symmetry

MDPI

Review

Comprehensive Survey of Multimedia Steganalysis: Techniques, Evaluations, and Trends in Future Research

Doaa A. Shehab * and Mohmmed J. Alhaddad

Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah 21589, Saudi Arabia; malhaddad@kau.edu.sa

* Correspondence: dshehab@stu.kau.edu.sa

Abstract: During recent years, emerging multimedia processing techniques with information security services have received a lot of attention. Among those trends are steganography and steganalysis. Steganography techniques aim to hide the existence of secret messages in an innocent-looking medium, where the medium before and after embedding looks symmetric. Steganalysis techniques aim to breach steganography techniques and detect the presence of invisible messages. In the modern world, digital multimedia such as audio, images, and video became popular and widespread, which makes them perfect candidates for steganography. Monitoring this huge multimedia while the user communicates with the outside world is very important for detecting whether there is a hidden message in any suspicious communication. However, steganalysis has a significant role in many fields, such as to extract the stego-message, to detect suspicious hidden messages and to evaluate the robustness of existing steganography techniques. This survey provides the general principles of hiding secret messages using digital multimedia as well as reviewing the background of steganalysis. In this survey, the steganalysis is classified based on many points of view for better understanding. In addition, it provides a deep review and summarizes recent steganalysis approaches and techniques for audio, images, and video. Finally, the existing shortcomings and future recommendations in this field are discussed to present a useful resource for future research.

Keywords: steganalysis; steganography; data hiding; information security

check for updates

Citation: Shehab, D.A.; Alhaddad, M.J. Comprehensive Survey of Multimedia Steganalysis: Techniques, Evaluations, and Trends in Future Research. *Symmetry* **2022**, *14*, 117. https://doi.org/10.3390/sym14010117

Academic Editor: Mihai Postolache

Received: 8 October 2021
Accepted: 3 December 2021
Published: 10 January 2022

1. Introduction

Digital communication has revolutionized our everyday lives. Robust and secure communication is in demand to preserve information security. Many existing secure methods have been proposed and applied, but they are still being developed, to make these methods more effective in terms of security and performance [1].

In general, information security systems are divided into two main categories, which are cryptography and data hiding. Both categories aim to secure data whilst the difference is implied in their techniques. Cryptography uses various data encryption techniques and converts secret data into a hash encrypted package, while steganography does not modify the format of data but depends on hiding the secret data in innocuous-looking data [2].

Despite the popularity of cryptography techniques, as long as a third party knows about the presence of a secret message, the attacks will continue. Steganography is a new step in the encryption world due to fast implementation and no need for large software, besides the complexity of the composition and decomposition process which makes it difficult to crack. Hence, cryptography approaches could be more secure by combining them with steganography techniques.

Steganography is one of the oldest security techniques, going back to the Greek age. The word 'Steganography' is made of two old Greek words, "Stegano" and "Graphy", which means "Cover Writing". Over thousands of years, it was used in different forms such as wax tables, human skin, astragali, parchment, linguistic syntax, and newspapers [1].

During the first world war, microdot technology, using waste materials from magazines was used by the Germans [3]. In World War II, there were many mechanisms utilized to write secret messages, such as writing open-coded messages, Enigma machines, and using invisible ink [4]. In Saudi Arabia, a project for secret writing was started at the Abdulaziz City of Science and Technology. The project was about translating some old Arabic manuscripts on secret writing into English. These manuscripts were written 1200 years ago. Some of them were collected from Germany and Turkey [1,5].

However, the concept of digital steganography is recently emerging in the past two decades. The evolution of wireless systems and digital multimedia moved steganography to digital processing. In this regard, many contributions in this field have been proposed to ensure the security of sensitive information during transmission [6–8]. Despite the advantages of steganography, unfortunately, most uses of steganography are regarding illegitimate objectives involving three major areas, which are terrorism, pornography, and stolen data [9].

The past years have seen many illegitimate uses for steganography, such as in Berlin in May of 2011, a suspected al-Qaeda member was arrested with a memory card. The German Federal Criminal Police claimed that the memory card contained more than 100 text files about the future operations of al-Qaeda. These files were hidden in a pornographic video [10]. In the same year, Microsoft researchers discovered a new form of the 'Alureon' trojan that exploits steganography to be indomitable [11]. In Japan in October 2018, a spam campaign targeted users to deliver a banking trojan using steganography. The malicious code was hidden in a normal looking medium to be undetected by signature-based detection [12].

Given the illegitimate and dangerous usage of steganography in the past, the researchers start investing many efforts in steganalysis to detect and prevent malicious usage [13–15]. Steganalysis is the art of extracting hidden messages from a stego-file. These days, steganalysis has become a complex procedure, especially when it deals with an encrypted embedded message [16]. Steganalysis plays a significant role in many applications such as law enforcement, digital forensics, and national security. In the academic and research field, steganalysis could also be used to evaluate the strength of the proposed steganography techniques. Figure 1 illustrates the applications of steganalysis techniques.

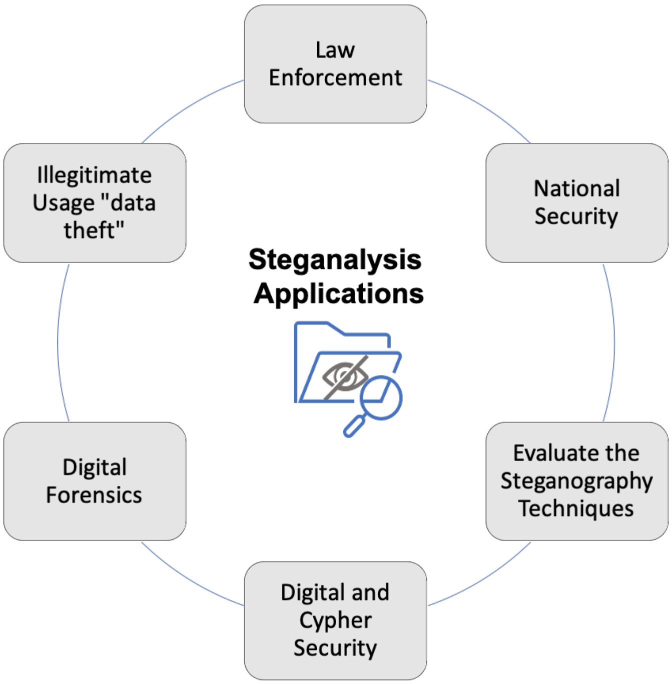
Law Enforcement
National Security
Evaluate the Steganography Techniques
Digital and Cypher Security
Digital Forensics
Illegitimate Usage "data theft"
Steganalysis Applications

Figure 1. The applications of steganalysis.

Steganography is about adding additional "confidential message" information to the regular medium by trying to maintain a non-suspicious looking content by ensuring the symmetry between the cover- and the stego- medium. Hence, to perform steganalysis, we need to select and extract some features from the cover/stego medium then analyze them to detect any changes. In general, there are two methods for steganalysis based on its application fields, which are the targeted and universal methods. The targeted method depends on the steganographic algorithm, hence, the main rule of this method is to analyze the statistical characteristics or "features" of a medium before and after embedding them using a specific steganography technique. Although this method mostly leads to accurate results, it is very restricted to specific embedding algorithms and a specific medium format [17]. In contrast, the steganographic algorithm in the universal method is unknown. Hence, the techniques that follow this type design a detector regardless of the steganographic algorithm, which makes it more practical. Due to that, this type is very widely used, although it is less efficient than the targeted method. The universal method is also divided into two blind and semi-blind approaches. The semi-blind approach depends on the cover and stego medium to determine the decision boundaries, while the blind approach uses only the cover medium for detection [18]. Figure 2 presents the classification of steganalysis methods.

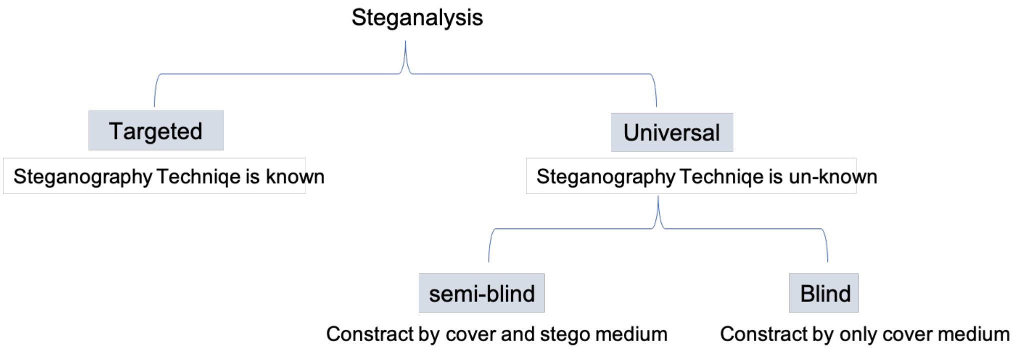
Steganalysis
Targeted
Steganography Techniqe is known
Universal
Steganography Techniqe is un-known
semi-blind
Constract by cover and stego medium
Blind
Constract by only cover medium

Figure 2. The General Classification of Steganalysis.

Steganalysis follows a common schema, which is illustrated in Figure 3. It starts with extracting some features from the input medium, then analyzes and classifies these features to detect the steganography. There are two types of features—handcrafted and deep features. In the first type, the well-known features are extracted manually such as statistical features. Deep features are not specified explicitly, and they are extracted automatically by Neural Networks or deep autoencoders [18]. After extracting the features, the classification is performed to distinguish the cover- and stego- medium. The classification could be performed in three different ways; first by using a statistical strategy such as an empirical threshold to detect the existence of a secret message. In the second way, specific features are fed to machine learning to train and learn the model of the cover medium; hence, in the test phase, it can distinguish the cover and stego-medium. The final method is by using Neural Networks. Neural Networks could be used not only for feature extraction but also as a classifier [19]. Finally, the output of steganalysis could be passive detection, which considers only the detection of the presence of hidden messages. In active detection, more information related to the length and/or the hidden information is provided [16,18].

The steganalysis of digital media, such as video, audio, and images, is very important as these are the most popular carrier files that will be analyzed. For this reason, this survey focuses on the steganalysis algorithms of digital video, image, and audio. The main contributions of this survey are highlighted in the following subsection.

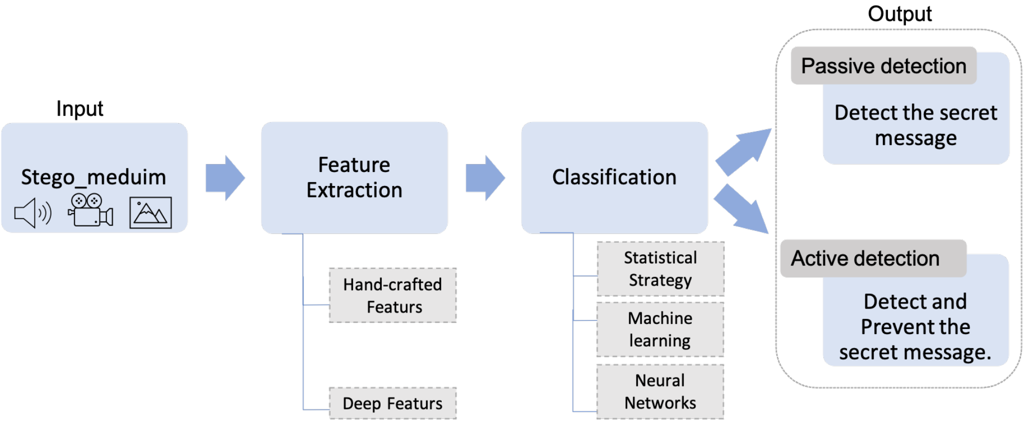

Figure 3. The Common Schema of Steganalysis.

