IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 26, Issue 1, Ser. 1 (Jan. – Feb. 2024), PP 49-62
www.iosrjournals.org

Advancements In Digital Steganography: A State-Of-The-Art Review

Sapna Kaneria, Dr. Varsha Jotwani
Ph.D Scholar, Department Of Computer Science, RNTU Bhopal, MP, India
Professor And HOD, Department Of Computer Science & IT, RNTU Bhopal, MP, India

Abstract –
Steganography, as one of the fundamental approaches, conceals data within other seemingly innocuous data or media to obscure its presence from unauthorized individuals. This technique stands in contrast to encryption, which relies on mathematical algorithms to encode information, making it indecipherable without the appropriate decryption key. While both approaches serve the overarching goal of information security, they differ fundamentally in their methodologies. In the realm of steganography, researchers have explored various techniques and methodologies, aiming to enhance the effectiveness and security of data concealment. These techniques encompass both linguistic and technical steganography, each offering unique advantages and challenges in concealing information within different types of data. the literature review highlights the differentiation within watermarking techniques, which can be categorized as robust or fragile watermarking. Robust watermarking focuses on embedding information that can withstand various manipulations or attacks, while fragile watermarking is designed to be highly sensitive to any alterations, making it suitable for applications where data integrity verification is crucial.In the modern era, where vast amounts of data are transmitted across various digital channels, the need for confidentiality and data integrity is paramount. While encryption plays a vital role in securing information by encoding it with complex algorithms, steganography offers an alternative approach. Instead of making data indecipherable, steganography focuses on hiding data within seemingly innocuous carriers, whether they are images, audio files, or other forms of media.The significance of steganography lies in its ability to conceal data in plain sight, making it exceedingly challenging for unauthorized individuals to even detect the presence of hidden information, let alone decipher it. This covert communication method can be especially valuable in situations where overt encryption might arouse suspicion or where subtle data exchange is necessary.A review paper on steganography would provide an in-depth analysis of the key concepts, techniques, applications, and recent advancements in the field of steganography. Steganography is the art and science of hiding information within other data in such a way that it remains undetectable to unintended recipients.

Keywords –*Steganography, deep learning,machine learning,encryption and decryption*

Date of Submission: 01-01-2024 Date of Acceptance: 11-01-2024

I. INTRODUCTION

In our contemporary age, the relentless evolution of digital communication technologies has assumed a pivotal role in our daily lives. The amalgamation of advancements in web-based technologies and the widespread digitalization of information have led to a profound increase in the volume and importance of data transfer. In this landscape, the paramount concern of information security emerges, as safeguarding user information becomes an imperative necessity. While several existing approaches to information security have proven themselves robust and secure, the ever-changing nature of digital threats necessitates ongoing efforts to enhance their safety and fortify their performance indicators. In this pursuit, it is crucial to recognize that information security systems can generally be categorized into two fundamental classes: information hiding and encryption [1].Both of these classes are instrumental in the mission to protect sensitive information, yet they employ distinctly different approaches to achieve their objectives. Information hiding techniques, which encompass methods like steganography and watermarking, focus on concealing the presence of information within other data or media. This covert approach ensures that unauthorized individuals are unable to detect the concealed data, thereby adding an additional layer of protection beyond encryption. On the other hand,

encryption techniques, as explored by researchers in [2], encrypt data using mathematical techniques such that it can only be decrypted using the associated decryption key. While encryption provides robust security by rendering data indecipherable, it does not conceal the fact that encryption is being employed, potentially drawing attention to sensitive information.

Figure 1, which illustrates a general classification of data security mechanisms, highlights the interconnected nature of three pivotal techniques: steganography, watermarking, and cryptography. Steganography, within this framework, further delineates into linguistic and technical steganography, each with its own unique methodologies for concealing data. Watermarking, in contrast, offers two distinct variants: robust watermarking, which is resilient to various alterations, and fragile watermarking, which is highly sensitive to changes and is particularly suited for data integrity verification.

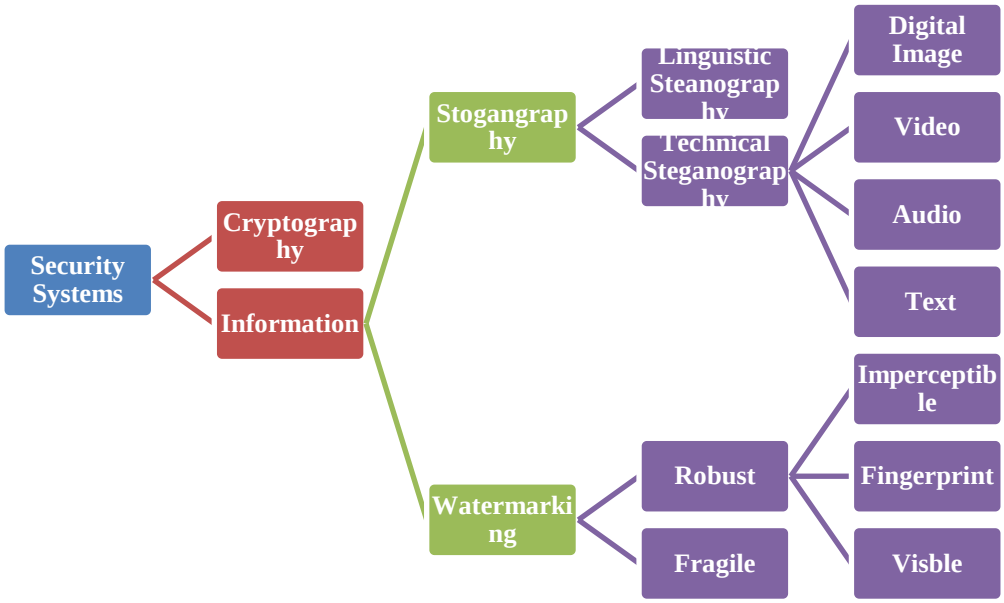

Figure 1. Classification tree of a general data security system.

The overarching goal in image steganography is to facilitate the secure and covert transmission of sensitive or confidential information within digital images. This field of study aims to seamlessly embed hidden data into the pixels of an image while preserving the visual appearance and quality of the original image. The primary objective is twofold: to ensure that the concealed data remains imperceptible to human observers, making it virtually undetectable, and to withstand various forms of analysis and attacks aimed at identifying the presence of hidden information.[3] By achieving these goals, image steganography serves as a crucial tool for safeguarding data privacy, enabling covert communication, and protecting against unauthorized access to sensitive information. Its applications extend to domains such as secure data transmission, copyright protection through watermarking, and authentication of digital media. Ultimately, the goal of image steganography is to strike a delicate balance between hiding data effectively and preserving the integrity of the cover image, thus ensuring secure and covert data exchange in a digital world

Developments in Image Steganography

Image steganography is a subfield of digital steganography that focuses on concealing information within digital images while maintaining the visual quality of the image. Over the years, it has witnessed

significant developments and innovations aimed at enhancing its effectiveness, security, and applicability in various domains. Below, we explore some key developments in image steganography:

Advanced Embedding Techniques: Traditional image steganography methods often used simple techniques like Least Significant Bit (LSB) substitution. Modern developments have introduced more sophisticated embedding techniques, such as matrix encoding, discrete cosine transform (DCT) modification, and frequency domain embedding. These techniques improve the capacity and security of hidden data.

