Int. j. adv. multidisc. res. stud. 2023; 3(4):215-222

Received: 21-05-2023
Accepted: 01-07-2023

International Journal of Advanced Multidisciplinary Research and Studies

ISSN: 2583-049X

Classification of the Modern Approaches in Steganalysis Technique, Scenarios Attacks and Future Trends

[1] Aoday H Ali, [2] Marwan B Mohammed, [3] Dlsoz abdalkarim Rashid
[1, 2] Department of Computer Science, Al-Nahrain University (NUST), Baghdad, Iraq
[3] Department of Computer Science, University of Sulymana, Sulymana, Iraq

Corresponding Author: **Aoday H Ali**

Abstract
Information Steganalysis techniques are a topic that has received great attention in recent years. Notice, the increasing demand from individuals and companies for these techniques because of the ability of this technology to secure the issue of hidden data that represents confidential information that is included within the file (such as image, audio, video, and text). In addition, it is the ability to detect malicious hidden data through analysis algorithms. This paper presents three important contributions. First, explain some of the methods and techniques used in the field of steganalysis. Second, the work presents a review of the most important challenges and problems facing researchers in this field that still exist. Finally, providing future directions that will benefit researchers in developing Steganalysis methods later.

Keywords: Steganography, Steganalysis Attacks, Steganalysis Techniques, Data Hiding, Cover Image

1. Introduction

Steganography is a popular science mainly based on hiding information or a message inside a cover (Amine & El Mamoun, 2019) [1]. The cover means is any file such as image, video, text, etc. although, this cover is clear in general, but, maybe there hidden information inside it, only those who have the right or who have knowledge of the hidden file(Santoso *et al*., 2018) [23]. The Steganography process is used within multiple fields depending on the type of carrier and is developed periodically, and current steganography trends include multimedia, files, networks, Skype, medical imaging, DNA, and so on. (Dalal & Juneja, 2021) [6].

Steganalysis of data hiding analysis is based on the opposite process, which is the detection of hidden data (Jung, 2019) [10]. Figure 1 showed concept work steganalysis in general. Steganalysis labels a digital object, like an image, as stego or just innocent, the main objective of Steganalysis is to identify suspicious sent files, whether they contain information, and how to extract them (Chutani & Goyal, 2019) [5], (Djebbar & Ayad, 2017) [8]. Usually, the Steganalysis concept has advantages and disadvantages. However, it depends on the idea used to reveal the presence of hidden data, and dividing into two parts. The first part is positive, which reveals the presence of data related to the country's security, and the other part is negative which represents some of the hidden data that is sensitive (Wu *et al*., 2021) [28].

This paper displays several strategies for the detection and analysis of steganalysis. In addition, also, this study focuses on viewing the steganalysis techniques for detecting multimedia which are considered the most common media due to their high level of repetition, and modern methods used to carry out the analysis process, where the detection techniques are adopted to the data embedded in the images, video, and audio. another side, this research assists the researchers in developing methods to identify concealed messages by presenting the current approaches used in steganalysis and the instruments used to reveal the host's secret data. In the end, this work presents several main contributions: a) Provide a background for steganography and steganalysis in general. b) Divide the steganalysis technologies into categories depending on their characteristics. c) viewing of the most recent state-of-the-art in steganalysis.