Contribution of This Survey

There are few surveys in the steganalysis domain compared with other domains in security. Table 1 provides a summary of the recent existing surveys published in high-ranking journals and conferences. Most of these surveys have been published recently in 2018–2020, where the image medium receives the biggest attention.

The contribution of this survey is presented in Table 2. This survey provides a comprehensive overview of the steganalysis for the most popular mediums (image, audio, video). It should be noticed that the mentioned criteria in Table 2 are chosen only to highlight the differences between our survey and the other works. The main contributions of this survey are:

1. Provide a background for steganography and steganalysis in general;
2. Classify the steganalysis techniques based on different aspects;
3. Deep review for the recent state-of-the-art in steganalysis;
4. Provide a comprehensive overview for new interested researchers in steganalysis.

Table 1. Recapitulation of the existing surveys for the steganalysis domain.

Ref	Published Year	Journal or Conference	Mediums	Contributions
[20]	2015	Int. J. of Information and Communication technology	Image	Provide an overview of steganography for different kinds of multimedia. - Review different image steganography and steganalysis techniques. - Explain the way in which each algorithm works.
[18]	2018	IET Signal Processing	Audio	- Provide a comprehensive review of audio steganalysis. - Classify the literature into different categories. - Conduct comparison between different works.
[16]	2018	Journal of information security and applications	Image	- Discuss and present various steganalysis techniques from earlier ones to state of the art. - Classify the literature into different categories.
[21]	2018	Int. J. Electronic Security and Digital Forensics	Video	- Present an overview of video steganalysis techniques - Discuss the challenging and open issues.
[22]	2019	IEEE Access	Image	- Provide a systematic review of DL applied to steganalysis - Show the evolution of steganalysis in recent years using the DL techniques. - Highlight the most significant results and possible future work.

Table 1. *Cont.*

Ref	Published Year	Journal or Conference	Mediums	Contributions
[23]	2019	Multimedia Tools and Applications	Image	- Provide an overview of the steganalysis techniques considering: the embedding algorithm, estimation of the secret message payload and stego key determination. - Describe and compare various features of the steganalysis techniques. - Discuss the challenges and future recommendations.
[24]	2020	book (Digital media steganography) in Elsevier (ScienceDirect)	Audio, Video, Image, Text	- Provide an explanation for the vital elements of steganalysis applied to digital media. - Present a review for the existing works based on ML and DL over the last 10 years. - Provide a short discussion for the challenging and open issues.
[25]	2020	Multimedia Tools and Applications	Image, Video	- Provide a basic guide for the research in steganography and steganalysis domain. - Mention the applications, dataset, tools and techniques available. - Discuss the challenges and future recommendations.
[26]	2020	Journal of Real-Time Image Processing	Image	- Discuss the impacts of the real-time Image Steganalysis (IS). - Provide a brief overview of the IS based on deep NNs. - Analyze a practical real-time IS application and prospect the future issues of real-time IS.
[27]	2020	book(Digital media steganography) in Elsevier (ScienceDirect)	Image	- Present different NNs structures of the existing literature from the period 2015–2018 - Discussed the memory and time complexity, and practical problems for efficiency. - Explored the link between some past approaches sharing similarities. - Discuss steganography by deep learning.
[28]	2020	IEEE International Conference on Visual Communications and Image Processing	Image	- Review the preprocessing modules associated with CNN models.
[29]	2020	KSII Transactions on Internet and Information and Systems	Image	- Analyze current research states from the latest image steganography and steganalysis techniques based on DL. - Highlights the strengths and weakness of existing up-to-date techniques. - Discuss the challenges and future recommendations.
[30]	2020	Science Technology Libraries	Image	- Provide a bibliometric analysis of digital image steganalysis from 2014 to early 2020. - Use a mind map approach to analyze the results obtained from various of aspects like renowned authors, funding agencies, and affiliations.
[31]	2021	IET Image Processing	Image	- Review the recent research works in DL based digital image steganalysis. - Introduce the paradigm shift from ML approaches to employing more promising DL architectures. - Conduct comparison between different works.

Table 2. The difference between our survey and other steganalysis surveys.

Ref	Image	Audio	Video	Steganography Background	Steganalysis Classification	Datasets	Available Tools	Systematic Review
[20]	✓	x	x	✓	✓	x	x	x
[24]	✓	✓	✓	x	✓	x	x	x
[16]	✓	x	x	x	✓	✓	x	x
[18]	x	✓	x	x	✓	x	x	x
[21]	x	x	✓	x	✓	x	x	x
[22]	x	x	x	x	x	✓	x	✓
[23]	✓	x	x	x	✓	x	x	x
[25]	✓	x	✓	✓	✓	✓	✓	x
[26]	✓	x	x	x	x	x	x	x
[27]	✓	x	x	✓	x	✓	x	x
[28]	✓	x	x	x	✓	x	x	x
[29]	✓	x	x	✓	✓	x	x	x
[30]	✓	x	x	x	✓	x	x	✓
[31]	✓	x	x	✓	✓	x	x	x
Our	✓	✓	✓	✓	✓	✓	✓	x

In the remainder of this survey, an overview of steganography and the common scheme of steganalysis is mentioned in Sections 2 and 3, respectively. In Section 4, the recent techniques for audio, image, and video steganalysis are reviewed. The database utilized in the steganlysis domain is presented in Section 5. In Section 6, we provide the evaluation metrics for steganalysis, followed by the popular digital multimedia steganalysis tools in Section 7. Finally, the open issues and the main shortcomings are discussed in Section 8 and the Conclusion of this survey is presented in Section 9.

2. Steganography: An Overview

Assuring the confidentiality of the transferred information is a crucial element. In this regard, a few techniques have been established to ensure message confidentiality. However, sometimes, keeping the existence of the message secret is demanded. This shows the importance of steganography usage.

The common concept of steganography is to hide the communication between two sides from the eyes of attackers. Hence, concealed communication can be embedded in an innocuous medium such as computer code, video film, or audio recording. After exchanging the data, both parties should destroy the cover message to prevent accidental reuse [32].

To hide data in any medium, embedding and extracting algorithms are required. The task of the embedding algorithm is to hide secret information within a cover medium. In this step, a secret key is applied to protect the process of embedding; hence, ensuring that only those with the secret keyword can access the hidden information. In contrast, the extracting algorithm is used on a feasibly modified medium and returns the hidden secret information [32].

2.1. Steganography Categories

Steganography has three main categories: pure steganography, secret key steganography, and public-key steganography [32].

2.1.1. Pure Steganography

This type has no requirement for the exchanging of particular secret information (such as a stego-key). The embedding operation can be demonstrated by the mapping $E : C \times M \rightarrow C$. The extracting process can be demonstrated by the mapping $D : C \rightarrow M$. Here, C indicates the set of probable covers and M indicates the set of probable messages; $|C| \geq |M|$. However, since the parties depend only on the assumption that this secret information is not known by others, this leads to a lack of security.

2.1.2. Secret Key Steganography

Secret key steganography requires a secret key (stego-key) during the communication. Hence, the sender and receiver should have the secret key to access and read the message. This results in more robustness and security.

2.1.3. Public Key Steganography

Public key steganography is enhanced by the concept of public-key cryptography. In this type, a *public key* and a private key are applied to ensure the security of communication. The *public key* is used by the sender through the encoding process. While the private key is used to decipher the secret message. Although the *public key* steganography is more robust, it decreases the size of the secret message to be embedded. This is because the encryption algorithms increase the size of the message to more than double its original size.

2.2. Steganography Techniques

The embedding process is very significant for hiding the data in digital media. In this regard, many techniques have been proposed to enhance the performance of embedding. These techniques could be categorized under several domains.

In this survey, the steganography domains are classified into six categories, although in some cases, exact classification is not possible. As illustrated in Figure 4, the domains are: spatial domain, transform domain, vector domain, entropy coding domain, adaptive domain, and distortion domain [33]. The spatial and transform domains are the most popular used in the state-of-the-art, where they contain various techniques that deal with different digital media steganography (image, audio, video), while the vector and entropy coding contain the techniques that deal with video steganography. Finally, the adaptive and distortion domains are a special case of spatial and transform domains [1].

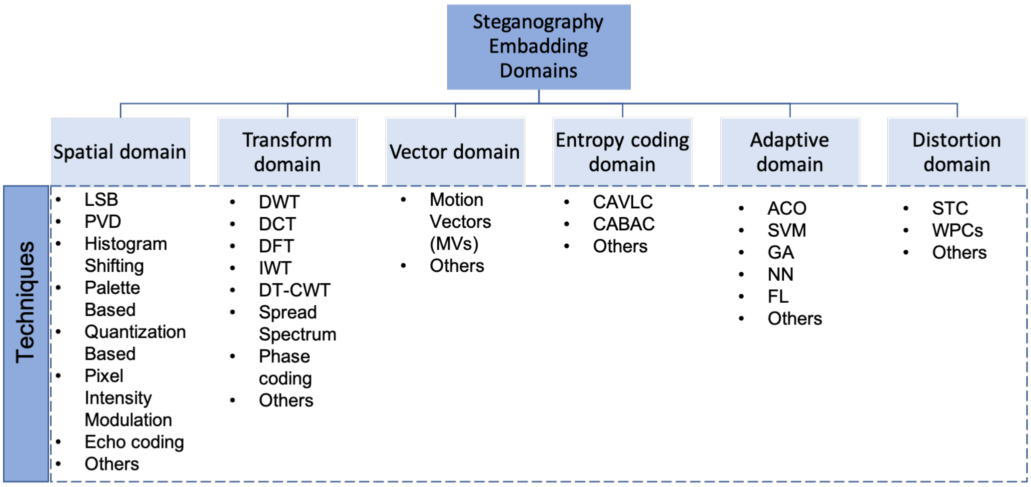

Figure 4. The classification of steganography techniques based on embedding domain.

One of the oldest and most used steganography techniques is Least Significant Bits (LSB), which was used as an example to explain the general steganography scheme [24] in Figure 5.

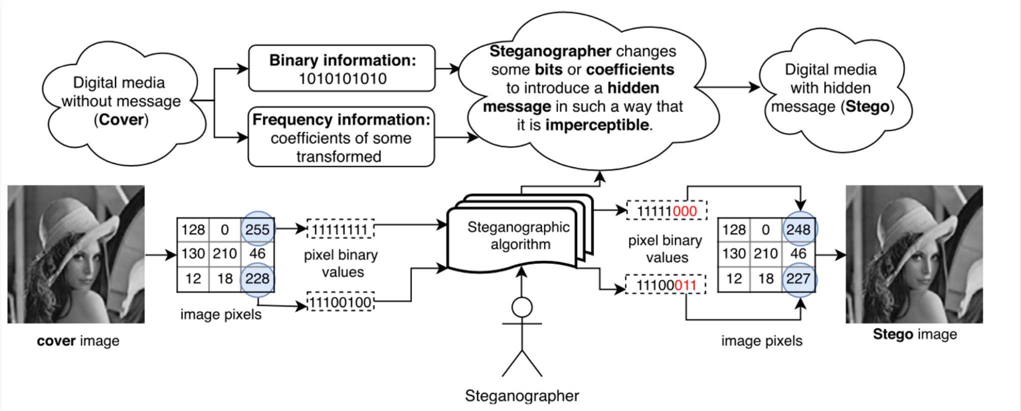
Digital media without message (Cover)
Binary information: 1010101010
Frequency information: coefficients of some transformed
Steganographer changes some bits or coefficients to introduce a hidden message in such a way that it is imperceptible.
Digital media with hidden message (Stego)
cover image
128 0 255
130 210 46
12 18 228
image pixels
11111111
11100100
pixel binary values
Steganographic algorithm
Steganographer
11111000
11100011
pixel binary values
128 0 248
130 210 46
12 18 227
image pixels
Stego image

Figure 5. Steganography scheme. Example of embedding a data in LSB. Taken from [24].

