COMPREHENSIVE LITERATURE REVIEW OF COVER OBJECTS AND THEIR EMBEDDING PROCEDURE IN STEGANOGRAPHY

[1]Khushi Kalra, [2]Anvesh Tewari,[3]Yash Gaur, [4]Ashish Kumar
Vivekananda Institute of Professional Studies-Technical Campus, New Delhi, India
[1]kalrakhushi2535@gmail.com,
[2]anvesh932@gmail.com,
[3]yashgaur3000@gmail.com,
[4]ashishkumar@vips.edu

Abstract

Steganography is the practice of obfuscating information such that it is difficult for an unauthorized individual to discover its presence inside other non-secret data, such as an image, audio file, or text. Steganography's primary function is to safeguard communication by disguising private data from prying eyes. Since the use of encryption techniques might draw attention to communication, steganography can also be used to evade discovery by uninvited parties. Steganography can offer an extra degree of protection by completely concealing the message's existence. Steganography's primary objective is to make sure that only the intended receiver can access the concealed message and that nobody else is aware of its existence. In the literature review, we have expanded upon four major types of steganography, i.e., Video, Image, Text and Audio. We have outlined the approaches, benefits, and drawbacks of the different steganography techniques. The goal of our literature study is to compile current, pertinent research on Steganography and combine it with other relevant studies to create a comprehensive overview of what is already known in Steganography.

Keywords: Steganography, Types of Steganography, Image Steganography, Video Steganography, Text Steganography.

1. INTRODUCTION

The worry of having data spied on while it is being sent from the sender to the recipient has increased because of development in the field of data transmission. Information Security is therefore becoming an integral component of data communication. Steganography is a method of hiding secret information to escape detection within a regular, non-secret communication or file. The hidden information is retrieved at the destination. Text, audio, image, and video are the carrier file formats used in steganography. [1]

The media which is sent hiding the message is known as a cover object and the actual concealed media is called a stego object. Steganography and encryption working together add another level of data security.

The Greek words "steganos," which mean covered or hidden, and "graph," which means to write, are the source of the word "steganography." Many sorts of digital content, such as text, images, videos, or audio files, can be hidden via steganography. Before being included into the seemingly innocent-looking cover text file or data stream, the data that needs to be hidden, known as hidden text, is often encrypted. When the hidden text is not encrypted, it is usually handled in a specific way to make it more challenging to figure out what it contains. Steganography is a term that refers to a variety of methods for concealing messages in apparently innocent objects. These methods have been used for centuries. [2]

For instance, hiding documents recorded on the microdot, which has a diameter as small as one millimetre, on or inside correspondence that appears to be legitimate; using invisible ink to cloak secret messages in otherwise inoffensive messages; or even using multiplayer gaming environments to share information.

Steganography is the process of concealing sensitive information within other types of data, such an image or audio file. Using a unique technique, the concealed message is first encrypted or obfuscated before being put into the data. Steganography is frequently used for watermarking, which is how online publishers locate the origin of media assets. One such method is to use l bit to embed a text file into an image file. [3] Either manually or with the aid of a steganography tool, this can be done. Although steganography and cryptography are distinct, combining the two can increase the security of sensitive data and guard against detection instead of relying solely on encryption for communication, steganographically disguised material that is encrypted may nevertheless be safe from detection. [4]

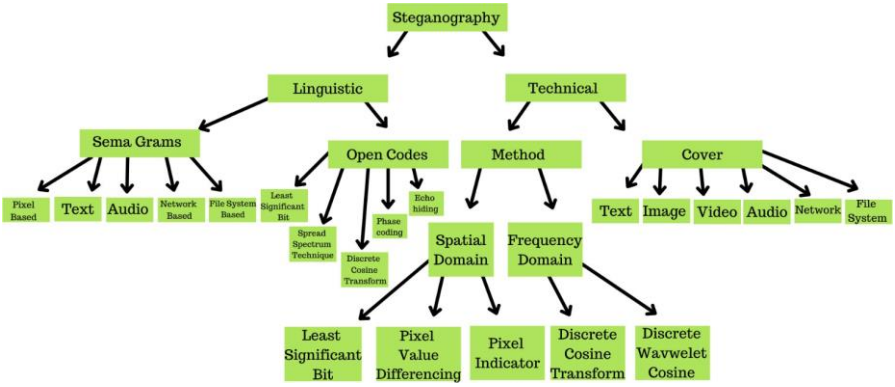

Figure 1. Classification of Image Steganography

2. RESEARCH PROBLEMS AND LITERATURE REVIEW

Finding ways to conceal sensitive information within another file or set of data without arousing suspicion is the central theme of the suggested algorithm's issue description. Even if someone intercepts the message or file, they won't be able to identify that there is concealed information because steganography aims to make the secret information untraceable.

Consequently, discovering appropriate file formats, encoding methods, and encryption algorithms that can be used to successfully hide data may be the issue statement in this system. Analysing the exchange between the degree of concealment and the potential effects on the size, quality, and performance of the host file may also be a part of the project. Our goal is to keep the information given anonymous. The proposed system might also help with the difficulties associated with detecting and preventing steganography, as this technology can also be employed maliciously to evade security measures or contain malware. As a result, the research may involve investigating techniques for detecting steganography in files and data as well as creating defenses against its abuse. [5]