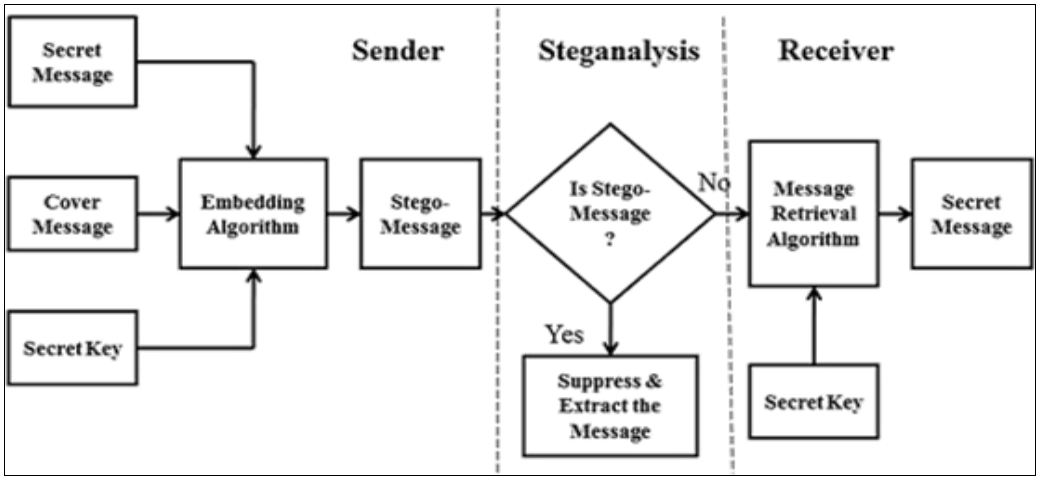

Fig 1: Procedures Basic of Steganalysis

2. Steganalysis Type

The research parts of steganalysis include the identification of confidential messages, valuation of embedding ratios, and message extraction. Steganalysis is used in computer forensics, cyber warfare, tracking criminal activity on the internet, and obtaining evidence for investigations, especially in cases involving anti-social groups. Apart from its law enforcement and anti-social implications, steganography has a peaceful application in that it improves the security of steganographic tools by analyzing and detecting their flaws (Nissar & Mir, 2010) [19].

1. Challenges of Steganalysis Scenarios Attacks

In terms of analysis and detection, the steganalysis methods used should be able to overcome the hurdles posed by steganography approaches (Bawaneh *et al*., 2021) [2]. There are several challenges of Steganalysis techniques (Kasapbaşi, 2019) [12] (Karampidis *et al*., 2018) [11]:

- Stego only attack: Analysis is limited to the stego object (Karampidis *et al*., 2018) [11] (Pathak *et al*., 2018) [20]. In this case, the only communication between the parties that is intercepted is the stego picture. Recovery from the initial message is still quite difficult (Kasapbaşi, 2019) [12].
- In a known cover attack, both the cover and the stego object are available for investigation (Karampidis *et al*., 2018) [11] (Kasapbaşi, 2019) [12] (Pathak *et al*., 2018) [20].
- Known message attack: The message is well known and comparable to the stego object (Karampidis *et al*., 2018; Pathak *et al*., 2018) [11, 20]. However, but it will be difficult because the message is scattered throughout(Kasapbaşi, 2019) [12].
- Both the original and the stego-object are available for stego attack, and the ste-ganography algorithm is known (Karampidis *et al*., 2018) [11] (Kasapbaşi, 2019) [12] (Pathak *et al*., 2018) [20].
- Selected stego attack: Both the stego object and the stego tool (algorithm) are available for examination (Karampidis *et al*., 2018) [11] (Pathak *et al*., 2018) [20].
- The Steg analyst creates stego-media from a known message using a steganography tool or algorithm. This attack aims to identify similar patterns in stego-media that can point to the employment of particular steganography tools or techniques (Karampidis *et al*., 2018) [11] (Pathak *et al*., 2018) [20].

3. Categories of Steganalysis Techniques

Steganography's most fundamental technique is to incorporate a message after the End of File (EOF) or hidden data in the exif header Both strategies are easy to use and deploy, but they are vulnerable to steganalysis. If the file is not encrypted, the message can be found by viewing it with a hex editor. This basic strategy is useful for those who have little or no expertise of steganalysis, but digital forensic experts can readily locate and extract the hidden data from the cover medium. New steganalysis procedures were improved as a result. This section will provide six major groups based on the attack technique used by a forensic examiner (Karampidis *et al*., 2018) [11].

3.1 Visual Steganalysis

Visual attacks are the most fundamental sort of steganalysis. A visual attack en-tails evaluating the suspicious image with the naked eye for any noticeable irregularities. This becomes incredibly difficult because the modifications made to an image while incorporating a message do not result in a decrease in quality. The majority of steganographic algorithms produce stego objects that look like their cover media. However, evidence of change can be observed when unaffected regions of a stego image are removed. As a consequence, a visual attack could uncover the presence of a hidden message if steganalysis can detect the image traits that designate it as stego (Karampidis *et al*., 2018) [11]. Visual attacks are the visual detection of variations between a container and a steganographic message(Bobok & Kobozeva, 2019) [3].

3.2 Signature or Specific Steganalysis

Another steganalytic strategy is to look for any steganography software's repeating patterns (signatures). These methods look for signature patterns to see if a secret message is there. Numerous steganalysis software packages examine files and detect signatures from various embedding methods. If the stego image was made with a tool that leaves its signature in the stego file, it is easy for a forensic examiner to figure out what it is (Karampidis *et al*., 2018) [11]. The signature or specific steganalysis are techniques that check for signature patterns to assess if there is a hidden message (Bobok & Kobozeva, 2019) [3].

3.3 Statistical Steganalysis

The term statistical steganalysis refers to approaches developed by investigating the embedding operation and identifying specific statistics which it alter as a consequence of the embedding procedure (Bobok & Kobozeva, 2019) [3]. As a result, a detailed grasp of the embedding process is critical to achieving the highest level of steganalysis accuracy. The spatial domain pixels of the image are directly subjected to the steganographic technique. The oldest techniques used in this field are the Least Significant Bit Substitution (LSB) technique(Karampidis *et al*., 2018) [11].

