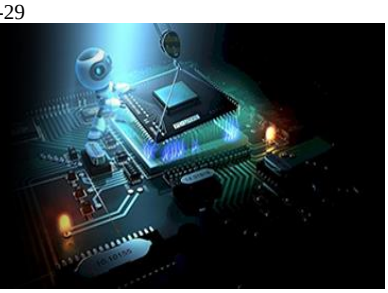
International Journal of Engineering in Computer Science



E-ISSN: 2663-3590
P-ISSN: 2663-3582
IJECS 2024; 6(1): 22-29
Received: 08-11-2023
Accepted: 13-12-2023

MC Basavaraja
Department of Electronics and Communication Engineering Sri Siddhartha Institute of Technology of Sri Siddhartha Academy of Higher Education, Tumakuru, Karnataka, India

Dr. Anitha Devi
M.D, Department of Electronics and Communication Engineering, Sri Siddhartha Institute of Technology of Sri Siddhartha Academy of Higher Education, Tumakuru, Karnataka, India

Corresponding Author:
MC Basavaraja
Department of Electronics and Communication Engineering Sri Siddhartha Institute of Technology of Sri Siddhartha Academy of Higher Education, Tumakuru, Karnataka, India

Review and Analysis on audio steganography techniques

MC Basavaraja and Dr. Anitha Devi

DOI: https://doi.org/10.33545/26633582.2024.v6.i1a.106

Abstract
The internet has become a crucial tool for modern society, allowing for instantaneous global contact and the sharing of vast amounts of information. Furthermore, we must take extra measures to ensure our safety while using the internet. When it comes to secure communication, steganography is a system that provides an improved secured approach. The Greek word steganos (meaning hidden or covered) is the root of the English word steganography. It hides the fact that we're trying to get in touch. Cryptography, on the other hand, provides a means through which the encrypted message can be deciphered. Steganography allows for not just non-repudiation but also confidentiality, authentication, and data integrity. Numerous studies on audio steganography exist. The purpose of steganalysis is to crack steganography and reveal hidden messages. Digital multimedia formats like audio, pictures, and video have become increasingly commonplace in the modern era, making them ideal for steganography. In order to determine if a suspicious communication contains a secret message, it is essential to be able to monitor this enormous multimedia as the user interacts with the outside world. Since there is a trade-off between capacity and invisibility, it is important to develop a strategy that maximises both features. The multi-objective evolutionary algorithm (MOEA) is a popular search tool for locating optimal solutions to the trade-off dilemma that arises in many different contexts. Using the MOEA Pareto dominance paradigm and the Non-dominated Sorting Genetic Algorithm-II (NSGA-II), this research proposed a novel strategy for optimising cover-audio selection in audio steganography. Based on inaudibility and storage capacity aspects, the proposed technique recommended cover audio to users. The sample difference formula was first developed to assess the size of the cover audio library. After that, NSGA-II was used to determine the most appropriate responses, this time factoring in the data provided by each chromosome. The new method additionally considered the fact that the trade-off resulted in the solution being chosen as the highest priority, whereas the previous method rated the same answer as low as position 71. The method improved the efficiency of the used audio steganography by optimising the cover audio chosen.

Keywords: Audio steganography, steganalysis, steganography, data hiding, information security

Introduction
Steganography is the study of concealing data in undetected ways by manipulating the values of data in seemingly unrelated media. Like encryption, steganography can be used to send messages in secret. The purpose of steganography, in contrast to cryptography, is not to guarantee the validity and integrity of the messages but rather to hide the existence of the secret. Using specialised techniques, steganography adds another layer of protection to encrypted data, making it impossible for unauthorised parties to discover the secret's presence. A novel architecture was given in this paper for the automatic eneration of low-weight audio steganography methods. Algorithms used in audio steganography conceal information within sounds designed to trick the human ear. Watermarking, copyright protection, and secret transmission are just a few of the many uses for audio steganography. There are currently three primary types of audio steganography techniques used today. The first is temporal domain approaches, which encode a secret message in binary using the Least Significant Bit (LSB) of individual sound samples.
The fields of steganography and steganalysis are crucial to the study of data concealment. Due to the simplicity of early steganography, steganalysis features had a modest dimension and required little computational effort.

Content adaptive steganographic techniques are studied to learn how to conceal information in less obvious places on a carrier by using distortion functions and the syndrome-trellis coding method. Traditional approaches rely heavily on human skill, and the majority of these strategies exploit their limitations in terms of capacity, security, and generalizability. Many sophisticated models have been applied to the fields of steganography and steganalysis since the advent of deep learning (Zou *et al*., 2019; Boroumand *et al*., 2018) [1, 2]. In recent studies, generative adversarial networks (GANs) have shown to compete favourably with other generative models when it comes to synthesis tasks. Signal creation and speech synthesis are two other tasks that GANs have been applied to. In this paper, we apply the concept of adversarial training to an algorithm for producing automatic audio steganography.

