IRAQI Academic Scientific Journals
Available at https://www.iasj.net/iasj
Iraqi Academic Scientific Journals
Journal homepage:
https://journals.uokerbala.edu.iq/index.php/UOKJ

Review Article

Coverless Text Information Hiding Techniques: A Review

Sabaa Hamid Rashid* Dhamyaa A. Nasrawi*

*Department of Computer Science, College of Computer Science and Information Technology, University of Kerbala, Iraq

Article Info

Article history:

Received 12 -3 -2024

Received in revised form 21-4 -2024

Accepted 29 -4 -2024

Available online 30 -6-2024

Keywords: Coverless text information hiding, Steganalysis, Information security, Steganography.

Abstract

In the digital era, protecting confidential information from unauthorized access is crucial. Information can be represented through a variety of communicative media, including text, video, audio, and images, with text being the most common. Traditional methods require carriers to disguise secret information, leading to carrier modifications which are challenging to avoid steganalysis. In contrast, coverless information hiding does not modify the carrier and transfers Secret message directly via the stego cover's built-in attributes. The most crucial positive significance for the development of coverless information hiding technology is based on the Chinese mathematical phrase. The primary goal of this review is to examine the most recent findings in the fields of coverless hiding, development approaches, selected datasets, metrics of performance, and issues of hiding applications in English, Chinese, and other languages. The findings demonstrate that researchers have considered the Keywords and tags, approaches while the approach-based Markov model is mainly used with the English language. Additionally, the study reveals that hiding capacity, success rate, and security analysis metrics are the most common metrics used to evaluate coverless information hiding performance. As a final point, the unresolved issues and potential future directions are addressed to improve hiding capacity and algorithm efficiency, embed and extract information correctly, and extend these techniques to other languages.

Corresponding Author E-mail : saba.h@uokerbala.edu.iq
Peer review under responsibility of Iraqi Academic Scientific Journal and University of Kerbala.

1.Introduction

With the significant improvements in signal processing and transmission systems, multimedia data becomes simple to alter, obtain, and replicate. Therefore, network security and secure communications via public and private channels are more crucial challenges, particularly as the use of computers grows in both social and professional contexts. One method for obtaining a secure communication medium and safeguarding the information during transmission is data hiding. It provides a method for embedding data into different types of media (text, video, and image) while minimizing the amount of “host” signal deterioration that can be detected; the hidden data should be unnoticeable and inaudible to an observer [1].

Due to the secret message’s modest size compared to the cover text’s massive amount of data, it is considerably easier and more reliable to hide and retrieve secret messages using electronic media rather than physical things. Since computers can effectively manipulate and execute data and algorithms required to retrieve Secret message, the extraction process can be mechanized when the data is electronic [2].

Steganography is the art of sending covert communications or concealed information via a network so that a third party cannot discover its existence [2]. Steganography comes from the Greek words ‘steganos,’ which means ‘covered or concealed’, and ‘graphene’, which means ‘writing’ [3]. The information intended to be concealed in the cover data is referred to as embedded data in the context of steganography. The data that includes both the embedded information and the cover signal is known as stego data. The method of embedding involves incorporating concealed or embedded information into cover data. The original, including the text, audio, and video, are all called the cover. While the field of steganalysis belongs to the detection of steganography, estimation of message length, and its extraction [2, 3].

There are numerous ways to arrange steganography. For instance, the kind of carrier determines whether a file is text, image, audio, video, or a protocol file used to incorporate hidden data. Pure steganography, secret key steganography, and public-key steganography are all different ways of hiding information based on the type of the used key. Additionally, three methods are utilized to secure information in a cover object dependent on the embedding method: insertion-based, substitution-based, and generation-based techniques [4, 5]. Due to the lack of redundant data in a text file compared to an image or an audio file, text steganography is thought to be the most challenging [6].

The chosen carrier can take various forms, including pictures, texts, audio, and videos. When performing the information-concealing process, the unnecessary portion of a picture, text, audio, or video carrier is employed to conceal secret information. Traditional information hiding techniques have a significant problem because they cause particular modifications in the selected carrier despite Secret message. The modified carrier cannot withstand all steganalysis attacks, making it a poor choice for carrying sensitive data. Therefore, in this approach, there is always a possibility that cyber criminals could access or destroy secret data [7].

The premise of coverless information hiding resolves the problematic issue of conventional data concealing methods’ poor security and low concealment. Without changing the carrier, such sensitive data would be transmitted between the sender and the receiver. The shared carrier can be used to choose or create a secret message. Due to their coverless nature, carriers can fend against most steganalysis techniques and malevolent attempts [8].

The fundamental aim of this literature review is to examine the most recent studies to provide answers to the proposed research questions concerning coverless hiding, development approaches, metrics of performance, selected datasets, and issues of hiding applications in English, Chinese, and other languages.

The current paper has the following key contributions:

1. It distinguishes coverless hiding from traditional methods by enabling direct transfer without carrier modification, reducing steganalysis susceptibility.
2. Explores recent advancements in technology across languages, focusing on English and Chinese, highlights prevalence of approach-based Markov model in English applications.
3. Identifies key performance metrics like hiding capacity, success rate, and security analysis.
4. Outlines unresolved challenges and future directions, including capacity enhancement, algorithm efficiency, and extension to other languages.

The rest of this paper is organized as follows. Section 2 presents a brief background on coverless text information hiding. Section 3 demonstrates the literature review methodology. A literature review relating to coverless text information hiding techniques presented in Section 4. The discussion is explained in Section 5. Finally, the conclusion is summarized in Section 6.

2.Coverless information hiding

Researchers recently coined the term "coverless information hiding" to address the problem with the typical information hiding methods now in use. It is essential to distinguish between the term "coverless" and the lack of a carrier signal. Coverless information hiding refers to the fact that the Secret message does not need to be embedded in a specified carrier.

Coverless information hiding refers to the fact that the Secret message does not need to be embedded in a specified carrier. Because the original carrier signal remains unchanged, this method of secret information hiding makes coverless information hiding approaches more resistant to existing steganalysis attacks [7].

Although coverless information concealment is a novel concept, it has been implemented daily. An acrostic poem is one of the finest examples that prove that the coverless concealment of data is not an entirely novel concept for people. Lewis Carroll wrote an acrostic poem 'Alice Pleasance Liddell' [9] is the individual name that is concealed in this acrostic poem [7], see Fig. 1.

A boat beneath a sunny sky,
Lingering onward dreamily
In an evening of July--

Children three that nestle near,
Eager eye and willing ear,
Pleased a simple tale to hear--

Long has paled that sunny sky:
Echoes fade and memories die.
Autumn frosts have slain July.

Still she haunts me, phantomwise,
Alice moving under skies
Never seen by waking eyes.

Children yet, the tale to hear,
Eager eye and willing ear,
Lovingly shall nestle near.

In a Wonderland they lie,
Dreaming as the days go by,
Dreaming as the summers die:

Ever drifting down the stream--
Lingering in the golden gleam--
Life, what is it but a dream?

