applied sciences

MDPI

Review

Systematic Review: Anti-Forensic Computer Techniques

Rafael González Arias, Javier Bermejo Higuera, J. Javier Rainer Granados, Juan Ramón Bermejo Higuera and Juan Antonio Sicilia Montalvo *

Escuela Superior de Ingeniería y Tecnología, Universidad Internacional de La Rioja, Avenida de La Paz, 137, 26006 La Rioja, Spain; rafael.gonzalez715@comunidadunir.net (R.G.A.); javier.bermejo@unir.net (J.B.H.); javier.rainer@unir.net (J.J.R.G.); juanramon.bermejo@unir.net (J.R.B.H.)
* Correspondence: juanantonio.sicilia@unir.net

Abstract: The main purpose of anti-forensic computer techniques, in the broadest sense, is to hinder the investigation of a computer attack by eliminating traces and preventing the collection of data contained in a computer system. Nowadays, cyber-attacks are becoming more and more frequent and sophisticated, so it is necessary to understand the techniques used by hackers to be able to carry out a correct forensic analysis leading to the identification of the perpetrators. Despite its importance, this is a poorly represented area in the scientific literature. The disparity of the existing works, together with the small number of articles, makes it challenging to find one's way around the vast world of computer forensics. This article presents a comprehensive review of the existing scientific literature on anti-forensic techniques, mainly DFIR (digital forensics incident response), organizing the studies according to their subject matter and orientation. It also presents key ideas that contribute to the understanding of this field of forensic science and details the shortcomings identified after reviewing the state of the art.

Keywords: computer anti-forensic; computer forensic; computer security

Citation: González Arias, R.; Bermejo Higuera, J.; Rainer Granados, J.J.; Bermejo Higuera, J.R.; Sicilia Montalvo, J.A. Systematic Review: Anti-Forensic Computer Techniques. *Appl. Sci.* **2024**, *14*, 5302. https://doi.org/10.3390/app14125302

Academic Editor: David Megías

Received: 30 April 2024
Revised: 5 June 2024
Accepted: 17 June 2024
Published: 19 June 2024

1. Introduction

In computer security, computer forensics is a set of procedures and techniques for identifying, collecting, and documenting evidence from a computer system to make this evidence acceptable during a legal proceeding.

Due to the constant growth of the importance of computer security in everyday life, both in the public and the professional sector, computer forensics continues to grow and become more specialized with each passing year.

Like every existing discipline within computer science, the forensic field has its antagonists. These are known as anti-forensic techniques. These methods, in their broadest definition, have as their main objective the hindering or impeding of the investigation and collection of the data contained in a computer system [1].

In 2009, an article by P. Pajek et al. [2] entitled "Computer anti-forensics methods and their impact on computer forensic investigation" had already began to highlight the problems generated by these increasingly automated techniques in computer forensics. In this article, tables are drawn up showing the results before and after the application of anti-forensic tools, allowing for a quick appreciation of the differences. The problem is becoming more and more evident.

On a first review of the state of the art in this subject, it may seem a relatively small and unimportant field, as shown by the results obtained in a specific thematic search example with the token "computer forensics" versus the search topic "computer anti-forensics", shown in Figure 1.

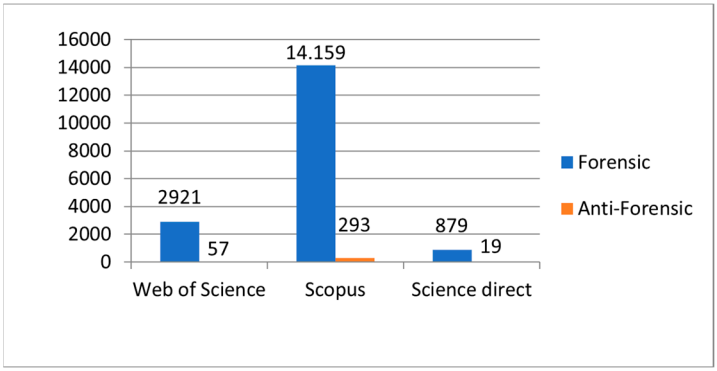

Figure 1. Thematic search results.

In addition, most of the results for anti-forensic techniques are related to image processing (image and video manipulation); it is necessary to refine and deepen the searches to find articles directly related to these techniques as applied to the general field of forensic analysis.

With such a vast difference between the scientific research in one field and the other, it could be assumed that the relevance of anti-forensic techniques is negligible, and that it is not worthwhile to delve into this field. However, when reviewing some of the most outstanding articles on this subject, we can see that the lack of knowledge of anti-forensics throws away the application of most of the existing forensic techniques and advances.

How is this possible and where does the big difference in the number of scientific investigations between the two fields come from? To answer this question, we must first analyze the following two articles:

- T. Latzo et al. [3] elaborate a taxonomy of forensic acquisition methods, which is a comprehensive survey of state-of-the-art memory acquisition techniques, independent of the operating system used and the hardware architecture.
- R. Palutke et al. [4] present a study with three novel methods that prevent user space memory from appearing in analysis tools and also make it inaccessible from the perspective of security analysts.

As can be seen, without knowing and avoiding the anti-forensic techniques described in the second article, the first study loses much of its value, despite its novelty. Therefore, although anti-forensic techniques represent a small percentage of computer forensics, their importance is very high.

The difference in the number of publications is also directly related to the number of years that forensic analysis techniques have been available in the international context, compared to the relatively few years that anti-forensic techniques have been studied.

The systematic review performed in this article followed the guidelines set out in the work of B. Kitchenham et al. [5–7], resulting in the following contributions:

- Review of the existing scientific literature on anti-forensic techniques.
- Grouping of the analyzed works according to the subject orientation within the field of anti-forensic techniques.
- Within each topic, grouping of the analyzed works according to the technique they include.
- Analysis of the state of the art of the last 6 years (2016–2022).
- Exposition of ideas for the improvement of the field of anti-forensic techniques based on the shortcomings analyzed in the review of the state of the art.

The document is structured as follows:

- Section 2—Materials and Methods: This section presents how the systematic review was carried and how documents were selected to be included in this study.
- Section 3—Fundamentals of anti-forensic science: Presentation of the most significant documents related to anti-forensics science in the recent literature.

- Section 4—Results: Grouping of the documents obtained into categories and presentation of the findings of our study of the documents.
- Section 5—Conclusions: General conclusions obtained from the review of the work included are detailed here, and recommendations are made as to how to correct the deficiencies detected.

2. Materials and Methods

2.1. Review Methodology

The guidelines set out in the work of B. Kitchenham et al. [5–7] were followed to prepare this review. To carry out this systematic review, the steps shown in Figure 2 were followed:

1. Definition of the research questions.
2. Selection of the bibliographic databases to be used.
3. Selection of search criteria.
4. Selection of criteria for inclusion and exclusion of results.

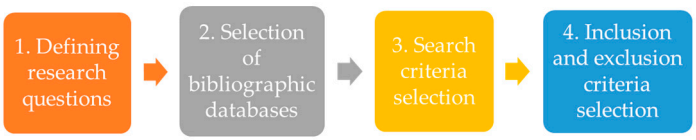

Figure 2. Review methodology.

2.1.1. Definition of Research Questions

As stated in previous paragraphs, the purpose of this article is to study and investigate the literature related to anti-forensic techniques and then to classify it and delve into the most significant documents published in each category. For this purpose, a series of questions have been elaborated, as shown in Table 1.

Table 1. Research questions.

Research Questions	Details
What is the current state of the art related to anti-forensic techniques? What type of these techniques are most emphasized in the literature? Is there any type of technique that is increasingly present?	Knowing the scope and extent of the current articles related to anti-forensic techniques allows us to better position them in the landscape of information communication technologies (ICT) forensics. A greater number of articles related to a particular technique may signify the need to focus on that type in the future.
A systematic review of anti-forensic techniques How can new studies be classified? What do the new studies have to offer?	Reviewing the current literature makes it possible to classify it according to its purpose. In addition, it is possible to evaluate the contributions made by comparing them with those already existing and with each other.

2.1.2. Bibliographic Databases Used

For a systematic review to be of high quality, it is necessary to use a large search source to find relevant literature. For this article, the following databases have been considered when searching:

- IEEE Xplore (https://ieeexplore.ieee.org).
- ACM (https://dl.acm.org).
- Science Direct (https://sciencedirect.com).
- Web Of Science (https://www.webofscience.com).
- Scopus (https://scopus.com).

2.1.3. Search Criteria

When searching for the most relevant research articles with respect to the subject of this research, a series of strings were created related to the subject matter. During the testing of these strings, it was found that using the terms "anti-forensic techniques", "anti-forensics", and "anti-forensics" returned very different results, some of which excluded articles that were candidates for analysis. Therefore, all these synonyms were used in the initial search.

Table 2 shows the search string for the three synonyms. The results field shows the total number of articles obtained by the string with the three synonyms.

Table 2. Search queries.

Source	Search Fields	Years	Documents	Results
ieeexplore.ieee.org	*(("Document Title": anti-forensic techniques) AND ("Abstract": anti-forensic techniques)) OR (("Document Title": anti-forensics) AND ("Abstract": anti-forensics)) OR (("Document Title": antiforensics) AND ("Abstract": antiforensics))*	2010–2022	Conferences, Journals, Articles, Early Access Articles, Papers, Books	47
dl.acm.org	*[[Title: "anti-forensic techniques"] OR [Title: "anti-forensics"] OR [Title: "antiforensics"]] AND [[Keywords: anti-forensic techniques] OR [Keywords: anti-forensics] OR [Keywords: antiforensics]]*	2006–2022	Idem	6
sciencedirect.com	*Title, abstract, keywords: "anti-forensic techniques" OR "anti-forensics" OR "antiforensics"*	2006–2022	Idem	90
Web of Science	*(((TS = ((anti-forensic techniques)OR(anti-forensics)OR(antiforensics))) AND TI = ((anti-forensic techniques)OR(anti-forensics)OR(antiforensics))) AND AB = ((anti-forensic techniques)OR(anti-forensics)OR(antiforensics)))*	2006–2022	Idem	143
Scopus	*TITLE-ABS-KEY ("anti-forensic techniques" OR "anti-forensics" OR "antiforensics") AND (LIMIT-TO (SUBJAREA,"COMP"))*	2006–2022	Idem	536
			Total Documents	822

The selected date range criterion ranges from the first recognized relevant publication in 2006 to 2022; however, some sources do not have documents from that date, so the furthest date available has been used.

2.1.4. Document Inclusion and Exclusion Criteria

Once the documents obtained from the search had been gathered, they went through a series of filtering stages until those relevant to the case study were obtained. In the first phase, duplicates were eliminated based on coincidence criteria such as DOI and, in the case of lack of a DOI, by identical title and authors.

The documents obtained in the second phase were classified according to type of objective/purpose for inclusion in Section 4 (Results). In this phase, 220 documents were obtained.

At the same time, among these 220 papers, those with a publication date within the last 6 years were selected for analysis of some of the most relevant ones in Section 3 (Fundamentals of anti-forensic science).

This process can be seen in Figure 3.

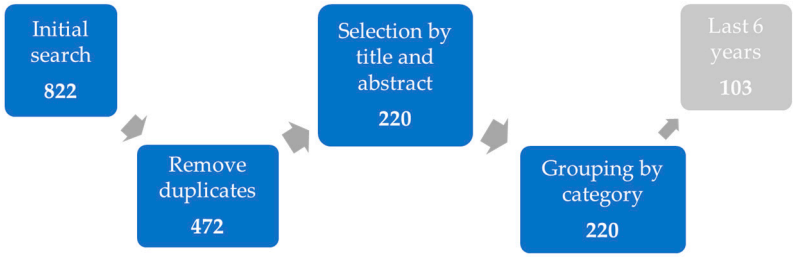

Figure 3. Document selection process.

Of the 220 total papers accepted according to the above criteria, it can be seen that from 2013 onwards, the average number of articles per year is much higher than in previous years, even doubling. This fact can be seen in Figure 4.

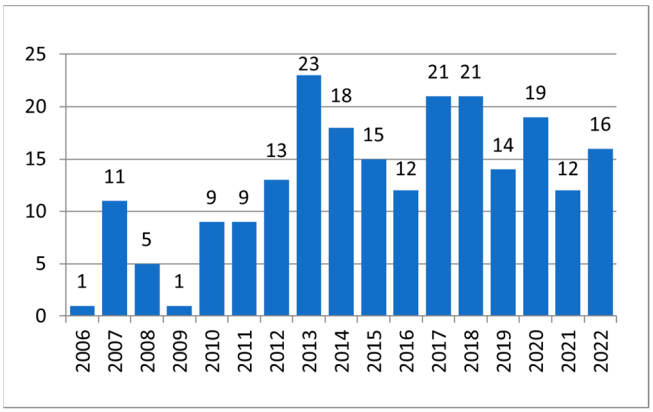

Figure 4. Publications accepted by year.

3. Fundamentals of Anti-Forensic Science

Having established the relevance of the knowledge of anti-forensic techniques in the context of computer forensics, a detailed and in-depth analysis of some of the most significant papers of the last 6 years (2016–2022) is performed, selected following the criteria of article impact and number of citations. Some studies present the first articles on a particular topic, others present the most-accepted taxonomies, and current articles of relevance to their categories are also included. All other articles included in this review will be analyzed in the following section (Section 4).

K. Conlan et al. [8] present an expanded version of the anti-forensic taxonomy originally presented by M. Rogers [9] and develop a "dataset" of anti-forensic tools. Based on the original classification proposed by M. Rogers [9], they expand and categorize the anti-forensic tools analyzed according to the following fields (Figure 5):

1. Data hiding.
2. Artefacts deletion.
3. Obfuscation of traces.
4. Direct attacks on forensic software and procedures.
5. Possible indications of anti-forensics.

The strength of this work resides in its dataset of 308 anti-forensic tools and their hashes, as well as the extension of the anti-forensic taxonomy to a specific case study.

Something remarkable that the research does not develop is the detailed explanation of each extra field added in the extended classification of anti-forensic tools; this is unlike the work of N. A. Hassan et al. [10], in which each section of the classification they use is explained.

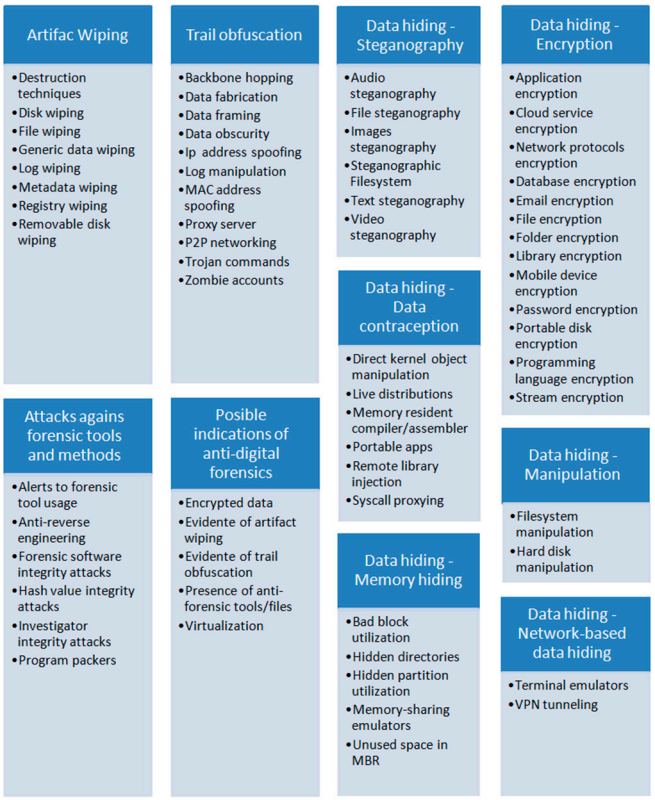

Figure 5. Expanded taxonomy of K. Conlan et al. [8].

N. A. Hassan et al. [10] elaborate a wide classification of the most common anti-forensic techniques and complement it with explanations, making use of tables and images. They focus their work on a legal case study, which can be used by entities who need to guarantee their privacy, such as diplomats, security professionals, military personnel, etc.

The study is divided into four major fields:

1. Data destruction.
2. Anti-forensic techniques in Windows.
3. Digital evidence destruction.
4. Direct attacks on forensic software.

It develops, in table form, some of the most common techniques for erasing information on hard disks (Table 3). It should be noted that in general, it is a good synthesis of the anti-forensic taxonomy. As the study is oriented towards legal use cases, the bias of the study leans towards that domain, lacking certain content that is more typical of illicit activities, that is, those related to computer viruses, malware, and (unethical) hacking.

B. Hoelz et al. [11] bring a new vision to the field of anti-forensic techniques, proposing a threat and risk management model to mitigate the negative impact they cause during a forensic analysis. Their study used the classification model presented by R. Harris [12], which organizes the actions executed by an attacker into four groups:

1. Evidence destruction.
2. Destruction of the source of evidence.
3. Evidence concealment.
4. Evidence tampering.

Table 3. Data destruction techniques.

Erasing Method	Security Level	Overwriting Rounds	Pattern Used	Comments
Single overwrite	Low	1	Writes a zero	Can prevent software recovery tools from recovering data but cannot stop hardware-based recovery tools from recovering deleted data.
NCSC-TG-025 (US National Security Agency)	High	3	All zeros, all ones, and finally writes a random character and verifies the write	Software recovery tools and most hardware-based recovery tools cannot recover data deleted this way. This technique is like HMG IS5 (UK) and DoD 5220.22-M (USA).
Gutmann	High	35	Writes a random character	This is an old technique invented in 1996; the encoding for HDD has changed since then. This method is not recommended for modern HDDs.
Schneier	High	7	All ones, all zeros; random characters are written five times	Prevents software recovery tools and almost all hardware-based techniques from recovering data.
ISM 6.2.92	Medium	1	Random pattern (only for disks bigger than 15 GB)	Invented in 2014 by the Australian Department of Defense: Intelligence and Security. Prevents software recovery tools and most hardware-based techniques from recovering data.