3.4 Spread Spectrum Steganalysis

Spread spectrum steganalysis is a technique for detecting embedded data introduced by steganographic methods that spread the frequency spectrum of the signal container by using methods to get the estimated value of the hidden message(Bobok & Kobozeva, 2019) [3]. The secret information is embedded in chaos, then it is injected to the digital photo using Spread Spectrum Image Steganography (SSIS). However, the unaided eye cannot see this noise when it is kept at lower levels (Karampidis *et al*., 2018) [11].

3.5 Transform Domain Steganalysis

The transform domain is studied in the steganalysis process to hide data in the transform domain of the cover image, e.g., discrete cosine transform domain, discrete wavelet transform domain, singular decomposition domain, etc. (Karampidis *et al*., 2018) [11] (Bobok & Kobozeva, 2019) [3] (Mohamed *et al*., 2020) [18]. Spatial domain steganalysis, on the other hand, identifies changes in pixel values in the spatial domain directly (Mohamed *et al*., 2020) [18].

3.6 Universal or Blind Steganalysis

Regardless of the steganographic approach used on the cover image, the universal steganalysis method aims to detect hidden messages within images. The main and difficult challenge is to find the aspects and features that relate to Stego Images. Following that, machine-learning strategies are employed can create a detection algorithm based on the collected information. When the system recognizes stego images regardless of the steganographic algorithms used to implant the hidden message in the cover media, it is called a universal-blind method. However, when dealing with explicit steganographic methods, the process can be referred to as semi-blind (Karampidis *et al*., 2018) [11]. This approach attempts to detect inline messages without modifying the steganography used on the cover photo (Bobok & Kobozeva, 2019) [3].

4. Modern of the Steganalysis Directions

This section focuses on some recent trends in steganalysis in the multimedia field by reviewing recent work related to this field.

4.1 Digital Text Steganalysis

Zhongliang Yang and colleagues(Yang, Huang, *et al*., 2019) [31] proposed a fast and efficient text steganalysis method to handle the problem of buried texts that correlate to statistical feature distributions in 2019. They began by examining the word associations in these generated hidden texts. They then used a hidden layer to map each word to a semantic space and extract the links between them. Finally, the authors classified the input text using a SoftMax classifier based on the extracted features, and the input results suggest that the model can attain accuracy in disclosing hidden information. To extract correlation characteristics, Zhongliang Yang and *et al* (Yang *et al*., 2020) [30] developed a novel approach to text steganalysis using convolutional-sliding-windows (TS-CSW) with different sizes in 2020. After being inserted with a hidden message, these words tieing qualities in generated steganographic texts were observed to be distorted. These slight changes in correlation attribute distribution might then be employed for text steganalysis. Researchers trained and tested the suggested steganalysis approach using samples from the T-Steg dataset.Hui Li, Shuyu Jin. (Li & Jin, 2021), 2021, focused on demonstrating that utilizing a capsule network to determine whether actual text includes hidden data achieves robust and accurate results. The capsule network captures and stores textual semantic information while also analyzing tiny differences between steganographic and natural language. They used the word-to-word (w2w) vector to generate steganographic writing and parse text using Recurrent-Neural-Network (RNN) and coding with variable length as the dataset for testing to increase the method's generality.

4.2 Digital Image Steganalysis

Ping Wang *et al*. (Wang *et al*., 2019) [25], 2019, proposed a steganalysis approach based on using image forensics and steganalysis instruments to avoid erroneous alarms. To differentiate the routinely processed photographs from the examined images, first, the fragile observation of picture modifications that are not resistant to steganography is employed. Following that, the remaining photos are loaded into the learned classifier for steganalysis. In 2021, Deepa D. Shankar and Adresya Suresh Azhakath (Shankar & Azhakath, 2021) [24] propose research with the primary objective of analyzing internet communication and preventing any undesirable outcomes that may follow from secret communication. So as to conduct the analysis with JPEG images with (10% embedding) and (10-fold cross-validation). The calibration method is used to approximate the cover image. In this steganalysis investigation, four embedding techniques were utilized: Replacement Pixel-Value-Differencing (PVD), Least-Significant-Bit-Matching (LSB), and F5. The researchers relied on Used INIRA holiday dataset and UCID dataset to implement the experiment. Baraa Tareq Hammad *et al*. (Hammad *et al*., 2022) [9], 2022, proposed an image steganalysis classification (ISC) technique to enhance accuracy and decrease the great dimensionality of obtained attributes based on the following three steps: The initial stage was preprocessing and then following that, SFTA, LBP, and GLCM were utilized to extract the attributes of the texture. In the end, the Gaussian Discriminant Analysis (GDA) and Naive Bayes (NB) were selected as the most effective classifiers. To apply the method, the researchers used IStego100K (a large-scale image steganalysis dataset).