In audio steganography, distortion-free embedding is the goal, which sets it apart from most audio synthesis tasks. We introduce the idea of zero-sum game theory and propose an embedding model with three neural networks: An encoder to embed the secret message in the carrier; a decoder to extract the message; and a discriminator to identify the carriers with secret messages. The secret audio is masked by another type of sound in the embedding model. This training problem can be thought of as a type of binary classification. While the encoder is busy transforming carrier audio and the secret message into steganographic audio, the discriminator is busy learning how to better spot the existence of concealed information by analysing the encoder's flaws. All the networks are trained simultaneously using the datasets until the encoder can produce high-quality steganographic audio. We show that our method is useful by generating steganographic audio, which includes both secret audio and it's decoding to a carrier, as well as the less distorted secret audio, which indicates that it was more frequently heard than the distorted carrier. Based on the realisation that GAN has not previously been applied to the audio information concealing challenge, we present the first known solution that employs an adversarial framework to generate steganographic audio. Because it is less than 5 MB in size, the proposed model can be used in a wide range of IoT-enabled smart devices.

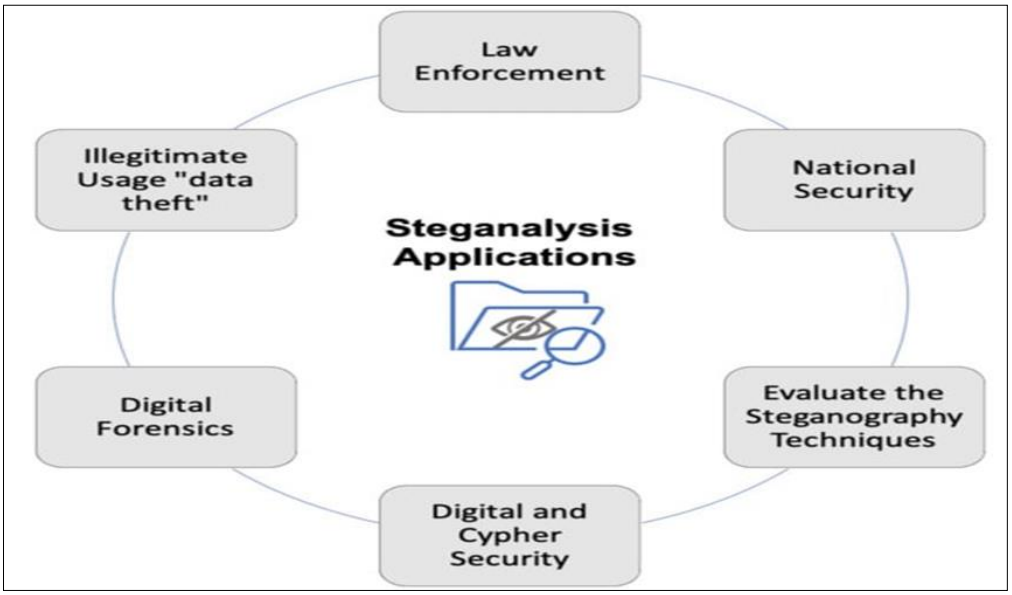


Fig 1: The applications of steganalysis

An alleged al-Qaeda member was arrested in Berlin using a steganographically encoded memory card in May of 2011. Over a hundred text files allegedly detailed future al-Qaeda assaults were found on the memory card, as reported by the German Federal Criminal Police. These documents were buried in a sex film. Researchers at Microsoft found a variant of the 'Alureon' virus that uses steganography to remain undetectable that same year. In October of 2018, a spam campaign in Japan used steganography to spread a banking malware [Trend Micro 2021]. The malicious code was cloaked in a seemingly innocuous media so as to evade signature-based detection.

Given the history of illegal and potentially harmful steganography applications, academics have begun putting significant time and energy into steganalysis in an effort to identify and prevent future malevolent applications (Xiang, L.; 2020) [5]. The process of deciphering a stego-file is known as steganalysis. These days, steganography is a tricky process, especially if the hidden message is encrypted (Karampidis K, 2018) [6]. Many fields rely heavily on steganalysis, including policing, digital forensics, and national security. Steganalysis could be used to test the efficacy of suggested steganography methods in the academic and research community. Steganalysis (and its many uses) are seen in Fig.1.

Audio Steganography Background

Steganography is a form of intelligent data concealing in which sensitive information is concealed behind a seemingly innocuous cover medium, rendering both the cover medium and its contents invisible to a would-be thief or attacker (Kadhim IJ, 2019) [7]. Even if the transmission is picked up, the message will be gibberish. Both cryptography and steganography are employed in the digital realm with the intention of storing and safeguarding the hidden message from prying eyes (Hussain, 2018) [8].