To conclude, sections on direct attacks on forensic software represent a very small fraction of the anti-forensic techniques dedicated to hiding the commission of illegal activities; therefore, it would be necessary to complement it with other articles to obtain a larger knowledge base.

Based on these considerations, they present the threat model shown in Figure 6.

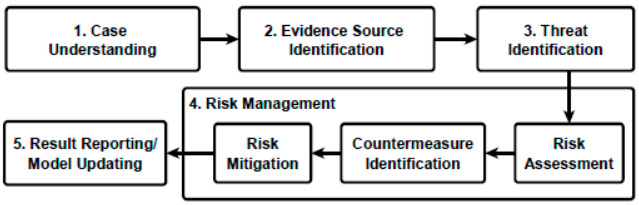

Figure 6. Threat model of B. Hoelz et al. [11].

With the development of these sections, they elaborate a system with which to apply the proposed threat model to the stages of forensic analysis, as detailed in the study by N. L. Beebe et al. [13].

The proposed model, although limited in its development, is an example of the need to apply risk analysis to digital forensic activities.

A significant expansion of the risks to be considered, as well as the sections to be included in the study, would be necessary in order to develop what could be considered a new standard for the study and assessment of risks in digital forensics.

M. I. Al-Saleh et al. [14] set out a series of analysis guidelines for gathering evidence when detecting user accounts that have been deliberately deleted. Generally, these accounts have been used in illicit activities, and it is desirable to detect whether they have existed previously, as well as to obtain information from them. The authors begin by outlining the artefacts they will use for analysis, along with a short description of the artefacts:

1. Windows events.
2. Windows registry.

3. RAM.
4. Memory paging system.
5. Windows prefetch system.
6. Windows Superfetch system.
7. Windows image cache.
8. Windows jump lists.
9. Navigation files.

The main utility of this development is that it serves as a starting point for research on user account deletion. It identifies the most important artefacts in this type of analysis and makes a detailed use case, which allows for extrapolation to different Windows operating systems.

The study itself mentions as its limitations the obtaining of information from the RAM if the equipment is turned off; some registers are not activated by default in the operating systems, and the browsers incorporate options easily modified by the user, which allow for almost all the stored registers to be eliminated.

This work, which is complemented by others detailing data deletion tools (N. A. Hassan et al. [10]), provides a better idea of how to recover evidence and determine if deletion tools have been used.

M. Gül et al. [15] have elaborated a study in which they highlight the great importance that the subject of "anti-forensics" has acquired, to the point of becoming an emerging field of study in need of major expansion. It exposes the general anti-forensic categories, bringing together what has been published by several authors in the following classification system:

- Data hiding, obfuscation, and encryption.
- Deletion or destruction of data.
- Data tampering.
- Prevention of analysis.
- Obstruction of trace collection.
- Subversion tools.

The study mentions the need to present more-modern anti-forensic techniques, and this is why it focuses on the following classifications:

- Data pooling.
- Non-standard RAID disks.
- File signature manipulation.
- Restricted file names.
- MACE time manipulation
- Loop references.
- Hash collisions.
- Fake hard disks.

In explaining each of these fields, they make these anti-forensic techniques known and suggest measures by which to avoid or mitigate them as much as possible. The objective of this study has two components:

- To serve as a knowledge update for anti-forensic experts.
- To show where to look if you suspect the use of any of these techniques.

The limitations of the work are evident based on the objectives it pursues. It is an update of knowledge, not a new classification of anti-forensic techniques; therefore, the detail in the explanation is quite limited compared to other more explicit explanations, such as the one elaborated by N. A. Hassan et al. [10].

A. R. Mothukur et al. [16] present several suggestions for how to address the following weaknesses present in computer forensics:

- The human element in the process.
- Reliance on forensic tools.

- Physical and logical limitations.

The paper aims to investigate some anti-forensic methods and tries to summarize some of the countermeasures that can be applied. The main limitations of this study are that the countermeasures proposed do not resemble a methodology by which to extract guidelines to follow or a practical guide to be applied in use cases. The authors propose a set of suggestions applied to each of the weaknesses exposed by R. Harris [12] in his article.

The work could be considered an exposition of ideas that should be considered when it comes to standardizing and further formalizing the guidelines of the computer forensic discipline.

M. A. Wani et al. [17] focus their attention on the study of anti-forensic techniques applied to file systems. To develop it, they use the traditional classification of anti-forensic techniques—i.e., artefacts deletion, data hiding, evidence obfuscation, and attack on forensic tools)—but focus on their application to file systems. For each of the sections into which the article is divided, the article defines what the anti-forensic technique consists of and some of the tools with which they are performed. The sections are as follows:

- Artefact wiping.
- Data hiding.
- Reserved locations.
- Slack space.
- Extended attributes, forks, and alternate data streams.
- Cryptographic file systems.
- Steganographic file systems.
- Mounting.
- Trail obfuscation.
- Forging timestamp.
- Modifying magic numbers.
- Using live distros.
- Attacking forensic tools.
- Dropping a compression bomb.
- Opening a sparse file.
- HPA/DCO, file encryption, and steganography.

The objective of the work being the exposition of anti-forensic techniques, focusing on the file system, it can be said that it exposes, briefly and concisely, each one of the above sections, making the forensic investigator aware of the most problematic techniques that can be found during the analysis of a computer system.

This study is a good complement to the rest of the works presented, and the limitation of this research is the same as most of them, which is that it does not present a methodology that allows the forensic investigator to detect or avoid the use of these anti-forensic techniques.

D. I. Jang et al. [18] present a forensic analysis method by which to detect a particular anti-forensic technique, known as timestamp forgery/time stomping, for the specific case of the NTFS file system. To carry out this work, they focus on the $MFT and $LOGFILE structures. The main attributes that the paper discusses are the $LogfileSequenceNumber (LSN), $Standarddy, and $Filename. The authors establish two timestamp forgery processes generated by the malware:

- Change the operating system timestamp.
- Manipulate the MACE values of NTFS system files.

Having explained all the above, the authors of the article go on to generate mathematical formulae to establish 14 normal file processing patterns and 7 comparison rules for detecting timestamp forgery.

Although it is a very particular and small analysis case, regarding the set of existing anti-forensic techniques, it is quite relevant since time stomping is a very frequent mode of

attack within the evidence tampering section, meaning that the study is directly concerned with the most frequent anti-forensic techniques used.

Further, a great number of the patterns to be categorized are missing; 14 patterns are not many with respect to the total number of actions that can be performed on a file, although they include the most frequent ones. It is, therefore, a very specific topic, but a useful one in its application by forensic investigators, and further development may result in an automatic tool that can detect these cases.

Sudhakar et al. [19] present an analysis method by which to detect a particular type of malware, known as "fileless malware", which makes use of many different anti-forensic techniques to accomplish its goals without being detected. In this study, they pursue the following objectives:

- Analyze the behavior and mechanisms of this malware, in detail.
- Analyze the solutions given by other researchers for its detection.
- Propose an incident investigation and response model.

For this purpose, they organize the document into four main sections:

- Introduction and knowledge about fileless malware.
- Analysis of fileless malware according to its persistence techniques.
- Fileless malware detection techniques.
- Incident model.

The infection flow can be seen in Figure 7.

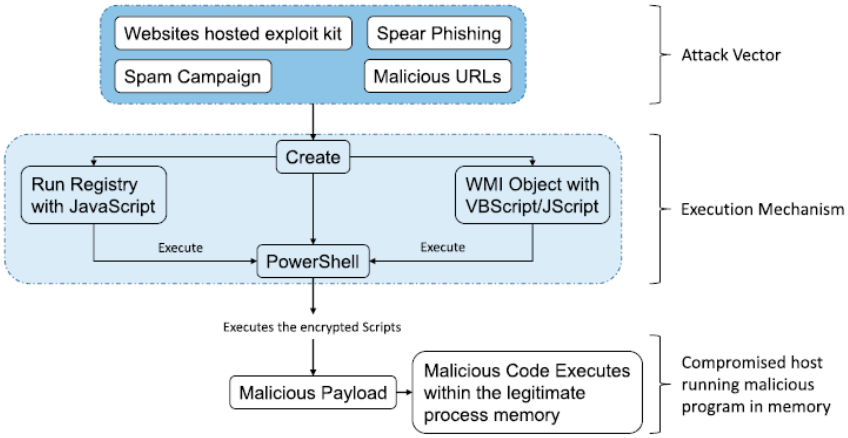

Figure 7. Malware injection flow (Sudhakar et al.) [19].

In conclusion, the authors mention the need to learn more about fileless malware attacks due to the ability of this kind of malware to evade signature-based detection systems.

They concisely explain the main infection processes, as well as the tools used for this purpose. Using several tables and figures, they present some of the main anti-forensic techniques used by this malware to obfuscate its code, comparing it with traditional malware.

The solutions they provide for detecting it in a system, together with the bibliography they provide, fall short of being able to reproduce it using analysis; however, it is a consistent basis on which to begin to investigate the subject in further depth.

H. Li et al. [20] designed a multipurpose classification model for detecting manipulations of a multimedia image to determine its authenticity by applying different anti-forensic techniques on images and measuring the similarities between the inconsistencies generated by each technique. They organized their study into the following sections:

- Image processing analysis and anti-forensic operations.
- Algorithm proposal.
- Experiment results.

They develop an algorithm to test in their experiments, and through 11 image processing and 12 anti-forensic operations, they conclude that the scheme they propose is effective and conclude the paper by suggesting, as future work, extending the study to detect and locate the regions that have been manipulated into the image.

This article is just another in a long line of articles demonstrating the need for serious consideration of anti-forensic techniques as they undermine many of the advances in forensic techniques.

4. Results

The papers included in this review employ such different techniques and deal with such disparate topics within the anti-forensic sciences that a direct comparison between them is not possible.

Therefore, for ease of understanding, in this chapter, the papers have been grouped into four main areas according to the type of objective/purpose of the paper: weaknesses and use cases of anti-forensic sciences; exposition of techniques; new threat models and forecasts; anti-forensic sciences and malware (see Figures 8 and 9).

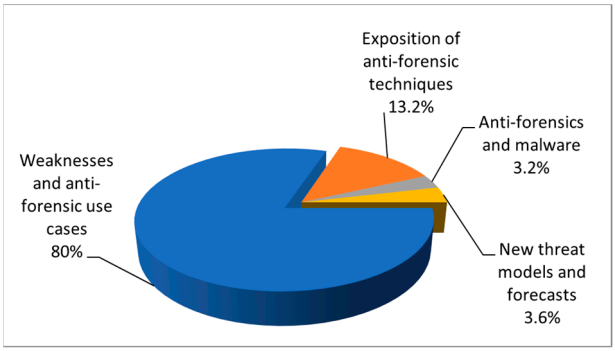

Figure 8. Publications grouped by section (percentages).

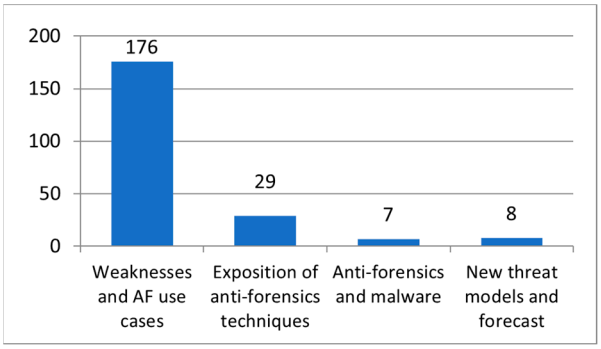

Figure 9. Publications by section and number of articles.

For each paper, a brief description of the article is mentioned, highlighting its main contribution in its field.

It is necessary to mention again that most of the studies presented are oriented towards digital forensic investigation for incident response (DFIR).

4.1. Weaknesses and Anti-Forensic Use Cases

This section, represented in Figures 10 and 11, groups the papers whose main theme is to expose the weaknesses of a domain and the related anti-forensic use cases. A multitude of papers could be included in several sections; therefore, the main criterion for their grouping is, more specifically, main objective sought by the authors.

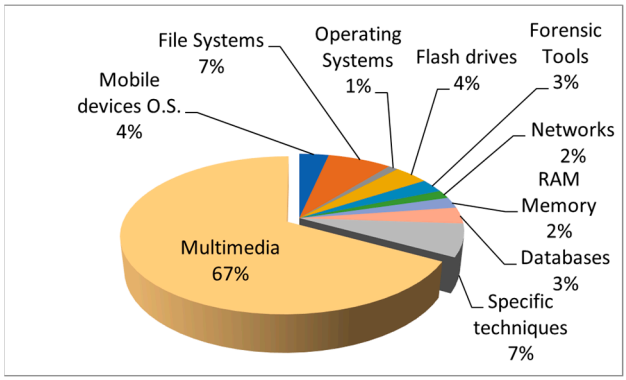

Figure 10. Weaknesses and anti-forensic use cases (percentages).

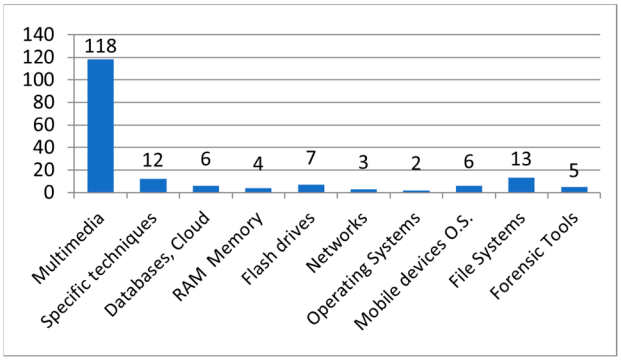

Figure 11. Weaknesses and anti-forensic use cases and number of articles.

Table 4 lists the works classified according to the categories established and described in Section 4.1.

Table 4. Studies classified by category in Section 4.1 (weaknesses and anti-forensic use cases).

Weaknesses and Anti-Forensic Use Cases	Number of Studies	References
Multimedia systems	118	[21–139]
Specific techniques	12	[140–151]
Databases, cloud	6	[152–157]
RAM Memory	4	[4,158–160]
Flash drives	7	[161–167]
Networks, IoT	3	[168–170]
Operating Systems	2	[171,172]
Mobile devices O.S.	6	[173–178]
File Systems	13	[17,18,179–189]
Forensic Tools	5	[190–194]

4.1.1. Weaknesses and Anti-Forensic Use Cases: Multimedia Systems

This section represents most of the articles and is oriented towards anti-forensic techniques applied to images and videos. With 53.64% of the total number of selected articles (220), it can be stated that most of the publications related to anti-forensic techniques are aimed at analyzing and addressing the weaknesses of multimedia systems.

- M. A. Qureshi et al. [21] provide an overview of various anti-forensic techniques and countermeasures proposed in the literature, together with a bibliographic analysis

of vanguard publications in different areas. J. Yu et al. [22,23] add a method for the general detection of these techniques using convolutional neural networks (CNNs). On the other hand, G. Cao et al. [24–29] attempt to detect contrast enhancement (CE) techniques. J. Y. Sun et al. [30,31] use CNNs to detect CE techniques.

Several studies [22,23,31,32] use neural networks (CNNs and GANs) to detect or generate forensic images, demonstrating their effectiveness in learning forensic traces and generating sophisticated anti-forensic attacks. Other approaches [25,26] are based on the analysis of first- and second-order statistics and Laplacian modeling to detect contrast enhancement and anti-forensic techniques. Methods based on CNN [22,31,32] and GAN (generative adversarial networks) [23,29] show high accuracy and robustness in detecting forgery and anti-forensic attacks. Anti-forensic approaches [25,29] focus on minimizing distortion and maintaining image quality, while others [26,27] identify anomalies introduced by anti-forensic techniques. The integration of GANs and CNNs represents a significant advance in the detection and generation of digital image forgeries. In addition, studies that optimize anti-forensic and forensic approaches [25,32] contribute to improving the accuracy and efficiency of existing methods.

- G. Cao et al. [32] propose a method for evaluating the performance of forensic systems that analyze the tampering of an image. M. Fontani et al. [33] propose a theoretical framework based on the Dempster–Shafer theory of evidence to merge the information provided by forensic tools and anti-forensic tools.

Both papers focus on improving the detection of manipulated images but from different perspectives. The article [32] proposes a model by which to evaluate the security of forensic techniques, considering both omission and false alarm errors. On the other hand, paper [33] focuses on countering anti-forensic techniques by fusing data from traditional forensic tools and CAF (computer-aided forensic) tools. Both studies agree that security and efficiency are crucial components of the forensic analysis of manipulated images.

The main differences between the articles lie in their objectives (performance evaluation vs. countering anti-forensic techniques), the methodologies employed (hypothesis testing model vs. data fusion based on Dempster–Shafer theory), and the aspects they emphasize (security against false alarms vs. relationships between forensic and CAF techniques).

Regarding novel contributions, paper [32] highlights the importance of security against false alarms in forensic evaluation, while paper [33] proposes a data fusion framework to counteract anti-forensic techniques.

- W. H. Chuang et al. [34] examine the anti-forensic techniques applied to color interpolation in digital images. Z. L. Laijie et al. [35] construct a review by applying it to image sharpening. Z. Shen et al. [36] performs the same review using CNN.

All three papers focus on anti-forensic techniques with which to hinder tampering detection in digital images. Article [34] evaluates the robustness of color interpolation identification against two anti-forensic techniques, while article [35] focuses on a specific anti-forensic scheme for USM sharpening. On the other hand, paper [36] questions the effectiveness of CNN-based sharpening detectors and proposes a GAN-based anti-forensic method.