<H2> Steganography in Video Cover Object

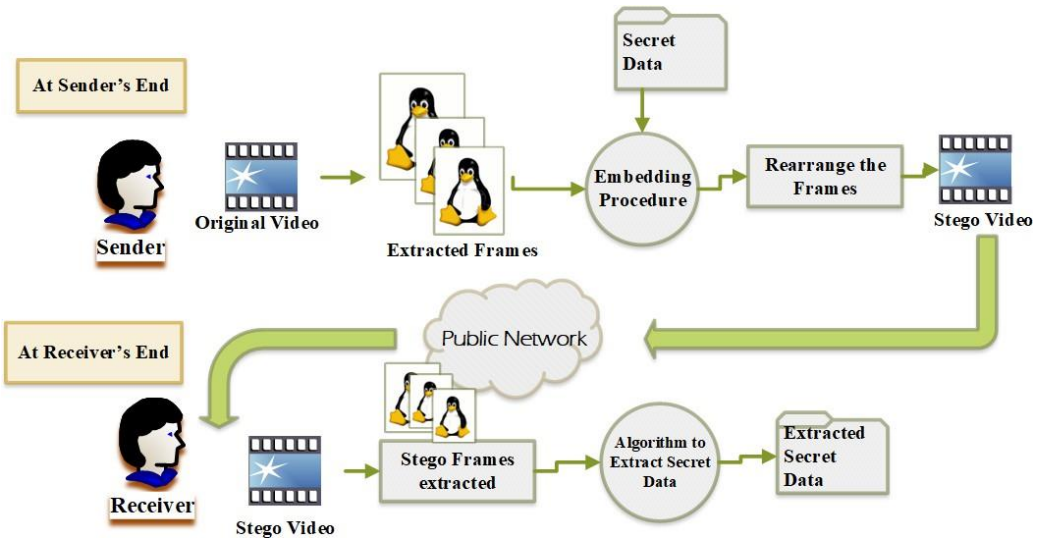

Figure 3. Steganography in Video Object

The art of video steganography allows you to conceal any form of file under a cover video file. Due to its size and complexity, video-based steganography may be more secure to utilise than other multimedia files. Video steganography can be classified into three categories: 1) Frame based steganography 2) Format-based steganography 3) Video codec-based steganography. In recent time, Researchers are interested in Frame-based steganography techniques and developed various algorithms on different multimedia. [6]

TABLE I: Literature Review of the Video based steganography systems

Reference Article	Title of the Paper	Methodology	Cover data	Sent data	Advantage	Disadvantage
[10]	Optimized Video Steganography Using Genetic Algorithm (GA)	The study uses a Genetic Algorithm (GA) to optimize for resilience and imperceptibility while embedding concealed data into a video.	Video	Video	Provides an effective and undetectable steganographic method for automatically optimized videos.	Possible processing overhead and a complex implementation.
[11]	A New Video Steganography Scheme Based on Shi-Tomasi Corner Detector	In order to improve robustness and imperceptibility, the paper uses the Shi-Tomasi corner detector to identify and	Video	Image	Enhanced resistance to detection, selective embedding in regions of interest, and robustness against standard video processing	Potential speed and capacity restrictions because corner-based methods might not be able to handle large data loads or real-time processing.

		insert hidden			processes.	
		data within video frames.				
[12]	Enhancing Data Security Using Video Steganography	The study improves data security by using video steganography techniques to conceal data inside videos.	Video	Image	Improved data security by hiding information in video files.	Videos with limited data capacity and possible detection vulnerabilities.
[13]	Video Steganography Based on Optimized Motion Estimation Perturbation	The study improves imperceptibility by using optimal motion estimation perturbation to conceal information in video.	video	Video	Enhanced durability, detection resistance, and concealment in video frames.	Possible complexity in calculations and longer encoding times.
[14]	Robust video steganography algorithm using adaptive skin-tone	The study uses strong video steganograph	Video	Image	Improved imperceptibility and resilience by	Restricted application to areas of videos without skin tones; possible

	detection	y with			the use of	difficulties in a
		adaptive skin-tone recognition to improve concealment in human skin areas.			adaptive skin-tone detection.	variety of content situations.
[15]	Video steganography using Flash Video (FLV)	After much experimentin g with the FLV file format to change and incorporate more data, a C++ application for video steganograph y was created as a result of the research.	Video	Video	The software provides strong security for sensitive data by achieving 100% lossless extraction, preserving original picture and sound quality, and guaranteeing hidden data integrity during transmission.	"Double-stegging" has the ability to corrupt or lose data from files that have undergone successive embedding, making the original message "inextractable" using the same application.

[16]	A secure video steganography based on the intra-prediction	The research develops a safe video steganograph	Video	Video	Enhanced security by integrating intra-predictio	Restricted data capacity and possible complexity in the extraction
	mode (IPM) for H264.	y method that increases imperceptibili ty by utilizing intra-predicti on modes in H.264.			n modes and H.264 compression.	and embedding procedures.
[17]	An Adaptive Video Steganography Based on Intra-prediction Mode and Cost Assignment	The research develops an adaptive video steganograph y technique using cost assignment and intra-predicti on modes.	Video	Video	Improved security and flexibility by integrating cost assignment with intra-predictio n.	Possible computational overhead and complexity in the extraction and embedding procedures.

[18]	A data-hiding technique using scene-change detection for video steganography	The study improves security and concealment by using scene-change detection to hide data in videos.	Video	Image	Enhanced security by using scene-change-based steganography, which increases the difficulty of detection.	Restricted ability to conceal data within scene transitions, sometimes leading to visual distortions.

[19]	Hiding large amount of data using a new approach of video steganography	This work uses video steganography to hide information in video frames during scene changes by using the Least Significant Bit (LSB) replacement technique. For further security, a chaotic sequence based on indexing is used to randomly determine the locations of pixels for information embedding.	Video	Video	Since the stego video and the original cover video are virtually identical, interceptors will have a very tough time identifying any variations in perception, guaranteeing strong concealment of any secret information.	Potential problems with the steganographic method's resilience, such as its ability to withstand different types of attacks or possible data loss during transmission or extraction, are not discussed in the research.