These methods work well in tandem or on their own. Combining them also yields outstanding results, but should be done in stages to guarantee maximum safety. Text, images, DNA, networks, music, and video are just some of

the many data types that can be hidden with digital steganography today (Taha, 2020) [9]. Given this breadth of steganography, it's easy to see why current steganography is crucial for security and integrity, especially in the context of the internet. Regulations and restrictions imposed by authorities have weakened the security of cryptosystems in the online community. For this reason, we employ steganography, a method that encrypts the given message so that it can only be read by the intended recipient who possesses the relevant decryption key from the host medium. Image steganography is still widely used despite the rise of other digital steganographic techniques (Saini, 2021) [10] because to its superior capacity to hide hidden data in the cover media via undetectable effects.

Properties of Steganography

The increasing popularity of digital steganography has shown the importance of thorough testing and evaluation. Existing steganography evaluation techniques can be classified according to their detectability, complexity, payload capacity, resilience, and undetectability/security. Since picture steganography is the most widely deployed kind of digital steganography [Wahab, 2021], this section will focus on the evaluation criteria unique to this subset of digital steganography.

Imperceptibility: After information has been hidden in an image, the image's quality declines significantly. Conventional testing procedures that can estimate or measure the visual modification levels must be utilised to determine if a steganographic technology is actually undetectable to the human eye. There are a number of metrics developed to assess the visual quality of digital steganography, including mean squared error, root mean squared error, PSNR, WPSNR, Q, SIMM, NCC, and IF.

Embedding capacity (EC): This value is the maximum number of secret bits that can be contained within a single pixel of cover material. A good cover media is one that maintains imperceptibility and other evaluation measures while having a high EC. Capacity embedding, also known as payload embedding, is a type of data compression.

Security/undetectability: This is another important precaution to take while working with digital steganography, as all steganographic methods could be breached by steganalysis detection attacks. This is because adversaries are always seeking for new ways to reveal the presence of concealed bits in the stegoimage. Future recovery of hidden bits from cover objects [ALRikabi, H. T., 2021] will rely heavily on steganalysis approaches like (i) visual steganalysis, (ii) standard steganalysis, and (iii) non-standard steganalysis.

Literature Review

Audio steganalysis is a technique used to detect changes to a signal caused by steganography. Data can be embedded in either a spatial or a "time" or "temporal" domain by manipulating the least significant bit (LSB) of a data sample in an audio file or by modulating various aspects of the signal in the transform domain. In addition, (Tabares-Soto, 2020) [13] categorises audio steganalysis into compressed (e.g., MP3 and AAC) and non-compressed (e.g., WAV and Ogg) steganalysis approaches. In order to uncover MP3Stego steganography, a target steganalysis method was presented, which takes into account the compressed file types. Audio cover is quantized modified discrete cosine transformed (QMDCT), and the authors found that MP3Stego changes the QMDCT coefficients during compression. The correlations between neighbouring QMDCTs are altered as a result. Therefore, QMDCT correlations are characterised by Markov features, which are generated from cover and stego audio. These features are then utilised to train a support vector machine classifier after going through a number of pre-processing steps. Experiments show that even with a low embedding rate, the suggested method provides precise detection results.

Wang *et al*. 2020 [14] present another Mp3 steganalysis method, in which the steganographic features are extracted by computing the QMDCT coefficient matrix of the MP3. Their method was made more sensitive to noise signals by employing a wealth of high-pass filtering. The authors state that changing a single QMDCT coefficient alters only a single Huffman codeword. Because of this, they proposed a correlations measure module to identify shifts in the QMDCT coefficients matrix in three distinct ways: Point-by-point, two-by-two blocks, and four-by-four blocks. An empirical threshold was used to narrow down the pool of potential traits and ultimately choose the best one. The ensemble classifier was taught to perform the classification process.

The linear prediction technique proposed by Han *et al*. 2018 [15] involves extracting linear prediction LP characteristics from a segmented audio stream. The tests proved that the LP can distinguish between the cover and the stego. In order to extract the LP coefficients, LP residual, LP spectrum, and LP cepstrum coefficients, we make use of both the time domain and the frequency domain. In order to train the SVM classifier, features were retrieved from cover- and stego-signals. Experiments with several different ratios of embedding are tried out and compared to other steganographic methods. When compared to well-known and cutting-edge steganography methods, where accuracy levels of 96% or higher are typically reached, the results demonstrated the efficacy of the proposed strategies.

Ren *et al*. (2019) [16] suggested a universal steganalysis method that utilises a ResNet to extract features. Input to the neural network was the audio signal's spectrogram, and the network was given the moniker "Spectrogram Deep Residual Network" (S-ResNet). The spectrogram, as illustrated in Figure 2, can represent the energy information of distinct frequency bands throughout time and provides useful time-frequency information in the audio signal. This is why the authors tried using it to record relative features created by audio steganography. Between the batch normalisation and ReLU layers in S-ResNet's architecture are 31 convolutional layers, each designed to speed up the learning process or help the network understand more complicated patterns. After each set of convolutional layers, the residual function is computed using a residual unit. Two average pooling layers are implemented after every five residual blocks to shrink the data set. The final layer used to generate the feature vector is a global average pooling layer. After a reliable model has been built with S-ResNe, it is fed into a support vector machine (SVM) for further training and binary classification. It turns out that AAC and MP3 are just as good as each other when it comes to detection; on average, they detect with an accuracy of 94.98% and 99.93%, respectively.

