Nicolás-Sánchez and Castro-Toledo
Crime Science (2024) 13:11
https://doi.org/10.1186/s40163-024-00209-7

Crime Science

SYSTEMATIC REVIEW

Open Access

Uncovering the social impact of digital steganalysis tools applied to cybercrime investigations: a European Union perspective

Alejandro Nicolás-Sánchez[1*] and Francisco J. Castro-Toledo[1,2*]

Abstract

Background European Union (EU) research on cybersecurity is actively developing more efficient digital steganalysis techniques aimed at uncovering hidden online illegal content in apparently legitimate multimedia files. Beyond issues such as the design, effectiveness and functionality of the technology, this paper addresses the recently raised concern of societal impact, which refers to the influence, consequences, or effects, whether expected or not, that a particular action, policy, or technological advance has on society as a whole or on different segments of society. These impacts can be broad and multifaceted, encompassing economic, social, cultural, environmental and ethical dimensions, amongst others.

Aim The aim of this article is to take an exploratory look at the societal challenges and benefits associated with the use of digital steganalysis tools in cybercrime investigations in EU member states, adopting a dual mixed-methods perspective.

Methods First, a systematic review of the scientific literature published within 2017–2023, focusing on the societal dimension of steganalysis tools, including peer reviewed journal and conference papers on steganalysis and crime ($N=55$) was carried out. For the second part of the paper, two nominal group discussions were conducted with experts from Law Enforcement Agencies (LEAs): the first on societal benefits ($N=7$), the second on societal challenges ($N=6$). These consensus-building discussions aimed to identify, quantitatively assess and rank the various challenges and potential social benefits associated with the use of digital steganalysis tools in police investigations.

Results Findings reveal a widespread oversight in addressing the social impact dimension by tool designers on academic papers, especially regarding societal acceptance issues. The expert-citizens argued for stakeholders and public awareness of both risks and benefits of steganalysis tools.

Conclusions This study highlights the current need to consider not only the technological aspects, but also the profound social dimension arising from the use of these tools, such as public awareness of cybercrime and the ethical design and use of digital crime investigation tools. Understanding and evaluating societal impacts is essential for making informed decisions, shaping policies, and addressing the needs and concerns of diverse stakeholders in various domains. This multidisciplinary approach is crucial to achieving a more balanced and comprehensive understanding of the impact of digital steganalysis tools in the field of digital criminal investigation.

*Correspondence:
Alejandro Nicolás-Sánchez
anicolas@plusethics.com
Francisco J. Castro-Toledo
fcastro@plusethics.com; toledo@paradigma-innovation.eu
Full list of author information is available at the end of the article

Keywords Steganalysis, Social impact, Forensic tools, Law Enforcement Agencies, Systematic Review, Nominal Group

Introduction

Cybercriminals are constantly adapting their methods to counter cybersecurity measures, and a notable trend in cybercrime is the increasing use of 'information hiding' or 'data hiding' to evade detection and prosecution (Collier & Hutchings, 2023; Wu et al., 2023). Data hiding, broadly speaking, is the process of embedding secret information within a carrier or cover work to enable extraction by authorised recipients (Megías, 2020). While there are many techniques for digitally hiding information (Fernandes, 2022), the focus here is on a specific technique within data hiding called steganography. Steganography, which derives its name from the Greek words 'steganos' (to cover) and 'grapho' (to write), is an ancient practice that predates electronic technology (Karampidis et al., 2018). It dates back to 440 BC and was used by ancient civilisations such as the Egyptians and Greeks, and during both world wars for covert communication (Araujo & Kazemian, 2020). Steganography encompasses various techniques for hiding messages or data in non-secret digital files, such as messages, audio, images or videos (Caviglione & Mazurczyk, 2022; Prakash et al., 2021), allowing secret information to be transmitted discreetly between communicating parties (Megías, 2020). In this respect, steganography is a practice with both legal and illegal applications. On the legal side, it is used for secure communication between individuals, banks, companies, the medical field and military and intelligence operations (Dalal & Juneja, 2021; Prakash et al., 2021). It is also used in multimedia for copyright protection (Megías, 2020) and access control to digital content (Araujo & Kazemian, 2020), as well as in electronic money, radar systems and remote sensing (Prakash et al., 2021). However, malicious actors use steganography for nefarious purposes, such as hiding terrorist or organised crime communications (Dalal & Juneja, 2021; Djebbar, 2021; Fernandes, 2022), distributing viruses (referred to as "stegomalware") (Caviglione & Mazurczyk, 2022), and sharing illegal content, including child sexual abuse material (Araujo & Kazemian, 2020; Casino et al., 2022). Steganalysis techniques and tools, on the other hand, play a crucial role in digital forensic investigations, allowing authorities to detect and decipher hidden evidence.

This hidden information is imperceptible to the human eye and requires specialised tools and knowledge to detect. In response, digital forensic tools have become a key element in the prevention and fight against delinquency (Casino et al., 2022; Wu et al., 2020). These tools allow Law Enforcement Agencies (LEAs) to collect and analyse digital evidence in criminal cases, increasing the effectiveness and judicial guarantees of investigations and the number of convictions (Wilson-Kovacs & Wilcox, 2023; Hughes et al., 2021; Arshad et al., 2018; on the contrary, Stoykova et al., 2022). To achieve this, steganalysis is the process of systematically detecting, analysing and extracting hidden information from steganographic content. It aims to uncover what has been hidden by steganography, to identify the presence of hidden data and, if possible, to recover this concealed information (Araujo & Kazemian, 2020; Karampidis et al., 2018). Despite historically limited attention in the academic literature, the use of information hiding techniques such as steganography in cybersecurity has gained increasing scientific interest due to their growing sophistication (see Fig. 1). In particular, this development underscores the technical need for steganalysis tools to evolve as well to ensure effective detection and analysis of these hidden contents.

However, the technological dimension of the prevention of criminal steganography is not the only noteworthy issue for the purposes of this work. Scientific and policy interest in positive and negative social impact has been growing in cybersecurity and security studies over the last decade (Hytönen & Ruoslahti, 2022; Bührer et al., 2022; Burton & Lain, 2020; Davey & Wootton, 2017). In other words, the aim of designers and end-users should not only be to pursue the beneficial effects of security research, such as improved health and well-being, reduced violence and social conflict, reduced anxiety and perceptions of insecurity, increased economic stability, confidence in financial markets and increased investment, etc., but also to avoid undesirable negative outcomes, including the increase in insecurity (Burgess, 2012), as well as the impact on societal values and fundamental rights (Christen et al., 2020) or the failure to work on human-centred solutions (Wu et al., 2023, Hytönen & Ruoslahti, 2022; Burton & Lain, 2020).

In light of these concerns, this paper is divided into two sections in order to assess these potential societal impacts, in particular the challenges and benefits of steganalysis tools applied to cybercrime investigations. The first section reviews the current state of the art on the societal impacts of steganalysis tools in the context of cybersecurity enforcement, based on a systematic quantitative analysis of specialised literature ($N=55$) published between 2017 and 2023. This analysis reveals a consistent neglect of the social dimension by researchers. To address this gap, the second section aims to identify and assess the potential societal benefits and challenges of steganalysis tools in combating cybercrime and their impact on end-users by presenting empirical evidence from two nominal

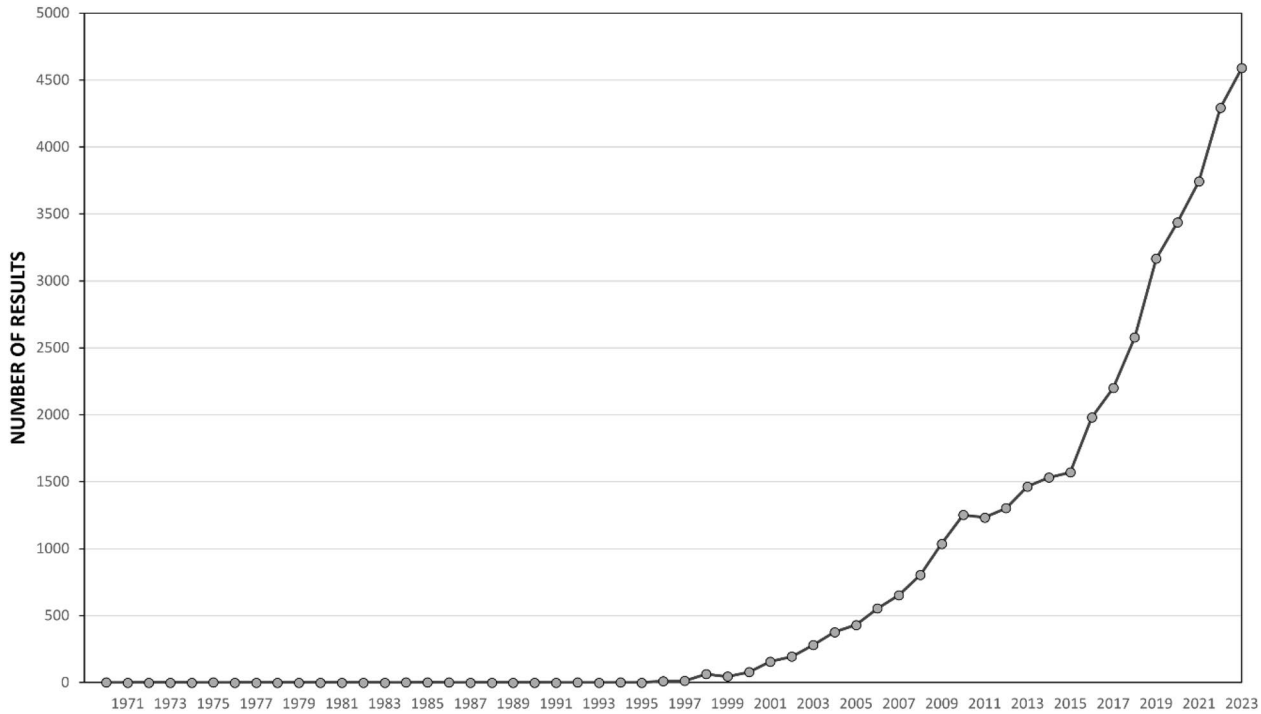

Fig. 1 Results of the search "steganography OR steganalysis" in Scopus database (1970–2023: N= 39,042 results).

groups involving LEAs, digital forensic experts and European citizens. The methodology of this consensus building analysis strategy is rigorously grounded in the social sciences, and the results provide new insights and challenges for consideration by key stakeholders.

A systematic review of the specialised literature on societal impact of steganalysis tools

Data and methodology

A systematic review of literature was conducted in line with the Preferred Reporting Items of Systematic reviews and Meta-Analyses (PRISMA) guidelines (Page et al., 2021; Moher et al., 2009) and (Pickering & Byrne, 2014) to carry out a quantitative analysis of peer-reviewed papers on the societal impact of steganalysis research and techniques. With these studies, a database was built with the appropriate information to assess the state of the art. Such a method is recommended for reliable, quantifiable, and reproducible findings, and for identifying gaps in the field (Pickering & Byrne, 2014).

Data sources and search strategy

A wide range of databases were used as sources: ProQuest, Springer, Scopus, and Institute of Electrical and Electronics Engineers (IEEE). They were chosen because of their broad range of journal papers and conference papers, the ease of applying filters to the search and their high reputation as scientific search engines. Specifically, IEEE was added to the search due to its reputation in the technology field. The systematic searching was performed during March 2023, thus including papers published prior to that date.

The keywords that were used for this study were the following: Steganography, Steganalysis, Steganographic, Forensics, Crime, Terrorism, Pornography, Societal Impact, Societal Acceptance, Privacy, Data Protection, Sustainability, Discrimination, Fundamental Rights, and so on. But the search for documents containing all these keywords provided null results. Therefore, the final search strategy included the following keywords: "stegan* AND forens* AND crim*". The asterisk was used as a wildcard Boolean search operator with the intention of finding every document, both in English or Spanish, that contains related words, such as "steganalysis", "steganography", "steganographic" (techniques), "forensics", "crime", "cybercrime", "criminal", "cybercriminal", "criminalistics", "criminology" and so forth. One of the databases, ProQuest, gave lower results using the wildcard "stegan*", so it was decided that the following keywords should be used for that source: "(steganalysis OR steganography) AND forens* AND crim*".

For this study, a broader approach that would have generated significantly more potential results ("…OR crim*" instead of "…AND crim*") was ruled out due to the fact that the study focuses on criminality, delinquency, and

the illicit use of data-hiding tools. The selected keywords were determined after filtering out irrelevant papers and were required to have all three terms with "AND" to reduce the possibility of finding a large amount of content that was not focused on the study's objective. Despite these efforts, it was still challenging to determine if a paper was adequate to assess whether the social dimension was or not addressed.

Inclusion and exclusion criteria

The systematic review was conducted based on the following criteria:

- Criterion 1: peer-reviewed full-text papers published in scientific journals, and conference papers due to the fact that the main publication venues in computer science are conference proceedings.
- Criterion 2: documents written in English or Spanish, both for being the most used language in the scientific field, and specifically, the last one for being the native language of the authors. However, no papers written in Spanish were found.
- Criterion 3: publications limited in time to the period 2017–2023, for two main reasons: (1) to assess the most up-to-date contributions (especially in a rapidly evolving field), and (2) because, according to Fig. 1, most of the publications are made in this period.
- Criterion 4: geographical scope, as papers whose first author is affiliated or associated with a research institution in a Member State of the European Union, or studies funded by EU Member States or the European Commission itself.[1] This criterion was mainly adopted due to the unique and complex EU regulatory framework that significantly influences the development, implementation and social impact assessment of online forensic tools, including steganography and steganalysis (Caianiello & Camon, 2021). This framework includes regulations such as the General Data Protection Regulation (GDPR) and specific regulations related to judicial forensics (e-evidence), which are significantly different from the regulatory frameworks or standards in other regions such as the United States (Caianiello & Camon, 2021), China (Kao et al., 2019) and Russia (Rusman & Morozova, 2022), among other key countries related to the scientific literature on this topic. On the other hand, this criterion addresses practical efficiency and focus, ensuring that the selected studies are likely to reflect the nuances of the European social context. It is in line with the specific interests of the project's funders (i.e. the EC), who seek to understand the societal implications of these instruments within the EU's legal, cultural and social framework. Finally, by prioritising studies with a strong EU connection, this review aims to produce knowledge that reflects the complexities of the social impact of these tools in a European social context, providing an in-depth, contextualised insight to inform EU policy and practice.
- Criterion 5: documents that contain references to (cyber)crime or security issues related to information hiding and the development of countermeasures. This criterion was adopted in order to avoid including irrelevant and particularly engineering content with little or no mention of crime prevention or security, which does not allow researchers to discuss or evaluate properly its social dimension.

In addition, after this screening process, other documents were added which were not retrieved in the query but were found while searching by authors known for their interest in the data hiding field, in particular frequently cited papers. In order to follow the same scientific standard and to preserve the most systematic procedure possible, only full text papers were included and the exact same screening criteria as in the above-mentioned search was followed.

Filtering stages and quality assessment

The selection process of specialised literature was organised in eight stages to be incorporated in the systematic review. Those stages are outlined in the following flowchart (see Fig. 2):

1. The identification of the studies on specialised scientific databases through keywords search.
2. A record after the filters are applied: studies identified after applying the filters indicated above.
3. Identification of titles duplicated or retracted papers: filtering and removing duplicated papers (by headings) or identified by the databases as retracted.
4. Locating the context: determined by the affiliation of the first author or the funding bodies, only studies related to a European Union Member State were considered.
5. Abstract screening: scanning the abstracts of the papers and conference papers to find out whether

[1] Despite the initial restriction to studies related to EU institutions, United Kingdom research was included due to its historical relevance and potential contribution to understanding societal impacts in the EU. This inclusion is justified by previous UK-EU collaboration, continuity in key research areas, the cross-border nature of the topics studied, and specific post-Brexit agreements that facilitate research collaboration (in particular in the EU funding programmes). Each UK study considered for inclusion was assessed individually to ensure its alignment with the objectives of the review and its relevance to EU interests.

