[1] Isaac Atta Senior Ampofo
[2] Peter Jorobon
[3] Ebenezer Takyi
[4] Isaac Atta Junior Ampofo, Beatrice Ampofo
[5] Charles Yeboah

Critical Review of Video, Audio, Image and Text Steganalysis Technique for Digital Forensics

Abstract: **-** In terms of security systems and digital forensics, steganography and steganalysis are relatively young fields of study, but they have advanced significantly over the past 20 years. In any field of human endeavor, it is necessary to periodically pause and assess the discipline state for what has been accomplished thus far. Steganography seeks to conceal messages, but steganography analysis seeks to either find them or, more importantly, recover the data they contain. Steganography and steganananalysis piqued the interest of many people, particularly law enforcement. Steganography is often used by cybercriminals and even terrorists to avoid being apprehended while in possession of encrypted incriminating evidence, even though cryptography is prohibited or restricted in many countries. A systematic strategy was used to find pertinent studies on video, audio, image, and text steganography in the Web of Science (WOS) All Database and the Scopus database. In Scopus and the Web of Science (WOS), all database search phrases were entered with the language set to English. The research presented software tools and techniques for text steganalysis, which make it simple to find concealed information in picture, audio, and video steganalysis. Future directions for the steganalysis technique for text, audio, video, and image steganography were highlighted in the paper.

Keywords: steganalysis technique, steganography, machine learning, deep learning.

I. INTRODUCTION

Since digital communication has seen such rapid development, secure communication has become a fundamental requirement in the modern digital world. Information is cloaked in a cover item in the practice of steganography, a form of covert communication [1]. Since the invention of the computer, there are now more ways and places to hide sensitive information [2]. For clandestine communication utilizing their mobile phones or own equipment with a connection to the internet, the ordinary person can now easily access and use steganography. Steganography is one method for secure communication; others include watermarking and cryptography [3]. The advantage of steganography over encryption and watermarking, however, is that after embedding, the steganography media seems to be identical to the cover media (in which data is buried) [4]. Combining steganography and cryptography can effectively create a concealed communication method [5]. Steganography is required for secure communication in a variety of settings, including banking, the military, and even by regular people, as detailed in this article's applications section [6]. Steganography's popularity can be attributed to both its ethical uses and some less ethical ones, such as the inclusion of viruses, spam, and dangerous links into data by cybercriminals [7]. Even terrorists have employed steganography for their nefarious purposes and carnage. As a result, individuals from all fields have become interested in steganography and steganography over the last ten years [8]. For the benefit of those who are interested in this field of study, researchers, and scientists, the writers have provided a critical evaluation of steganalysis.

Hackers frequently attempt to circumvent the security of communication channels (such as SMS, network protocols, etc.) to access private information while data is being transmitted [9]. As a result, there is an increasing need for multimedia security studies and intelligence that cover covert communication, which is essentially data concealment rather than just encryption [10], [11]. Text concealing, also known as data hiding or information hiding in digital texts, has received a lot of attention recently because of its widespread use and potential uses in the network communication and cybersecurity industries [12]-[14]. Text concealment is the practice of incorporating secret data through supportable technology such as SMS, network protocols, and so on, or a cover text, so that the existence of

[1] University of Liverpool, Brownlow Hill, Liverpool, L69 7ZX, United Kingdom. ampofoisaac10@yahoo.com
[2] Faculty of Science, University of Energy and Natural Resources. Jorobonpeter2000@gmail.com
[3] Faculty of Technology, Art and Design (TKD), Oslomet - Oslo Metropolitan University, Oslo, Norway. ebenfocus1@gmail.com
[4] University of Liverpool, Brownlow Hill, Liverpool, L69 7ZX, United Kingdom. ampofoatta159@gmail.com
[5] Faculty of Science, University of Cape Coast, Ghana. yebochar19@yahoo.com

the data is obscured or untraceable for casual viewers or adversaries [15], [16]. It is extensively regarded as an appealing method to enhance traditional encryption algorithms' usage in the multimedia security realm by blending a cover text file or message with a hidden message or watermark to safeguard private information. According to Song et al. [17], a 2-D Gabor wavelet's Shannon entropy can be used as a feature in an image steganography approach for JPEG images. The benefit is the ability for joint localization in experiments and the spatial domain; primarily, the JPEG picture was transformed into the spatial domain. Sheng et al. [18] introduced a video steganography method for altering HEVC intra-prediction mode to identify secret message embedding. The authors used numerous prediction unit sizes for their trials, including 4 x 4, 8 x 8, 16 x 16, 32 x 32, and 64 x 64. A useful feature set for the SVM classifier is the change rate between the prediction unit's prediction rate before and after recompression. While Li et al. [19] and Chandramouli and Subbalakshmi [20] provide an outdated review of steganalysis, Nissar and Mir [21] and Chanu et al. [22] suggest a distinct taxonomy of steganalysis that is particular and statistical. While Luo et al. [23] only discuss methods for universal (blind) detection for picture steganography, Pal and Dubey [24] only discuss steganography techniques suited to jpeg images. The steganography of digital media is crucial since these are the most common carrier files that will be examined. This includes video, audio, text, and image files. This review concentrates on the structural analysis of digital video, text, audio, and image as a result. The following subsection focuses on the survey's main contributions.

II. Literature Review

Numerous articles have put forth numerous implementation strategies for the detection of steganography in photos. Steganalysis can be accomplished using simple detection techniques, deep learning, or even machine learning. You et al. [25] adopted a CNN-based Siamese architecture that reveals the results of classification based on the relations between various image sub-regions' sounds. BOSSbase 1.01 and ALASKA #2 were used in the tests to verify the network. The suggested model has strong transferability across a range of image sizes. The approach reported by Boroumand et al. [26] offers enhanced accuracy for both spatial-domain steganography and blind picture steganography in JPEG. To avoid repressing the stego-signal, pooling is turned off in the detector applied to compute residual noise in this case. By providing the channel selection as a second channel, performance can be enhanced. This method searches for anomalies in picture noise patterns to locate locally modified regions. Mustafa et al. [27] proposed a new CNN approach called IGNCNN (Improved Gaussian Convolutional Neural Network) to detect steganography in photos with low payloads. To reduce the cost of the detection mistake, the pre-processing model uses a high-pass filter with a predetermined number of coefficients. This significantly increased accuracy in blind picture steganography compared to traditional CNN-based systems. The YeNet architecture has been enhanced by Fuji-Tsang and Fridrich [28] to recognize spatial steganography. The system modifies the payload in response to image size, utilizing the square root law for persistent detectability to efficiently analyze photos of various sizes. Lower detection errors have been noted as image size and resolution have increased. A successful and accurate size-independent detector is the study's final product.

An efficient image steganography technique for concealing sensitive data in digital photos was presented by Rehman et al. [29]. The proposed approach raised the cover picture's bit planes from 8-bit planes to 12-bit planes by using the Fibonacci number decomposition. As a result, the suggested method by Rehman et al. [29] created high-quality stego images and had a high embedding capacity (i.e., according to PSNR values). By breaking down the pixels in the image cover into a number sequence of Fibonacci, a high rate of embedding is achieved. However, the criterion of Zeckendorf was likewise used to obtain a special sequence of Fibonacci before embedding the secret message. With regards to stego image quality and secret data concealment, the suggested method by Rehman et al. [29] was assessed and contrasted with various earlier, widely used strategies. The findings show that the algorithm proposed did exceptionally well. It is likewise promising that the stego picture's aesthetic appearance blends seamlessly with the appropriate cover image as the capacity of the hidden data is raised. Rehman et al. [29] concluded that our method has the capability to produce stereo high-quality images and offer greater security compared to other ways through the experimental findings of the suggested system. Additionally, the suggested method is practical for steganography applications because it is straightforward and efficient. Rehman et al. [29] wants to expand the hidden data (payload) of the suggested approach in a subsequent study. The emphasis will also be on improving the method's effectiveness using metaheuristic optimization approaches.