Figure 1. "A Boat Beneath a Sunny Sky" by Lewis Carroll [9]

Texts have less redundant information than images and videos, making it more challenging to apply the techniques of text information-hiding. Nevertheless, texts offer some benefits, including easy encoding, a large amount of data, a small amount of space occupied, and frequent use. Various scholars have expressed interest in text information concealment technology due to its significance in wireless transmission, covert communication, copyright complications, and other areas. In parallel with the development of text information concealment and automatic text-generating technology, text steganalysis technology also continues flourishing. This has become a significant challenge to information hiding [10]. In general, coverless information hiding techniques have three main characters (no modification, no embedding, resistant to steganalysis attacks) [11-13].

The methods of coverless text information hiding, according to Xiang et al. [10], generally fall into two categories:

1. Search method [6]: The suggested method searches for accessible carriers on the Internet that are compatible with the secret message's statistical characteristics expecting that a suitable carrier webpage will be found after applying this method. Following the selection of a carrier, the secret message's distribution within the carrier is scrutinized, and communication relations are added to the carrier's address.
2. Generation method [14, 15] This method automatically generates paraphrases; it is a new and helpful source of transformations for linguistic steganography.

In contrast, Wang et al. [16] present three primary categories of these methods:

1. Steganography by Cover Search: This method scans the Internet for an appropriate
2. website that can serve as a carrier. This page must contain every character from the hidden message. The URL will be updated with the resulting string after those characters' places on the website are encoded[6].
3. Steganography by Cover Generation: As the carrier, Chang and Clark [15] create a new text using the N-gram model. Another common example is the NiceText system, which transforms secret messages into different sentences using a sizable code vocabulary [17]. Luo and Huang [18] use the RNN Encoder-Decoder framework to create Chinese poetry. High-quality text coverings can be created based on the RNN to conceal a hidden bitstream. [19].
4. Steganography by Cover Index: A text corpus from the Internet with books, news, articles, and other contents is developed by Zhou et al. [13]. After breaking down texts into words and creates indexes for each word "label and keyword", it embeds these into secret messages, providing qualified texts. The natural language processing NLP technology's imperceptibility is weak when a secret message is long. Besides, additional semantic problems, including syntax mistakes and poor readability, mainly if a lengthy text is generated.

Although all types are progressing quickly, limitations are also being placed on them by the advancement of natural language processing technologies. When the secret information is lengthy, it is challenging to use the search method. Additionally, the generating method may have further shortcomings, such as semantic ambiguity, sentence failure, and poor readability.

3.Methodology

This review presents a comprehensive analysis of various studies on coverless text information hiding methods. Fig. 2 show the block diagram of review steps.

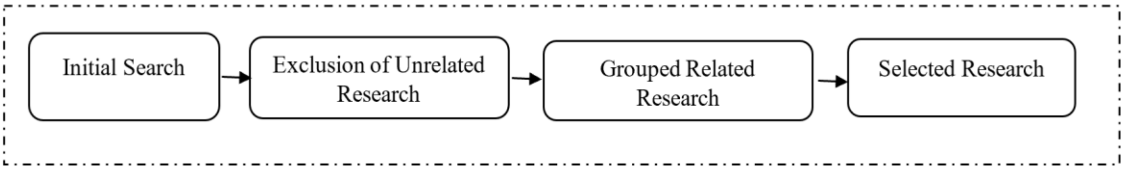

Figure 2: Block diagram of review steps

A. Initial Search

The initial research used search engine file browsers to enter keywords. With the aid of these keywords, related research papers that successfully address the research problem could be found. There were just two Boolean operators used: AND and OR. The search keywords were "Carrier-free Text Steganography," "Coverless information hiding," "Coverless Text Information Hiding," and "Coverless Arabic Text Information Hiding." The platforms searched for were Google Scholar, Academia.edu, Research Gate, IEEE Xplore Digital Library, and ScienceDirect.

B. Exclusion of Unrelated Research

Excluding unrelated works in the current study means that the study is limited to text only, i.e., other media such as images, videos, and audio are not included. This study focuses on text only. Additionally, it removes all research about traditional information hiding since they are not within the scope of this study. All related research was considered in development techniques, surveys, analysis, evaluation, etc. Furthermore, the study examines papers written in English only.

C. Grouped Related Research

The selected research was grouped based on approach, authors, language, metrics, and types to make the comparison and analysis more reliable and easier.

D. Selected Research

The total number of related previous research in this study is 34. All papers are read and grouped for evaluation, comparisons, and analysis.

4.Related Work

This section discusses the literature review on coverless text information hiding techniques, their strength, weakness, and performance metrics researchers use.

The most crucial positive significance for the development of coverless information hiding technology suggested by Chen et al. 2015 [20] was coverless text information hiding based on the Chinese mathematical phrase. Chinese characters were separated into tags, each calculated and connected to an expression in Chinese mathematics. In order to conceal information without modifying the carrier text, this method promotes the premise of "tag + keyword" as the central concept. The proposed method involves stego-vector generation, obtaining a normal text from a more extensive database, and transmitting the retrieved information. The sender sends normal texts to the receiver, who then utilizes an inverse method to recover confidential information while maintaining the integrity of the carrier signal. This technique has low capacity (One keyword in a 1-kilobyte), lacks total keyword count, and needs a vast database, yet is resistant to steganalysis attacks and maintains carrier originality.

Zhou et al. 2016 [14], [21] proposed a new method to address the small hiding capacity in previous method conducted by Chen et al. [20] by hiding multiple Chinese keywords simultaneously in the same text. The method slightly enhanced the capacity with an average hiding capacity of 1.57 (character/text) but required an extensive text database and had a low success rate.

A new coverless text information hiding method was developed by Zhang et al. 2016 [22] using a word rank map and stego-vectors from secret data. They extracted common texts with hidden stego-text, transmitted them without altering the original carrier signal, and used inverse procedures to uncover sensitive information. The method withstands steganalysis attacks and requires a large text database.

Shi et al. 2016 [6] proposed a new model for detecting secret messages by searching webpages on the Internet. The model matches secret message statistical characteristics, analyses carrier distribution, embeds correspondence relations, sends secret messages to a Webpage Searching Server, encodes and compresses positional information, and extracts secret messages by position information. The method offers high embedding capacity (10.32%-80.98%) and good imperceptibility.

Liu et al. 2017 [23] improved the previous methods presented by Chen et al. [20],Zhou et al. [13] , [20] by incorporating part of speech tagging and multi-keywords, enhancing success rate, extraction accuracy, hiding capacity which was equal to 2.24 (character/text), time, and space efficiency. They used the "Word2Vec" language model and expanded the keyword set, improving time efficiency, extraction accuracy, success rate, and hiding capacity. The method also surpassed current steganalysis techniques due to unmodified text carriers.

Zhang et al. 2017[24], [25] enhanced the previous method presented by Zhang et al. [22] by using a hash of frequently occurring terms, words rank map, and distance to hide secret information. The method created a text database, calculated frequent words distance and word rank map, and obtained regular text. The method escaped steganalysis attacks but required an extensive text database, affecting performance.

