What a Digital Forensics Investigator Should Know About Steganalysis of Digital Content

James Foley

B00151368

Word Count:4006

Abstract

Regarding digital forensics, this paper looks at the methodologies, problems, and applications of steganography and steganalysis. The report bases its analysis on the fundamental significance of these techniques. Although steganography embeds data into multimedia files, it presents significant challenges for forensic investigators who require advanced steganalysis tools. Typical steganographic approaches, such as Least Significant Bit (LSB) replacement and transform domain methods, and their relative imperceptibility, resilience, and data capacity are reviewed in this study. The performance metrics of these techniques are also analysed. This work highlights the inherent limitations of the methodologies currently being utilised using insights obtained from a comprehensive literature review conducted by Apau et al. (2024) and experimental research conducted with the OpenPuff tool. This highlights the fact that an even more significant number of sophisticated detection methods are required.

As part of the best practices for digital forensic investigators, there is also an emphasis on being legally prepared to meet problems such as data heterogeneity, encryption, investigations that span international borders, standardised frameworks, and ethical compliance.

Table of Contents

Introduction

Steganography and steganalysis are crucial techniques in digital forensics to bridge the gap between covert communication and investigative analysis. As the nature of cybercrime continues to evolve, forensic investigators face substantial hurdles brought on by the capacity to integrate sensitive information in multimedia files. Since steganography is increasingly being utilised to conceal illegal conduct, investigators must be able to identify and evaluate concealed information effectively. Steganography is an essential countermeasure that uses statistical and machine learning techniques to uncover concealed information and arrive at meaningful conclusions.

This paper aims to provide the findings of that inquiry and comprehensive research on steganographic techniques, their detection methods, and the challenges of applying them in digital forensics. Based on the findings of experiments and in-depth analyses of the relevant literature, it highlights how important it is for forensic investigations to conform to ethical standards and utilise advanced frameworks. The paper aims to provide best practices for researchers by addressing challenges particular to a domain and those span domains. Additionally, the report tries to ensure the admissibility and validity of evidence in a legal setting. To keep up with more complicated steganographic approaches, this study emphasises modern methods and draws attention to significant areas that require creativity.

Background of Steganalysis

Steganalysis analyses and uncovers hidden material in digital files by finding key characteristics in the format. Feature extraction is the first step in the process, which looks at the file's attributes and statistical trends. According to Ghasemzadeh and Kayvanrad (2018, as cited in Shehab & Alhaddad, 2022). features may be divided into two categories: handmade features, which are manually generated using well-established statistical approaches, and deep features, which are automatically retrieved using sophisticated techniques like neural networks and deep autoencoders.

The medium is categorised as either a "stego," which indicates that it contains hidden data, or a "cover," which suggests that it has not been altered once the characteristics have been recovered. Classification procedures may take many forms, starting with fundamental statistical techniques like using empirical thresholds to identify anomalies. As an alternative, machine learning techniques may be applied, whereby the algorithm is taught on existing stego and cover files to identify modifications in newly undiscovered data. Neural networks in this context perform feature extraction and classification, improving their ability to recognise complex or flexible steganographic approaches (Paulin et al., 2016, as cited in Shehab & Alhaddad, 2022).

Steganalysis findings go into one of two categories: passive or active detection. While passive detection finds hidden information within a file, active detection looks for other information, including the size or characteristics of the secret message. In digital forensics, these processes are essential because they allow for discovering and analysing hidden data, which is often crucial evidence in criminal investigations (Karampidis et al., 2018; Ghasemzadeh & Kayvanrad, 2018, as cited in Shehab & Alhaddad, 2022).

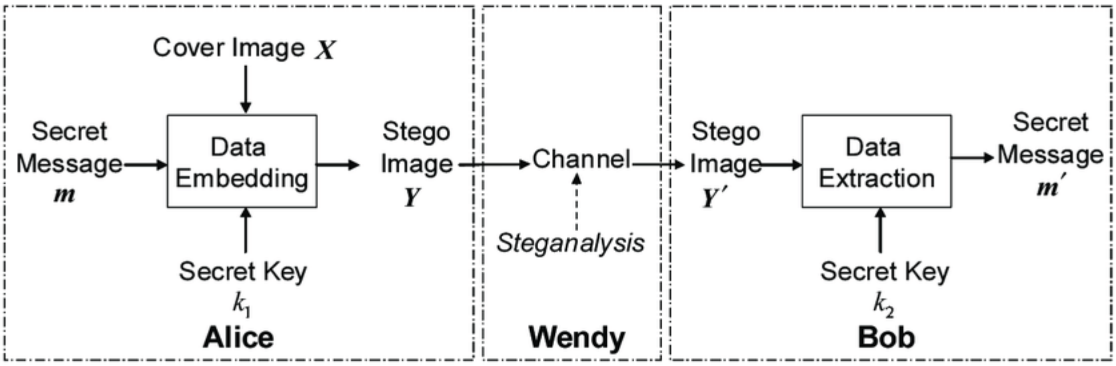


FIGURE 1: STEGANOGRAPHY VS. STEGANALYSIS **(LI ET AL., 2011)**

Steganographic Techniques

Steganography is a covert communication technique that entails concealing data in multimedia files, including audio, video, and images so that a viewer cannot identify it (Krenn, 2004). In contrast to cryptography, which concentrates on encrypting data, steganography completely hides the existence of the concealed message. This method exploits the limits of human vision by enclosing the message in a routine file that can be sent without raising red flags.