Techniques like Gabor, which are capable of successfully capturing changes in visual texture, are the kind of methods that the researchers hope to examine in the future. In addition to this, they want to utilize deep learning in order to put the concept into practice.

4.3 Digital Audio Steganalysis

A supervisor can use steganalysis as a defense against these

covert transmissions, and it can also help make current steganography methods more secure. This is because steganography typically alters the cover signal's content, leaving a fingerprint that can be picked up detection (Chaharlang *et al*., 2020) [4]. Javad and colleagues (Chaharlang *et al*., 2020) [4], in 2020, proposed a blind quantum steganalysis approach that detects encoded data in host quantum audio waves using the quantum circuit network. The steganalyzer's feature extraction module is in charge of computing and storing the quantum audio signal frames' mean value. The quantum of the KKN approach and the quantum hamming distance criteria are used in this steganalyzer's classification procedure. The researchers point out that simulation-based experiments indicate the proposed system's high simulation efficiency and performance. The researchers recommended that future work concentrates on developing a strategy for providing a network of quantum circuits to derive quantum attributes from quantum frequency domains, like the quantum Fourier transform (QFT) and quantum-wavelet-transform(QWT). To create deep learning-based audio steganalysis, deep audio steganalysis in the temporal domain of pure audio format, Daewon Lee and colleagues (Lee *et al*., 2020) [13], 2020, proposed the development of a convolutional neural network, BSNet, it combines channel attention, weight-standardized convolution, and bitplane separation. This was done in order to develop audio steganalysis.

In the year 2021, the authors Hanna and *et al*. (Martyniuk *et al*., 2021) [16] proposed a technique for locating the mysterious peculiarities of the cover signal. This method consisted of the following three steps: 1. determine whether or not the data are stationary; 2. identify any instances of signal disharmony; 3. time series simulation at each piecewise regular period in order to reconstruct the audio signal. They also presented a classification of methods for audio signal steganalysis. through the presentation of a classification of these methods as well as the fundamental formulas. At this point, there are a few steganalysis methods for Advanced Audio Coding (AAC) (Ren *et al*., 2016) [22]. Traditional AAC (Advanced-Audio-Coding) audio steganalysis methods, as a result, dependence on manual feature extraction, which leads to poor accuracy and efficiency in detection. The authors, Zhongyuan and Kaixi, were able to build the new steganalysis model using a neural network. Although this model is visually pleasing, it has a huge scale and might be enhanced further in terms of detection accuracy. They proposed a Res-NeXt-based lightweight AAC audio general steganalysis model. To begin, the remaining signal of the coefficients of QMDCT (Quantized Modified Discrete Cosine Transform) are computed using a fixed convolution layer collected of numerous sets of high-pass filters. Then, using the original ResNeXt network structure, Two ResNeXt blocks are designed to construct a remaining learning module from which the steganalysis features in the QMDCT constants are extracted in greater detail. Finally, the classification module is made up of two layers: the completely linked layer and the Softmax layer, which determines the classification result (Wei & Wang, 2022) [27].

5. Comparative and the Future Trend

This section is broken into two sub-sections. The first will review various past research described in the preceding parts by comparing each set within the same discipline to illustrate advantages and disadvantages, the type of dataset used, and key contributions produced by authors. The other explains deduces and ideas accessed in this work that benefit academics interested in developing the field of steganalysis.