A histogram of pixel structure elements is used in the statistical model presented by Lu *et al*. (2019) [17]. In

contrast to colour and grayscale images, which contain a range of values from 0 to 1, this approach is designed to extract steganography from binary images. Each structure element (SE) in an image has its own histogram, and as can be seen in Fig. 3, a single large SE can include many nearby little SEs. Then, the bins of SEs with the highest likelihood of flappable pixels are selected as a feature set using an empirical threshold. To uncover the stego-image, the SVM classifier is employed. The authors also make publicly accessible datasets for binary images, which they refer to as DBLST. The proposed strategy outperforms state-of-the-art methods in detecting various stego images, as shown by experiments on the publicly available DBLST and BIVC datasets.

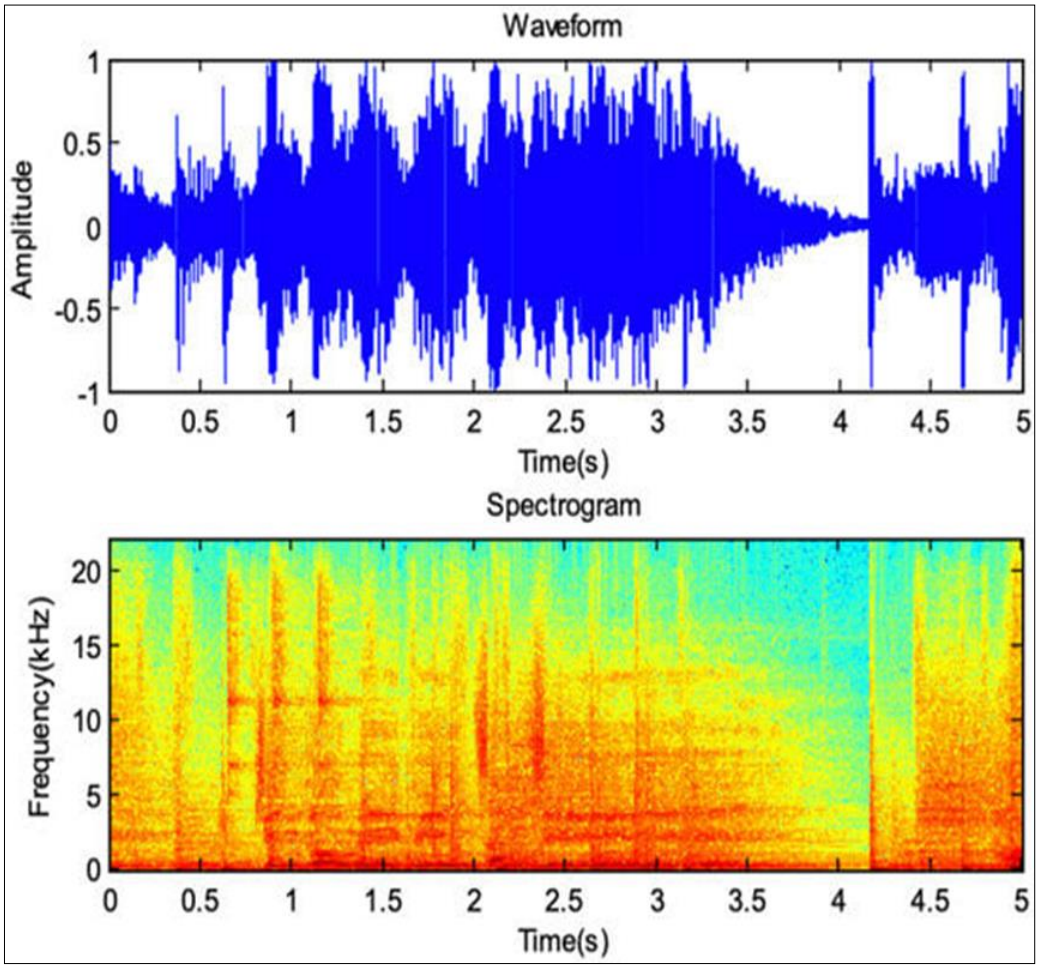


Fig 2: A depiction of an audio clip in wave form and spectrogram

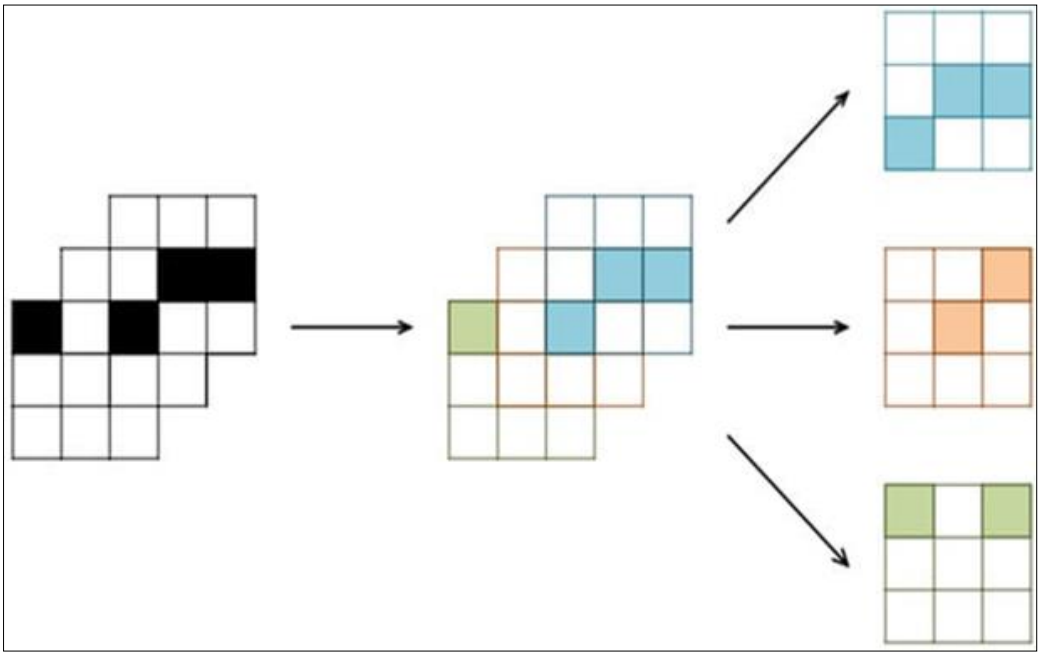


Fig 3: The union of many tiny SEs in the vicinity constitutes a huge SE

Laimeche *et al*. 2018 [18] presented the universal steganalysis method, which makes use of Zipf's law to extract features from the wavelet transform. The three-step procedure at the heart of Zipf's law for visual representation. The mask size for the pattern count must be established initially. In the second stage, significant wavelet coefficients are identified in order to reduce the total number of patterns, which results in a more even distribution of pattern frequencies. Zipf curves are generated in the third step to graphically illustrate the pattern frequency and the number of pattern axes. It is possible to build a Zipf curve and then get information about it, such as its AUC, inflection point, and Subband Auto-Similarity Metric. The stego images are recognised by a random forest classifier that was trained on the UCID dataset.

In their recent paper, Guttikonda and Sridevi 2019 [19] present a novel steganalysis technique that prioritises efficiency over other factors, such as computation and time. The Walsh Hadamard Transform with a Coefficient and a Grey Level Co-occurrence Matrix are used to extract features from the transform and spatial domains, respectively. Pine Growth Optimisation was used to choose the most important characteristics and reduce the dimensionality of the data. The following stage is to use the specified features to train a Cross Integrated Machine Learning classifier to decide how to distinguish between the cover- and stego-images. Detection accuracy and execution time were both improved using the proposed method compared to the established Multi-SVM method, as demonstrated by the experimental findings.