Audio Steganography

By using the masking effect and other features of the human auditory system (HAS), audio steganography uses digital audio files as carriers to hide data. It ensures excellent quality in clandestine communications by using HAS restrictions to insert data in audio signals imperceptibly.

Techniques

1. **Least Significant Bit (LSB) Encoding**:
   - Replace the least significant bits of audio samples with data bits.

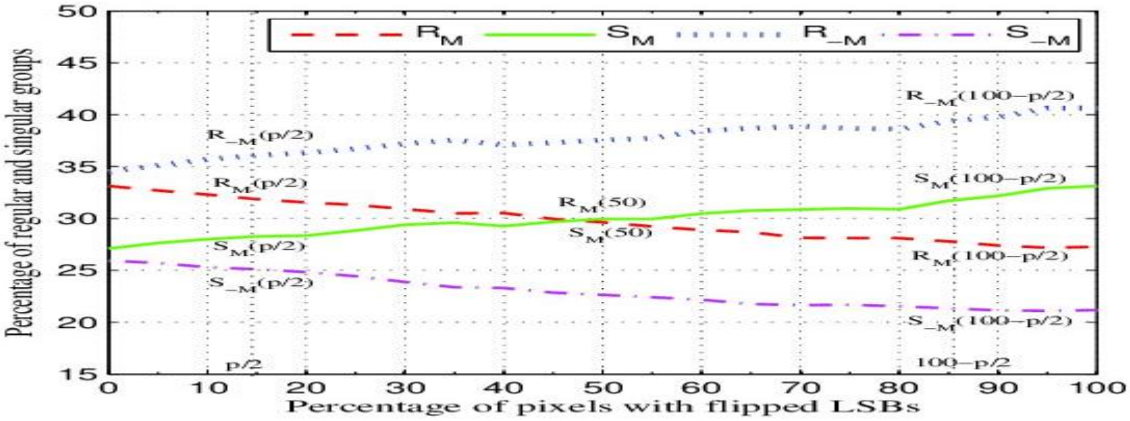


FIGURE 2: LEAST SIGNIFICANT BIT (LSB) ENCODING DIAGRAM **(LI ET AL., 2011)**

   - Offers high capacity but is sensitive to compression and noise (Djebbar et al., 2012).

2. **Echo Hiding**:
   - This technique adds echoes to the audio signal to conceal data. The audio quality is maintained because the echoes are meticulously engineered to be undetectable to the human ear (Djebbar et al., 2012).

3. **Methods for Transforming Domains**:

- **Discrete Wavelet Transform (DWT)**: Information is included in the audio signal’s wavelet coefficients. According to Djebbar et al. (2012), this method increases the buried data’s resistance to compression and other signal-processing methods.
- **Spread Spectrum**: According to Djebbar et al. (2012), the concealed data is more secure and difficult to identify since it is dispersed over the whole audio spectrum.

Performance Metrics

- **Imperceptibility**: Makes sure that the changes made to the audio stream are sufficiently modest for human listeners to miss them (Djebbar et al., 2012).
- **Robustness**: Assesses the concealed data’s resistance to outside influences such as noise or compression (Djebbar et al., 2012).
- **Capacity**: Measures the volume of data that can be embedded into the audio, usually expressed in bits per second (bps) (Djebbar et al., 2012).

Applications

- Audio steganography has practical uses in secure messaging, such as transmitting sensitive information in telemedicine or covert communication for military operations (Djebbar et al., 2012).
- Embedding additional metadata, such as subtitles, within audio tracks.

Cited from Djebbar et al. (2012).

Image Steganography

Image steganography hides data in digital images, taking advantage of the redundancy in pixel values to embed secret information. The aim is to maintain the quality of the stego image while providing high data capacity.

Techniques

1. **Least Significant Bit (LSB) Substitution**: This method incorporates information into the pixel values’ least significant bits.
   - Offers simplicity and great capacity but is susceptible to compression (Lee et al., 2021).
2. **Techniques for Transforming Domains**:
   - **Discrete Cosine Transform (DCT)**: Provides resistance against compression by embedding data in frequency coefficients.
   - **Discrete Wavelet Transform (DWT)**: Embeds data in perceptually less important regions to provide high imperceptibility.
3. **Hybrid Methods**:
   - Combines many techniques, including distributed steganography or XOR-based encoding, for increased security.

Performance Metrics

- **Capacity**: Measured in bits per pixel (bpp).
- **Imperceptibility**: Evaluated through PSNR, with higher values indicating less distortion.
- **Robustness**: Indicates resistance to compression, cropping, and noise.

Applications

- Digital watermarking to protect intellectual property.
- Authentication through embedded metadata in official documents.

Cited from Lee et al. (2021).

Video Steganography

Video steganography conceals information inside video files using their substantial storage capacity and frame-by-frame redundancy. It supports a variety of embedding techniques in both the compressed and raw domains.

Techniques

1. **Raw Domain Methods**:
   - Least Significant Bit (LSB) Substitution: Adjusts the LSBs of video frame pixel values to balance imperceptibility and capacity.
   - For increased resilience, the Discrete Wavelet Transform (DWT) embeds data in high-frequency sub bands (Kunhoth et al., 2023).
2. **Methods in the Compressed Domain**:
   - To achieve a compromise between computing efficiency and imperceptibility, embed data into encoded streams, such as motion vectors or transform coefficients.