Liu et al. 2017 [26] proposed a coverless text information hiding technique using news aggregation. The technique involves turning a secret message into a number, concealing it within a visible online news piece, and allowing the receiver to use the secret information. The algorithm is easy to use, reliable, and efficient for sending stego messages. The maximum hiding capacity was determined by three parameters (number of news subjects, blocks, and headlines), where the max bit of secret information was 43 per two div blocks in hiding.

Sun et al.2017 [27] proposed a coverless text information hiding approach using NER systems. The secret message was converted into keywords, searched, and noted using a named entity recognition system. This method embeds directly without modifying the stego-text, allowing it to withstand current steganalysis and detection techniques.

Xia et al. 2017 [28] proposed a coverless text information hiding approach using the LSB of the Character's Unicode. This method converts internet-collected texts into LSB texts and stores them in a database. The method requires an extensive text database and low capacity texts (14 or 15 bits when the number of texts was approximately 200,000) texts.

Wu et al.2018 [11] proposed a coverless text information hiding approach using Chinese conversion strategies. They segmented secret information into keywords, obtained tag sets based on protocol and ID, and selected specific rules from each set. This method improved success rates and hiding capacity, and resisted steganalysis.

Wu et al.2018 [29] improved the method proposed by Wu et al. [11] in western languages by proposing a steganography based on English texts. The method involves breaking secret messages into keywords and using a secret key to obtain tag sets. The study showed effectiveness in hiding capability and steganalysis resistance but had a low success rate compared to Chinese coverless steganography.

Long and Liu 2018 [30] improved the method suggested by Chen et al. [20] using word2vec and distance to obtain similar keywords. They then used similar keywords to increase the set of keywords and retrieved stego-texts with location tags and keywords, achieving 100% success rate. Experimental results showed that the method would not leave any modification trace in texts, and it was robust for current steganalysis tools.

Fu et al. 2018 [12] enhanced method presented by Chen et al. [20] by incorporating a header file for tag placement. The goal was to locate multiple hidden keywords in a text using binary strings and a certain number of keywords. The method used a large-scale index, breaking the original text into terms, generating tags, and providing a header file for more keywords. Despite its effectiveness, it required an extensive database and had some limitations especially the success rate still had some weaknesses.

Chen X. and Chen S. 2019 [31] proposed a text coverless information hiding algorithm based on the compound and selection of words to improve the methods proposed by Ji and Fu [13], Wu and Sun [11] methods. The algorithm aims to select popular terms or words as a compound, separating secret information, reducing carrier texts, and enhancing hiding capacity. The algorithm's efficiency is high, and resistance to steganalysis methods is maintained. However, compound words may be invalid if secret information is encrypted or not natural.

A coverless information hiding method based on keywords was introduced by Ji H. and Fu Z. in 2019 [13]. The signal keyword following preprocessing was utilized as the units, while the word components from method proposed by Chen et al. [20] were used as location tags. The method creates a mapping between binary strings and keywords to conceal numerous keywords in a text. The process involves dividing the document into keywords sequences and attaching a location tag. The method has a high success rate for short text but has weak robustness and low hiding capacity.

Wu et al. proposed several coverless text steganography methods-based Markov chain model. They proposed a coverless text steganography method based on single bit rules in 2019 [32] . The method involves navigating a dataset, selecting sentences with the same began term, establishing a Markov state transition diagram, trimming it for optimal results, and setting a binary code. The method was tested on movie reviews and news datasets, resulting in improved embedding rate (embedding rate= 2.73), and low perplexity (15.38±6.77, 17.05±15.21). This method was improved in 2019 [33] using the maximum variable bit embedding instead of the usual fixed bit embedding in method presented by Wu et al. [32]. Experimental results showed improved embedding rate (embedding rate= 2.75) and low perplexity (15.29, 16.91) in movie reviews and news datasets compared to previous works. In 2019 [34] new improvement was implemented based on half-frequency crossover rule. They used 3-gram and 4-gram half-frequency crossover as examples and tested the method on movie reviews and news datasets. The results showed an embedding rate of 2.78 and perplexity of 15.97±7.57 and 17.41±8.91, respectively. Another improvement was implemented in 2019 [35] based multi-rule language models instead of a single gram model. The embedding rate= 2.85, and the perplexity was (52.05±35.80, 20.52±13.98) in the two datasets. Then, two improvements were made in 2020, the first in [36] using state transition-binary sequence (STBS)-based to generate semantically smooth texts. The result of perplexity (14.07 ± 8.83, 13.34 ± 9.90, 12.89 ± 8.75) is minimal compared to similar models in Twitter, IMDB, and News datasets, and embedding rate is 2.18. The second improvement that made in 2020 in [37] by index and one-bit embedding. The perplexity is small among similar models (16.78 ± 7.89, 14.97 ± 2.55, 25.92 ± 18.59) in Twitter, IMDB, and News datasets respectively, with a 2.95 embedding rate.

Long et al. 2019 [38] proposed a coverless information hiding method using web texts. They segmented secret information into keywords and extracted them using the TextRank algorithm. They used web spider technology to capture web texts with secret information, then used a 2-D coordinate system to describe the location. The method also used the "Word2Vec" language model to expand the keyword set. The study found a high success rate of 99% for different secret information lengths, with an average hiding capacity of 10.53, but revealed decreased extraction accuracy with longer information lengths.

Wang K. and Gao Q. 2019 [39] proposed a coverless information hiding method using character features to represent binary digits. They found a mapping function between character features and a Binary Digit String (BDS) and used the Parity of Chinese Characters' Stroke Number (PCCSN) as a character feature. The experiments revealed that the proposed methods had a high embedding rate of 6.25% in best case and reached 25% in the improved method, as well as more security, good robustness, and a high success rate. Besides, this method had some advantages, such as resisting the format transformation attack and improving semantic and statistical detection. It exhibited no need for additional information and applied in many languages. Notably, large-scale text corpus was significant for these methods; hence, they needed large text corpus.

Zhou et al. 2020 [40] proposed a coverless information hiding method based on the double-tags and twice-send. This method was improved methods presented by Zhou et al. [21], Sun et al. [27] in terms of low capacity. They established two-character combinations in a two-dimensional array with a combo number threshold. The experimental results displayed that the proposed method made an improvement in the hiding capacity = 31.38%.

Zhang W. et al. 2020 [41] presented a coverless text steganography method based on the characteristics of word association to construct the word node tree by both sender and receiver. The sender chooses texts from an isomorphic set, sends messages, and decodes hidden data. This method has a higher average hiding capacity (82.35 bits per text) than popular methods, stable success rate, and resistance to detection.

Liu Y. and Wu J. 2020 [42] proposed a method using Chinese Pinyin to select hidden tags from Pinyin combinations of two words. They used part of speech (POS) to hide keyword numbers, eliminating redundancy and ensuring uniqueness in stego-texts. The method expanded the keyword set using the "Word2Vec" language model. The proposed method, without modification to text carriers, effectively resists existing steganalysis methods and attacks, demonstrating high hiding capacity, success rate, extraction accuracy, and time efficiency.