2.2.1. Spatial Domain

The techniques of this domain change particular information in the digital mediums which will be invisible to the human eye. There are various spatial domain techniques such as LSB, Pixel Value Differencing (PVD), Histogram Shifting, Pixel Intensity Modulation, Echo coding, and so forth [24].

2.2.2. Transform Domain

The opposite of the spatial domain, the embedding in the transform domain is done in transformed coefficients instead of straight to the intensity values. Some of the existing transform domain techniques are Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT), phase coding, Spread Spectrum (SS), and so forth.

2.2.3. Vector Domain

The techniques of this domain embed the information into the pixels of video frames. It is utilized for the H.264/AVC and recently HVC Video coding standard. The Motion Vectors (MVs) technique is applied in both spatial and temporal domains due to the correlation between the adjoining MVs [34].

2.2.4. Entropy Coding Domain

The techniques of this domain are used to exploit the benefit of the multimedia format structure [35]. For example, the H.264/AVC video coding standards provided two kinds of entropy encoding techniques for embedding, which are CAVLC (Context-Adaptive Variable Length Coding) and CABAC (Context-based Adaptive Binary Arithmetic Coding). These techniques were recently also used to embed the data in the H.265/HEVC video coding standard [25].

2.2.5. Adaptive Domain

This is sometimes referred to as "*Masking*" or "*Statistics-aware domain*" [25]; techniques that use statistics are applied to embed the data into a digital medium by changing some statistical features of the cover. It mostly depends on splitting the cover into blocks or "regions". Then, the best regions, which are sometimes called regions-of-interest (ROI), are determined in order to embed the data [36]. To find ROI, the researchers used statistical strategies or combined the techniques of other fields such as Ant Colony Optimization (ACO) [37]. In addition, to enhance the embedding process, some researchers switched to machine learning techniques [25] such as Support Vector Machine (SVM), Genetic Algorithm (GA), Fuzzy Logic (FL), Neural Networks (NN).

2.2.6. Distortion Domain

The distortion techniques hide the data using signal distortion in the encoding phase. Then, in the decoding phase, the deviation is measured from the original cover. Mainly, this approach intends to reduce the resulting errors produced by embedding and therefore to minimize the total signal distribution [36]. This domain includes matrix embedding strategy (MES), Syndrome Trellis Code (STC) [38], the wet paper code [39], and so forth.

3. Steganalysis: A Common Scheme

The aim of steganalysis is to detect hidden data embedded using steganographic techniques. Steganalysis includes several tasks concerning the hidden data in the digital medium like predicting the payload used to embed the data, predicting the steganographic techniques used, and the classification process of whether the files contain hidden data or not. The classification is one of the most important tasks in steganalysis [24]. The classification task includes two significant components, the features, and the classifier. The following subsections describe them in detail.

3.1. Feature Extraction

The art of steganalysis makes a major contribution to the selection of features or characteristics that might be shown by Stego- and Cover-objects. There are two types of features which are *deep features* and *handcrafted features*, which are sometimes called "statistical features" or "specific features". As illustrated in Figure 6, the steganalysis based on features could be classified into:

3.1.1. Signature Steganalysis

In this type, the features are considered as a unique pattern or signature. Hence, if the steganographic embedding technique is identified or was popular, it becomes easy to select and extract frequent special patterns that have been produced, like histogram arrangement, minimum and maximum intensity range, and so forth. This type is called *target* or *specific*, while the other one is the *universal* type where the features are identified as a behavioral pattern regardless of the embedding technique. Some steganography techniques follow sequentially or linear access of the cover medium unit for embedding [40]. This leads to an obvious pattern that can be easily detected; for example, a change in the expected JPEG compression quantization nature [16].

3.1.2. Statistical Steganalysis

Statistical steganalysis is mainly dependent on extracting statistical features and properties of cover- and stego- mediums. It also includes *target* and *universal* methods. The target methods are developed by studying and analyzing the steganographic embedding techniques and determining particular statistics features that have been modified as a consequence of the embedding operation. Therefore, it is important to deeply understand the embedding techniques to enhance steganalysis accuracy. That will produce another steganalysis category depending on the embedding domain (LSB matching steganalysis, LSB embedding steganalysis, Transform domain steganography steganalysis, etc.) [16].

On the other hand, *universal* statistical steganalysis does not target any special steganography techniques. It mainly depends on the concept of learning and training to find out suitable sensitive statistical features with 'distinguishing' capabilities. These features are then used to build a learning model for machine learning and neural networks [41].

3.1.3. Deep Steganalysis

We named this category deep steganalysis due to the concept of deep features. Recently, neural networks became a trend in both deep learning and classification tasks due to their accuracy and ability to enable deep understanding to obtain higher robustness and effectiveness for semantics representation. Deep steganalysis is like *universal* statistical steganalysis in terms of not depending on the embedding steganography techniques, but the difference is that the first one extracts deep features while the last extracts hand-crafted features, respectively. However, this method is still recent and needs more investigation.

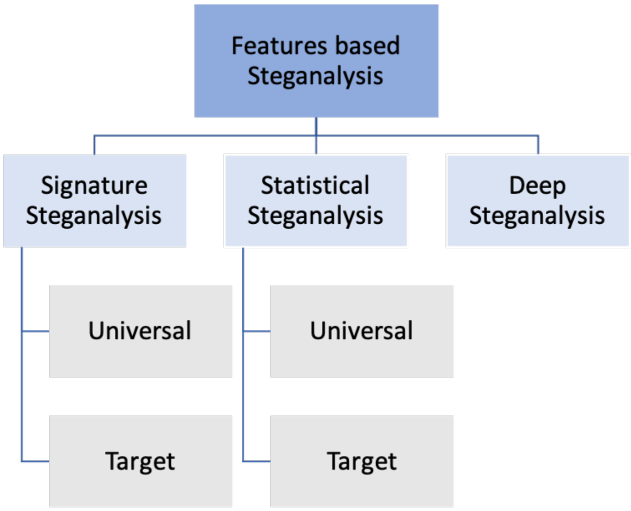

Figure 6. The classification of steganography techniques based on features.

3.2. *Classification*

After feature extraction, the classification step is performed which generally includes three methods, statistical strategy method, machine learning method, deep learning method. The steganalysis techniques start detecting the stego-medium by comparing the features of the cover and stego mediums in the case of the *targeted* techniques. The other way was to use a statistical strategy such as a threshold, so the stego medium is detected if the extracted features exceed or are below it. Emerging of Artificial Intelligence (AI) including pattern recognition, machine learning, deep learning, etc., opened the door for researchers to exploit their advantages in steganalysis. There are many existing techniques based on machine learning, while deep learning is still a new area in this field. [25]. The steganalysis techniques based on the classification method would be classified as presented in the following subsections.

3.2.1. Statistical Strategy-Based Techniques

In this type, the steganalysis techniques rely on statistical methods such as comparing the result of the detection with an empirical threshold. Hence, after extracting the features which are commonly statistic features like mean, variance, histogram, etc., an empirical threshold is used to distinguish the cover-steg-mediums [42,43].

3.2.2. Machine Learning-Based Techniques

There are two methods for machine learning: supervised and unsupervised learning. Supervised learning is referred also to as “semi-blind”, this method needs the cover- and stego-medium to build a training model that is used for detection in the test phase. The most popular classifier under this method is Support Vector Machine (SVM) which was applied in many steganalysis techniques. The typical scheme of supervised machine learning classifiers is presented in Figure 7. On another side, unsupervised learning which is referred also to as “blind”, only needs the cover-medium to detect the stego-medium using clustering methods such as K means.

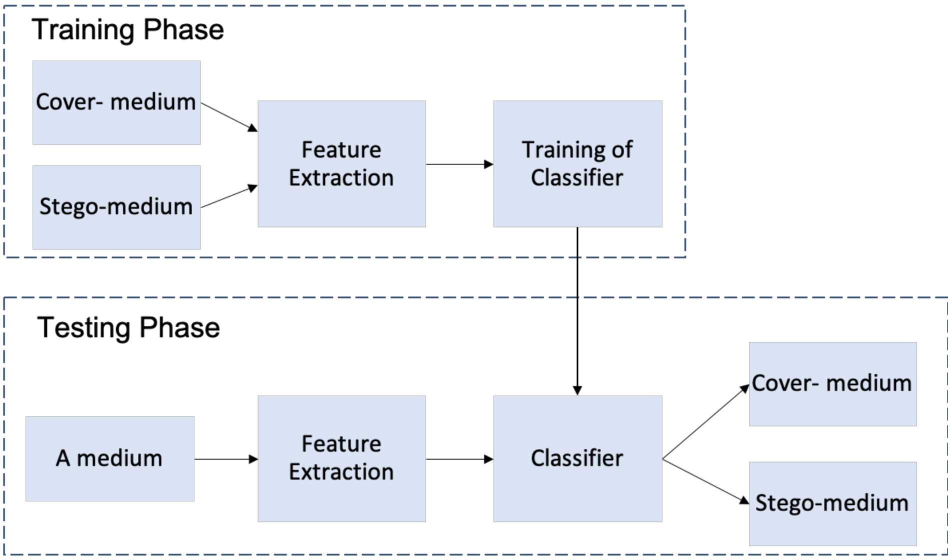

Figure 7. The typical scheme of supervised machine learning algorithms.

3.2.3. Deep Learning-Based Techniques

Deep learning is a subfield of machine learning and, recently, the deep learning concept is applied in steganalysis. Neural Networks (NN) such as Deep Neural Networks (DNN), Convolution Neural Networks (CNN), etc. are able to automatically extract the features and detect the stego-mediums. This area is still new where few techniques have used CNN in the steganalysis domain. Figure 8 present the CNN deep learning framework. The CNN contains various hierarchical layers such as the conventional layer, pooling layer, and fully connected layer. The conventional layer contains filters and is responsible for feature extraction. In the filtering layer, the down-sampling operation is performed to decrease the learnable parameters. Finally, the final features of the last layer are flattened and fed to one or more fully connected layers to get the classification as a final output [44].

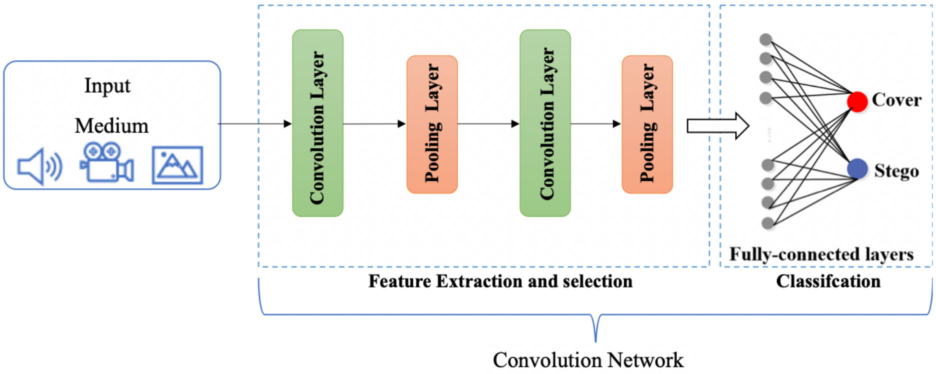

Figure 8. Basic Architecture of CNN Framework.