Performance Metrics

- **Imperceptibility**: Assessed using PSNR and SSIM, indicating the visual quality of stego videos.
- **Robustness**: Tests the resistance to compression and noise attacks, ensuring data integrity.
- **Hiding Capacity**: Refers to the embedded data volume, measured in bits per frame.

Applications

- Covert communication.
- Authentication and tamper detection in forensic analysis.

Cited from Kunhoth et al. (2023).

Steganalysis Techniques

Steganalysis is a method used to find and delete hidden data from multimedia files, therefore helping to avoid steganography. While steganography aims to preserve information's confidentiality, steganalysis searches for hidden signals without disclosing the embedding techniques used (Kaur & Kaur, 2014). Finding illicit communications and protecting multimedia assets are two valuable applications for it.

Steganalysis techniques can be broadly categorised into two main types: signature-based and statistical-based methods. Signature-based methods detect repetitive patterns or identifiable features left behind by steganographic tools. On the other hand, statistical-based methods analyse changes in the properties of multimedia content, such as pixel values, frequencies, or statistical distributions, to identify the presence of hidden data (Kaur and Kaur, 2014; Djebbar et al., 2012).

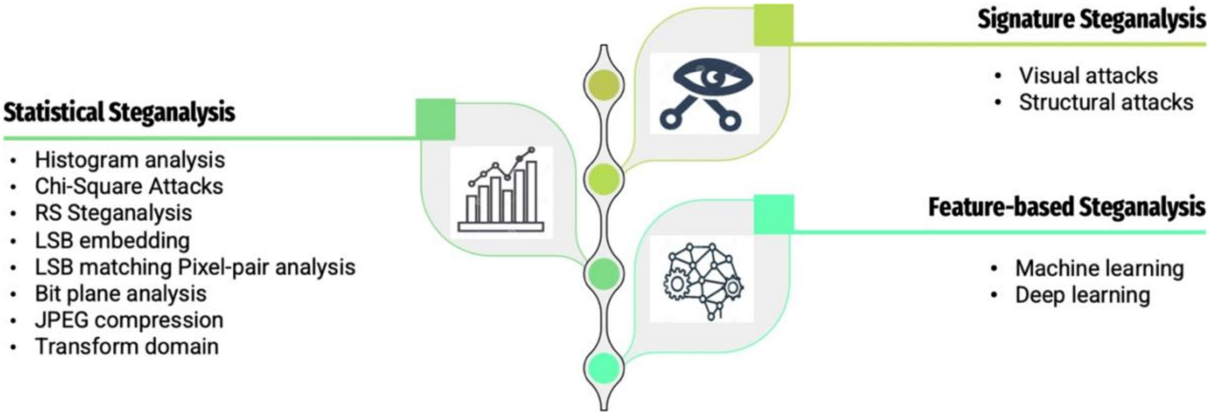


FIGURE 3: TYPES OF STEGANALYSIS TECHNIQUES (KAUR & KAUR, 2014).

Types of Steganalysis Techniques

Signature-Based Steganalysis

Signature-based steganalysis identifies patterns or anomalies created by embedding tools, such as changes in the palette of GIF images or visible repetitive patterns. Although effective for simple steganography techniques, this method struggles against advanced embedding schemes and needs more automation capabilities (Kaur and Kaur, 2014).

Steganalysis with Statistics

Data in multimedia files is analysed using statistical approaches, which use mathematical models to reveal hidden information. These techniques consist of:

- **Specific Statistical Steganalysis**: Focusing on specific steganographic approaches, such as LSB replacement and JPEG compression, specific statistical steganalysis uses a thorough grasp of the embedding process. According to Kaur and Kaur (2014), the outcomes are accurate for the application.
- **Universal Statistical Steganalysis**: A versatile approach that detects hidden data across various steganographic methods without knowledge of embedding operations. Techniques such as machine learning and clustering algorithms are commonly employed in this category (Kunhoth et al., 2023).

Techniques Used in Steganalysis

1. **Chi-Square Statistical Attack**

This method is one of the earliest statistical techniques for detecting hidden image data. It identifies changes in the statistical distribution of pixel values caused by embedding schemes like LSB substitution. Chi-square attacks are particularly effective for detecting hidden data in spatial and JPEG-compressed images (Kaur and Kaur, 2014).

2. **RS Analysis and Sample Pair Analysis (SPA)**

These techniques detect patterns introduced during the embedding process. RS analysis identifies dependencies between pixel groups, while SPA evaluates statistical alterations caused by steganographic operations (Kaur and Kaur, 2014; Djebbar et al., 2012).

3. **Transform Domain Analysis**

Discrete Wavelet Transform (DWT) and Discrete Cosine Transform (DCT) analyse frequency domain properties to detect hidden information. According to Djebbar et al. (2012), these methods work exceptionally well for locating data embedded in compressed domains like JPEG or MP3 files.

4. **Methods Based on Machine Learning**

Multimedia files are categorised as stego or ego using machine learning methods like Support Vector Machines (SVMs). High accuracy and flexibility to new steganographic techniques are provided by these approaches, which are based on statistical characteristics taken from the text (Kunhoth et al., 2023).

5. **Randomness Tests in Bit Planes**

This technique finds deviations from natural distributions, which point to hidden information, by evaluating the randomness in the bit planes of an image or video. According to Kaur and Kaur (2014), it works exceptionally well at separating stego content from natural media.