The first research on image steganography was put forth by Chandramouli et al. [30] and Johnson and Jajodia [31] in the late twentieth century. Image steganalysis has progressed from manual feature extraction and visual steganalysis to feature automatic extraction and deep learning. Researchers initially looked for a pattern or signature

to identify famous techniques of steganography [31], but this approach has only a few practical uses. Robust steganography analysis approaches became more important as steganography techniques developed and expanded. Many statistical analysis approaches have been developed to extract statistical traits to replicate imperceptible variations in the digital medium. An illustration of this is the blind statistical steganography analysis method presented by Chaeikar et al. [32] for identifying the image flipping steganography of the Least Significant Bit (LSB). The authors discovered that when the data is embedded, the pixel's natural color harmony is impacted. To identify the presence of the hidden message, a feature of statistics that evaluates color correlation is derived from the pixel image. First, the pixels were divided into three groups based on how closely their colors matched those of their immediate surroundings, and the degree of suspicion associated with each group was determined using the standard deviation and mean. This results in a dataset that may be applied to train SVM to gauge and recognize the length of an embedded message.

Videos are now widely used thanks to the internet's speed. Detecting these modifications is crucial since videos might be edited to transmit covert messages [32]. The modifications caused by the encoded message were initially detected directly using steganography techniques for photos. However, because there isn't much variation between the video's subsequent frames, these methods didn't yield satisfactory outcomes. The methods for steganography of images and those for steganography of videos are vastly different. The inter-frame methods-based level and the motion methods-based vector field are the two basic techniques for finding hidden messages in digital video. These techniques have been used for videos using the AVC/H.264 standard as well as the more recent HEVC standard. Taking advantage of the benefits of content variation, Wang et al. [33] proposed a vector-based steganalytical motion technique. Each subclass of the video has frames with comparable intensities. Following that, the improved MVRBR (Motion Vector Reversion-Based Steganalysis Revisited) and NPELO (Near-Perfect Estimation for Local Optimality) features from all classes were extracted and fed into an SVM independent classifier [34]. Depending on how intense the frames were, different weights were assigned to the separate classifiers; the classifier for the high-intensity class was given a higher weight. The combined classifiers also determine whether the video is stereo or surround. Each of the 100 YUV sequences in the used database has 150–300 frames at 30 frames per second in CIF format. The x264 tool handled the database for the H.264/AVC standard.

Text steganalysis, as opposed to steganography of text (or watermarking), is the science and technique of estimating if a particular file or text message contains hidden information and, if so, recovering or extracting the hidden information [35]. This phrase is used in a manner akin to cryptanalysis in the field of cryptography. Due to the wide range of features of digital texts, the extensive diversity of embedding techniques, and the often-modest embedding distortion, text steganography is a challenging process in practice. Because data embedding can change the statistics of the file or cover message, text steganography is sometimes achievable [36]. In other words, the presence of embedded symbols (for example, those methods that adapt the CM to keep the bits secret) still causes a CM original and its consistent CMHM to differ in certain aspects, even if this is frequently imperceptible to the human vision system. Steganalysis techniques are frequently classified as specialized or universal based on their application [37]. The latter strives to defeat all watermarking and steganography algorithms, whereas the former tries to disrupt a specific algorithm of steganography or watermarking. Specific approaches have higher detection accuracy in practice than universal approaches because they use prior knowledge of how a specific target algorithm function [38]. However, as they might operate irrespective of the embedding technique and potentially be adapted to unidentified approaches of watermarking or steganography, worldwide steganalysis is more appealing in practical application [39]. We can categorize potential attacks into three groups from a steganalysis perspective: structural attacks, visual attacks, and probabilistic/statistical attacks.

III. METHODOLOGY

The ISI Web of Science and Scopus database offers assurance for raw data validity used in visual analysis because of its extensive duration and high quality and volume of entries [40]. Furthermore, the accuracy of the knowledge map analysis is dependent on the quality of the literature retrieval, and the foundation for correct data collection is the building of the search query. Controlling the literature within the scope of the inquiry is essential. A purview that is too broad will lessen search results' comprehensiveness and filter out pertinent literature, whereas a purview that is too narrow would exclude relevant literature and contaminate the retrieval results. To ensure that the search results are as precise and thorough as possible, the search type must be modified in response to the search results. We used a systematic technique to find pertinent studies on video, audio, image, and text steganography in the Web of Science (WOS) All Database and Scopus databases. For the content analysis, we selected all the search results,

including published articles, patent work, and conference papers, based on the journal quality. Search phrases were used to look up academic literature. These search terms were combined, and the search rules used were:

1. steganography AND steganalysis OR "steganalysis technique" AND "digital forensic"
2. video AND steganalysis OR "steganalysis technique" AND "digital forensic"
3. audio AND steganalysis OR "steganalysis technique" AND "digital forensic"
4. image AND text AND steganalysis OR "steganalysis technique" AND "digital forensic"
5. steganalysis OR "steganalysis technique" AND "digital forensic"
6. video AND audio AND image AND text AND steganalysis OR "steganalysis technique" AND "digital forensic"

These were then put in the searching criterion Topic in the Web of Science (WOS) – All Database and Scopus with the language set to English.

IV. RESULTS

A transmission medium, such as text, audio, video, or images, is used in steganography. Any common format specific to that medium is considered the format of the transmission medium. The embedding can contain text, audio, photos, or video [41]. Any percentage may be used for embedding. Any optimization strategy can be used alone or in combination with any classification method. Any kernel relevant to the classifiers may be chosen as the kernel. Any standard statistical feature, or a combination of standard statistical features, may be utilized as a feature. Any feature reduction method may be used [42]. Both calibrated and uncalibrated photos can be used with this. The image size can be any standard size, and all video and audio formats are the same [43]. In a calibrated and uncalibrated transmission medium, Shankar [41] hypothesized that steganalysis can be utilized for LSB matching, LSB replacement, PVD, and F5. Because of its high dimensionality and optimization for improving classifier efficiency, steganography uses less principal component analysis and produces fewer false positives and false negatives in real-time data. The outcomes of the investigation are outlined in Fig. 1.

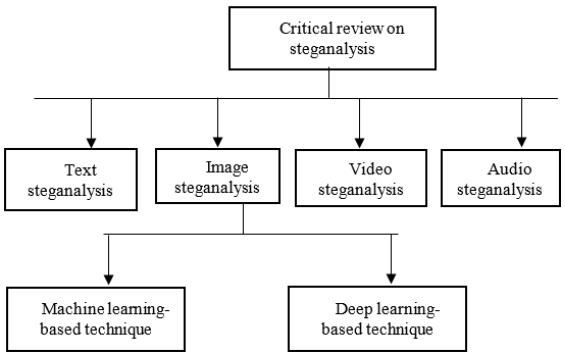

Fig. 1. Analysis framework.

A. Text steganalysis

The fundamental purpose of text steganography algorithms is to identify stego-texts produced using linguistic steganography methods, which produce texts that appear to be practically unmodified [10]. Utilizing statistical techniques like synonym frequency and semantic correlation is the primary method for dealing with the detection of stego-texts. The statistically examined data can be fed as features into support vector machine classifiers and other machine learning classifiers. Convolutional and recurrent neural networks are mostly used in deep learning methodologies that have also been put into practice to extract text features. In terms of statistical algorithms, machine learning, and deep learning (DL), the techniques outlined appear promising. But there isn't a clear baseline of work, and there aren't many resources available for text steganography right now. A data-text-based concealing method named UniSpaCh was suggested by Por et al. [44]; it creates the SM's binary string and separates it by 2-bit categorization (specifically, "10, 01, 00, and 11"). Additionally, it replaces all 2-bits with a unique space (for example, "hair," "thin," "punctuation," and "six per em"). Finally, it inserts extra spaces into the MS Word file at predetermined points such as between words, phrases, lines, and paragraphs. However, this method has a low EC rate, provides high robustness and excellent invisibility against optical and structural attacks (two bits between spaces), and is unapplicable to inserting long SMbits into a short CM.

