Journal of Theoretical and Applied Information Technology
15th March 2022. Vol.100. No 5
2022 Little Lion Scientific

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

A LITERATURE REVIEW OF VARIOUS STEGANOGRAPHY METHODS

[1]MUSTAFA MUNEEB TAHER, [1]ABD RAHIM BIN HJ AHMAD, [2,3]RANA SAMI HAMEED, [2]SITI SALASIAH MOKRI

[1]College of Computing Science & Information Technology, University of Tenaga, Malaysia
[2]Faculty of Engineering & Built Environment, Universiti Kebangsaan Malaysia
[3]College of Law and Political Science, University of Kirkuk Iraq

E-mail: [1]st23197@student.uniten.edu.my, [1]Abdrahim@uniten.edu.my, [2]p103503@siswa.ukm.edu.my ,[2]siti1950@ukm.edu.my

ABSTRACT

Nowadays, the volume of data shared over the Internet is growing. As a result, data security is referred to as a major issue while processing data communications through the Internet. During communication procedures, everyone requires their data to remain secure. Steganography is the science and art of embedding audio, message, video, or image into another audio, image, video, or message to conceal it. It is used to secure confidential information from harmful attacks. This research offers a classification of digital steganography based on cover object categories, as well as a classification of steganalysis art. Image visual quality, structural similarity (SSIM), mean square error, Image Fidelity (IF), payload capacity, Normalized Cross-Correlation (NCC), and robustness are some of the important aspects of steganography. Researchers have made tremendous advances in the realm of digital steganography. Nonetheless, it is vital to emphasize the advantages and disadvantages of modern steganography techniques. The purpose of this research is to examine and compare several steganography methods using characteristics such as PSNR, MSE, and Robustness. This study arrived at 15 possible research directions for developing high-quality stego objects, strong stenography techniques, and high payload based on the analysis of the studied parameters.

Keywords: *Information hidings, Audio Steganography, Image Steganography, Video Steganography, DNA Steganography, Network Steganography.*

1. INTRODUCTION

Presently, an unlimited and easy communication of digital data (video, audio, image, text, network, etc.) over the internet became possible via the World Wide Web (WWW). Meanwhile, such free access to the vast amount of information has posed severe threats in terms of the secured and privacy preserved communication over the WWW, thereby securing the information over the non-secured network became challenging. Often, attackers or adversaries can corrupt the information by manipulating the message, causing financial or ethical damages [1, 2]. Thus, to attain secured data communications, various information encryption and hiding schemes have been developed [3]. Figure 1 shows the classification of various security systems proposed so far.

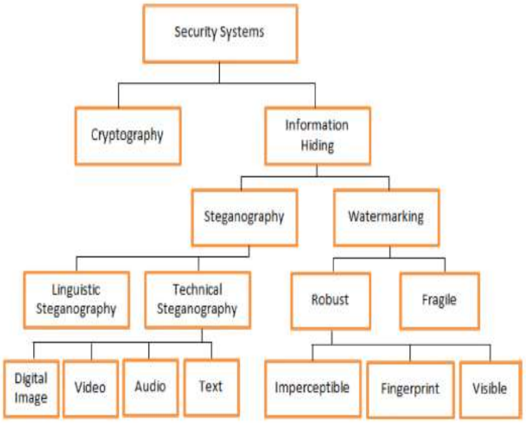

Figure 1. Classification of various security systems [4].

Information hiding domains are of two types, including steganography and watermarking [3,4]; both are used to hide the secret message. In addition, these two methods have a close relationship, but each has its objectives.

Watermarking is aimed at preserving the integrity of the secret data via keeping the knowledge of the existence of the communication from outsiders [5] while steganography refers to the act of concealing information via hiding the secret message in a public cover media without any evidence of its existence [3]. In the information encryption process called cryptography, the secret message is scrambled in a way to make it unintelligent (encrypted) communication to the eavesdroppers [6]. However, an encrypted secret message is often inapplicable, drawing the attention or making it visible to the eavesdroppers [4].