Wu *et al*. 2018 [20] employ extremely deep learning and automated feature extraction in their study. A new type of Convolutional Neural Network (CNN) model, called a Deep Residual learning Network (DRN), is created for the purpose of image steganalysis. The researchers showed that a very deep neural network with lots of layers may accurately reflect complex statistical parameters used to differentiate stego-images. The key idea behind their method is to provide the network with noise components of the image rather than the true image in order to get it to consider the weak signal produced by data embedding. Then, we train DRN to identify the most salient features of cover- and stego-images. The binary classification was performed using a fully connected layer and a softmax classifier. As demonstrated by experimental findings on the BOSSbase dataset, the suggested method outperforms alternatives based on deep neural networks.

Wang *et al*. 2020 [14] suggest another deep neural network-based method for extracting characteristics across many domains. To get started, we model two popular steganalysis methods: The spatial rich model (SRM) for detecting steganography features in the spatial domain and the DCT residual for doing the same in the transform domain. The linear and nonlinear SRM characteristics are then sent into the CNN layer so that the general features can be extracted. Finally, stego and cover photos are categorised using the completely linked layer. Experiments showed that taking into account nonlinear feature extraction and feature extraction from several domains improved detection accuracy by 0.3-6 percent and 2.3 percent, respectively.

Audio steganography with intensified security and hiding capacity

In order to communicate rapidly and safely, the amount of digital data transmitted via the internet is growing steadily. People need to be able to communicate securely online, which makes internet security an extremely important topic. In order to feel safe when surfing the web, people resort to a wide variety of methods. In the midst of so many options, cryptography stands out. Steganography, on the other hand, successfully hides information. However, cryptography is not able to hide the existence of sensitive information. Multimedia files of all kinds are used for communication among people. Steganography is the most widely used method for secretly embedding information within a moving or still digital media file. It's an important part of how we convey and receive information. The privacy of the conversation is protected as well. Different steganographic algorithms can be used to hide data in audio signals in that region. Karampidis, 2018 [6] Steganography and its analysis are used to conceal messages for marriage security.