Odeh et al. [45] proposed a new algorithm of text steganography named ZW_4B that applies the characters of ZWCs to hide SMbits in a Word file of MS. This algorithm engages 4 ZWCs to mark 4 bits of the SMbits among the CM file letters. For example, if the algorithm embeds all four ZWCs after a CM letter, it indicates that the buried code is "0001," 3 ZWCs are marked as "0001," etcetera. This method is suitable for multilingual texts and provides excellent invisibility as well as higher embedding capacities. Since only the embeddable position is in between letters, it has minimal robustness. Additionally, this approach can protect the embedded bits from structural assaults. Homomorphic encryption is used in Naqvi et al.'s [46] multi-layer text steganography technique known as MHST, which conceals the SM by swapping out its characters for those of the CM. According to the experimental findings, the algorithm has a low vulnerability to visual or MBR attacks but a high-capacity embedding, strong robustness, and unnoticeable transparency against structural attacks. namely, if an attacker manipulates the CMHM portion, the SM's extraction process may fail because of the likelihood of eliminating certain characters of the SM through the CM. Odeh and Elleithy [47] presented a method of text steganography named ZWBSP that inserts the SMbits by adding the normal space (U+0020) alongside a ZWC (U+200B) among words in a Word file of MS. Based on a specified pattern, this method takes into account the embeddable placement after or before the typical space between words. This approach provides high invisibility, medium robustness, and low EC in real-world applications. Furthermore, it is appropriate in diverse languages and guards the SMbits embedded against visual and structural attacks.

Rizzo et al. [48] developed TWSM, a text watermarking method that may include a password-based watermark in a CM Latin-based. This method marks the watermark SMbits in the CM using homoglyphic Unicode characters and special spaces. According to the researchers, this method offers excellent invisibility and high capacity while also hiding a watermark (64 bit) inside a short CM of 46 letters only. It is nevertheless susceptible to visual attacks and structural attacks (such as changing the CMHM font type, which causes the SMbits to be lost). This technique could only be used in cover texts that were based in Latin because it used homoglyphic letters. Later, Rizzo et al. [49] used the same technique to mark or embed a watermark in social media platforms. Two methods of watermarking centered on changing the cover text with Unicode spaces and ZWCs were proposed by Alotaibi and Elrefaei [50]. The first algorithm makes use of the Arabic language's dotting feature, which Alotaibi and Elrefaei [50] applied to improve the functionality of earlier work. In addition, the ZWNJ is used to mark or embed, depending on whether a letter is pointed or not, before and after the standard space. The second approach, known as 4-SpaCh, uses four Unicode characters to add after a standard space (such as ZWNJ, Thin, Hair, and ZW). All four SMbits bits are embedded or marked by corresponding Unicode order and characters: the second bit is denoted by the thin space, the first bit by the ZWNJ, the fourth bit by the ZW space, and the third bit by the hair space. Therefore, the algorithm represents a "1" if it embeds every fourth space; otherwise, it signifies a "0." Due to the use of Unicode characters to mark the SMbits in the CMHM, the second approach can really be used for embedding in multilingual texts. With regard to visual attacks, this method has a greater EC, higher imperceptibility, and lower DR; specifically, if the CMHM portion is manipulated by an attacker (comprising certain spaces), then it causes extraction by the corresponding Ext() to fail for the whole of the SM. Lin et al. [51] offered an algorithm for text steganography by using a combination of whitespace and WS_EL (extended-line), which offers social media secure communication. This method embeds a further white space between words and produces an SM binary string at the line end and at the paragraph end to mark the SMbits. According to the experimental findings, this technique provides the best EC and high invisibility; nonetheless, it likewise has a low DR against optical attacks. Since Chinese does not employ spaces between words, any strategies that are effective in this regard cannot be applied to writings in this language.

B. Image steganalysis

From traditional machine learning algorithms that manually extract features to deep learning feature extraction algorithms that automatically extract features, image steganography has come a long way [1]. The most recent image steganography methods were covered in this section along with a comparison of each method, starting with machine learning methods and ending with deep learning methods.

C. Machine learning techniques

In the literature, there are numerous machine learning-based image steganography approaches. Specific types of image steganography are the focus of some steganalysis tools. A good example of this is the Chutani and Goyal [52] study, which used an ensemble regression classifier with an Extreme Learning Machine (ELM)-based

steganography algorithm to analyze photos. The writers were capable to spot the common LSBR (Least Significant Bit Replacement), HUGO (Highly Undetectable stego), MiPOD (Minimizing the Power of Optimal Detector) and LSBMR (Least Significant Bit Matching Replacement) spatial steganography domain-based methods using Spatial Rich Model (SRM) and Subtractive Pixel Adjacency Matrix (SPAM) features [53]. In another study, Chaeikar et al. [32] used the Pixel Similarity Weight (PSW) to determine how similar the red, green, and blue cannels' colors are to find the hidden data. The secret data length concealed by the steganography image approach was also estimated by the authors. They examined the four nearby zones' pixel values, calculated the PSW, and then compared it to the reference profiles to determine its degree of doubtfulness. The planned approach could attain detection precision of 67%, 98%, and 75% for cover, 0.25bpp, and 0.125bpp correspondingly, according to the SVM classifier findings. Additionally, using 0.125 bpp and 0.25 bpp, the scheme could evaluate the secret data length to be around 44% and 97%, respectively. Desai et al. [54] suggested a different method for detecting spatial steganography domain-based using SVM. Additionally, Veena and Arivazhagan [55] used tri-level optimization with Discretized-All Condensed Nearest Neighbour (D-AIICNN), Greedy Randomised Adaptive Search Procedure (GRASP) and Recursive Feature Elimination (RFE) method for reduction feature in domain-based spatial picture steganalysis.

Following feature reduction, the authors trained and tested adaptive LSB-based embedding schemes using an ensemble classifier with a regression tree. To recuperate the Multiple LSB (MLSB) stego-key picture steganography technology, Yang et al. [56] developed a steganalysis technique. A recent steganalysis image method for binary pictures employing classifier of SVM was presented by Lu et al. [57]. The suggested technique made use of a feature known as Structuring Elements (SE) that is centered on a local first-order texture pattern, in the form of histogram bins pixels. To test various spatial domain-based approaches, two diverse s-patterns, 50D and 500D, were used in the studies. Additionally, there are numerous additional works in domain-based spatial image steganography; new researchers and readers are advised to read the paper review for more information [58]. Additionally, Song et al.'s [59] proposal for an image steganalysis approach for JPEG images used the 2-D Gabor wavelet's Shannon entropy as a feature. The benefit is the ability for localization joint in experiments and the spatial domain; primarily, the JPEG picture was transformed into the spatial domain. A gradient channel feature correlation for steganalysis of image color steganography methods was proposed by Kang et al. [60]. Additionally, the authors used an ensemble classifier to classify the well-known WOW and S-UNIWARD techniques of steganography using SCRQ1 (Spatio-Color Rich Model with Quantization Step q = 1) [61]. The experimental results showed that, in comparison to the current state-of-the-art steganalysis techniques, the planned scheme could lower the error detection rate. After that, Yang et al. [62] significantly decreased the detection error rate while keeping the payload at 0.05 bpp, doing so by 5.20% for WOW and 4.90% for SUNIWARD. Additionally, two classifiers Random sub-space Fisher Linear Discriminant (FLD) and Random Vector Functional Link (RVFL) were employed by Fan et al. [63] to increase various steganographic systems' detection accuracy centered on the spatial domain and DCT. The experimental findings demonstrated the FLD ensemble classifier's superior high accuracy to RVFL.