[20]	Wavelet Based Color Video Steganography	The technique described in this research uses wavelet transforms to mask data in color video frames so as to increase capacity without sacrificing quality.	Video	Image	Superior visual clarity and increased data capacity over some other techniques.	A possible increase in computing complexity and vulnerability to sophisticated steganalysis.
[21]	Stego machine-video steganography using LSB algorithm	In order to encrypt video, the study uses the Least Significant Bit (LSB) technique, which embeds data in the least significant bits of video frames.	Video	Text	The LSB algorithm's simplicity, which makes it simple to use.	LSB steganography has a limited ability to conceal data and is susceptible to detection.

[22]	Video steganography using motion vector and linear block codes	The paper performs video steganography by using motion vectors and linear block codes, using motion information for data embedding.	Video	Video	With motion vector integration, security and data capacity are increased.	Possible for the extraction process to be complex and vulnerable to distortions caused by motion.

3. STEGANOGRAPHY IN IMAGE COVER OBJECT

The method of hiding information, such as text, images, or videos, under a cover

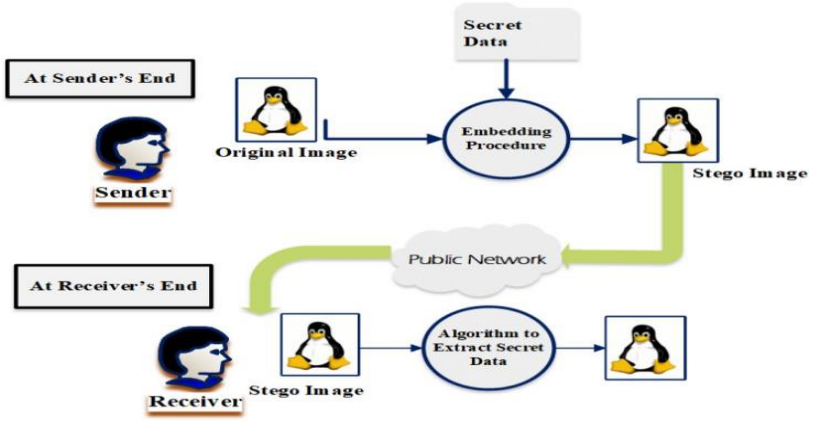

Figure 4. Steganography in Image Cover Object

picture is known as image steganography. The secret information is concealed so that human eyes cannot see it. Recent years have seen a surge in interest in deep learning technology, which has shown to be a potent tool in a number of applications, including picture steganography. It is observed that image steganography is popular among all the steganography techniques. [7]

TABLE II: Literature Review of the Image based steganography systems

Reference Article	Title of the Paper	Methodology	Cover data	Sent data	Advantage	Disadvantage
[23]	Spread spectrum image steganography	The study employs spread spectrum techniques to provide resilience and detection resistance by hiding data inside images.	Image	Text	Improved resistance to many types of attacks, robustness, and imperceptibility.	Greater computational complexity in contrast to more straightforward steganographic techniques.
[24]	Analysis of LSB based image steganography techniques	The efficacy and weaknesses of several LSB-based image steganography algorithms are evaluated in this research.	Image	Text	Ease of use and the capacity to conceal information in pictures.	Higher vulnerability to optical artifacts and possible detection.

[25]	A new cost function for spatial image steganograph y	With the help of two low-pass filters to cluster low-cost values and a high-pass filter to locate less predictable picture areas, this research presents a unique cost function for spatial image steganography. In order to reduce embedding distortion, this method focuses on embedding changes in texture regions.	Image	Im a ge	The suggested cost function is a potential development in picture steganography since it improves the steganographic method's resistance against cutting-edge steganalysis tools, surpassing earlier studies like HUGO, WOW, and S-UNIWARD.	The novel cost function's possible shortcomings and restrictions aren't thoroughly examined in the study, which could be crucial for a thorough assessment of its suitability in a range of situations.

[26]	Edge-based image steganograph y	The study presents a novel steganography method that employs the cover image's edges for message embedding. Weaker edges are prioritized for larger data payloads, and the selection of edges is based on the quantity of data to be hidden.	Image	Im a ge	The suggested method offers a larger embedding capacity and outperforms state-of-the-art steganography techniques, indicating that it is a promising development in data concealment.	The novel technique's possible downsides and limitations are not included in the report, which could be crucial for a thorough grasp of its applicability and potential weaknesses.
[27]	Digital image steganograph y using	The paper presents a brand-new steganography technique. It guides	Image	Im a ge	This method improves security and works in a variety of fields, such	The potential implementatio n problems are not covered in the paper.

	universal distortion	embedding adjustments in difficult-to-model picture areas using a universal distortion metric.			as side-informed JPEG, spatial, and JPEG.	
[28]	A New Method in Image Steganograph y with Improved Image Qualit y	By finding similar bits between the message and image pixels, comparing it with the LSB benchmarking method, and analyzing the findings, the paper's methodology entails hiding a hidden message.	Image	Im a ge	The suggested steganography technique achieves an 83% accuracy rate while improving image quality. It is effective, straightforward, quick, and resistant to attacks.	The proposed method's possible shortcomings and weaknesses are not thoroughly examined in the research, which leaves opportunity for unidentified consequences.

[29]	Securing Data in Internet of Things (IoT) Using Cryptography and Steganograph y Techniques	In order to conceal the encrypted data in an image, the study first introduces an elliptic Galois cryptography protocol. Next, it employs Matrix XOR encoding steganography and an Adaptive Firefly optimization algorithm to choose cover blocks inside the image.	Image	Tex t and Ima ge	By integrating steganography and cryptographic techniques, this methodology improves the security of Internet of Things data and provides a strong solution for user authentication and data privacy.	The suggested approach's possible downsides and practical difficulties are not discussed in the research, leaving implementation issues unsolved in the actual world.
[30]	Steganograph y Technique Based on DCT Coefficients	Through the use of sophisticated approaches that use criteria or DCT coefficients above a threshold for information insertion, the strategy replaces LSBs in the cover image with secret data bits through the use of LSB-based spatial steganography.	Image	Im a ge	For the purpose of hiding data in the spatial domain, LSB-based steganography techniques are widely used and provide a convenient approach to embedding confidential information into cover images.	Although DCT-based methods offer a way to find possible insertion places by utilizing DCT coefficient values, they might not be very sophisticated and might not completely address security and robustness issues in steganography.