Security Enhancement: Researchers have focused on making image steganography more secure against detection and attacks. This has led to the development of algorithms that adaptively adjust embedding parameters based on image characteristics, making it harder for adversaries to detect hidden information.

Robustness: Another significant development is the incorporation of error-correcting codes and redundancy into steganographic algorithms. These techniques enhance the robustness of hidden data against lossy compression, image manipulations, or transmission errors.

Hybrid Approaches: Recent advancements have resulted in the combination of image steganography with various different encryption and security methods. Hybrid approaches combine steganography with cryptography, watermarking, or digital signatures to offer enhanced security and authentication.

Deep Learning: Image steganography has been done using machine learning and deep learning methods. Convolutional neural networks (CNNs) and generative adversarial networks (GANs) have been used to automate the embedding process and create stego pictures that are harder to detect.

Spatial Domain vs. Transform Domain: Advances have been made in both the spatial and transform domains of image steganography. Spatial domain methods modify pixel values directly, while transform domain methods operate on transformed image data (e.g., DCT, wavelet transform). Developments in both domains cater to different use cases and security requirements.

Focusing on Payload Size: Recent research has concentrated on optimizing the payload size (amount of hidden data) while maintaining the visual quality of the stego image. This is crucial in scenarios where limited capacity is a concern.[4]

Countermeasures and Detection: As steganography advances, so do the methods for detecting hidden information. Research has also focused on developing countermeasures and detection techniques to identify stego images and uncover concealed data.Watermarking, on the other hand, are meant to protect patents from being broken. Both watermarking and fingerprinting involve marking things in some way. The only difference is that every item with a watermark has the same watermark, but every fingerprinting needs a different fingerprint to prove ownership [5]. Steganography is the process of hiding messages inside of something else. For watermarking, a certain item is put in on purpose so that anyone from the outside can see it [6].The hardest part of steganography is keeping the capacity high enough to hide as much of the secret message as possible while keeping the cover media undetectable. Also, reliability is the main problem with both watermarking and encryption. Last but not least, in cryptography, keys are needed, but they aren't in the other ways. In Table 1, the differences between cryptography, watermarking, and steganography are shown.

Table 1. Comparison among different information security techniques.

Technique	Description	Methodology	Key Advantage	Key Disadvantage
Steganography	Conceals data within other data or media.	Covert data embedding	Covert communication; Data presence is hidden	Limited data capacity; Vulnerable to detection
Encryption	Converts data into an unreadable format.	Mathematical algorithms	Strong data protection; Requires decryption key	Encryption can attract attention; Data not hidden
Watermarking	Embeds a watermark to verify data integrity.	Embedded data integrity	Data integrity verification; Various applications	May be altered or removed without detection
Access Control	Restricts access to authorized users only.	User authentication	Effective access restriction; User-specific	Vulnerable to password breaches; Requires setup
Firewalls	Monitors and controls network traffic.	Packet inspection	Network security; Filters unauthorized traffic	Can create network bottlenecks; False positives

Intrusion Detection	Monitors for suspicious activities.	Anomaly detection	Detects network intrusions; Real-time alerts	False alarms; May miss sophisticated attacks
Antivirus Software	Scans for and removes malware.	Signature-based detection	Protects against known threats; Regular updates	Limited against zero-day threats; System resource
Biometric Authentication	Uses unique biological traits for access control.	Fingerprint, iris, etc.	Highly secure; Difficult to impersonate	Costly; Requires specialized hardware

In recent years, there has been a surge in the technology known as natural language processing (NLP), and as a result, researchers have begun looking into the automatic production of steganographic text in order to communicate hidden data. This method of steganography is referred to as "natural modification of the cover media," and it involves concealing information in a text while it is still in the process of being created. In this study, we investigate the evolution of steganography over time as well as how it compares to other classification systems. This will assist specialists in comprehending how the functioning of the current approaches.[7]

II. MATERIALS AND METHODS

This study looked at the techniques and methods for hiding text that have been released from 2016 to 2023. Studies that didn't have anything to do with text steganography were left out. We only used the original, full versions of the report. This part has the subsections Data Sources, Search Process, Data Selection, and Data Extraction.

Data Sources

Search using Keywords: Use relevant keywords related to study, such as "steganography," "information security," "data encryption," Combine these keywords with Boolean operators (AND, OR) to refine search.

Advanced Search: Utilize the advanced search features provided by these databases to narrow down your results based on publication date, authors, journals, and other criteria.

Review Citations: Look at the citations of papers that are closely related to topic. This helps find more recent research that builds upon the earlier work.

Google Scholar: Since you have access to Google Scholar, use it to search for papers and articles. Google Scholar often provides a broader search scope and may include papers not available in other databases.

Search Process

The first query focuses on text steganography techniques and includes variations of the term "text steganography" along with keywords related to different approaches, such as "format based," "linguistic," "random," and "statistical." This query aims to capture papers discussing various methods and a technique in text steganography.The second query delves into the intersection of text steganography and neural networks or deep learning. It includes variations of "text data steganography" and "text steganography method," combined with keywords related to neural networks, deep learning, natural language processing (NLP), and natural language understanding. This query seeks to identify research that explores the application of machine learning and NLP techniques in text steganography.

Data Selection

When conducting reviews of previously conducted research, careful consideration must be given to the selection of data. After obtaining the results of the search based on the keywords that we employed, we made use of three different filtering procedures to incorporate the criteria for the search. The criteria were decided upon during the preliminary stage of the filtering process. We compiled all of the findings of the investigation into separate research articles and arranged them according to these keywords. The subsequent stage was to finish a second filter that examines the title and reads the abstract of each article to determine whether or not it is relevant to the research issue. The third and final filter consisted of reading the material that was contained in a research article that was chosen from the candidate studies. The following are the criteria that were used to choose the data:

- Did the study paper come out between 2016 and 2023?
- Is the study article mentioned in any of the data sources you listed?

- Does the research article reference or talk about one of the text steganography categories?

Data Extraction

We examined each of the preliminary studies to evaluate whether or not there were any text steganography-related subjects. In a spreadsheet, we included all of the research we discovered, along with their titles, abstracts, and justifications. The search procedure was finished in March of 2021, and a total of 203 publications were found. Following the selection and refusal criteria, the pertinent research papers were painstakingly pulled from the database making use of the search strategy depicted in Figure 2. In the end, fifty different preliminary investigations were discovered.