One method proposed by Alhusban 2017 to hide its embedding is to insert Kashida between letters (whether they be pointed or unpointed). In order to embed Kashida, we consult two tables that show us how to combine the four secret bits (00, 01, 10, and 11) in four different ways. Cover text first halves must conform to the rules outlined in the first table. For the second half of each word, follow the guidelines laid out in the second table. But since inserting Kashida between disconnected characters is required for this method's secret bit concealing, most unconnected characters are rendered useless. In addition, many characters are missed because their design precludes them from matching a scenario for Kashida insertion, which is why this method is so inefficient. In this case, the payload is 2%.

Anuradha *et al*. 2021 [21] developed network steganography by analysing the UDP packet flow and other characteristics of data file storage to create a technique that relied on the UDP packet length. The sender initiates the transmission of some data packets using this method. The secret data is sent along with the packet's length because of the randomness of its arrival. The router then forwards data from many IP addresses. It is also possible to increase the secrecy of data transfer by introducing some bogus packets to throw off the monitor. As a result of its superiority in simulating everyday traffic and its ability to circumvent flaws in existing solutions, random coding technology is used for this purpose.

To increase channel capacity without degrading VoIP call quality, Sabine and Wojciech 2021 [22] created the StegVAD algorithm. This technique changes a VoIP stream that has been activated by speech activity detection into one that has not been triggered by voice activity detection. During the subsequent silence, the encoder will increment the timestamp and sequence number in order to produce bogus RTP packets. While the system was able to increase channel capacity, the robustness and anti-detection performance were subpar.

In their presentation of a hash-based system for data concealing, Deepika and Saravanan 2021 [23] explained how the "voice stream is first obtained from the UDP protocol before constructing the hash array from the frame data." Each subsequent frame requires a fresh update to the hash array. Once the sensitive data has been filtered, the appropriate bit position is selected in accordance with the hash function. When the embedding process is complete, the value of the hash array is 0. The secret message is then extracted by the receiver using the flag value from the hash

array, which was included in the VoIP frame along with the audio samples. When tested for detectability, computational complexity, and sender and receiver speech quality, the method fared well. Issues arise due to the hash array's inefficient use of available bandwidth during VoIP calls.

Audio steganography using multi-objective evolutionary algorithm

The purpose of audio steganography is to covertly communicate information by hiding it within an audio file (Setiadi, 2022) [24]. Various methods of audio steganography have been proposed in the past, including low bit embedding, parity coding, echo concealment, phase coding, spread spectrum, and the wavelet domain. Capacity, imperceptibility, and robustness are three requirements for an effective audio steganography technique.

The capacity of a covert communication is the quantity of information that can be transmitted without being detected, whereas the robustness of a covert message is its resistance to intrusion. Finally, imperceptibility refers to the degree to which secret information can be embedded in an audio stream without being picked up by the human ear. First, there is a tradeoff between inaudibility and storage capacity. Second, there is a tradeoff between storage capacity and robustness. Finally, there is a tradeoff between robustness and inaudibility.

If capacity is raised, imperceptibility decreases and noise becomes more noticeable, while the opposite is true if imperceptibility is decreased. Similarly, there is a strong negative correlation between increasing capacity and increasing robustness. Finally, there is a trade-off between stealth and durability, wherein the former suffers as the latter improves.

In order to develop a novel audio steganography methodology, it is usual practise to first analyse existing methods, then propose a solution, and last evaluate the effectiveness of the proposed approach. The quality of the cover audio is often disregarded despite the fact that researchers have made numerous enhancements to the audio steganography procedure. The user's task is to pick a song at random and type in a coded message without taking any of these considerations into account. Careful selection of the cover audio is essential for successful audio steganography. Careless selection of cover audio for a stego file (cover audio encoded with a secret message) can reduce the file's storage capacity or make the message undetectable. Since this is a quality issue, the current strategy involves emphasising either the capacity or imperceptibility of the audio steganography technology. However, it is clear from a survey of the available literature that studies focusing on the best way to resolve this particular trade-off are still lacking. Because increasing either capacity or invisibility reduces the other, balancing these two requirements is a multiobjective optimisation problem (MOP). Multi-objective optimisation problems (MOPs) are typically solvable by use of MOEAs.

Author	Capacity	SNR	Output
Mazdak Zamani 1, Azizah A. Manaf 2019 [25]	Higher capacity and robustness	-	Efficiently hide secret data
Padmashree G, Venugopala PS 2022 [26]	-	Less than zero	Efficiently hide secret data
Nedeljko Cvejic, Tapio Seppänen 2018 [27]	-	-	Compress the stego audio signal and encrypt the message.
Mazhar B. Tayel, Ahmed Gamal Abdalatife 2020 [28]	-	-	Hides sensitive information and uses PSNR as a quality metric for steganographic audio signals. In addition to a better PSNR value, the method's output also features significantly lower MSE values.
Orora Tasnim Nisha 2023 [29]	Obtain high hiding capacity	SNR value is positive which is near to 1.	Successfully conceal sensitive information within an audio transmission while preserving its quality. With a high SNR value and a sizable hiding capacity, the output provides a safe way.