6. **Histogram-Based Techniques**

These techniques examine histogram discrepancies caused by steganographic embedding. Features such as neighbourhood degree and run-length histograms are analysed to detect inconsistencies in pixel distributions (Lee et al., 2021).

Applications of Steganalysis

1. **Cybersecurity**: Detecting and neutralising covert communication channels used for malicious purposes, such as identifying steganographic methods employed by attackers (Kaur and Kaur, 2014; Kunhoth et al., 2023).
2. **Digital Forensics**: Assisting investigations by revealing concealed data or altered media, this field ensures justice in court (Kaur & Kaur, 2014).
3. **Copyright Protection**: Preventing unauthorised usage by guaranteeing the integrity of digital watermarks included in multimedia content (Lee et al., 2021).

Steganalysis's Difficulties

Steganalysis has made great strides, but it still confronts several obstacles:

1. **Trade-off Between Robustness and Detection**: To cover a wide range of embedding techniques, universal approaches frequently compromise detection accuracy (Kunhoth et al., 2023).
2. **Developing Steganographic Techniques**: As sophisticated techniques like GAN-based steganography are developed, detection becomes more challenging (Kunhoth et al., 2023).
3. **High Data Volume**: Real-time analysis of sizable multimedia file collections presents processing difficulties (Lee et al., 2021).

Case Study and Experiment

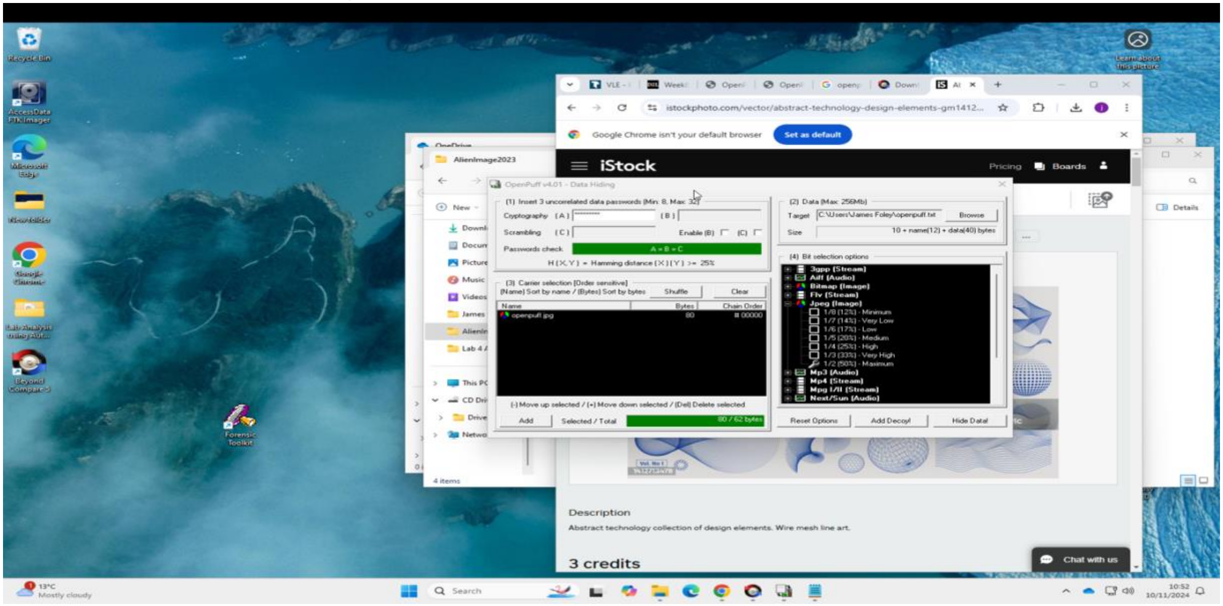
Research and practical applications depend critically on steganalysis, which has proven indispensable in revealing hidden facts inside digital media. This part presents two methods: a hands-on experiment with OpenPuff and ideas derived from a systematic review by Apau et al. (2024). These cases show how steganographic technologies interact with related steganalysis approaches to reveal their weaknesses.

1. Experiment using OpenPuff

This experiment implanted hidden data into an image file using the widely used steganography application OpenPuff. It evaluated the security limits, essential operation, and imperceptibility of a spatial-domain steganographic technique.

Procedure:

1. The secret message was a text file called open puff.txt.
2. Disabling secondary passwords, the embedding procedure used the carrier file openpuff.jpg and a single password (Puff1234!).
3. The "Hide Data!" command was followed using the maximum embedding capacity to test the storage capacity of the file.



OpenPuff v4.01 - Data Hiding

(1) Insert 3 uncorrelated data passwords (Min: 8, Max: 32)
Cryptography (A) ********** (B)
Scrambling (C) Enable (B) □ (C) □
Passwords check A = B = C
H (X, Y) = Hamming distance (X) (Y) >= 25%

(2) Data (Max: 256Mb)
Target C:\Users\James Foley\openpuff.txt
Size 10 + name(12) + data(40) bytes

(3) Carrier selection [Order sensitive]
(Name) Sort by name / (Bytes) Sort by bytes

Name	Bytes	Chain Order
openpuff.jpg	80	# 00000

(-) Move up selected / (+) Move down selected / (Del) Delete selected
Selected / Total 80 / 62 bytes