[31]	An analysis of LSB based image steganograph y techniques	The efficacy, detection potential, and vulnerabilities of several LSB-based image steganography algorithms are evaluated in this research.	Image	Im a ge	Ease of use and the capacity to conceal information in pictures.	Higher vulnerability to optical artifacts and possible detection.
[32]	A Novel Techniqu e for Data Steganograp h y	Presents a new steganography method that uses the decimal value of the characters in the secret message to hide data within a cover image.	Image	Im a ge	Its simplicity and ease of implementation, as well as its resistance to various steganalysis techniques due to its use of a random key to determine the number of bits used for each character in the secret message.	A limited amount of secret data that can be embedded in the cover image and the possibility of losing some of the cover image's quality due to the embedding process.

[33]	Investigation on Cost Assignment in Spatial Image Steganography	In order to improve resistance to steganalysis with rich model characteristics in spatial images, the research presents a five-step cost assignment scheme, divides cost assignment into two phases, and specifies a cost-value distribution.	Image	Image	By dissecting cost assignment, the paper's technique presents a novel strategy that, when combined with a uniform distribution, produces a linear relationship between the steganography payload and cover element change rate.	The suggested cost assignment scheme's possible shortcomings are not fully covered in the study, leaving opportunity for unanswered questions and pragmatic concerns.
[34]	Edge Adaptive Image Steganography Based on LSB Matching Revisited	In order to improve security and visual quality, the research builds on LSB matching revisited picture steganography by using an edge adaptive approach that chooses embedding regions selectively based on cover image	Image	Image	By picking embedding regions based on the cover picture content and secret message size, the proposed edge adaptive LSB-based steganography technique improves security while maintaining visual quality and improving data concealing.	It ignores practical issues by skipping over any potential computational challenges or restrictions related to putting the suggested approach into practice.

		content and secret message size.				
[35]	A novel image steganograph	In order to improve data hiding security, the paper's	Image	Im a ge	When it comes to steganography, quantum substitution	The lack of discussion of potential implementation
	y technique based on quantum substitution boxes	methodology uses quantum substitution boxes for image steganography.			boxes can provide more security and encryption than traditional methods.	difficulties or barriers when integrating quantum technologies in the research could be a drawback in real-world implementations.

[36]	CNN-Based Adversarial Embedding for Image Steganograph y	The technique for adversarial embedding in image steganography using Convolutional Neural Networks (CNNs) is examined in this research.	Image	Im a ge	CNNs improve data hiding security by offering strong and efficient adversarial embedding techniques in picture steganography.	It's possible that the research leaves out important details about processing costs and other restrictions that come with employing CNNs in real-world applications.
[37]	Coverless Image Steganograph y Without Embedding	In order to enable information concealment without embedding, the study presents a coverless picture steganography architecture that chooses original images containing the secret data directly from a database built using hash sequences. This eliminates the necessity for a predetermined cover image.	Image	Im a ge	uncovered picture By preventing alteration traces in cover images, increasing the difficulty of steganalysis, and exhibiting resilience against popular image attacks, steganography improves security.	The construction and management of the original picture database may provide certain practical difficulties in real-world applications, which are not addressed in the study.

[38]	Biometric Inspired Digital Image Steganography	The study makes use of distinct physiological or behavioral traits to embed data in digital photographs using biometric attributes.	Image and Video	Image	This method increases steganography's resilience and security because biometric features are hard to copy, protecting data.	The use of biometric data, however, may give rise to privacy issues and restrict application in situations where biometric data is not easily accessible.
[39]	Medical JPEG image steganography based on preserving inter-block dependencies	The inter-block interdependence in medical JPEG images are maintained by the use of steganography techniques in this paper.	Image	Image	This method ensures little influence on patient care while maintaining the diagnostic quality of medical imaging.	When complexity rises, embedding capacity may decrease and computational resources may be needed, which could have an impact on efficiency.
[40]	SteganoGAN: High Capacity Image Steganography with GANs	In order to accomplish high-capacity image steganography, a unique method utilizing Generative Adversarial Networks (GANs) is presented in this research.	Image	Image	By utilizing GANs to imbue a vast quantity of information into photos, SteganoGAN offers high-capacity steganography that can be advantageous for a range of uses.	GAN-based steganography can encounter difficulties with security and detection as advanced techniques for identifying content created by GANs keep developing.

[41]	A chaotic video steganograph	Using chaotic systems for data hiding, the method	Image	Vid e o	Chaotic video steganography is a flexible and reliable	If not used appropriately, this method can be
	y technique for carrying different types of secret messages	uses chaos theory to insert several kinds of secret messages within video material.			technique that provides a high degree of security and the capacity to carry many kinds of hidden messages within the same video.	computationally demanding and have an effect on the quality of the video, which could cause suspicion or detection issues.
[42]	RGB Intensity Based Variable-Bits Image Steganograp h y	This method embeds secret information at different bit rates by varying the intensity levels of the red, green, and blue (RGB) color channels of an image.	Image	Im a ge	By balancing data concealment and image quality, the approach enables effective steganography with the ability to modify the embedding capacity.	The amount of hidden data and the possible impact on image fidelity can be traded off depending on the bit rate selected for steganography, and if the technique is not used carefully, it may be discovered.