Regarding the differences, the aim of article [34] is to evaluate robustness, that of article [35] is to invalidate existing forensic methods, and that of article [36] is to question the effectiveness of CNN detectors. Regarding manipulation, article [34] addresses color interpolation, article [35] focuses on USM sharpening, and article [36] addresses sharpening in general. In terms of methodology, paper [34] employs parameter perturbation and algorithm mixing, paper [35] uses artifact removal, and paper [36] is based on generative antagonistic networks (GANs).

Novel contributions include two anti-forensic techniques with which to hinder color interpolation identification in paper [34], an anti-forensic scheme to evade USM (unsharp

mask) sharpening detection in paper [35], and a GAN-based anti-forensic method that challenges the effectiveness of CNN-based sharpening detectors in paper [36].

- Authors such as K. Sitara et al. [37–39] present techniques for the detection and classification of video tampering, while M. C. Stamm et al. [40,41] focus on detecting the use of anti-forensics in video, and X. Kang et al. [42] describe techniques for detecting video tampering using video inter-frame spoofing techniques. On the other hand, S. Milani et al. [43,44] propose an anti-forensic technique with which to hide the camera used to record the video. C. Chen et al. [45] propose a similar technique and also use GAN.

Papers [40,42] focus on the race between forensic and anti-forensic techniques. Paper [40] proposes a theoretical model (VIF game) and techniques with which to detect the use of anti-forensics in video frame removal. Article [42] improves a frame removal detection algorithm and proposes an anti-anti-forensic method to deal with the manipulation of this fingerprint.

Articles [41,43–45] focus on source camera identification. Articles [41,42] analyze the fingerprints left by video compression (H.264/AVC) to detect tampering. Articles [44,45] address anti-forensics in source camera identification. Article [44] proposes to detect whether the camera model has been spoofed by analyzing local pixel ratios. Paper [45] employs GANs to forge the source camera model while maintaining image quality.

Novel contributions include the VIF game in paper [40] to model the interaction between forgers and forensic analysts, an anti-anti-forensic method for video frame removal in paper [42], an algorithm for detecting anti-anti-forensic forgery of the source camera model in paper [44], and a GAN-based anti-anti-forensic attack to forge the source camera model with high fidelity in paper [45].

- H. Yao et al. [46] discusses anti-forensic techniques applied to the deletion of frames in digital videos.

The main novel contribution of this paper is the introduction of a joint global and local feature to detect frame dropping in video footage via the anti-forensic technique of frame interpolation. This feature overcomes the limitations of previous methods by being robust to weak residuals in HEVC videos and enabling real-time detection.

- Ding et al. [47–51,53] propose anti-forensic tools and methods by which to bypass "DeepFake" detection on videos. On the other hand, Zhao, X et al. [52,54] apply it to "DeepFake" detection in GAN-generated images.

Studies [47–54] propose different strategies and models for generating DeepFakes that can evade forensic detection. Paper [47] propose GAN models with additional features and loss functions designed to improve visual quality and model efficiency. Article [48] employs local perturbations to expose the vulnerability of forensic detectors, while article [49] uses a bidirectional conversion between computer-generated and natural face images. Articles [50,51] focus on adversarial attacks for DeepFake detectors, reducing detection accuracy and highlighting the need to consider visual perception in the generation of these attacks. Article [53] investigates the use of anti-forensics for the creation of fake personal profiles and proposes defense strategies by which to improve the robustness of forensic systems. On the other hand, papers [52,54] presents a CG anti-forensic facial image regeneration scheme, achieving a balance between visual quality and deception capability. Taken together, these studies represent a significant advance in the field of DeepFakes anti-forensics, offering new strategies and models with which to improve visual quality and evade forensic detection.

- Liu [55–66] discuss techniques for tampering detection using median filtering (MF) on JPEG images.

W. Fan et al. [67,68] describe a method for improving the quality of median-filtered (MF) images while making such manipulation more difficult to detect forensically.

Paper [57] proposes a technique by which to detect blocking artifacts in JPEG images, while [58] introduces a forensic fingerprint based on residual median filtering. Paper [59] focuses on anti-forensic techniques to counter contrast enhancement detectors in digital images, and [60] presents an anti-forensic attack method for median filtering by adding uniformly distributed noise. Paper [61] proposes new variants of contrast enhancement operators that are undetectable by existing contrast enhancement detectors, while [62,66] analyzes the traces left by anti-forensic techniques for median filtering and proposes an anti-forensic method. Paper [63] proposes a robust residual median filtering residual difference domain (MFRD)-based detector; on the other hand, [64] proposes a two-stage median filtering anti-forensic framework to hide median filtering artifacts in JPEG images, while [65] presents an anti-forensic technique to counteract contrast enhancement detection in digital images. Paper [67] introduces a variational convolution framework for the quality enhancement and anti-forensics of median filtered images. On the other hand, [68] proposes an anti-forensic technique that hides traces left by median filtering while preserving the quality of the processed image.

As novel contributions, papers [57,58] propose methods by which to detect JPEG compression artifacts and JPEG blocking, respectively. Articles [59,60] present anti-forensic techniques for improving contrast enhancement detection and median filtering, while [61] introduces undetectable contrast enhancement operators. Article [62] analyzes and proposes an anti-forensic method for median filtering. In addition, Refs. [63,68] provide novel approaches to detect and counteract median filtering-based image manipulations, including robust detection methods, two-stage anti-forensic frameworks, and variational convolution techniques.

- A considerable number of authors, such as J. Waleed et al. [69–105], cover techniques for the detection of anti-forensics based on image compression. B. Li et al. [106] do the same using CNNs. Authors such as S. Milani et al. [107,108] apply it to double image compression. D. Huang et al. [109] focus their study on the double compression of JPG images and also base it on GAN.

Articles [69–74,77,108] propose anti-forensic methods by which to remove JPEG compression fingerprints and make it difficult to detect image manipulation, while articles [75,78,105,106] propose methods by which to identify images that have undergone anti-forensic processing. Articles [76,107] propose anti-forensic methods based on Benford's law, and articles [78,109] propose anti-forensic methods based on the generative adversarial network (GAN), which offer better performance and image quality than the previous methods.

Regarding novel contributions, several approaches have been proposed, including statistical modeling [69], artifact modification [71,108], parameter tuning [72], dithering [73], FSD distribution recovery [74], and DCT coefficient modification [77], as well as methods ranging from eliminating fingerprints with a high failed detection rate [69] to confusing fingerprints to hinder detection [77]. Convolutional neural networks (CNN) [75,106] and FSD distribution retrieval [105] have been proposed to identify images that have undergone anti-forensic processing. These are techniques that allow for the differentiation of manipulated images from those with single compression [105] and the detection of double-compression and related anti-forensics operations [75,106]. Others provide the modification of first-digit statistics to remove JPEG compression fingerprints based on Benford's law [76,107], while some authors propose the use of generative adversarial networks (GANs) to remove double JPEG compression fingerprints and improve image quality [78,109].

- J. Wu et al. [110–115] discuss anti-forensic techniques for both median filtering (MF) and image compression, some of them using generative adversarial networks (GAN).

A. Peng et al. [116] propose anti-forensic detection applied to the resampling of digital images to check if an image has undergone a resizing attempt.

P. He et al. [117] analyze anti-forensic techniques applied to images manipulated with GAN and present a mitigation model with CNN-based detection algorithms.

H. Xie et al. [118] develop a method by which to generate manipulated images that are indistinguishable from the originals using GAN.

Some anti-forensics methods are based on GANs, as noted in papers [110,114,118]. These methods achieve high image quality and evade forensic detection effectively. Other articles propose approaches based on statistical analysis [112,113] or domain modifications [115,116]. Article [111] presents a simple method by which to classify manipulated images with anti-forensics, while article [112] proposes a forensic method by which to detect previous JPEG compressions and an improved anti-forensic method for denoising. Article [113] presents an anti-forensic method based on the discrete fractional block-shifted fractional cosine transform (DFrCT) to remove compression artifacts. Article [115] describes an anti-forensic method that adds noise specifically designed to hide the processing history of an image. Article [116] proposes a method of detecting anti-forensic resampling using partial autocorrelation coefficients. In the field of prevention, paper [117] performs a systematic review of forensic and anti-forensic methods for GAN-generated images. Paper [118] proposes a dual-domain GAN-based anti-forensics (DDGAN) framework that incorporates operation-specific forensic features and machine-learned knowledge for better undetectability.

Regarding novel contributions, papers [110,114,118] propose GAN-based anti-forensics methods that achieve high image quality and evade forensic detection. Article [111] presents a simple method by which to classify manipulated images with anti-forensics. Article [112] proposes a forensic method by which to detect previous JPEG compressions and an improved anti-forensic method for denoising. Article [113] presents an anti-forensic method based on the discrete fractional block-shifted fractional cosine transform (DFrCT) to remove compression artifacts. Article [115] describes an anti-forensics method that adds noise specifically designed to hide the processing history of an image. Article [116] proposes a method pf detecting anti-forensic resampling using partial autocorrelation coefficients. Article [117] provides a systematic review of forensic and anti-forensic methods for GAN-generated images. Finally, paper [118] proposes a dual-domain GAN-based anti-forensics (DDGAN) framework that incorporates operation-specific forensic features and machine-learned knowledge for better undetectability.

- Authors such as J. Ravan et al. [119] deal with the detection of image forgery using the copy-and-paste technique. O. Mayer et al. [120,121] discuss the same, focusing on lateral chromatic aberrations (LCA). Other authors, such as L. Dou et al. [122], focus on the diffusion filling technique to analyze image forgeries.

Article [119] presents a method of detecting copy–paste forging using "Dyadic Wavelet SIFT" descriptors and DoG features. On the other hand, papers [120,121] focus on lateral chromatic aberration (LCA) as it can be manipulated to hide evidence of cut-and-paste tampering. Article [120] proposes a vector based on size differences between color channels to detect anti-forensic tampering, while [121] presents an anti-forensic method to fake LCA and disguise evidence of forging. Finally, paper [122] focuses on diffusion-based "inpainting" trace removal, a method of repairing or filling damaged areas in an image.

Regarding contributions, paper [119] proposes a novel method of detecting detect copy–paste forging using "Dyadic Wavelet SIFT" descriptors and DoG features. Article [120] presents an anti-forensic method by which to manipulate lateral chromatic aberration and a vector based on channel size differences for its detection. And paper [122] proposes a novel technique by which to remove diffusion-based inpainting traces by means of noise pattern analysis and statistical models.

- M. Salman et al. [123] elaborate an alternative forensic method that uses a different type of keypoint in images to avoid anti-forensic techniques based on SIFT (scale-invariant feature transform).

This paper proposes a forensic approach that counters SIFT keypoint removal by using a different type of keypoint in forensic analysis, demonstrating clear advantages over traditional SIFT keypoint-based techniques. The authors provide an innovative approach that uses a different type of keypoint in forensic analysis to overcome anti-forensic techniques that hide image manipulation.

- J. Wu et al. [124] expose a method of image tampering using a specific type of artificial neural network called a Wasserstein generative adversarial network with gradient penalty (WGAN-GP), which makes them appear to be original.

This paper proposes a novel method that uses Wasserstein-type generative adversarial networks enhanced with gradient penalty (WGAN-GP) to model image anti-forensics as an image-to-image translation problem. This multi-operation anti-forensics scheme manages to fool state-of-the-art forensic algorithms without significantly degrading image quality, and even improving it in most cases.

- Other authors, such as C. Chen et al. [125,126], propose a universal anti-forensic scheme via adaptive substitution of the quantization table present in the images.

Articles [125,126] focus specifically on the manipulation of the quantization table in JPEG images. They come as a novelty. Article [125] proposes a universal anti-forensic scheme that adaptively replaces the quantization table, while article [126] presents a general model that replaces the quantization table for both purposes: hiding forgeries and improving the detection of existing forgeries.

- H. Zhao et al. [127] analyze the contest between forensic techniques for detecting splices in audio recordings and anti-forensic techniques used to hide such splices. On the other hand, B. Tao et al. [128] do the same with the anti-forensic technique of double audio compression. Authors such as T. Liu et al. [129] focus their analysis on audio resampling and recompression using GAN.

M. Mascia et al. [130] describe a system for classifying whether an audio recording was made in an indoor or outdoor environment and anti-forensic techniques with which to deceive the classification system. Authors such as X. Li et al. [131] apply anti-forensic techniques using GAN to try to misidentify the source of the recording.

W.H. Chuang et al. [132] report anti-forensic attacks on the electrical network frequency (ENF) signal, which determines the creation date of digital audio and video recordings.

Papers [127,130] focus on the environmental signature of recordings, with paper [127] proposing an anti-forensic attack based on reverberation removal, and paper [130] presenting classifiers with which to distinguish indoor and outdoor recordings. On the other hand, papers [128,129] address compression history manipulation. Article [128] describes an anti-forensic method of removing traces of double MP3 compression, while article [129] focuses on the creation of fake stereo audio from mono audio, avoiding the detection of this manipulation. Papers [131,132] are notable for their use of generative adversarial neural networks (GANs); article [131] uses them to falsify the source of an audio, while article [132] analyzes their application in the anti-forensic application of the ENF signal, used to date recordings.

As a novelty, paper [127] introduces machine-learning-based countermeasures to detect anti-forensic attacks on the environmental signature. Articles [129,131] use novel techniques based on GANs for audio anti-forensic techniques. And paper [132] discusses the ENF signal anti-forensic technique, a novel approach for dating recordings.

S. K. Moon et al. [133] propose an algorithm based on reversible crypto-steganography, which hides sensitive information inside multimedia files such as images or videos. Also, S. K. Moon et al. [134,135] obtain a steganography algorithm applied to videos, while M. Sun et al. [136,137] develop a steganography algorithm for images. In contrast, P. P. Amritha et al. [138] describe a method by which to remove steganography in images and videos, without knowing the algorithm used for this purpose.

R. J. Chen et al. [139] develop an anti-forensic steganography system using the proposed multi-bit MER, which employs a flexible bit location embedding method (multi-bit MER-FBL embedding method), to overcome the problem of forensics and to achieve strong performance, including both large embedding capacity and high image quality.

Articles [133,134] propose techniques for video steganography that address security and authentication, while article [135] combines image and audio steganography in video, using forensic techniques for authentication. In the field of image steganography, papers [136,137] introduce anti-forensic methods for images based on HoEMD and AdEMD, and multi-bit MER with flexible location, respectively, increasing capacity and making detection more difficult. Paper [139] analyzes the properties of multi-bit minimum replacement error (MER) in image steganography. On the other hand, paper [138] proposes a generic anti-forensic method by which to remove hidden information in images without knowledge of the steganographic algorithm.

As novelties, articles [133,134] introduce techniques for video steganography that address security and authentication. Articles [136,137,139] contribute to the development of anti-forensic methods for image steganography. Article [138] proposes a generic anti-forensic method of removing information hidden in images.

4.1.2. Weaknesses and Anti-Forensic Use Cases: Specific Techniques

This section gathers the works whose purpose is to explain specific anti-forensic techniques, applied in very diverse fields, such as the Firefox browser in the study by D. Gupta et al. [140] or the secure and selective deletion of evidence in the article by A. Castiglione et al. [141].

H. Jahankhani et al. [142] aim to present some of the current anti-forensic approaches, along with some applicable solutions and some available tools.

N. Ding et al. [143] propose a new notion of secure disguisable symmetric encryption schemes, which captures the idea that the attacker can decrypt a cipher text he encrypted to different meaningful values when different keys are put to the decryption algorithm.

A. Srinivasan et al. [144] proposes "HIDEINsIDE", a new method for hiding data in unused disk space (slack space). This proposed method is an anti-forensic as well as a steganographic technique.

D. Forte et al. [145] examine the tactics of anti-forensic malicious software, which aims to eliminate or alter digital evidence to hinder investigations. This is the first article in a series exploring these software tactics.

S. Mansfield-Devine [146] explores, in general, the evolving landscape of anti-forensics techniques employed by criminals and malware, alongside countermeasures used for forensic analysis.

J. Sammons [147] presents an introduction to encryption technology and the threat it poses, as well as the attacks used to break encryption and the techniques used to hide and destroy data.

A. Srinivasan et al. [148] propose "FROST", an innovative asynchronous "Digital Dead Drop" that is resistant to detection and data loss, with adjustable fault tolerance. This system facilitates the secure and clandestine exchange of information asynchronously, guaranteeing the operational security and integrity of the exchanged data.

S. S. Lee et al. [149] present a simple encryption scheme using AES and XOR. A tool to implement this scheme is described, which allows for the encryption of files and the modification of timestamps.

M. Raggo et al. [150] develop guidelines for digital forensic investigators, equipping them with knowledge of anti-forensic techniques of data concealment, as well as the tools with which to counteract them and successfully recover hidden digital evidence.

E. Filiol [151] explores how encrypted data on a hard drive can influence forensic investigations. The paper discusses how an attacker can manipulate analysts and judges using malicious cryptographic techniques to wrongfully incriminate innocent people.

The articles discuss a range of techniques used to hinder digital forensic investigation and prevent evidence recovery [140,142,145]. Some methods focus on removing or manipulating traces of digital activity [140,142], while others propose techniques with which to hide information in slack space for anti-forensic and covert communication purposes [144,148]. Privacy protection through the secure erasure of information and encryption with anti-forensic techniques that make recovery by attackers difficult is also a central theme in [141,143]. The use of encryption to hinder forensic investigation is also addressed from different angles in [149,151]. Article [149] proposes double encryption, while [151] raises the use of encryption for malicious purposes to confuse investigators.