4. Literature Review

Digital image steganalysis algorithms focus on the dependencies of inter-pixels, which is the foundation of natural images. While digital audio steganalysis algorithms are based on the file's characteristic aspects such as the audio signal's distortion measure and its high-order statistics. Steganalysis algorithms for digital video target the "spatial and temporal redundancies in the video signals within the individual frames and at inter-frame level" [45]. In this section, the recent state-of-the-art regarding the steganalysis techniques for digital video, image, and audio are reviewed. At the end of each section a summary is provided in Table 3 for audio steganalysis, Table 4 for image steganalysis, and Table 5 for video steganalysis.

Table 3. Comparison of state-of-the-art in audio steganalysis.

Ref.	Year	Type of Features	Detection Method	Database	Steganography Technique	Advantage	Limitation
[46]	2017	Hand crafted Statistical (Markov features)	Machine learning SVM	Unknown dataset consists of 1000 stereo WAV audios	MP3Stego steganography.	Detecting low embedding-rate in the MP3 audios	Time consumption for the feature construction phase.
[47]	2020	Hand crafted Statistical (Multi-scale correlations measure for QMDCT coefficients)	Machine learning (ensemble classifier)	General dataset consists of 10,000 mp3 files with 10 s duration.	Different steganography techniques includes HCM, MP3Stego, and EECS	good performance in several MP3 steganography algorithms, bitrates, duration, and relative payloads.	High dimensionality
[48]	2017	Hand crafted Statistical (Markov features)	Machine learning SVM	Two datasets consist of 4169 wave music clips and 1029 speech wave files.	Different steganography techniques includes LSB, SS, DCT, and others	High accuracy detection against target and universal techniques	The detection accuracy decreases in the low embedding rate for speech datasets in most of the cases.
[49]	2018	Hand crafted Statistical (LP features)	Machine learning SVM	General datasets consist of 2000 WAV files with rate of 44.1 kHz.	Different steganography techniques includes Hide4PGP,S-Tools, StegoMagic, and Xiao	High accuracy detection for high embedding ratio	The accuracy detection for low embedding ratio not sufficient comparing with high embedding
[50]	2019	Deep features using CNN	Fully connected Layer (softmax)	A dataset cotains 6300 mono WAV files with rate of 16 kHz.	LSB matching and STC steganography techniques	Improving the architecture of CNN to enhance the detection performance.	Moderate detection accuracy for low embedding rate
[51]	2019	Deep features using (S-ResNet)	Machine learning SVM	Two datasets cotain 10,000 with 16-kHz rate and (2 s) duration in AAC format, and 9000 with 44.1 kHz rate and (5 s) duration in mp3 format	Different steganography techniques includes LSB, MIN, SIGN, and MP3Stego	High detection accuracy	High dimensionality

Table 4. Comparison of state-of-the-art in image steganalysis.

Ref.	Year	Type of Features	Detection Method	Database	Steganography Technique	Advantage	Limitation
[52]	2018	Hand crafted Statistical feature (color correlativity)	Machine learning SVM	UW image database consisting of 1333 images	LSB flipping image steganography.	High efficiency with single dimension analysis	Low detection accuracy in case the low embedding rates
[53]	2017	Statistical feature (variance)	Hand crafted Statistical strategy	BossBase image database	SS steganography.	Fast and low computation complexity comparing with [54]	The extraction performance decrease with high embedding distortion.
[55]	2019	Hand crafted Statistical feature (histograms of SE)	Machine learning SVM	DBLST and BIVC database	Different steganography techniques including distortion-based, pattern-based, and others.	Simple and high performance	Not taking in to account the frequencies of different SEs patterns.
[56]	2018	Hand crafted Statistical feature (Zipf's law in the wavelet transform)	Machine learning RF	UCID database	Different steganography techniques including spatial-based, transform-based.	Adapting new and effective statistical law for extracting features in the wavelet transform domain	The pre-processing steps before features extraction may produced high execution time.
[57]	2019	Hand crafted Statistical features from transform and spatial domains)	Machine learning CIML	BSD300 dataset contains 150 JPEG images	Different steganography techniques including distortion-based, spatial-based, and others.	Low computation complexity, low time consumption, and high performance	Small dataset
[58]	2018	Deep features from spatial domain using DRN	Fully connected layer (softmax classifier)	BOSSbase dataset contains 10,000 images	Spatial UNIversal WAvelet Relative Distortion (S-UNIWARD) steganography.	High detection accuracy	High computation complexity
[59]	2020	Deep features from spatial and transform domains using CNN	Fully connected layer (softmax classifier)	BOSSbase dataset contains 10,000 images	Spatial UNIversal WAvelet Relative Distortion (S-UNIWARD) and Wavelet Obtained Weights steganography.	Considering the spatial and transform domains to increase the accuracy	An ordinary accuracy although the high computational complexity

Table 5. Comparison of state-of-the-arts in Video steganalysis.

Ref.	Year	Type of Features	Detection Method	Database	Steganography Technique	Advantage	Limitation
[60]	2017	Hand crafted features NPELO (36-dimensional) + MVRBR	Machine learning (SVM)	Contains 100 YUV sequences (H.264/AVC standard), each sequence has 150 to 300 frames	MV steganography	Takes into account the motion characteristic of video content.	Uses small datasets
[61]	2018	Hand crafted features (entropy,motion, and statistic features)	Machine learning (SVM)	284 uncompressed video (H.264/AVC standard) from internet	MV steganography	The detection accuracy does not affect by the bit rate variations	Their experiment limited and can not detect the currently best steganography methods
[62]	2017	Hand crafted features (motion intensity and texture histograms)	Machine learning (SVM)	Contains 14 YUV sequences (H.264/AVC standard), only the first 90 frames from each sequences	SS steganography	Exploit the videos spatial and temporal redundancies simultaneously	Uses small datasets
[63]	2019	Hand crafted features (statistic change in distribution of the PU)	Machine learning (SVM)	33 videos each contains 80 frames in 720P and 30 videos each contains 50 frames in 1080P (HEVC standard), only the first 90 frames from each sequences	PU partition modes steganography	Exploit the videos spatial and temporal redundancies simultaneously	Considering as a *targeted* steganalysis technique
[64]	2020	Hand crafted features (statistical features of inter-frame and intra-frame)	mMchine learning (SVM)	22 PAL QCIf video dataset (H.264/AVC standard)	MV steganography	Blind steganalysis technique and can be adjusted to various video codec standards.	computational complexity due to the high dimensionality of features
[65]	2020	Deep features (steganographic noise residual features) using CNN	Fully connected Layer(softmax classifier)	Unknown dataset contains (200,000 frames for training and testing	MV and Intra Prediction Mode steganography	Universal steganalysis technique	Did not taking into account the temporal domain.
[66]	2020	Deep features (512-dimensional) using CNN	Fully connected Layer (softmax classifier)	Xiph Video Test Media database(HEVC standard)	MV steganography	Extract deep features and estimates the embedding rate	Extract the features from fixed-size block motion estimation

4.1. Audio Steganalysis

The goal of audio steganalysis is to detect any change in a signal due to embedding data. There are two main domains for embedding the data, either use a spatial or sometimes a "time" or "temporal" domain and that mostly happened by changing the least significant bit (LSB) of a data sample in the audio file, or in the transform domain by modifying different parameters of the signal. In the addition, the audio steganalysis is classified based on format into steganalysis techniques for compressed formats such as MP3 and AAC, and steganalysis techniques for non-compressed formats [24]. Regarding the compressed formats, Jin et al. [48] proposed a target steganalysis technique for detecting MP3Stego steganography. The authors noticed that the MP3Stego alters the quantized modified discrete cosine transform QMDCT coefficients during compression which impacts the correlations between neighboring QMDCTs of audio cover. Therefore, Markov features are extracted from cover and stego audio to describe the correlations of the QMDCTs. These features are then crossed through pre-processing steps to select the optimal features to train an SVM classifier. According to the experiments, the proposed technique achieves high detection accuracy in the case of a low embedding rate.

Another steganalysis technique for Mp3 is proposed by Wang et al. [47], where the QMDCT coefficient matrix of MP3 is calculated to extract the steganalytic features. The rich high-pass filtering was applied to increase the sensitiveness of their technique against noise signals. The authors claimed that the replacement of one QMDCT coefficient results in the changing of one Huffman codeword. For this reason, they suggested a correlations measure module to detect any possible modification in the QMDCT coefficients matrix at pointwise, 2 × 2 block-wise, and 4 × 4 block-wise, separately. To reduce the dimension of the features and select the optimal one, an empirical threshold was applied. For the classification task, the ensemble classifier [67] was trained.

For non-compressed formats, it includes two methods: the collaborated method and the non-collaborated method. In the first method, the techniques depend on the comparison between the estimated cover signal and the stego signal. There are many ways to estimate the cover including denoising based, liner bases of cover, re-embedding, and others. However, the estimation of the stego signal for calibration is also possible, which is applied by Ghasemzadeh et al. [46], where the authors proposed a universal steganalysis technique based on calibration. In their technique, the re-embedding method was used to embed the signal with a random message. The energy features were extracted, where each signal and re-embedded signal are segmented into many chunks and calculated the energy for each. Then, the energy of each chunk from the signal and its re-embedded counterpart is subtracted. Finally, the statistical properties of the energy features, including mean, skewness, standard deviation, and kurtosis, are selected to train the SVM classifier. Their technique has been evaluated using a wide range of various steganography techniques. The experimental results showed its effectiveness in detection in the targeted and universal cases.

On the other hand, the non-collaborated method extracts the features directly from the audio signal according to the embedding feature domain. Han et al. [49] suggested a linear prediction method, where linear prediction LP features are extracted from the segmented audio file. According to the experiments, the authors found that the LP can significantly distinguish between the cover and the stego. Therefore, the LP coefficients, LP residual, LP spectrum, and LP cepstrum coefficients features are extracted from the time domain and the frequency domain. The SVM classifier was trained based on the extracted features from cover- and stego-signals. A wide range of experiments are conducted with various ratio embedding and are tested against different steganography techniques. The results proved the effectiveness of the proposed techniques compared with popular and recent steganalysis techniques, where above 96% accuracy is achieved.

Recently, deep learning has attracted more attention and has achieved superior results in the steganalysis field. Lin et al [50] proposed an improved method based on CNN to detect the audio steganalysis in the time domain. At first, a High-Pass Filter layer is used to extract the residual signal from the input audio. Then the hierarchical representations of the input are obtained using six various sets of layers, where the first set contains only the activation of the first convolutional layer and the remaining sets contain a convolutional layer and a pooling layer. After each convolution operation, the non-linear activation is applied. By the end of these layers, the audio signal is transformed into 215-features. To detect the steganography, the extracted features are fed into the binary classifier that contains a softmax layer and a fully connected layer. This approach proved its effectiveness at detecting different embedding rates.