D. Deep learning-based techniques

Researchers studying image steganography currently rely on deep learning-based algorithms to increase detection efficiency and accuracy due to changes and advancements in technology [37]. Several researchers have recently suggested learning-based deep image steganography algorithms, and some of the first methods are covered here. An image CNN-based steganalyzer with five convolutional layers was presented by Xu et al. [64]. The proposed model's use of an absolute value layer (ABS) and a 1 x 1 convolutional kernel strengthened the statistical model. The authors trained CNNs using the suggested model network as a learner base to achieve more accurate detection [64]. Additionally, to enhance the pre-processing CNN layers' filters' weights A new steganography method was put forth by Zhang et al. [65] to decrease the contents of the image and increase the noise steganographic power. The proposed method employs 3 x 3 convolutional kernels that are enhanced during pre-processing. The method used various convolutions to provide residual spatial and channel correlations for a better feature picture. For local features, they used SPP (Spatial Pyramid Pooling), and they also analyzed random image sizes to improve the feature representation [66]. Transfer learning was also used by Qian et al. [67] to switch CNN parameters trained on high-steganography payload images to CNN parameters trained on low-steganography payload images. The findings showed that the proposed transfer learning model performed more accurately than non-transfer learning models. The spatial domain approaches S-UNIWARD and WOW were used in the studies. Additionally, Ye et al. [68] created a model of CNN-based, spatial domain-based methods employing 8 convolutional layers. The concept

suggested self-activating truncation linear units (TLUs) and filter banks for image processing. In contrast to earlier CNNs, this model initialized the SRM-based weights for residual characteristic maps using the filter banks. Once more, Yedroudj et al. [69] improved steganographic noise extraction by applying filters decided in SRM, and arrangement was carried out by applying CNN. To enhance the outcomes, the model made use of activation TLU units, an ABS layer, five convolutional layers, and the best elements of YeNet and XuNet [68]. For the steganography examination of spatial steganography domain-based methods, Tang et al. [70] applied two networks of reference. The Generative Adversarial Network (GAN) approach employed two networks (one for steganalysis and the other for steganography) to determine the ideal location to conceal data. Additionally, Tsang and Fridrich [71] adapted the YeNet network, utilizing the network of CNNs for training with low-resolution pictures to classify high-resolution stego-images. JPEG images can be steganographically analyzed for big picture datasets; Zeng et al. [72] suggested a method that combined rich model (RM) pre-processing based on CNN. Additionally, Chen et al. [73] suggested a technique of deep learning (DL) based on payload prediction in the frequency domain and spatial domain-based techniques of steganography. In addition, Li et al. [74] increased the detection accuracy by running three CNNs simultaneously. For feature extraction, each of the 3 networks applied a separate layer of pre-processing, including linear SRM, Gabo filters, and nonlinear SRM [59]. Additionally, the CNN model utilized three activation functions concurrently for additional pre-processed data. Zhang et al.'s [75] adaptive steganalysis method for steganography JPEG image schemes was used to create a new paradigm. To achieve excellent detection accuracy, the technique combined rich model features with DCT basis function features. This method's flaw is that it takes a lot of time and has poor real-time performance. To detect spatial domain-based approaches, Kim et al. [76] recently built a CNN based picture steganalysis model with additional payload. Claiming it would be sufficient after embedding to identify photographs without or with secret data, further embedded data was used.

E. Video steganalysis

One of the methods to find hash-centered 2, 3, and 4 LSB steganography videos was put out by Fan et al. [77] for spatial domain-based steganalysis. The cross-correlation property of video frames was used by the authors, and a hash function was used to detect the sites' embedding; however, it is particularly vulnerable to attacks. The experimental outcomes showed that the suggested technique is effective at detecting LSB-based hash steganography videos and that it can likewise reasonably approximate encoded message length. Tasdemir et al. [78] suggested a vector-based motion steganography method with a rich model that includes several high-pass filters. Seven different steganalysis methods and five steganalysis strategies were taken into consideration for comparison while doing the steganalysis utilizing an ensemble classifier. The findings showed that using both temporal and spatial reliance improved detection accuracy by five percent in large payload ranges and twenty percent in low payload ranges. The data hidden and factor gain of the spectrum spread embedding rules for steganalysis are also evaluated by Zarmehi and Akhaee [79]. Six characteristics total three from a video frame and three from a residual matrix were extracted for implementation. Additionally, Sheng et al. [18] provided a steganography video method for altering HEVC intra-prediction mode to discover secret message embedding. The authors used various prediction unit sizes, such as 4 x 4, 8 x 8, 16 x 16, 32 x 32, and 64 x 64, in their trials. A useful feature set for the SVM classifier is the change rate between the prediction unit's prediction rate before and after recompression. A steganography video method centered on the spatial-temporal detector (ST_D) was anticipated by Tasdemir et al. [78] to spot steganography that is spatial domain-based for H.264 and MPEG-2 coding criteria. The texture complexity and local motion intensity were determined using histogram distribution by dividing each frame into 8 8 blocks. With an average identification accuracy of about 99% for MPEG-2 and H.264 films, the experiments were conducted using a classifier of SVM with kernels of chi-square. The outcomes were likened to those from advanced approaches.

Wang et al. [33] suggested a different method to identify steganography using MV-based techniques by minimizing the impact of statistical traits derived from movies. Additionally, Sadat et al. [80] suggested a method centered on the value of entropy to identify motion vector embedding in H.264-compressed videos. To determine the motion vector’s texture in the blocks, the suggested approach considered intrinsic and statistical properties of the video. The studies were conducted using an SVM classifier with a Gaussian kernel and an accuracy of 99.9%, which ultimately demonstrated the method’s great performance. Using a fuzzy cluster, the blocks were grouped. Li et al. [81] proposed a video steganography method that modifies the unit of prediction in the mode of partition in P-frames to detect HEVC video steganography. 25-dimension characteristics were first calculated, then they were optimized to become 3-dimension features. Results from experiments utilizing an SVM classifier with an

approximate 93% detection accuracy were obtained. A universal feature set for video steganography was also published by Zhai et al. [82] for the detection of partition mode and motion embedding on a vector-domain basis. A universal method of video steganography analysis employing deep learning for vector motion and mode-based intra-prediction steganography was also proposed by Liu and Li [83]. The pixel values used as a detection feature by the Noise Removal - Convolutional Neural Network (NR—CNN) framework are altered by embedding in vector motion and the intra-prediction mode. Each of the three sets used in the experiments a training set, a verification set, and a test set contained 20,000 video frames [83]. The set test was applied to determine the detection accuracy of the network of the NR-CNN, which was trained using verification and training sets. Different embedding rates were used in the trials: for intra-prediction, the maximum rate of embedding was 100%, while for vector motion video steganography, the highest embedding rate was 20% [83]. For intra-prediction and motion vector embedding, the findings showed detection accuracy of 99.74% and 95.3%, respectively [83].

F. Audio steganalysis

Audio steganalysis seeks to identify any shift in an indication brought on by embedded information [2]. The two primary domains for data embedding are spatial and occasionally "time" or "temporal," and this is typically done by changing a data sample's least significant bit (LSB) in a file audio or in the domain transform by changing various signal characteristics [3]. Additionally, the steganalysis audio is divided based on format into methods of steganalysis for steganalysis methods and non-compressed formats for compressed formats like MP3 and AAC [84]. Jin et al. [85] suggested a target technique of steganography analysis for MP3-Stego detection about compressed formats. The authors observed that the modified quantized cosine discrete transform coefficients QMDCT of the MP3Stego are modified during compression, which influences the correlations between nearby QMDCTs of the cover audio. Hence, to define the correlations of the QMDCTs, features of Markov are retrieved from stego and cover audio [85]. To choose the best features to train a classifier with SVM, these features are next subjected to pre-processing processes. The studies show that the suggested technique produces good detection accuracy even when the embedding rate is low. MP3's QMDCT coefficient matrix is constructed to extract features of the steganalytic in Wang et al.'s [86] alternative steganalytic method for MP3. The application of rich high-pass filtering increased the technique's sensitivity to noise signals.

According to Wang et al. [86], modifying one QMDCT coefficient causes one Huffman codeword to change. They proposed a correlations measure module to identify any potential modification in the QMDCT coefficients matrix at pointwise, 4 x 4 block-wise, and 2 x 2 block-wise levels, independently. An empirical threshold was used to lower the characteristics' dimension and choose the best one. The classifier ensemble was trained for the classification job [87]. It offers both the cooperative approach and the non-cooperated way for non-compressed formats. The first method relies on a contrast between the projected stego signal and the cover signal for its techniques. The cover can be estimated in a variety of ways, including using denoising bases, re-embedding, liner bases, and other techniques. Though Ghasemzadeh and Arjmandi [88] employed stego signal estimation for calibration, based on the calibration, Ghasemzadeh and Arjmandi [88] suggested a general technique of steganalysis. In their method, a random message was embedded in the signal using the re-embedding technique. To extract the energy features, the re-embedded signal and each signal were split into numerous chunks, and each energy was calculated. Each signal chunk's energy and its equivalent are then re-embedded and removed. Lastly, the SVM classifier is trained using the energy features' statistical characteristics, such as skewness, mean, kurtosis, and standard deviation.