5.1 Comparative Analysis of Steganalysis Techniques

Steganalysis methods mainly include creating a number of corresponding statistical features and then determining the statistical distribution variations between the stego-text and the cover-text based on these features (Yang, Huang, *et al*., 2019) [31]. Zhongliang and colleagues (Yang, Huang, *et al*., 2019) [31] develop a model for convolutional sliding window-based text steganography (TS-CSW). This model is separated into two modules: word correlation extraction and feature classification. They created the T-Steg text steganalysis dataset, which is available in the Github repository dataset; it comprises a total of 396,000 texts with varying embedding rates in different kinds. They separated writings into two types. One has five words per line (FW), whereas the other has seven (SW). Every format is further divided into two types: poems with four lines (FL) or poems with eight lines (FL) (EL). The researchers then used multi-size convolutional sliding windows (CSW) to extract these phrases' characteristics of relation and TS-CSW (single) to compare efficiency. The results reveal that the suggested model performs well in steganalysis and can perform steganographic detection analysis on these texts in real-time. They used precision, recall, and accuracy criteria to assess the performance of their model. They are determined by the average time. TS-CSW (Single) and TS-CSW (Multi) take 9.78/9.83 ms. These results show that the suggested form has a very high steganalysis performance and can perform steganographic detection analysis of these texts in near real-time. can also get the same conclusion, namely that TS-CSW (single) is more suited for recognizing lengthier texts, whereas TS-CSW (multiple) better suited for detecting shorter texts. The Hui Li, and Shuyu Jin (Li & Jin, 2021) have collected data set containing a total of 15000 sentences based on three sources datasets IMDB (Mikolov *et al*., 2013) [17], news reviews (Maas *et al*., 2011) [15], and Twitter (dataset). They employed the CBOW method to extract features for words to steganalysis with the use capsule-net model with dynamic routing. The average time was 3.736 ms when using RNN compared with CNN. The discovering accuracy of victories text was 92% with low average embedding and 94% with high average embedding. The reason for the difference in average time between (Yang, Huang, *et al*., 2019) [31] and (Li & Jin, 2021) are dataset size used. Zhongliang and colleagues used a dataset bigger than the Hui Li, and Shuyu dataset. Also, the principle of text analysis by the author Zhongliang differs from the Hui Li, and Shuyu.

Regarding the digital image, Deepa and Adresy (Shankar & Azhakath, 2021) [24] employed four embedded methods for steganalysis: Least Significant Bit Matching, LSB Replacement, Pixel Value Differencing (PVD), and F5. In addition, four alternative samplings are respected: linear, shuffle, stratified, and automated. The proposed method employs 10-fold cross-validation over several kernels and four samplings. With 10% embedding, the SVM and SVM-PSO classifiers are modified. They utilized image steganography in JPEG file format. JPEG uses lossy compression to maintain the data in JPEG File Interchange Format (JFIF), and pixel blocks are encoded using the

Huffman entropy. The image is broken down into 8X8 blocks, followed by feature mining. For analysis, a minimum embedding rate of 10% is assumed. The Discrete Cosine Transform (DCT) is used to include the pictures and eliminate the pertinent aspects of each image. For the proposed blind steganalysis, two distinct picture databases are considered: the INRIA vacation dataset (Lee *et al*., 2020) [13] and the UCID image dataset [47]. The findings suggest that the multi-quadratic kernel is an effective substitute for automated, shuffled, linear, and stratified sampling. The polynomial kernel is the second-best choice. In general, and irrespective of the sample, the Multiquadric kernel provides positive and equitable results. In comparison to the SVM classifier, most other kernels behaved preferentially (without PSO). All four samples considered can obtain better results using the ANOVA kernel, polynomial kernel, Epanechnikov kernel, and dot kernel. Ping Wang and *et al* (Wang *et al*., 2019) [25] introduced a contrived framework built on a combination of steganalysis multi-tools: the S-UNIWARD with gamma transformation detection, and LSB identical. In addition, creating a modern attribute that does the sum of products in two histogram bins adjacent to zero value histogram bins. They used image forensics with the tools above to enhance the consistency of steganography in the actual world by relying on accurate image manipulation identification and stego detection. This framework aims to reduce false alarms from steganalysis. The framework evaluation achieved high accuracy with a low false alarm rate. The framework they proposed, however, was unable to reduce the missed detection rate. It's worth noting that they used a fixed-size image of 512 × 512 that was trimmed, and resized from real pictures of various sizes. Note, they used 10.000 of the original image dataset by BossBase version 1.011 to validate of the performance the proposed framework. In 2022 Baraa and colleagues (Hammad *et al*., 2022) [9] authors present steganalysis classification-based texture features such as fractal texture features (SFTA), local binary pattern (LBP), and gray level co-occurrence matrix (GLCM). In addition, they used two classifiers gaussian decrement analysis (GDA) and NaiveBase (NB). proposed fractal texture features(SFTA) based on (GDA) after selecting the best one of two classifiers GDA and NaiveBase. They compared the proposed work with image steganalysis classification(ISC) methods. The accuracy results showed that the model proposed exceeded the ISC methods so that achieved 90% detection accuracy compared with NB was 75 %. althguth of all classifiers used the same feature vector. noticed the SFTA was higher results than the remainder of the texture features used. The dataset used was a public database named istego 100K datasets (large scale image steganalysis dataset) (Yang, Wang, *et al*., 2019) to evaluate work it. In terms, of digital Audio Steganalysis, the authors Javad and colleagues (Chaharlang *et al*., 2020) [4] proposed model consist of two parts. The first part used steganography to reduce the impact of the procedure for embedding while raising the SNR (Signal-Noise-Ratio). The second section employed steganalysis to identify between stego audio signals based on statistical parameters collected from the audio data. A mean feature extraction module extracts features from audio signal frames and quantum circuits in the universal steganalyzer that implement the KNN algorithm and the Hamming distance requirement. They dealt with two sorts of audio signals: speech and music. They employed embedding rates of 100%, 50%, and 25% in a 1024-sample quantum host audio stream. Each quantum is split into 32 Qframes, each with 32 samples, and the average for every Qframe is calculated. The suggested quantum steganalysis model evaluation showed satisfying results according to the embedding rate percentage. However, this model deals with fixed length because it's implemented as a simulation only. As a result, only a small number of audio signals with low sample rates were employed. In 2022, Zhongyuan Wei and Kaixi Wang proposed LARXNet, a lightweight generic steganalysis approach based on ResNeXt, to detect Advanced Audio Coding (AAC) steganography schemes. The authors relied on the Reference (Chutani & Goyal, 2019) [5], which supplied a big WAV audio dataset with a sampling frequency of 44.1 KHz and a length of 10s when they employed the dataset. AAC audio encoder selects 15,000 WAV audios and encodes them into M4A files at a bitrate of 128 Kbps. Four existing audio steganalysis methods are compared with LARXNet under different relative embedding rates for the three steganography algorithms used, comprising two manual feature extraction-based traditional audio steganalysis approaches (MDI2 (Chutani & Goyal, 2019) [5] and JPBC(Djebbar & Ayad, 2017) [8], and two neural network-based audio steganalysis models (Spec-ResNet (Ren *et al*., 2019) [21] and WASDN (Wang *et al*., 2018) [26]). When compared to approaches based on manual feature extraction, the detection accuracy of LARXNet for the MIN algorithm is greater than 98%. When the relative embedding rate is low, the suggested model achieves a high classification impact. As a result, with an embedding rate of 0.1, it achieved detect an accuracy of 85.5%. This model associates the benefits of GoogleNet and ResNet, which not only increases the model's performance in detection but also decreases the model's number of parameters. Furthermore, their model employs a residual structure, which helps relieve network overfitting and network degradation issues while also speeding up model training. Compared with Spec-ResNet and WASDN. Their model, however, should be developed further to discover adaptive steganography approaches. As a result, they recommend Continuing to refine the network structure based on the characteristics of the adaptive steganography algorithms in the future, this model's detection performance for adaptive steganography approaches will be improved. Table1 is displaying advantages and disadvantages for each work and Table 2 is describes all works researchers above as briefly.