Xiang et al. 2021 [10] introduced a coverless text steganography method using multi-index segmentation to segment secret information into keywords. The method uses a word index table, random increment factor, and mixed indexes to convert big data texts into secret data, with the greediest algorithm being used. The results showed an improvement in robustness, so this method resisted attacks and had high security and a fast average hiding rate= 42.48 (bit/s). However, the name entities could not be hidden in this method, and the average success rate was 94.89%.

Qin et al. 2021 [43] presented a robust coverless text steganography method based on the big data text on the Internet. The mixed index was transmitted as secret information, which contained the TF-IDF features of the words and topic model distribution of the text. The results revealed that this method resisted attacks and had high security. However, the name entities could not be hidden in this method, and the average success rate was 98.24%. In comparison, the average hiding capacity reached (60.40, 64.36) with and without removing the highest point.

Liu et al. 2021 [44] improved the previous methods presented by Chen et al. [20], Wu et al.[11] in terms of success rate, extraction accuracy, and hiding capacity. Part of Speech (POS) used to hide keyword numbers and optimize stego-text retrieval. They used Chinese character components as locating marks and expanded the keyword set using the "Word2Vec" language model. The method improved embedding capacity and removed ambiguity in locating markers. As well as the method enhances extraction accuracy by increasing the number of keywords in stego-texts mapped to POS, improving embedding success rate, and withstands current steganalysis techniques.

Wang et al. 2021 [16] introduced a new coverless text steganography method using Chinese character component structures. These structures were divided into groups based on usage frequency, expressing a specific Binary Digital String (BDS). The Minimal Square Matrix (MSM) was converted into a Code Square Matrix (CSM). The BDSs were converted into binary digital slices (BiDSs) using the Chinese remainder theorem. The receiver then reconstructed the BDS and determined the corresponding row and column numbers. As a result, the method did not modify a text in any way, had a good imperceptibility, high robustness, high success rate (100%), high capacity, no detection by semantics and statistical steganalysis methods, and extensibility to implement in different languages.

Wen et al. 2021 [45] introduced a new text coverless information concealment technique using Morse Code, lists, loops, initiators, and groupings. The method creates a character correspondence table and allows high-frequency words to be represented. Experiments showed this method improved hiding capacity, confidentiality, and text search rate, but longer words took longer to hide and extract.

Guan et al. 2022 [8] proposed a polynomial-based coverless information hiding technique for Chinese text. To increase the number of keywords in the index table, additional keywords could be chosen using the tags (one tag to multiple keywords). The location of the keyword in a secret message was determined by text vocabulary matching. The study uses polynomials to encrypt tag index and location data, resulting in increased security. Besides, the hiding success could nearly approach 100% for any size of the webpage text database, which went up with the increased size of the webpage text database. Even if the smallest database was selected for testing, the proposed method could approach above 95% success rate. The average hidden capacity with experiments implemented on four message sets showed that the proposed method was higher than the similar methods proposed by Chen et al. [20], Fu et al. [11].

A. Majumder et al. 2023 [48] proposed new method by creating a dataset for the domain values of its attributes, the method focuses on synthesising a database. The concealed message is revealed when the dataset is sorted using a comparison-based approach. The trick of the trade is to conceal everything and everything while maintaining the database's semantic integrity. The effectiveness of our strategy, which outperforms recently proposed approaches and offers a solution for highly resistant covert communication, is assessed by considering multiple security measures and doing a thorough analysis of time complexity.

Table I below concludes the methods used in the studies and shows the strengths and weaknesses of each one.

TABLE I. OVERVIEW OF COVERLESS TEXT INFORMATION HIDING TECHNIQUES

References with year	Methodology	Strength	Weakness	Dataset	Metrics	Language
2015 [20]	It uses and portrays Chinese characters as mathematical expressions.	It Resists the attacks of steganalysis and preserves the carrier's originality.	With low capacity, unknown the number of keywords, requiring a vast text database.	Chinese text database	Capacity	Chinese
2016 [14], [21]	It retrieves stego-text that contains both the number of keywords and the private information.	It enhances the capacity, knows the total number of keywords, resists steganalysis attacks	It demands an extensive text database, consumes time, limited improvement and a low success rate.	Sogou Labs	Capacity, success rate	Chinese
2016 [22]	Using the rank map to generate stego-vectors from the secret message.	Resisting all kinds of existing steganalysis methods, no cover modification.	Capacity is inadequate, an extensive text database is needed.	Text big data	Capacity, robustness	English
2016 [6]	Based on features of huge amount	Sending only a URL, no original	It needs enormous	Set of	Capacity, validity of	Chinese

References with year	Methodology	Strength	Weakness	Dataset	Metrics	Language
	Internet webpages	text change, high embedding capacity, and good imperceptibility.	webpages.	webpages	the algorithm	
2017 [23]	Based on the part of speech tagging using multi-keywords.	It improves success rate, extraction accuracy, hiding capacity, time, and space efficiency.	It needs an extensive text database.	Chinese corpus of Sogou Lab	Capacity, success rate,extraction accuracy, security, time efficiency.	Chinese
2017[24], [25]	Using a hash of frequently occurring terms and the words rank map.	Safe, can escape from almost all steganalysis methods, no cover modification.	It has a low capacity, needs an extensive text database, needs to change the private keys periodically.	News websites	Capacity	English
2017 [26]	Based on news aggregation, which transforms the secret message M into a large integer	The algorithm is easy to use, reliable against any steganalysis, not need an extensive database.	The database needs regular intervals updates, and capacity is based on the amount of news.	Sina News	Capacity, robustness, security.	Chinese
2017 [27]	Named entities are used to mark the locations of the Secret message based on big data.	Reliable against any steganalysis, no modification, high security.	It needs an extensive text database.	CoNLL03, ACE05	Robustness, security.	English
2017 [28]	Based the LSBs of the character's Unicode of the covers.	Resisting current detecting techniques, no modification in cover.	It has low capacity, needs an extensive text database.	Databases of 200,000 texts	Capacity	Chinese
2018 [11]	Based on two tag selecting strategies to determine the tags	Improving success rate and hiding capacity, resisting the steganalysis.	It needs an extensive text database, low capacity, need an index of the database	Sougou Lab.	Capacity, success rate, security.	Chinese
2018 [29]	coverless information hiding based on English texts.	Improving hiding capacity, resisting the steganalysis.	Low success rate, needs an extensive database, need an index of the database	Reuters Corpus Volume1 (RCV1)	Capacity, success rate, security.	English
2018 [30]	Method of text coverless information hiding based on word2vec to obtain similar keywords.	High success rate, improving hiding capacity, resists steganalysis, used similar words when text retrieval fails.	It fails if the keyword does not exist in the text big data, needs an extensive database	Sogou Lab	Capacity, success rate.	Chinese
2018 [12]	Use a tag to position the keywords as much as possible	It hides more information, resists all steganalysis methods	It needs an extensive database. weaknesses of success rate	Text from the Internet.	Capacity, success rate.	Chinese
2019 [31]	Based on the compound and selection of words	High algorithm efficiency, resists all steganalysis methods	It needs an extensive database, low security.	Text from the Internet.	Capacity, success rate, security	Chinese
2019 [13]	Based on keywords that are used with	resists all steganalysis	It has weak robustness and low	Sougou	Capacity, success rate,	Chinese