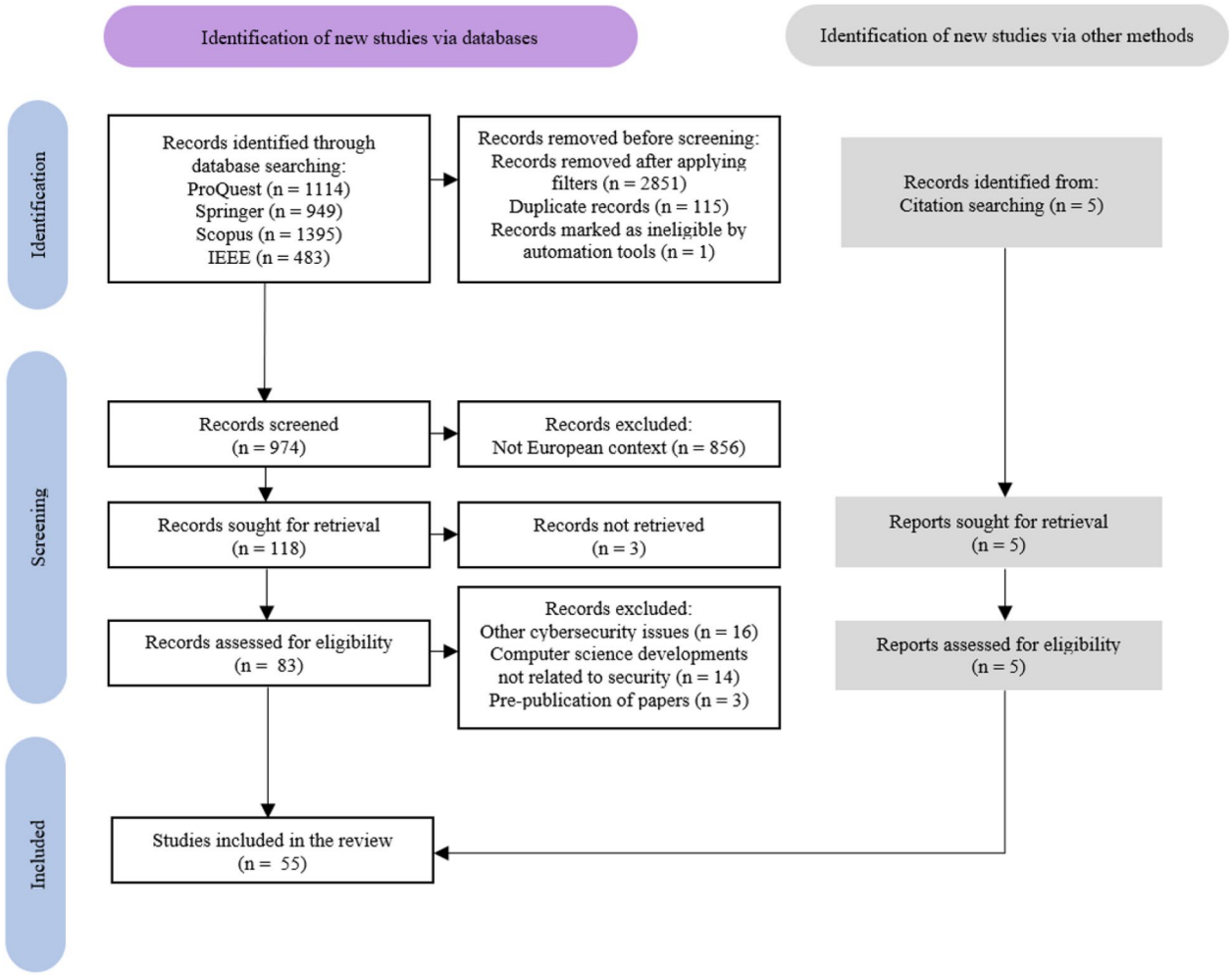

Fig. 2 Flow Diagram of the systematic review

they deal with information hiding, steganography or steganalysis and crime.

6. Full paper review: full text reading to gain in-depth knowledge of the content and ultimately to select it for consideration.
7. Other documents: searching by author's name or cited papers not previously included.
8. Studies included in the systematic review.

Once the 88 texts assessed for eligibility were read by one of the researchers and discussed by both researchers, 33 were rejected as their content did not coincide with the topic of this review. Many of them do not focus on information hiding, but on other cybersecurity and forensic issues such as bots, robots, criminal profiling, attribution of attacks, document leakage, mitigation of data loss and so on. Some others, while focusing on developing steganography or steganalysis tools, or other hiding-detection computer, do not include any reference to crime or security matters. Some of the excluded papers were pre-publications of papers that were subsequently published, and that are included in the review. That said, all papers dealing with the subject of "information hiding", such as steganography, steganalysis, stegomalware, tampering of evidence, content forgery, covert channels and imaging device identification methods were included. These subjects, while focusing on technical developments in similar domains, allow researchers to address, for example, the debate between data accessibility and privacy, so it was considered interesting to approach this issue more generally. Otherwise, if only pure "steganalysis as a forensic technique to fight crime" texts had been included, this systematic review would have been so limited in number of papers and conference papers that the results would hardly be reliable.

Thus, there are 33 journal papers and 22 conference papers, included in this systematic quantitative literature review, resulting in a total of 55 documents. The papers

chosen may not specifically deal with the societal impact of steganalysis, but some do include comments on the social relevance of these kinds of tools to fight crime, or some of the challenges they may have to face soon regarding, in some cases, the technological issues, but, in others, also the ethical ones.

Data extraction strategy

To respond to the objectives listed above, one of the researchers extracted the relevant information of all papers and conference papers included in the review. Within the first category, the features of the study such as author's affiliation and journal/conference discipline were considered. Moreover, since the subject matter of the selected studies was not limited to the specific aspect of steganalysis that would have been desirable to discuss, it seemed necessary to categorise a range of research topics in order to obtain a broader, richer, and more detailed picture of the issue.

Utilizing the Societal Impact Checklist for Security Research (Burgess, 2012) as a framework, the following categories were adapted to assess the present status of the societal dimension within steganalysis tools in cybersecurity research. The term 'social/societal impact' was employed as the foundation for assessing the pertinence, effectiveness, and accountability of this genre of security research.

First, it was examined if steganalysis research meets the needs of society:

- That is, whether it addresses documented societal security needs and if the proposed output meets them. The criteria for this assessment included an analysis to ascertain if the study's purpose is to improve and enhance security issues and which ones it focused on.
- These studies were evaluated to determine if the outputs are designed to produce outcomes that can benefit society by providing practical value. Therefore, both when the purpose of the study is not to create or assess the effectiveness of a data hiding (or its detection) tool and when the authors themselves highlight the limitations of their tools, negative responses were given, as no practical solutions were produced. Sometimes, tools are not created but collected from other sources and compared in reviews, leading to affirmative responses.
- Each document was assessed to identify technical descriptions of the tools under development or accumulations of techniques, methods and strategies, aiming to gauge the level of descriptiveness and transparency that the paper intends to achieve.
- An assessment was made to determine if the design of the tool included an evaluation of societal acceptance, or at least a brief consideration of whether the public should have a role in the design process.
- An analysis was conducted to identify whether the research addressed threats and dangers related to society's security, and which ones it focused on.

Secondly, an assessment was made to determine if steganalysis research has positive impacts on society (as societal benefits):

- In order to approach this broad concept, it was questioned if only specific segments of society will benefit from the research, or if it will be the society as a whole who will profit from the utilities derived from the tools. However, this is a complex question that the systematic review should not answer. So only the explicit observations of the original authors included in each paper were taken into consideration. In some cases, authors may not address this question, or it may not be explicitly stated in the text, in which case it was marked as "not specified". Therefore, caution should be observed when drawing conclusions.
- The papers' enhancement of societal values and other ethical aspects that refer to the idea of societal benefits of steganalysis research was also examined, to understand how the regulatory framework and social context shapes cybersecurity research, and, in particular, steganalysis research. This needs to be clear in this systematic review, as it was more than frequent to not see any explicit reference in the texts to these specific principles. That does not mean that they were not a backbone of the research or that authors did not consider societal benefits can be pursued. It means that they just were not mentioned. Providing an implicit and subjective appraisal of these values would only render this review not reproducible and biased. However, there were some analysed contributions that tended to focus more on this particular aspect than others did, albeit in different terms, and that also needed to be identified as clearly as possible. This is a limitation of this systematic quantitative literature review, but it was felt necessary in order to avoid achieving such results.

Finally, an examination was conducted to look into the potentially negative societal effects that may be caused as side effects of steganalysis research:

- In particular, in a similar but opposite sense to the previous category, the aim was to assess what potential negative impacts could result from steganalysis

research applied to cybercrime. This may include the impact on fundamental rights, social values, potential discrimination against certain groups that may result from the proposed research, and so on. The same considerations as above apply here, as the aim is not to demonstrate this possibility, but to explore the views and perceptions of the authors on this issue.
- Finally, any specific measures taken or reminded by the researchers to ensure compliance with human rights and to ease its negative impacts, if any, were gathered.

The encoding of the categories for each variable was designed based on an initial reading of the documents subject to the review, so as to be able to encompass the different topics of the papers in the most detailed and summarised way possible.

Quantitative results

As included in Table 1, the literature reviewed revealed a clear lack of interest in addressing social issues related to steganalysis uses. The papers are mainly published in technology-oriented journals, with a clear focus on producing practical results in the form of tools, regarding different (cyber) security threats and needs that justify the research on developing steganalysis, such as authenticity of digital content in relation to the criminal use of steganography, forensic investigations in crimes with digital evidence, or data protection in cyberattacks.

From a technical and descriptive point of view, various image or video steganalysis techniques, including visual attacks, signature-based methods, structural analyses, statistical examinations, spread spectrum techniques, blind probing, and so on, are developed, tested, or mentioned to reveal hidden information. Within this landscape, deep learning techniques are occasionally mentioned for their effectiveness and growing importance. A set of studies focuses on developing data hiding techniques, while the others test them against countermeasures. Continuously, the concept of wardens emerges as a prevalent countermeasure against the illicit sharing of data across networks. In the field of digital forensics, part of the research efforts is focused on preserving the chain of evidence while investigating possible tampering of legal evidence or trying to identify the source device of images or videos to ensure the reliability of such critical data. On the other hand, the emergence of stegomalware, a malicious technique that exploits data hidden in apparently innocuous files, is noted in scientific discourse and is rigorously tested against developed defence strategies. In the context of copyright management, watermarking protocols and advances in steganography are proving beneficial, while also facilitating the verification of the originality and attribution of ownership/authorship of images in the context of digital forensics. Each of these tools and methods plays a specific role in the field of steganalysis, providing solutions to challenges such as secure communications, copyright protection and digital forensics. The variety and complexity of these tools highlights the rapidly evolving nature of steganography and steganalysis technologies.

However, none of the selected research addresses societal acceptance, and, in general, it can be said that the societal dimension is not adequately covered. That said, we can identify from the research some of the potential societal benefits that can derive from steganalysis developments, such as the enhancement on the protection of human rights (ethics and protection of personal data), as well as the strict observance of international chain of custody laws, the improvement of cross-border cooperations, or the strengthening of public accountability and transparency. On the other hand, issues such as potential negative discrimination, negative impacts on rights and values, and ways to overcome these legal and ethical challenges are not sufficiently discussed throughout the texts, with brief and scarce mentions to privacy and data protection (such as illicit cloud-based invasions of the privacy of non-suspects via indiscriminate decryption of data), among other challenges or potential societal harms of steganalysis research.

Certainly, it is important to recognise that the reluctance to address social and ethical issues in academic papers (and especially conference papers) may be due to space constraints, which often prioritise technical aspects and results over broader ethical or social considerations. In addition, researchers may assume that ethical considerations and compliance with fundamental rights are implicitly understood or covered in the ethical review processes of their own research projects or institutions. This could explain the lack of explicit reference to these issues in published papers. However, it is also possible that there is a prevailing perception within the steganalysis community that societal impacts and ethical considerations are secondary to the primary technical focus of their research. Academic culture and publication norms may contribute to the omission of these aspects. Researchers may not be fully aware of the potential societal implications of their work, or may lack a framework for systematically assessing and addressing issues such as stakeholder engagement and societal acceptance, or the presence of discriminatory biases that may have been unconsciously transferred from designers to software. This highlights the importance of promoting interdisciplinary collaboration and ethical reflection within the field of steganalysis to ensure a more comprehensive

Table 1 Summary of quantitative results of the systematic review of steganalysis literature

Category	Variables	Modalities	N	%[a]
General information	Field of publication	Technology	19	35
		Security	18	33
		Computing sciences	15	27
		Information sciences	14	25
		Forensic sciences	8	15
		Multimedia development	7	13
		Imaging techniques	5	9
		Other	5	9
		Communications	4	7
		Electronics	1	2
		Ethics	1	2
	Research topic	Digital content originality	15	27
		Evidence in criminal courts and forensic laboratories	15	27
		Steganography	11	20
		Image forgeries detection	9	16
		Imaging device identification methods	7	13
		Stegomalware or covert channels detection	5	9
		Covert channels	5	9
		Steganography and steganalysis	4	7
		Review of digital forensics challenges	4	7
		Review of stegomalware and its detection	3	5
		Review of steganalysis techniques	1	2
		Review of steganography techniques	1	2
		Steganalysis	1	2
Steganalysis research meets the needs of society	Societal cybersecurity need(s) addressed	Ownership and authenticity of digital content	23	42
		Data protection (cybersecurity)	23	42
		Justice (forensics)	21	38
		Linkage of forensic investigations	7	13
		Public security	2	4
		Privacy of criminal investigations sensitive data	1	2
		Border control	1	2
	Research output	Yes: tool developed	35	64
		Yes: tools collected	12	22
		No	8	14
	Description of tool(s)	Yes	47	100
		No	0	0
		N/A[b]	8	–
	Societal acceptance assessment	Yes	0	0
		No	47	100
		N/A[b]	8	-
	Threats addressed	Crimes with digital evidence	17	31
		Cyberattacks	17	31
		Criminal use of steganography	15	27
		Privacy leakages	4	7
		Fake images	3	5
		Fake news	3	5
		Terrorism	3	5
		Copyright violations	2	4
		Fraudulent documents	2	4

Table 1 (continued)

Category	Variables	Modalities	N	%[a]
		Tampering of evidence	2	4
		Scientific misconduct	1	2
		Impersonation and fake profiles	1	2
		Money laundering	1	2
		Contract cheating	1	2
Steganalysis research has positive impacts (benefits) on society	Segment(s) of society benefitted	Specific segments: digital forensic community	2	4
		Specific segments: content owners	2	4
		Specific segments: academic staff	1	2
		Specific segments: victims	1	2
		Specific segments: social networks users	1	2
		Specific segments: big companies	1	2
		Society in general	7	12
		Not specified	40	72
	Identified societal positive impact(s)	Yes: human rights (ethics and protection of personal data)	6	11
		Yes: strict observance of international law (chain of custody)	4	7
		Yes: public accountability and transparency	3	5
		Yes: cross-border cooperation	3	5
		Yes: protection of the rights of the child	1	2
		Yes: sustainable development	1	2
		Yes: protection of external borders	1	2
		Yes: psychological wellbeing of young people	1	2
		Yes: mitigate economic risks	1	2
		No	44	80
Steganalysis research does not have negative impacts (challenges) on society	Identified societal negative impact(s)	Yes: privacy and data protection	4	7
		No	0	0
		Not specified	51	93
	Mitigation/minimisation measures	Yes: gathering and use of evidence rules	3	5
		Yes: data storage, protection and processing guidelines	2	4
		Yes: European law	2	4
		Yes: legal and ethical requirements of cloud-service-providers	1	2
		Yes: confidentiality case levels	1	2
		Yes: confidentiality agreements	1	2
		Yes: "responsible encryption"	1	2
		Yes: forensic standardization (ISO)	1	2
		No	51	93

[a] The percentages have been calculated in relation to the total number of studies reviewed ($N = 55$). For this reason, there are variables that can exceed 100% when different modalities occur at the same time as field of publication, research subject, societal cybersecurity needs, threats, beneficiaries, positive impacts, and mitigation measures

[b] In the variables where "N/A" is included, the percentages have been calculated in relation to the total number of studies that created or mentioned tools (n = 47). For this reason, the "N/A" papers are not included in these calculations

understanding and communication of the societal dimensions associated with this research.