A broad variety of steganography techniques have been used to evaluate their technique. The outcomes of the investigation demonstrated its efficacy in detecting both targeted and general instances. The non-collaborated technique, on the other hand, extracts the audio signal features directly in accordance with the embedding feature domain. A linear prediction approach, proposed by Han et al. [89], involves extracting linear prediction LP characteristics from the segmented audio file. The trials revealed that the LP can discern significantly between the stem and cover, according to the authors. As a result, the frequency and time domains are used to extract the characteristics of the LP residual, LP coefficients, LP cepstrum, and LP spectrum coefficients. Based on the features that were recovered from cover and stego signals, the SVM classifier was trained. Numerous experiments using various ratio embeddings are carried out and contrasted with various steganography methods. The comparison with popular and modern steganalysis approaches, where accuracy levels of above 96% are attained, demonstrated the usefulness of the presented techniques. In the subject of statistics, deep learning has recently drawn greater attention and produced better outcomes. A better approach based on CNN was put forth by Lin et al. [90] to identify

steganography audio in the temporal domain. The leftover signal from the input audio is first extracted using a filter high-pass layer. Then, using six different sets of layers, the input's hierarchical representations are created. The initial set just comprises the initial convolutional layer's activation, while the following sets each comprise a convolutional layer and a layer pooling [13].

Non-linear activation is used following each convolution step. When these layers are finished, the signal audio is changed into 215 features. The retrieved characteristics are passed into the classifier binary, which has a completely linked layer and a softmax layer, to detect steganography. This method demonstrated its efficacy in identifying various embedding rates. A worldwide steganography method using a ResNet for feature extraction was proposed by Ren et al. [91]. The network neural known as the Residual Network Spectrogram Deep received its input from the spectrogram of the audio stream (S-ResNet). Fig. 2 shows the way the spectrogram can signify energy information from different bands of frequency across time in addition to including useful time-frequency data from the audio stream.

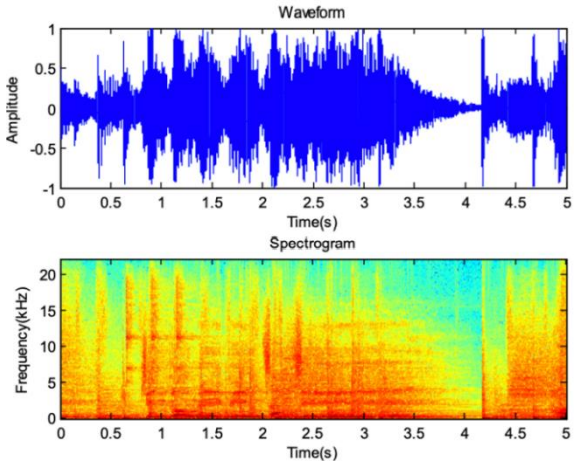

Fig. 2. Spectrogram and wave-form picture for a segment audio
Source: Ren et al. [91]

The writers tried to utilize it to capture features generated by the technique of audio steganography for this reason. Between the ReLU layers and batch normalization of S-architecture ResNets, there are 31 convolutional layers that are used to speed up learning and learn more complicated patterns, respectively [91]. There is a unit residual to calculate the function residual after individual group layers of convolutional neural networks. After every five residual blocks, two average layers of pooling are used to reduce the size of the data. To create the feature vector, a global average pooling layer is then used [91]. The S-ResNe trained an effective model, and this model is input to the SVM for binary classification and last training. Findings of the experiment demonstrate greater detection, with average precision being 94.98% for the AAC format and 99.93% for the MP3 format, respectively [91].

V. Future Directions

Because most authentication systems use SMS to confirm users' identities, structural-based authentication is the best choice for providing secure communication against network-wide attacks such as MITM, guessing attacks, and brute-force attacks. Structural-based steganography methods may be used to meet this need when secret information transmission over open networks is the main concern. To label subtle documents over private networks for unwanted tracking access, a mix of ZWC-based and machine-learning algorithms can be used. In a government institution, for instance, classified documents might be noticeable with identifiers like an illegible signature that is hard to spot. To defend valuable information against malicious attacks, a combination of structurally based text hiding and learning unsupervised algorithms can be used to intelligently analyze information in data reproduction or resharing. This is since social media has become an integral part of end users' daily communications. To enhance the embedding capacity criteria, algorithms of lossless compression like LZW, Huffman coding, arithmetic, and others can be used at structural-based techniques' encoding stage. To achieve a particular level of security, an effective algorithm of text hiding must offer the best trade-off between the three essential standards. Researchers in cybersecurity must consider a variety of factors, including the advantages and disadvantages of different text-hiding algorithms as well as the suggestions we have provided. They should also consider whether the strategies for hiding text would be appropriate for the specific application or not. When a researcher realizes that certain algorithms'

advantages might be suitable for the requirements of the application under consideration, the algorithm should probably be tried. For copyright and security reasons, some photographs might include watermarking, which could impede the steganography process and forecast inaccurate results. A proposed system should be able to distinguish between steganographic features and watermarking traces as a potential future upgrade. Considering the current bibliographic review, the following further work is possible:

1. Create novel CNNs that combine the benefits of current networks or create a completely novel architecture (shallow, dense, or/and deeper architectures) to increase the percentages of detection in the frequency and spatial domains.
2. Use various digital picture databases to undertake more experiments and conduct in-depth research on the cover-source mismatch effect while taking into consideration factors like the use of various cameras.
3. Test additional steganographic methods in the JPEG domain as part of steganography analysis.
4. Modify the Generative Adversarial Network methodology to do automatic steganography in the domain of JPEG as well as steg-analysis in the spatial domain.
5. Modify the CNNs that perform statistical analysis quantitatively to enhance the accuracy of your prediction of payload.
6. Use DL to perform quantitative steganography analysis to forecast the frequency domain payload of an image (JPEG).
7. Use larger picture sizes and larger databases to retrain existing CNNs. To achieve the demands of memory and processing, it is essential to conduct the training using a cluster architecture of central processing units and graphics processing units.
8. To determine how much transfer there can be from one algorithm to another, train CNNs using a specific steganographic algorithm and test them using a different approach.

Digital forensic professionals, cyber experts, and researchers working in this field are given several recommendations for the future.

A. New Steganalysis Tools

The number of strategies and tools for embedding outnumbers those for finding and extracting concealed data. Numerous steganography tools are available for free or at no cost, however this is not the case for steganalysis, which requires more work and a keen understanding of the steganography tools and procedures to evaluate. Therefore, forensic and cyber professionals must create more effective steganalysis tools.

B. Practical steganalysis Techniques

When creating useful steganalysis tools, time consumption and computation complexity are two important factors that must be considered. No matter how complicated the computation is, most current techniques focus on accuracy detection. Nowadays, the development of artificial intelligence and learning deep opens novel possibilities for more precise and quicker detection. Despite their benefits, several considerations should be made, including limiting the training phase's complexity, avoiding overfitting, and properly fixing and setting hyperparameters prior to training.

C. General steganalysis Techniques

Most steganography algorithms now in use rely on the training dataset to train and develop classifiers on representations of solely cover medium (blind) or stego and cover medium (semi-blind). As a result, there is a strong correlation between training datasets and classification accuracy, with accuracy typically decreasing as the training and testing datasets diverge. In fact, most procedures now in use fall under the semi-blind approach. Numerous steganography methods exist in the actual world, together with various cover contents, size, noise levels, sampling frequencies, etc. It is impossible to limit the training datasets with this quantity, especially for stego-media. A few methods (Lerch-Hostalot and Megas, 2016) use the unsupervised method to address this problem, but accuracy still must be increased.

D. New Standards

According to academics, the most recent compression standard, H.265/HEVC, is still relatively new, but because it has numerous cutting-edge capabilities, it will soon displace the others. Therefore, from the perspective of steganography, it appears that there is plenty of room to investigate this field for building a steganography method. Additionally, because steganography's new standard is HEVC/H.265, it is probable to be used by terrorists and criminals, necessitating the need for tools and algorithms that can detect the presence of hidden data.