Ren et al. [51] proposed a universal steganalysis technique where a ResNet is applied for the features extraction. The spectrogram of the audio signal was used as input for the neural network, called the Spectrogram Deep Residual Network (S-ResNet). Figure 9 illustrates how the spectrogram can represent the energy information of various frequency bands over time as well as consisting of valuable time-frequency information in the audio signal. For this reason, the authors attempted to use it for capturing relative features produced by the audio steganography technique. The architecture of S-ResNet contains 31 convolutional layers between the batch normalization and ReLU layers, for accelerating the learning process and learning more complex patterns, respectively. After each group of convolutional layers, there is a residual unit to compute a residual function. Two average pooling layers are applied to decrease the data size after every five residual blocks. Finally, a global average pooling layer is applied to produce the feature vector. After the S-ResNe trained an efficient model, this model is fed to an SVM for final training and binary classification. The experiment's results show superior detection, where the average accuracy is 94.98% and 99.93% for both AAC and MP3 formats, respectively.

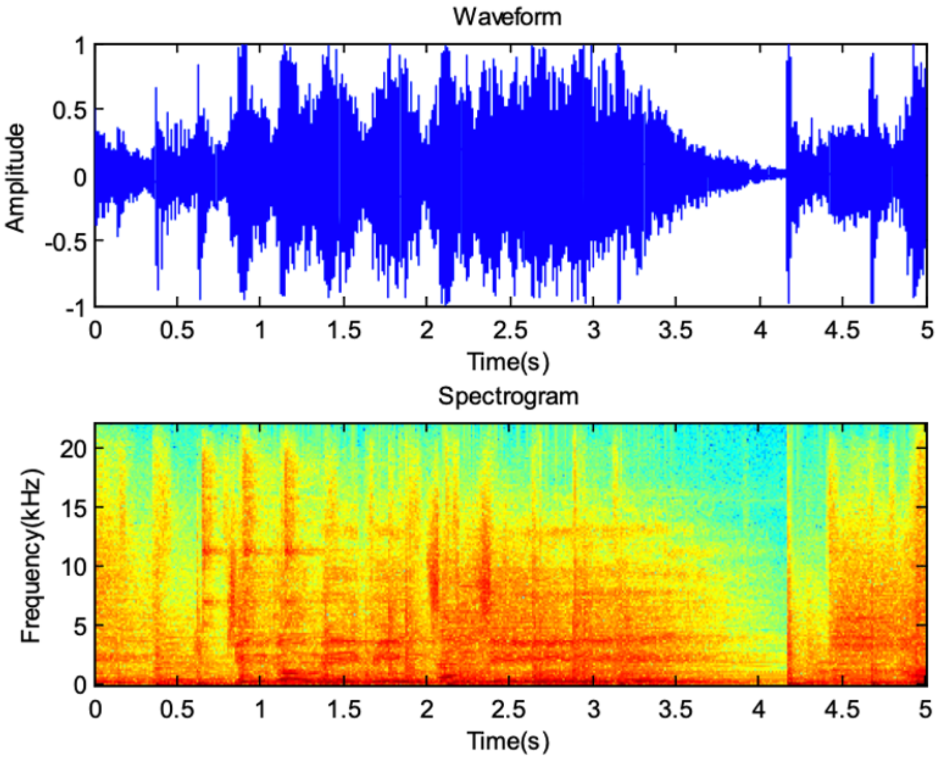

Figure 9. Wave-form and spectrogram representation for an audio segment [51].

4.2. Image Steganalysis

The history of image steganalysis starts in the late twentieth century, with the first studies proposed by Johnson and Jajodia [68] and Chandramouli et al. [69]. Image steganalysis has cut a long way starting with visual steganalysis and manual features extraction up to use deep learning and automatic feature extraction.

In the beginning, the researchers tried to find a signature or pattern to detect specific well-known steganographic techniques [68]; however, this type has only limited applications. With the evolution and variety of steganography techniques, robust steganalysis techniques became more necessary. Many steganalysis techniques started to extract statistical features that can reflect invisible changes in the digital medium. As an example, Chaeikar et al. [52] proposed a blind statistical steganalysis technique for detecting the Least Significant Bit (LSB) flipping image steganography. The authors found that the natural color harmony of the pixel is affected when embedding the data. Hence, a statistical feature that analyses the color correlativity is extracted from the image pixels to detect the existence of the secret message. At first, the pixels were classified into three classes depending on the color similarity with the neighboring pixels, and the level of suspiciousness of pixels was identified according to the mean and standard deviation. That leads to a dataset used to train SVM for detecting and estimating the embedded message length.

Another blind image steganalysis is proposed by Soltanian and Ghaemmaghami [53] to detect the spread spectrum steganography. The core of their method is to discover the carrier and stego message matrices using a well-known least-squares method. The carrier matrix is randomly initialized, then the carrier and message matrices are updated based on a univariate gradient descent method. Their technique is based on the work of Li et al. [54], where the aim is to reduce the computation complexity and to rely on no prior knowledge about the number of spread spectrum carriers. Therefore, the proposed technique consecutively extracts the data bits of each carrier by extracting the variance to reduce the computational cost. To detect and estimate the number of embedded messages without prior knowledge, the proposed technique intends to reach the disturbance of the residual stego-image to a minimum by reducing the variance of the residual stego-image.

A statistical model based on a histogram of pixel structuring elements is proposed by Lu et al. [55]. This model is developed to extract the steganography in binary images, where the image contains only two values (0 and 1) unlike color and grayscale images. The histograms are computed for all structure elements (SE) in the image; Figure 10 represents how large SE can contain several neighboring small SEs. Then, only the bins of SEs that have a high probability of flippable pixels are selected as a feature set using an empirical threshold. The SVM classifier is used to detect the stego-image. In addition, the authors create available datasets for binary images called DBLST. The DBLST and the open BIVC dataset are used for experiments which show that the proposed technique outperforms the state-of-the-art techniques in detecting different types of stego images.

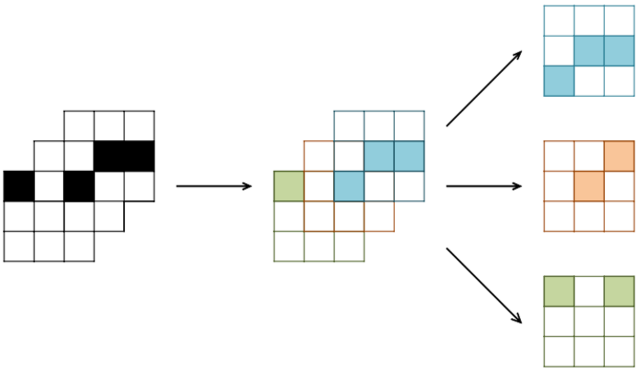

Figure 10. A large SE can be considered a union of various neighboring small SEs [55].

Laimeche et al. [56] proposed a universal steganalysis technique, where Zipf's law [70] is exploited to extract the features in the wavelet transform. The basic idea of Zipf's law in image representation includes three phases. The first phase is a mask size for counting the frequency of patterns appearance. The second phase is to minimize the number of patterns by identifying significant wavelet coefficients, this leads to a more significant distribution for pattern frequency. In the third phase, the Zipf curve, is produced, which represents the pattern frequency and the number of pattern axes. Finally, Area under the Curve of

Zipf, Inflection Point, and Subband Auto-Similarity Metric) features are extracted from the produced Zipf curve. To detect the stego images, the random forest classifier is trained using the UCID dataset.

A novel steganalysis technique that aims to reduce the computation and time consumption along with high performance is proposed by Guttikonda and Sridevi [57]. Each Coefficient based Walsh Hadamard Transform and Gray Level Co-occurrence Matrix is used to extract the features from the transform and spatial domains, respectively. To reduce the feature dimensionality and select the most relevant features, the Pine Growth Optimization algorithm was applied. Finally, the selected features are used to train the Cross Integrated Machine Learning classifier to distinguish the cover- and stego-images. The experiment's results showed the effectiveness of the proposed technique in terms of detection accuracy and the execution time, where it reduced the time by about 0.66 compared with the existing Multi-SVM technique.

Very deep learning and automatic feature extraction are applied in the work of Wu et al. [58]. Specifically, a novel CNN model called Deep Residual learning Network (DRN) is proposed for image steganalysis. The authors have proved that the very deep neural network that contains many layers can reflect complex statistical properties, which leads to more effective distinguishing the stego-images. The main idea of their technique is to feed the network with noise components of the image, instead of the original image to force the network to consider the weak signal produced by data embedding. Thereafter, DRN is trained to learn the effective features of cover- and stego-images. For the binary classification, a fully connected layer with a softmax classifier was performed. The experimental results conducted using the BOSSbase dataset showed the superiority of the proposed technique compared with other deep neural networks-based techniques.

Another deep neural network-based technique that extracts features from multi-domains is proposed by Wang et al. [59]. Firstly, two famous steganalysis methods are simulated which are spatial rich model SRM and DCT residual for detecting the steganography features in both spatial and transform domains. In the next step, the previous linear features with nonlinear SRM features are fed to the CNN layer to extract general features. Finally, the fully connected layer is applied for stego- and cover-image classification. Through the experiments, the authors proved the effectiveness of considering the nonlinear features extraction as well as extracting features from multi-domains, where the detection accuracy is increased by 0.3~6% and 2~3%, respectively.

4.3. Video Steganalysis

The rapidity of the internet led to the wide usage of videos. Videos can be altered to send hidden messages, therefore detecting these changes are necessary. At first, the steganalysis techniques for images were straight utilized to detect the changes that produced from the embedded message. But since there is not change much between the successive frames in the video, these approaches did not produce good results. Therefore, there are significant differences between image steganalysis techniques and video steganalysis techniques. There are two main methods to detect the hidden messages in digital video, which are methods-based motion vectors field and methods-based inter-frame level. These methods have been utilized in videos in H.264/AVC standard and, newly, in HEVC standard.

Wang et al. [60] proposed a steganalytical technique based on motion vectors, taking the advantages of content variety. The video is divided into subclasses; each class contains frames with similar intensity. After that, the improved NPELO (Near-Perfect Estimation for Local Optimality) [71] and MVRBR (Motion Vector Reversion- Based steganalysis Revisited) [72] features were extracted from each class and fed to an independent SVM classifier. The independent classifiers were given different weights depending on the intensity amount of the frames, where the classifier of the high-intensity class has a higher weight. Finally, the integrated classifiers detect the video whether is cover or stego. The used database contains 100 YUV sequences, each sequence has 150 to 300 frames with

30 fps in CIF format. The database was addressed in the H.264/AVC standard by the ×264 tool.

Another steganalytical technique based on MV is proposed by Sadat et al. [61], where the entropy and motion estimation field is utilized for selecting the features. After dividing the frame into blocks, local optimization of the cost function is used to extract intrinsic and statistical features include the sum of absolute differences (SAD) and the sum of absolute transformed differences (SATD). Then all blocks have given weight depending on the amount of texture, where high textures gave a high weighted value in decision making during training of the SVM classifier. For evaluation, 284 video sequences have been used which were downloaded from the Internet. Their technique obtained high accuracy up to 99.9%.

Spatial and temporal motion features are considered simultaneously in the technique of Tasdemir et al. [62]. The frames are first divided into three-dimensional blocks (8 × 8 × temporal axis). Then, from each block, three histograms are computed for the three dimensions, then the motion and texture features are extracted. After calculating these features, the blocks are categorized into three classes, where the first-class contains the blocks in which its features remained unchanged; the second-class contains the blocks with slight changes, and the third-class includes the blocks containing a large change. Each class is given a weight value that is identified empirically. For the classification task, the comprehensive presentation of the spatiotemporal features and the weighted modulation are fed to the SVM for training. The used database contains 14 YUV sequences; only the first 90 frames of each sequence are used for the experiments. The database was addressed in the MPEG2 and H.264 formats standard. The authors have proved that using spatial and temporal simultaneously can increase detection accuracy by 20 % and 5% in low and high payloads, respectively, compared with seven different steganalysis techniques.