In addition, the data extraction spreadsheet of the full sample of studies reviewed can be found in Appendix I: Table 4. Considering all of these results, the following section is therefore intended to address this gap in the literature.

An evaluation (through mixed methods) of social benefits and challenges of steganalysis tools

Methodology of nominal groups

Given the limited societal benefits and challenges associated with the use of such tools and techniques in crime prevention found in the systematic review, it was decided to use the Nominal Group Technique (NGT) with LEAs and digital forensics experts to fill the literature gaps identified in the previous section. This mixed-methods technique, originally developed by Delbecq & Van de Ven (1971), is one of the most appropriate methods for gathering information in situations where no prior data is available. This type of research allows for the exploration of questions that may not be best answered by purely quantitative approaches due to technical complexity or limited information available, and has an exploratory nature that can uncover dimensions that would otherwise be overlooked (Bachman & Schutt, 2017; Bush et al., 2020). In contrast, a large-scale survey to measure the societal benefits and challenges of these tools was deemed inappropriate due to the technical complexity of steganalysis topic and the limited information publicly available, making the results impractical. Instead, this methodology was used to capture the perspectives of experts in the field of digital forensic investigation tools (who are also European citizens who may be affected by the use of these tools). However, it is important to note that due to the limited availability of a sample of experts from LEAs, it was decided to conduct two nominal groups (one for positive impacts or benefits, one for negative impacts or challenges), thus making the study exploratory in nature. Certainly, this may be a limitation in terms of the ecological validity of the results, but the purpose of the nominal group technique is different, as mentioned above.

It can be thought of as a variation on small focus groups that are brought together in order to reach a consensus that can be quantified. Information is gathered by asking individuals to respond to questions posed by a moderator, and then participants are asked to prioritise the ideas or suggestions of all group members. The suitability of nominal groups for our purposes lies mainly in their nature as a consensus-building method, which is defined below:

> *"NGT is a highly structured technique combining characteristics of an individual survey and a focus group. Its structure limits researcher influence and influence from group dynamics. It increases the likelihood of equal participation for all group members and equal influence of (conflicting) values and ideas. NGT can be used in an exploratory (phase of a) study, can be used to generate hypotheses about topics which are relatively unfamiliar to the researcher, or to become familiar with the ideas found to be relevant to a research population that is socially and culturally different from the researcher. NGT is particularly relevant in applied research as a decision-making tool and as a consensus method" (Vander Laenen, 2015, p. 11).*

In summary, the process prevents one person from dominating the discussion, encourages all members of the group to participate, and results in a set of prioritised solutions or recommendations that represent the preferences of the group (De Ruyter, 1996; Hugé & Mukherjee, 2018; Vander Laenen, 2015).

In this regard, for the second part of this study, two nominal groups were conducted for the evaluation of key socio-economic, moral and legal factors potentially influencing the design of steganalysis tools and their positive and negative impacts on end-users. The aim of these groups was to use this consensus building method to formulate recommendations for the improvement of steganalysis tools and methods within the UNCOVER EU project.

The session was structured as follows, and it was briefly explained to the participants:

- Define the task: in the form of a question about societal benefits and challenges, in writing and visible to the group, ensuring that it is understood by everyone.
- Individual generation of ideas: participants were asked to individually write down in the chat 3 words or sentences related to the question, for 5 min.
- Record all ideas: they were typed into an Excel file by the moderator while sharing the screen.
- Clarify and discussion of ideas: for 20 min, each of the ideas generated was addressed in order to obtain clarification: similar ideas were grouped, rephrased and merged, or divided into several ones.
- Rank or prioritise ideas: individually, each participant selected what they considered to be the top 5 societal benefits/challenges and scored them from 5 points (top 1 benefit/challenge) to 1 point (top 5 benefit/challenge), giving a different score to each of them.
- Quantitatively determine priorities: when these scores were typed into the Excel file, it automatically showed quantitative results. The moderator also explained to the participants what these results meant.

There was a single session divided into two parts corresponding to the following questions:

1. Considering both your professional experience and your condition as a European citizen, what do you identify as the main societal benefits faced by steganalysis tools?
2. Considering both your professional experience and your condition as a European citizen, what do you identify as the main societal challenges faced by steganalysis tools?

With regard to the characteristics of the participants, a sample of LEAs and digital forensic experts belonging to the UNCOVER EU project consortium was selected. At the beginning, 7 participants participated in the "societal benefits" nominal group, which is a good number considering that the number of participants in a nominal group session is recommended to be less than 8 participants (De Ruyter, 1996; Hugé & Mukherjee, 2018; Vander Laenen, 2015). In the second part of the session, the nominal group on societal challenges, one participant had to leave due to an urgent matter, leaving 6 participants. Similarly, the nominal group session was conducted via online video conferencing a few weeks after the systematic review was conducted, and lasted 140 min (60 min each with a 20 min break). Prior to the session, the activity was ethically reviewed within the project and all participants gave their informed consent.

Nominal group results on social benefits of steganalysis tools

The first set of ideas discussed by the participants pertains to the societal benefits of steganalysis tools. Initially, there were 16 ideas proposed by participants, but this was eventually narrowed down to 9. Some ideas were duplicates, like those related to "getting information about crime," "proving crimes," and "providing court-proof evidence." Others were merged due to their similarity, such as "cooperation between law enforcement agencies (LEAs) and forensic institutes" and "cooperation in Europe" involving academia, industry, and other institutions. A few ideas about improving police work and providing better methods for LEAs were also combined. Some ideas were excluded for being too broad or not fitting the concept of "societal benefits." Certain concepts were clarified and debated, like "catching bad guys," which was divided into three separate ideas. Similarly, "treating people fairly" was distinguished from "providing a quicker and better response from LEAs."

The most rated societal benefit, both in terms of the number of points and the percentage of participants who supported it, was idea number 9 ("understanding the real size and impact of the problem"). Idea number 4 ("better scientific understanding of the world around us") ranked third in the number of votes. This suggests that steganalysis tools can assist society in understanding the workings of data hiding, the types of hidden illegal information, and their societal impacts, rather than solely in apprehending suspects or providing court-proof evidence. In second place was idea number 7 ("creating a safe environment for everyone"), which also connects to these notions but in a more general sense by improving overall societal security and trust in communication. Idea number 8 ("establishing confidence and trust in LEAs") was not highly voted but still ranked among the top five benefits, indicating the importance of improving public perception of law enforcement agencies (LEAs) and enhancing their cooperation with citizens in Europe (idea number 5). Conversely, ideas number 6 ("police treating people fairly") and 3 ("providing a quicker and better response from LEAs than manual intervention") were the least emphasised in this analysis. However, it is noted that these ideas should not be disregarded as they were brought up during the discussion. All this information is detailed in Table 2 below.

Nominal group results on social challenges of steganalysis tools

In terms of societal challenges in steganalysis, the discussion began with 10 ideas, and one more was removed during the discussion, resulting in 9 ideas (see Table 3). This round of discussions was more demanding, with fewer participants. Some ideas were merged, and others were removed. There was a debate about the balance between privacy and security, especially related to the use of steganalysis by law enforcement.

The most voted societal challenge, both in terms of points and the percentage of participants who supported it, was idea number 7 (lack of knowledge about the existence of steganography and steganalysis tools). It was ranked highly by everyone in the sample, with 50% considering it the top challenge. This indicates a consensus that there is limited knowledge about these tools, and it might need to stay that way to maintain their effectiveness against criminals. The lack of knowledge hampers research by academia and limits implementation by law enforcement agencies (LEAs). This relates to other challenges like demonstrating the efforts made in steganalysis, informing and training relevant parties, finding a balance between legal use, and trust in government/LEAs using these tools. Ideas number 5 (reliable results from steganalysis tools), 4 (building and maintaining state-of-the-art understanding and use by non-criminals), and 6 (proving the respect of chain of custody) are more technically related challenges in steganalysis development. While not the top challenge, the reliability of results generated by steganalysis tools is considered a significant

concern, especially in providing valid proof in court proceedings.

In summary, participants believe that improving the technical aspects, along with raising awareness about steganalysis, can help overcome the challenges. This not only addresses technical limitations but also the reluctance of stakeholders and society to rely on these digital crime investigation tools. That idea can be translated into a potential harm of steganalysis development, as creating something that civil society do not trust, with concerns about potential invasion of privacy rights, can potentially lead to societal rejection and discontent, both from the public and from key stakeholders.

Discussion and conclusions

In the last decade, considerable progress has been made in the tools of steganography, a technique for hiding information in digital files, as well as in its technological interest in the scientific and practitioners' community. However, digital forensics to detect (and potentially prevent) this type of cyberthreats have not only a technical dimension, but also societal issues of paramount importance. Throughout this paper, the need to approach this latter aspect from a rigorous and scientific evaluation has been taken as a starting point, in order to obtain quality evidence to assess the balance between the social benefits and challenges of these steganalysis tools. The ambition of this paper is to, from a European perspective: (1) establish, for the first time, the state-of-the-art on the social impact of steganalysis tools through a quantitative systematic review; and (2) obtain empirical evidence on the expert-citizen consensus on the challenges and social benefits of steganalysis tools through mixed methods (i.e., nominal groups). While the systematic review showed that these societal dimensions of digital steganalysis tools have not been adequately addressed by most of the previous scientific literature, only a few papers have partially developed these aspects (ethical issues: Casino et al., 2022, Stoyanova et al., 2020, Caviglione et al., 2017; privacy needs: Casino et al., 2022, Stoyanova et al., 2020, Caviglione et al., 2017; privacy invasions in the cloud: Odebade et al., 2017; confidentiality agreements: Stoyanova et al., 2020; chain of custody preservation and cross-border collaborations: Casino et al., 2022, Stoyanova et al., 2020; transparency of forensic tools: Stoyanova et al., 2020; explainability of procedures: Casino et al., 2022, Caviglione et al., 2021a; and legitimacy of solutions: Caviglione et al., 2021a).

From this work, the nominal groups aim to fill this large gap in the literature with empirical evidence. They also aim to validate what has been reported in other studies with new data in the following areas: (a) Improving the security of society by understanding how the criminal activity of data hiding works ("data hiding trends", Caviglione et al., 2021a), what kind of illegal information is hidden and to what extent it can harm society ("challenges for forensics", Ghanmi et al., 2021; Yari & Zargari, 2017) is the main benefit of steganalysis; and b) Raising awareness of the data hiding paradigm and the tools to combat its criminal use, both technically ("pursue explainability", Caviglione et al., 2021a) and among stakeholders ("understanding between all the actors involved", Casino et al., 2022) and the public ("trade-off between users' right to privacy and the success of the forensics investigation", Stoyanova, 2020; Odebade et al., 2017), is the priority societal challenge of steganalysis.

Our findings also help to confirm the claim that social impact assessment is crucial in cybersecurity research, as these policy areas are typically characterised by limited public transparency, justified by confidentiality and national interest, which often excludes stakeholders and hinders public acceptance of such measures, thus leading to suspicion (Wadhwa et al., 2014). It is also worth noting some concerns that European security research projects prioritise international techno-military industrial advances over addressing local and urban issues, which are closer to citizens and their (in)security experiences, or tackling the root causes of crime (Davey & Wootton, 2017). Nevertheless, the European Union's latest research and innovation funding programme, 'Horizon Europe', clearly recognises this concern, stating that in the field of security research, it is crucial that projects take into account human factors and societal contexts, while respecting fundamental rights such as privacy and the protection of personal data. The involvement of citizens and communities in assessing the societal impact of security technologies is essential to enhance the quality of research and public confidence. The integration of social sciences and humanities (SSH) and social innovation in security research is fundamental, as it fosters active citizen participation and promotes social change and ownership (EC, 2023, p. 8). While societal considerations are consistently overlooked in scholarly papers dedicated to stego-issues, it may be reasonable that within such a technical discipline, these aspects are confined to the ethical review processes, mandatory in all projects conducted in the European Union and institutions bound to its legal framework. Nevertheless, for the purpose of disseminating results and fostering increased social and end-users' acceptability of these technology solutions, additional time, tasks, and content should be allocated for the aim of ensuring a positive social impact, extending beyond purely technical advancements in computer science.

In conclusion, digital forensic tools in general, and advanced steganalysis tools in particular, are crucial for preventing and fighting cybercrime. However, it is also

Table 2 Summary of nominal group results on social benefits of steganalysis tools

Ideas	Votes			Participants	
	Points	%	*M*	*N*	%
1. Getting useful information to identify suspects	7	6.7	1.0	4	57.1
2. Providing court-proof evidence	11	10.5	1.6	5	71.4
3. Provide a quicker and better (accuracy and reliability) response from LEAs than only manual intervention	9	8.6	1.3	2	28.6
4. Better scientific understanding of the world around us (data structures and communication strategies): being able to detect and decipher hidden messages in order to understand which information in particular is important to people using steganography	14	13.3	2.0	4	57.1
5. Improvement of cooperation in Europe (academia, forensics institutes, LEAs, industrial, policy makers, military intelligence, etc.)	6	5.7	0.9	4	57.1
6. Police treat people fairly	3	2.9	0.4	1	14.3
7. Creating a safe environment to everyone	16	15.2	2.3	4	57.1
8. Establishing confidence and trust on LEAs	13	12.4	1.9	5	71.4
9. Understanding the real size and the impact of the problem	26	24.8	3.7	6	85.7
Total	105	100	–	7	–

Table 3 Summary of nominal group results on social challenges of steganalysis tools

Ideas	Votes			Participants	
	Points	%	*M*	*N*	%
1. No balance with legal use (stego as privacy/security tool)	2	2.2	0.3	2	33.3
2. Non-disclosure to society: security by obscurity (LEAs can't or don't want to share everything they know)	18	20.0	3.0	5	83.3
3. R&D/LEA efforts made in this field vs. its cost	13	14.4	2.2	4	66.7
4. Building-up and maintaining state-of-the-art understanding and use (by non-criminals)	8	8.9	1.3	4	66.7
5. Results generated by developed tools are reliable	18	20.0	3.0	5	83.3
6. Provide proof that CoC is respected (and built trust in process)	1	1.1	0.2	1	16.7
7. Lack of knowledge of the existence of stego as well as tools	21	23.3	3.5	6	100.0
8. Trust in government/LEAs in using the developed tools/techniques	0	0.0	0.0	0	0.0
9. Informing and training relevant parties	9	10.0	1.5	3	50.0
Total	90	100	–	6	–

important to consider the social impact and to ensure that they are used in a legitimate and responsible manner towards citizens. In addition to the benefits in terms of improved prevention and response by LEAs to these forms of cybercrime, this could include issues related to the potential privacy breaches through the monitoring of citizens' online activities; the potential risk of misuse by researchers or investigators, which could have serious implications for fundamental rights, civil liberties or the fair democratic processes; or the challenge in ensuring transparent and accountable use of these tools by authorities as a key element to maintain their legitimacy, among other negative social impacts. It is hoped that this work serves as a beginning point for the development of future research in this particular aspect, both within and outside the European context. Particularly relevant is to go beyond the European framework, for this study is limited by research and participants bound by European inclusion criteria.

