in das von der Schadsoftware befallene System einzuschleusen oder gestohlene Daten wie Passwörter aus dem System auszuschleusen, ohne dabei bei IT-Sicherheitssystem wie Firewalls oder Antivirenprogrammen aufzufallen. Die genannte Vorgänge sind jeweils als Dateninfiltration und Datenexfiltration bekannt. [3, 4]

Die Verwendung von Steganografie in Bilddateien kann bereits in vielen Fällen erkannt werden. Jedoch folgt darauf meist keine genauere Zuordnung zu einem bestimmten Algorithmus, einer möglicherweise verwendeten Bibliothek zur Verarbeitung von Bilddaten oder sogar einer bestimmten Malware oder Malware-Familie. Eine derartige Zuordnung kann vielfältige Informationen zum Angriffshergang, Beschaffenheit und Ursprung der Malware wie auch zur Herkunft der damit operierenden Täter liefern, die für die strafrechtliche Verfolgung von großer Bedeutung sein können.

Neben der Verwendung durch Malware wird Steganografie zudem auch für das Einbetten sogenannter digitalter Wasserzeichen genutzt, bei dem Bilddateien mit einem versteckten Code versehen werden, um ungewünschte Distributionen oder Manipulationen des Bildes nachverfolgen zu können. Dies ist wichtig, um Urheberrechte zu schützen und deren Bruch durch beispielsweise Piraterie ahnden zu können. Die Analyse von potenziell mit Wasserzeichen gekennzeichneten Bildern kann also wie bei Malware Aufschluss auf Herkunft und konkrete Art der Einbettung liefern, um beispielsweise Robustheit des verwendeten Algorithmus zu testen und sicherzustellen, dass bei der Einbettung keine privaten Informationen preisgegeben werden. [5]

1.2. Zielsetzung

Die Zielstellung dieser Arbeit konzentriert sich auf die folgenden Punkte:

*. Erstellung einer umfänglichen Liste von Malware-Vorkommnissen, in denen Steganografie mit Bildern als Trägermedium verwendet wurde *. Erstellung einer Auswahlliste an Steganografie-Tools, die vergelichbar in ihrer Funktionalität zu den gefundenen Malwares sind *. Erstellung einer Auswahlliste an Wasserzeichen-Tools *. Recherche und/oder Aufbau von Forschungsdaten aus Cover- und Stego-Bilder-Paaren *. Entwicklung eines Prototyps eines Werkzeugs zur Identifikation von Merkmalen für den Einsatz bestimmter Steganografieverfahren, Bildverarbeitungsbibliotheken und weitere

Durch das Erreichen der genannten Ziele soll ein erster Ansatz zur Identifikation von Steganografie-Tools basierend auf deren verwendeter Bilder erarbeitet werden, welcher sowohl für den Einsatz mit Malware als mit Wasserzeichen weiterausgebaut werden kann, wobei dies nicht mehr im Fokus dieser Arbeit liegt.

Da die Menge der Malware-Vorkommnisse erwartbar weit größer als die Menge der Steganografie- und Wasserzeichen-Tools sein dürfte, werden erstere nur mittels Literaturrecherche, während letztere auch praktisch durch Tests ausgewertet werden.

Die beschriebene Ziele werden fortan im Rahmen dieser Arbeit als **Z.1** bis **Z.5** referenziert.

1.3. Forschungsfragen und Hypthoesen

Aus der Zielsetzung lassen sich folgende Forschungsfragen und zugehörigen Hypthosen ableiten:

Frage: Können Werkzeuge zur Einbettung von Daten mittels Steganografie nur anhand ihrer Ausgabe-Bilder und der Original-Bilder automatisiert identifiziert werden?

> **Hypothese**: Ja, es lassen sich immer wiederkehrende Merkmale in den Bildern nachweisen, die mit dem verwendeten Einbettungswerkzeug in Zusammenhang stehen.

Frage: Gibt es eine Schnittmenge der verwendeten Steganografie-Algorithmen und technischen Umsetzung zwischen Malwares, Steganografie- und Wasserzeichen-Tools?

> **Hypthese**: Ja, es kann eine Schnittmenge zumindest in der Kategorie der Steganografie-Algorithmen und der zur Umsetzung verwendeten Programmiersprachen und Bibliotheken abgesteckt werden.

Frage: Worin unterscheiden sich die drei Kategorien?

> **Hypothese**: Die Malwares legen einen größeren Wert auf Performance als auf Robustheit, während Wassezeichen-Tools umgekehrt gewichtet sind. Steganografie-Tools sind je nach Gewichtung der Autoren aufgestellt.

Die beschriebene Fragen werden fortan im Rahmen dieser Arbeit als **F.1** bis **F.3** referenziert.

1.4. Aufbau der Arbeit

Im folgenden Kapitel Chapter 2 werden die theoretischen Grundlagen kurz dargelegt, ohne

tiefergehend auf die mathematische Basis einzugehen, da im Rahmen dieser Arbeit keine eigenen steganografischen Algorithmen entwickelt werden. Im Kapitel Chapter 3 werden das Vorgehen zu den Literaturrecherchen und der Entwicklung von Programmen zur Erreichung von **Z.5** dokumentiert. Das Kapitel Chapter 4 stellt die gesammelten Ergebnisse, aufbereitet in Grafiken und als Code-Listings mit entsprechenden Interpretation, vor. Die Kaptiel Chapter 5 und Chapter 6 geben schließlich einen kurzen Rückblick der Arbeit wider und zeigen weitere Ausbaumöglichkeiten des entwickelten Programmcodes sowie Richtungen zur Forschung auf.

Chapter 2. Theoretische Grundlagen

2.1. Information Hiding

2.1.1. Steganografie

2.1.2. Watermarking

2.2. Attributierung

Chapter 3. Methodik

3.1. Literaturrecherche zu Malware-Vorkommnissen im Zusammenhang mit Steganografie

3.2. Literaturrecherche zur Attributierung steganografischer Bilddaten

3.3. Implementierung eines Programms zum Vergleich zweier Bilder

3.4. Implementierung eines Prototypen zur Attributierung steganografischer Bilddaten

Chapter 4. Ergebnisse

4.1. Malware-Vorkommnisse im Zusammenhang mit Steganografie

4.2. Übersicht von Attributen steganografischer Bilddaten

4.3. Prorgamm zum Vergleich zweier Bilder

4.4. Prototyp zur Attributierung steganografischer Bilddaten

Chapter 5. Zusammenfassung

Chapter 6. Ausblick

Bibliografie

[1] W. Gemoll, K. Vretska, T. Aigner, und R. Wachter, *Griechisch-deutsches Schul- und Handwörterbuch*, 10., Völlig neu bearb. Aufl., [Nachdr.]. Oldenbourg.

[2] S. Singh, *The code book: the science of secrecy from ancient Egypt to quantum cryptography*, 1. Ed. Anchor Books, 2000.

[3] R. Benson, „Data Infiltration - DFIQ (Digital Forensics Investigative Questions)“. Zugegriffen: Feb. 09, 2024. [Online]. Verfügbar unter: https://dfiq.org/scenarios/S1002/.

[4] R. Benson, „Data Exfiltration - DFIQ (Digital Forensics Investigative Questions)“. Zugegriffen: Feb. 09, 2024. [Online]. Verfügbar unter: https://dfiq.org/scenarios/S1001/.

[5] J. Dittmann, „Motivation und Einführung“, in *Digitale Wasserzeichen: Grundlagen, Verfahren, Anwendungsgebiete*, J. Dittmann, Hrsg. Springer, 2000, S. 1–7.