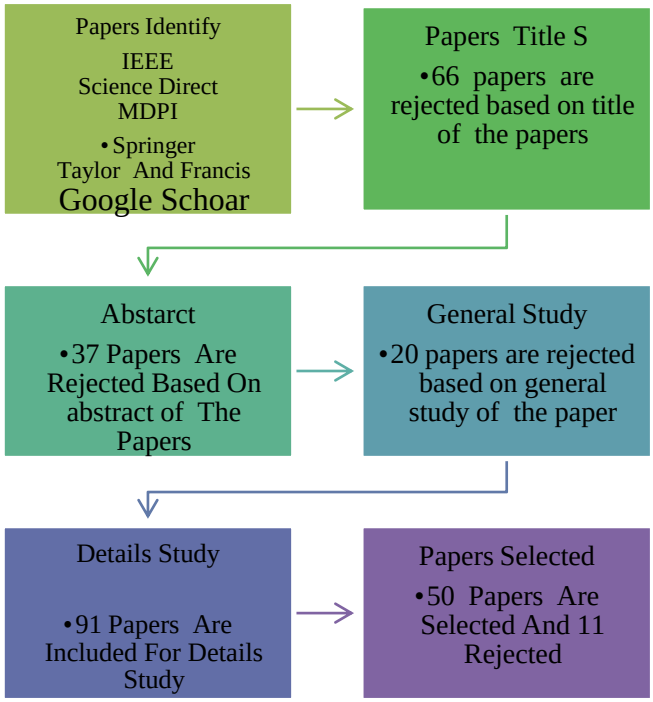

Figure 2. Search process

Background of Steganography

Two ancient Greek terms, "Stegano" and "Graphy," are combined to form the modern word "Steganography." Both of these words mean "Cover Writing." The first known application of steganography occurred several centuries ago. For instance, Histiaeus used steganography to send a secret message by tattooing the message on the head of one of his slaves. The slave didn't go anywhere until his hair had grown long enough to cover his scar. The ancient Greeks were well-known for their skill at sending messages in code. For instance, Demaratus made use of a tablet that had a wax coating. Carving was used to write a message on the tablet, and then the tablet was waxed when the carving was complete. After the wax was removed, the message became scratched and scuffed. The tablet had more wax applied to it, giving the impression that it was a fresh tablet with nothing written on it. After then, the communication was safely transmitted without arousing any suspicion [8]. Jerome Carden, a mathematician from Italy, was the one responsible for reviving the art of penning secret messages, a practice that was utilised by the ancient Chinese. The method involved using a piece of paper with grid holes as a mask, and then writing a secret message and putting it on another piece of blank paper. This mask was used by both the sender and the responder at the same time. After the grid mask was taken off, words that at first looked harmless were written on the blank part of the paper. During World War I, the Germans used a microdot technology that was based on many stages and made use of magazine scraps [9]. During the Second World War, there were many different ways to write secret communications, such as the Enigma machine, open-coded messages, multiple null cyphers, and invisible inks [10]. Invisible inks were also used. It was revealed that a Saudi Arabian king had started a project for covert writing at the Abdul-Aziz City of Science and Technology. The project was found written about in a book that was 1200 years old. These handwritten

documents originated in Turkey and Germany [11] a variety of literary works offer a more in-depth perspective on the history of steganography as well as the methods that are currently in use around the world. Digitising data has made it much more likely that information can be retrieved and shared, thanks to the growth of interconnected multimedia sets, wireless systems, and electronic digital cameras. Because computers and the internet have become faster and better at processing information, steganography methods have been adapted to be used with digital means.

New studies and developments, like those in signal processing [12], encoding techniques, and the philosophy of information, are making it easier to make secure steganography methods. The most modern methods of steganography aren't just for hiding secret information in pictures; they can also be used to hide information in text, codes, audio movies and DNA [13]. They also include hiding information in different forms, such as executables, extensible mark-up language (XML), and hypertext mark-up language (HTML) [28,29]. The body of research presented in [14] evaluated and investigated a variety of emerging tendencies within digital steganographic approaches.

Steganography General Procedures

Objective of Steganography: The fundamental purpose of digital steganography is to covertly infiltrate private or confidential material within cover media. This confidential data can be in the form of photos, text, binary data, or video, and it is hidden behind what is referred to as cover media, which is comprised of other types of media.

Steganographic Terminology: The terminology used in steganography includes "secret data" (data to be concealed), "cover media" (the media in which the data is hidden), and "stego media" (the result of embedding the secret data into the cover media).

Secure Communication: The purpose of steganography is to facilitate the secure transmission of secret data through potentially unsecured communication channels. By embedding the data within cover media, it can be sent without arousing suspicion or drawing attention.

Steganographic Setup: In this setup, secret data is concealed within the cover media at the sender's end to create stego media. The stego media is then transmitted to the recipient.

Enhanced Security: During the embedding process, certain steganographer systems incorporate either a security key or an encryption structure, or both, to increase the level of security offered by the system. These additional features might include encryption passwords, embedding maps, and threshold values that are used to direct the embedding process.[15]

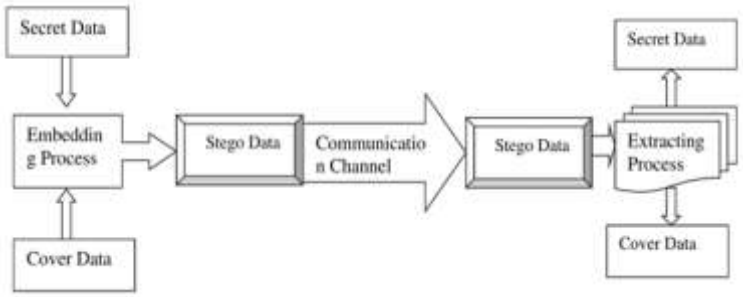

Figure 3. Block diagram of a steganographer system.

Attributes of Steganography

Steganography relies on three key characteristics security, imperceptibility, and capacity to successfully conceal confidential information [16]. The research presented in [17] outlined the aforementioned three features, in addition to robustness. These are the most important criteria that decide how successful a steganography setup will be. For the management of a variety of steganographic designs, there are particular requirements that must be met that are peculiar to their application. These characteristics are present in steganography and watermarking as a means of embedding data. However, one of the most typical compromises that people make is between the quantity of secret data and the quality of the stego files. Let's say there is a big amount of confidential data that needs to be incorporated. If this is the case, changing the stego files will be more difficult because achieving imperceptibility will be more challenging due to the presence of a risk of distortion. As a result, ensuring that these qualities are kept in the best possible condition need to be the primary

focus. There are times when robustness is not required. Having said that, security, imperceptibility, and the ability to disguise oneself are always requirements. When it comes to digital watermarking, a higher capacity and an undetectable appearance are not requirements. When it comes to fending off malicious and unwelcome attacks, stressed the importance of having a powerful defense.which can be found .The following section will provide an in-depth explanation of the characteristics that have been talked about. Capacity is the number of hidden messages that can be put into the cover text without changing the meaning of the text itself. It is usually measured in bits. When we talk about security, we mean that an attack route can quickly find out private information. A system's "robustness" might be defined as its capacity to withstand the possibility of sensitive data being altered or lost.

Imperceptibility

Steganography places an emphasis on undetectability above all else, with the primary goal are the concealment of confidential data within other types of media. Even with the application of statistical methodologies, it is impossible for the human eye to comprehend it [18]. Attackers can gain an advantage by using statistical approaches to assess whether or not confidential material is being shared between two parties through communication. So, the embedding of the secret data shouldn't change the cover media in a noticeable way. That is, if we find similar statistical data in both the original file and the stego file, we can assume that the security is good enough to let the data be sent. When sharing across unsafe networks, the quality of the cover media must be kept even though the embedding process adds noise [19].

Security: The concepts of "undetectability" and "unnoticeability" are related to one another in the field of steganography, where the term "security" refers to these concepts. Therefore, an approach to steganography is considered to be secure when the data it is concealing cannot be discovered by any third party making use of statistical tools. The primary criterion for security is to prevent access by unauthorized individuals or computers when communicating across an unprotected route, which ensures that the data will continue to be secure.