Recently, Li et al. [63] proposed a steganalytical technique for HEVC video steganography. The frame in the HEVC standard can divide into the same size code tree unit (CTU). In the addition, CTU can divide into smaller code units (CU), each CU can further divide into a transform unit (TU) and prediction unit (PU) as illustrated in Figure 11. Their technique is based on the fact the PU partition modes would be changed after embedding the data. Hence, they selected the rate of change of PU partition modes in the cover- and stego-video as features. These features are the input for the SVM classifier. According to the experiment, the detection accuracy reaches approximately 93%.

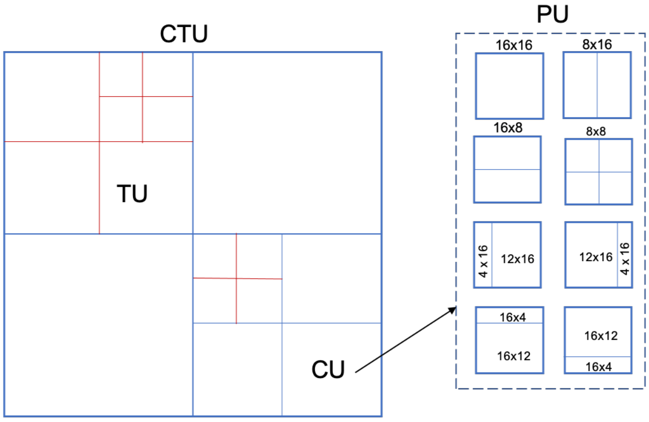

Figure 11. The partition CTU and PU in HEVC standard.

Ghamsarian et al. [64] proposed a blind technique to detect many types of MV steganography. A novel feature called MVs' Spatio-Temporal features termed (MVST) is proposed where consists of 36 and 18 spatial and temporal feature sets, respectively. The features are extracted from the various partitions of H.264/AVC standard instead of a fixed size of blocks. For computing the detection accuracy of the proposed technique, the SVM classifier is utilized in four situations. One of them is a real-world situation where the technique does not have any information regarding the steganography techniques and the embedding rate. The experiment result on the 22 PAL QCIf video dataset showed the stability and high detection accuracy reach 95% in a real-world situation.

The first universal steganalysis technique based on deep learning was proposed by Liu and Li [65]. The proposed noise residual feature has arisen from the fact of the intra-prediction mode and motion vector steganography techniques affect the pixel values of the decoded frames. Therefore, the authors developed an NR-CNN framework to extract features from noise residuals and learn the steganographic noise residual features that are independent of the content of the frame. The fully connected layer and softmax classifier are used for binary classification. The experimental dataset was contained 200,000 frames for training, 20,000 for verification, and 200,000 frames for testing. The experiments demonstrated satisfying results regarding low embedding rate, and high performance in the case of a high embedding rate with 59.82% and 99.74% detection accuracy for intra prediction, respectively, and 62.53% and 95.39% detection accuracy for MV, respectively.

Huang et al. [66] proposed the first deep learning-based video quantitative steganalysis technique. The features are extracted from 4 × 4 PU of each frame since it is the most basic unit in the HEVC video standard. To ensure the robustness of the neural network against low and high bitrates that exist in the same video, each of the motion vectors and the prediction matrices has been calculated, respectively, for each 4 × 4 PU. These matrices are fed to CNN, which is consequently, extracts a 512-dimensional feature vector and submits it to the last fully connected layer. The softmax classifier is used to detect the stego-video and estimate the bitrate. The experimental results on the Xiph Video Test Media database demonstrated that the proposed techniques can estimate different embedding rates with low mean absolute error MAE.

5. Databases

A standard database is necessary to evaluate and compare the results of the existing techniques. In this section, we review the existing datasets used for evaluation. Table 6 provides a minor description for the existing global trusted datasets. It is clear that there are few public datasets for audio steganalysis, while most are for image steganalysis. However, the ASD and ASDIIE datasets are provided recently which will inspire many researchers in audio steganalysis. On the other hand, currently there is no available standard dataset for video steganalysis. As in the audio steganalysis field, the researchers in video steganalysis use their own datasets to evaluate, which leads to unfair comparisons.

Table 6. The available datasets in the Steganalysis Field.

Name	Media Type	Description	Availability
BOSSBase V1.01 [73]	Image	No. of images: 10,000, Format: Portable Gray Map (PGM) of 8 bits, Size: 512 × 512	Public
BOWS2 [74]	Image	No. of images: 10,000, Format: PGM of 8 bits, Size: 512 × 512	Public
ImageNet [75]	Image	No. of images:more than 14 million, Format: mostly JPEG, Size: different sizes	Public
Stegoappdb [76]	image	No. of images: 960,000, Format:DNG and JPEG, Size: different sizes	Public
Corel [77]	Image	No. of images: 10,800, Format: DNG and JPEG, Size: different sizes	Public
USC-SIPI [78]	Image and video	No. of images: 237 and 96 in 4 sequences, Format: TIFF, Size: different sizes	Public
Audio Steganalysis Dataset IIE (ASDIIE) [1]	Audio	No. of clips: 22,671, Format:WAV with a sampling rate of 44.1 kHz and duration of 10 s	Public
Audio Steganalysis Dataset [79]	Audio	No. of clips: 33,038, Format: MP3-WAV, Sampling rate: 44.1 kHz, Duration: 10 s	Public
Speech dataset [80]	Audio	No. of clips: 320 Chinese and English speech, Format: PCM	Public

[1] Available in: https://ieee-dataport.org/documents/audio-steganalysis-dataset#files, accessed on 11 October 2021.

6. Evaluation metrics

The steganalysis approach always produces binary classification classes (cover and stego), so the accuracy, detection rate, and error rate metrics are enough to evaluate the steganalysis techniques. Given the following:

- tp: stego-media classified as stego-media
- tn: cover-media classified as cover-media
- fp: stego-media classified as cover-media
- fn: cover-media classified as stego-media

Then:

$$\text{Accuracy} = (tp + tn)/all$$
$$\text{DetectionRate (TRP)} = tp/(tp + fn)$$
$$\text{ErrorRate (FPR)} = fp/(fp + tp)$$

In addition, the ROC curve is mostly used to evaluate and compare the classification task of many steganalysis techniques. It presents the True Positive Rate with respect to the False Positive Rate, where FPR = 0 and TPR = 1 indicates a perfect detector.

7. Digital Multimedia Steganalysis Tools

There are various software tools that exist which allow easy detection the hidden data in digital multimedia [45]. Most of them are targeting well-known steganography techniques. Although most of the researchers focused on steganalysis methods, few papers are focused to evaluate the existing steganalysis tools [45,81]. However, a comparison between some of the popular steganalysis tools is provided in paper [45].

Table 7 summarizes the most popular existing steganalysis tools for digital media: audio, image, and video. As illustrated in the table, most of the steganalysis tools are designed for detecting the hidden data in images, while a few tools deal with video and audio mediums.

Table 7. The Existing Steganalysis Tools.

Software	Producer	Platform	Medium Type	Availability
StegSpy [82]	SpyHunter	Windows	Image	Freeware
StegDetect [83]	Niels Provos	Linux, windwos	Image	Freeware
StegSecret [84]	Alfonso Muñoz	Java-based	Image, Audio, Video	Freeware
StegoHunt [85]	WetStone Technologies	Windows	Image, Audio, Video	License purchase
StegExpose [86]	Benedikt Boehm	Java-based	image	Freeware
StegAlyzerAS [87]	Backbone Security	Windows	Image	License purchase
StegalyzerSS [88]	Backbone Security	Windows	Image	License purchase
StegAlyzerFS [89]	Backbone Security	Windows, Linux, Apple OS	Image, Audio, Video	License purchase
VSL [90]	Michal Wegrzyn	Java-based	Image	Freeware

8. Perspectives and Open Issues

In this section, we will discuss the existing status in this domain and present some open issues that need to take into consideration in future works.

- **Standard dataset:** For an easier and fair comparison between the published steganalysis techniques, it is necessary to use a standard and fixed dataset. In image steganalysis, there are standard databases where the most popular are BOSSbase and BOWS2 databases. On the other hand, audio steganalysis was until recent lacked for the standard dataset, where the researchers generated their own datasets. Fortunately, a public dataset for audio steganalysis was generated for WAV, mp3 formats. However, still there is a need for developing a unified and public dataset for video and other formats for audio steganalysis.
- **Practical steganalysis techniques:** Computation complexity and time consumption are two significant terms that should be considered when developing practical ste-

ganalysis techniques. Most of the existing techniques give attention to accuracy detection regardless of the complexity of the computation.
Nowadays, the emerging of machines and deep learning opens a new horizon for faster and more accurate detection. Although of their advantages, many issues should be taken into consecration such as avoiding the complexity of the training phase, adjusting and fixing well hyperparameters before training, and avoid overfitting.

- **Virtual and online services:** The digital technology era increased the chances for criminals to exploit new unsuspicious spots for hiding such as online games, cloud storage systems, and the virtual world. Steganalysis techniques for these network traffic services should be developed.
- **Balancing:** There is a clear unbalancing in this domain, starting with the proposed steganography and steganalysis techniques. As illustrating in Figure 12, there is a big gap between the number of published steganography and steganlysis techniques. This gap back to the difficulty and obstecals that faced by researcher and forensic expertsin the steganalysis field. So, there is highly needed for more investigation and work from dedicated and adept researchers in steganalysis domain.
Regarding medium based steganalysis, image steganalysis, then audio, receives more attention from the researcher than video steganalysis. However, researchers have shown that by 2021, video traffic will consume 82% of all traffic of the Internet [61]. Besides that, the video medium provides sufficient space for hiding data which makes the video medium a good scope to exploited by steganography technique. So, video steganalysis should attract more attention from the researchers.
In addition, the researchers focus on some formats more than others. For example, in audio steganalysis, most of the existing techniques are proposed for mp3 format, especially for Mp3stego steganography. Among these techniques, LSB techniques have the biggest share, where the non-LSB techniques need to more investigate [16].
- **General steganalysis technique:** Most of the existing steganlysis techniques relied on the training dataset to make the classifier learns and trains on the representation of cover and stego medium (semi-blind) or only cover medium (blind). Hence, there a high relation between classification accuracy and training datasets, where mostly the accuracy reduces as the testing dataset differs from the training dataset. Indeed, most of the existing techniques are belong to the *semi-blind* approach.
In the real world, there are thousands of steganography techniques and different types of cover contents, size, noise, and sampling frequency, etc. This amount of training datasets especially for stego- mediums makes it impossible to restrict them. There are a few techniques that exploit the unsupervised approach to deal with this issue [91], but still, the accuracy needs to be improved.
- **Keeping up:** The steganalyser should be keeping up with the new trends related to steganography and steganalysis domain. For instance, the recent formats as H.265/HEVC will be highly exploited for steganography, since it contains various advanced features.
IoT (Internet of Things) has been utilized by a few researchers for the transfer and storage of data hidden using steganography. So, there is a big chance to used by criminals for hiding the secret data [25].
Last but not least, the steganalysis techniques deal with digital medium audio, image, and video separately. However, the video file normally contains video coding format alongside audio data in an audio coding format. The sound-video or audio-video provides a high capacity for embedding secret data for the criminal. Although there are few steganography techniques in this regard [92–94], no steganalysis technique available till date. However, the existing image and audio steganalysis could detect that type of steganography, but there are no experiments for evaluation.