Accordingly, LEAs and other security authorities need to take all possible precautions when designing, implementing or using these digital forensic tools. They need to work closely with social, ethical, legal and policy experts to ensure that they meet the highest standards and that decisions are taken in the most legitimate and procedurally appropriate way. In consequence, any technological innovation, especially when it comes to preventing crime and improving public safety, must be accompanied by a rigorous and scientific assessment of its social impact in order to ensure a safe and just democratic society.

Appendix I

See Table 4

Table 4 Data extraction spreadsheet of steganalysis literature systematic review

General information				Steganalysis research meets the needs of society					Steganalysis research has positive impacts (benefits) on society		Steganalysis research does not have negative impacts (challenges) on society	
Reference	**Country**	**Field of publication**	**Research topic**	**Societal cybersecurity need(s) addressed**	**Research output**	**Description of tool(s)**	**Societal acceptance assessment**	**Threats addressed**	**Segment(s) of society benefitted**	**Identified societal positive impact(s)**	**Identified societal negative impact(s)**	**Mitigation/ minimisation measures**
Almeida, J. R., Fajarda, O., & Oliveira, J. L. (2020). File Forgery Detection Using a Weighted Rule-Based System. In A. Arampatzis et al. (Eds.), *Experimental IR Meets Multilinguality, Multimodality, and Interaction. CLEF 2020. Lecture Notes in Computer Science, vol 12260*, 85–96	Portugal Spain	Computing sciences, Security	Image forgeries detection	Justice (forensics)	Yes: tool developed	A weight rule-based system that assembles the different approaches used for forgery detection. The main solution is based on an orchestration of specialised rule-based models. For each model, a set of rules was defined with the purpose of identifying a specific file or message. Additionally, when there are insufficient rules to provide a good result, other complementary strategies have been combined, namely a random forest classifier	No	Criminal use of steganography, Crimes with digital evidence	Not specified	No	Not specified	No
Araujo, I. I., & Kazemian, H. (2020). Improving Steganographic capacity using distributed steganography over BMP. *Multimedia Tools and Applications, 79*(35–36), 26,181–26,195	United Kingdom	Multimedia development	Steganography, Digital content originality, Evidence in criminal courts and forensic laboratories	Ownership and authenticity of digital content, Data protection (cybersecurity)	Yes: tool developed	A steganographic method called DSoBMP-I (Distributed Steganography over BMP faze I) to improve the issues of low capacity, high detectability and distortion. The methodology consists of a new distributed steganographic approach to minimise the main weaknesses of today's methods, including Discrete Cosine Transform, where the capacity, detectability and distortion needs an upgrade to accommodate securer steganography for our data protection. The proposed prototype approach that evolved after a few experiments using the distributed steganographic method, where secrete data is secure into a set of BMP files (as it is proven more reliable), originates from a raw file that is not necessarily a BMP at the start. After applying a layer of encryption for extra security using two different methods such as RC4 & RSA, comparing the two encryption techniques for its agility and extra security to address the issue of low capacity and better security using the DSoBMP-I method, all deriving from the supplied image	No	Copyright violations, Cyberattacks	Specific segments: content owners	No	Not specified	No

Table 4 (continued)

General information				Steganalysis research meets the needs of society					Steganalysis research has positive impacts (benefits) on society		Steganalysis research does not have negative impacts (challenges) on society	
Reference	**Country**	**Field of publication**	**Research topic**	**Societal cybersecurity need(s) addressed**	**Research output**	**Description of tool(s)**	**Societal acceptance assessment**	**Threats addressed**	**Segment(s) of society benefitted**	**Identified societal positive impact(s)**	**Identified societal negative impact(s)**	**Mitigation/ minimisation measures**
Athanasiadou, E., Geradts, Z., & Van Eijk, E. (2018). Camera recognition with deep learning. *Forensic Sciences Research, 3*(3), 210–218	The Netherlands	Forensic sciences	Imaging device identification methods, Digital content originality, Evidence in criminal courts and forensic laboratories	Justice (forensics), Linkage of forensic investigations	No	N/A	N/A	Crimes with digital evidence	Not specified	No	Not specified	No
Aumayr, D., & Schöttle, P. (2022). U Can't (re)Touch This – A Deep Learning Approach for Detecting Image Retouching. In: S. Sclaroff, C. Distante, M. Leo, G. M. Farinella, F. Tombari. (Eds.), *Image Analysis and Processing – ICIAP 2022. ICIAP 2022. Lecture Notes in Computer Science, vol 13232*, 127–138	Austria	Computing sciences, Imaging techniques	Image forgeries detection	Ownership and authenticity of digital content	Yes: tool developed	A solution for an automatic recognition of image retouching. They adapt a well-known convolutional neural network (CNN) to the domain of RGB images and create a data set to train it. Specifically, they process 1000 images with nine different filters using Snapseed, an image editing app. Then, they use these 10,000 images in two different experiments to train the adapted CNN. The first experiment compares each single filter with the original images, while the second experiment tries to distinguish all ten classes at once	No	Fake images	Not specified	Yes: Psychological wellbeing of young people	Not specified	No

Table 4 (continued)

General information				Steganalysis research meets the needs of society					Steganalysis research has positive impacts (benefits) on society		Steganalysis research does not have negative impacts (challenges) on society	
Reference	**Country**	**Field of publication**	**Research topic**	**Societal cybersecurity need(s) addressed**	**Research output**	**Description of tool(s)**	**Societal acceptance assessment**	**Threats addressed**	**Segment(s) of society benefitted**	**Identified societal positive impact(s)**	**Identified societal negative impact(s)**	**Mitigation/ minimisation measures**
Bammey, Q., Grompone von Gioi, R., & Morel, J. M. (2020). An Adaptive Neural Network for Unsupervised Mosaic Consistency Analysis in Image Forensics. In *2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, 14182–14192	France	Computing sciences, Imaging techniques	Image forgeries detection	Ownership and authenticity of digital content	Yes: tool developed	A blind method that can train directly on unlabelled and potentially forged images to point out local mosaic inconsistencies. To this aim they designed a CNN structure inspired from demosaicing algorithms and directed at classifying image blocks by their position in the image modulo (2 × 2). Creating a diversified benchmark database using varied demosaicing methods, they explore the efficiency of the method and its ability to adapt quickly to any new data	No	Fake news Scientific misconduct	Not specified	No	Not specified	No
Bernacki, J., & Scherer, R. (2022). Digital forensics: a fast algorithm for a digital sensor identification. *Journal of Information and Telecommunication*, *6*(4), 399–419	Poland	Communications, Information sciences, Multimedia development	Imaging device identification methods, Digital content originality, Evidence in criminal courts and forensic laboratories	Justice (forensics), Linkage of forensic investigations, Ownership and authenticity of digital content	Yes: tool developed	MSE-DSI algorithm: a high-speed algorithm for the identification of imaging devices (models and brands) is proposed. A denoising filter is applied only to one colour channel of an RGB image. Only fragments of images of size 512 × 512 pixels are processed instead of the whole image	No	Crimes with digital evidence	Not specified	No	Not specified	No

Table 4 (continued)

General information				Steganalysis research meets the needs of society					Steganalysis research has positive impacts (benefits) on society		Steganalysis research does not have negative impacts (challenges) on society	
Reference	**Country**	**Field of publication**	**Research topic**	**Societal cybersecurity need(s) addressed**	**Research output**	**Description of tool(s)**	**Societal acceptance assessment**	**Threats addressed**	**Segment(s) of society benefitted**	**Identified societal positive impact(s)**	**Identified societal negative impact(s)**	**Mitigation/ minimisation measures**
Bertini, F., Sharma, R., & Montesi, D. (2022). Are Social Networks Watermarking Us or Are We (Unawarely) Watermarking Ourself? *Journal of Imaging, 8*(5), 132	Italy	Imaging techniques	Steganography and steganalysis, Imaging device identification methods, Digital content originality	Ownership and authenticity of digital content, Linkage of forensic investigation, Data protection (cybersecurity)	Yes: tool developed	A method based on the Photo-Response Non-Uniformity (PRNU) technique, which is usually used in digital forensic or image forgery detection activities, can be successfully used as a watermarking approach for authorship attribution and verification of pictures on social networks, successfully passing through different social networks, solving related problems such as profile linking and fake profile detection. It can help to address serious questions about privacy and security on social networks	No	Impersonation and fake profiles	Specific segments: social networks users; content owners	No	Not specified	No
Bobkowska, K., Nagaty, K., & Przyborski, M. (2019). Incorporating iris, fingerprint and face biometric for fraud prevention in e-passports using fuzzy vault. *IET Image Processing, 13*(13), 2516–2528	Poland Egypt	Imaging techniques	Steganography	Border control	Yes: tool developed	Fingerprint fuzzy vault (for coding and decoding biometric data): a type of crypto-biometrics where cryptography and biometrics are combined to achieve high security and user's convenience in the same time. Encoding is done on the basis of information that can be found in the fingerprints – the location of characteristic minutiae points. Positions of the first pixels, which contain information, are encrypted using the polynomial and then hidden in a vault of genuine and chaff points	No	Terrorism	Society in general	Yes: Protection of external borders	Not specified	No

Table 4 (continued)

General information				Steganalysis research meets the needs of society					Steganalysis research has positive impacts (benefits) on society		Steganalysis research does not have negative impacts (challenges) on society	
Reference	**Country**	**Field of publication**	**Research topic**	**Societal cybersecurity need(s) addressed**	**Research output**	**Description of tool(s)**	**Societal acceptance assessment**	**Threats addressed**	**Segment(s) of society benefitted**	**Identified societal positive impact(s)**	**Identified societal negative impact(s)**	**Mitigation/ minimisation measures**
Bortolameotti, R., van Ede, T., Caselli, M., Everts, M. H., Hartel, P., Hofstede, R., Jonker, W., & Peter, A. (2017). DECANTeR: DEteCtion of Anomalous outbouND HTTP TRaffic by Passive Application Fingerprinting. In *ACSAC '17 Proceedings of the 33rd Annual Computer Security Applications Conference*, 373–386	The Netherlands	Computer sciences, Security	Stegomalware or covert channels detection	Data protection (cybersecurity)	Yes: tool developed	DECANTeR: a system that uses a passive application fingerprinting technique to model benign traffic only, and hence not relying on any malicious sample. For each monitored host, it passively generates fingerprints for each application communicating from the host. The fingerprints are composed of different HTTP request features that describe the network behavior of an application. The solution uses a hybrid approach, since the set of features for fingerprints is dynamically adapted to the type of the application, and the content of the features represents static patterns extracted from the traffic	No	Cyberattacks	Not specified	No	Not specified	No
Cabaj, K., Caviglione, L., Mazurczyk, W., Wendzel, S., Woodward, A., & Zander, S. (2018). The New Threats of Information Hiding: The Road Ahead. *IT Professional, 20*(3), 31–39	Poland Italy Germany United Kingdom Australia	Technology	Review of stegomalware and its detection	Data protection (cybersecurity)	No	N/A	N/A	Cyberattacks	Not specified	No	Not specified	No

Table 4 (continued)

General information				Steganalysis research meets the needs of society					Steganalysis research has positive impacts (benefits) on society		Steganalysis research does not have negative impacts (challenges) on society	
Reference	**Country**	**Field of publication**	**Research topic**	**Societal cybersecurity need(s) addressed**	**Research output**	**Description of tool(s)**	**Societal acceptance assessment**	**Threats addressed**	**Segment(s) of society benefitted**	**Identified societal positive impact(s)**	**Identified societal negative impact(s)**	**Mitigation/ minimisation measures**
Cardamone, N., & d'Amore, F. (2019). DWT and QR Code Based Watermarking for Document DRM. In C. Yoo, Y. Q. Shi, H. Kim, A. Piva, G. Kim (Eds.), *Digital Forensics and Watermarking. IWDW 2018. Lecture Notes in Computer Science, vol 11378*, 137–150	Italy	Forensic sciences, Multimedia development	Digital content originality	Data protection (cybersecurity)	Yes: tool developed	A digital rights protection scheme for every type of document presented as an image, by using steps that use cryptography and watermarking. The watermarked version contains a QR code that is repeatedly inserted, and scrambled, by the document rights owner, into the frequency components of the image, thus producing the watermarked image. The QR code contains a signed ID that uniquely identifies every users using the system. The schema, a non-blind type, achieves good perceptive quality and fair robustness using the third level of the Discrete Wavelet Transform	No	Privacy leakages	Specific segment: big companies	No	Not specified	No
Casino, F., Dasaklis, T. K., Spathoulas, G. P., Anagnostopoulos, M., Ghosal, A., Borocz, I., Solanas, A., Conti, M., & Patsakis, C. (2022). Research Trends, Challenges, and Emerging Topics in Digital Forensics: A Review of Reviews. *IEEE Access, 10*, 25464–25493	Spain Greece Norway Denmark Ireland Belgium Italy The Netherlands	Technology	Review of digital forensics challenges	Justice (forensics)	Yes: tools collected	Image and video steganalysis, JPEG carving, hyperspectral image, noise affectation, deep learning techniques, video forgery detection, video surveillance analysis, video content authentication, etc	No	Crimes with digital evidence	Society in general	Yes: Human rights (ethics and protection of personal data), Cross-border cooperation, Sustainable development, Public accountability and transparency Strict observance of international law (chain of custody)	Yes: privacy and data protection	Yes: European law, Confidentiality case levels, Confidentiality agreements, Data storage, protection and processing guidelines, Gathering and use of evidence rules, "Responsible encryption"

Table 4 (continued)

General information				Steganalysis research meets the needs of society					Steganalysis research has positive impacts (benefits) on society		Steganalysis research does not have negative impacts (challenges) on society	
Reference	**Country**	**Field of publication**	**Research topic**	**Societal cybersecurity need(s) addressed**	**Research output**	**Description of tool(s)**	**Societal acceptance assessment**	**Threats addressed**	**Segment(s) of society benefitted**	**Identified societal positive impact(s)**	**Identified societal negative impact(s)**	**Mitigation/ minimisation measures**
Castillo-Camacho, I., & Wang, K. (2021). Data-Dependent Scaling of CNN's First Layer for Improved Image Manipulation Detection. In: X. Zhao, Y. Q. Shi, A. Piva, H. J. Kim (Eds.), *Digital Forensics and Watermarking. IWDW 2020. Lecture Notes in Computer Science, vol 12617*, 208–223	France	Forensic sciences, Multimedia development	Image forgeries detection	Ownership and authenticity of digital content	Yes: tool developed	A simple and practical method for adjusting the CNN's first layer, based on a proper scaling of first-layer filters with a data-dependent approach. The key idea is to keep the stability of the variance of data flow in a CNN. The proposed method can cope well with different first-layer initialization algorithms and different CNN architectures	No	Fake images	Not specified	No	Not specified	No
Caviglione, L., & Mazurczyk, W. (2022). Never Mind the Malware, Here's the Stegomalware. *IEEE Security & Privacy, 20*(5), 101–106	Italy Poland	Technology, Information sciences, Security	Review of stegomalware and its detection	Data protection (cybersecurity)	No	N/A	N/A	Cyberattacks	Not specified	No	Not specified	No

Table 4 (continued)