Regarding the contributions they offer, several articles propose novel methods of hiding information and hindering forensic investigation in general [144,148,149], while article [151] raises an interesting discussion on the malicious use of cryptography in the forensic context.

4.1.3. Weaknesses and Anti-Forensic Use Cases in Databases and the Cloud

The works whose main topic focuses on local or distributed DBs, as well as cloud functionalities, are collected in this section. Authors such as D. Vadlamudi et al. [152,153] expose anti-forensics techniques and detection in the cloud, and others, like S. Schmitt [154], discuss weaknesses in SQLite Corpora.

V. T. Patil et al. [155] propose a system that monitors anti-forensic attacks on SQL, identifying them using a pattern-matching algorithm and generating corresponding reports.

S. K. Mohiddin et al. [156] present a unique methodology by which to mitigate anti-forensics in a cloud with the effective usage of the relevant graphs.

D. R. Rani et al. [157] deploy a mechanism for identifying suspicious packets in a cloud environment. To categorize the type of attack that affected the packet, both signature analysis and anomaly detection at the cloud layers are applied.

The analyzed articles explore the challenges of cloud forensics due to anti-forensic techniques used to hide digital evidence [152,153,156]. Various technical solutions are proposed to detect and mitigate these attacks, including detection frameworks [153], monitoring systems [155], the use of graphs for mitigation [156], and the identification of suspicious packets [157]. Article [154] differentiates itself by focusing on the vulnerability of SQLite databases on mobile devices and the need for improved forensic tools to analyze them.

As novel contributions, article [154] presents a collection of manipulated SQLite databases to evaluate the effectiveness of forensic tools. In addition, papers [156,157] propose novel methods with which to mitigate and detect anti-forensic attacks in the cloud using graph and packet analysis, respectively.

4.1.4. Weaknesses and Anti-Forensic Use Cases of RAM

Other sections may be somewhat open-ended; this one, however, is very specific, as focuses only on the RAM of a computer system. Researchers such as R. Palutke et al. [4] explain how to hide data in RAM, and others, such as H. Jahankhani et al. [158], deal with anti-forensic techniques and tools applied to RAM.

The study by J. Stüttgen [159] examines anti-forensic techniques, tests commercial and free memory acquisition tools, and presents a novel technique based on direct page table manipulation and PCI hardware introspection, which does not depend on operating system facilities, being more difficult to subvert.

S. Eschweiler et al. [160] focus on the difficulty of acquiring volatile data (temporary information in memory) due to the limitations of current forensic tools and the rise of anti-forensic techniques. Their paper raises the need to develop new methods to counter these techniques.

Certain papers explore the challenges of digital memory forensics due to the anti-forensic techniques used by malware to hide evidence [4,158,159]. Various technical solutions are proposed to detect and mitigate these attacks, including new anti-forensic

methods [4], memory acquisition techniques resistant to these techniques [158,159], and discussion of the limitations of current forensic tools [160].

As novel contributions, paper [4] presents three novel anti-forensic methods for hiding information in RAM, while paper [158] proposes an innovative technique for acquiring memory in a way that is resistant to simple anti-forensic techniques.

4.1.5. Weaknesses and Anti-Forensic Use Cases in Flash Drives

In contrast to the previous section, this one is very general, as it gathers studies applied to Flash memories, which include USB flash drives, SSD hard disks, MMC and SD cards, etc.

Authors such as N. Y. Ahn et al. [161] deal with anti-forensic techniques applied to invalid spaces of NAND flash memories; others, such as J. Kwak et al. [162], expose anti-forensic wiping techniques for flash drives.

H. Jahankhani et al. [163] focus on anti-forensic techniques, specifically those that use RAM to hinder digital forensics using Live CD's and the variety of software packages that can be used for anti-forensic purposes.

P. Thomas et al. [164] evaluate the information that can identify the use of a USB flash drive on a Windows XP computer and seek to understand how this information could be used by a computer forensic investigator. An anti-forensic tool was created to perform a function to modify the information related to the use of USB flash drives.

Another article from N. Y. Ahn et al. [165] focuses on the challenge of forensic data recovery on NAND flash memory due to background management operations that make it difficult to completely remove information. They propose a secure reverse copying technique that minimizes the possibility of exposing residual data and altering adjacent cells to avoid reliability issues.

G. Bonetti et al. [166] develop a methodology for investigators and forensic analysts in making informed decisions about the recovery of digital evidence on SSDs, taking into account hardware optimizations and the possible anti-forensic techniques applied.

G. Hong Pyo et al. [167] examine how the anti-forensic tool "Fbinst" interferes with the digital forensics investigation of USB media and proposes methods by which to counteract its effects.

Further papers explore the vulnerabilities of flash drives, especially in recovering deleted data due to the nature of NAND memory [161,162,165,166]. Methods for secure data erasure on these drives are proposed [161,165], as well as schemes by which to minimize data erasure delay [162]. On the other hand, general anti-forensic techniques are described [163], including the use of live CDs for malicious purposes, and how to modify the Windows registry to hide the use of USB sticks is discussed [164]. A specific tool (Fbinst) used to create hidden partitions on flash drives and hinder digital forensics is also discussed [167].

As novel contributions, article [166] proposes a methodology by which to evaluate the "forensic friendliness" of an SSD disk, and article [167] discusses a specific anti-forensic tool (Fbinst) used to create hidden partitions on flash drives.

4.1.6. Weaknesses and Anti-Forensic Use Cases in Networking and IoT

Studies related to networks (LAN, WAN, GAN, VPN, etc.) and the broad section of the IOT (Internet of Things) are classified in this section.

R. Chandran et al. [168] attempt to detect and prevent network attacks. They indicate that the main modus operandi in network forensics is the successful implementation and analysis of attack graphs from the collected evidence. Therefore, in their paper, they convey the main concepts of attack graphs, the requirements for modeling, and the implementation of graphs.

R. Chandran et al. [169] also carry out an exhaustive study of anti-forensic techniques applied to networks to improve their security.

Other authors, such as Yaacoub et al. [170], provide a general review of forensic and anti-forensic techniques in the IoT domain, highlighting the importance of developing advanced forensic methods to deal with increasing cyber-attacks.

Further articles explore the challenges of network and Internet of Things (IoT) security in the face of increasing cyber-attacks and the use of anti-forensic techniques by attackers [168–170]. Article [168] proposes an innovative approach to analyzing anti-forensic techniques in networks using attack graphs, enabling the development of better defense strategies. Article [169] exposes, in depth, the general anti-forensic techniques related to networks. On the other hand, article [170] highlights the severity of cyber-attacks targeting IoT devices and the need for advanced forensic techniques to counter the anti-forensic techniques used by attackers.

As novel contributions, paper [168] proposes a novel approach to analyzing anti-forensic techniques in networks using attack graphs, and article [170] highlights the importance of developing advanced forensic techniques to combat IoT-specific threats.

4.1.7. Weaknesses and Anti-Forensic Use Cases in Operating Systems

Most of the articles studied focus on a specific aspect within the O.S.S. such as file systems, and not on the O.S. in particular; however, this section gathers the studies that deal directly with the operating system.

E. Jadied [171] presents two anti-forensic techniques related to the swap file on the Linux operating system.

Eterovic-Soric et al. [172] point out the paucity of research on techniques that hinder digital forensic analysis of electronic devices, focusing specifically on Windows 7 computers. They propose a method that removes or hides much of the digital evidence that forensic analysts typically use in their investigations.

Article [171] focuses on anti-forensics techniques for swap files, proposing two methods: fake data injection and creation of fake swap files. Article [172] discusses the lack of recent research on anti-forensics and proposes a general approach to hiding evidence on Windows 7 systems using Trojan software.

As novel contributions, article [171] proposes two specific anti-forensics techniques for swap files, an area that has been little studied; on the other hand, article [172] highlights the need for updated research on anti-forensic techniques for operating systems.

4.1.8. Weaknesses and Anti-Forensic Use Cases in Mobile Device Operating Systems

These studies include those applied to the case of S.S.O.O. of mobile devices of any kind, i.e., phones, tablets, smartwatches, televisions, etc. The O.S.S. treated by the authors refers to two in particular: Android and IOS.

Some articles focus on exposing techniques that make it difficult to gather forensic information on Android, such as that of S. Azadegan et al. [173,174].

L. Gómez-Miralles et al. [175] describe a tool designed to hinder the forensic analysis of iOS mobile devices (iPhone and iPad).

This category also includes works on O.S. applications for mobile devices, such as the work by M. Mirza et al. [176] on anti-forensic techniques dedicated to the WhatsApp messaging application.

A. Distefano et al. [177] relate anti-forensic techniques applied to mobile devices, presenting some automated instances of such techniques to Android devices, testing the effectiveness of such techniques against a cursory examination of the device and some acquisition tools.

J. Zheng et al. [178] present an anti-forensic approach for Android devices that protects AES keys from being acquired by forensic tools.

Further articles explore techniques such as data deletion and manipulation to evade existing forensic tools [173], operating system modifications to block data extraction [174,177], and the exploitation of vulnerabilities in applications such as WhatsApp [176]. The articles in question also highlight the need to develop more robust forensic tools and methods

to counter anti-forensic techniques, crucial for criminal investigation and the protection of digital evidence on mobile devices. Some articles propose solutions such as disabling vulnerable services on iOS [175] and protecting encryption keys on Android [178].

As novel contributions, several articles [173,174,177] demonstrate the need to improve forensic tools for mobile devices. Article [175] analyses the vulnerabilities of specific forensic services on iOS. Article [176] explores WhatsApp vulnerabilities for anti-forensic purposes. Finally, article [178] proposes a novel method of protecting encryption keys on Android.

4.1.9. Weaknesses and Anti-Forensic Use Cases in File Systems

The subject of file systems is an issue that is dealt with quite frequently in the studies analyzed. This section brings together those that deal specifically with file systems anti-forensics.

M.A. Wani et al. [17], in their study, collect techniques and anti-forensic tools against file systems. Other authors, such as P. Sanda et al. [179], exploit file system journaling to detect file deletion. File deletion detection is achieved by analyzing the ExT file system journal.

J. Cifuentes et al. [180] present a strategy by which to implement anti-forensics techniques on "ZFS" file systems (developed by Oracle), which brings benefits and functionality based on easy administration and robust design.

The works of T. Göbel et al. [181] and C. G. Sang [182] deal with specific types of file systems, i.e., ext4 in the first study and NTFS in the second study.

C. G. Sang et al. [183] also elaborate a new anti-forensic method for hiding data in the timestamp of a file in the Windows NTFS filesystem. The proposed method utilizes the 16 least-significant bits of the 64 bits in the timestamps.

X. Ding et al. [184] propose a forensic approach based on temporal cross-referencing for NTFS, analyzing both the discrepancies and the similarities between various pieces of temporal evidence associated with file metadata and the registry to address the problems caused by anti-forensic techniques based on the manipulation of temporal references.

D. Palmbach et al. [185] present a new use of four existing windows artifacts (the USNjrnl, link files, prefetch files, and Windows event logs), which can provide valuable information during investigations and can be used to prove timestamp forgery.

Authors such as T. Göbel et al. [186] evaluate various techniques for hiding data in the ext4 filesystem.

B. Singh et al. [187] describe the identification of timestamp patterns of various file operations on independent NTFS and ext4 file systems, as well as file interactions between file systems to detect timestamp manipulations.

M. A. Wani et al. [188] analyze the forensic value of the Linux B-tree file system (Btrfs) and its robustness against anti-forensic activities.

G. S. Cho [189] presents a tool that allows for the hiding of messages within the NTFS file system, taking advantage of the free space in the directory indexes.

Further articles explore anti-forensic techniques used to hide evidence in file systems [17,179,180]. Some anti-forensic techniques include the secure deletion of files, the manipulation of timestamps, and the hiding data in different parts of the file system [179,181–183,186,189]. Forensic researchers are also developing methods by which to detect and counteract anti-forensic techniques, such as the analysis of inconsistencies in timestamps and the use of multiple digital artefacts [184,185,187].

As novel contributions, a method for detecting secure file deletion on ext4 systems is proposed [179]. The anti-forensic capabilities of the Btrfs file system are analyzed [188]. A tool for hiding messages in NTFS system directories is developed [189]. And several articles propose new techniques for hiding data using timestamps [181,183,186].

4.1.10. Weaknesses and Anti-Forensic Use Cases in Forensic Tools

This section could be considered mixed as it brings together studies with different purposes: some deal with anti-forensic techniques on specific forensic tools; and others explain techniques that nullify the legal validity of evidence collected with forensic tools.

The common point among all the articles in this group is that they all deal with forensic tools, but their purposes are very different.

C. S. Meffert et al. [190] use "TD3", a popular disk duplicator and hardware write blocker with network capabilities, and design an attack that corrupts the integrity of the target drive (a drive with the duplicated evidence) without the user's knowledge to reveal the vulnerability of digital forensic tools to anti-forensic attacks.

Paper [191] discusses how the Metasploit Anti-Forensic Investigation Arsenal (MAFIA), which is a toolkit designed to obstruct digital forensic investigations, is being used to attack popular forensic tools. This is similar to the study by M. Wundram et al. [192], which exposes anti-forensic attacks on these tools in general and presents possible countermeasures.

G. Horsman et al. [193] analyze and defend the need to investigate "digital tool marks" (DTMs), i.e., indicators of anti-forensics use, in a digital forensics investigation and highlight the advantages of doing so.

Authors such as W. A. Bhat et al. [194] analyze the effectiveness of digital forensic tools in extracting complete and credible evidence in scenarios with anti-forensic file system attacks.

The articles assessed expose the vulnerability of digital forensic tools used to collect evidence in investigations. Forensic investigators face a major problem in the form of anti-forensic techniques that aim to hide or destroy digital evidence [190–192,194]. Some articles analyze specific attacks on popular forensic tools (example, using Metasploit) [191,192]. Others perform a more general analysis of the effectiveness of forensic tools against anti-forensic techniques on the file system [194]. To address this challenge, the articles propose improved security testing methods for forensic tools [190,192,194]. The possibility of targeted attacks against forensic tools in the cloud is also raised [190]. Furthermore, the concept of "digital tool marks" (DTMs) is proposed as a new source of forensic evidence [193].

As novel contributions, article [190] raises the possibility of targeted attacks against cloud forensic tools. Article [192] presents the first code injection attack against a commercial forensic analysis tool. Article [193] proposes the concept of "digital tool marks" (DTMs) as a new source of forensic evidence. Finally, article [194] demonstrates the inability of some forensic tools to detect common anti-forensic attacks.

4.2. Exposition of Anti-Forensic Techniques

This section, represented in Figures 12 and 13, groups the documents whose main objective is to classify and expose techniques employed for anti-forensic purposes.

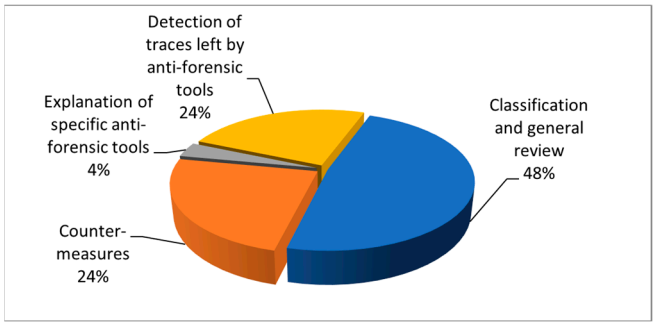

Figure 12. Exposition of anti-forensic techniques in percentage.

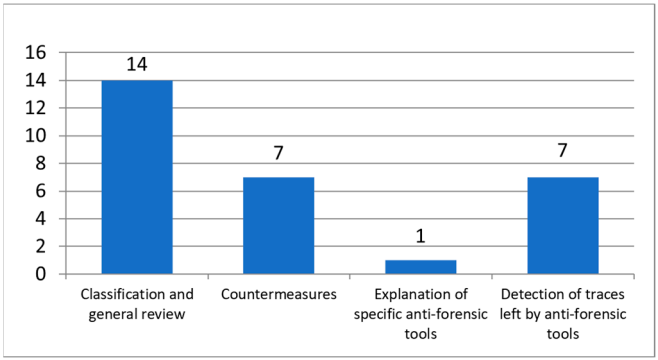

Figure 13. Exposition of anti-forensic techniques in number of articles.

Table 5 lists the works classified according to the categories established and described in Section 4.2.

Table 5. Studies classified by category in Section 4.2 (exposition of anti-forensic techniques).

Exposition of Anti-Forensic Techniques	Number of Studies	References
Classification and general review	14	[1,8,10,11,15,82,195–202]
Countermeasures	7	[16,203–208]
Explanation of specific anti-forensic tools	1	[209]
Detection of traces left by anti-forensic tools	7	[2,14,210–214]

4.2.1. Exposition of Anti-Forensic Techniques: Classification and General Review

Together with Sections 4.1.2 and 4.1.9, this is one of the sections with the largest number of articles. It includes studies that aim to classify anti-forensic techniques, such as those of N.A. Hassan et al. [10], and K. Conlan et al. [8], as well as articles which, without attempting to classify them, give an overview of anti-forensic techniques, such as that of S. Garfinkel [195–199].

H. Berghel [200] exposes and classifies different methods of hiding data, as well as the anti-forensic tools used to execute such methods.

B. Shavers et al. [201] discuss the anti-forensic techniques used by suspects to hinder the digital forensic analysis of storage devices and the need for training to recognize and counteract such anti-forensic techniques.

J. C. Sremack et al. [202] attempt to construct a comprehensive taxonomy of anti-forensic threats according to research and threat type.

Digital forensics is facing a growing challenge: anti-forensic techniques. These techniques, used to hide, destroy, or alter digital evidence, hinder the collection of evidence in legal investigations [195–199,201,202]. Forensic investigators develop new anti-forensic tactics and new tools to detect and counter them [8,195,201,202]. Collaboration between forensic investigators and computer security experts is crucial to address this threat [10]. Other articles propose taxonomies of anti-forensic threats or introduce concepts such as time-sensitive anti-forensics [198,202].