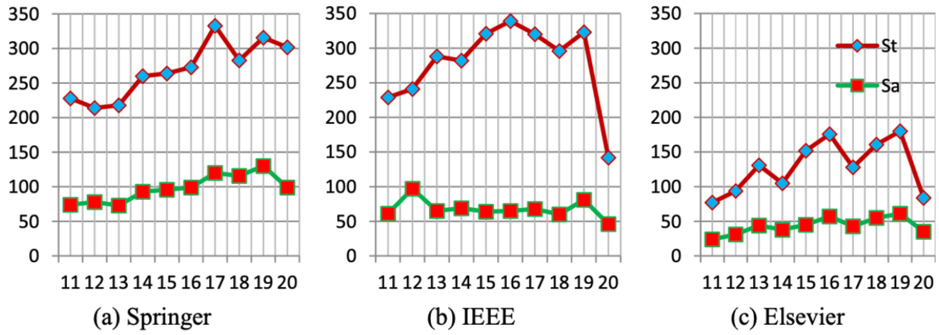

Figure 12. Frequency of published steganography and steganalysis research articles throughout the years. Where St : steganography and Sa: steganalysis. Taken from [25].

9. Conclusions

This survey provided an overview of the basic concepts of steganography and steganalysis and their classification. In addition, a comprehensive review of the recent research on steganalysis techniques for *audio*, *image*, and *video* mediums was provided in detail. The applications, datasets, and popular tools available for steganalysis were mentioned. In the end, this survey discussed the main shortcomings in this domain and suggested some future recommendations.

Author Contributions: Conceptualization, M.J.A.; methodology, D.A.S. writing—original draft preparation, D.A.S.; writing—review and editing, D.A.S. and M.J.A.; visualization, D.A.S.; supervision, M.J.A. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Acknowledgments: This project was funded by the Deanship of Scientific Research (DSR) at King Abdulaziz University, Jeddah. The authors, therefore, acknowledge with thanks DSR for technical and financial support.

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

References

1. Kadhim, I.J.; Premaratne, P.; Vial, P.J.; Halloran, B. Comprehensive survey of image steganography: Techniques, Evaluations, and trends in future research. *Neurocomputing* **2019**, *335*, 299–326. [CrossRef]
2. Abikoye, O.C.; Ojo, U.A.; Awotunde, J.B.; Ogundokun, R.O. A safe and secured iris template using steganography and cryptography. *Multimed. Tools Appl.* **2020**, *79*, 23483–23506. [CrossRef]
3. Petitcolas, F.A.; Katzenbeisser, S. *Information Hiding Techniques for Steganography and Digital Watermarking (Artech House Computer Security Series)*; Artech House: Norwood, MA, USA, 2000.
4. Kahn, D. The history of steganography. In *International Workshop on Information Hiding*; Springer: Berlin/Heidelberg, Germany, 1996; pp. 1–5.
5. Cheddad, A.; Condell, J.; Curran, K.; Mc Kevitt, P. Digital image steganography: Survey and analysis of current methods. *Signal Process.* **2010**, *90*, 727–752. [CrossRef]
6. Liao, X.; Yu, Y.; Li, B.; Li, Z.; Qin, Z. A new payload partition strategy in color image steganography. *IEEE Trans. Circuits Syst. Video Technol.* **2019**, *30*, 685–696. [CrossRef]
7. Saravanan, M.; Priya, A. An Algorithm for Security Enhancement in Image Transmission Using Steganography. *J. Inst. Electron. Comput.* **2019**, *1*, 1–8. [CrossRef]
8. Yi, X.; Yang, K.; Zhao, X.; Wang, Y.; Yu, H. AHCM: Adaptive Huffman code mapping for audio steganography based on psychoacoustic model. *IEEE Trans. Inf. Forensics Secur.* **2019**, *14*, 2217–2231. [CrossRef]
9. Rout, H.; Mishra, B.K. Pros and cons of cryptography, steganography and perturbation techniques. *IOSR J. Electron. Commun. Eng.* **2014**, 76–81.
10. CNN. Documents Reveal al Qaeda’s Plans for Seizing Cruise Ships, Carnage in Europe. 2012. Available online: https://edition.cnn.com/2012/04/30/world/al-qaeda-documents-future/index.html (accessed on 5 October 2021).
11. Zielińska, E.; Mazurczyk, W.; Szczypiorski, K. Trends in steganography. *Commun. ACM* **2014**, *57*, 86–95. [CrossRef]

12. Trend Micro. Spam Campaign Targets Japan, Uses Steganography to Deliver the BEBLOH Banking Trojan. 2018. Available online: https://www.trendmicro.com/vinfo/nz/security/news/cybercrime-and-digital-threats/spam-campaign-targets-japan-uses-steganography-to-deliver-the-bebloh-banking-trojan (accessed on 5 October 2021).
13. Xiang, L.; Guo, G.; Yu, J.; Sheng, V.S.; Yang, P. A convolutional neural network-based linguistic steganalysis for synonym substitution steganography. *Math. Biosci. Eng.* **2020**, *17*, 1041–1058. [CrossRef] [PubMed]
14. Yousfi, Y.; Butora, J.; Fridrich, J.; Giboulot, Q. Breaking ALASKA: Color separation for steganalysis in JPEG domain. In Proceedings of the ACM Workshop on Information Hiding and Multimedia Security, Paris, France, 3–5 July 2019; pp. 138–149.
15. Yang, Z.; Yang, H.; Hu, Y.; Huang, Y.; Zhang, Y.J. Real-time steganalysis for stream media based on multi-channel convolutional sliding windows. *arXiv* **2019**, arXiv:1902.01286.
16. Karampidis, K.; Kavallieratou, E.; Papadourakis, G. A review of image steganalysis techniques for digital forensics. *J. Inf. Secur. Appl.* **2018**, *40*, 217–235. [CrossRef]
17. Banerjee, P. ALASKA2: Image Steganalysis—All You Need to Know. 2020. Available online: https://www.kaggle.com/prashant111/alaska2-image-steganalysis-all-you-need-to-know (accessed on 5 October 2021).
18. Ghasemzadeh, H.; Kayvanrad, M.H. Comprehensive review of audio steganalysis methods. *IET Signal Process.* **2018**, *12*, 673–687. [CrossRef]
19. Paulin, C.; Selouani, S.A.; Hervet, E. Audio steganalysis using deep belief networks. *Int. J. Speech Technol.* **2016**, *19*, 585–591. [CrossRef]
20. Amsaveni, A.; Vanathi, P. A comprehensive study on image steganography and steganalysis techniques. *Int. J. Inf. Commun. Technol.* **2015**, *7*, 406–424. [CrossRef]
21. Dalal, M.; Juneja, M. Video steganalysis to obstruct criminal activities for digital forensics: A survey. *Int. J. Electron. Secur. Digit. Forensics* **2018**, *10*, 338–355. [CrossRef]
22. Reinel, T.S.; Raul, R.P.; Gustavo, I. Deep learning applied to steganalysis of digital images: A systematic review. *IEEE Access* **2019**, *7*, 68970–68990. [CrossRef]
23. Chutani, S.; Goyal, A. A review of forensic approaches to digital image Steganalysis. *Multimed. Tools Appl.* **2019**, *78*, 18169–18204. [CrossRef]
24. Tabares-Soto, R.; Ramos-Pollán, R.; Isaza, G.; Orozco-Arias, S.; Ortíz, M.A.B.; Arteaga, H.B.A.; Rubio, A.M.; Grisales, J.A.A. Digital media steganalysis. In *Digital Media Steganography*; Elsevier: Amsterdam, The Netherlands, 2020; pp. 259–293.
25. Dalal, M.; Juneja, M. Steganography and Steganalysis (in digital forensics): A Cybersecurity guide. *Multimed. Tools Appl.* **2020**, *80*, 5723–5771. [CrossRef]
26. Ruan, F.; Zhang, X.; Zhu, D.; Xu, Z.; Wan, S.; Qi, L. Deep learning for real-time image steganalysis: A survey. *J. Real-Time Image Process.* **2020**, *17*, 149–160. [CrossRef]
27. Chaumont, M. Deep learning in steganography and steganalysis. In *Digital Media Steganography*; Elsevier: Amsterdam, The Netherlands, 2020; pp. 321–349.
28. Berthet, A.; Dugelay, J.L. A review of data preprocessing modules in digital image forensics methods using deep learning. In Proceedings of the 2020 IEEE International Conference on Visual Communications and Image Processing (VCIP), Macau, China, 1–4 December 2020; pp. 281–284.
29. Hussain, I.; Zeng, J.; Xinhong, X.; Tan, S. A survey on deep convolutional neural networks for image steganography and steganalysis. *KSII Trans. Internet Inf. Syst. (TIIS)* **2020**, *14*, 1228–1248.
30. Gokhale, A.; Mulay, P.; Pramod, D.; Kulkarni, R. A bibliometric analysis of digital image forensics. *Sci. Technol. Libr.* **2020**, *39*, 96–113. [CrossRef]
31. Selvaraj, A.; Ezhilarasan, A.; Wellington, S.L.J.; Sam, A.R. Digital image steganalysis: A survey on paradigm shift from machine learning to deep learning based techniques. *IET Image Process.* **2021**, *15*, 504–522. [CrossRef]
32. Alarood, A.A.S. Improved Steganalysis Technique Based on Least Significant BIT Using Artificial Neural Network for Mp3 Files. Ph.D. Thesis, Universiti Teknologi Malaysia, Skudai, Malaysia, 2017.
33. Alyousuf, F.Q.A.; Din, R.; Qasim, A.J. Analysis review on spatial and transform domain technique in digital steganography. *Bull. Electr. Eng. Inform.* **2020**, *9*, 573–581.
34. Tasdemir, K.; Kurugollu, F.; Sezer, S. Spatio-temporal rich model-based video steganalysis on cross sections of motion vector planes. *IEEE Trans. Image Process.* **2016**, *25*, 3316–3328. [CrossRef] [PubMed]
35. Sadek, M.M.; Khalifa, A.S.; Mostafa, M.G. Video steganography: A comprehensive review. *Multimed. Tools Appl.* **2015**, *74*, 7063–7094. [CrossRef]
36. Sumathi, C.; Santanam, T.; Umamaheswari, G. A study of various steganographic techniques used for information hiding. *arXiv* **2014**, arXiv:1401.5561.
37. Khan, S.; Bianchi, T. Ant colony optimization (aco) based data hiding in image complex region. *Int. J. Electr. Comput. Eng.* **2018**, *8*, 379–389. [CrossRef]
38. Filler, T.; Judas, J.; Fridrich, J. Minimizing additive distortion in steganography using syndrome-trellis codes. *IEEE Trans. Inf. Forensics Secur.* **2011**, *6*, 920–935. [CrossRef]
39. Fridrich, J.; Goljan, M.; Lisonek, P.; Soukal, D. Writing on wet paper. *IEEE Trans. Signal Process.* **2005**, *53*, 3923–3935. [CrossRef]
40. AlSabhany, A.A.; Ali, A.H.; Ridzuan, F.; Azni, A.; Mokhtar, M.R. Digital audio steganography: Systematic review, classification, and analysis of the current state of the art. *Comput. Sci. Rev.* **2020**, *38*, 100316. [CrossRef]