Table 1: Description advantages and dis advantages of related work as briefly

Research	Advantage	Disadvantage
Zhongliang (Yang, Huang, *et al*., 2019) [31]	- The system can execute high-performance text analysis in a very short period of time. - The TS-CSW (single) is better suited for detecting longer texts than the TS-CSW (multiple).	TCS-Multi outperforms TCS-Single when dealing with shorten text, But, with long texts, it becomes inefficient. thus, it is opposite TCS-Single.
Hui Li, And Shuyu Jin (Li & Jin, 2021)	- Capsent was chosen because its convergence speed is faster than that of CNN, and it reduces time complexity at the expense of spatial complexity. - Text with mixed unknown embedding rate improves by 1-2%.	A minor improvement in recall rate will make the discriminating possibility less.
Deepa And Adresy(Shankar & Azhakath, 2021) [24]	Most of the kernels that were left responded favorably without the use of pso. When the four samples applied the anova kernel, polynomial kernel, epanechnikov kernel, and dot kernel, they saw improvements in their outcomes.	The use of the multi-quadratic kernel in SVM-PSO methodologies has not been effective for linear purposes.
Wang And Etal (Wang *et al*., 2019) [25]	- The framework evaluation obtained high efficiency while minimizing false alarms.	The framework is unable to reduce missed detection rates.
Baraa And Etal (Hammad *et al*., 2022) [9]	- The proposed model outperformed ISC approaches, achieving high accuracy versus results for NB. - Despite the fact that all classifiers employed the same feature vector. but The SFTA produced better outcomes than the other texture features tested.	Not using more than one dataset to evaluate the system makes the proposed model restricted
Javad And Colleagues (Chaharlang *et al*., 2020) [4]	The evaluation of the proposed model for detecting hidden data in quantum systems yielded satisfactory outcomes.	The model only uses a fixed length because it's designed as a simulation. This means that it was only tested on a limited number of audio signals that had a low sample rate.Therefore, the scope of the approach is somewhat limited
Zhongyuan Wei And Kaixi Wang (Wei & Wang, 2022) [27]	In comparison to techniques that rely on manually extracting features, LARXNet's detection accuracy for the MIN algorithm is above 98%. Additionally, when the relative embedding rate is low, the proposed model produces a significant impact in classification.	Although the model has shown success in experiments, they suggest further improving the network structure by considering the unique characteristics of adaptive steganography algorithms. This would lead to better detection performance for adaptive steganography techniques.