[43]	A Secure And High Capacity Image Steganograph y Technique	This technology safely embeds a lot of data into photos by using sophisticated encryption and data concealment techniques.	Image	Im a ge	It is appropriate for situations where data capacity and secrecy are crucial since it provides both security and great data capacity.	This method might need a lot of computer power, depending on how complicated the data embedding and encryption are, and it might make steganalysis difficult for skilled attackers.
[44]	Robust Invertible Image Steganograph y	The goal of this technique is to reliably and losslessly extract hidden data from images by embedding it in a way that is fully invertible and resilient to conventional image processing techniques.	Image	Im a ge	The technique preserves the quality of the image by making sure the hidden data is kept hidden even after the stego image goes through a number of image processing steps.	It can be difficult to strike a compromise between robustness and full invertibility, which could restrict the amount of data that can be hidden and necessitate the use of more sophisticated algorithms.

4. STEGANOGRAPHY IN TEXT COVER OBJECT

Text steganography is a method of concealing a secret text message as a covering message inside of another text or by creating a cover message that is connected to the original hidden message. As text papers are frequently used in businesses, employing one as a cover media could be a better option there. [8]

TABLE III: Literature Review of the Text based steganography systems

Reference Article	Title of the Paper	Methodology	Cover data	Sent data	Advantage	Disadvantage
[45]	Information hiding: A new approach in text steganography" proposes a new approach to text steganography.	The paper proposes a new technique for text steganography called the Matrix Encoding Technique (MET), which involves encoding a secret message into a matrix of characters in the cover text.	Text	Text	MET provides a high degree of security as the hidden message is encoded into a matrix rather than being inserted into the text directly, making it difficult to detect.	The size of the cover text must be sufficiently large to accommodate the matrix encoding, and the encoding process can be computationally expensive.
[46]	A New Approach to Persian/Arabic Text Steganography	The article provides an overview of different image segmentation techniques including thresholding, region-based methods, edge-based methods, and clustering algorithms.	Text	Text	The article highlights the strengths and weaknesses of each segmentation technique and provides insights into which techniques may be best suited for	The article does not provide a comprehensive evaluation of the performance of each technique, and the effectiveness of the segmentation may depend heavily on the

					different remote sensing applications.	characteristics of the remote sensing data being analyzed.
[47]	Text Steganography in chat	This study presents a novel approach to secure communication in chat rooms by utilizing abbreviated text steganography, which is based on the SMS texting language and is implemented in Java programming.	Text	Text	By addressing the requirement for safe chat communication, the suggested approach improves online privacy and information security.	Unresolved issues may arise since the research does not thoroughly examine any potential restrictions or practical difficulties associated with using this steganographic technique in real-world chat applications.
[48]	Text Steganography by Changing Words Spelling	The study presents a novel steganography technique for English texts that discreetly hides data within the text by using the US and UK spellings of words like "color" and "colour."	Text	Text	By taking use of the minute variations in word spelling between American and British English, this method offers a distinctive and discrete means of	The efficiency of this technique in various situations may be impacted by linguistic or contextual constraints when employing word spelling variants for

					data concealment in English texts.	steganography, although these issues are not explored in the research.
[49]	Emoticon-based text steganography in chat	In contrast to earlier approaches, the research presents a text steganography technique that increases embedding capacity by employing emoticons, or emotional icons, in chat rooms to conceal sensitive information within phrases.	Text	Text	This method makes use of the common emoticon usage in chat rooms to increase data hiding ability, which makes it appropriate for practical and user-friendly text steganography.	The method's efficacy in various chat contexts may be impacted by variations in emoticon usage, which are not addressed in the paper as potential constraints or difficulties.
[50]	Experimenting with the Novel Approaches in Text Steganography	The drawbacks of current text-based steganography are addressed by the paper, which proposes novel steganographic methodologies that combine random character sequences with feature coding	Text	Text	Compared to alternative ways for text-based steganography, the suggested methods offer lower overhead and higher randomization, which may improve security.	The study leaves open the possibility of unidentified disadvantages in the real-world application of the suggested techniques by failing to fully address any potential difficulties

		techniques to conceal information in text files.				or restrictions.
[51]	An innovative method of Text Steganography	In order to obtain a secret code, the study uses Discrete Wavelet Transform (DWT) to divide an input image into sub-bands, conceal text information in a low-frequency band, use DWT to compress the image, and then apply Inverse Discrete Wavelet Transform (IDWT) to recover the image and decode it.	Text	Text	The suggested approach hides information in the lowest plane of the image to reduce noise while combining DWT and encryption approaches to offer robust security, resistance to many types of attacks, and good hidden invisibility.	The suggested method may have computational complexity or constraints that need to be considered for practical implementation in a variety of contexts, however they are not covered in the study.
[52]	Text Steganography Based on Ci-poetry	This method creates Ci-poetry, a kind of traditional Chinese poetry, using a	Text	Text	By using Ci-poetry, text steganography can be made less	The limitations of the Ci-poetry structure may restrict the ability

	Generation Using Markov Chain Model	Markov Chain model and conceals sensitive information in the poetry.			obvious to possible detectors by using a delicate and culturally rich medium.	to hide data, and the linguistic and cultural environment may have an impact on how well this technique works.

5. STEGANOGRAPHY IN AUDIO COVER OBJECT

The goal of audio steganography is to incorporate the covert message into the audio. Audio file is taken as input and the audio file is converted into one-dimensional array. Audio steganography is usually done in the frequency domain. It is a method for concealing or securing the transfer of sensitive information. If the communication is encrypted, it could also guarantee the message's secrecy. [9]

TABLE IV: Literature Review of the Audio based steganography systems

Reference Article	Title of the Paper	Methodology	Cover data	Sent data	Advantage	Disadvantage
		In addition to discussing several steganography techniques, the research reviews			By fixing shortcomings in substitution approaches,	Practical aspects may go unexplored

[53]	A secure audio steganography approach	current approaches, looks into two shortcomings in substitution techniques, and presents a novel method that enhances robustness by embedding message bits in	Audio	Audio	the suggested genetic algorithm methodology increases steganography's robustness and may even be able to fully utilize the power and promise of these techniques.	because the research may not completely address computational complexities or other challenges related to implementing the genetic algorithm in real-world steganographic applications.
		many higher-order LSB layers using a genetic algorithm.				
		This study uses the Least Significant Bit (LSB) modification technique for audio steganography.			The suggested method improves audio	

[54]	An enhanced least significant bit modification technique for audio steganography	In order to increase security, it introduces enhancements by randomly selecting the sample number that contains the next bit of secret data and the bit number in the host message that is used to embed secret data.	Audio	Audio	steganography security by strengthening its resistance to steganalysis and lowering the possibility that unauthorized users would extract confidential information. The secret communication is further secured by the use of Advanced Encryption Standard (AES).	Practical implications are left unexamined, and potential constraints or obstacles related to the suggested strategy are not fully discussed in the research.