References with year	Methodology	Strength	Weakness	Dataset	Metrics	Language
	location tags to build the index.	methods, high success rate for small text with limit.	hiding capacity.	Labs.	security, robustness.	
2019 [32], [33], [34], [35], 2020 [36], [37]	Based on the Markov model, the transition probability is used to create stegotext	It preserves the characteristics and affects the algorithm, It preserves the characteristics and affects the algorithm.	Based on a sample library of sentences with the same word, It needs an extensive database.	Collection of reviews about movies and news.	Algorithm performance , embedding rate.	English
2019 [38]	Based on web text regards existing massive internet text as big data	The presence of many webpages.	Extraction accuracy will be decreased with increasing secret information length.	Chinese corpus of Sogou Lab	Capacity, success rate, extraction accuracy.	Chinese
2019 [39]	Based on the parity of Chinese characters' stroke numbers.	It resists attacks, no need for additional information, applied in many languages.	It needs a large text corpus.	webpages	Embedding rate, success rate, availability.	Chinese
2020 [40]	Based on the double tags in a text by odd-even adjudgment.	Improving the success rate, hiding capacity, and efficiency of algorithm.	It needs an extensive database.	20 million selected carriers	Capacity, success rate.	Chinese
2020 [41]	Based on characteristics of word association to build the word node tree.	Stable success rate, improved hiding capacity, and resistance to detection.	It needs an extensive database.	Online news and film reviews	Resistance to detection Capacity, security,	English
2020 [42]	The Pinyin combinations of two words are used to choose the hidden tags.	It shows improvement in success rate, extraction accuracy, hiding capacity, time, and space efficiency.	It needs an extensive database.	Chinese corpus of Sogou Lab	Capacity, success rate, extraction accuracy, security, time efficiency.	Chinese
2021 [10]	Based on segmenting the secret information into several keywords	Improving robustness, resisted attacks, high security, high success rate, fast average hiding rate	It needs big data text, cannot hide some entity names, and does not reach a 100% success rate.	Chinese corpus of Sogou Lab	Robustness, success rate, security, hiding rate.	Chinese
2021 [43]	Based on the big data on the Internet. secret information contains the TF-IDF and topic model.	Resisting attacks, showing high security.	needs big data text, cannot hide some entity names, not reach a 100% success rate.	Sogou Lab	Robustness, success rate, security, hiding rate, hiding capacity	Chinese
2021 [44]	POS is utilized to hide the number of keywords after pretreatment.	It shows improvement in success rate, extraction accuracy, hiding capacity, time, and space efficiency.	It needs an extensive database.	Chinese corpus of Sogou Lab	Capacity, success rate, extraction accuracy, security, time efficiency.	Chinese
2021 [16]	Using structures' encoding to express various BiDSs to guarantee that a secret message can	No matter how long a text is, no modification, good imperceptibility, high robustness,		Collected from the Internet science, novels, news,	Capacity, success rate, robustness.	Chinese

References with year	Methodology	Strength	Weakness	Dataset	Metrics	Language
	be effectively concealed.	success rate, and capacity, resist steganalysis methods, extensibility to other languages.		and e-commerce.		
2021 [45]	Based on a combination of Morse Code.	Improve hiding capacity, confidentiality, efficiency and text search rate.		5076 English texts from the Internet	Capacity, efficiency testing,	English
2022 [8]	Hiding a secret message using polynomial encryption.	It shows an improvement in success rate, hiding capacity, security, and extraction accuracy	It needs an extensive database.	Collected from the Internet:	Capacity, success rate, extraction accuracy, security	Chinese
2023[48]	unique database synthesis technique	Hiding in any language,		Database from kaggle	Capacity, success rate, extraction accuracy, security, time complixty	Any language

5.Discussion

Several surveys have been published about coverless information hiding in image based [46], video based [47], as well as text based [7]. The survey on the text has been limited to specific years. Those researchers discuss the current scope of the technique used in the coverless text information hiding till 2018. The primary goal of this literature review is to examine cutting-edge research in Chinese, English, and other languages to answer the proposed questions on the type of coverless text information hiding method, the development approaches, selected dataset, performance metrics, authors countries, and challenges of hiding applications. To achieve these objectives, six research questions are addressed. Table II presents the research questions and motivations. In comparison, the subsequent subsections explain the details of each research question.

Q1: What are the approaches used for coverless text information hiding?

As shown from the previous related works in Table 1, specific techniques affect the development of coverless text information hiding. These techniques are based on keywords, tags, frequency, Markov model, part of speech, etc. All these studies have several datasets and languages. Table 3 shows the details.

From Table 3, most approaches depend on (keywords and Tags) with indexing which they have more efficient in hiding and extraction process, show Fig. 3.

TABLE 2. LIST OF THE SURVEY RESEARCH QUESTIONS

No.	Research Questions	Motivations
Q1	What are the approaches and techniques used for coverless text information hiding?	Identifying the state-of-the-art approaches may be significant for developers to provide more fit solutions by working and evolving the recent techniques and trends.
Q2	What is language?	Identifying the languages used in coverless text information hiding techniques.
Q3	What is the authors' country that interesting coverless text information hiding techniques?	Identifying the country of authors interested in this topic and which country significantly affects the development of coverless text information hiding techniques.
Q4	What are the commonly used metrics to evaluate the performance of coverless text information hiding techniques?	Identifying the commonly used metrics to evaluate and comparing the performance of coverless text information hiding techniques.
Q5	What are the quantities of the coverless text information hiding publication in each year?	Counting the number of published papers to figure out when the subject became popular and significant.
Q6	What are the main challenges facing the implementation of coverless text information hiding techniques?	Spotting open-research problems in developing coverless text information hiding techniques and providing future guidelines to continue developing the current issues.