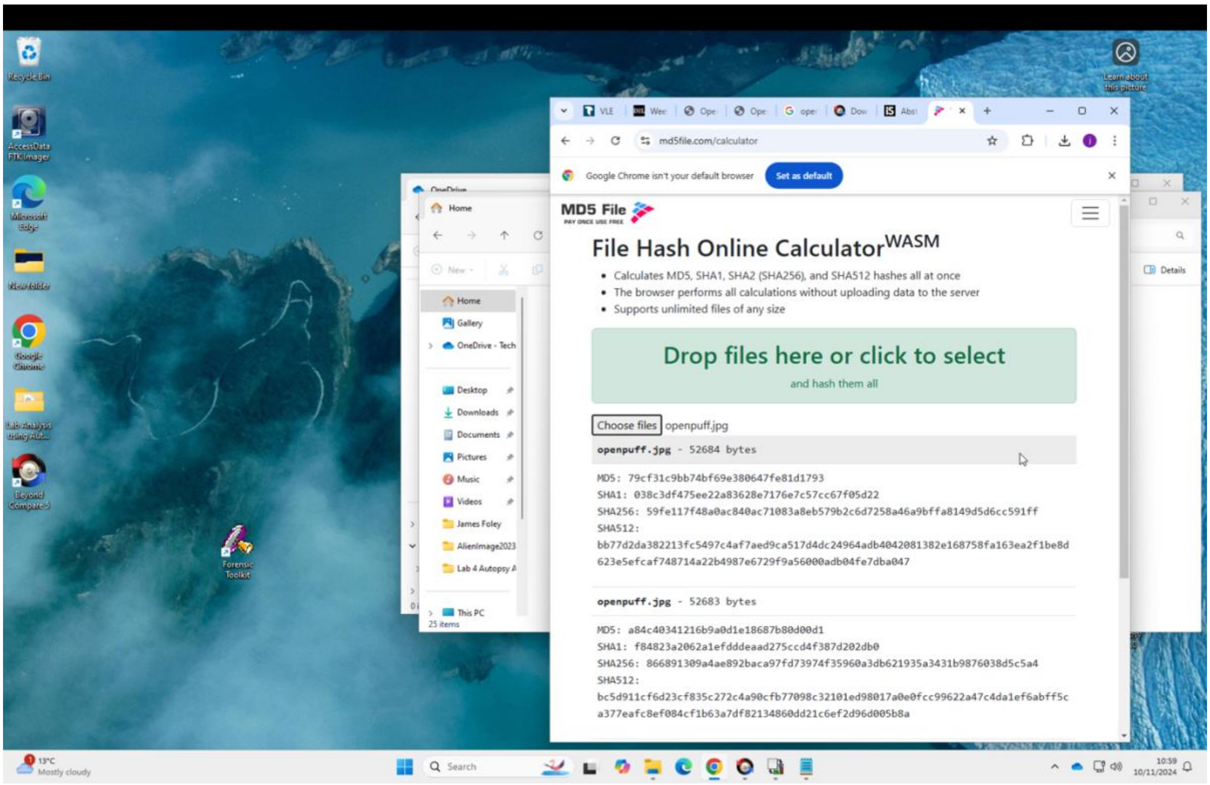
(4) Bit selection options
3gpp (Stream)
Aiff (Audio)
Bitmap (Image)
Flv (Stream)
Jpeg (Image)
□ 1/8 (12%) - Minimum
□ 1/7 (14%) - Very Low
□ 1/6 (17%) - Low
□ 1/5 (20%) - Medium
□ 1/4 (25%) - High
□ 1/3 (33%) - Very High
1/2 (50%) - Maximum
Mp3 (Audio)
Mp4 (Stream)
Mpg I/II (Stream)
Next/Sun (Audio)

Browse
Shuffle
Clear
Add
Reset Options
Add Decoy!
Hide Data!
istockphoto.com/vector/abstract-technology-design-elements-gm1412...
Google Chrome isn't your default browser
Set as default
iStock
Pricing
Boards
AlienImage2023
Description
Abstract technology collection of design elements. Wire mesh line art.
3 credits
Chat with us
13°C
Mostly cloudy
Search
10:52
10/11/2024

FIGURE 4 – EMBEDDING THE DATA (AUTHOR'S OWN WORK)

4. Using MD5file.com, hashes were produced for the original picture and the stego-image. Confirming the file had been changed allowed the different hash values to prove successful embedding.

- **Results**:



File Hash Online Calculator WASM

- Calculates MD5, SHA1, SHA2 (SHA256), and SHA512 hashes all at once
- The browser performs all calculations without uploading data to the server
- Supports unlimited files of any size

Drop files here or click to select

and hash them all

Choose files openpuff.jpg

```
openpuff.jpg - 52684 bytes

MD5: 79cf31c9bb74bf69e380647fe81d1793
SHA1: 038c3df475ee22a83628e7176e7c57cc67f05d22
SHA256: 59fe117f48a0ac840ac71083a8eb579b2c6d7258a46a9bffa8149d5d6cc591ff
SHA512:
bb77d2da382213fc5497c4af7aed9ca517d4dc24964adb4042081382e168758fa163ea2f1be8d
623e5efcaf748714a22b4987e6729f9a56000adb04fe7dba047

openpuff.jpg - 52683 bytes

MD5: a84c40341216b9a0d1e18687b80d00d1
SHA1: f84823a2062a1efdddeaad275ccd4f387d202db0
SHA256: 866891309a4ae892baca97fd73974f35960a3db621935a3431b9876038d5c5a4
SHA512:
bc5d911cf6d23cf835c272c4a90cfb77098c32101ed98017a0e0fcc99622a47c4da1ef6abff5c
a377eafc8ef084cf1b63a7df82134860dd21c6ef2d96d005b8a
```