Payload Capacity The goal of any good steganographic apparatus, in general, is to transmit the most possible amount of data while making use of the medium that offers the least amount of cover. This lowers the likelihood of information being intercepted when it is being transmitted across a channel that is not secure and consequently calls for a significant capacity for embedding. The rate of embedding the bits was given in reference [20], and it was compared to the size of the cover image. In steganography, one of the most important challenges is to keep a large payload capacity while also keeping a low profile and being undetectable.

Robustness-"Robustness" is the ability of an embedding and removing method to withstand any kind of corruption caused by a third party using any kind of processing method. In steganography, an attack hasn't happened if the stego files aren't destroyed or changed while they're being sent over the internet. In this scenario, the recipient will get the stego file as it was intended to be delivered to them. In that case, assaults like compression, converting file formats, and transforming between digital and analogue format could take place throughout the process of communication. However, when it comes to fingerprint systems, robustness is required if there is intentional modification or alteration of files.

Text Steganography Categories

Compared to digital data like audio, image, or video files. Text steganography can be roughly divided into three groups, language, format-based, and random and statistical generation

Format-Based Method

In this kind of steganography, the shapes of writing marks are used to hide information. The features have been changed in a way that makes it hard for human eyes to see them. For example, bits of secret data can be hidden by moving lines up and down in the text. Then, words are shifted to the left, right, or up and down. White space between words, between paragraphs, and between lines is sometimes used to hide information. For feature-based reading, the information is hidden by changing the way the words look. This is based on words and signs. Many studies have shown that changing the way the text looks makes it easier to hide information in text. For example, ref. [21] maps the binary digits of the hidden message to the binary digits of the cover text by using the letters, spaces, and symbols of the American Standard Code for Information Interchange (ASCII). The secret text is first turned into cypher text by using a one-time code to protect it. Then, each letter is turned into a series of seven-bit binary numbers. The process of embedding involves mapping one bit of the secret text to the first bit of the first character in the cypher text that has the same number of bits. As a stego key, each bit point of

the secret text is written down and put on each bit of the code text. The stego key is a key that can be used to find the secret text that is hidden in the cypher text.

Linguistic

This way of hiding secret information in text files uses language steganography. In [22], a method for hiding information in language called topic-aware neural-linguistic steganography was proposed. With the help of knowledge graphs (KGs), a steganographic text about a certain topic can be made. A KG gives information about important topics and material to help people make coherent, multi-sentence texts for better hiding. The method suggested tells you how good the steganographic text is and how well it fits with a certain subject.

In [46], the author suggested a way to deal with the problem of not being able to control the semantic expression in steganographic text created by neural networks. The author talked about control cognitive imperceptibility as a new problem that steganography models will have to try to solve in the future. The author compared the Gated Recurrent Unit (GRU) model, the Transformer model, and the Topic-Aware model, which are all encoder models for semantic extraction. Categorical sampling creates steganographic sentences to make the candidate pool that picks words based on the total conditional probability distribution. Experiments have shown that the proposed method can also limit how the created steganographic text makes sense.

In [23], A language steganography method was proposed that uses an adaptive probability distribution and a generative adversarial network to automatically create the stego text. The suggested method fixed the exposure bias caused by the difference between the training and inference stages in a good way. Also, the suggested method figures out the candidate word space and embedding capacity based on the likelihood that two words are similar. This is done to reduce the deviation that results. The tests showed that the proposed method is better than the earlier ones, especially in its ability to prevent steganography analysis, and that it could be used to make steganography more secure.

[24] suggested a safe generative linguistic steganographic method that uses Adaptive Dynamic Grouping (ADG) to embed secret information in a recursive way, based on the abilities of a standard language tool. The suggested method aimed to make the hidden data less obvious by putting tokens into groups based on their likelihood at each step. This allowed secret information to be hidden in the stego text in a way that wasn't clear. Experiments showed that the suggested way is safe and can make stego text that flows well.

Another linguistic steganographic method was suggested in [25], which uses Variation Auto-Encoder (VAE-Stega) to make stego text automatically. The purpose of this method was to make steganographic writing less obvious and safer. The encoder in VAE-Stega is used for two main purposes: to learn the statistical distribution features of big, regular texts and to make steganographic words. The test results showed that the proposed way makes the steganographic sentences less noticeable.

In [26], the author suggests building a language model with a generative text steganographic method based on a long short-term memory (LSTM) network and a large-scale regular text database. The produced word is tried based on the LSTM network's planned conditional probability distribution (of words) and the secret value that is kept on the receiver side. On the receiving end, the secret info is retrieved using the same model. The results showed that it does better than other works like it.

Recurrent Neural Networks (RNN-Stega), which use a discrete bit stream to automatically make text covers, were suggested in [27]. Fixed- and variable-length coding (FLC and VLC) are used to look at how words used for decoding are spread out in different situations. The tests showed that there was a high capacity for embedding and a high level of security against harmful attempts.

In [28], it was suggested that using word replacement is a new way to make language steganography better at hiding information. HC was used to change the change-tracking method so that the message could be hidden inside MS Word files.So that a third party doesn't know there's a message, people often use words to hide information and avoid suspicion.

Random and Statistical Generation

When making header text, the statistical traits of a language are taken into account. The work in [29] suggested a statistical text steganography method that focuses on transition chance. This is one of the most important ideas of the Markov Chain model. Based on the ideas, this method made state transition-binary sequence pictures and used them to control the production of new texts with hidden information. With this method, the shift chance is used to make steganographic text. This method also stores the state transition-binary sequence picture that the receiver needs in order to get the information. This makes the knowledge about

steganography even safer. The results showed that this model was better than the ones that had been used before at hiding things.

For Arabic text steganography, a Markov Chain (MC) encoder/decoder was combined with HC to make the statistical steganography method better at hiding information. The length of the stego text depends on the settings of the encoder/decoder that was made. The capacity performance of the suggested Arabic steganography method was looked at in terms of the length of the hidden message and different encoder settings. The results showed that putting certain constraints on MC made the embedding capacity go up until it reached a maximum number.

Ref. [30] suggested an MC-model-based coverless statistic steganography method. The goal of this method is to make steganographic text that looks more like the training text. The method uses maximum variable bit embedding instead of standard fixed bit embedding. This is because maximum variable bit embedding is based on the value and properties of the model's transition probability. This method doesn't put fixed bits of hidden data into each word of the text. Instead, it keeps more of the features of the training model. When it was put together with the transition probability, this model's hidden capacity results were better than those of other methods.

In the work [31], the authors describe a way to use single-bit rules based on the MC model for coverless statistical steganography. In this method, the hidden information is sent through the model, and then the steganographic information that matches it is made. During the process of text generation, the importance of transition probability is stressed and used as much as possible in order to make steganographic text that looks more like the training text. This is done so that steganographic text can be made that can hide information. Instead of fixed bit embedding, which is what most people do, this method uses maximum variable bit embedding. This method doesn't hide any information in every single word of the text. The results of the tests done with the proposed approach showed that it could be used to hide things well. On the other hand, it wasn't better than the method that came before it, which used variable bit embedding. [32] Presented a statistical coverless text steganography model that was based on multi-

III. Discussion and Future Directions

In comparison to other forms of files, such as images, videos, and audio files, text steganography is the most difficult form of the covert communication technique known as steganography. This is because there are no superfluous bits in text files. In contrast to the structure of other files, such as pictures and movies, the structure of the file containing the text is exactly the same as what can be seen by the naked eye. As a consequence of this, it is extremely simple to conceal information in later papers because, in comparison to the text, no changes are seen. The human eye, on the other hand, is highly sensitive and can readily spot even the smallest of modifications made to a written document. provides a count of the various text steganography methods that have been developed to hide secret communications and published between the years 2016 and 2021. When compared to other forms of digital material, such as image, audio, and video files, the lack of redundant data in textual documents presents the greatest obstacle in the field of text steganography. This is typically the source of the low concealing capacity.