TABLE 3. LIST OF MOST USED APPROACHES

No.	Approach	Description	References
1	Keywords and tags, word frequency	The structure is expressed as "label and keyword" with frequency.	[20-26], [8], [11-14], [29], [31],[40]
2	Markov Model and word tree	Based on the Markov model, the transition probability is used to create steganographic text based on a word tree.	[32-37], [41]
3	Index with POS	The structure is expressed as "label + keyword," and Part of Speech (POS) is utilized to hide the number of keywords.	[42], [44]
4	Search method	Techniques will search the Internet for an appropriate webpage to serve as a carrier.	[6], [38]
5	Others	Based on character components, Unicode, character features, NER, word2vec, Tf-idf, uniqe database	[45], [16], [27], [28], [39], [30], [10], [43], [48]

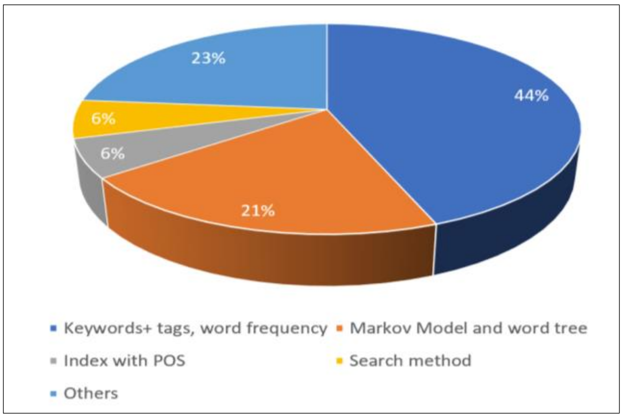

Figure 3. Illustration of most used approaches of coverless text information hiding

Q2: What are languages used for coverless text information hiding?

Most papers presented in Table 1 were implemented in the Chinese language based on characters components, features, structures, etc., but there were some papers implemented in the English language, Table 4 shows the details.

TABLE 4. LIST OF LANGUAGES USED FOR COVERLESS TEXT INFORMATION HIDING

No.	Language	Description	References
1	Chinese	Based on characters components, features, structures, punctuation, Unicode, stroke, Pinyin	[6], [8], [10-14], [16], [20-21], [23], [26], [28], [30], [31], [38-40], [42-44]
2	English	Based on word frequency, probability in the Markov model, and word tree.	[22], [24-25], [27], [29], [32-37], [41],[45]
3	Others	Unfortunately, no papers implement another language.	No papers

Q3: What is the authors' country?

Identifying the country of authors interested in this topic means which country significantly affects the development of coverless text information hiding techniques? It is noted from Table 5 that 31 papers are from Chinese, while only 3 papers are from other nationalities.

TABLE 5. LIST OF AUTHORS' COUNTRY INTERESTED IN COVERLESS TEXT INFORMATION HIDING

No.	Nationality	References
1	Chinese, USA, Japan	[20]
2	Chinese, Canada, Taiwan	[14]
3	USA	[27]
4	India	[48]
5	Chinese	[6], [8], [10-13],[16], [21-45]

Fig. 4 and Fig. 5 explain the answers to questions 2 and 3 respectively.

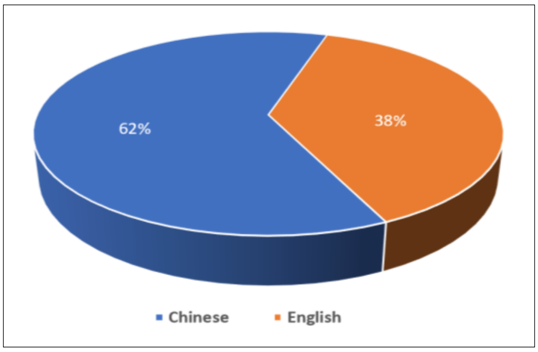

Figure 4. Illustration of the languages used in coverless text information hiding

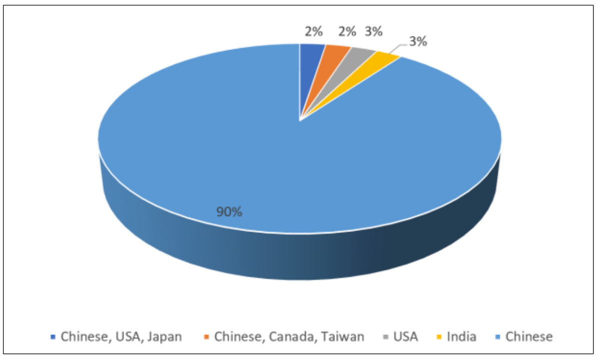

Figure 5. Authors' country interested in coverless text information hiding

Q4: What are the evaluation metrics?
The available coverless text information hiding methods are evaluated and contrasted based on a variety of critical factors such as hiding capacity, algorithm efficiency, success rate, ability to resist steganalysis, and theoretical and real-world significance. Table 6 presents a summary and comparison of 8 evaluation metrics types used in developing coverless text information hiding methods over the selected papers. The table shows that the most common measure used for both languages (Chinese and English) is hiding capacity, then the success rate and security analysis, respectively.

TABLE 6. LIST OF EVALUATION METRICS USED FOR COVERLESS TEXT INFORMATION HIDING

No.	Language	Description	References
1	Hiding capacity	The number of characters or keywords that can be hidden in one text.	All papers except [27]
2	Success rate	Evaluating the performance of the embedding algorithm	[8], [10-14], [16], [21], [23], [29-31], [38-40], [42-44], [48]
3	Extracting accuracy	Evaluating the performance of the extracting algorithm (distance between the secret message and the extracted message).	[23], [8], [38], [42], [44], [48]
4	Security Analysis	Resistance to attacks.	[8], [10-11], [13], [23], [26-27], [29], [31],[41-44], [48]
5	Perplexity	Measuring the quality of the language generation model. The smaller the perplexity is, the closer the statistical distribution of the text.	[32-37]
6	Hiding efficiency	The time needed to hide information.	[23], [44-45], [42], [48]
7	Availability	A large scale-corpus will prompt the availability of these methods.	[39], [48]
8	Validity of Algorithm	Can the algorithm embed and extract secret messages correctly?	[6]

Q5: What is the paper publication in each year?
The most crucial positive significance of the development of coverless information hiding technology was suggested in 2015; the topic became an interesting issue in the following years. Table 7 shows the number of papers about coverless information hiding technology published each year until this report is written.

TABLE 7. LIST OF LANGUAGES USED FOR COVERLESS TEXT INFORMATION HIDING

No.	Year	References
1	2015	[20]
2	2016	[14], [21], [22], [6]
3	2017	[23-28]
4	2018	[11], [29], [30], [12]
5	2019	[13], [31-35], [38-39]
6	2020	[36-37], [40-42]
7	2021	[10], [16], [43-45]
8	2022	[8]
9	2023	[48]

Table 7 illustrates that most publications occurred in 2019, then 2017, 2020, and 2021 respectively.

Researchers have become interested in the idea of coverless information hiding since it was first published in 2015; yet, only a few publications addressing hiding capacity and success rate have been authored. The number of publications decreased after 2019 despite an increase in the proposed methods, which could be attributed to the Coronavirus outbreak, which was one of the year's most popular topics. This study examines the body of prior research up until 2023, Fig. 6 and Fig. 7 explain the answers to questions 4 and 5 respectively.