[55]	Adaptive Digital Audio Steganography Based on Integer Wavelet Transform	In order to attain imperceptibility, this technique modifies the embedding process of hidden data in digital audio signals using the Integer Wavelet Transform.	Audio	Audio	Adaptive and reliable steganography is made possible by the use of the integer wavelet transform, which can also be useful for preserving audio quality while concealing data.	Depending on the parameters selected and the properties of the audio signal, the amount of data that can be hidden may be restricted, and it may be vulnerable to being discovered by sophisticated steganalysis techniques.
[56]	A GA based audio steganography with enhanced security	Genetic algorithm based audio steganography technique with a random key and a hash function.	Audio	Audio	Provides high security against various attacks, allows for adaptive selection of embedding positions, and has a high embedding capacity.	May slightly decrease the audio quality, requires a significant amount of computational resources, and can be time-consuming.
[57]	AHCM: Adaptive Huffman Code Mapping for Audio Steganography	This method uses an adaptive Huffman code mapping methodology, informed by	Audio	Audio	Adaptive coding and psychoacoustic models are combined by AHCM to	The psychoacoustic model's accuracy, the audio encoding type selected, and the approach's data capacity constraints

	Based on Psychoacoustic Model	psychoacoustic models, to embed hidden			increase the steganography's imperceptibility	could all affect how effective the method is.
		information into audio recordings while accounting for the perceived properties of the human auditory system.			and reduce human auditory detection.	
[58]	Audio Steganography Using GA	This method optimizes the arrangement of the data for imperceptibility by embedding concealed data within audio recordings using genetic algorithms.	Audio	Audio	The best embedding places can be found with the use of genetic algorithms, strengthening the steganography's resilience and making it more difficult to decipher.	Genetic algorithms can be computationally demanding, requiring more processing power; also, the efficiency of the method and the audio file type selected can affect the algorithm's ability to hide data.

[59]	Blowfish–Secur ed Audio Steganograph y	This method embeds and secures secret data within audio files by combining audio steganography and Blowfish encryption.	Audio	Audio	The security of the hidden data is increased by using Blowfish encryption, and audio steganograph y can offer a discrete method of data delivery.	The technique might not be able to handle large amounts of data, and there might be difficulties in decoding and finding hidden information in audio recordings.

6. CONCLUSION

In this paper, we discussed the four varieties of steganography: image, text, video, and audio. Research problems and requirements to execute steganography, a literature review focused on specific approaches, along with methodologies, benefits, drawbacks, cover objects, and sent objects, are supplied. Different methods of applying Steganography are found in the literature review.

With an emphasis on video, picture, text and audio steganography in particular, the literature study provided a thorough overview of the many techniques and procedures utilised in steganography. The articles under consideration addressed a wide range of methodologies, including, among others, chaotic systems, genetic algorithms, and neural networks.

In order to achieve high security, resilience, and embedding capacity in video steganography, various articles investigated the use of evolutionary algorithms and motion estimation perturbation. However, several of these techniques were computationally costly, which constrained their usefulness. For increased resilience, some approaches made use of adaptive skin-tone detection and intra-prediction mode, however, they might not be successful against all kinds of attacks.

The majority of works on image steganography concentrated on LSB-based techniques, wavelet-based strategies, and spread spectrum steganography. These methods showed a number of benefits, including a high embedding capacity,

security, and resistance to steganalysis, but they also encountered difficulties due to the complexity of the computations involved and the possible effects on picture quality.

Researchers have investigated adaptive approaches for audio steganography utilising evolutionary algorithms, chaotic systems, and encryption-based techniques. These methods have strong embedding and security capacities but needed significant computational resources.

It is clear that the subject of steganography is always changing, and as technology and cryptography develop, new problems and possibilities will appear. To find the best strategies for various types of data and applications, future research should concentrate on fixing the shortcomings of existing techniques, investigating innovative ways, and performing thorough assessments under various circumstances.

To sum up, steganography research continues to be crucial for improving data security and secrecy in many digital media. The articles that were evaluated provided insight into the advancements made in this area as well as the difficulties still to be overcome, which was a significant addition to the development of steganographic methods. To maintain the security and integrity of sensitive information, researchers must continue to be cautious in creating and improving strong and secure steganography technologies.

REFERENCES

[1] Rakhi, S. G. (2013). A review on steganography methods. *International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering*, *2*(10).

[2] Kour, J., & Verma, D. (2014). Steganography techniques–A review paper. *International Journal of Emerging Research in Management &Technology ISSN*, 2278-9359.

[3] Walia, E., Jain, P., & Navdeep, N. (2010). An analysis of LSB & DCT based steganography. *Global Journal of Computer Science and Technology*, *10*(1), 4-8.

[4] Karthikeyan, B., Kosaraju, A. C., & Gupta, S. (2016, March). Enhanced security in steganography using encryption and quick response code. In *2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)* (pp. 2308-2312). IEEE.

[5] Johnson, N. F., & Jajodia, S. (1998, September). Steganalysis: The investigation of hidden information. In *1998 IEEE Information Technology Conference, Information Environment for the Future (Cat. No. 98EX228)* (pp. 113-116). IEEE.