General information				Steganalysis research meets the needs of society					Steganalysis research has positive impacts (benefits) on society		Steganalysis research does not have negative impacts (challenges) on society	
Reference	**Country**	**Field of publication**	**Research topic**	**Societal cybersecurity need(s) addressed**	**Research output**	**Description of tool(s)**	**Societal acceptance assessment**	**Threats addressed**	**Segment(s) of society benefitted**	**Identified societal positive impact(s)**	**Identified societal negative impact(s)**	**Mitigation/ minimisation measures**
Caviglione, L., Choras, M., Corona, I., Janicki, A., Mazurczyk, W., Pawlicki, M., & Wasielewska, K. (2021a). Tight Arms Race: Overview of Current Malware Threats and Trends in Their Detection. *IEEE Access, 9*, 5371–5396	Italy Germany Poland	Technology	Review of stegomalware and its detection	Data protection (cybersecurity)	No	N/A	N/A	Cyberattacks	Not specified	Yes: Public accountability and transparency	Not specified	No
Caviglione, L., Mazurczyk, W., Repetto, M., Schaffhauser, A., & Zuppelli, M. (2021b). Kernel-level tracing for detecting stegomalware and covert channels in Linux environments. *Computer Networks, 191*, 108010	Italy Poland Germany	Communications, Computing sciences	Stegomalware or covert channels detection	Data protection (cybersecurity)	Yes: tool developed	The extended Berkeley Packet Filter (eBPF), a recent code augmentation feature provided by the Linux kernel, is leveraged for detecting stegomalware. Two realistic use cases are investigated implementing different attack mechanisms, i.e., two processes colluding via the alteration of the file system and hidden network communication attempts nested within IPv6 traffic flows	No	Cyberattacks	Not specified	No	Not specified	No

Table 4 (continued)

General information				Steganalysis research meets the needs of society					Steganalysis research has positive impacts (benefits) on society		Steganalysis research does not have negative impacts (challenges) on society	
Reference	**Country**	**Field of publication**	**Research topic**	**Societal cybersecurity need(s) addressed**	**Research output**	**Description of tool(s)**	**Societal acceptance assessment**	**Threats addressed**	**Segment(s) of society benefitted**	**Identified societal positive impact(s)**	**Identified societal negative impact(s)**	**Mitigation/ minimisation measures**
Caviglione, L., Wendzel, S., & Mazurczyk, W. (2017). The Future of Digital Forensics: Challenges and the Road Ahead. *IEEE Security & Privacy, 15*(6), 12–17	Italy Germany Poland	Technology, Information sciences, Security	Review of digital forensics challenges	Justice (forensics)	No	N/A	N/A	Crimes with digital evidence, Criminal use of steganography	Society in general	Yes: Human rights (ethics and protection of personal data), Cross-border cooperation, Strict observance of international, law (chain of custody)	Not specified	No
Chang, C. C. (2021). Cryptospace Invertible Steganography with Conditional Generative Adversarial Networks. *Security and Communication Networks, 2021*, 1–14	United Kingdom	Technology, Information sciences, Security	Steganography, Digital content originality	Data protection (cybersecurity), Ownership and authenticity of digital content	Yes: tool developed	They introduced generative adversarial networks to cryptospace invertible steganography. They validated the effectiveness of the RCGAN for learning structural information of bit-planes and generating realistic ones in a top-down manner. In addition, they analysed the performance of spatial, spectral, and structural discrimination functions and demonstrated the superiority of deep neural networks over traditional handcrafted analytics. Furthermore, they showed that the applied encryption scheme for digital images satisfies semantic and statistical perfect secrecy	No	Cyberattacks	Not specified	No	Not specified	No
Chang, C. C. (2022). Automation of reversible steganographic coding with nonlinear discrete optimisation. *Connection Science, 34*(1), 1719–1735	United Kingdom	Other	Steganography, Digital content originality, Evidence in criminal courts and forensic laboratories	Data protection (cybersecurity), Ownership and authenticity of digital content	Yes: tool developed	A reversible steganographic coding as a nonlinear discrete optimisation problem with a logarithmic capacity constraint and a quadratic distortion objective. Linearisation techniques are developed to enable iterative mixed-integer linear programming. Experimental results validate the near-optimality of the proposed optimisation algorithm when benchmarked against a brute-force method	No	Cyberattacks	Not specified	No	Not specified	No

Table 4 (continued)

General information				Steganalysis research meets the needs of society					Steganalysis research has positive impacts (benefits) on society		Steganalysis research does not have negative impacts (challenges) on society	
Reference	**Country**	**Field of publication**	**Research topic**	**Societal cybersecurity need(s) addressed**	**Research output**	**Description of tool(s)**	**Societal acceptance assessment**	**Threats addressed**	**Segment(s) of society benefitted**	**Identified societal positive impact(s)**	**Identified societal negative impact(s)**	**Mitigation/ minimisation measures**
Chang, C. C., Li, C. T., & Chen, K. (2019). Privacy-Preserving Reversible Information Hiding Based on Arithmetic of Quadratic Residues. *IEEE Access, 7*, 54117–54132	United Kingdom Australia China	Technology	Steganography, Evidence in criminal courts and forensic laboratories	Data protection (cybersecurity)	Yes: tool developed	A privacy-preserving reversible information hiding scheme inspired by the mathematical concept of quadratic residues. A quadratic residue has four (not necessarily distinct) square roots, which enables payloads to be encoded in a dynamic fashion. Furthermore, a predictive model based upon the projection theorem is devised to assist carrier signal recovery	No	Cyberattacks	Not specified	No	Not specified	No
Cozzolino, D., Marra, F., Gragnaniello, D., Poggi, G., & Verdoliva, L. (2020). Combining PRNU and noiseprint for robust and efficient device source identification. *EURASIP Journal on Information Security, 2020*(1)	Italy	Technology, Information sciences, Security	Imaging device identification methods, Digital content originality, Evidence in criminal courts and forensic laboratories	Justice (forensics), Linkage of forensic investigations, Ownership and authenticity of digital content	Yes: tool developed	Improved PRNU-based image processing by leveraging the image noiseprint, a recently proposed camera-model fingerprint. Assuming to know the camera model of the image to analyse, the search for the source device can be restricted only to devices of the same model, thereby reducing the risk of wrong identification, especially in the most critical cases. However, in real-world scenarios, camera models may not be known in advance, calling for a preliminary model identification phase, which is itself prone to errors. Therefore, with the hierarchical procedure outlined before, there is the non-negligible risk of excluding right away the correct device. For this reason, it is preferred to exploit the two pieces of information jointly, rather than hierarchically, by suitably combining the two distances	No	Crimes with digital evidence	Not specified	No	Not specified	No

Table 4 (continued)

General information				Steganalysis research meets the needs of society					Steganalysis research has positive impacts (benefits) on society		Steganalysis research does not have negative impacts (challenges) on society	
Reference	**Country**	**Field of publication**	**Research topic**	**Societal cybersecurity need(s) addressed**	**Research output**	**Description of tool(s)**	**Societal acceptance assessment**	**Threats addressed**	**Segment(s) of society benefitted**	**Identified societal positive impact(s)**	**Identified societal negative impact(s)**	**Mitigation/ minimisation measures**
Crișan, D., Irimia, A., Gota, D., Miclea, L., Puscasiu, A., Stan, O., & Valean, H. (2021). Analyzing Benford's Law's Powerful Applications in Image Forensics. *Applied Sciences, 11*(23), 1148	Romania	Other	Steganography, Digital content originality, Evidence in criminal courts and forensic laboratories	Justice (forensics), Ownership and authenticity of digital content	Yes: tool developed	Based on the Newcomb-Benford law and using the image's luminance channel and JPEG coefficients, a technique is described for determining the quality factor with which a JPEG image is compressed, which could be applicable to any procedure that involves the analysis of digital images and in which it is strongly suggested that the image authenticity be verified prior to beginning the analysing process	No	Crimes with digital evidence	Not specified	No	Not specified	No
Darmet, L., Wang, K., & Cayre, F. (2020). Weakly Supervised Adaptation to Re-sizing for Image Manipulation Detection on Small Patches. In: H. Wang, X. Zhao, Y. Shi, H. Kim, A. Piva (Eds.), *Digital Forensics and Watermarking. IWDW 2019. Lecture Notes in Computer Science, vol 12022*, 99–114	France	Forensic sciences, Multimedia development	Image forgeries detection	Ownership and authenticity of digital content	Yes: tool developed	A simple weakly-supervised (making use of around 2000 labelled patches) adaptation method to re-sized testing samples for image forgery detection. A method to adapt both GMM-based feature extractor, by adjusting weights, and DNN classifier, by fine-tuning	No	Fake images	Not specified	No	Not specified	No

Table 4 (continued)

General information				Steganalysis research meets the needs of society					Steganalysis research has positive impacts (benefits) on society		Steganalysis research does not have negative impacts (challenges) on society	
Reference	**Country**	**Field of publication**	**Research topic**	**Societal cybersecurity need(s) addressed**	**Research output**	**Description of tool(s)**	**Societal acceptance assessment**	**Threats addressed**	**Segment(s) of society benefitted**	**Identified societal positive impact(s)**	**Identified societal negative impact(s)**	**Mitigation/ minimisation measures**
Djebbar, F. (2021). Securing IoT Data Using Steganography: A Practical Implementation Approach. *Electronics, 10*(21), 2707	Sweden	Electronics	Steganography	Data protection (cybersecurity)	Yes: tool developed	An audio, noise-resilient, low-overhead, lightweight steganography solution adequate for use in the IoT environment. The accuracy of hidden data is tested against corruption using multiple modulations and coding schemes (MCSs). Additive white Gaussian noise (AWGN) is added to the modulated data to simulate the noisy channel as well as several wireless technologies such as cellular, WiFi, and vehicular communications that are used between communicating IoT devices	No	Cyberattacks	Not specified	No	Not specified	No
Douglas, M., Bailey, K., Leeney, M., & Curran, K. (2017). An overview of steganography techniques applied to the protection of biometric data. *Multimedia Tools and Applications, 77*(13), 17333–17373	Ireland	Multimedia development	Review of steganography techniques	Data protection (cybersecurity)	Yes: tools collected	Visual attack, structural, statistical (chi-squared test/pairs of values, extended chi-squared attack, regular singular steganalysis), blind (JPEG calibration)	No	Cyberattacks, Privacy leakages	Society in general	No	Not specified	No
Fernández-Menduiña, S., & Pérez-González, F. (2021). On the information leakage quantification of camera fingerprint estimates. *EURASIP Journal on Information Security*, 2021 (6)	United Kingdom Spain	Technology, Information sciences, Security	Imaging device identification methods	Privacy of criminal investigations sensitive data	No	N/A	N/A	Privacy leakages	Specific segments: victims	Yes: Protection of the rights of the child	Not specified	No

Table 4 (continued)

General information				Steganalysis research meets the needs of society					Steganalysis research has positive impacts (benefits) on society		Steganalysis research does not have negative impacts (challenges) on society	
Reference	**Country**	**Field of publication**	**Research topic**	**Societal cybersecurity need(s) addressed**	**Research output**	**Description of tool(s)**	**Societal acceptance assessment**	**Threats addressed**	**Segment(s) of society benefitted**	**Identified societal positive impact(s)**	**Identified societal negative impact(s)**	**Mitigation/ minimisation measures**
Frattolillo, F. (2022). Digital Copyright Protection: Focus on Some Relevant Solutions. *International Journal of Communication Networks and Information Security, 9*(2), 282–293	Italy	Technology, Information sciences, Security	Digital content originality	Ownership and authenticity of digital content	Yes: tools collected	Solutions to the problem of copyright protection based on DRM systems (HTML5, EME, CENC, CDMs), and watermarking protocols (TTP-Free, Client-Side Embedding, Buyer-Friendly)	No	Copyright violations	Specific segments: content owners	No	Not specified	No
Frick, R. A., Liu, H., & Steinebach, M. (2020). Detecting Double Compression and Splicing using Benfords First Digit Law. In ARES´20 Proceedings of the 15th International Conference on Availability, Reliability and Security, (47)	Germany	Technology, Security	Image forgeries detection	Ownership and authenticity of digital content	Yes: tool developed	A passive forensic detection framework to detect image manipulations based on compression artefacts and Benford's First Digit Law. It incorporates a supervised approach to reconstruct the compression history as well as provides an unsupervised detection approach to detect double compression for unknown quantization tables	No	Fake news	Not specified	No	Not specified	No

Table 4 (continued)

General information				Steganalysis research meets the needs of society					Steganalysis research has positive impacts (benefits) on society		Steganalysis research does not have negative impacts (challenges) on society	
Reference	**Country**	**Field of publication**	**Research topic**	**Societal cybersecurity need(s) addressed**	**Research output**	**Description of tool(s)**	**Societal acceptance assessment**	**Threats addressed**	**Segment(s) of society benefitted**	**Identified societal positive impact(s)**	**Identified societal negative impact(s)**	**Mitigation/ minimisation measures**
Ghanmi, N., Nabli, C., & Awal, A. M. (2021). CheckSim: A Reference-Based Identity Document Verification by Image Similarity Measure. In E. H. Barney Smith, U. Pal (Eds.), *Document Analysis and Recognition – ICDAR 2021 Workshops. ICDAR 2021. Lecture Notes in Computer Science, vol 12916*, 422–436	France	Imaging techniques	Image forgeries detection	Ownership and authenticity of digital content, Data protection (cybersecurity), Public security (cybersecurity)	Yes: tool developed	CheckSim: a generic deep-learning based framework for identity document verification, based on two particular architectures of CNN models	No	Terrorism, Money laundering Fraudulent documents	Not specified	Yes: Mitigate economic risks	Not specified	No

Table 4 (continued)

General information				Steganalysis research meets the needs of society					Steganalysis research has positive impacts (benefits) on society		Steganalysis research does not have negative impacts (challenges) on society	
Reference	**Country**	**Field of publication**	**Research topic**	**Societal cybersecurity need(s) addressed**	**Research output**	**Description of tool(s)**	**Societal acceptance assessment**	**Threats addressed**	**Segment(s) of society benefitted**	**Identified societal positive impact(s)**	**Identified societal negative impact(s)**	**Mitigation/ minimisation measures**
Göbel, T., & Baier, H. (2018). Anti-Forensic Capacity and Detection Rating of Hidden Data in the Ext4 Filesystem. In G. Peterson, S. Shenoi (Eds.), *Advances in Digital Forensics XIV. DigitalForensics 2018. IFIP Advances in Information and Communication Technology, vol 532*, 87–110	Germany	Forensic sciences	Evidence in criminal courts and forensics laboratories	Justice (forensics)	Yes: tools collected	17 data hiding techniques in ext4 filesystems (File and Directory Slack Space, Null Directory Entries, Partition Boot Sector, Superblock, Block Bitmap, Inode Bitmap, Groy Descriptor Table…) are tested against forensic tools to evaluate capacity and detection rating	No	Criminal use of steganography, Crimes with digital evidence	Specific segment: digital forensic community	No	Not specified	No

Table 4 (continued)

General information				Steganalysis research meets the needs of society					Steganalysis research has positive impacts (benefits) on society		Steganalysis research does not have negative impacts (challenges) on society	
Reference	**Country**	**Field of publication**	**Research topic**	**Societal cybersecurity need(s) addressed**	**Research output**	**Description of tool(s)**	**Societal acceptance assessment**	**Threats addressed**	**Segment(s) of society benefitted**	**Identified societal positive impact(s)**	**Identified societal negative impact(s)**	**Mitigation/ minimisation measures**
Göbel, T., & Baier, H. (2019). Fishy – A Framework for Implementing Filesystem-Based Data Hiding Techniques. In F. Breitinger, I. Baggili (Eds.), *Digital Forensics and Cyber Crime. ICDF2C 2018. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol 259*, 23–42	Germany	Computing sciences, Security, Forensic sciences	Steganography	Justice (forensics)	Yes: tool developed	Fishy: a framework designed to implement and analyse different filesystem-based data hiding techniques. Fishy is implemented in Python and collects various common exploitation methods that make use of existing data structures on the filesystem layer	No	Crimes with digital evidence, Criminal use of steganography	Specific segment: digital forensic community	No	Not specified	No
Gragnaniello, D., Marra, F., Poggi, G., & Verdoliva, L. (2018). Analysis of Adversarial Attacks against CNN-based Image Forgery Detectors. In *2018 26th European Signal Processing Conference (EUSIPCO)*, 967–971	Italy	Other	Image forgeries detection	Ownership and authenticity of digital content	Yes: tools collected	CNN-based detectors of image manipulation: SPAM + SVM, convolutional neural networks (CNN), very deep nets (Xception)…	No	Fake news	Society in general	No	Not specified	No