As a novel contribution, one article differentiates between traditional anti-forensics (protecting privacy) and malicious anti-forensics (hiding criminal evidence) [198]. Several articles highlight the need to develop better methods of detecting and counteracting anti-forensic techniques [8,195,201,202]. Finally, article [200] discusses open-source anti-forensic tools.

4.2.2. Exposition of Anti-Forensic Techniques: Countermeasures

Some authors have focused on explaining countermeasures to mitigate the effects of anti-forensics in a more general scope, such as. A. R. Mothukur et al. [16,203–205]. Others, however, detail, in depth, the techniques used to mitigate specific attacks.

G. Cho et al. [206] focus on avoiding information being hidden in an NTFS file system and elaborate guidelines to prevent it.

B. Z. Adamu et al. [207] explore anti-forensic agents in databases, present a taxonomy of the impact they cause, and focus their study on providing a list of mitigation recommendations.

H. Lee et al. [208] use reverse engineering on the "Steg" software (steganography software using the IDA tool) to propose countermeasures to detect and defeat this type of software.

Further articles explore different aspects of the anti-forensic field, including the definition and classification of anti-forensic techniques [204], their impact on the investigation of cybercrime [16], their application in blogs to maintain anonymity [205], methods by which to hide data in NTFS partitions [206], the analysis of anti-forensic techniques in databases [207], and the reverse engineering of steganography tools [208], all of them focusing on the proposal of countermeasures to solve these problems.

Among the contributions of these studies are the definition and classification of anti-forensic techniques [204], the proposal of countermeasures for law enforcement [16], the analysis of anti-forensic techniques in blogs to maintain anonymity [205], methods by which to hide data in NTFS partitions [206], the analysis of techniques with which to prevent anti-forensic techniques in databases [207], and countermeasures for "Steg" software (steganography software using the IDA tool) [208].

4.2.3. Exposition of Anti-Forensic Techniques: Explanation of Specific Anti-Forensic Tools

Many of the studies reviewed use anti-forensic tools, but this is not their purpose; rather, they are part of the research aimed at demonstration their conclusions. This section includes an article by S. Hilley [209], whose purpose is to present a set of anti-forensic tools.

The article warned about the increasing sophistication of anti-forensic techniques and the emergence of specialized tools such as MAFIA (Metasploit Anti-Forensic Investigation Arsenal). These tools resemble hacking arsenals that historically targeted conventional software; but in this case, their aim is to hinder digital forensic investigations.

The article's objective is to expose the problematic nature of these tools.

4.2.4. Exposition of Anti-Forensic Techniques: Detection of Traces Left by Anti-Forensic Tools

This section discusses articles that evidence traces of having used anti-forensic techniques and tools.

M. I. Al-Saleh et al. [14] expose artefacts related to intentional user account deletion techniques.

C. Lees [210] discusses forensic artifact removal by analyzing the update sequence number journal present when NTFS logs are active.

S. Lim et al. [211] expose the traces left by encryption tools. While M.Ç. Fanuscu et al. [212] focus on the detection of anti-forensic incidents using security incident and information management systems (SIEM).

A. S. M. Irwin [213] explores common security techniques and methods, such as system logging, vulnerability scanning, and network monitoring. The paper then analyzes the traces left behind and suggests security approaches to reducing the effectiveness of these anti-forensic practices.

T. Mehrotra et al. [214] analyze whether "Wickr" (a free app that allows users to send files and messages that self-destruct) delivers on its promise of leaving no digital traces, which would be a challenge for forensic investigation on Android devices.

Among the contributions of these studies are the detection of traces in deleted user accounts [14], the identification of patterns in the USN registry to detect trace cleaning software [210], the analysis of the behavior of virtual disk encryption tools [211], the detection of anti-forensic activities by SIEM systems [212], the analysis of how common

security tools can be used for anti-forensic purposes [213], and the evaluation of the Wickr application [214].

4.3. Anti-Forensics and Malware

This section groups the papers that relate the use of anti-forensic techniques to malware. Table 6 lists the papers related to this topic.

Table 6. Studies classified by category in Section 4.3 (anti-forensics and malware).

Anti-Forensics and Malware	Number of Studies	References
Anti-forensics and Malware	7	[19,215–220]

Authors such us I. You et al. [215] discuss the anti-forensic aspect of obfuscation as applied to malware.

Sudhakar et al. [19] expose a type of malware (fileless malware) that makes very advanced use of anti-forensic techniques to avoid detection. M. Brand [216] explains forensic avoidance techniques (anti-forensics) used by malware.

Ratcliffe et al. [217] bring together anti-forensic techniques and malware on the same level when explaining how to detect malware in RAM.

M. Agarwal et al. [218] propose a method of detecting the anti-forensic technique of tampering with network sensors of host-based intrusion detection systems (HIDS).

Li, J. et al. [219] propose systematic procedures for the analysis of anti-forensic techniques typical of malware in the Android mobile operating system.

Also, M. Brand et al. [220] propose the detection of malware by searching for indicators of anti-forensic techniques in the analyzed system.

Among the contributions of these studies are the analysis of anti-forensic techniques directly related to malware [216], the development of process models to handle fileless malware attacks [19], the detection of malware in memory using machine learning [217], the detection of stealthy malware by comparing network sensors [218], and the analysis of malware behavior on Android mobile devices [219].

4.4. New Threat Models and Forecasts

This chapter groups papers whose main theme is to expose threat modeling methodologies to mitigate anti-forensic techniques. The papers deal with forecasts on the evolution of these techniques as well as suggestions for future research in this field. Table 7 lists the papers related to this section.

Table 7. Studies classified by category in Section 4.4 (new threat models and forecasts).

New Threat Models and Forecasts	Number of Studies	References
New threat models and forecasts	8	[11,12,221–226]

B. Hoelz et al. [11] propose a threat model to manage the risks associated with anti-forensic threats. J. Nikolai et al. [221] present a framework within which to examine the risks associated with the human facet.

Articles such as those by R. Harris [12], K. Dahbur et al. [222], and B. Schlicher et al. [223] made forecasts and warned about the anti-forensic threat in the early days of the anti-forensic threat.

M. Ölvecký et al. [224] aim to define future research focused on establishing a suitable digital environment for the anti-forensic technique of secure file wiping.

K. Dahbur et al. [225] highlight the challenges posed by anti-forensics by exploring various mechanisms, tools, and techniques.

Finally, the article by D. Forte [226] addresses the concern that digital forensic software could be manipulated by attackers using anti-forensic techniques, which would call into question the validity of the evidence obtained.

The use of threat models [11] to manage anti-forensic risks, the understanding of the motivations behind the use of anti-forensic tools [221], the development of effective countermeasures [12,222,225], and the establishment of standards for secure data erasure [224] are essential elements in ensuring the integrity of digital evidence in forensic investigations.

As a novel contribution, a conceptual framework is proposed with which to understand the motivation behind the use of anti-forensic tools [221], an approach to evaluating secure erasure standards by creating a test environment is suggested [224], and an analysis of the feasibility of theoretical attacks against forensic software is presented [226].

5. Conclusions

The review, grouping, and presentation of all these articles has the purpose, among other things, of exposing the existing literature, making it easier to consult works with similar objectives and scope.

The trends of the last 6 years (2016–2022) have been oriented both towards better classifying the new anti-forensic techniques that are emerging and dealing, in greater depth, with some of the most transcendental ones.

The contribution of the articles by B. Hoelz et al. [11] and A.R. Mothukur et al. [16] are recent developments that had not been addressed or had hardly been outlined previously.

Anti-forensic techniques can be understood as a threat/risk to forensic techniques. If we consider that the anti-forensics field started to be treated as such with the article by C. S. J. Peron et al. [1], wherein the concept was defined, 12 years would have passed (2005-2017) until the publication of the first article that proposes threat/risk models.

This fact shows how little research effort has been devoted to a field that is increasingly known to criminals, which makes forensic analysis more and more difficult and its legal validity in court more difficult to obtain.

The relative closeness in time of the proposals of A.R. Mothukur et al. [16] to mitigate anti-forensic techniques means that their application is still valid today and is thus useful for recent analyses.

Some of the improvements they propose are already in practice, such as having a standardized training process. Some universities offer accredited master's degrees in computer forensics, providing a common knowledge base for forensic science professionals. Most of the articles collected (53.63%) deal with anti-forensic techniques applied to multimedia, which makes it clear that analyzing image, video, and audio manipulations is a priority in this field compared to, for example, classifying anti-forensic techniques (6.75%), or the rest of the categories in Section 4.1 combined (26.36%).

The works gathered in Section 4.3 by I. You et al. [210], Sudhakar et al. [19], M. Brand [211], etc., are small examples of authors who directly relate anti-forensic techniques and malware. To state that malware and anti-forensic techniques are intrinsically related is not far-fetched; M.A. Wani et al. [17], among others, mentioned the use of reserved locations, steganography, cryptography, and trace obfuscation, i.e., techniques that are also used by malware to achieve its goals.

It can be concluded that having good knowledge in the field of anti-forensic techniques is a good prerequisite to going deeper into the field of malware.

Considering the number and subject matter of articles published in the last 6 years on this theme, it can be concluded that research into anti-forensic techniques is far behind the annual developments in forensic analysis. Therefore, those who seek to hinder or disrupt a forensic analysis have an advantage over those whose mission is to prevent this from happening.

Given all that has been exposed in this study, to strengthen forensic analysis, the first important step is to consolidate the knowledge of the techniques that weaken it, and

for this, nothing is more significant than the development of a general methodology for mitigating anti-forensic techniques.

In this way, the knowledge base would be established to efficiently deal with the anti-forensic techniques classified by the authors N. A. Hassan et al. [10], K. Conlan et al. [8], and M. Gül et al. [15].

On this premise, each section could be explored in more depth as, for example, M. I. Al-Saleh et al. [14], M. A. Wani et al. [17], and D.I. Jang et al. [18] did in their articles.

The creation of the previously mentioned methodology would be the factor that would solidify the path to follow to obtain an even more reliable and productive forensic analysis, in addition to the benefits it would also bring to the study of those who seek to prevent the threat presented by malware.

The omission of gray literature is one of the limitations of the study. By limiting the search to studies that contain the term "anti-forensics" in its title, abstract, or keywords, some of the articles dealing with issues related to MITRE's ATT&CK matrix, system security breach techniques, and other techniques, such as those discussed in malware articles, have not been included in this study.

Developing a method for finding this gray literature and cataloging it is proposed as a future study to extend this work.

Author Contributions: Conceptualization, J.B.H. and R.G.A.; Methodology, J.R.B.H. and J.A.S.M.; Validation, J.R.B.H., J.A.S.M. and J.J.R.G.; Formal analysis, J.R.B.H., J.A.S.M. and J.J.R.G.; Investigation, R.G.A., J.B.H. and J.J.R.G.; Writing—original draft, R.G.A. and J.B.H.; Writing—review and editing, J.A.S.M., J.J.R.G. and J.R.B.H. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Peron, C.S.J.; Legary, M. Digital anti-forensics: Emerging trends in data transformation techniques. In Proceedings of the E-Crime and Computer Evidence Conference, Montecarlo, Monaco, 28–30 March 2005.
2. Pajek, P.; Pimenidis, E. Computer anti-forensics methods and their impact on computer forensic investigation. *Commun. Comput. Inf. Sci.* **2009**, *45*, 145–155. [CrossRef] [PubMed]
3. Latzo, T.; Palutke, R. Freiling. A universal taxonomy and survey of forensic memory acquisition techniques. *Digit. Investig.* **2019**, *28*, 56–69. [CrossRef]
4. Palutke, R.; Block, F.; Reichenberger, P.; Stripeika, D. Hiding Process Memory Via Anti-Forensic Techniques. *Forensic Sci. Int. Digit. Investig.* **2020**, *33*, 301012. [CrossRef]
5. Kitchenham, B.; Charters, S. *Guidelines for Performing Systematic Literature Reviews in Software Engineering Version 2.3*; Technical Report; Keele University: Keele, UK; University of Durham: Durham, UK, 2007.
6. Kitchenham, B.; Brereton, O.P.; Budgen, D.; Turner, M.; Bailey, J.; Linkman, S. Systematic literature reviews in software engineering—A systematic literature review. *Inf. Softw. Technol.* **2009**, *51*, 7–15. [CrossRef]
7. Kitchenham, B.; Brereton, P. A Systematic Review of Systematic Review Process Research in Software Engineering. *Manuscr. Publ. Inf. Softw. Technol.* **2013**, *55*, 2049–2075. [CrossRef]
8. Conlan, K.; Baggili, I.; Breitinger, F. Anti-forensics: Furthering digital forensic science through a new extended, granular taxonomy. *Digit. Investig.* **2016**, *18*, S66–S75. [CrossRef]
9. Rogers, M. Anti-Forensics: The Coming Wave in Digital Forensics. 2006. Available online: https://www.cerias.purdue.edu/news_and_events/events/symposium/2006/materials/pdfs/antiforensics.pdf (accessed on 10 June 2024).
10. Hassan, N.A.; Hijazi, R. Antiforensic Techniques. In *Data Hiding Techniques in Windows OS*; Syngress: Rockland, MA, USA, 2017; pp. 267–290. [CrossRef]
11. Hoelz, B.; Maues, M. Anti-forensic threat modelling. *IFIP Adv. Inf. Commun. Technol.* **2017**, *511*, 169–183. [CrossRef]
12. Harris, R. Arriving at an anti-forensics consensus: Examining how to define and control the anti-forensics problem. *Digit. Investig.* **2006**, *3*, 44–49. [CrossRef]
13. Beebe, N.L.; Clark, J.G. A hierarchical, objectives-based framework for the digital investigations process. *Digit. Investig.* **2005**, *2*, 147–167. [CrossRef]
14. Al-Saleh, M.I.; Al-Shamaileh, M.J. Forensic artefacts associated with intentionally deleted user accounts. *Int. J. Electron. Secur. Digit. Forensics* **2017**, *9*, 167–179. [CrossRef]

15. Gül, M.; Kugu, E. A survey on anti-forensics techniques. In Proceedings of the 2017 International Artificial Intelligence and Data Processing Symposium (IDAP), Malatya, Turkey, 16–17 September 2017. [CrossRef]
16. Mothukur, A.R.; Balla, A.; Taylor, D.H.; Sirimalla, S.T.; Elleithy, K. Investigation of Countermeasures to Anti-Forensic Methods. In Proceedings of the 2019 IEEE Long Island Systems, Applications and Technology Conference (LISAT), Farmingdale, NY, USA, 3 May 2019. [CrossRef]
17. Wani, M.A.; AlZahrani, A.; Bhat, W.A. File system anti-forensics–types, techniques and tools. *Comput. Fraud. Secur.* **2020**, *2020*, 14–19. [CrossRef]
18. Jang, D.-I.; Ahn, G.-J.; Hwang, H.; Kim, K. Understanding anti-forensic techniques with timestamp manipulation. In Proceedings of the 2016 IEEE 17th International Conference on Information Reuse and Integration, IRI, Pittsburgh, PA, USA, 28–30 July 2016; pp. 609–614. [CrossRef]
19. Sudhakar; Kumar, S. An emerging threat Fileless malware: A survey and research challenges. *Cybersecurity* **2020**, *3*, 1–12. [CrossRef]
20. Li, H.; Luo, W.; Qiu, X.; Huang, J. Identification of Various Image Operations Using Residual-Based Features. *IEEE Trans. Circuits Syst. Video Technol.* **2018**, *28*, 31–45. [CrossRef]
21. Qureshi, M.A.; El-Alfy, E.-S.M. Bibliography of digital image anti-forensics and anti-anti-forensics techniques. *IET Image Process.* **2019**, *13*, 1811–1823. [CrossRef]
22. Yu, J.; Zhan, Y.; Yang, J.; Kang, X. A multi-purpose image counter-anti-forensic method using convolutional neural networks. *Lect. Notes Comput. Sci.* **2017**, *10082*, 3–15. [CrossRef]
23. Stamm, M.C.; Zhao, X. Anti-Forensic Attacks Using Generative Adversarial Networks. Multimedia Forensics. In *Advances in Computer Vision and Pattern Recognition*; Springer: Singapore, 2022.
24. Cao, G.; Zhao, Y.; Ni, R.; Tian, H.; Yu, L. Attacking contrast enhancement forensics in digital images. *Sci. China Inf. Sci.* **2014**, *57*, 1–13. [CrossRef]
25. Ravi, H.; Subramanyam, A.V.; Emmanuel, S. ACE-An effective anti-forensic contrast enhancement technique. *IEEE Signal Process. Lett.* **2016**, *23*, 212–216. [CrossRef]
26. Bharathiraja, S.; Kanna, B.R. Anti-Forensics Contrast Enhancement Detection (AFCED) Technique in Images Based on Laplace Derivative Histogram. *Mob. Netw. Appl.* **2019**, *24*, 1174–1180. [CrossRef]
27. Kwok, C.-W.; Au, O.C.; Chui, S.-H. Alternative anti-forensics method for contrast enhancement. *Lect. Notes Comput. Sci.* **2012**, *7128*, 398–410. [CrossRef]
28. Lin, X.; Li, C.-T.; Hu, Y. Exposing image forgery through the detection of contrast enhancement. In Proceedings of the 2013 IEEE International Conference on Image Processing, ICIP 2013, Melbourne, VIC, Australia, 15–18 September 2013; pp. 4467–4471. [CrossRef]
29. Zou, H.; Yang, P.; Ni, R.; Zhao, Y. Anti-forensics of image contrast enhancement based on generative adversarial network. *Secur. Commun. Networks* **2021**, *2021*, 1–8. [CrossRef]
30. Sun, J.Y.; Kim, S.W.; Lee, S.W.; Ko, S.J. A novel contrast enhancement forensics based on convolutional neural networks. *Signal Process. Image Commun.* **2018**, *63*, 149–160. [CrossRef]
31. Dong, W.; Wang, J.-J. Contrast Enhancement Forensics Based on Modified Convolutional Neural Network. *Yingyong Kexue Xuebao/J. Appl. Sci.* **2017**, *35*, 745–753.
32. Cao, G.; Wang, Y.; Zhao, Y.; Ni, R.; Lin, C. On the security of image manipulation forensics. *Lect. Notes Comput. Sci.* **2015**, *9314*, 97–105. [CrossRef] [PubMed]
33. Fontani, M.; Bonchi, A.; Piva, A.; Barni, M. Countering anti-forensics using data fusion. In Proceedings of the SPIE—The International Society for Optical Engineering, San Francisco, CA, USA, 2–6 February 2014; Volume 9028. [CrossRef]
34. Chuang, W.-H.; Wu, M. Robustness of color interpolation identification against anti-forensic operations. *Lect. Notes Comput. Sci.* **2013**, *7692*, 16–30. [CrossRef] [PubMed]
35. Lu, L.; Yang, G.; Xia, M. Anti-forensics for unsharp masking sharpening in digital images. *Int. J. Digit. Crime Forensics* **2013**, *5*, 53–65. [CrossRef]
36. Shen, Z.; Ding, F.; Shi, Y. Anti-forensics of Image Sharpening Using Generative Adversarial Network. *Lect. Notes Comput. Sci.* **2020**, *12022*, 150–157. [CrossRef] [PubMed]
37. Sitara, K.; Mehtre, B.M. Digital video tampering detection: An overview of passive techniques. *Digit. Investig.* **2016**, *18*, 8–22. [CrossRef]
38. Shelke, N.A.; Kasana, S.S. A comprehensive survey on passive techniques for digital video forgery detection. *Multimed. Tools Appl.* **2021**, *80*, 6247–6310. [CrossRef]
39. Bestagini, P.; Battaglia, S.; Milani, S.; Tagliasacchi, M.; Tubaro, S. Detection of temporal interpolation in video sequences. In Proceedings of the 2013 IEEE International Conference on Acoustics, Speech and Signal Processing, Vancouver, BC, Canada, 26–31 May 2013; pp. 3033–3037. [CrossRef]
40. Stamm, M.C.; Lin, W.S.; Liu, K.J.R. Forensics vs. anti-forensics: A decision and game theoretic framework. In Proceedings of the ICASSP, IEEE International Conference on Acoustics, Speech and Signal Processing, Kyoto, Japan, 25–30 March 2012; pp. 1749–1752. [CrossRef]
41. Su, P.-C.; Suei, P.-L.; Chang, M.-K.; Lain, J. Forensic and anti-forensic techniques for video shot editing in H.264/AVC. *J. Vis. Commun. Image Represent.* **2015**, *29*, 103–113. [CrossRef]