[6] Mstafa, R. J., & Elleithy, K. M. (2017). Compressed and raw video steganography techniques: a comprehensive survey and analysis. *Multimedia Tools and Applications*, *76*, 21749-21786.

[7] Morkel, T., Eloff, J. H., & Olivier, M. S. (2005, June). An overview of image steganography. In *ISSA* (Vol. 1, No. 2, pp. 1-11).

[8] Krishnan, R. B., Thandra, P. K., & Baba, M. S. (2017, March). An overview of text steganography. In *2017 Fourth International Conference on Signal Processing, Communication and Networking (ICSCN)* (pp. 1-6). IEEE.

[9] Dutta, H., Das, R. K., Nandi, S., & Prasanna, S. M. (2020). An overview of digital audio steganography. *IETE Technical Review*, *37*(6), 632-650.

[10] Dasgupta, K., Mondal, J. K., & Dutta, P. (2013). Optimized video steganography using genetic algorithm (GA). Procedia Technology, 10, 131-137.

[11] Mstafa, R. J., Younis, Y. M., Hussein, H. I., & Atto, M. (2020). A new video steganography scheme based on Shi-Tomasi corner detector. IEEE Access, 8, 161825-161837.

[12] Wajgade, V. M., & Kumar, D. S. (2013). Enhancing data security using video steganography. International Journal of Emerging Technology and Advanced Engineering, 3(4), 549-552.

[13] Cao, Y., Zhang, H., Zhao, X., & Yu, H. (2015, June). Video steganography based on optimized motion estimation perturbation. In Proceedings of the 3rd ACM workshop on information hiding and multimedia security (pp. 25-31).

[14] Sadek, M. M., Khalifa, A. S., & Mostafa, M. G. (2017). Robust video steganography algorithm using adaptive skin-tone detection. Multimedia Tools and Applications, 76, 3065-3085.

[15] Mozo, A. J., Obien, M. E., Rigor, C. J., Rayel, D. F., Chua, K., & Tangonan, G. (2009, May). Video steganography using flash video (FLV). In 2009 IEEE Instrumentation and Measurement Technology Conference (pp. 822-827). IEEE.

[16] Cao, M., Tian, L., & Li, C. (2020). A secure video steganography based on the intra-prediction mode (IPM) for H264. Sensors, 20(18), 5242.

[17] Zhang, L., & Zhao, X. (2017). An adaptive video steganography based on intra-prediction mode and cost assignment. In Digital Forensics and Watermarking: 15th International Workshop, IWDW 2016, Beijing, China, September 17-19, 2016,

Revised Selected Papers 15 (pp. 518-532). Springer International Publishing.

[18] Ramalingam, M., & Isa, N. A. M. (2016). A data-hiding technique using scene-change detection for video steganography. Computers & Electrical Engineering, 54, 423-434.

[19] Paul, R., Acharya, A. K., Yadav, V. K., & Batham, S. (2013, September). Hiding large amount of data using a new approach of video steganography. In Confluence 2013: The next generation information technology summit (4th international conference) (pp. 337-343). IET.

[20] Kolakalur, A., Kagalidis, I., & Vuksanovic, B. (2016). Wavelet based color video steganography. International Journal of Engineering and Technology, 8(3), 165.

[21] Ramalingam, M. (2011). Stego machine–video steganography using modified LSB algorithm. International Journal of Information and Communication Engineering, 5(2), 170-173.

[22] Pan, F., Xiang, L., Yang, X. Y., & Guo, Y. (2010, July). Video steganography using motion vector and linear block codes. In 2010 IEEE International conference on software engineering and service sciences (pp. 592-595). IEEE.

[23] Marvel, L. M., Boncelet, C. G., & Retter, C. T. (1999). Spread spectrum image steganography. IEEE Transactions on image processing, 8(8), 1075-1083.

[24] Chandramouli, R., & Memon, N. (2001, October). Analysis of LSB based image steganography techniques In Proceedings 2001 international conference on image processing (Cat. No. 01CH37205) (Vol. 3, pp. 1019-1022). IEEE.

[25] Li, B., Wang, M., Huang, J., & Li, X. (2014, October). A new cost function for spatial image steganography. In 2014 IEEE International conference on image processing (ICIP) (pp. 4206-4210). IEEE.

[26] Islam, S., Modi, M. R., & Gupta, P. (2014). Edge-based image steganography. EURASIP Journal on Information Security, 2014, 1-14.

[27] Holub, V., & Fridrich, J. (2013, June). Digital image steganography using universal distortion. In Proceedings of the first ACM workshop on Information hiding and multimedia security (pp. 59-68).

[28] Al-Shatnawi, A. M. (2012). A new method in image steganography with improved image quality. Applied Mathematical Sciences, 6(79), 3907-3915.

[29] Khari, M., Garg, A. K., Gandomi, A. H., Gupta, R., Patan, R., & Balusamy, B. (2019). Securing data in Internet of Things (IoT) using cryptography and

steganography techniques. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 50(1), 73-80.

[30] Patel, H., & Dave, P. (2012). Steganography technique based on DCT coefficients. International Journal of Engineering Research and Applications, 2(1), 713-717.

[31] Thangadurai, K., & Devi, G. S. (2014, January). An analysis of LSB based image steganography techniques. In 2014 international conference on computer communication and informatics (pp. 1-4). IEEE.

[32] Hindi, A. Y., Dwairi, M. O., & AlQadi, Z. A. (2019). A novel technique for data steganography. Engineering, Technology & Applied Science Research, 9(6), 4942-4945.

[33] Li, B., Tan, S., Wang, M., & Huang, J. (2014). Investigation on cost assignment in spatial image steganography. IEEE Transactions on Information Forensics and Security, 9(8), 1264-1277.

[34] Luo, W., Huang, F., & Huang, J. (2010). Edge adaptive image steganography based on LSB matching revisited. IEEE Transactions on information forensics and security, 5(2), 201-214.