Table 4 (continued)

General information				Steganalysis research meets the needs of society					Steganalysis research has positive impacts (benefits) on society		Steganalysis research does not have negative impacts (challenges) on society	
Reference	**Country**	**Field of publication**	**Research topic**	**Societal cybersecurity need(s) addressed**	**Research output**	**Description of tool(s)**	**Societal acceptance assessment**	**Threats addressed**	**Segment(s) of society benefitted**	**Identified societal positive impact(s)**	**Identified societal negative impact(s)**	**Mitigation/ minimisation measures**
Hegarty, M. T., & Keane, A. J. (2020). Modern Techniques for Discovering Digital Steganography. In *21st European Conference on Cyber Warfare and Security*	Ireland	Computing sciences, Security	Steganalysis, Stegomalware or covert channels detection	Justice (forensics)	Yes: tool developed	Least Significant Bit (LSB) Steganography using Convolutional Neural Networks (CNN) for image classification. The CNN algorithm was trained using datasets of images (some from the DarkWeb) with known steganography and then applied to datasets with images to identify concealed data	No	Criminal use of steganography	Not specified	No	Not specified	No
Johnson, C. & Davies, R. (2020) Using Digital Forensic Techniques to Identify Contract Cheating: A Case Study. *J Acad Ethics 18*, 105–113	United Kingdom	Ethics	Digital content originality	Ownership and authenticity of digital content	No	N/A	N/A	Contract cheating	Specific segments: academic staff	No	Not specified	No
Kanwal, N., Asghar, M. N., Ansari, M. S., Fleury, M., Lee, B., Herbst, M., & Qiao, Y. (2020). Preserving Chain-of-Evidence in Surveillance Videos for Authentication and Trust-Enabled Sharing. *IEEE Access, 8*, 153413–153424	Ireland Pakistan United Kingdom	Technology	Steganography, Digital content originality, Evidence in criminal courts and forensic laboratories	Ownership and authenticity of digital content	Yes: tool developed	A computationally inexpensive method of preserving a chain-of-evidence in surveillance videos by means of hashing and steganography. Encryption keys are stored in a hardware wallet independently of the video capture device itself, while evidential information is stored steganographically within video frames themselves, independently of the content. Added protection is provided by hiding information within the two least-valued of pixel bitplanes, using a newly introduced technique that randomizes the pixel storage locations on a per video frame and video-capture device basis	No	Tampering of evidence	Not specified	Yes: Human rights (ethics and protection of personal data), Strict observance of international law (chain of custody)	Not specified	Yes: European law

Table 4 (continued)

General information				Steganalysis research meets the needs of society					Steganalysis research has positive impacts (benefits) on society		Steganalysis research does not have negative impacts (challenges) on society	
Reference	**Country**	**Field of publication**	**Research topic**	**Societal cybersecurity need(s) addressed**	**Research output**	**Description of tool(s)**	**Societal acceptance assessment**	**Threats addressed**	**Segment(s) of society benefitted**	**Identified societal positive impact(s)**	**Identified societal negative impact(s)**	**Mitigation/ minimisation measures**
Karampidis, K., Kavallieratou, E., & Papadourakis, G. (2018). A review of image steganalysis techniques for digital forensics. *Journal of Information Security and Applications, 40*, 217–235	Greece	Technology, Information sciences, Security	Review of steganalysis techniques	Justice (forensics)	Yes: tools collected	Visual (Least Significant Bit), signature (Discrete Cosine Transform), statistical (Pairs of Values, Raw Quick Pair, RS, image quality metrics, GEFR, Pairs Analysis, DIH…), spread spectrum (Histogram Characteristic Function, blocked based scatter difference detection…), transform domain (wavelet domain quantization modulation technique, QIM…), universal or blind (wavelet-like decomposition, CUSUM, local binary pattern texture operator, co-ocurrence matrix of differential image, GLCM matrix properties, sparse representation, CNN, Steganography Pattern Discovery, deep residual network…)	No	Crimes with digital evidence, Criminal use of steganography	Not specified	No	Not specified	No
Keller, J., & Wendzel, S. (2021). Reversible and Plausibly Deniable Covert Channels in One-Time Passwords Based on Hash Chains. *Applied Sciences, 11*(2), 731	Germany	Other	Covert channels	Data protection (cybersecurity)	Yes: tool developed	A covert channel between two devices where one device authenticates itself with Lamport's onetime passwords based on a cryptographic hash function. This channel enables plausible deniability jointly with reversibility and is applicable in different contexts, such as traditional TCP/IP networks, CPS/IoT communication, blockchain-driven systems and local interprocess communications that apply hash chains. Countermeasures are also described to detect the presence of such a covert channel, which are non-trivial because hash values are random-looking binary strings, so that deviations are not likely to be detected	No	Criminal use of steganography	Not specified	No	Not specified	No

Table 4 (continued)

General information				Steganalysis research meets the needs of society					Steganalysis research has positive impacts (benefits) on society		Steganalysis research does not have negative impacts (challenges) on society	
Reference	**Country**	**Field of publication**	**Research topic**	**Societal cybersecurity need(s) addressed**	**Research output**	**Description of tool(s)**	**Societal acceptance assessment**	**Threats addressed**	**Segment(s) of society benefitted**	**Identified societal positive impact(s)**	**Identified societal negative impact(s)**	**Mitigation/ minimisation measures**
Kilts, S., Altschaffel, R., & Dittman, J. (2022). Hidden in Plain Sight – Persistent Alternative Mass Storage Data Streams as a Means for Data Hiding With the Help of UEFI NVRAM and Implications for IT Forensics. In *IH&MMSec ´22 Proceedings of the 2022 ACM Workshop on Information Hiding and Multimedia Security*, 107–112	Germany	Information sciences, Security	Steganography and steganalysis	Data protection (cybersecurity), Justice (forensics)	Yes: tool developed	A proof of concept to embed in and retrieve from media data within UEFI NVRAM, a storage channel largely ignored by forensics at present. It is evaluated using 10 different computer systems with 10 successful cases	No	Cyberattacks	Not specified	No	Not specified	No

Table 4 (continued)

General information				Steganalysis research meets the needs of society					Steganalysis research has positive impacts (benefits) on society		Steganalysis research does not have negative impacts (challenges) on society	
Reference	**Country**	**Field of publication**	**Research topic**	**Societal cybersecurity need(s) addressed**	**Research output**	**Description of tool(s)**	**Societal acceptance assessment**	**Threats addressed**	**Segment(s) of society benefitted**	**Identified societal positive impact(s)**	**Identified societal negative impact(s)**	**Mitigation/ minimisation measures**
Kuppa, A., Grzonkowski, S., & Le-Khac, N. A. (2018). Enabling Trust in Deep Learning Models: A Digital Forensics Case Study. In *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/ BigDataSE)*, 1250–1255	Ireland	Security, Computing sciences	Evidence in criminal courts and forensics laboratories	Justice (forensics)	Yes: tool developed	ATF: a domain-independent framework for systematically testing security robustness of black-box DNN with varying threat models and adversary goals. They introduced a new method, Feature Influence Calculator, for bypassing black-box DNN. They tested ATF with a DNN tool used in digital forensics operating in constraint settings	No	Criminal use of steganography, Crimes with digital evidence	Not specified	No	Not specified	No
Li, Z., Liu, F., & Bors, A. G. (2018). 3D Steganalysis Using Laplacian Smoothing at Various Levels. In X. Sun, Z. Pan, E. Bertino. (Eds.), *Cloud Computing and Security. ICCCS 2018. Lecture Notes in Computer Science, vol 11068*, 223–232	United Kingdom China	Computing sciences, Security	Steganography and steganalysis, Stegomalware or covert channels detection	Public security (cybersecurity)	Yes: tool developed	They propose to combine the 3D steganalytic feature sets obtained from considering various degrees of Laplacian smoothing as the input into the steganalysers. The level of the Laplacian smoothing is controlled by two parameters: the scale factor, λ, and the number of iterations of the smoothing, k. During the experiments undertaken in this research study, they have combined the LFS76 feature sets based on the Laplacian smoothing at various levels. The steganalyser trained over the combined feature set showed better performance than any of the individual LFS76 feature set, for the steganalysis of three embedding algorithms	No	Criminal use of steganography, Terrorism	Not specified	No	Not specified	No

Table 4 (continued)

General information				Steganalysis research meets the needs of society					Steganalysis research has positive impacts (benefits) on society		Steganalysis research does not have negative impacts (challenges) on society	
Reference	**Country**	**Field of publication**	**Research topic**	**Societal cybersecurity need(s) addressed**	**Research output**	**Description of tool(s)**	**Societal acceptance assessment**	**Threats addressed**	**Segment(s) of society benefitted**	**Identified societal positive impact(s)**	**Identified societal negative impact(s)**	**Mitigation/ minimisation measures**
Martínez-Tornés, B., Boros, E., Doucet, A., Gomez-Krämer, P., Ogier, J. M., & d'Andecy, V. P. (2023). Knowledge-Based Techniques for Document Fraud Detection: A Comprehensive Study. In A. Gelbukh. (Ed.), *Computational Linguistics and Intelligent Text Processing. CICLing 2019. Lecture Notes in Computer Science, vol 13,451*, 17–33	France	Technology, Computing sciences, Information sciences	Image forgeries detection	Data protection (cybersecurity), Ownership and authenticity of digital content	Yes: tools collected	Knowledge-based fact-checking techniques for document fraud detection: matrix factorization models (RESCAL, ComplEX, QuatE, SimplE, TuckER, HolE), geometric models (Structured Embedding, TransE, TransH, TransR, TransD, CrossE, RotatE, MurE, KG2E), and deep learning models (ConveE, ERMLP, ProjE)	No	Fraudulent documents	Not specified	No	Not specified	No
Mazurczyk, W., Wendzel, S., Chourib, M., & Keller, J. (2019). Countering adaptive network covert communication with dynamic wardens. *Future Generation Computer Systems, 94*, 712–725	Poland Germany	Computing sciences	Covert channels	Data protection (cybersecurity)	Yes: tool developed	Dynamic wardens: modification of the warden's behaviour over time, making it difficult for the adaptive covert communication parties to infer its strategy and perform a successful hidden data exchange	No	Cyberattacks	Society in general	No	Not specified	No

Table 4 (continued)

General information				Steganalysis research meets the needs of society					Steganalysis research has positive impacts (benefits) on society		Steganalysis research does not have negative impacts (challenges) on society	
Reference	**Country**	**Field of publication**	**Research topic**	**Societal cybersecurity need(s) addressed**	**Research output**	**Description of tool(s)**	**Societal acceptance assessment**	**Threats addressed**	**Segment(s) of society benefitted**	**Identified societal positive impact(s)**	**Identified societal negative impact(s)**	**Mitigation/ minimisation measures**
Meden, B., Rot, P., Terhorst, P., Damer, N., Kuijper, A., Scheirer, W. J., Ross, A., Peer, P., & Struc, V. (2021). Privacy–Enhancing Face Biometrics: A Comprehensive Survey. *IEEE Transactions on Information Forensics and Security*, 16, 4147–4183	Slovenia Germany United States of America	Forensic sciences, Information sciences, Security	Steganography	Data protection (cybersecurity)	Yes: tools collected	Biometric privacy–enhancing techniques: image-level techniques (obfuscation, adversarial, synthesis), representation-level techniques (transformation-based, elimination-based, homomorphic encryption), inference-level techniques (NFR, PE-MIU)	No	Cyberattacks, Privacy leakages	Not specified	Yes: Human rights (ethics and protection of personal data)	Not specified	No
Neuner, S., Voyiatzis, A., Schmiedecker, M., & Weippl, E. R. (2017). Timestamp hiccups: Detecting manipulated filesystem timestamps on NTFS. In ARES´17 Proceedings of the 12th International Conference on Availability, Reliability and Security, (33)	Austria	Computing sciences, Security	Steganography and steganalysis, Evidence in criminal courts and forensics laboratories	Justice (forensics)	Yes: tools collected	They evaluate the steganographic capabilities of TOMS channels and propose techniques to aid digital forensic investigations: storage technology and scripted creation, regular use of the filesystem, enterprise environment	No	Criminal use of steganography	Not specified	No	Not specified	No

Table 4 (continued)

General information				Steganalysis research meets the needs of society					Steganalysis research has positive impacts (benefits) on society		Steganalysis research does not have negative impacts (challenges) on society	
Reference	**Country**	**Field of publication**	**Research topic**	**Societal cybersecurity need(s) addressed**	**Research output**	**Description of tool(s)**	**Societal acceptance assessment**	**Threats addressed**	**Segment(s) of society benefitted**	**Identified societal positive impact(s)**	**Identified societal negative impact(s)**	**Mitigation/ minimisation measures**
Odebade, A., Welsh, T., Mthunzi, S., & Benkhelifa, E. (2017). Mitigating Anti-forensics in the Cloud via Resource-Based Privacy Preserving Activity Attribution. In *2017 Fourth International Conference on Software Defined Systems*, 143–149	United Kingdom	Computing sciences	Evidence in criminal courts and forensics laboratories	Justice (forensics), Data protection (cybersecurity),	Yes: tool developed	An architecture agnostic, privacy-preserving solution to reducing the digital forensics target search space of a investigation within cloud and edge computing environments which will leverage standard metering and network logs for efficient activity attribution. A solution was proposed to efficiently search for forensic evidence in anti-forensic data within cloud and edge computing environments. A case scenario was considered in which a forensic investigation attributed to a multi-tenant edge cloud aims to streamline the number of target VMs without compromising the privacy of non-target VMs, whilst minimising resource intensive work	No	Criminal use of steganography, Crimes with digital evidence	Not specified	Yes: Human rights (ethics and protection of personal data)	Yes: privacy and data protection	Yes: Legal and ethical requirements of cloud-service-providers (CSP) to preserve privacy of non-suspects
Peng, J., & Tang, S. (2021). Covert Communication Over VoIP Streaming Media With Dynamic Key Distribution and Authentication. *IEEE Transactions on Industrial Electronics, 68*(4), 3619–3628	United Kingdom	Other	Covert channels	Data protection (cybersecurity)	Yes: tool developed	A new dynamic steganographic algorithm is devised for the covert VoIP communications. It includes one-way accumulation integrating into dynamic key updating and exchange, which can protect steganographic systems from man-in-the-middle attacks, which threaten covert steganographic communications	No	Cyberattacks	Not specified	No	Not specified	No

Table 4 (continued)