FIGURE 5 – IMAGE AFTER DATA EMBEDDING (AUTHOR'S OWN WORK)

- **Visual Evaluation**: The visual evaluation indicated no apparent differences between the original picture and the stego-image, underlining the technique's effectiveness in avoiding detection by human observers.
- **Capacity**: The method used the maximum allowed data embedding without compromising the image's visual quality.
- **Discussion**:

This experiment shows the advantages and drawbacks of spatial-domain steganographic methods. Apau et al. (2024) mention that they are vulnerable to statistical steganalysis assaults like Chi-square and RS analysis, even if they shine in simplicity and capability here. Their results show that secret data can be revealed by even minor statistical errors, a restriction not entirely covered by this experiment.

2. Case Study: Systematic Literature Review by Apau et al. (2024)

Apau et al. (2024) performed a systematic literature study to assess the strength of many picture steganography methods against statistical steganalysis. Their results offer a theoretical structure to augment the OpenPuff experiment's discoveries.

- **Key Findings**:

1. Reviewed Techniques:

- **Spatial Domain Techniques**: Simple, effective, and able to hide big payloads, including LSB embedding and others. However, because of observable pixel value correlations (Apau et al., 2024), they are susceptible to statistical assaults such as RS and Chi-square.
- **Transform Domain Methods**: Techniques like the Discrete Cosine Transform (DCT) embed data in frequency coefficients, strengthening its resistance to geometric transformations and compression. However, their computational complexity surpasses spatial techniques (Apau et al., 2024).
- **Advanced Techniques**: Dynamic adaption to cover material allows advanced systems such as Generative Adversarial Networks (GANs) to resist detection dynamically. However, these methods demand enough information and processing capacity (Apau et al., 2024).

2. Performance Criteria:

- **Imperceptibility**: A fundamental measure in all fields that guarantees changes to the cover item stay invisible to human viewpoint.
- **Robustness**: Transform and adaptive approaches resist statistical steganalysis assaults better than conventional spatial procedures.
- **Capacity**: Although transform and adaptive approaches balance capacity and resilience, spatial strategies allow for greater payloads (Apau et al., 2024).

1. Applications and Challenges

Apau et al. (2024) underlined the rising steganography in cybersecurity, digital watermarking, and covert communication acceptance in digital infrastructure. They underlined, nonetheless, continuous difficulties, including:

- Juggling imperceptibility and resilience with embedding ability.
- Overcoming the computing difficulty of adaptive methods such as GANs.
- Addressing weaknesses in developing statistical assaults.

2. Discussion

This case study offers a broader view of the present status of steganography, therefore complementing the OpenPuff experiment. The observed practical restrictions in spatial approaches throughout the experiment match the weaknesses noted in the systematic study by Apau et al. (2024). Their emphasis on modern technology highlights the need for innovative ideas to stop always complicated attacks.

3. Conclusion

Combining a practical experiment with Apau et al. (2024), insights highlight the dual possibilities and difficulties in steganography and steganalysis. Although spatial methods such as those applied in the OpenPuff experiment show simplicity and great capacity, their weaknesses in statistical analysis emphasise the necessity of more solid solutions. Emphasising the need for ongoing innovation to solve the increasing complexity of steganalysis, the systematic review by Apau et al. (2024) offers a thorough knowledge of present approaches and their performance. These points of view present a complete picture of the present scene and future paths in this crucial field of information security.

Best Practices for Digital Forensics Investigators

Introduction

Modern forensic science is based on Edmond Locard's exchange principle: every interaction traces something (Casino et al., 2022). Although this idea started in conventional forensics, its importance now resides in the digital sphere as criminal activity leaves notable digital traces. The complexity of forensic investigations has become as digital devices and services become essential to everyday life and calls for a methodical approach to guarantee evidence integrity, appropriate methods, and legal admissibility (Casino et al., 2022). These parts offer practical instructions for digital forensics experts to solve problems and improve the results of their investigations.

Knowing Difficulties in Digital Forensics

Digital forensics involves technological, legal, and procedural obstacles. Casino et al. (2022) underline the need to understand domain-specific and cross-domain issues to improve forensic methods. Using a challenges-based, domain-specific mindmap, Figure 3 shows the range of problems across digital forensics fields, including mobile, IoT, cloud, and multimedia forensics.