E. Machine Learning

The accuracy of the steganography process can also be increased by using machine learning techniques. It might be useful in identifying video steganography methods, which are typically challenging to investigate and identify.

F. IoT

A few academics are already employing the IoT (Internet of Things) in this technological age to transfer and store data that has been steganographically concealed. It is conceivable that cybercriminals will also use it to access confidential information stored in embedded components' memory and actuators. There is currently no steganalysis instrument or strategy available for this new method of hiding.

G. Search Engines

New search engines that can detect, recognize, and trace the usage of steganography through various channels are needed to prevent steganography on the Internet. Additionally, there need to be certain applications running continuously to find media hidden files on the internet, necessitating the use of a sizable clustered or distributed system for parallel evaluation. Even though millions of media files are transferred and posted online each second, it seems challenging. Though, it might be accomplished in the upcoming years with the help of highly qualified forensic and cyber professionals, preventing the devastating situation.

H. Other Online Services

Online services that are widely used and appear to be benign, including IP telephony, Bit Torrent, Skype, and cloud storage, can be used for clandestine communication. These traffic services of network offer numerous places to conceal sensitive information, and as there is no tool of steganalysis for traffic inspection of network, it is difficult for forensic examiners to detect them. Criminals now have more opportunities than ever to use new, unassuming hiding places, like online games, cloud storage systems, and virtual worlds. It is necessary to build steganalysis methods for these network traffic services.

VI. CONCLUSION

There are algorithms for text steganalysis. Some of the effective algorithms are UniSpaCh, AITSteg, ZWBSP, ZW_4B, 4-SpaCh, WS_EL, TWSM, EM_ST, 4&3SpaCh. There are numerous software programs that make it simple to find hidden info in images, text, video, and audio steganalysis. Most of them aim to exploit famous steganography methods. While most researchers concentrated on steganalysis techniques, only a small number of papers examined the state-of-the-art steganalysis tools. However, the literature presented a comparison of a few of the well-known steganalysis techniques. The steganalysis tools are discussed below;

1. SpyHunter created StegSpy, which is set up on Windows. Freeware that can now recognize steganography produced by the Hiderman, JPHideandSeek, Masker, JPegX, and Invisible Secrets tools is used for image steganalysis.
2. Niels Provos created StegDetect, which can be downloaded and used on Linux, Mac, and Windows. It is a freeware program that is used for image steganalysis.
3. Alfonso Muoz is the creator of the Java-based program StegSecret. It is a freeware program used for picture, audio, and video steganalysis.
4. WetStone Technologies created the Windows-based program StegoHunt. It is a licensed purchase and is used for image, audio, and video steganalysis.
5. Benedikt Boehm created the Java-based program StegExpose. It is a freeware program that is used for image steganalysis.
6. Backbone Security created the Windows-based program StegAlyzerAS. It is a licensed buy and is used for image steganalysis.
7. Backbone Security created the Windows-based product StegalyzerSS. It is a licensed buy and is used for image steganalysis.
8. Backbone Security created Windows, Apple OS, and Linux program StegAlyzerFS. It is a licensed purchase and is used for image, audio, and video steganalysis.
9. VSL is a Java-based program created by Michal Wegrzyn. It is a freeware program that is used for image steganalysis.

REFERENCES

[1] M. Dalal, and M. Juneja, "Steganalysis of DWT Based Steganography Technique for SD and HD Videos," Wireless Personal Communications, 2022, pp.1-12.

[2] K.D. Michaylov, and D.K. Sarmah, "Steganography and steganalysis for digital image enhanced Forensic analysis and recommendations," Journal of Cyber Security Technology, 2024, pp.1-27.

[3] M. Dalal, and M. Juneja, Steganography and Steganalysis (in digital forensics): a Cybersecurity guide. Multimedia Tools and Applications, vol. 80, no. 4, pp.5723-5771, 2021.

[4] G. Georgieva-Tsaneva, G. Bogdanova, and E. Gospodinova, "Mathematically Based Assessment of the Accuracy of Protection of Cardiac Data Realized with the Help of Cryptography and Steganography," Mathematics, vol. 10. No. 3, pp.390, 2022.

[5] M. M. Hashim, M. S. Taha, A. H. M. Aman, A. H. A. Hashim, M. S. M. Rahim, and S. Islam, "Securing medical data transmission systems based on integrating algorithm of encryption and steganography," In 2019 7th International Conference on Mechatronics Engineering (ICOM) (2019, pp. 1-6). IEEE

[6] H. Majed, H. N. Noura, and A. Chehab, "Overview of Digital Forensics and Anti-Forensics Techniques," In 2020 8th International Symposium on Digital Forensics and Security (ISDFS) (2020, pp. 1-5). IEEE

[7] M. A. Wani, A. AlZahrani, and W. A. Bhat, "File system anti-forensics–types, techniques and tools," Computer Fraud & Security, vol. 2020, no. 3, pp. 14-19, 2020.

[8] Y. Zou, G. Zhang, and L. Liu, "Research on image steganography analysis based on deep learning," Journal of Visual Communication and Image Representation, vol. 60, pp. 266-275, 2019.

[9] N. T. Cyriac, and L. Sadath, "Is Cyber security enough-A study on big data security Breaches in financial institutions," In 2019 4th International Conference on Information Systems and Computer Networks (ISCON) (2019, pp. 380-385). IEEE

[10] M.T. Ahvanooey, Q. Li, J. Hou, A.R. Rajput, and C. Yini, "Modern text hiding, text steganalysis, and applications: a comparative analysis," Entropy vol. 21, no. 4, pp. 355, 2019.

[11] N.S. Kamaruddin, A. Kamsin, L.Y. Por, and H. Rahman, "A Review of Text Watermarking: Theory, Methods, and Applications," IEEE Access, vol. 6, 2018, pp. 8011–8028.

[12] M. Bouzegza, A. Belatreche, A. Bouridane, and M. Tounsi, "A comprehensive review of video steganalysis," IET Image Processing, vol. 16, no. 13, pp.3407-3425, 2022.

[13] W.M. Eid, S.S. Alotaibi, H.M. Alqahtani, and S.Q. Saleh, "Digital image steganalysis: current methodologies and future challenges," Ieee Access, vol. 10, 2022, pp.92321-92336.

[14] W.D. Ferreira, C.B. Ferreira, G. da Cruz Júnior, and F. Soares, "A review of digital image forensics," Computers & Electrical Engineering, vol. 85, 2020, p.106685.

[15] D.A. Shehab, and M.J. Alhaddad, "Comprehensive survey of multimedia steganalysis: Techniques, evaluations, and trends in future research," Symmetry, vol. 14, no. 1, p.117, 2022.

[16] W. Akanji, O. Okey, S. Adelanwa, O. Odesanya, T. Olaleye, M. Amusu, A. Akinrinlola, and A. Oladejo, "A blind steganalysis-based predictive analytics of numeric image descriptors for digital forensics with Random Forest & SqueezeNet," In 2022 5th Information Technology for Education and Development (ITED) (2022, pp. 1-7). IEEE.

[17] X. Song, Z. Li, L. Chen, and J. Liu, "Entropy feature based on 2D Gabor wavelets for JPEG steganalysis," in International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage, 2016, pp. 59–72.

[18] Q. Sheng, R.D. Wang, M.L. Huang, Q. Li, and D.W. Xu, "A prediction mode steganalysis detection algorithm for hevc," J Opt vol. 28, no. 4, pp. 433–440, 2017.

[19] B. Li, J. He, J. Huang, and Q. Y. Shi, "A survey on image steganography and steganalysis," Journal of Information Hiding and Multimedia Signal Processing, vol. 2, no. 2, pp. 142–72, 2011.

[20] R. Chandramouli, and K. P. Subbalakshmi, "Current trends in steganalysis: a critical survey," In: ICARCV 2004 8th control, automation, robotics and vision conference, 2, 2004, pp. 964–7.

[21] A. Nissar, and A. H. Mir, "Classification of steganalysis techniques: a study," Digital Signal Processing, vol. 20, no. 6, pp. 1758–70, 2010.