General information				Steganalysis research meets the needs of society					Steganalysis research has positive impacts (benefits) on society		Steganalysis research does not have negative impacts (challenges) on society	
Reference	**Country**	**Field of publication**	**Research topic**	**Societal cybersecurity need(s) addressed**	**Research output**	**Description of tool(s)**	**Societal acceptance assessment**	**Threats addressed**	**Segment(s) of society benefitted**	**Identified societal positive impact(s)**	**Identified societal negative impact(s)**	**Mitigation/ minimisation measures**
Phan-Ho, A. T., & Retraint, F. (2022). A Comparative Study of Bayesian and Dempster-Shafer Fusion on Image Forgery Detection. *IEEE Access, 10*, 99268–99281	France	Technology	Digital content originality, Evidence in criminal courts and forensic laboratories	Justice (forensics), Ownership and authenticity of digital content	Yes: tool developed	Two fusion techniques are proposed, Bayesian and Dempster-Shafer theory-based fusion, for tampering detection applications. Two fusion scenarios have been considered and experimental results have been tested on two different datasets. In the first scenario, the fusion method is applied to aggregate the decision maps of PRNU based approach and SF based approach. In the second scenario, the fusion method is applied to integrate the decision maps of the algorithm based on demosaicing artifacts and the one based on SIFT key-points and descriptors	No	Crimes with digital evidence, Tampering of evidence	Not specified	No	Not specified	No
Rajba, P., & Mazurczyk, W. (2021). Information Hiding Using Minification. *IEEE Access, 9*, 66436–66449	Poland	Technology	Steganography	Data protection (cybersecurity)	Yes: tool developed	A new information hiding method based on the JavaScript files minification, in order to transfer secrets between a web server and a web client, providing robustness, stealthiness, and reasonable data hiding capacity	No	Cyberattacks	Not specified	No	Not specified	No
Ramos Lopez, R., Almaraz Luengo, E., Sandoval Orozco, A. L., & Villalba, L. J. G. (2020). Digital Video Source Identification Based on Container's Structure Analysis. *IEEE Access, 8*, 36363–36375	Spain	Technology	Imaging device identification methods, Digital content originality, Evidence in criminal courts and forensic laboratories	Justice (forensics), Linkage of forensic investigations, Ownership and authenticity of digital content	Yes: tool developed	A technique that identifies the source camcorder of digital videos generated by digital devices through the use of unsupervised algorithms based on the analysis of the structure of multimedia video devices. The technique uses clustering algorithms to make the correct grouping of both, brand and model, and the digital video	No	Crimes with digital evidence	Not specified	No	Not specified	No

Table 4 (continued)

General information				Steganalysis research meets the needs of society					Steganalysis research has positive impacts (benefits) on society		Steganalysis research does not have negative impacts (challenges) on society	
Reference	**Country**	**Field of publication**	**Research topic**	**Societal cybersecurity need(s) addressed**	**Research output**	**Description of tool(s)**	**Societal acceptance assessment**	**Threats addressed**	**Segment(s) of society benefitted**	**Identified societal positive impact(s)**	**Identified societal negative impact(s)**	**Mitigation/ minimisation measures**
Schaffhauser, A., Mazurczyk, W., Caviglione, L., Zuppelli, M., & Hernandez-Castro, J. (2022). Efficient Detection and Recovery of Malicious PowerShell Scripts Embedded into Digital Images. *Security and Communication Networks*, 2022, 1–12	Germany Poland Italy United Kingdom	Technology, Information sciences, Security	Stegomalware or covert channels detection	Data protection (cybersecurity)	Yes: tool developed	Mavis: a method for addressing Invoke-PSImage attacks, detecting hidden payloads, retrieving the embedded information, and estimating its size. Its effectiveness is compared against McAfee SAT and StegExpose	No	Cyberattacks	Not specified	No	Not specified	No
Spiekermann, D., Keller, J., & Eggendorfer, T. (2017). Towards Covert Channels in Cloud Environments: A Study of Implementations in Virtual Networks. In C. Kraetzer, Y. Q. Shi, J. Dittmann, H. Kim, (Eds.), *Digital Forensics and Watermarking. IWDW 2017. Lecture Notes in Computer Science, vol 10431*, 248–262	Germany	Forensic sciences, Multimedia development	Covert channels	Justice (forensics)	Yes: tools collected	Countermeasures to covert channels: protocols (active wardens, traffic normalization), migration (VM-based technique)	No	Criminal use of steganography	Not specified	No	Not specified	No

Table 4 (continued)

General information				Steganalysis research meets the needs of society					Steganalysis research has positive impacts (benefits) on society		Steganalysis research does not have negative impacts (challenges) on society	
Reference	**Country**	**Field of publication**	**Research topic**	**Societal cybersecurity need(s) addressed**	**Research output**	**Description of tool(s)**	**Societal acceptance assessment**	**Threats addressed**	**Segment(s) of society benefitted**	**Identified societal positive impact(s)**	**Identified societal negative impact(s)**	**Mitigation/ minimisation measures**
Stoyanova, M., Nikoloudakis, Y., Panagiotakis, S., Pallis, E., & Markakis, E. K. (2020). A Survey on the Internet of Things (IoT) Forensics: Challenges, Approaches, and Open Issues. *IEEE Communications Surveys & Tutorials, 22*(2), 1191–1221	Germany Greece	Communications	Review of digital forensics challenges	Justice (forensics), Ownership and authenticity of digital content, Linkage of forensic investigations	No	N/A	No	Crimes with digital evidence Criminal use of steganography	Society in general	Yes: Human rights (ethics and protection of personal data), Cross-border cooperation, Public accountability and transparency, Strict observance of international law (chain of custody)	Yes: privacy and data protection	Yes: European law, Forensic standardization (ISO), Data storage, protection and processing guidelines, Gathering and use of evidence rules
Szary, P., Mazurczyk, W., Wendzel, S., & Caviglione, L. (2022). Analysis of Reversible Network Covert Channels. *IEEE Access, 10*, 41226–41238	Poland Germany Italy	Technology	Covert channels	Data protection (cybersecurity)	Yes: tools collected	Active wardens or traffic engineering. Traffic shaping, buffering, random packet dropping, "signalling" strategies, noise adding, code layering, augmentation of the kernel, DS and per-packet granularity, alterations of the perceived QoE, Scapy, NetFilterQueue, page loading time, etc	No	Criminal use of steganography	Not specified	No	Yes: privacy and data protection	No

Table 4 (continued)

General information				Steganalysis research meets the needs of society					Steganalysis research has positive impacts (benefits) on society		Steganalysis research does not have negative impacts (challenges) on society	
Reference	**Country**	**Field of publication**	**Research topic**	**Societal cybersecurity need(s) addressed**	**Research output**	**Description of tool(s)**	**Societal acceptance assessment**	**Threats addressed**	**Segment(s) of society benefitted**	**Identified societal positive impact(s)**	**Identified societal negative impact(s)**	**Mitigation/ minimisation measures**
Timmerman, D., Bennabhaktula, G. S., Alegre, E., & Azzopardi, G. (2021). Video Camera Identification from Sensor Pattern Noise with a Constrained ConvNet. In *Proceedings of the 10th International Conference on Pattern Recognition Applications and Methods (ICPRAM 2021)*, 417–425	The Netherlands Spain	Computing sciences, Information sciences	Imaging device identification methods, Digital content originality, Evidence in criminal courts and forensic laboratories	Justice (forensics), Linkage of forensic investigations, Ownership and authenticity of digital content	Yes: tool developed	A method to identify the source camera of a video based on camera specific noise patterns that they extract from video frames. An extended version of a constrained convolutional layer capable of processing colour inputs. Their system is designed to classify individual video frames which are in turn combined by a majority vote to identify the source camera. They evaluated this approach on the benchmark VISION data set consisting of 1539 videos from 28 different cameras	No	Crimes with digital evidence	Not specified	No	Not specified	No

Table 4 (continued)

General information				Steganalysis research meets the needs of society					Steganalysis research has positive impacts (benefits) on society		Steganalysis research does not have negative impacts (challenges) on society	
Reference	**Country**	**Field of publication**	**Research topic**	**Societal cybersecurity need(s) addressed**	**Research output**	**Description of tool(s)**	**Societal acceptance assessment**	**Threats addressed**	**Segment(s) of society benefitted**	**Identified societal positive impact(s)**	**Identified societal negative impact(s)**	**Mitigation/ minimisation measures**
Yari, I. A., & Zargari, S. (2017). An Overview and Computer Forensic Challenges in Image Steganography. In *2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, 360–364	United Kingdom	Information sciences, Computing sciences, Communications	Review of digital forensics challenges	Justice (forensics)	Yes: tools collected	Testing of open-source steganography tools: JPHIDE, SilentEye, S-tool, OpenPuff, OpenStego, QuickStego	No	Criminal use of steganography, Crimes with digital evidence	Not specified	No	Not specified	No

Acknowledgements
We would like to express our gratitude to the participants of the nominal groups for their invaluable contributions to this research. We also extend our appreciation to the anonymous reviewers for their constructive comments.

Author contributions
The individual contributions of authors to the manuscript are as follows: ANS carried out the systematic review of the literature, assisted in the nominal groups, analysed the results and drafted the manuscript. FJCT proposed the study design, assisted in the systematic review and data analysis, conducted the nominal groups, and revised and drafted the manuscript. Both authors read and approved the final manuscript.

Funding
This work is funded by the European Union's Horizon 2020 Research and Innovation programme under grant agreement No. 101021687 (UNCOVER).

Availability of data and materials
The authors confirm that all data generated or analyzed during this study are included in this published article. No dataset is analyzed or generated.

Declarations

Competing interests
The authors declare that they have no competing interests.

Author details
[1]Plus Ethics, Elche, Spain. [2]PARADIGMA Innovation, Elche, Spain.

Received: 27 October 2023 Accepted: 22 April 2024
Published online: 14 May 2024

References

Almeida, J. R., Fajarda, O., & Oliveira, J. L., et al. (2020). File forgery detection using a weighted rule-based system. In A. Arampatzis (Ed.), *Experimental IR meets multilinguality, multimodality, and interaction. CLEF 2020 lecture notes in computer science*. Cham: Springer International Publishing.

Araujo, I. I., & Kazemian, H. (2020). Improving steganographic capacity using distributed steganography over BMP. *Multimedia Tools and Applications, 79*(35–36), 26181–26195. https://doi.org/10.1007/s11042-020-09298-3

Arshad, H., Jantan, A., & Abiodun, O. (2018). Digital Forensics: Review of issues in scientific validation of digital evidence. *Journal of Information Processing Systems, 14*(2), 346–376. https://doi.org/10.3745/jips.03.0095

Athanasiadou, E., Geradts, Z., & Van Eijk, E. (2018). Camera recognition with deep learning. *Forensic Sciences Research, 3*(3), 210–218. https://doi.org/10.1080/20961790.2018.1485198

Aumayr, D., & Schöttle, P. (2022). U can't (re)touch this—a deep learning approach for detecting image retouching. In S. Sclaroff, C. Distante, M. Leo, G. M. Farinella, & F. Tombari (Eds.), *Image analysis and processing—ICIAP 2022*. Cham: Springer International Publishing.

Bachman, R. D., & Schutt, R. K. (2017). *Fundamentals of research in criminology and criminal justice* (4ª). Sage.

Bammey, Q., Grompone von Gioi, R., & Morel, J. M. (2020). An Adaptive Neural Network for Unsupervised Mosaic Consistency Analysis in Image Forensics. In *2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR),* 14182–14192. https://doi.org/10.1109/CVPR42600.2020.01420

Bernacki, J., & Scherer, R. (2022). Digital forensics: a fast algorithm for a digital sensor identification. *Journal of Information and Telecommunication, 6*(4), 399–419. https://doi.org/10.1080/24751839.2022.2058252

Bertini, F., Sharma, R., & Montesi, D. (2022). Are social networks watermarking us or are we (unawarely) watermarking ourself? *Journal of Imaging, 8*(5), 132. https://doi.org/10.3390/jimaging8050132

Bobkowska, K., Nagaty, K., & Przyborski, M. (2019). Incorporating iris, fingerprint and face biometric for fraud prevention in e-passports using fuzzy vault. *IET Image Processing, 13*(13), 2516–2528. https://doi.org/10.1049/iet-ipr.2019.0072

Bortolameotti, R., van Ede, T., Caselli, M., Everts, M. H., Hartel, P., Hofstede, R., Jonker, W., & Peter, A. (2017). DECANTeR: DEteCtion of Anomalous outbouND HTTP TRaffic by Passive Application Fingerprinting. In *ACSAC '17 Proceedings of the 33rd Annual Computer Security Applications Conference*, 373–386. https://doi.org/10.1145/3134600.3134605

Bührer, S., Feidenheimer, A., Walz, R., Lindner, R., Beckert, B., & Wallwaey, E. (2022). Concepts and methods to measure societal impacts – an overview. *Discussion Papers Innovation Systems and Policy Analysis, 74*. https://publica-rest.fraunhofer.de/server/api/core/bitstreams/06cee3b3-f386-4ef5-8026-26c9311e0923/content

Burgess, J. P. (2012). The Societal Impact of Security Research. *PRIO Policy Brief, 9*. https://www.prio.org/publications/7377

Burton, J., & Lain, C. (2020). Desecuritising cybersecurity: towards a societal approach. *Journal of Cyber Policy, 5*(3), 449–470. https://doi.org/10.1080/23738871.2020.1856903

Bush, A., Amechi, M., & Persky, A. (2020). An exploration of pharmacy education researchers' perceptions and experiences conducting qualitative research. *American Journal of Pharmaceutical Education, 84*(3), 7129. https://doi.org/10.5688/ajpe7129

Cabaj, K., Caviglione, L., Mazurczyk, W., Wendzel, S., Woodward, A., & Zander, S. (2018). The new threats of information hiding: the road ahead. *IT Professional, 20*(3), 31–39. https://doi.org/10.1109/MITP.2018.032501746

Caianiello, M., & Camon, A. (Eds.) (2021). *Digital forensic evidence. Towards common European standards in antifraud administrative and criminal investigations*. Wolters Kluwer. https://iris.unimore.it/bitstream/11380/1230941/2/CAIANIELLO-CAMON%2C%20Digital%20forensic%20evidence.pdf

Cardamone, N., & d'Amore, F. (2019). DWT and QR code based watermarking for document DRM. In C. Yoo, Y. Q. Shi, H. Kim, A. Piva, & G. Kim (Eds.), *Digital forensics and watermarking IWDW 2018*. Cham: Springer International Publishing.

Casino, F., Dasaklis, T. K., Spathoulas, G. P., Anagnostopoulos, M., Ghosal, A., Borocz, I., Solanas, A., Conti, M., & Patsakis, C. (2022). Research trends, challenges, and emerging topics in digital forensics: a review of reviews. *IEEE Access, 10*, 25464–25493. https://doi.org/10.1109/ACCESS.2022.3154059

Castillo-Camacho, I., & Wang, K. (2021). Data-dependent scaling of CNN's first layer for improved image manipulation detection. In X. Zhao, Y. Q. Shi, A. Piva, & H. J. Kim (Eds.), *Digital forensics and watermarking*. Cham: Springer International Publishing.

Caviglione, L., Choras, M., Corona, I., Janicki, A., Mazurczyk, W., Pawlicki, M., & Wasielewska, K. (2021a). Tight arms race: overview of current malware threats and trends in their detection. *IEEE Access, 9*, 5371–5396. https://doi.org/10.1109/ACCESS.2020.3048319

Caviglione, L., & Mazurczyk, W. (2022). Never mind the malware, here's the stegomalware. *IEEE Security & Privacy, 20*(5), 101–106. https://doi.org/10.1109/MSEC.2022.3178205

Caviglione, L., Mazurczyk, W., Repetto, M., Schaffhauser, A., & Zuppelli, M. (2021b). Kernel-level tracing for detecting stegomalware and covert channels in linux environments. *Computer Networks, 191*, 108010. https://doi.org/10.1016/j.comnet.2021.108010

Caviglione, L., Wendzel, S., & Mazurczyk, W. (2017). The future of digital forensics: challenges and the road ahead. *IEEE Security & Privacy, 15*(6), 12–17. https://doi.org/10.1109/MSP.2017.4251117

Chang, C. C. (2021). Cryptospace invertible steganography with conditional generative adversarial networks. *Security and Communication Networks, 2021*, 1–14. https://doi.org/10.1155/2021/5538720

Chang, C. C. (2022). Automation of reversible steganographic coding with nonlinear discrete optimisation. *Connection Science, 34*(1), 1719–1735. https://doi.org/10.1080/09540091.2022.2078792

Chang, C. C., Li, C. T., & Chen, K. (2019). Privacy-preserving reversible information hiding based on arithmetic of quadratic residues. *IEEE Access, 7*, 54117–54132. https://doi.org/10.1109/ACCESS.2019.2908924

Christen, M., Gordijn, B., & Loi, M. (Eds.). (2020). *The ethics of cybersecurity*. Cham: Springer.