Fig 4: Comparison of capacity, snr and output

A. LSB

The original proposal for low-bit embedding (later popularised as LSB) was made. Many academics have worked to boost the method's capacity, stealth, and durability since then. Covert audio and hidden messages are both encoded in a stream of binary value using the LSB embedding method. Next, the secret message's bit sequence is substituted for the LSBs of the audio samples.

LSB can be broken down into two distinct types: Tabares-Soto *et al.* (2019) [31] distinguish between direct embedding and selective embedding. In order to embed data into the initial sample without skipping any following audio samples, direct LSB embedding must be used. In contrast, the selective LSB embedding approach provided by Alsabhany *et al.* (2020) [30] only embeds the data until a positive outcome is achieved by selecting only samples that pass the embedding requirement.

B. MOEA

MOEA is a well-known search strategy due to its applicability in both theoretical and practical settings. Its use has expanded over the past two decades to include fields including engineering, security, and the military. Additionally, the method is straightforward, and no derivative data is necessary. Non-dominated Sorting Genetic Algorithm (NSGA) and its successor, NSGA-II, are just two of the many MOEAs that have been created in recent years with the express purpose of optimising practical problems.

It was in 1994 when NSGA was first presented, by Siinivas and Deb (1994) [32]. This algorithm ranks the population by eliminating the currently non-dominated subgroup from consideration and giving it a rating of zero (0). Another non-dominated subset is identified from the remaining population and given rank one (1) before being eliminated from further evaluation. This continues until every member of the population has been assigned a ranking.

Because of its benefits, MOEA is also used to the field of steganography in order to enhance its qualities in terms of storage capacity, stealth, and durability. Recently, used MOEA and steganography to conceal images, using NSGA to optimise the stego file. The findings suggested that the discrete wavelet transform might be enhanced with the use

of singular value decomposition (SVD) and non-dominated sorting genetic algorithm (NSGA). The secret message (image)'s singular values were replaced with those extracted from the high-frequency band using singular value decomposition (SVD). Boosting the image's invisibility feature raised both its embedding capacity and image quality. As a result, the search efficiency of MOEA can be improved by include the ability to locate optimum cover audio.

Conclusion

This review study covered the fundamentals of steganography, steganalysis, and their categorization. In addition, a thorough study of the most recent studies on steganalysis methods for audio, image, and video formats was provided. There are benefits and drawbacks to each of the studied strategies. According to the cited sources, the security and reliability of an image steganography scheme can be improved by combining spatial and frequency domains in the design of the scheme, by using a new encryption method to prepare the secret text, and by selecting image pixels in a random fashion. We looked at the newest steganographic approaches and compared how they embed and how easily they can be extracted from data to the majority of already used methods. A robust and efficient system that can achieve a high payload, data embedding, and data reconstruction without significant impact on data quality and data security is needed in light of the pros and limitations of each of the evaluated methodologies. Using the NSGA-II method and bit-level adaptive LSB embedding, this study showed that high capacity and imperceptibility may be attained by optimising the trade-off between capacity and imperceptibility. The experimental outcomes validated the effectiveness of the proposed strategy in optimising cover and bps selection. It also triumphed over the preceding selection process, which relied on a single criterion for making the final call. The proposed generic architecture can also serve as the basis for cover audio selection, with the MOEA and audio steganography components being modified as needed for the specific goal at hand.