42. Kang, X.; Liu, J.; Liu, H.; Wang, Z.J. Forensics and counter anti-forensics of video inter-frame forgery. *Multimed. Tools Appl.* **2016**, *75*, 13833–13853. [CrossRef]
43. Milani, S.; Bestagini, P.; Tagliasacchi, M.; Tubaro, S. Antiforensic synthesis of motion vectors using template algorithms. In Proceedings of the ICASSP, IEEE International Conference on Acoustics, Speech and Signal Processing, Florence, Italy, 4–9 May 2014; pp. 2709–2713. [CrossRef]
44. Chen, C.; Zhao, X.; Stamm, M.C. Detecting anti-forensic attacks on demosaicing-based camera model identification. In Proceedings of the International Conference on Image Processing, ICIP, Beijing, China, 17–20 September 2017; pp. 1512–1516. [CrossRef]
45. Chen, C.; Zhao, X.; Stamm, M.C. Mislgan: An Anti-Forensic Camera Model Falsification Framework Using a Generative Adversarial Network. In Proceedings of the International Conference on Image Processing, ICIP, Athens, Greece, 7–10 October 2018; pp. 535–539. [CrossRef]
46. Yao, H.; Ni, R.; Zhao, Y. An approach to detect video frame deletion under anti-forensics. *J. Real-Time Image Process.* **2019**, *16*, 751–764. [CrossRef]
47. Ding, F.; Zhu, G.; Li, Y.; Zhang, X.; Atrey, P.K.; Lyu, S. Anti-Forensics for Face Swapping Videos via Adversarial Training. *IEEE Trans. Multimed.* **2022**, *24*, 3429–3441. [CrossRef]
48. Zhang, H.; Chen, B.; Wang, J.; Zhao, G. A Local Perturbation Generation Method for GAN-generated Face Anti-forensics. *IEEE Trans. Circuits Syst. Video Technol.* **2022**, *33*, 661–676. [CrossRef]
49. Peng, F.; Yin, L.; Long, M. BDC-GAN: Bidirectional Conversion Between Computer-Generated and Natural Facial Images for Anti-Forensics. *IEEE Trans. Circuits Syst. Video Technol.* **2022**, *32*, 6657–6670. [CrossRef]
50. Fan, L.; Li, W.; Cui, X. Deepfake-image anti-forensics with adversarial examples attacks. *Future Internet* **2021**, *13*, 288. [CrossRef]
51. Wang, Y.; Ding, X.; Yang, Y.; Ding, L.; Ward, R.; Wang, Z.J. Perception matters: Exploring imperceptible and transferable anti-forensics for GAN-generated fake face imagery detection. *Pattern Recognit. Lett.* **2021**, *146*, 15–22. [CrossRef]
52. Zhao, X.; Stamm, M.C. Making Generated Images Hard to Spot: A Transferable Attack on Synthetic Image Detectors. In *Pattern Recognition, Computer Vision, and Image Processing*; Lecture Notes in Computer Science; Springer: Cham, Switzerland, 2022; Volume 13646. [CrossRef]
53. Ngoc, N.H.; Chan, A.; Binh, H.T.T.; Ong, Y.S. Anti-Forensic Deepfake Personas and How To Spot Them. In Proceedings of the International Joint Conference on Neural Networks, Padua, Italy, 18–23 July 2022. [CrossRef]
54. Peng, F.; Yin, L.-P.; Zhang, L.-B.; Long, M. CGR-GAN: CG Facial Image Regeneration for Antiforensics Based on Generative Adversarial Network. *IEEE Trans. Multimed.* **2020**, *22*, 2511–2525. [CrossRef]
55. Liu, Q. An approach to detecting JPEG down-recompression and seam carving forgery under recompression anti-forensics. *Pattern Recognit.* **2017**, *65*, 35–46. [CrossRef]
56. Luo, Y.; Zi, H.; Zhang, Q.; Kang, X. Anti-forensics of JPEG compression using generative adversarial networks. In Proceedings of the European Signal Processing Conference, Rome, Italy, 3–7 September 2018; pp. 952–956. [CrossRef]
57. Bhardwaj, D.; Pankajakshan, V. A JPEG blocking artefact detector for image forensics. *Signal Process. Image Commun.* **2018**, *68*, 155–161. [CrossRef]
58. Peng, A.; Kang, X. Robust median filtering detection based on filtered residual. *Lect. Notes Comput. Sci.* **2013**, *7809*, 344–357. [CrossRef]
59. Sharma, S.; Ravi, H.; Subramanyam, A.V.; Emmanuel, S. Anti-forensics of median filtering and contrast enhancement. *J. Vis. Commun. Image Represent.* **2020**, *66*, 102682. [CrossRef]
60. Kang, X.; Qin, T.; Zeng, H. Countering median filtering anti-forensics and performance evaluation of forensics against intentional attacks. In Proceedings of the 2015 IEEE China Summit and International Conference on Signal and Information Processing, ChinaSIP 2015, Chengdu, China, 12–15 July 2015; pp. 483–487. [CrossRef]
61. Cao, G.; Zhao, Y.; Ni, R.; Tian, H. Anti-forensics of contrast enhancement in digital images. In Proceedings of the MM and Sec'10, 2010 ACM SIGMM Multimedia and Security Workshop, Rome, Italy, 9–10 September 2010; pp. 25–34. [CrossRef]
62. Wu, Z.-H.; Stamm, M.C.; Liu, K.J.R. Anti-forensics of median filtering. In Proceedings of the ICASSP, IEEE International Conference on Acoustics, Speech and Signal Processing, Vancouver, BC, Canada, 26–31 May 2013; pp. 3043–3047. [CrossRef]
63. Peng, A.-J.; Kang, X.-G. Median filtering forensics based on multi-directional difference of filtering residuals. *JisuanjiXuebao/Chin. J. Comput.* **2016**, *39*, 503–515.
64. Singh, K.; Kansal, A.; Singh, G. An improved median filtering anti-forensics with better image quality and forensic undetectability. *Multidimens. Syst. Signal Process.* **2019**, *30*, 1951–1974. [CrossRef]
65. Sharma, S.; Subramanyam, A.V.; Jain, M.; Mehrish, A.; Emmanuel, S. Anti-forensic technique for median filtering using L1-L2 TV model. In Proceedings of the 8th IEEE International Workshop on Information Forensics and Security, WIFS, Abu Dhabi, United Arab Emirates, 4–7 December 2016. [CrossRef]
66. Zeng, H.; Qin, T.; Kang, X.; Liu, L. Countering anti-forensics of median filtering. In Proceedings of the ICASSP, IEEE International Conference on Acoustics, Speech and Signal Processing, Florence, Italy, 4–9 May 2014; pp. 2704–2708. [CrossRef]
67. Fan, W.; Wang, K.; Cayre, F.; Xiong, Z. Median filtered image quality enhancement and anti-forensics via variational deconvolution. *IEEE Trans. Inf. Forensics Secur.* **2015**, *10*, 1076–1091. [CrossRef]
68. Fontani, M.; Barni, M. Hiding Traces of Median Filtering in Digital Images. In Proceedings of the European Signal Processing Conference, Bucharest, Romania, 27–31 August 2012; pp. 1239–1243. Available online: https://www.scopus.com/inward/record.uri?eid=2-s2.0-84869807478&partnerID=40&md5=53ba0ecb13a67b9540393515ca0b3f90 (accessed on 14 June 2024).

69. Waleed, J.; Hasan, T.M.; Abbas, T. Comprehensive expansion in Anti-Forensics Techniques (AFTs) based compressed image. In Proceedings of the 2017 Annual Conference on New Trends in Information and Communications Technology Applications, NTICT, Baghdad, Iraq, 7–9 March 2017; pp. 156–161. [CrossRef]
70. Yang, H.; Zhou, Z. Hiding the Trace of JPEG compression history. In Proceedings of the 2014 4th International Conference on Communication Systems and Network Technologies, CSNT, Bhopal, India, 7–9 April 2014; pp. 909–913. [CrossRef]
71. Afshin, N.; Razzazi, F.; Moin, M.-S. A dictionary based approach to JPEG anti-forensics. In Proceedings of the 2016 IEEE 8th International Conference on Intelligent Systems, IS 2016, Sofia, Bulgaria, 4–6 September 2016; pp. 778–783. [CrossRef]
72. Feng, C.; Xu, Z.; Zheng, X. An anti-forensic algorithm of JPEG double compression based forgery detection. In Proceedings of the 2012 4th International Symposium on Information Science and Engineering, ISISE, Shanghai, China, 14–16 December 2012; pp. 159–164. [CrossRef]
73. Sheng, G.; Su, Q. Erasing the JPEG compression artefacts: An improved counter-forensic algorithm based on parameter adjustment. In Proceedings of the 2014 9th International Conference on Broadband and Wireless Computing, Communication and Applications, BWCCA, Guangdong, China, 8–10 November 2014; pp. 321–324. [CrossRef]
74. Singh, A.K.; Rawat, C.S.; Bhatia, A. Alleviation of quantization artefact using anti-forensic in image processing. In Proceedings of the 2017 International Conference on Energy, Communication, Data Analytics and Soft Computing, ICECDS, Chennai, India, 1–2 August 2017; pp. 2697–2701. [CrossRef]
75. Singh, G.; Singh, K. Counter JPEG anti-forensic approach based on the second-order statistical analysis. *IEEE Trans. Inf. Forensics Secur.* **2019**, *14*, 1194–1209. [CrossRef]
76. Stamm, M.C.; Tjoa, S.K.; Lin, W.S.; Liu, K.J.R. Anti-forensics of JPEG compression. In Proceedings of the ICASSP, IEEE International Conference on Acoustics, Speech and Signal Processing, Dallas, TX, USA, 14–19 March 2010; pp. 1694–1697. [CrossRef]
77. Valenzise, G.; Nobile, V.; Tagliasacchi, M.; Tubaro, S. Countering JPEG anti-forensics. In Proceedings of the International Conference on Image Processing, ICIP, Brussels, Belgium, 11–14 September 2011; pp. 1949–1952. [CrossRef]
78. Kaimal, A.B.; Manimurugan, S.; Rajivkumar, J.; Anitha. A new technique for removing forensically detectable traces from digital images. In Proceedings of the 7th International Conference on Intelligent Systems and Control, ISCO, Coimbatore, India, 4–5 January 2013; pp. 321–324. [CrossRef]
79. Fan, W.; Wang, K.; Cayre, F.; Xiong, Z. JPEG anti-forensics with an improved tradeoff between forensic undetectability and image quality. *IEEE Trans. Inf. Forensics Secur.* **2014**, *9*, 1211–1226. [CrossRef]
80. Chu, X.; Stamm, M.C.; Chen, Y.; Liu, K.J.R. Concealability-rate-distortion tradeoff in image compression anti-forensics. In Proceedings of the ICASSP, IEEE International Conference on Acoustics, Speech and Signal Processing, Vancouver, BC, Canada, 26–31 May 2013; pp. 3063–3067. [CrossRef]
81. Bhardwaj, D.; Pankajakshan, V. An approach to expose dithering-based JPEG anti-forensics. *Forensic Sci. Int.* **2021**, *328*, 111040. [CrossRef]
82. Qian, Z.; Zhang, X. Improved anti-forensics of JPEG compression. *J. Syst. Softw.* **2014**, *91*, 100–108. [CrossRef]
83. Sutthiwan, P.; Shi, Y.Q. Anti-forensics of double JPEG compression detection. *Lect. Notes Comput. Sci.* **2012**, *7128*, 411–424. [CrossRef]
84. Chu, X.; Stamm, M.C.; Chen, Y.; Liu, K.J.R. On antiforensic concealability with rate-distortion tradeoff. *IEEE Trans. Image Process.* **2015**, *24*, 1087–1100. [CrossRef]
85. Jiang, Y.; Zeng, H.; Kang, X.; Liu, L. The game of countering JPEG anti-forensics based on the noise level estimation. In Proceedings of the 2013 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference, APSIPA 2013, Kaohsiung, Taiwan, 29 October–1 November 2013. [CrossRef]
86. Shelke, P.M.; Prasad, R.S. An improved anti-forensics JPEG compression using Least Cuckoo Search algorithm. *Imaging Sci. J.* **2018**, *66*, 169–183. [CrossRef]
87. Kumar, A.; Singh, G.; Kansal, A.; Singh, K. Digital image forensic approach to counter the JPEG anti-forensic attacks. *IEEE Access* **2020**, *9*, 4364–4375. [CrossRef]
88. Singh, G.; Singh, K. Improved JPEG anti-forensics with better image visual quality and forensic undetectability. *Forensic Sci. Int.* **2017**, *277*, 133–147. [CrossRef] [PubMed]
89. Stamm, M.C.; Tjoa, S.K.; Lin, W.S.; Liu, K.J.R. Undetectable image tampering through JPEG compression anti-forensics. In Proceedings of the International Conference on Image Processing, ICIP, Hong Kong, China, 26–29 September 2010; pp. 2109–2112. [CrossRef]
90. Fahmy, G. Detectable Tampering of JPEG Anti-Forensics. In Proceedings of the WIAR 2012—National Workshop on Information Assurance Research, Riyadh, Saudi Arabia, 18 April 2012; pp. 45–48. Available online: https://www.scopus.com/inward/record.uri?eid=2-s2.0-84929257836&partnerID=40&md5=d92e5c5870e0554b15f2f635e6cc943c (accessed on 12 June 2024).
91. Fahmy, G.; Wurtz, R. Phase based forgery detection of JPEG anti forensics. In Proceedings of the 2016 IEEE International Symposium on Signal Processing and Information Technology, ISSPIT, Limassol, Cyprus, 12–14 December 2016; pp. 144–149. [CrossRef]
92. Li, Y.; Zhou, J. Anti-Forensics of Lossy Predictive Image Compression. *IEEE Signal Process. Lett.* **2015**, *22*, 2219–2223. [CrossRef]
93. Qian, Z.; Qiao, T. Simplified anti-forensics of JPEG compression. *J. Comput.* **2013**, *8*, 2483–2488. [CrossRef]
94. Kumar, A.; Kansal, A.; Singh, K. An improved anti-forensic technique for JPEG compression. *Multimed. Tools Appl.* **2019**, *78*, 25427–25453. [CrossRef]