41. Nissar, A.; Mir, A.H. Classification of steganalysis techniques: A study. *Digit. Signal Process.* **2010**, *20*, 1758–1770. [CrossRef]
42. Fridrich, J.; Long, M. Steganalysis of LSB encoding in color images. In Proceedings of the 2000 IEEE International Conference on Multimedia and Expo, ICME2000, Latest Advances in the Fast Changing World of Multimedia (Cat. No. 00TH8532), New York, NY, USA, 30 July–2 August 2000; Volume 3, pp. 1279–1282.
43. Dittmann, J.; Hesse, D. Network based intrusion detection to detect steganographic communication channels: On the example of audio data. In Proceedings of the IEEE 6th Workshop on Multimedia Signal Processing, Siena, Italy, 29 September–1 October 2004; pp. 343–346.
44. Qian, Y.; Dong, J.; Wang, W.; Tan, T. Feature learning for steganalysis using convolutional neural networks. *Multimed. Tools Appl.* **2018**, *77*, 19633–19657. [CrossRef]
45. Serrano, J. Steganalysis: A Study on the Effectiveness of Steganalysis Tools. Ph.D. Thesis, Utica College, Utica, NY, USA, 2019.
46. Ghasemzadeh, H.; Arjmandi, M.K. Universal audio steganalysis based on calibration and reversed frequency resolution of human auditory system. *IET Signal Process.* **2017**, *11*, 916–922. [CrossRef]
47. Wang, Y.; Yi, X.; Zhao, X. MP3 steganalysis based on joint point-wise and block-wise correlations. *Inf. Sci.* **2020**, *512*, 1118–1133. [CrossRef]
48. Jin, C.; Wang, R.; Yan, D. Steganalysis of MP3Stego with low embedding-rate using Markov feature. *Multimed. Tools Appl.* **2017**, *76*, 6143–6158. [CrossRef]
49. Han, C.; Xue, R.; Zhang, R.; Wang, X. A new audio steganalysis method based on linear prediction. *Multimed. Tools Appl.* **2018**, *77*, 15431–15455. [CrossRef]
50. Lin, Y.; Wang, R.; Yan, D.; Dong, L.; Zhang, X. Audio steganalysis with improved convolutional neural network. In Proceedings of the ACM Workshop on Information Hiding and Multimedia Security, Paris, France, 3–5 July 2019; pp. 210–215.
51. Ren, Y.; Liu, D.; Xiong, Q.; Fu, J.; Wang, L. Spec-resnet: A general audio steganalysis scheme based on deep residual network of spectrogram. *arXiv* **2019**, arXiv:1901.06838
52. Chaeikar, S.S.; Zamani, M.; Manaf, A.B.A.; Zeki, A.M. PSW statistical LSB image steganalysis. *Multimed. Tools Appl.* **2018**, *77*, 805–835. [CrossRef]
53. Soltanian, M.; Ghaemmaghami, S. Blind consecutive extraction of multi-carrier spread spectrum data from digital images. In Proceedings of the 2017 Iranian Conference on Electrical Engineering (ICEE), Tehran, Iran, 2–4 May 2017; pp. 1835–1839.
54. Li, M.; Kulhandjian, M.K.; Pados, D.A.; Batalama, S.N.; Medley, M.J. Extracting spread-spectrum hidden data from digital media. *IEEE Trans. Inf. Forensics Secur.* **2013**, *8*, 1201–1210.
55. Lu, W.; Li, R.; Zeng, L.; Chen, J.; Huang, J.; Shi, Y.Q. Binary image steganalysis based on histogram of structuring elements. *IEEE Trans. Circuits Syst. Video Technol.* **2019**, *30*, 3081–3094. [CrossRef]
56. Laimeche, L.; Merouani, H.F.; Mazouzi, S. A new feature extraction scheme in wavelet transform for stego image classification. *Evol. Syst.* **2018**, *9*, 181–194. [CrossRef]
57. Guttikonda, J.B.; Sridevi, R. A new steganalysis approach with an efficient feature selection and classification algorithms for identifying the stego images. *Multimed. Tools Appl.* **2019**, *78*, 21113–21131. [CrossRef]
58. Wu, S.; Zhong, S.; Liu, Y. Deep residual learning for image steganalysis. *Multimed. Tools Appl.* **2018**, *77*, 10437–10453. [CrossRef]
59. Wang, Z.; Chen, M.; Yang, Y.; Lei, M.; Dong, Z. Joint multi-domain feature learning for image steganalysis based on CNN. *EURASIP J. Image Video Process.* **2020**, *2020*, 1–12. [CrossRef]
60. Wang, P.; Cao, Y.; Zhao, X. Segmentation based video steganalysis to detect motion vector modification. *Secur. Commun. Netw.* **2017**, *2017*, 8051389. [CrossRef]
61. Sadat, E.S.; Faez, K.; Saffari Pour, M. Entropy-based video steganalysis of motion vectors. *Entropy* **2018**, *20*, 244. [CrossRef] [PubMed]
62. Su, Y.; Yu, F.; Zhang, C. Digital Video Steganalysis Based on a Spatial Temporal Detector. *TIIS* **2017**, *11*, 360–373.
63. Li, Z.; Meng, L.; Xu, S.; Shi, Y. A HEVC video steganalysis algorithm based on pu partition modes. *Comput. Mater. Contin.* **2019**, *59*, 607–624. [CrossRef]
64. Ghamsarian, N.; Schoeffmann, K.; Khademi, M. Blind MV-based video steganalysis based on joint inter-frame and intra-frame statistics. *Multimed. Tools Appl.* **2020**, *80*, 9137–9159. [CrossRef]
65. Liu, P.; Li, S. Steganalysis of Intra Prediction Mode and Motion Vector-based Steganography by Noise Residual Convolutional Neural Network. In *IOP Conference Series: Materials Science and Engineering*; IOP Publishing: Bristol, UK, 2020; Volume 719, p. 012068.
66. Huang, X.; Hu, Y.; Wang, Y.; Liu, B.; Liu, S. Deep Learning-based Quantitative Steganalysis to Detect Motion Vector Embedding of HEVC Videos. In Proceedings of the 2020 IEEE Fifth International Conference on Data Science in Cyberspace (DSC), Hong Kong, China, 27–30 July 2020; pp. 150–155.
67. Kodovsky, J.; Fridrich, J.; Holub, V. Ensemble classifiers for steganalysis of digital media. *IEEE Trans. Inf. Forensics Secur.* **2011**, *7*, 432–444. [CrossRef]
68. Johnson, N.F.; Jajodia, S. Steganalysis of images created using current steganography software. In *International Workshop on Information Hiding*; Springer: Berlin/Heidelberg, Germany, 1998; pp. 273–289.
69. Chandramouli, R.; Li, G.; Memon, N.D. Adaptive steganography. In *Security and Watermarking of Multimedia Contents IV*; International Society for Optics and Photonics: Bellingham, WA, USA, 2002; Volume 4675, pp. 69–78.
70. Wilson, L. *Zipf, George K: Human Behavior and the Principle of Least Effort*; Addison Wesley: New York, NY, USA, 1949.

71. Zhang, H.; Cao, Y.; Zhao, X. A steganalytic approach to detect motion vector modification using near-perfect estimation for local optimality. *IEEE Trans. Inf. Forensics Secur.* **2016**, *12*, 465–478. [CrossRef]
72. Wang, P.; Cao, Y.; Zhao, X.; Wu, B. Motion vector reversion-based steganalysis revisited. In Proceedings of the 2015 IEEE China Summit and International Conference on Signal and Information Processing (ChinaSIP), Chengdu, China, 12–15 July 2015; pp. 463–467.
73. BOSS Web Page. Retrieved: 2020. Available online: http://agents.fel.cvut.cz/boss/index.php?mode=VIEW&tmpl=materials (accessed on 5 October 2021).
74. BOWS2 Web Page. Retrieved: 2020. Available online: http://bows2.ec-lille.fr/index.php?mode=VIEW&tmpl=index1 (accessed on 5 October 2021).
75. ImageNet Web Page, Retrieved: 2020. Available online: http://www.image-net.org (accessed on 5 October 2021).
76. Center for Statistics and Applications in Forensic Evidence. Stegoappdb Homepage. Retrieved: 2020. Available online: https://forensicstats.org/stegoappdb/ (accessed on 5 October 2021).
77. Coral. Corel Image Database. Retrieved: 2020. Available online: http://www.corel.com (accessed on 5 October 2021).
78. University of Southern California. The USC-SIPI Image Database. Retrieved: 2020. Available online: http://sipi.usc.edu/database/ (accessed on 5 October 2021).
79. Wang, K.Y.; Yang, Y.J.X. Audio Steganalysis Dataset. 2019. Available online: https://ieee-dataport.org/documents/audio-steganalysis-dataset (accessed on 5 October 2021).
80. Lin, Z.; Huang, Y.; Wang, J. RNN-SM: Fast Steganalysis of VoIP Streams Using Recurrent Neural Network. *IEEE Trans. Inf. Forensics Secur.* **2018**, *13*, 1854–1868. [CrossRef]
81. Meghanathan, N.; Nayak, L. Steganalysis algorithms for detecting the hidden information in image, audio and video cover media. *Int. J. Netw. Secur. Its Appl. (IJNSA)* **2010**, *2*, 43–55.
82. spyhunter. StegSpy. 2004. Available online: http://www.spy-hunter.com/stegspy (accessed on 5 October 2021).
83. Provos, N. stegdetect. 2002. Available online: https://github.com/abeluck/stegdetect (accessed on 5 October 2021).
84. Muñoz, A. stegsecret. 2007. Available online: http://stegsecret.sourceforge.net (accessed on 5 October 2021).
85. WetStone Technologies. StegoHunt. 2019. Available online: https://www.wetstonetech.com/products/stegohunt-steganography-detection/ (accessed on 5 October 2021).
86. Boehm, B. StegExpose. 2014. Available online: https://github.com/b3dk7/StegExpose (accessed on 5 October 2021).
87. Backbone Security. StegAlyzerAS. Retrieved: 2020. Available online: https://www.backbonesecurity.com (accessed on 5 October 2021).
88. Backbone Security. StegAlyzerSS. Retrieved: 2020. Available online: https://www.backbonesecurity.com (accessed on 5 October 2021).
89. Backbone Security. StegAlyzerFS. Retrieved: 2020. Available online: https://www.backbonesecurity.com (accessed on 5 October 2021).
90. SourceForge. Virtual Steganographic Laboratory. Retrieved: 2020. Available online: https://sourceforge.net/projects/vsl/ (accessed on 5 October 2021).
91. Lerch-Hostalot, D.; Megías, D. Unsupervised steganalysis based on artificial training sets. *Eng. Appl. Artif. Intell.* **2016**, *50*, 45–59. [CrossRef]
92. Kakde, Y.; Gonnade, P.; Dahiwale, P. Audio-video steganography. In Proceedings of the 2015 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS), Coimbatore, India, 19–20 March 2015; pp. 1–6.
93. Lalwani, D.; Sawant, M.; Rane, M.; Jogdande, V.; Ware, S. Secure Data Hiding in Audio-Video Steganalysis by Anti-Forensic Technique. *Int. J. Eng. Comput. Sci.* **2016**, *5*, 15996–16000. [CrossRef]
94. Mudusu, R.; Nagesh, A.; Sdanandam, M. Enhancing Data Security Using Audio-Video Steganography. *Int. J. Eng. Technol.* **2018**, *7*, 276–279. [CrossRef]