This was the case with the format-based solutions. The first element to take into consideration is the vocabulary of the cover text. The qualities of the language help to identify the methods for concealing data within the text cover. These methods include the attributes of the font and the forms of the letters for languages such as English and Indian. In contrast, the Arabic language makes use of kashida, points, and diacritics on individual words.

As can be observed in [33], the English language makes use of a variety of different linguistic qualities These things include the font, uppercase and lowercase letters, double letters, high-frequency letters, punctuation, and other symbols. Messages can also be hidden using the shape of the English capital letters. This is accomplished by grouping the letters into categories based on the direction in which they are oriented (curved, vertical, horizontal, etc.). These qualities are utilised in order to conceal confidential information within the English language. As can be seen in [34], spaces can also be used in conjunction with Unicode characters to conceal information.

Arabic, which is composed of "points" or "dots," is also utilised in text steganography, as can be seen in [35]. Some alphabets have both point characters and diacritical marks for individual words. A letter's pronunciation can be changed by adding various diacritics, which are markings that go on top of or underneath the letter. Therefore, authors have utilised Kashida is good because it can be used fast without hurting the work,

and Unicode characters (zero-width character and zero-width joiner) can be used to make the most of the spaces in points, between letters and signs, or in the shape of Arabic letters.

In [36], the Indian language is used in a way that separates the letters into eight groups based on how they are pronounced. The secret message bits are then hidden inside the cover text letter based on the specific positions of the cover text letter bits and the shape of the alphabets. (The forms can be put into groups like curves, verticals, horizontals, etc.).

The properties of the cover text can also be used as a component of the steganography process. As an illustration, the cover material for is a text file, and it makes use of both the gaps between the characters and the vacant spaces in the file. Another purpose for the text colour is to conceal information using it. For instance, a pattern to hide secret texts can be created in a Microsoft Word document by altering the typeface, the capitalization or lowercaseness of the letters, or the colour of the letters themselves, as well as by increasing the amount of white space in the document. PDF files can also be utilised for text steganography, as demonstrated in the ways in [37], by using a procedure called "Justify" to remove the ragged edges of the text. This process is reused during the process of hiding the message.

In terms of the linguistic approach, a variety of strategies are utilised in order to find the most suitable match. In order to achieve this objective, the syntax, semantics, and linguistic integrity of a language will need to be utilized. Deep learning, or DL for short, is becoming increasingly popular and is being put to use in a broad variety of different applications as a direct result of the vast amounts of data that are currently available. In recent years, DL has been used to several aspects of linguistic steganography, most notably text steganography [38]. On the other hand, this presents a fresh obstacle in terms of the safety of the methods that are being offered. This is due to the fact that the DL itself provides auto-generation of text-linguistic steganography while keeping the text's semantics intact. In order for linguistic steganography to be successful, this is one of the most important characteristics. In order to accomplish this goal, the research paper referred to in this phrase (57) utilised a knowledge graph, which supplies information about pertinent themes and contents, to construct coherent multi-sentence writings and so improve data concealing.

Pranab K. Muhuri and colleagues (2022): Limited investigation of integrating integer wavelet transformation and particle swarm optimization for image steganography, specifically in terms of capacity, imperceptibility, and robustness.[39]

Ayushi Chaudhary et al. (2022):Lack of comprehensive analysis of pros and cons of different steganographic methods, including combination of sequence and asymmetric encryption.Need to evaluate effectiveness of methods against steganalysis.[40]

Wafa M. Eid et al. (2022): Lack of comprehensive overview and analysis of steganalysis methodologies for spatial and transform domains in 2D and 3D images.Need to consider conventional machine learning and deep learning techniques.[41]

Jiahao Liu et al. (2022): Need for comprehensive overview and analysis of steganalysis methodologies for spatial and transform domains in 2D and 3D images.Need to consider conventional machine learning and deep learning techniques.[42]

Bibek Ranjan Ghosh et al. (2022): Need for comprehensive overview of diverse steganographic methods utilized for concealment of information in 2D and 3D images.Focus on dataset used and evaluation of methods.[43]

Ismail Taha Ahmed et al. (2022): Limited exploration of deep learning application, particularly utilization of pre-existing CNNs like AlexNet, in image steganalysis for binary classification.[44]

Bhatia, A. et al. (2021): Limited investigation of GANs in image steganography, including steganographic capacity, visual quality, and robustness against steganalysis.[45]

Hu, Y. et al. (2021): Need to enhance steganographic capacity and robustness through application of multi-scale feature fusion techniques in CNN-based image steganography.[46]

M. Esaiselvam et al. (2021):Limited exploration of using steganography techniques (Contour reframing, Deep Image prior, PEM method) to detect and quantify image tilt angles for piracy detection.[47]

Nandhini Subramanian et al. (2021): Limited exploration of deep learning methods (standard, CNNs, GANs) in image steganography.Need for more comprehensive evaluation measures.[48]

Pei Li et al. (2021) Limited exploration of deep learning integration in steganography and steganalysis.Need for analysis of challenges and future developments.[49]

Ismail Kich et al. (2021): Limited exploration of CNN-inspired approach using Auto-Encoder networks and U-net design for color image steganography.Need for performance evaluation on popular datasets.[50]

Luo et al. (2020): Opportunity to improve robustness and imperceptibility of image steganography using deep learning models and exploring pixel-value differencingProposed Algorithm for Steganography Limited discussion on the specific techniques or mechanisms employed in the proposed algorithm for embedding and extracting data.Lack of detailed exploration of potential vulnerabilities, robustness, and security considerations of the proposed algorithm.[51]

Srushti S Yadahalli et al. (2020):Absence of comparison with more recent and advanced steganography techniques beyond LSB and Discrete Wavelet Transform.Insufficient exploration of the trade-offs between different steganographic methods in terms of capacity, security, and visual quality.[52]

B. Vishnu; Leena Vishnu Namboothiri et al. (2020): Limited discussion on the specific mathematical or computational details of the Pixel Value Differentiating (PVD) technique.Need for a comprehensive analysis of the impact of Edge Detection in enhancing security and embedding capacity.[53]

T. Kalaichelvi; P. Apuroop et al. (2020): Lack of in-depth explanation of the CAPTCHA-based authentication mechanism and its integration with image steganography.Need for a more detailed comparison of the proposed approach's security benefits and challenges compared to traditional methods.[55]

J. H. Lee; D. Y. Kang et al. (2020): Inadequate discussion on the specific architecture and training process of the deep neural network model used for recovering hidden image information.Limited exploration of the potential limitations or cases where the proposed approach may not work effectively.[56]