[35] Abd EL-Latif, A. A., Abd-El-Atty, B., & Venegas-Andraca, S. E. (2019). A novel image steganography technique based on quantum substitution boxes. Optics & Laser Technology, 116, 92-102.

[36] Tang, W., Li, B., Tan, S., Barni, M., & Huang, J. (2019). CNN-based adversarial embedding for image steganography. IEEE Transactions on Information Forensics and Security, 14(8), 2074-2087.

[37] Zhou, Z., Sun, H., Harit, R., Chen, X., & Sun, X. (2015). Coverless image steganography without embedding. In Cloud Computing and Security: First International Conference, ICCCS 2015, Nanjing, China, August 13-15, 2015. Revised Selected Papers 1 (pp. 123-132). Springer International Publishing.

[38] Cheddad, A., Condell, J., Curran, K., & Mc Kevitt, P. (2008, March). Biometric inspired digital image steganography. In 15th Annual IEEE International Conference and Workshop on the Engineering of Computer Based Systems (ecbs 2008) (pp. 159-168). IEEE.

[39] Liao, X., Yin, J., Guo, S., Li, X., & Sangaiah, A. K. (2018). Medical JPEG image steganography based on preserving inter-block dependencies.

[40] Zhang, K. A., Cuesta-Infante, A., Xu, L., & Veeramachaneni, K. (2019). SteganoGAN: High capacity image steganography with GANs. arXiv preprint arXiv:1901.03892.

[41] Valandar, M. Y., Ayubi, P., Barani, M. J., & Irani, B. Y. (2022). A chaotic video steganography technique for carrying different types of secret messages. Journal of Information Security and Applications, 66, 103160.

[42] Parvez, M. T., & Gutub, A. A. A. (2008, December). RGB intensity based variable-bits image steganography. In 2008 IEEE Asia-Pacific Services Computing Conference (pp. 1322-1327). IEEE.

[43] Acharya, U. D., & Kamath, P. R. (2013). A secure and high capacity image steganography technique. arXiv preprint arXiv:1304.3629.

[44] Xu, Y., Mou, C., Hu, Y., Xie, J., & Zhang, J. (2022). Robust invertible image steganography. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (pp. 7875-7884).

[45] Delina, B. (2008). Information hiding: A new approach in text steganography. In Proceedings of the International Conference on Applied Computer and Applied Computational Science, World Scientific and Engineering Academy and Society (WSEAS 2008) (pp. 689-695).

[46] Shirali-Shahreza, M. H., & Shirali-Shahreza, M. (2006, July). A new approach to Persian/Arabic text steganography. In 5th IEEE/ACIS International Conference on Computer and Information Science and 1st IEEE/ACIS International Workshop on Component-Based Software Engineering, Software Architecture and Reuse (ICIS-COMSAR'06) (pp. 310-315). IEEE.

[47] Shirali-Shahreza, M. H., & Shirali-Shahreza, M. (2007, September). Text steganography in chat. In 2007 3rd IEEE/IFIP International Conference in Central Asia on Internet (pp. 1-5). IEEE.

[48] Shirali-Shahreza, M. (2008, February). Text steganography by changing words spelling. In 2008 10th international conference on advanced communication technology (Vol. 3, pp. 1912-1913). IEEE.

[49] Wang, Z. H., Kieu, T. D., Chang, C. C., & Li, M. C. (2009, November). Emoticon-based text steganography in chat. In 2009 Asia-Pacific Conference on Computational Intelligence and Industrial Applications (PACIIA) (Vol. 2, pp. 457-460). IEEE.

[50] Dulera, S., Jinwala, D., & Dasgupta, A. (2012). Experimenting with the novel approaches in text steganography. arXiv preprint arXiv:1203.3644.

[51] Gupta, S., & Jain, R. (2015, December). An innovative method of Text Steganography. In 2015 Third International Conference on Image Information Processing (ICIIP) (pp. 60-64). IEEE.

[52] Luo, Y., Huang, Y., Li, F., & Chang, C. (2016). Text steganography based on

ci-poetry generation using Markov chain model. KSII Transactions on Internet and Information Systems (TIIS), 10(9), 4568-4584.

[53] Zamani, M., Manaf, A. B. A., Ahmad, R. B., Jaryani, F., Taherdoost, H., & Zeki, A. M. (2009, November). A secure audio steganography approach. In 2009 International Conference for Internet Technology and Secured Transactions, (ICITST) (pp. 1-6). IEEE.

[54] Asad, M., Gilani, J., & Khalid, A. (2011, July). An enhanced least significant bit modification technique for audio steganography. In International Conference on Computer Networks and Information Technology (pp. 143-147). IEEE.

[55] Delforouzi, A., & Pooyan, M. (2008). Adaptive digital audio steganography based on integer wavelet transform. Circuits, Systems & Signal Processing, 27(2), 247-259.

[56] Bhowal, K., Bhattacharyya, D., Jyoti Pal, A., & Kim, T. H. (2013). A GA based audio steganography with enhanced security. Telecommunication Systems, 52, 2197-2204.

[57] Yi, X., Yang, K., Zhao, X., Wang, Y., & Yu, H. (2019). AHCM: Adaptive Huffman code mapping for audio steganography based on psychoacoustic model. IEEE Transactions on Information Forensics and Security, 14(8), 2217-2231.

[58] Bhowal, K., Pal, A. J., Tomar, G. S., & Sarkar, P. P. (2010, November). Audio steganography using GA. In 2010 International Conference on Computational Intelligence and Communication Networks (pp. 449-453). IEEE.

[59] Hemeida, F., Alexan, W., & Mamdouh, S. (2019, October). Blowfish–secured audio steganography. In 2019 Novel Intelligent and Leading Emerging Sciences Conference (NILES) (Vol. 1, pp. 17-20). IEEE.