Table 2: Description of related work as briefly

Research	Year	Research Direction	Dataset Used	Model Proposed
Zhongliang (Yang, Huang, *et al*., 2019) [31]	2019	Text Steganalysis	(T-Steg)	Ts-Csw
Hui Li, and Shuyu Jin (Li & Jin, 2021)	2020	Text Steganalysis	Collection	Capsnet Model
Deepa and Adresy (Shankar & Azhakath, 2021) [24]	2020	Image Steganalysis	Inria Holiday Dataset [23] And the Ucid Image Dataset [47].	Applied Four of Embedded Techniques That Have Been for Steganalysis
Wang and *et al* (Wang *et al*., 2019) [25]	2019	Image Steganalysis	10.000 Of Orginal Image Dataset	Framework Built on A Combination of Steganalysis Multi-Tools: The S-Uniward with Gamma Transformation Detection, And Lsb Identical.
Baraa and Etal (Hammad *et al*., 2022) [9]	2022	Image Steganalysis	Istego 100k Datasets (Yang, Wang, *et al*., 2019)	Proposed Fractal Texture Features (Sfta) Based on (Gda)
Javad and Colleagues (Chaharlang *et al*., 2020) [4]	2020	Audio Steganalysis	Creating Dataset Consist of Speech and Music	Quantum Steganalysis Model
Zhongyuan Wei and Kaixi Wang (Wei & Wang, 2022) [27]	2022	Audio Steganalysis	Depending Dataset on the Reference (Wang *et al*., 2018) [26]	Larxnet Based on Resnext Model

The Trends of the Future

Based on the previously mentioned research in the field of steganalysis and how to access and extract hidden data, in addition to the current challenges, there is a set of future research directions that can be expected, these research directions can Increase the possibility of quick access to the data hidden within the multimedia, such as:

1. Develop tools that detect the presence of hidden data in the field of steganalysis.
2. Focusing on evaluating the steganalysis tools.
3. Dealing with static databases is necessary to increase the accuracy of the workbook's steganalysis work.

6. Conclusion

In recent years between 2006 until 2017. This categorization offered a high-level summary of the fundamental ideas

underlying steganography, steganalysis, and their respective classifications. In addition, a discussion of the most recent findings from research on steganography methods applied to text, images, and audio was presented. There was a discussion of the applications, datasets, and widely used tools that are available for steganography. This assessment came to a conclusion by discussing the most pressing issues in this sector and offering some recommendations for the years to come.