Omar Elharrouss; Noor Almaadeed et al. (2020): Lack of detailed explanation of the k-LSB-based method and its potential impact on capacity and security compared to other steganography techniques.Insufficient analysis of the trade-offs between image resolution enhancement and potential loss of steganographic content during decoding.[57]

Table 2 a table form for each paper, including author names, advantages, and disadvantages:

Paper Title & Authors (Year)	Advantages	Disadvantages
Ahmed A. et al. (2022)	Development of new image steganography using quantum substitution boxes. Potential to improve robustness, security, and imperceptibility. Exploration of quantum computing benefits	Complex implementation due to quantum principle Limited real-world quantum computing resources
Pranab K. Muhuri et al. (2022)	Novel steganography method using integer wavelet transformation and PSO.Potential for increased image quality and robustness	Complexity in optimizing PSO parameters Computational intensity for large images
Ayushi Chaudhary et al. (2022)	New perspective on steganography methods, Consideration of pros and cons, Utilization of sequence and asymmetric encryption	Method description is brief Limited evaluation details
Wafa M. Eid et al. (2022)	Comprehensive overview of steganalysis methodologies, Exploration of spatial and transform domains, Analysis of diverse steganographic methods	Limited information on specific datasets Lack of in-depth evaluation metrics
Jiahao Liu et al. (2022)	Comprehensive analysis of steganalysis methodologies Exploration of spatial and transform domains Consideration of conventional and deep learning techniques	Repetition of content with similar paper Lack of unique contribution
Bibek Ranjan Ghosh et al. (2022)	Comprehensive overview of steganographic methods, Highlighting commonly used datasets, Exploration of information concealment	Minimal innovation beyond existing studies Limited focus on unique contributions
Ismail Taha Ahmed et al. (2022)	Utilization of deep learning in steganalysis, Expedited training using pre-existing CNNs High classification precision	Limited focus on the proposed method's uniqueness Lack of comparison with other deep learning models
Bhatia, A. et al. (2021)	Application of GANs in image steganography Exploration of steganographic capacity and visual quality	Limited depth in analyzing GAN-based steganography Lack of comprehensive evaluation metrics
Hu, Y. et al. (2021)	Enhancing steganographic capacity and robustness,Multi-scale feature fusion using CNNs	Methodology and approach could be further detailed Lack of quantitative performance improvement assessment

M. Esaiselvam et al. (2021)	Unique application of steganography for image tilt angle detection, Exploration of multiple steganography methods	Limited depth in analyzing the method Focus on a specific aspect of steganography
Nandhini Subramanian et al. (2021)	Exploration of deep learning methods in steganography Overview of datasets and evaluation measures, Contribution to understanding deep learning's role	Lack of in-depth analysis and comparison Potential overlap with other papers' content
Pei Li et al. (2021)	Integration of deep learning in steganography and steganalysis, Focus on challenges and future developments	Lack of detailed analysis of proposed method, Limited demonstration of superior performance
Ismail Kich et al. (2021)	CNN-inspired approach for color image steganography, Utilization of Auto-Encoder networks and U-net design	Lack of detailed performance evaluation, Limited exploration beyond specific approach
Luo et al. (2020)	Application of deep learning for improved steganograph,Exploration of pixel-value differencing, Focus on enhancing robustness and imperceptibility	Limited explanation of deep learning model architecture, Emphasis on a specific steganography technique
J. H. Lee; D. Y. Kang et al. (2020)	Automatic recovery of hidden image information, Use of deep neural network model and entropy features	Limited clarity on the proposed approach, Lack of detailed experimental results
Omar Elharrouss; Noor Almaadeed et al. (2020)	K-LSB-based steganography method, Resolution enhancement of stego image	Lack of detailed explanation of K-LSB approach. Unclear impact of resolution enhancement
Srushti S Yadahalli et al. (2020)	Comparison of two image steganography techniques, Analysis of resulting image parameters	Limited focus on broader context of steganography, Lack of exploration beyond specific methods
B. Vishnu; Leena Vishnu Namboothiri et al. (2020)	Use of PVD for improved image steganography, Incorporation of Edge Detection technique	Limited comparison with other steganography methods, Limited depth in discussing advantages and disadvantages
T. Kalaichelvi; P. Apuroop et al. (2020)	Combination of CAPTCHA and Image Steganography, Improved security and confidentiality	Lack of detailed implementation description, Limited exploration beyond proposed combination
J. H. Lee; D. Y. Kang et al. (2020)	Automated recovery from image steganography, Use of deep neural network and entropy features	Unclear methodology and approach detail, Lack of comprehensive experimental results
S. Kavitha et al. (2020)	Exploration of image steganography with different techniques, Evaluation of image quality and security	Limited depth in discussing proposed technique, Lack of detailed advantages and disadvantages
Jawwad A R. et al. (2020)	Comparative analysis of steganography algorithms, Evaluation based on accuracy, precision, recall, and f1-score	Limited exploration of unique steganography approach. Lack of broader context discussion

IV. CONCLUSIONS

The following is a comprehensive review of recent text steganography approaches provided by this study. In addition to this, it offers a categorization of steganography based on the various methods. The techniques of text steganography can be broken down into three distinct categories: those that are format-based, those that rely on random or statistical creation, and those that are based on linguistics. In addition to that, comparisons between these different methods are emphasized. According to the findings of this study, two of the most discussed aspects of text steganography are expanding the capacity factor of format-based methods and boosting the level of security provided by linguistic steganography. Researchers in this discipline have, however, given less attention to robustness than they might have. In this study, the evolution of the field of text steganography was analyzed, and it was demonstrated how new technologies are being utilized in this particular subject. These technologies were linked with the current steganography categories in order to assist researchers. This was accomplished by compiling the existing approaches. As a consequence of this, the paper presents factors that can be explored for potential future paths, hence pointing to new research fields in text steganography.