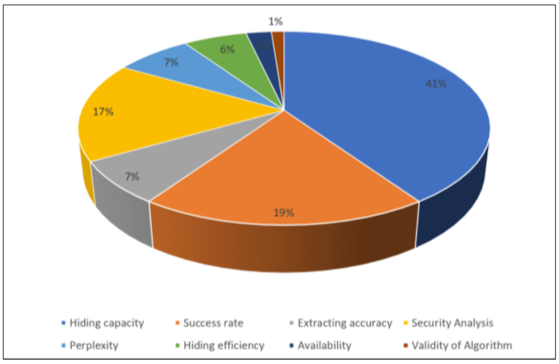

Figure 6.Illustration of the evaluation metrics

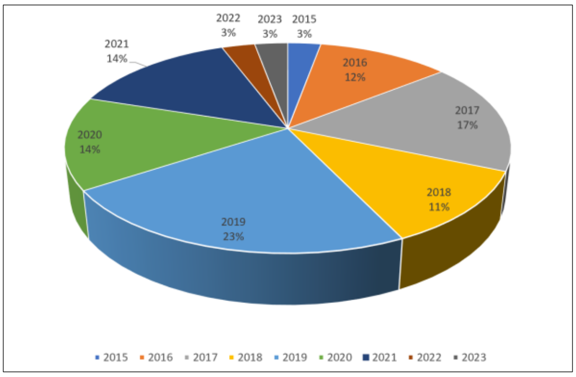

Figure 7. Paper's publications in each year

Q6: What are the challenges in coverless text information hiding techniques?
In brief, the problem of the low hiding capacity continues to be the key obstacle for the research. In fact, certain methods fail to successfully conceal or extract some secret messages. Additional complications include the requirement for enormous databases in all varieties of coverless information hiding. As opposed to this, the core problem with generation-based types is ambiguity and semantic analysis. Therefore, it is extremely difficult to apply similar methods to other languages like French, Japanese, or Arabic, which incorporate an array of inherent features that may be helpful in coverless information hiding.

6.Conclusions

This survey has covered several selected papers that have focused specifically on coverless text information hiding techniques and methods which have no cover modification, no embedding, and resist all kinds of existing steganalysis methods. In general, information hiding is the art of sending secret messages via a network without a third party being able to detect them. Most of the coverless text information hiding techniques are divided into two models: the Generation-based model and the Search-based model. These techniques are sometimes classified into three models: cover search, cover generation, and cover index. This work addresses six research questions for studying state of the art research for Chinese, English, and other languages. These questions include the type of coverless hiding models, the development approaches, selected dataset and language, performance metrics, authors' countries, and development challenges of hiding applications. However, there is little research in the search model, while most research is in the cover index model. The complexity of the generation-based model is more than the others because of the ambiguity in natural language processing. Several approaches have been used to implement coverless text information in the discussed studies, based on multi keywords and tags, Markov model, frequency, part of speech, etc., while 62% of research was implemented in Chinese and the rest ration in English. The most common measure used for both languages (Chinese and English) is hiding capacity, then the success rate and security analysis, respectively. Coverless information hiding gained researchers' interest in 2015. In 2019, there was an increase in suggested methods but a decline in publications over the years. Future studies are expected to focus on coverless text information hiding.
Coverless text information hiding techniques still had limitations, like low capacity, extraction accuracy, and dataset size. Consequently, coverless text information hiding techniques may face challenges in the accuracy of hiding and extracting, hiding capacity, and implementation in other languages. However, from the survey above, it can be said that the coverless text information hiding has high leverage in improving the security and robustness of transmitted data and high resistance to attacks.

REFERENCES

[1] M. K. Khan, "Research advances in data hiding for multimedia security," Multimed. Tools. Appl., vol. 52, pp. 257-261, 2011.

[2] K. Rabah, "Steganography-The Art of Hiding Data," Inf. Technol. J., vol. 3, pp. 245-269, 2004.

[3] M. Mahajan and N. Kaur, "Adaptive steganography: a survey of recent statistical aware steganography techniques," Int. J. Comput. Netw. Inf. Secur., vol. 4, no. 10, p. 76, 2012.

[4] R. Oppliger, Security technologies for the world wide web. London, UK: Artech House, 2003.

[5] S. S. Baawi, D. A. Nasrawi, and L. T. abdulameer, "Improvement of “Text Steganography Based on Unicode of Characters in Multilingual” by Custom Font with Special Properties," IOP Conf. Ser.: Mater. Sci. Eng., vol. 870, no. 1, p. 012125, 2020.

[6] S. Shi, Y. Qi, and Y. Huang, "An approach to text steganography based on search in internet," in International Computer Symposium (ICS), Chiayi, Taiwan, 2016, pp. 227-232: IEEE.

[7] S. Ali, "A State-of-the-Art Survey of Coverless Text Information Hiding," Int. J. Comput. Netw. Inf. Secur., vol. 10, no. 7, pp. 52-58, 2018.

[8] B. Guan, L. Gong, and Y. Shen, "A novel coverless text steganographic algorithm based on polynomial encryption," Secur. Commun. Netw. , vol. 2022, p. 12, 2022.

[9] L. Carroll. (2023, Sep. 07, 2023). A Boat Beneath a Sunny Sky. Available: https://www.poetryfoundation.org/poems/43907/a-boat-beneath-a-sunny-sky

[10] L. Xiang, J. Qin, X. Xiang, Y. Tan, and N. N. Xiong, "A robust text coverless information hiding based on multi-index method," Intell. Autom. Soft Comput., vol. 29, no. 3, pp. 899-914, 2021.

[11] Y. Wu and X. Sun, "Text coverless information hiding method based on hybrid tags," J. Internet Technol., vol. 19, no. 3, pp. 649-655, 2018.

[12] Z. Fu, H. Ji, and Y. Ding, "Label model based coverless information hiding method," J. Internet Technol., vol. 19, no. 5, pp. 1509-1514, 2018.

[13] H. Ji and Z. Fu, "Coverless information hiding method based on the keyword," Int. J. High Perform. Comput. Netw., vol. 14, no. 1, pp. 1-7, 2019.

[14] Z. Zhou, Y. Mu, N. Zhao, Q. M. J. Wu, and C.-N. Yang, "Coverless Information Hiding Method Based on Multi-keywords," in Cloud Computing and Security, Cham, 2016, pp. 39-47: Springer International Publishing.

[15] C. Y. Chang and S. Clark, "Linguistic steganography using automatically generated paraphrases," in Human Language Technologies: The 2010 Annual Conference of the North American Chapter of the Association for Computational Linguistics, LosAngeles,California, 2010, pp. 591-599.

[16] K. Wang, X. Yu, and Z. Zou, "A Coverless Text Steganography by Encoding the Chinese Characters' Component Structures," Int. J. Digit. Crime Forensics, vol. 13, no. 6, pp. 1-17, 2021.

[17] M. Chapman and G. Davida, "Hiding the hidden: A software system for concealing ciphertext as innocuous text," in Information and Communications Security, Berlin, Heidelberg, 1997, pp. 335-345: Springer Berlin Heidelberg.

[18] Y. Luo and Y. Huang, "Text steganography with high embedding rate: Using recurrent neural networks to generate chinese classic poetry," in Proceedings of the 5th ACM workshop on information hiding and multimedia security, New York, United States, 2017, pp. 99-104.