7. References

1. Amine BM, El Mamoun S. Introduction to steganography in RRNS based communications. Proceedings of the 2nd International Conference on Networking, Information Systems & Security, 2019.
2. Bawaneh MJ, Al-Shalabi EF, Al-Hazaimeh OM. A novel RGB image steganography using simulated annealing and LCG via LSB. International Journal of Computer Science & Network Security. 2021; 21(1):143-151. Doi: https://doi.org/https://doi.org/10.22937/IJCSNS.2021.21.1.19
3. Bobok I, Kobozeva A. Steganalysis method efficient for the hidden communication channel with low capacity. Radiotekhnika. 2019; 198:19-31. Doi: https://doi.org/https://doi.org/10.30837/rt.2019.3.198.02
4. Chaharlang J, Mosleh M, Rasouli-Heikalabad S. A novel quantum steganography-Steganalysis system for audio signals. Multimedia Tools and Applications. 2020; 79(25):17551-17577. Doi: https://doi.org/https://doi.org/10.1007/s11042-020-08694-z
5. Chutani S, Goyal A. A review of forensic approaches to digital image Steganalysis. Multimedia Tools and Applications. 2019; 78(13):18169-18204. Doi: https://doi.org/https://doi.org/10.1007/s11042-019-7217-0
6. Dalal M, Juneja M. Steganography and Steganalysis (in digital forensics): A Cybersecurity guide. Multimedia Tools and Applications. 2021; 80(4):5723-5771. Doi: https://doi.org/https://doi.org/10.1007/s11042-020-09929-9
7. Dataset, t. https://www.kaggle.com/snap
8. Djebbar F, Ayad B. Energy and Entropy Based Features for WAV Audio Steganalysis. J. Inf. Hiding Multim. Signal Process. 2017; 8(1):168-181.
9. Hammad BT, Ahmed IT, Jamil N. A Steganalysis Classification Algorithm Based on Distinctive Texture Features. Symmetry. 2022; 14(2):p236. Doi: https://doi.org/https://doi.org/10.3390/sym14020236
10. Jung KH. A study on machine learning for steganalysis. Proceedings of the 3rd International Conference on Machine Learning and Soft Computing, 2019.
11. Karampidis K, Kavallieratou E, Papadourakis G. A review of image steganalysis techniques for digital forensics. Journal of information security and applications. 2018; 40:217-235. Doi: https://doi.org/https://doi.org/10.1016/j.jisa.2018.04.005
12. Kasapbaşi MC. A new chaotic image steganography technique based on Huffman compression of Turkish texts and fractal encryption with post-quantum security. IEEE Access. 2019; 7:148495-148510. Doi: https://doi.org/https://doi.org/10.1109/access.2019.2946807
13. Lee D, Oh TW, Kim K. Deep audio steganalysis in time domain. Proceedings of the 2020 ACM Workshop on Information Hiding and Multimedia Security, 2020.
14. Li H, Jin S. Text steganalysis based on capsule network with dynamic routing. IETE Technical Review. 2021; 38(1):72-81. Doi: https://doi.org/https://doi.org/10.1080/02564602.2020.1780959
15. Maas A, Daly RE, Pham PT, Huang D, Ng AY, Potts C. Learning word vectors for sentiment analysis. Proceedings of the 49th annual meeting of the association for computational linguistics: Human language technologies, 2011.
16. Martyniuk H, Kozlovskiy V, Meleshko T, Sorokun A. Method of Finding Cover Signal for Audio Steganalysis Calibrated Methods. 2021 11th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), 2021.
17. Mikolov T, Chen K, Corrado G, Dean J. Efficient estimation of word representations in vector space. arXiv preprint arXiv:1301.3781, 2013.
18. Mohamed N, Rabie T, Kamel I. IoT Confidentiality: Steganalysis breaking point for J-UNIWARD using CNN. 2020 Advances in Science and Engineering Technology International Conferences (ASET), 2020.
19. Nissar A, Mir AH. Classification of steganalysis techniques: A study. Digital Signal Processing. 2010; 20(6):1758-1770. Doi: https://doi.org/https://doi.org/10.1016/j.dsp.2010.02.003
20. Pathak S, Roy R, Changder S. Performance analysis of image steganalysis techniques and future research directives. International Journal of Information and Computer Security. 2018; 10(1):1-24. Doi: https://doi.org/https://doi.org/10.1504/ijics.2018.10010646
21. 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 preprint arXiv:1901.06838, 2019.
22. Ren Y, Xiong Q, Wang L. Steganalysis of AAC using calibrated Markov model of adjacent codebook. 2016 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), 2016.
23. Santoso HA, Rachmawanto EH, Sari CA. An improved message capacity and security using divide and modulus function in spatial domain steganography. 2018 international conference on information and communications technology (ICOIACT), 2018.
24. Shankar DD, Azhakath AS. Minor blind feature based Steganalysis for calibrated JPEG images with cross validation and classification using SVM and SVM-PSO. Multimedia Tools and Applications. 2021; 80(3):4073-4092. Doi: https://doi.org/https://doi.org/10.1007/s11042-020-09820-7
25. Wang P, Liu F, Yang C, Luo X. Steganalysis aided by fragile detection of image manipulations. Multimedia Tools and Applications. 2019; 78(16):23309-23328. Doi: https://doi.org/https://doi.org/10.1007/s11042-019-7654-9
26. Wang Y, Yang K, Yi X, Zhao X, Xu Z. CNN-based steganalysis of MP3 steganography in the entropy code domain. Proceedings of the 6th ACM workshop on

information hiding and multimedia security, 2018.
27. Wei Z, Wang K. Lightweight AAC Audio Steganalysis Model Based on ResNeXt. Wireless Communications and Mobile Computing, 2022. Doi: https://doi.org/https://doi.org/10.1155/2022/9074771
28. Wu Z, Guo J, Zhang C, Li C. Steganography and steganalysis in voice over ip: A review. Sensors. 2021; 21(4):p1032. Doi: https://doi.org/https://doi.org/10.3390/s21041032
29. Yang Z, Huang Y, Zhang YJ. A fast and efficient text steganalysis method. IEEE Signal Processing Letters. 2019; 26(4):627-631. Doi: https://doi.org/https://doi.org/10.1109/lsp.2019.2902095
30. Yang Z, Huang Y, Zhang YJ. TS-CSW: Text steganalysis and hidden capacity estimation based on convolutional sliding windows. Multimedia Tools and Applications. 2020; 79(25):18293-18316. Doi: https://doi.org/https://doi.org/10.1007/s11042-020-08716-w
31. Yang Z, Wang K, Ma S, Huang Y, Kang X, Zhao X. Istego100k: Large-scale image steganalysis dataset. International Workshop on Digital Watermarking, 2019.