References

[1]. Cheddad, A.; Condell, J.; Curran, K.; Mc Kevitt, P. Digital Image Steganography: Survey And Analysis Of Current Methods. Signal. Process. 2010, 90, 727–752.
[2]. Anderson, R.; Petitcolas, F. On The Limits Of Steganography. Ieee J. Sel. Areas Commun. 1998, 16, 474–481
[3]. Srikumar, R.; Malarvizhi, C.S. Strong Encryption Using Steganography And Digital Watermarking. In Proceedings Of The 22nd Picture Coding Symposium, Seoul, Korea, 25–27 April 2001; Pp. 425–428.
[4]. Al-Daweri, M.S.; Abdullah, S.; Ariffin, K.A.Z. A Homogeneous Ensemble Based Dynamic Artificial Neural Network For Solving The Intrusion Detection Problem. Int. J. Crit. Infrastructure. Prot. 2021, 34, 100449.
[5]. Majeed, M.A.; Sulaiman, R. An Improved Lsb Image Steganography Technique Using Bit-Inverse In 24 Bit Colour Image. J. Theor. Appl. Inf. Technol. 2015, 80, 2.
[6]. Johnson, N.F.; Jajodia, S. Exploring Steganography: Seeing The Unseen. Computer 1998, 31, 26–34.
[7]. Premaratne, P.; Desilva, L.C.; Burnett, I. Low Frequency Component-Based Watermarking Scheme Using 2d Data Matrix. Int. J. Inf. Technol. 2006, 12, 1–12.
[8]. Le, T.H.N.; Nguyen, K.H.; Le, H.B. Literature Survey On Image Watermarking Tools, Watermark Attacks, And Benchmarking Tools. In Proceedings Of The 2nd International Conference On Advance Multimedia, Ieee, Athens, Greece, 13–19 June 2010; Pp. 67–73
[9]. Cox, I.J.; Miller, M.L.; Bloom, J.A.; Fridrich, J.; Kalker, T. Digital Watermarking And Steganography; Morgan Kaufmann: Burlington, Ma, Usa, 2008.
[10]. Shih, F.Y. Digital Watermarking And Steganography: Fundamentals And Techniques; Crc Press: Boca Raton, Fl, Usa, 2017.
[11]. Al-Naqeeb, A.B.; Nordin, M.J. Robustness Watermarking Authentication Using Hybridisation Dwt-Dct And Dwt-Svd. Pertanika J. Sci. Technol. 2017, 25, 73–86.
[12]. Judge, J.C. Steganography: Past, Present, Future; Lawrence Livermore National Lab.: Livermore, Ca, Usa, 2001.
[13]. Kamil, S.; Ayob, M.; Abdullah, S.N.H.S.; Ahmad, Z. Challenges In Multi-Layer Data Security For Video Steganography Revisited. Apijtm 2018, 07, 53–62. Stefan, K.; Fabien, A.P.P. Information Hiding Techniques For Steganography And Digital Watermarking (Artech House Computer Security Series); Artech House: London, Uk, 2000.
[14]. Mishra, M.; Mishra, P.; Adhikary, M.C. Digital Image Data Hiding Techniques: A Comparative Study. Arxiv 2014, Arxiv:1408.3564.
[15]. Provos, N.; Honeyman, P. Hide And Seek: An Introduction To Steganography. Ieee Secur. Priv. Mag. 2003, 1, 32–44.
[16]. Petitcolas, F.A.P.; Anderson, R.J.; Kuhn, M. Information Hiding-A Survey. Proc. Ieee 1999, 87, 1062–1078
[17]. Du, J.-X.; Huang, D.-S.; Wang, X.-F.; Gu, X. Computer-Aided Plant Species Identification (Capsi) Based On Leaf Shape Matching Technique. Trans. Inst. Meas. Control 2006, 28, 275–285.
[18]. Zheng, C.-H.; Huang, D.-S.; Sun, Z.-L.; Lyu, M.R.; Lok, T.-M. Nonnegative Independent Component Analysis Based On Minimizing Mutual Information Technique. Neurocomputing 2006, 69, 878–883.
[19]. Bhattacharjya, A.K.; Ancin, H. Data Embedding In Text For A Copier System. In Proceedings Of The 2018 Ieee International Conference On Image Processing, Athens, Greece, 7–10 October 2018; Pp. 245–249.
[20]. Baawi, S.S.; Mokhtar, M.R.; Sulaiman, R. A Comparative Study On The Advancement Of Text Steganography Techniques In Digital Media. Arpn J. Eng. Appl. Sci. 2018, 13, 1854–1863.
[21]. Awais, M.; Müller, H.; Tang, T.B.; Meriaudeau, F. Reversible Data Embedding In Golomb Rice Code. In Proceedings Of The 2011 Ieee Inter-National Conference On Signal And Image Processing Applications, Kuala Lumpur, Malaysia, 16–18 November 2011; Pp. 515–519.
[22]. Kadhim, I.J. A New Audio Steganography System Based On Auto-Key Generator. Al-Khwarizmi Eng. J. 2012, 8, 27–36.
[23]. Santhi, B.; Radhika, G.; Reka, S.R. Information Security Using Audio Steganography—A Survey. Res. J. Appl. Sci. Eng. Technol. 2012, 4, 2255–2258.
[24]. Limkar, S.; Nemade, A.; Badgujar, A.; Kate, R. Improved Data Hiding Technique Based On Audio And Video Steganography. Smart Comput. Inform. 2017, 581–588.
[25]. Jeyasheeli, P.G.; Selva, J.J. A Survey On Dna And Image Steganography. In Proceedings Of The 2017 4th International Conference On Advanced Computing And Communication Systems (Icaccs), Coimbatore, India, 6–7 January 2017.
[26]. Haughton, D.; Balado, F. A Modified Watermark Synchronisation Code For Robust Embedding Of Data In Dna. In Proceedings Of The 2013 Ieee International Conference On Acoustics, Speech And Signal Processing, Vancouver, Bc, Canada, 26–31 May 2013; Pp. 1148–1152.
[27]. Odeh, A.; Elleithy, K.; Faezipour, M.; Abdelfattah, E. Novel Steganography Over Html Code. In Innovations And Advances In Computing, Informatics, Systems Sciences, Networking And Engineering; Springer: Berlin/Heidelberg, Germany, 2015; Pp. 607–611.
[28]. Memon, A.G.; Khawaja, S.; Shah, A. Steganography: A New Horizon For Safe Communication Through Xml. J. Theor. Appl. Inf. Technol. 2008, 4, 187–202.
[29]. Zielinska,´ E.; Mazurczyk, W.; Szczypiorski, K. Trends In Steganography. Common. Acm. 2014, 57, 86–95.
[30]. Subhedar, M.S.; Mankar, V.H. Current Status And Key Issues In Image Steganography: A Survey. Comput. Sci. Rev. 2014, 13–14, 95–113.
[31]. Li, B.; He, J.; Huang, J.; Shi, Y.Q. A Survey On Image Steganography And Steganalysis. J. Inf. Hiding Multimed. Signal Process. 2011, 2, 142–172.
[32]. Marvel, L.M.; Retter, C.T.; Boncelet, C.G. A Methodology For Data Hiding Using Images. In Proceedings Of The Ieee Military Communications Conference, Los Angeles, Ca, Usa, 19–21 October 1998; Pp. 1044–1047.
[33]. Mathkour, H.; Al-Sadoon, B.; Touir, A. A New Image Steganography Technique. In Proceedings Of The 2008 4th International Conference On Wireless Communications, Networking And Mobile Computing, Dalian, China, 12–17 October 2008; Pp. 1–4.
[34]. Altaay, A.A.J.; Sahib, S.B.; Zamani, M. An Introduction To Image Steganography Techniques. In Proceedings Of The 2012 International Conference On Advanced Computer Science Applications And Technologies (Acsat), Kuala Lumpur, Malaysia, 26–28 November 2012; Pp. 122–126.

[35]. Ramu, P.; Swaminathan, R. Imperceptibility—Robustness Tradeoff Studies For Ecg Steganography Using Continuous Ant Colony Optimization. Expert Syst. Appl. 2016, 49, 123–135.

[36]. Abraham, A.; Paprzycki, M. Significance Of Steganography On Data Security. In Proceedings Of The Itcc 2004 International Conference On Information Technology: Coding And Computing, Las Vegas, Nv, Usa, 5–7 April 2004; Pp. 347–351.

[37]. Baawi, S.S.; Mokhtar, M.R.; Sulaiman, R. Enhancement Of Text Steganography Technique Using Lempel-Ziv-Welch Algorithm And Two-Letter Word Technique. In Proceedings Of The 3rd International Conference Of Reliable Information And Communication Technology (Irict 2018), Kuala Lumpur, Malaysia, 23–24 July 2018; Pp. 525–537.