95. Fan, W.; Wang, K.; Cayre, F.; Xiong, Z. A variational approach to JPEG anti-forensics. In Proceedings of the ICASSP, IEEE International Conference on Acoustics, Speech and Signal Processing, Vancouver, BC, Canada, 26–31 May 2013; pp. 3058–3062. [CrossRef]
96. Bhatia, A.; Rawat, C.D.; Kumarjetawat, A. Digital artifacts-anti-forensics approach for optimization of digital images. In Proceedings of the IEEE International Conference on Power, Control, Signals and Instrumentation Engineering, ICPCSI, Chennai, India, 21–22 September 2017; pp. 544–548. [CrossRef]
97. Fan, W.; Wang, K.; Cayre, F.; Xiong, Z. JPEG anti-forensics using non-parametric DCT quantization noise estimation and natural image statistics. In Proceedings of the IH and MMSec 2013, 2013 ACM Information Hiding and Multimedia Security Workshop, Montpellier, France, 17–19 June 2013; pp. 117–122. [CrossRef]
98. Bhardwaj, D.; Kumawat, C.; Pankajakshan, V. A method for detecting JPEG anti-forensics. *Commun. Comput. Inf. Sci.* **2018**, *841*, 190–197. [CrossRef]
99. Cao, Y.; Gao, T.; Sheng, G.; Fan, L.; Gao, L. A new anti-forensic scheme-hiding the single JPEG compression trace for a digital image. *J. Forensic Sci.* **2015**, *60*, 197–205. [CrossRef]
100. Das, T.K. Anti-forensics of JPEG compression detection schemes using an approximation of DCT coefficients. *Multimed. Tools Appl.* **2018**, *77*, 31835–31854. [CrossRef]
101. Valenzise, G.; Tagliasacchi, M.; Tubaro, S. The cost of JPEG compression anti-forensics. In Proceedings of the ICASSP, IEEE International Conference on Acoustics, Speech and Signal Processing, Prague, Czech Republic, 22–27 May 2011; pp. 1884–1887. [CrossRef]
102. Zeng, H.; Yu, J.; Kang, X.; Lyu, S. Countering JPEG anti-forensics based on noise level estimation. *Sci. China Inf. Sci.* **2018**, *61*, 032103. [CrossRef]
103. Sheng, G.; Yang, B. An improved counter-forensic algorithm to erase the JPEG compression artifacts. *Int. J. Mob. Comput. Multimed. Commun.* **2014**, *6*, 22–32. [CrossRef]
104. Stamm, M.C.; Liu, K.J.R. Anti-forensics of digital image compression. *IEEE Trans. Inf. Forensics Secur.* **2011**, *6*, 1050–1065. [CrossRef]
105. Pasquini, C.; Boato, G. JPEG compression anti-forensics based on first significant digit distribution. In Proceedings of the 2013 IEEE International Workshop on Multimedia Signal Processing, MMSP, Pula, Italy, 30 September–2 October 2013; pp. 500–505. [CrossRef]
106. Li, B.; Zhang, H.; Luo, H.; Tan, S. Detecting double JPEG compression and its related anti-forensic operations with CNN. *Multimed. Tools Appl.* **2019**, *78*, 8577–8601. [CrossRef]
107. Milani, S.; Tagliasacchi, M.; Tubaro, S. Antiforensics attacks to Benford's law for the detection of double compressed images. In Proceedings of the ICASSP, IEEE International Conference on Acoustics, Speech and Signal Processing, Vancouver, BC, Canada, 26–31 May 2013; pp. 3053–3057. [CrossRef]
108. Li, H.; Luo, W.; Huang, J. Anti-forensics of double JPEG compression with the same quantization matrix. *Multimed. Tools Appl.* **2015**, *74*, 6729–6744. [CrossRef]
109. Huang, D.; Tang, W.; Li, B. Anti-forensics for Double JPEG Compression Based on Generative Adversarial Network. *Lect. Notes Comput. Sci.* **2021**, *12888*, 759–771. [CrossRef] [PubMed]
110. Wu, J.; Sun, W. Towards multi-operation image anti-forensics with generative adversarial networks. *Comput. Secur.* **2021**, *100*, 102083. [CrossRef]
111. Bhardwaj, D.; Kumawat, C.; Pankajakshan, V. Detection of Various Anti-Forensic Operations Based on DCT Coefficient Analysis. In Proceedings of the INDICON 2018—15th IEEE India Council International Conference, Coimbatore, India, 16–18 December 2018. [CrossRef]
112. Shelke, P.M.; Prasad, R.S. Improving JPEG image anti-forensics. In Proceedings of the ACM International Conference Proceeding Series, Udaipur, India, 4–5 March 2016. [CrossRef]
113. Kumar, A.; Kansal, A.; Singh, K. Anti-forensic approach for JPEG compressed images with enhanced image quality and forensic undetectability. *Multimed. Tools Appl.* **2020**, *79*, 8061–8084. [CrossRef]
114. Wu, J.; Liu, L.; Kang, X.; Sun, W. A Generative Adversarial Network Framework for JPEG Anti-Forensics. In Proceedings of the 2020 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference, APSIPA ASC 2020, Virtual, Auckland, New Zealand, 7–10 December 2020; pp. 1442–1447. Available online: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85100919989&partnerID=40&md5=dd7789183499aa6683b62c0c5c977229 (accessed on 14 June 2024).
115. Kaimal, A.B.; Manimurugan, S.; Anitha, J. A modified anti-forensic technique for removing detectable traces from digital images. In Proceedings of the 2013 International Conference on Computer Communication and Informatics, ICCCI 2013, Coimbatore, India, 4–6 January 2013. [CrossRef]
116. Peng, A.; Zeng, H.; Lin, X.; Kang, X. Countering anti-forensics of image resampling. In Proceedings of the International Conference on Image Processing, ICIP, Quebec City, QC, Canada, 27–30 September 2015; pp. 3595–3599. [CrossRef]
117. He, P.; Li, W.; Zhang, J.; Wang, H.; Jiang, X. Overview of passive forensics and anti-forensics techniques for GAN-generated image. *J. Image Graph.* **2022**, *27*, 88–110. [CrossRef]
118. Xie, H.; Ni, J.; Shi, Y.Q. Dual-Domain Generative Adversarial Network for Digital Image Operation Anti-Forensics. *IEEE Trans. Circuits Syst. Video Technol.* **2022**, *32*, 1701–1706. [CrossRef]

119. Ravan, J.; Thanuja. Image Forgery Detection against Forensic Image Digital Tampering. In Proceedings of the International Conference on Computational Techniques, Electronics and Mechanical Systems, CTEMS, Belgaum, India, 21–22 December 2018; pp. 315–321. [CrossRef]
120. Mayer, O.; Stamm, M.C. Countering anti-forensics of lateral chromatic aberration. In Proceedings of the IH and MMSec 2017, 2017 ACM Workshop on Information Hiding and Multimedia Security, Philadelphia, PA, USA, 20–22 June 2017; pp. 15–20. [CrossRef]
121. Mayer, O.; Stamm, M.C. Anti-forensics of chromatic aberration. In Proceedings of the SPIE—The International Society for Optical Engineering, San Francisco, CA, USA, 8–12 February 2015; p. 9409. [CrossRef]
122. Dou, L.; Qian, Z.; Qin, C.; Feng, G.; Zhang, X. Anti-forensics of diffusion-based image inpainting. *J. Electron. Imaging* **2020**, *29*, 043026. [CrossRef]
123. Salman, M.; Uhl, A. Countering anti-forensics of SIFT-based copy-move detection. In Proceedings of the International Conference on Pattern Recognition, Milan, Italy, 10–15 January 2020; pp. 2701–2707. [CrossRef]
124. Wu, J.; Wang, Z.; Zeng, H.; Kang, X. Multiple-operation image anti-forensics with WGAN-GP framework. In Proceedings of the 2019 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference, APSIPA ASC, Lanzhou, China, 18–21 November 2019; pp. 1303–1307. [CrossRef]
125. Chen, C.; Li, H.; Luo, W.; Yang, R.; Huang, J. Anti-forensics of JPEG Detectors via Adaptive Quantization Table Replacement. In Proceedings of the International Conference on Pattern Recognition, Stockholm, Sweden, 24–28 August 2014; pp. 672–677. [CrossRef]
126. Wang, H.; Wang, J.; Luo, X.; Yin, Q.; Ma, B.; Sun, J. Modify the Quantization Table in the JPEG Header File for Forensics and Anti-forensics. *Lect. Notes Comput. Sci.* **2022**, *13180*, 72–86. [CrossRef] [PubMed]
127. Zhao, H.; Chen, Y.; Wang, R.; Malik, H. Anti-Forensics of Environmental-Signature-Based Audio Splicing Detection and Its Countermeasure via Rich-Features Classification. *IEEE Trans. Inf. Forensics Secur.* **2016**, *11*, 1603–1617. [CrossRef]
128. Tao, B.; Wang, R.; Yan, D.; Jin, C. Anti-forensics of double compressed MP3 audio. *Int. J. Digit. Crime Forensics* **2020**, *12*, 45–57. [CrossRef]
129. Liu, T.; Yan, D.; Yan, N.; Chen, G. Anti-forensics of fake stereo audio using generative adversarial network. *Multimed. Tools Appl.* **2022**, *81*, 17155–17167. [CrossRef]
130. Mascia, M.; Canclini, A.; Antonacci, F.; Tagliasacchi, M.; Sarti, A.; Tubaro, S. Forensic and anti-forensic analysis of indoor/outdoor classifiers based on acoustic clues. In Proceedings of the 2015 23rd European Signal Processing Conference, EUSIPCO, Nice, France, 31 August–4 September 2015; pp. 2072–2076. [CrossRef]
131. Li, X.; Yan, D.; Dong, L.; Wang, R. Anti-Forensics of Audio Source Identification Using Generative Adversarial Network. *IEEE Access* **2019**, *7*, 184332–184339. [CrossRef]
132. Chuang, W.-H.; Garg, R.; Wu, M. Anti-forensics and countermeasures of electrical network frequency analysis. *IEEE Trans. Inf. Forensics Secur.* **2013**, *8*, 2073–2088. [CrossRef]
133. Moon, S.K.; Raut, R.D. Anti-forensic reversible multi frame block to block pixel mapping information concealing approach to increase the robustness and perceptibility. *Int. J. Inf. Comput. Secur.* **2021**, *14*, 403–439. [CrossRef]
134. Moon, S.K. Authentication and Security Aspect of Information Privacy Using Anti-forensic Audio–Video Embedding Technique. *Lect. Notes Networks Syst.* **2022**, *436*, 157–171. [CrossRef]
135. Moon, S.K.; Raut, R.D. Application of data hiding in audio-video using anti forensics technique for authentication and data security. In Proceedings of the Souvenir of the 2014 IEEE International Advance Computing Conference, IACC, Gurgaon, India, 21–22 February 2014; pp. 1110–1115. [CrossRef]
136. Sun, H.-M.; Weng, C.-Y.; Lee, C.-F.; Yang, C.-H. Anti-forensics with steganographic data embedding in digital images. *IEEE J. Sel. Areas Commun.* **2011**, *29*, 1392–1403. [CrossRef]
137. Chen, R.-J.; Horng, S.-J.; Huang, P.-H. Anti-forensic steganography using multi-bit MER with flexible bit location. *Int. J. Ad Hoc Ubiquitous Comput.* **2015**, *18*, 54–66. [CrossRef]
138. Amritha, P.P.; Sethumadhavan, M.; Krishnan, R.; Pal, S.K. Anti-forensic approach to remove stego content from images and videos. *J. Cyber Secur. Mobil.* **2019**, *8*, 295–320. [CrossRef]
139. Chen, R.-J.; Lai, J.-L.; Horng, S.-J. Anti-forensic steganography using multi-bit minimum error replacement with flexible bit location. In Proceedings of the 2012 International Symposium on Computer, Consumer and Control, IS3C, Taichung, Taiwan, 4–6 June 2012; pp. 175–178. [CrossRef]
140. Gupta, D.; Mehtre, B.M. Mozilla firefox browsing artefacts in 3 different anti-forensics modes. *Lect. Notes Inst. Comput. Sci. Soc. Telecommun. Eng.* **2014**, *132*, 247–251. [CrossRef] [PubMed]
141. Castiglione, A.; Cattaneo, G.; De Maio, G.; De Santis, A. Automatic, selective and secure deletion of digital evidence. In Proceedings of the 2011 International Conference on Broadband and Wireless Computing, Communication and Applications, BWCCA, Barcelona, Spain, 26–28 October 2011; pp. 392–398. [CrossRef]
142. Jahankhani, H.; Anastasios, B.; Revett, K. Digital Anti Forensics: Tools and Approaches. In Proceedings of the 6th European Conference on Information Warfare and Security 2007, ECIW 2007, Shrivenham, UK, 2–3 July 2007; pp. 115–120. Available online: https://www.scopus.com/inward/record.uri?eid=2-s2.0-84873801938&partnerID=40&md5=d18c2598185c62531d703bdd25aa7ff5 (accessed on 14 June 2024).
143. Ding, N.; Gu, D.; Liu, Z. Disguisable symmetric encryption schemes for an anti-forensics purpose. *Lect. Notes Inst. Comput. Sci. Soc. Telecommun. Eng.* **2011**, *56*, 241–255. [CrossRef] [PubMed]

144. Srinivasan, A.; Nazaraj, S.T.; Stavrou, A. HIDEINSIDE—A novel randomized & encrypted antiforensic information hiding. In Proceedings of the 2013 International Conference on Computing, Networking and Communications, ICNC, San Diego, CA, USA, 28–31 January 2013; pp. 626–631. [CrossRef]
145. Forte, D.; Power, R. A tour through the realm of anti-forensics. *Comput. Fraud Secur.* **2007**, *2007*, 18–20. [CrossRef]
146. Mansfield-Devine, S. Fighting forensics. *Comput. Fraud Secur.* **2010**, *2010*, 17–20. [CrossRef]
147. Sammons, J. Antiforensics. *Basics Digit. Forensics* **2015**, 83–103. [CrossRef]
148. Srinivasan, A.; Dong, H.; Stavrou, A. FROST: Anti-Forensics Digital-Dead-DROp Information Hiding RobuST to Detection & Data Loss with Fault Tolerance. In Proceedings of the 12th International Conference on Availability, Reliability and Security, Reggio Calabria, Italy, 29 August–1 September 2017. [CrossRef]
149. Lee, S.S.; Chang, K.-Y.; Lee, D.; Hong, D. A new anti-forensic tool based on a simple data encryption scheme. In Proceedings of the Future Generation Communication and Networking, FGCN, Jeju, Republic of Korea, 6–8 December 2007; Volume 2, pp. 114–118. [CrossRef]
150. Raggo, M.; Hosmer, C. Forensics and Anti-Forensics. *Data Hiding* **2013**, 193–211. [CrossRef]
151. Filiol, E. Anti-Forensic Techniques Based on Malicious Cryptography. In Proceedings of the 9th European Conference on Information Warfare and Security 2010, ECIW 2010, Thessaloniki, Greece, 1–2 July 2010; pp. 63–72. Available online: https://www.scopus.com/inward/record.uri?eid=2-s2.0-84871242431&partnerID=40&md5=1bc89c9a336c7d5a80fa0f4f95cfcce8 (accessed on 14 June 2024).
152. Vadlamudi, D.; Rao, K.T.; Vidyullatha, P.; Rajasekhar Reddy, B. Analysis on Digital Forensics Challenges and Anti-Forensics Techniques in Cloud Computing. *Int. J. Eng. Technol.* **2018**, *7*, 1072–1075. Available online: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85077495880&partnerID=40&md5=b2b8cf8573fafd8c8f647ca5be85419e (accessed on 14 June 2024). [CrossRef]
153. Rani, D.R.; Kumari, G.G. A framework for detecting anti-forensics in cloud environment. In Proceedings of the IEEE International Conference on Computing, Communication and Automation, ICCCA, Greater Noida, India, 29–30 April 2016; pp. 1277–1280. [CrossRef]
154. Schmitt, S. Introducing Anti-Forensics to SQLite Corpora and Tool Testing. In Proceedings of the 11th International Conference on IT Security Incident Management and IT Forensics, IMF, Hamburg, Germany, 7–9 May 2018; pp. 89–106. [CrossRef]
155. Patil, V.T.; Manjrekar, A.A. A Novel Approach for Monitoring SQL Anti-Forensic Attacks Using Pattern Matching for Digital Forensic Investigation. *Commun. Comput. Inf. Sci.* **2013**, *377*, 162–167. [CrossRef]
156. Mohiddin, S.K.; Babu, Y.S. Unique methodology to mitigate anti-forensics in cloud using attack-graphs. *Int. J. Innov. Technol. Explor. Eng.* **2019**, *8*, 1569–1574. [CrossRef]
157. Rani, D.R.; Geethakumari, G. A framework for the identification of suspicious packets to detect anti-forensic attacks in the cloud environment—All Databases. *Peer-to-Peer Netw. Appl.* **2020**, *14*, 2385–2398. [CrossRef]
158. Jahankhani, H.; Beqiri, E. Memory-Based Antiforensic Tools and Techniques. *Int. J. Inf. Secur. Priv.* **2008**, *2*, 1–13. [CrossRef]
159. Stüttgen, J.; Cohen, M. Anti-forensic resilient memory acquisition. *Digit. Investig.* **2013**, *10*, S105–S115. [CrossRef]
160. Eschweiler, S.; Gerhards-Padilla, E. Towards sound forensic acquisition of volatile data. *Commun. Comput. Inf. Sci.* **2012**, *318*, 289–298. [CrossRef] [PubMed]
161. Ahn, N.Y.; Lee, D.H. Security of IoT Device: Perspective Forensic/Anti-Forensic Issues on Invalid Area of NAND Flash Memory. *IEEE Access* **2022**, *10*, 74207–74219. [CrossRef]
162. Kwak, J.; Kim, H.C.; Park, I.H.; Song, Y.H. Anti-forensic deletion scheme for flash storage systems. In Proceedings of the 2016 5th International Conference on Network Infrastructure and Digital Content, IEEE IC-NIDC, Beijing, China, 23–25 September 2016; pp. 317–321. [CrossRef]
163. Jahankhani, H.; Beqiri, E.; Revett, K. Advanced Manipulation of Digital Evidence Using Memory Based Anti-Forensic Tools. In Proceedings of the 3rd International Conference on Information Warfare and Security, Omaha, NE, USA, 24–25 April 2008; pp. 213–220. Available online: https://www.scopus.com/inward/record.uri?eid=2-s2.0-84896502398&partnerID=40&md5=d212a9af6260b551253286157555f0452 (accessed on 14 June 2024).
164. Thomas, P.; Morris, A. An investigation into the development of an anti-forensic tool to obscure USB flash drive device information on a windows XP platform. In Proceedings of the 3rd International Annual Workshop on Digital Forensics and Incidents Analysis, WDFIA, Malaga, Spain, 9 October 2008; pp. 60–66. [CrossRef]
165. Ahn, N.Y.; Lee, D.H. Forensics and Anti-Forensics of a NAND Flash Memory: From a Copy-Back Program Perspective. *IEEE Access* **2021**, *9*, 14130–14137. [CrossRef]
166. Bonetti, G.; Viglione, M.; Frossi, A.; Maggi, F.; Zanero, S. Black-box forensic and antiforensic characteristics of solid-state drives. *J. Comput. Virol. Hacking Tech.* **2014**, *10*, 255–271. [CrossRef]
167. Gil, H.P.; Kim, D.-H. A study on counter anti-forensics for hidden areas of removable media-All Databases. *Digit. Forensics Res.* **2021**, 72–84. [CrossRef]
168. Chandran, R.; Yan, W.Q. Attack graph analysis for network anti-forensics. *Int. J. Digit. Crime Forensics* **2014**, *6*, 28–50. [CrossRef]
169. Chandran, R.; Yan, W.Q. *A Comprehensive Survey of Antiforensics for Network Security*; Informa UK Limited: London, UK, 2013. [CrossRef]
170. Yaacoub, J.-P.A.; Noura, H.N.; Salman, O.; Chehab, A. Advanced digital forensics and anti-digital forensics for IoT systems: Techniques, limitations and recommendations. *Internet Things* **2022**, *19*, 100544. [CrossRef]