Collier, B., & Hutchings, A. (2023). Cybercrime: a social ecology. In A. Liebling, S. Maruna, & L. McAra (Eds.), *The oxford handbook of criminology* (pp. 456–478). Oxford: Oxford University Press.

European Commission (2023). Horizon Europe Work Programme 2023–2024. Civil Security for Society. https://ec.europa.eu/info/funding-tenders/

opportunities/docs/2021-2027/horizon/wp-call/2023-2024/wp-6-civil-security-for-society_horizon-2023-2024_en.pdf
Cozzolino, D., Marra, F., Gragnaniello, D., Poggi, G., & Verdoliva, L. (2020). Combining PRNU and noiseprint for robust and efficient device source identification. *EURASIP Journal on Information Security*. https://doi.org/10.1186/s13635-020-0101-7
Crișan, D., Irimia, A., Gota, D., Miclea, L., Puscasiu, A., Stan, O., & Valean, H. (2021). Analyzing Benford's law's powerful applications in image forensics. *Applied Sciences, 11*(23), 1148. https://doi.org/10.3390/app112311482
Dalal, M., & Juneja, M. (2021). Steganography and steganalysis (in digital forensics): a cybersecurity guide. *Multimedia Tools and Application, 80*, 5723–5771. https://doi.org/10.1007/s11042-020-09929-9
Darmet, L., Wang, K., & Cayre, F. (2020). Weakly supervised adaptation to resizing for image manipulation detection on small patches. In H. Wang, X. Zhao, Y. Shi, H. Kim, & A. Piva (Eds.), *Digital forensics and watermarking*. Cham: Springer International Publishing.
Davey, C. L., & Wootton, A. B. (2017). Prospects for EU-funded security research – The ethics of impact outside the EU discourse. In C. Heinzelmann, & E. Marks (Eds.), *International Perspectives of Crime Prevention 9, Contributions from the 10th Annual International Forum 2016 within German Congress on Crime Prevention Forum Verlag Godesberg GmbH 2017*, 171–196. https://www.praeventionstag.de/nano.cms/vortraege/id/3340
De Ruyter, K. (1996). Focus versus nominal group interviews: a comparative analysis. *Marketing Intelligence & Planning, 14*(6), 44–50. https://doi.org/10.1108/02634509610131153
Delbecq, A. L., & Van de Ven, A. H. (1971). A group process model for problem identification and program planning. *The Journal of Applied Behavioral Science, 7*(4), 466–492. https://doi.org/10.1177/002188637100700404
Djebbar, F. (2021). Securing IoT data using steganography: a practical implementation approach. *Electronics, 10*(21), 2707. https://doi.org/10.3390/electronics10212707
Douglas, M., Bailey, K., Leeney, M., & Curran, K. (2017). An overview of steganography techniques applied to the protection of biometric data. *Multimedia Tools and Applications, 77*(13), 17333–17373. https://doi.org/10.1007/s11042-017-5308-3
Fernandes, C. S. (2022). Steganography and computer forensics—the art of hiding information: a systematic review. *ARIS2 Advanced Research on Information Systems Security, 2*(2), 31–38. https://doi.org/10.5639/aris2.v2i2.20
Fernández-Menduiña, S., & Pérez-González, F. (2021). On the information leakage quantification of camera fingerprint estimates. *EURASIP Journal on Information Security*. https://doi.org/10.1186/s13635-021-00121-6
Frattolillo, F. (2022). Digital copyright protection: focus on some relevant solutions. *International Journal of Communication Networks and Information Security, 9*(2), 282–293. https://doi.org/10.1776/ijcnis.v9i2.2425
Frick, R. A., Liu, H., & Steinebach, M. (2020). Detecting Double Compression and Splicing using Benfords First Digit Law. In *ARES´20 Proceedings of the 15th International Conference on Availability, Reliability and Security*. https://doi.org/10.1145/3407023.3409200
Ghanmi, N., Nabli, C., & Awal, A. M. (2021). CheckSim: a reference-based identity document verification by image similarity measure. In E. H. Barney Smith & U. Pal (Eds.), *Document analysis and recognition—ICDAR 2021 workshops*. Cham: Springer International Publishing.
Göbel, T., & Baier, H. (2018). Anti-forensic capacity and detection rating of hidden data in the Ext4 filesystem. In G. Peterson & S. Shenoi (Eds.), *Advances in digital forensics XIV*. Cham: Springer International Publishing.
Göbel, T., & Baier, H. (2019). Fishy—a framework for implementing filesystem-based data hiding techniques. In F. Breitinger & I. Baggili (Eds.), *Digital forensics and cyber crime*. Cham: Springer International Publishing.
Gragnaniello, D., Marra, F., Poggi, G., & Verdoliva, L. (2018). Analysis of Adversarial Attacks against CNN-based Image Forgery Detectors. In *2018 26th European Signal Processing Conference (EUSIPCO)*, 967–971. https://doi.org/10.23919/EUSIPCO.2018.8553560
Hegarty, M. T., & Keane, A. J. (2020). Modern Techniques for Discovering Digital Steganography. In *21st European Conference on Cyber Warfare and Security*. https://arrow.tudublin.ie/engscheleart/348/
Hugé, J., & Mukherjee, N. (2018). The nominal group technique in ecology & conservation: application and challenges. *Methods in Ecology and Evolution, 9*(1), 33–41. https://doi.org/10.1111/2041-210X.12831
Hughes, N., Ziemak, E., Martinez, C., & Stout, P. (2021). Toward a cost–benefit analysis of quality programs in digital forensic laboratories in the United States. *WIREs Forensic Science*. https://doi.org/10.1002/wfs2.1422
Hytönen, E., Trent, A., & Ruoslahti, H. (2022). Societal Impacts of Cyber Security in Academic Literature: Systematic Literature Review. In T. Eze, N. Khan, & C. Onwubiko (Eds.), *Proceedings of the 21st European Conference on Cyber Warfare and Security*. Reading: Academic Conferences International Limited, 86–93. https://doi.org/10.34190/eccws.21.1.288
Johnson, C., & Davies, R. (2020). Using digital forensic techniques to identify contract cheating: a case study. *J Acad Ethics, 18*, 105–113. https://doi.org/10.1007/s10805-019-09358-w
Kanwal, N., Asghar, M. N., Ansari, M. S., Fleury, M., Lee, B., Herbst, M., & Qiao, Y. (2020). Preserving chain-of-evidence in surveillance videos for authentication and trust-enabled sharing. *IEEE Access, 8*, 153413–153424. https://doi.org/10.1109/ACCESS.2020.3016211
Kao, D. Y., Wu, N. C., Tsai, F. (2019). The Governance of Digital Forensic Investigation in Law Enforcement Agencies. In *2019 21st International Conference on Advanced Communication Technology (ICACT)*, 61–65. https://doi.org/10.23919/ICACT.2019.8701995
Karampidis, K., Kavallieratou, E., & Papadourakis, G. (2018). A review of image steganalysis techniques for digital forensics. *Journal of Information Security and Applications, 40*, 217–235. https://doi.org/10.1016/j.jisa.2018.04.005
Keller, J., & Wendzel, S. (2021). Reversible and plausibly deniable covert channels in one-time passwords based on hash chains. *Applied Sciences, 11*(2), 731. https://doi.org/10.3390/app11020731
Kilts, S., Altschaffel, R., & Dittman, J. (2022). Hidden in Plain Sight – Persistent Alternative Mass Storage Data Streams as a Means for Data Hiding With the Help of UEFI NVRAM and Implications for IT Forensics. In *IH&MMSec´22 Proceedings of the 2022 ACM Workshop on Information Hiding and Multimedia Security*, 107–112. https://doi.org/10.1145/3531536.3532965
Kuppa, A., Grzonkowski, S., & Le-Khac, N. A. (2018). Enabling Trust in Deep Learning Models: A Digital Forensics Case Study. In *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, 1250–1255. https://doi.org/10.1109/TrustCom/BigDataSE.2018.00172
Li, Z., Liu, F., & Bors, A. G. (2018). 3D steganalysis using laplacian smoothing at various levels. In X. Sun, Z. Pan, & E. Bertino (Eds.), *Cloud computing and security*. Springer International Publishing.
Martínez-Tornés, B., Boros, E., Doucet, A., Gomez-Krämer, P., Ogier, J. M., & d'Andecy, V. P. (2023). Knowledge-based techniques for document fraud detection: a comprehensive study. In A. Gelbukh (Ed.), *Computational linguistics and intelligent text processing CICLing 2019*. Springer Nature Switzerland.
Mazurczyk, W., Wendzel, S., Chourib, M., & Keller, J. (2019). Countering adaptive network covert communication with dynamic wardens. *Future Generation Computer Systems, 94*, 712–725. https://doi.org/10.1016/j.future.2018.12.047
Meden, B., Rot, P., Terhorst, P., Damer, N., Kuijper, A., Scheirer, W. J., Ross, A., Peer, P., & Struc, V. (2021). Privacy-enhancing face biometrics: a comprehensive survey. *IEEE Transactions on Information Forensics and Security, 16*, 4147–4183. https://doi.org/10.1109/TIFS.2021.3096024
Megías, D. (2020). Data hiding: New opportunities for security and privacy? In *Proceedings of the 2020 European Interdisciplinary Cybersecurity Conference (EICC 2020). ACM, New York, USA, Article 15, (1–6)*. ACM, https://doi.org/10.1145/3424954.3425511
Moher, D., Liberati, A., Tetzlaff, J., Altman, D. G., & PRISMA Group (2009). Preferred reporting items for systematic reviews and meta-analyses: the PRISMA statement. *PLoS medicine*. 6(7); e1000097. https://doi.org/10.1371/journal.pmed.1000097
Neuner, S., Voyiatzis, A., Schmiedecker, M., & Weippl, E. R. (2017). Timestamp hiccups: Detecting manipulated filesystem timestamps on NTFS. In ARES´17 Proceedings of the 12th International Conference on Availability, Reliability and Security, (33). https://doi.org/10.1145/3098954.3098994
Odebade, A., Welsh, T., Mthunzi, S., & Benkhelifa, E. (2017). Mitigating Anti-forensics in the Cloud via Resource-Based Privacy Preserving Activity Attribution. In *2017 Fourth International Conference on Software Defined Systems*, 143–149. https://doi.org/10.1109/SDS.2017.7939155
Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., & Moher, D. (2021). The PRISMA 2020 statement: an

updated guideline for reporting systematic reviews. *Systematic Reviews*. https://doi.org/10.1186/s13643-021-01626-4

Peng, J., & Tang, S. (2021). Covert communication over VoIP streaming media with dynamic key distribution and authentication. *IEEE Transactions on Industrial Electronics, 68*(4), 3619–3628. https://doi.org/10.1109/TIE.2020.2979567

Phan-Ho, A. T., & Retraint, F. (2022). A comparative study of bayesian and dempster-shafer fusion on image forgery detection. *IEEE Access, 10*, 99268–99281. https://doi.org/10.1109/ACCESS.2022.3206543

Pickering, C., & Byrne, J. (2014). The benefits of publishing systematic quantitative literature reviews for PhD candidates and other early-career researchers. *Higher Education Research & Development*. 33(3),534–548. https://doi.org/10.1080/07294360.2013.841651

Prakash, V., Williams, A., Garg, L., Savaglio, C., & Bawa, S. (2021). Cloud and edge computing-based computer forensics: challenges and open problems. *Electronics, 10*(11), 1229. https://doi.org/10.3390/electronics10111229

Rajba, P., & Mazurczyk, W. (2021). Information hiding using minification. *IEEE Access, 9*, 66436–66449. https://doi.org/10.1109/ACCESS.2021.3077197

Ramos Lopez, R., Almaraz Luengo, E., Sandoval Orozco, A. L., & Villalba, L. J. G. (2020). Digital video source identification based on container's structure analysis. *IEEE Access, 8*, 36363–36375. https://doi.org/10.1109/ACCESS.2020.2971785

Rusman, G., & Morozova, J. (2022). Legal analysis in forensic investigation. In N. S. Malik, E. A. Gromova, S. Gupta, & B. Balusamy (Eds.), *Legal analytics the future of analytics in law.* Chapman and Hall/CRC.

Schaffhauser, A., Mazurczyk, W., Caviglione, L., Zuppelli, M., & Hernandez-Castro, J. (2022). Efficient detection and recovery of malicious powershell scripts embedded into digital images. *Security and Communication Networks, 2022*, 1–12. https://doi.org/10.1155/2022/4477317

Spiekermann, D., Keller, J., & Eggendorfer, T. (2017). Towards covert channels in cloud environments: a study of implementations in virtual networks. In C. Kraetzer, Y. Q. Shi, J. Dittmann, & H. Kim (Eds.), *Digital forensics and watermarking IWDW 2017*. Springer International Publishing.

Stoyanova, M., Nikoloudakis, Y., Panagiotakis, S., Pallis, E., & Markakis, E. K. (2020). A survey on the internet of things (IoT) forensics: challenges, approaches, and open issues. *IEEE Communications Surveys & Tutorials, 22*(2), 1191–1221. https://doi.org/10.1109/COMST.2019.2962586

Stoykova, R., Andersen, S., Franke, K., & Axelsson, S. (2022). Reliability assessment of digital forensic investigations in the Norwegian Police. *Forensic Science International: Digital Investigation, 40*, 301351. https://doi.org/10.1016/j.fsidi.2022.301351

Szary, P., Mazurczyk, W., Wendzel, S., & Caviglione, L. (2022). Analysis of reversible network covert channels. *IEEE Access, 10*, 41226–41238. https://doi.org/10.1109/ACCESS.2022.3168018

Timmerman, D., Bennabhaktula, G. S., Alegre, E., & Azzopardi, G. (2021). Video Camera Identification from Sensor Pattern Noise with a Constrained ConvNet. In *Proceedings of the 10th International Conference on Pattern Recognition Applications and Methods (ICPRAM 2021)*, 417–425. https://doi.org/10.5220/0010246804170425

Vander Laenen, F. (2015). Not just another focus group: making the case for the nominal group technique in criminology. *Crime Science*. https://doi.org/10.1186/s40163-014-0016-z

Wadhwa, K., Barnard-Wills, D., & Wright, D. (2014). The state of the art in societal impact assessment for security research. *Science & Public Policy, 42*(3), 339–354. https://doi.org/10.1093/scipol/scu046

Wilson-Kovacs, D., & Wilcox, J. (2023). Managing policing demand for digital forensics through risk assessment and prioritization in England and wales. *Policing: A Journal of Policy and Practice.* https://doi.org/10.1093/police/paac106

Wu, L., Peng, Q., & Lemke, M. (2023). Research trends in cybercrime and cybersecurity: a review based on web of science core collection database. *International Journal of Cybersecurity Intelligence & Cybercrime, 6*(1), 5–28. https://doi.org/10.5230/OZMB2721

Wu, T., Breitinger, F., & O'Shaughnessy, S. (2020). Digital forensic tools: recent advances and enhancing the status quo. *Forensic Science International: Digital Investigation, 34*, 300999. https://doi.org/10.1016/j.fsidi.2020.300999

Yari, I. A., & Zargari, S. (2017). An Overview and Computer Forensic Challenges in Image Steganography. In *2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, 360–364. https://doi.org/10.1109/iThings-GreenCom-CPSCom-SmartData.2017.60

Publisher's Note