References

1. Zou Y, *et al*. Research on image steganography analysis based on deep learning. J Vis. Commun. Image Represent; c2019.
2. Boroumand M, *et al*. Deep residual network for steganalysis of digital images. IEEE Trans. Inf. Forensics Secur; c2018.
3. CNN. Documents Reveal al Qaeda's Plans for Seizing Cruise Ships, Carnage in Europe. 2012. Available from: https://edition.cnn.com/2012/04/30/world/al-qaeda-documents-future/index.html Accessed 5 October 2021.
4. Trend Micro. Spam Campaign Targets Japan, Uses Steganography to Deliver the BEBLOH Banking Trojan. 2018. Available from: https://www.trendmicro.com/vinfo/nz/security/news/cybercrime-and-digital-threats/spam-campaign-targets-japan-uses-steganography-to-deliver-the-bebloh-banking-trojan Accessed 5 October 2021.
5. Xiang L, Guo G, Yu J, Sheng VS, Yang P. A convolutional neural network-based linguistic steganalysis for synonym substitution steganography. Math. Biosci. Eng. 2020;17:1041-1058.
6. Karampidis K, Kavallieratou E, Papadourakis G. A review of image steganalysis techniques for digital forensics. J Inf. Secur. Appl. 2018;40:217-235.
7. Kadhim IJ, Premaratne P, Vial PJ, Halloran B. Comprehensive survey of image steganography: Techniques, Evaluations, and trends in future research. Neurocomputing. 2019;335:299-326.
8. Hussain M, *et al*. Image steganography in spatial domain: A survey. Signal Processing: Image Communication. 2018;65:46-66.
9. Taha MS, *et al*. Information Hiding: A Tools for Securing Biometric Information. Technology Reports of Kansai University. 2020;62(04):1383-1394.
10. Saini R, Joshi K, Nandal R. An Adapted approach of image steganography using pixel mutation and bit augmentation. In: Smart Computing Techniques and Applications. Springer, Singapore; c2021. p. 217-224.
11. Wahab OFA, *et al*. Hiding data using efficient combination of RSA Cryptography, and Compression Steganography Techniques. IEEE Access. 2021;9:31805-31815.
12. ALRikabi HT, Hazim HT. Enhanced data security of communication system using combined encryption and steganography. Int. J Interact. Mobile Technol. 2021;15(16).
13. Tabares-Soto R, *et al*. Digital media steganalysis. In: Digital Media Steganography. Elsevier, Amsterdam, The Netherlands; c2020. p. 259-293.
14. Wang Y, Yi X, Zhao X. MP3 steganalysis based on joint point-wise and block-wise correlations. Inf. Sci. 2020;512:1118-1133.
15. Han C, *et al*. A new audio steganalysis method based on linear prediction. Multimed. Tools Appl. 2018;77:15431-15455.
16. Ren Y, *et al*. Spec-resnet: A general audio steganalysis scheme based on deep residual network of spectrogram. ARXIV. 2019;ARXIV:1901.06838.
17. Lu W, *et al*. Binary image steganalysis based on histogram of structuring elements. IEEE Trans. Circuits Syst. Video Technol.. 2019;30:3081-3094.
18. Laimeche L, Merouani H, Mazouzi S. A new feature extraction scheme in wavelet transform for stego image classification. Evol. Syst. 2018;9:181-194.
19. Guttikonda JB, Sridevi R. A new steganalysis approach with an efficient feature selection and classification algorithms for identifying the stego images. Multimed. Tools Appl. 2019;78:21113-21131.
20. Wu S, Zhong S, Liu Y. Deep residual learning for image steganalysis. Multimed. Tools Appl. 2018;77:10437-10453.
21. Anuradha M, Jayasankar T, Prakash NB, Sikkandar MY, Hemalakshmi GR, Bharatiraja C, *et al*. IoT enabled cancer prediction system to enhance the authentication and security using cloud computing. Microprocessors and Microsystems. 2021 Feb 1;80:103301.
22. Deng L, Wojciech L, Gascoigne NR, Peng G, Tan KS. New insights into the interactions between Blastocystis, the gut microbiota, and host immunity. PLOS pathogens. 2021 Feb 25;17(2):e1009253.
23. Deepika S, Rong SZ. Low-cost draw-on electronics: investigation of pen-substrate interaction. In IRC-SET 2020: Proceedings of the 6th IRC Conference on Science, Engineering and Technology, July 2020,

Singapore, Springer Singapore; c2021. p. 307-316.
24. Simanjuntak MB, Suseno M, Setiadi S, Lustyantie N, Barus IR. Integration of curricula (curriculum 2013 and Cambridge curriculum for junior high school level in three subjects) in pandemic situation. Ideas: Journal Pendidikan, Sosial, Dan Budaya. 2022 Feb 24;8(1):77-86.
25. Nilashi M, Samad S, Manaf AA, Ahmadi H, Rashid TA, Munshi A, *et al*. Factors influencing medical tourism adoption in Malaysia: A Dematel-Fuzzy Topsis approach. Computers & Industrial Engineering. 2019 Nov 1;137:106005.
26. Gutub A. Regulating watermarking semi-authentication of multimedia audio via counting-based secret sharing. Pamukkale Üniversitesi Mühendislik Bilimleri Dergisi. 2022 Apr 4;28(2):324-32.
27. Xu J, Cheng L. Objective evaluation method of fusion image quality based on the completed local binary pattern. Journal of Engineering Science & Technology Review. 2018 May 1;11(3).
28. Nisha OT, Hossain MS, Rahman M. Audio steganography with intensified security and hiding capacity (Doctoral dissertation, Hajee Mohammad Danesh Science and Technology University).
29. Nisha OT, Hossain MS, Rahman M. Audio Steganography with Intensified Security and Hiding Capacity (Doctoral dissertation, Hajee Mohammad Danesh Science and Technology University).
30. AlSabhany AA, Ali AH, Ridzuan F, Azni AH, Mokhtar MR. Digital audio steganography: Systematic review, classification, and analysis of the current state of the art. Computer Science Review. 2020 Nov 1;38:100316.
31. Arias OS, Isaza G, Guyot R, Soto TR. A systematic review of the application of machine learning in the detection and classification of transposable elements. PeerJ. 2019 Dec 18;7:e8311.
32. Srinivas N, Deb K. Muiltiobjective optimization using non-dominated sorting in genetic algorithms. Evolutionary Computation. 1994 Sep;2(3):221-48.