171. Jadied, E. Swap files Anti-Forensics on Linux. In Proceedings of the APMediaCast, Bali, Indonesia, 17–19 November 2016; pp. 73–79. [CrossRef]
172. Eterovic-Soric, B.; Choo, K.K.R.; Mubarak, S.; Ashman, H. Windows 7 Antiforensics: A Review and a Novel Approach. *J. Forensic Sci.* **2017**, *62*, 1054–1070. [CrossRef]
173. Azadegan, S.; Yu, W.; Liu, H.; Sistani, M.; Acharya, S. Novel anti-forensics approaches for smartphones. In Proceedings of the 2012 45th Hawaii International Conference on System Sciences, Maui, HI, USA, 4–7 January 2012; pp. 5424–5431. [CrossRef]
174. Karlsson, K.J.; Glisson, W.B. Android anti-forensics: Modifying cyanogenmod. In Proceedings of the 2014 47th Hawaii International Conference on System Sciences, Waikoloa, HI, USA, 6–9 January 2014; pp. 4828–4837. [CrossRef]
175. Gómez-Miralles, L.; Arnedo-Moreno, J. Hardening iOS Devices Against Remote Forensic Investigation. In *Security and Resilience in Intelligent Data-Centric Systems and Communication Networks*; Academic Press: Cambridge, MA, USA, 2018; pp. 261–283. [CrossRef]
176. Mirza, M.; Salamh, F.E.; Karabiyik, U. An Android Case Study on Technical Anti-Forensic Challenges of WhatsApp Application. In Proceedings of the 8th International Symposium on Digital Forensics and Security, ISDFS, Beirut, Lebanon, 1–2 June 2020.
177. Distefano, A.; Me, G.; Pace, F. Android Anti-Forensics through a Local Paradigm. In Proceedings of the DFRWS 2010 Annual Conference, Portland, OR, USA, 2–4 August 2010; Volume 7, pp. S83–S94. Available online: https://www.scopus.com/inward/record.uri?eid=2-s2.0-84868576837&partnerID=40&md5=0db5d221d544b6977c7ad28b54837f8a (accessed on 14 June 2024).
178. Zheng, J.; Tan, Y.-A.; Zhang, X.; Liang, C.; Zhang, C.; Zheng, J. An Anti-Forensics Method against Memory Acquiring for Android Devices. In Proceedings of the 2017 IEEE International Conference on Computational Science and Engineering and IEEE/IFIP International Conference on Embedded and Ubiquitous Computing, CSE and EUC 2017, Guangzhou, China, 21–24 July 2017; Volume 1, pp. 214–218. [CrossRef]
179. Sanda, P.; Pawar, D.; Radha, V. VM Anti-forensics: Detecting File Wiping Using File System Journals. *Smart Innov. Syst. Technol.* **2022**, *303*, 497–508. [CrossRef]
180. Cifuentes, J.; Cano, J. Analysis and implementation of anti-forensics techniques on ZFS. *IEEE Lat. Am. Trans.* **2012**, *10*, 1757–1766. [CrossRef]
181. Göbel, T.; Baier, H. Anti-forensics in ext4: On secrecy and usability of timestamp-based data hiding. In Proceedings of the DFRWS 2018 EU—Proceedings of the 5th Annual DFRWS Europe, Florence, Italy, 21–23 March 2018; pp. S111–S120. [CrossRef]
182. Sang, C.G. A Maximum Data Allocation Rule for an Anti-forensic Data Hiding Method in NTFS Index Record-All Databases. *Int. J. Internet Broadcast. Commun.* **2017**, *9*, 17–26. [CrossRef]
183. Sang, C.G. Data Hiding in NTFS Timestamps for Anti-Forensics-All Databases. *Int. J. Internet Broadcast. Commun.* **2016**, *8*, 31–40. [CrossRef]
184. Ding, X.; Zou, H. Time based data forensic and cross-reference analysis. In Proceedings of the ACM Symposium on Applied Computing, TaiChung, Taiwan, 21–24 March 2011; pp. 185–190. [CrossRef]
185. Palmbach, D.; Breitinger, F. Artifacts for Detecting Timestamp Manipulation in NTFS on Windows and Their Reliability. *Forensic Sci. Int. Digit. Investig.* **2020**, *32*, 300920. [CrossRef]
186. Göbel, T.; Baier, H. Anti-forensic capacity and detection rating of hidden data in the ext4 filesystem. *IFIP Adv. Inf. Commun. Technol.* **2018**, *532*, 87–110. [CrossRef] [PubMed]
187. Singh, B.; Gupta, G. Analyzing Windows Subsystem for Linux metadata to detect timestamp forgery. *IFIP Adv. Inf. Commun. Technol.* **2019**, *569*, 159–182. [CrossRef] [PubMed]
188. Wani, M.A.; Bhat, W.A.; Dehghantanha, A. An analysis of anti-forensic capabilities of B-tree file system (Btrfs). *Aust. J. Forensic Sci.* **2020**, *52*, 371–386. [CrossRef]
189. Cho, G.-S. Development of an anti-forensic tool for hiding a message in a directory index of NTFS. In Proceedings of the 2015 World Congress on Internet Security, WorldCIS, Dublin, Ireland, 19–21 October 2015; pp. 144–145. [CrossRef]
190. Meffert, C.S.; Baggili, I.; Breitinger, F. Deleting collected digital evidence by exploiting a widely adopted hardware write blocker. In Proceedings of the DFRWS 2016 USA, 16th Annual USA Digital Forensics Research Conference, Seattle, WA, USA, 7–10 August 2016; pp. S87–S96. [CrossRef]
191. Anti-forensics–subverting justice with exploitation. *Comput. Fraud Secur.* **2007**, *2007*, 16–18. [CrossRef]
192. Wundram, M.; Freiling, F.C.; Moch, C. Anti-forensics: The next step in digital forensics tool testing. In Proceedings of the 7th International Conference on IT Security Incident Management and IT Forensics, IMF, Nuremberg, Germany, 12–14 March 2013; pp. 83–97. [CrossRef]
193. Horsman, G.; Errickson, D. When finding nothing may be evidence of something: Anti-forensics and digital tool marks. *Sci. Justice* **2019**, *59*, 565–572. [CrossRef] [PubMed]
194. Bhat, W.A.; AlZahrani, A.; Wani, M.A. Can computer forensic tools be trusted in digital investigations? *Sci. Justice* **2021**, *61*, 198–203. [CrossRef] [PubMed]
195. Garfinkel, S. Anti-Forensics: Techniques, Detection and Countermeasures. In Proceedings of the ICIW 2007: 2nd International Conference on i-Warfare and Security, Monterey, CA, USA, 8–9 March 2007; pp. 77–84. Available online: https://www.scopus.com/inward/record.uri?eid=2-s2.0-84857978988&partnerID=40&md5=5a6022743fedb889133666c14446edb3 (accessed on 14 June 2024).
196. Majed, H.; Noura, H.N.; Chehab, A. Overview of Digital Forensics and Anti-Forensics Techniques. In Proceedings of the 8th International Symposium on Digital Forensics and Security, ISDFS, Beirut, Lebanon, 1–2 June 2020. [CrossRef]

197. Hausknecht, K.; Gruicic, S. Anti-computer forensics. In Proceedings of the 2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics, MIPRO 2017, Opatija, Croatia, 22–26 May 2017; pp. 1233–1240. [CrossRef]
198. Kessler, G.C. Anti-Forensics and the Digital Investigator. In Proceedings of the 5th Australian Digital Forensics Conference, Perth, WA, Australia, 3 December 2007; pp. 1–7. Available online: https://www.scopus.com/inward/record.uri?eid=2-s2.0-84867717801&partnerID=40&md5=949c3f0a566465c16a1f530e1b5b5471 (accessed on 14 June 2024).
199. Jain, A.; Chhabra, G.S. Anti-forensics techniques: An analytical review. In Proceedings of the 2014 7th International Conference on Contemporary Computing, IC3, Noida, India, 7–9 August 2014; pp. 412–418. [CrossRef]
200. Berghel, H. Hiding data, forensics, and anti-forensics. *Commun. ACM* **2007**, *50*, 15–20. [CrossRef]
201. Shavers, B.; Bair, J. Antiforensics. In *Hiding Behind the Keyboard*; Syngress: Rockland, MA, USA, 2016; pp. 153–172. [CrossRef]
202. Sremack, J.C.; Antonov, A.V. Taxonomy of Anti-Computer Forensics Threats. In Proceedings of the Lecture Notes in Informatics (LNI), Series of the Gesellschaft fur Informatik (GI), Stuttgart, Germany, 11–13 September 2007; Volume P-114, pp. 103–112. Available online: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85134610642&partnerID=40&md5=6cbddcdf4ade67ceb03e9dfc5bc9b13d (accessed on 14 June 2024).
203. Shin, W. Countermeasures against Anti-forensics by Analyzing Anti-forensics Techniques. *J. Secur. Eng.* **2014**, *11*, 605–614. [CrossRef]
204. Al-Mousa, M.R.; Sweerky, N.A.; Samara, G.; Alghanim, M.; Hussein, A.S.I.; Qadoumi, B. General Countermeasures of Anti-Forensics Categories. In Proceedings of the 2021 Global Congress on Electrical Engineering, GC-ElecEng, Valencia, Spain, 10–12 December 2021; pp. 5–10. [CrossRef]
205. Dardick, G.S.; La Roche, C.R.; Flanigan, M.A. Blogs: Anti-Forensics and Counter Anti-Forensics. In Proceedings of the 5th Australian Digital Forensics Conference, Perth, WA, Australia, 3 December 2007; pp. 199–203. Available online: https://www.scopus.com/inward/record.uri?eid=2-s2.0-77949588587&partnerID=40&md5=808ff63b75556dc1b1e5161fd12b5470 (accessed on 14 June 2024).
206. Cho, G. A Problem Solving Method for Non-Admittable Characters of a Windows File Name in a Directory Index Anti-Forensic Technique. *J. Korea Soc. Digit. Ind. Inf. Manag.* **2015**, *11*, 69–79. [CrossRef]
207. Adamu, B.Z.; Karabatak, M.; Ertam, F. A Conceptual Framework for Database Anti-forensics Impact Mitigation. In Proceedings of the 8th International Symposium on Digital Forensics and Security, ISDFS, Beirut, Lebanon, 1–2 June 2020. [CrossRef]
208. Lee, H.; Lee, H.-W. New Approach on Steganalysis: Reverse-Engineering based Steganography SW Analysis. In Proceedings of the ACM International Conference Proceeding Series, Langkawi, Malaysia, 18–21 February 2020; pp. 212–216. [CrossRef]
209. Hilley, S. Anti-forensics with a small army of exploits. *Digit. Investig.* **2007**, *4*, 13–15. [CrossRef]
210. Lees, C. Determining removal of forensic artefacts using the USN change journal. *Digit. Investig.* **2013**, *10*, 300–310. [CrossRef]
211. Lim, S.; Park, J.; Lim, K.-S.; Lee, C.; Lee, S. Forensic artifacts left by virtual disk encryption tools. In Proceedings of the 2010 3rd International Conference on Human-Centric Computing, HumanCom, Cebu, Philippines, 11–13 August 2010. [CrossRef]
212. Fanuscu, M.Ç.; Koçak, A.; Alkan, M. Detection of Counter-Forensic Incidents Using Security Information and Incident Management (SIEM) Systems [Güvenlik Bilgilerive Olay Yönetimi (SIEM) Sistemleri Kullanilarak Karşi Adli Bilişim Olaylarinin Tespiti]. In Proceedings of the 15th International Conference on Information Security and Cryptography, ISCTURKEY 2022, Ankara, Turkey, 19–20 October 2022; pp. 74–79. [CrossRef]
213. Irwin, A.S.M. Double-Edged Sword: Dual-Purpose Cyber Security Methods. *Adv. Sci. Technol. Secur. Appl.* **2018**, 101–112. [CrossRef] [PubMed]
214. Mehrotra, T.; Mehtre, B.M. Forensic analysis of Wickr application on android devices. In Proceedings of the 2013 IEEE International Conference on Computational Intelligence and Computing Research, IEEE ICCIC, Enathi, India, 26–28 December 2013. [CrossRef]
215. You, I.; Yim, K. Malware obfuscation techniques: A brief survey. In Proceedings of the 2010 International Conference on Broadband, Wireless Computing, Communication and Applications, Fukuoka, Japan, 4–6 November 2010; pp. 297–300. [CrossRef]
216. Brand, M. Forensic Analysis Avoidance Techniques of Malware. In Proceedings of the 5th Australian Digital Forensics Conference, Perth, WA, Australia, 3 December 2007; pp. 59–66. Available online: https://www.scopus.com/inward/record.uri?eid=2-s2.0-84867721509&partnerID=40&md5=20608384614fe39e7661e9a26c6defff (accessed on 14 June 2024).
217. Ratcliffe, C.; Bokolo, B.G.; Oladimeji, D.; Zhou, B. Detection of Anti-forensics and Malware Applications in Volatile Memory Acquisition. *Lect. Notes Comput. Sci.* **2022**, *13343*, 516–527. [CrossRef]
218. Agarwal, M.; Puzis, R.; Haj-Yahya, J.; Zilberman, P.; Elovici, Y. Anti-forensic = suspicious: Detection of stealthy malware that hides its network traffic. *IFIP Adv. Inf. Commun. Technol.* **2018**, *529*, 216–230. [CrossRef]
219. Li, J.; Gu, D.; Luo, Y. Android malware forensics: Reconstruction of malicious events. In Proceedings of the 32nd IEEE International Conference on Distributed Computing Systems Workshops, ICDCSW, Macau, China, 18–21 June 2012; pp. 552–558. [CrossRef]
220. Brand, M.; Valli, C.; Woodward, A. Malware forensics: Discovery of the intent of deception. In Proceedings of the 8th Australian Digital Forensics Conference, Perth, Australia, 30 November–2 December 2010; pp. 39–45. [CrossRef]
221. Nikolai, J.; Wang, Y.; Nepali, R.K. A Framework for Examining the Human Side of Anti-Forensic Measures. In Proceedings of the 20th Americas Conference on Information Systems, AMCIS, Savannah, GA, USA, 7–9 August 2014. Available online: https://www.scopus.com/inward/record.uri?eid=2-s2.0-84905978253&partnerID=40&md5=ba50e6d0113dcd3889b7e8f0bb529be8 (accessed on 14 June 2024).

222. Dahbur, K.; Mohammad, B. The Anti-Forensics Challenge. In Proceedings of the 2011 International Conference on Intelligent Semantic Web-Services and Applications, Amman, Jordan, 18–20 April 2011. [CrossRef]
223. Schlicher, B. Emergences of cyber anti-forensics impacting cyber security. In Proceedings of the CSIIRW'08—4th Annual Cyber Security and Information Intelligence Research Workshop: Developing Strategies to Meet the Cyber Security and Information Intelligence Challenges Ahead, Oak Ridge, TN, USA, 12–14 May 2008. [CrossRef]
224. Ölvecký, M.; Gabriška, D. Wiping Techniques and Anti-Forensics Methods. In Proceedings of the SISY 2018—IEEE 16th International Symposium on Intelligent Systems and Informatics, Subotica, Serbia, 13–15 September 2018; pp. 127–131. [CrossRef]
225. Dahbur, K.; Mohammad, B. Toward Understanding the Challenges and Countermeasures in Computer Anti-Forensics. *Cloud Comput. Adv. Des. Implement. Technol.* **2012**, 176–189. [CrossRef]
226. Forte, D. Dealing with forensic software vulnerabilities: Is anti-forensics a real danger? *Netw. Secur.* **2008**, *2008*, 18–20. [CrossRef]