[22] Y.J. Chanu, K.M. Singh, and T. Tuithung, "Image steganography and steganalysis: a survey," International Journal of Computing Applications, vol. 52, no. 2, pp. 975–8887, 2012.

[23] X.Y. Luo, D.S. Wang, P. Wang, and F.L. Liu, "A review on blind detection for image steganography," In: Signal processing, vol. 88, Elsevier, 2008, pp. 2138–57.

[24] P. Pal, and S. Dubey, "Various JPEG image steganography techniques: a review," International Journal of Scientific & Engineering Research, vol. 7, no. 2, pp. 417–21, 2016.

[25] W. You, H. Zhang, and X. Zhao, "A Siamese CNN for image steganalysis," IEEE Transactions on Information Forensics and Security vol. 16, 2020, pp. 291-306.

[26] M. Boroumand, M. Chen, and J. Fridrich, "Deep residual network for steganalysis of digital images," IEEE Transactions on Information Forensics and Security vol. 14, no. 5, pp. 1181-1193, 2018.

[27] M.E. Mustafa, M.A. Elshafey, and M.M. Fouad, "Accuracy enhancement of a blind image steganalysis approach using dynamic learning rate-based CNN on GPUs," In 2019 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), vol. 1, 2019, pp. 28-33. IEEE.

[28] C. Fuji-Tsang, and J. Fridrich, "Steganalyzing images of arbitrary size with CNNs," In A. Alattar and N. D. Memon, editors, Proceedings IS&T, Electronic Imaging, Media Watermarking, Security, and Forensics 2018, San Francisco, CA.

[29] A. Rehman, T. Saba, T. Mahmood, Z. Mehmood, M. Shah, and A. Anjum, "Data hiding technique in steganography for information security using number theory," Journal of information science, vol. 45, no. 6, pp.767-778, 2019.

[30] R. Chandramouli, G. Li, and N.D. Memon, "Adaptive steganography," In Security and Watermarking of Multimedia Contents IV; International Society for Optics and Photonics: Bellingham, WA, USA, Vol. 4675, 2002, pp. 69–78.

[31] N.F. Johnson, and S. Jajodia, "Steganalysis of images created using current steganography software," In International Workshop on Information Hiding; Springer: Berlin/Heidelberg, Germany, 1998, pp. 273–289.

[32] S.S. Chaeikar, M. Zamani, A.B.A., Manaf, and A.M. Zeki, "PSW statistical LSB image steganalysis," Multimed Tools Appl vol. 77, no. 1, pp. 805–835, 2018.

[33] P. Wang, Y. Cao, and X. Zhao, "Segmentation based video Steganalysis to detect motion vector modification," Secur Commun Networks, pp. 1–12, 2017.

[34] H. Zhang, Y. Cao, and X. Zhao, "A steganalytic approach to detect motion vector modification using near-perfect estimation for local optimality," IEEE Trans. Inf. Forensics Secur., vol. 12, 2016, pp. 465–478.

[35] H. Gashi, S. Zargari, and S. J. Ghazaani, "Data Hiding in Anti-forensics—Exploit Delivery Through Digital Steganography," In International Conference on Global Security, Safety, and Sustainability (2023, pp. 65-76). Cham: Springer Nature Switzerland.

[36] B. Aziz, J. Jung, J. Lee, and Y.T. Chun, "A false negative study of the steganalysis tool stegdetect," Applied Sciences, vol. 10, no. 22, 2020, pp. 81-88.

[37] H. Kheddar, M. Hemis, Y. Himeur, D. Megías, and A. Amira, "Deep learning for steganalysis of diverse data types: A review of methods, taxonomy, challenges and future directions," Neurocomputing, pp.127528, 2024.

[38] S. Agarwal, and K.H. Jung, "Digital image steganalysis using entropy driven deep neural network," Journal of Information Security and Applications, vol. 84, pp.103799, 2024.

[39] B.G. Banik, and S.K. Bandyopadhyay, "Novel Text Steganography Using Natural Language Processing and Part-of-Speech Tagging," IETE J. Res., pp. 1–12, 2018.

[40] G.C. Yu, D. Kun, and L. Shengbo, "Realization mechanism of patent knowledge visualization based on CiteSpace II and its application," J. Chin. Soc. Sci. Tech. Info. Vol. 29, no. 4, pp. 663–670, 2010.

[41] D.D. Shankar, Steganalysis for LSB Matching, LSB Replacement in a calibrated and uncalibrated transmission medium, comprises a medium of transmission that is images, audio, video, or text, and format of the medium of transmission is any standard format. 2021, Patent Number: IN201941038817-A.

[42] Z. Yang, K. Wang, S. Ma, Y. Huang, X. Kang, and X. Zhao, "Istego100k: Large-scale image steganalysis dataset," In Digital Forensics and Watermarking: 18th International Workshop, IWDW 2019, Chengdu, China, November 2–4, 2019, Revised Selected Papers 18 (2020, pp. 352-364). Springer International Publishing.

[43] O. Evsutin, A. Melman, and R. Meshcheryakov, "Digital steganography and watermarking for digital images: A review of current research directions," IEEE Access, vol. 8, pp.166589-166611, 2020.

[44] L.Y. Por, K. Wong, and K.O. Chee, "UniSpaCh: A text-based data hiding method using Unicode space characters," J. Syst. Softw., vol. 85, pp. 1075–1082, 2012.

[45] A. Odeh, K. Elleithy, and M. Faezipour, "Steganography in text by using MS word symbols," In Proceedings of the Proceedings of the 2014 Zone 1 Conference of the American Society for Engineering Education, Bridgeport, CT, USA, 2014, pp. 1–5.

[46] N. Naqvi, A.T. Abbasi, R. Hussain, M.A. Khan, and B. Ahmad, "Multilayer Partially Homomorphic Encryption Text Steganography (MLPHE-TS): A Zero Steganography Approach," Wirel. Pers. Commun., vol. 103, pp. 1563–1585, 2018.

[47] A. Odeh, and K. Elleithy, "Steganography in Text by Merge ZWC and Space Character," In Proceedings of the 28th International Conference on Computers and Their Applications (CATA-2013), Honolulu, HI, USA, 2013, pp. 1–7.

[48] S.G. Rizzo, F. Bertini, and D. Montesi, "Content-preserving Text Watermarking through Unicode Homoglyph Substitution," In Proceedings of the 20th International Database Engineering & Applications Symposium (IDEAS '16), Montreal, QC, Canada, 2016, pp. 97–104.

[49] S.G. Rizzo, F. Bertini, D. Montesi, and C. Stomeo, "Text Watermarking in Social Media," In Proceedings of the 2017 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining, Sydney, Australia, 31 July–3 August.

[50] R.A. Alotaibi, and L.A. Elrefaei, "Improved capacity Arabic text watermarking methods based on open word space," J. King Saud Univ. Comput. Inf. Sci., vol. 30, pp. 236–248, 2018.

[51] W.B. Lin, T.H. Lai, and K.C. Chang, "Statistical feature-based steganalysis for pixel-value differencing steganography," EURASIP Journal on Advances in Signal Processing, 2021, pp.1-18.