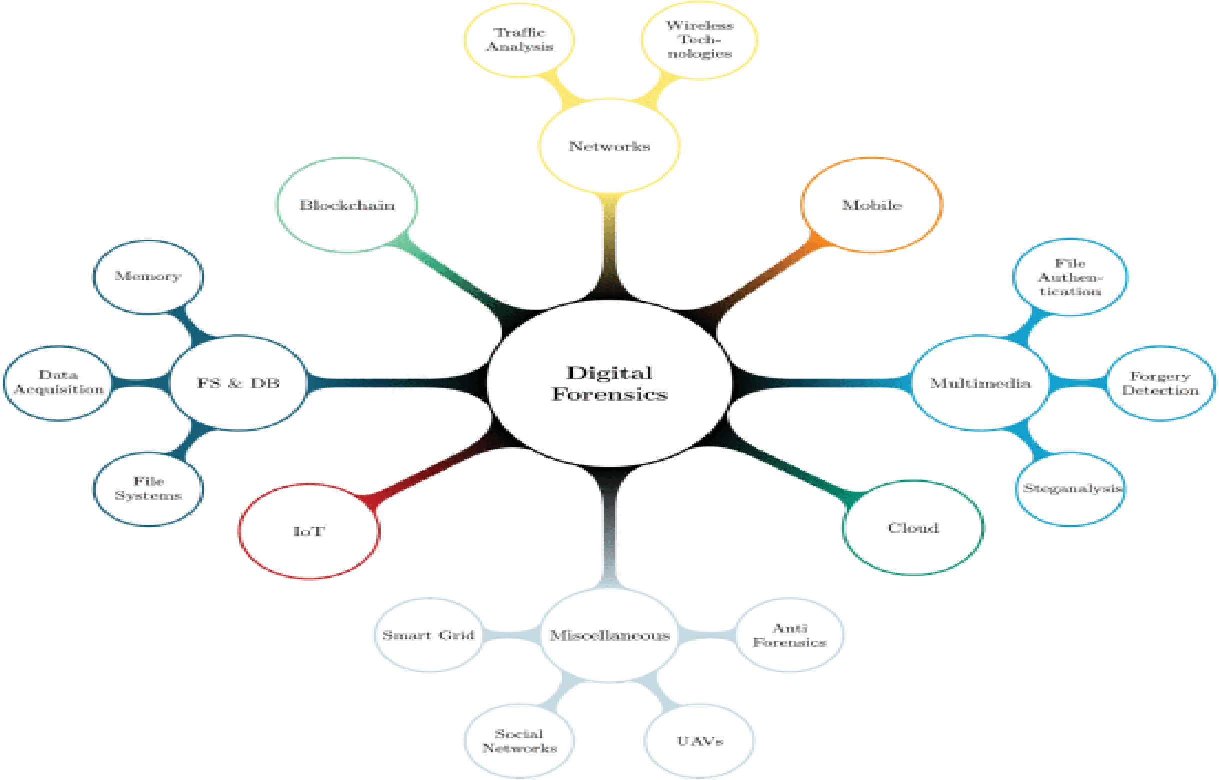


Figure 6: Challenges in Digital Forensics (Casino et al., 2022).

- **Legal Challenges**:

Legal challenges, data heterogeneity, and anti-forensics tactics severely hinder forensic methods. The expanding use of encryption, distributed platforms, and cross-border data transfer worsens these issues. Investigators require the right tools to address these issues appropriately.

Best Practices in Methodology

Researchers must adhere to specific protocols and standards to ensure exceptional forensic quality. From evidence gathering to reporting, standardised frameworks encompassing the whole investigation process—from Casino et al. (2022) and NIST criteria—emphasise their value.

- **Adopting Standardised Frameworks**:

NIST 800-86 and ISO/IEC 27043 offer methodologies for managing digital evidence under integrity preservation (Casino et al., 2022).

- **Chain of Custody**:

Maintaining an unbroken chain of custody will help ensure evidence's admissibility. Methods like timestamping and digital fingerprinting—e.g., SHA-2 hash—can assist (Ćosić & Bača, 2010).

- **Integrated Systems**:

Forensic systems should allow evidence from several domains (e.g., IoT and mobile forensics), guaranteeing smooth technology integration.

Forensic Problems in Multiple Domains

Casino et al. (2022) map digital forensic difficulties to many phases of the investigative process. Figure 4 graphically shows these difficulties, emphasising the need to tackle problems throughout evidence collecting, processing, and reporting.

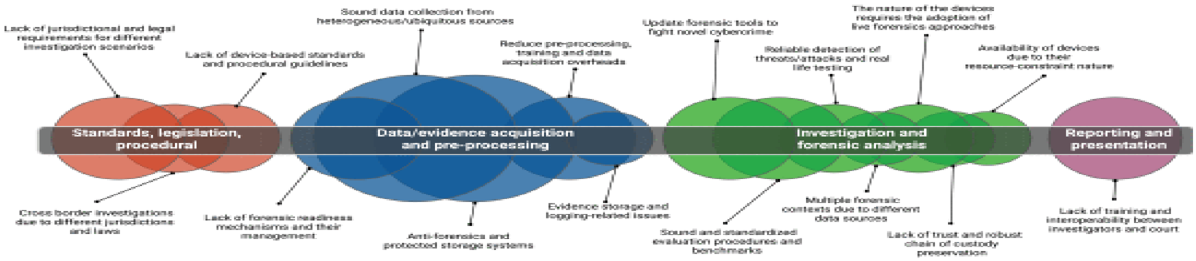

Lack of jurisdictional and legal requirements for different investigation scenarios
Lack of device-based standards and procedural guidelines
Sound data collection from heterogeneous/ubiquitous sources
Reduce pre-processing, training and data acquisition overheads
Update forensic tools to fight novel cybercrime
Reliable detection of threats/attacks and real life testing
The nature of the devices requires the adoption of live forensics approaches
Availability of devices due to their resource-constraint nature
Standards, legislation, procedural
Data/evidence acquisition and pre-processing
Investigation and forensic analysis
Reporting and presentation
Cross border investigations due to different jurisdictions and laws
Lack of forensic readiness mechanisms and their management
Anti-forensics and protected storage systems
Evidence storage and logging-related issues
Sound and standardized evaluation procedures and benchmarks
Multiple forensic contexts due to different data sources
Lack of trust and robust chain of custody preservation
Lack of training and interoperability between investigators and court

FIGURE 7: DIGITAL FORENSIC CHALLENGES MAPPED TO INVESTIGATION PHASES (CASINO ET AL., 2022).