[38]. Pranab K. Muhuri, Zubair Ashraf, Swati Goel (2022), A Novel Image Steganographic Method Based On Integer Wavelet Transformation And Particle Swarm Optimization, Applied Soft Computing, Volume 92, 106257, Issn 1568-4946, Https://Doi.Org/10.1016/J.Asoc.2020.106257.

[39]. Ayushi Chaudhary; Ashish Sharma; Neeraj Gupta Digital Data Protection Using Barcode & Steganographic Approach 2022 International Conference On Automation, Computing And Renewable Systems (Icacrs)Year: 2022

[40]. Wafa M. Eid;Sarah S. Alotaibi;Hasna M. Alqahtani;Sahar Q. Saleh Digital Image Steganalysis: Current Methodologies And Future Challenges Ieee Access Year: 2022

[41]. Jiahao Liu; Ge Jiao; Xiyu Sunfeature Passing Learning For Image Steganalysis Ieee Signal Processing Letters Year: 2022

[42]. Bibek Ranjan Ghosh; Siddhartha Banerjee; Ayush Chakraborty; Swapnajoy Saha; Jyotsna Kumar Mandal A Deep Learning Based Image Steganalysis Using Gray Level Co-Occurrence Matrix 2022 Second International Conference On Advances In Electrical, Computing, Communication And Sustainable Technologies (Icaect) Year: 2022

[43]. Ismail Taha Ahmed; Baraa Tareq Hammad; Norziana Jamil Image Steganalysis Based On Pretrained Convolutional Neural Networks 2022 Ieee 18th International Colloquium On Signal Processing & Applications (Cspa) Year: 2022

[44]. Bhatia, A., & Bedi, P. (2021). Image Steganography Using Generative Adversarial Networks. Journal Of Information Security And Applications, 60, 102805.

[45]. Hu, Y., & Guo, S. (2021). Image Steganography Based On Convolutional Neural Networks With Multi-Scale Feature Fusion. Soft Computing, 25(4), 2943-2954.

[46]. M. Esaiselvam; R. Sambathkumar; K. Yuvaraj; D. Sriram Technique For Estimating Position Of The Pirate Identification Using Machine Learning Algorithms From An Image 2021 International Conference On System, Computation, Automation And Networking (Icscan) Year: 2021

[47]. Nandhini Subramanian; Omar Elharrouss; Somaya Al-Maadeed; Ahmed Bouridane Image Steganography: A Review Of The Recent Advances Ieee Access Year: 2021

[48]. Pei Li; Yeli Li; Hongjuan Wang; Chang Liu Research On Steganalysis Of Digital Image Based On Deep Learning2021 4th International Conference On Advanced Electronic Materials, Computers And Software Engineering (Aemcse) Year: 2021

[49]. Ismail Kich; El Bachir Ameur; Youssef Taouil; Amine Benhfid Image Steganography Scheme Using Dilated Convolutional Network 2021 12th International Conference On Information And Communication Systems (Icics) Year: 2021

[50]. Luo, C., Zhang, W., & Huang, J. (2020). Deep Learning Based Image Steganography Using Pixel-Value Differencing. Journal Of Ambient Intelligence And Humanized Computing, 11(6), 2325-2335.

[51]. Srushti S Yadahalli;Shambhavi Rege;Reena Sonkusare (2020) Implementation And Analysis Of Image Steganography Using Least Significant Bit And Discrete Wavelet Transform Techniques2020 5th International Conference On Communication And Electronics Systems (Icces) Ieee

[52]. B. Vishnu;Leena Vishnu Namboothiri;Sandeep R. Sajeesh;Leena Vishnu Namboothiri (2020) Enhanced Image Steganography With Pvd And Edge Detection2020 Fourth International Conference On Computing Methodologies And Communication (Iccmc) Ieee

[53]. T. Kalaichelvi;P. Apuroop (2020) Image Steganography Method To Achieve Confidentiality Using Captcha For Authentication2020 5th International Conference On Communication And Electronics Systems (Icces) Ieee

[54]. J. H. Lee;D. Y. Kang;J. E. Lee;S. H. Lee;J.-I. Park (2020) Automatic Recovery Of Hidden Image From Image Steganography Using Dnn And Local Entropy Features2020 35th International Technical Conference On Circuits/Systems, Computers And Communications (Itc-Cscc) Iee

[55]. Omar Elharrouss;Noor Almaadeed;Somaya Al-Maadeed (2020) An Image Steganography Approach Based On K-Least Significant Bits (K-Lsb)2020 Ieee International Conference On Informatics, Iot, And Enabling Technologies (Iciot) Ieee

[56]. Xu, X., Pan, J. S., Wang, J., & Zhu, W. (2018). A Survey On Image Steganography And Steganalysis Techniques. Journal Of Information Hiding And Multimedia Signal Processing, 9(6), 1361-1376.

[57]. Zhang, X., Cao, X., & Niu, Y. (2019). A Survey On Deep Learning For Image Steganography And Steganalysis. Information, 10(11), 352. Ksii Transactions On Internet And Information Systems Vol. 14, No. 3, Mar. 2020 1228 Copyright ⓒ 2020 Ksii

[58]. Li, L.; Qian, J.; Pan, J.-S. Characteristic Region Based Watermark Embedding With Rst Invariance And High Capacity. Aeu—Int. J. Electron. Commun. 2011, 65, 435–442.

[59]. Naharuddin, A.; Wibawa, A.D.; Sumpeno, S. A High Capacity And Imperceptible Text Steganography Using Binary Digit Mapping On Ascii Characters. In Proceedings Of The 2018 International Seminar On Intelligent Technology And Its Applications (Isitia), Bali, Indonesia, 30–31 August 2018; Pp. 287–292.

[60]. Malik, A.; Sikka, G.; Verma, H.K. A High Capacity Text Steganography Scheme Based On Lzw Compression And Color Coding. Eng. Sci. Technol. Int. J. 2017, 20, 72–79

[61]. Sadié, J.K.; Metcheka, L.M.; Ndoundam, R. A High Capacity Text Steganography Scheme Based On Permutation And Color Coding. Arxiv 2020, Arxiv:2004.00948.

[62]. Al-Azzawi, A.F. A Multi-Layer Arabic Text Steganographic Method Based On Letter Shaping. Int. J. Netw. Secur. Its Appl. (Ijnsa) 2019, 11. Available Online: Https://Ssrn.Com/Abstract=3759471 (Accessed On 29 September 2021).

[63]. Liang, O.W.; Iranmanesh, V. Information Hiding Using Whitespace Technique In Microsoft Word. In Proceedings Of The 2016 22nd International Conference On Virtual System & Multimedia (Vsmm), Kuala Lumpur, Malaysia, 17–21 October 2016; Pp. 1–5.

[64]. Baawi, S.S.; Nasrawi, D.A. Improvement Of "Text Steganography Based On Unicode Of Characters In Multi-Lingual" By Custom Font With Special Properties. In Proceedings Of The Iop Conference Series: Materials Science And Engineering, Jonkoping, Sweden, 22–23 June 2020; Volume 870, P. 012125.

[65]. Shah, S.T.A.; Khan, A.; Hussain, A. Text Steganography Using Character Spacing After Normalization. Int. J. Sci. Eng. Res. 2020, 11, 949–957.