[19] Z.-L. Yang, X.-Q. Guo, Z.-M. Chen, Y.-F. Huang, and Y.-J. Zhang, "RNN-stega: Linguistic steganography based on recurrent neural networks," IEEE Trans. Inf. Forensics Secur., vol. 14, no. 5, pp. 1280-1295, 2018.

[20] X. Chen, H. Sun, Y. Tobe, Z. Zhou, and X. Sun, "Coverless Information Hiding Method Based on the Chinese Mathematical Expression," in Cloud Computing and Security, Cham, 2015, pp. 133-143: Springer International Publishing.

[21] Z. Zhou, Y. Mu, C.-N. Yang, and N. Zhao, "Coverless multi-keywords information hiding method based on text," Int. J. Secur. its Appl., vol. 10, no. 9, pp. 309-320, 2016.

[22] J. Zhang, J. Shen, L. Wang, and H. Lin, "Coverless Text Information Hiding Method Based on the Word Rank Map," in Cloud Computing and Security, Cham, 2016, pp. 145-155: Springer International Publishing.

[23] Y. Liu, "Institute of Electrical and Electronics Engineers, and IEEE Circuits and Systems Society," in 13th International Conference on Natural Computation, Fuzzy Systems and Knowledge Discovery Guilin, Guangxi, China, 2017, pp. 29–31.

[24] J. Zhang, H. Huang, L. Wang, H. Lin, and D. Gao, "Coverless Text Information Hiding Method Using the Frequent Words Hash," Int. J. Netw. Secur., vol. 19, no. 6, pp. 1016-1023, 2017.

[25] J. Zhang, Y. Xie, L. Wang, and H. Lin, "Coverless Text Information Hiding Method Using the Frequent Words Distance," in Cloud Computing and Security, Cham, 2017, pp. 121-132: Springer International Publishing.

[26] C. Liu, G. Luo, and Z. Tian, "Coverless Information Hiding Technology Research Based on News Aggregation," in Cloud Computing and Security, Cham, 2017, pp. 153-163: Springer International Publishing.

[27] C. Yuan, Z. Xia, and X. Sun, "Coverless image steganography based on SIFT and BOF," J. Internet Technol., vol. 18, no. 2, pp. 435-442, 2017.

[28] Z. Xia and X. Li, "Coverless information hiding method based on LSB of the character's unicode," J. Internet Technol., vol. 18, no. 6, pp. 1353-1360, 2017.

[29] Y. Wu, X. Chen, and X. Sun, "Coverless steganography based on english texts using binary tags protocol," J. Internet Technol., vol. 19, no. 2, pp. 599-606, 2018.

[30] Y. Long and Y. Liu, "Text Coverless Information Hiding Based on Word2vec," in Cloud Computing and Security, Cham, 2018, pp. 463-472: Springer International Publishing.

[31] X. Chen and S. Chen, "Text coverless information hiding based on compound and selection of words," Soft Comput., vol. 23, pp. 6323-6330, 2019.

[32] N. Wu, P. Shang, J. Fan, Z. Yang, W. Ma, and Z. Liu, "Research on Coverless Text Steganography Based on Single Bit Rules," J. Phys. Conf. Ser., vol. 1237, no. 2, p. 022077, 2019.

[33] N. Wu, P. Shang, J. Fan, Z. Yang, W. Ma, and Z. Liu, "Coverless Text Steganography Based on Maximum Variable Bit Embedding Rules," J. Phys. Conf. Ser., vol. 1237, no. 2, p. 022078, 2019.

[34] N. Wu, W. Ma, Z. Liu, P. Shang, Z. Yang, and J. Fan, "Coverless text steganography based on half frequency crossover rule," in 4th International Conference on Mechanical, Control and Computer Engineering (ICMCCE), Hohhot, China, 2019, pp. 726-7263: IEEE.

[35] N. Wu, Z. Liu, W. Ma, P. Shang, Z. Yang, and J. Fan, "Research on coverless text steganography based on multi-rule language models alternation," in 4th International Conference on Mechanical, Control and Computer Engineering (ICMCCE), Hohhot, China, 2019, pp. 803-8033: IEEE.

[36] N. Wu et al., "STBS-Stega: Coverless text steganography based on state transition-binary sequence," Int. J. Distrib. Sens. Netw., vol. 16, no. 3, pp. 1-12, 2020.

[37] N. Wu et al., "Coverless Text Hiding Method Based on Improved Evaluation Index and One-Bit Embedding,"

Comput. Model. Eng. Sci., vol. 124, no. 3, pp. 1035-1048, 2020.

[38] Y. Long, Y. Liu, Y. Zhang, X. Ba, and J. Qin, "Coverless information hiding method based on web text," IEEE Access, vol. 7, pp. 31926-31933, 2019.

[39] K. Wang and Q. Gao, "A coverless plain text steganography based on character features," IEEE Access, vol. 7, pp. 95665-95676, 2019.

[40] X. Zhou, X. Chen, F. Zhang, and N. Zheng, "A novel coverless text information hiding method based on double-tags and twice-send," Int. J. Comput. Eng. Sci., vol. 21, no. 1, pp. 116-124, 2020.

[41] W. Zhang, X. Wang, C. Zhang, and J. Zhang, "Coverless text steganography method based on characteristics of word association," in IEEE 20th International Conference on Communication Technology (ICCT), Nanning, China, 2020, pp. 1139-1144: IEEE.

[42] Y. Liu, J. Wu, and G. Xin, "Multi-keywords carrier-free text steganography method based on Chinese Pinyin," International Int. J. Comput. Sci. Eng., vol. 21, no. 2, pp. 202-209, 2020.

[43] J. Qin, Z. Zhou, Y. Tan, X. Xiang, and Z. He, "A big data text coverless information hiding based on topic distribution and TF-IDF," Int. J. Digit. Crime Forensics, vol. 13, no. 4, pp. 40-56, 2021.

[44] Y. Liu, J. Wu, and X. Chen, "An Improved Coverless Text Steganography Algorithm Based on Pretreatment and POS," KSII Trans. Internet Inf. Syst., vol. 15, no. 4, pp. 1553-1567, 2021.

[45] Y. Wen, J. Zhang, Y. Xia, H. Lin, and G. Sun, "Coverless Information Hiding Method Based on Combination Morse Code and Double Cycle Application of Starter," in Advances in Artificial Intelligence and Security, Cham, 2021, pp. 299-311: Springer International Publishing.

[46] J. Qin, Y. Luo, X. Xiang, Y. Tan, and H. Huang, "Coverless image steganography: a survey," IEEE Access, vol. 7, pp. 171372-171394, 2019.

[47] M. A. Kadhim and M. J. Jawad, "A Coverless video steganography: A Survey," in 5th International Conference on Engineering Technology and its Applications (IICETA), Al-Najaf, Iraq, 2022, pp. 522-527: IEEE.

[48] A. Majumder, S. Kundu, and S. Changder, “A unique database synthesis technique for coverless data hiding,” *J. Vis. Commun. Image Represent.*, vol. 96, p. 103911, Oct. 2023, doi: 10.1016/j.jvcir.2023.103911.