[52] S. Chutani, and A. Goyal, "Improved universal quantitative steganalysis in spatial domain using ELM ensemble," Multimed Tools Appl vol. 77, no. 6, pp. 7447–7468, 2018.
[53] J. Fridrich, and J. Kodovsky, "Rich models for steganalysis of digital images," IEEE Trans Inf Forensics Secur, vol. 7, no. 3, pp. 868–882, 2012.
[54] M.B. Desai, S.V. Patel, and B. Prajapati, "ANOVA and fisher criterion based feature selection for lower dimensional universal image Steganalysis," Int J Image Process, vol. 10, no. 3, pp. 145–160, 2016.
[55] S.T. Veena, and S. Arivazhagan, "Quantitative steganalysis of spatial LSB based stego images using reduced instances and features," Pattern Recogn Lett vol. 105, pp. 39–49, 2018.
[56] C. Yang, X. Luo, J. Lu, and F. Liu, "Extracting hidden messages of MLSB steganography based on optimal stego subset," Sci. China Inf. Sci vol. 61, no. 11, pp.119103, 2018.
[57] W. Lu, R. Li, L. Zeng, J. Chen, J. Huang, and Y.Q. Shi, "Binary image steganalysis based on histogram of structuring elements," IEEE Transactions on Circuits and Systems for Video Technology, vol. 30, no. 9, pp.3081-3094, 2019.
[58] S. Chutani, and A. Goyal, "A review of forensic approaches to digital image Steganalysis," Multimed Tools Appl vol. 78, no. 13, pp. 18169–18204, 2019.
[59] X. Song, F. Liu, C. Yang, X. Luo, and Y. Zhang, "Steganalysis of adaptive JPEG steganography using 2D Gabor filters," in Proceedings of the 3rd ACM workshop on information hiding and multimedia security, 2015, pp. 15–23.
[60] Y. Kang, F. Liu, C. Yang, L. Xiang, X. Luo, and P. Wang, "Color image steganalysis based on channel gradient correlation," Int. J. Distrib. Sens. Networks, vol. 15, no. 5, pp. 1550147719852031, 2019.
[61] M. Goljan, and J. Fridrich, "CFA-aware features for steganalysis of color images," in Media Watermarking, Security, and Forensics 2015, vol. 9409, p. 94090V.
[62] C. Yang, Y. Kang, F. Liu, X. Song, J. Wang, and X. Luo, "Color image steganalysis based on embedding change probabilities in differential channels," Int. J. Distrib. Sens. Networks vol. 16, no. 5, pp. 1550147720917826, 2020.
[63] [63] L. Fan, W. Sun, and G. Feng, "Image steganalysis via random subspace fisher linear discriminant vector functional link network and feature mapping," Mob Networks Appl vol. 24, no. 4, pp. 1269–1278, 2019.
[64] G. Xu, H-Z. Wu, and Y.Q. Shi, "Ensemble of CNNs for steganalysis: An empirical study," in Proceedings of the 4th ACM Workshop on Information Hiding and Multimedia Security, pp. 103–107, 2016.
[65] Zhang, R., Zhu, F., Liu, J. and Liu, G. (2018). Efficient feature learning and multi-size image steganalysis based on CNN. arXiv Prepr. arXiv1807.11428.
[66] K. He, X. Zhang, S. Ren, and J. Sun, "Spatial pyramid pooling in deep convolutional networks for visual recognition," IEEE Trans Pattern Anal Mach Intell, vol. 37, no. 9, pp.1904–1916, 2015.
[67] Y. Qian, J. Dong, W. Wang, and T. Tan, "Learning and transferring representations for image steganalysis using convolutional neural network, " in 2016 IEEE international conference on image processing (ICIP), pp. 2752–2756.
[68] J. Ye, J. Ni, and Y. Yi, "Deep learning hierarchical representations for image steganalysis," IEEE Trans Inf Forensics Secur, vol. 12, no. 11, pp. 2545–2557, 2017.
[69] M. Yedroudj, F. Comby, and M. Chaumont, "Yedroudj-net: An efficient CNN for spatial steganalysis," in 2018 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), 2018, pp. 2092–2096.
[70] W. Tang, S. Tan, B. Li, and J. Huang, "Automatic steganographic distortion learning using a generative adversarial network," IEEE Signal Process Lett, vol. 24, no. 10, pp. 1547–1551, 2017.
[71] C.F. Tsang, and J. Fridrich, "Steganalyzing images of arbitrary size with CNNs," Electron. Imaging, vol. 2018, no. 7, pp. 121, 2018.
[72] J. Zeng, S. Tan, B. Li, and J. Huang, "Large-scale JPEG image steganalysis using hybrid deep-learning framework," IEEE Trans Inf Forensics Secur, vol. 13, no. 5, pp. 1200–1214, 2017.
[73] M. Chen, M. Boroumand, and J. Fridrich, "Deep learning regressors for quantitative steganalysis," Electron Imaging, vol. 2018, no. 7, pp.160–161, 2018.
[74] B. Li, W. Wei, A. Ferreira, and S. Tan, "ReST-net: diverse activation modules and parallel subnets-based CNN for spatial image steganalysis," IEEE Signal Process Lett, vol. 25, no. 5, pp. 650–654, 2018.
[75] T. Zhang, H. Zhang, R. Wang, and Y. Wu, "A new JPEG image steganalysis technique combining rich model features and convolutional neural networks," Math Biosci Eng, vol. 16, no. 5, pp. 4069–4081, 2019.
[76] J. Kim, H. Park, and J-I. Park, "CNN-based image steganalysis using additional data embedding," Multimed Tools Appl, vol. 79, no. 1–2, pp. 1355–1372, 2020.
[77] M. Fan, P. Liu, H. Wang, and X. Sun, "Cross correlation feature mining for steganalysis of hash based least significant bit substitution video steganography," Telecommun Syst, pp. 1–7, 2016.
[78] K. Tasdemir, F. Kurugollu, and S. Sezer, "Spatio-temporal rich model-based video Steganalysis on cross sections of motion vector Planes," IEEE Trans Image Process, vol. 25, no. 7, pp. 3316–3328, 2016.
[79] N. Zarmehi, and M.A. Akhaee, "Digital video steganalysis toward spread spectrum data hiding," IET Image Process, vol. 10, no. 1, pp. 1–8, 2016.
[80] E.S. Sadat, K. Faez, and M. Saffari-Pour, "Entropy-based video Steganalysis of motion vectors," Entropy, vol. 20, no. 4, pp. 244–257, 2018.

[81] Z. Li, L. Meng, S. Xu, Z. Li, Y. Shi, and Y. Liang, "A HEVC video steganalysis algorithm based on pu partition modes," Comput Mater Contin, vol. 59, no. 2, pp. 607–624, 2019.

[82] L. Zhai, L. Wang, and Y. Ren, "Universal detection of video steganography in multiple domains based on the consistency of motion vectors," IEEE transactions on information forensics and security, 15, pp.1762-1777, 2019.

[83] P. Liu, and S. Li, "Steganalysis of Intra Prediction Mode and Motion Vector-based Steganography by Noise Residual Convolutional Neural Network," IOP Conference Series: Materials Science and Engineering vol. 719, no. 1, pp. 12068, 2020.

[84] R. Tabares-Soto, R. Ramos-Pollán, G. Isaza, S. Orozco-Arias, M.A.B. Ortíz, H.B.A. Arteaga, A.M. Rubio, and J.A.A. Grisales, "Digital media steganalysis," In Digital Media Steganography; Elsevier: Amsterdam, The Netherlands, 2020, pp. 259–293.

[85] C. Jin, R. Wang, and D. Yan, "Steganalysis of MP3Stego with low embedding-rate using Markov feature," Multimed. Tools Appl., vol. 76, pp. 6143–6158, 2017.

[86] Y. Wang, X. Yi, and X. Zhao, "MP3 steganalysis based on joint point-wise and block-wise correlations," Inf. Sci., vol. 512, pp. 1118–1133, 2020.

[87] J. Kodovsky, J. Fridrich, and V. Holub, "Ensemble classifiers for steganalysis of digital media," IEEE Trans. Inf. Forensics Secur., vol. 7, pp. 432–444, 2011.

[88] H. Ghasemzadeh, and M.K. Arjmandi, "Universal audio steganalysis based on calibration and reversed frequency resolution of human auditory system," IET Signal Process., vol. 11, pp. 916–922, 2017.

[89] C. Han, R. Xue, R. Zhang, and X. Wang, "A new audio steganalysis method based on linear prediction," Multimed. Tools Appl., vol. 77, pp. 15431–15455, 2018.

[90] Y. Lin, R. Wang, D. Yan, L. Dong, and X. Zhang, "Audio steganalysis with improved convolutional neural network," In Proceedings of the ACM Workshop on Information Hiding and Multimedia Security, Paris, France, 2019, pp. 210–215.

[91] Y. Ren, D. Liu, Q. Xiong, J. Fu, and L. Wang, "Spec-resnet: A general audio steganalysis scheme based on deep residual network of spectrogram," 2019, arXiv, arXiv:1901.06838.