Finding Evidence

- **Challenges**:

Data heterogeneity, instability, and encryption all typically impede evidence collection. Jurisdictional issues, decentralised IoT devices, and cloud platform designs also provide unique difficulties.

- **Recommendations**:

Investigators should use reliable acquisition technologies and frameworks that cater to specific fields (Casino et al., 2022).

Examining and Interpreting Data

- **Challenges**:

Managing big datasets (e.g., multimedia files) and opposing anti-forensics policies complicates the study even more.

- **Technological Support**:

Machine learning and AI-based techniques have shown promise in automating aspects of the research while preserving accuracy (Casino et al., 2022).

Legal Compliance: Reporting

- **Importance**:

Good reporting guarantees that results are readily available to non-technical players such as attorneys and judges.

- **Approach**:

Investigators must follow set reporting forms to improve readability and guarantee the admissibility of evidence in court (Casino et al., 2022).

Legal and Technological Readiness

Digital forensics detectives must always be technologically and legally ready to handle new problems. Casino et al. (2022) and NIST rules are essential to keeping ahead of hackers, so researchers should always learn innovative forensic tools and methodologies.

- **Emerging Technologies**:

Blockchain, artificial intelligence, and IoT need fresh forensic approaches to handle their particular features (Casino et al., 2022).

- **Ethical Issues**:

Digital evidence needs ethical handling. Following international norms and privacy regulations assures that investigations remain legally sound (Casino et al., 2022).

Conclusion

Driven by consumers' massive digital footprints, digital forensics has become necessary for modern investigations. Still, managing different data and negotiating international legal complications can be challenging. Following standardised approaches, using innovative technology, and guaranteeing ethical compliance can help researchers overcome obstacles and strengthen the validity of their results.

As Casino et al. (2022) underlined, expanding the area of digital forensics depends on a comprehensive strategy addressing issues in many spheres and research stages.

Conclusion

The field of digital forensics is expanding quickly, and two methods that are becoming increasingly significant are steganography and steganalysis. As evidenced by a thorough examination of steganographic methods and detection processes, strong investigative tools and frameworks are necessary to handle the constantly changing problems caused by hidden data. The results of Apau et al. (2024) and the OpenPuff experiment highlight the limitations and combined promise of the currently employed approaches. Both trials highlight the need to fuse theoretical innovations with real-world applications.

Researchers can use the best practices described in this study as a guide to improve the precision and dependability of their research. These best practices include being technologically prepared, following ethical guidelines, and following standardised frameworks like NIST and ISO. Data diversity, encryption, jurisdictional complexity, and the need for ongoing innovation and cross-disciplinary cooperation are some of the difficulties. The study concludes that steganography competence is crucial for maintaining justice in the digital era. It also encourages forensic professionals to use cutting-edge, flexible, and moral methods to be ahead of the curve regarding cybercrime issues.

Bibliography

Apau, R., Asante, M., Twum, F., Ben Hayfron-Acquah, J. and Peasah, K.O. (2024) ‘Image Steganography Techniques for Resisting Statistical Steganalysis Attacks: A Systematic Literature Review’. *PLOS One*, Vol. 19 (9), e0308807.

Casino, F., Dasaklis, T.K., Spathoulas, G.P., Anagnostopoulos, M., Ghosal, A., Borocz, I., Solanas, A., Conti, M. and Patsakis, C. (2022) ‘Research Trends, Challenges, and Emerging Topics in Digital Forensics: A Review of Reviews’. *IEEE Access*, Vol. 10, pp. 25464–25493.

Djebbar, F., Ayad, B., Meraim, K.A. and Hamam, H. (2012) ‘Comparative Study of Digital Audio Steganography Techniques’. *EURASIP Journal on Audio, Speech, and Music Processing*, Vol. 2012, pp. 1–16.

Kaur, M. and Kaur, G. (2014) ‘Review of Various Steganalysis Techniques’. *International Journal of Computer Science and Information Technologies*, Vol. 5 (2), pp. 1744–1747.

Krenn, R. (2004) ‘Steganography and Steganalysis’. Available at: https://www.krenn.nl/univ/cry/steg/article.pdf (Accessed: 1st December, 2024).

Lee, C., Weng, C., Wang, C., Chakraborty, G., Sakurai, K. and Tsai, K. (2021) ‘Research on Multimedia Application on Information Hiding Forensics and Cybersecurity’. *International Journal of Network Security (IJNS)*, Vol. 23, pp. 1093–1107.

Li, B., He, J., Huang, J. and Shi, Y.Q. (2011) ‘A Survey on Image Steganography and Steganalysis’. *Journal of Information Engineering*, Vol. [Details Missing], pp. [Details Missing]. Available at: https://www.researchgate.net/publication/228527555_A_survey_on_image_steganography_and_steganalysis (Accessed: 1st December, 2024).

Shehab, D.A. and Alhaddad, M.J. (2022) ‘Comprehensive Survey of Multimedia Steganalysis: Techniques, Evaluations, and Trends in Future Research’. *Symmetry*, Vol. 14 (1), p. 117.