Steganography is coined from 2 Greek words - steganos (meaning covered) and graphy (meaning writing) [7]. The Greek historian, Herodotus presented the first written description of steganography in 440 BC [4]. Numerous scholars have developed several information hiding schemes over the years. For the ancient Greeks, they write messages on wood tablets and protect them from public view by covering them with wax. They also used the method of scripting the message on the shaved head of the messenger to be sent when the hair has re-grown [8]. The Germans came up with the microdot technology during World War 1 by using several non-suspicious cover materials to conceal their messages [7]. Invisible inks were used during World War II to script messages. German spies also used open-coded messages during World War II to avoid suspicion [9]. Several studies have documented the history of steganography and readers are referred to some of these works [4, 10, 11, 1] for more information about steganography. Nowadays, internet availability and powerful computers have seen to the development of steganography as an adaptive embedding scheme in different cover media like audio, text, DNA, video, network and images [12]. The goal of this paper is to study and discuss recent works on different types of 1 steganography method. Matrices of various performance measures and their counterparts are also discussed as steganographic analysis attacks. Finally, the research directions of the aimed study were presented in this study.

The organization of this study is as follows: Section 2 is the overview of steganography, its properties and key issues, as well as types. Section 3 explained steganalysis science and its categories. Section 4 presents the research directions of steganography. Finally, the conclusion is discussed in section 5.

2. STEGANOGRAPHY: A PREVIEW

Steganography is an intelligent data hiding technique where the secret data is embedded in a cover media in a way that the media carrying the secret message are undetectable and unnoticed by the intruder or attacker [4]. The message will be unintelligible even if it is detected. In the context of the digital world, the aim of both cryptography and steganography is to hold and save the secret message and protect it from hackers or attackers [12]. These techniques are useful when performed together or alone. Their combination also gives excellent output but should be in multiple layers to ensure high security. Different data formats are used with digital steganography nowadays, such as text, image, DNA, network, audio, and video [13]. When considering this scope of steganography, it can be imagined that the importance of modern steganography, especially with the internet, is for both security and integrity. Due to strict rules imposed by authorities and their impediments, the durability of cryptosystems in the cyberspace group has been weakened [4]. This is the reason why we need steganography where the sent message is secure and cannot be extracted by an intruder from the host media except with the appropriate key. To the best of our knowledge, among the various digital steganography types, image steganography remains the commonest medium because of its high ability to conceal the secret data in the cover media with invisible effects [7].

2.1 Properties of Steganography

The expansion of digital steganography has increased the importance of evaluation methods. The existing steganography evaluation schemes are characterized by their imperceptibility (visual quality), robustness, undetectable/security, payload capacity, and complexity. As mentioned earlier, digital steganography based on the carrier has been divided into six types, and since image steganography is the most used type [14, 4], this section will discuss the evaluation metrics of digital image steganography.

A. Imperceptibility: Without a doubt, the visual quality of cover images is significantly reduced beyond human eye recognition following the embedment of secret bits in them. To determine if the steganographic method is perceptually transparent or not, standard measuring procedures that can estimate or judge the visual modification levels are required [4.12]. However, numerous metrics have been developed for visual quality assessment in the area of digital steganography; these include MSE, RMSE, PSNR, WPSNR, Q, SIMM, NCC, and IF). These metrics are listed with their formulas in Table 1.

Table 1. A different evaluation metrics of information hiding

Evaluation Metric	Formulation
MSE	$\frac{1}{H*W}\sum_{i-1}^{H*W}(C^i - S^i)$
PSNR	$10log_{10}\,(\frac{Max^2}{MSE})$
RMSE	$\sqrt{MSE}$
WPSNR	$10log_{10}(\frac{\max(p(x,y)^2}{MSE * NVF)})$
NCC	$(\frac{\sum_{i=1}^{W*H}(C_i*S_i)}{\sum_{i=1}^{W*H}(C_i)^2})$
IF	1- $(\frac{\sum_{i=1}^{W*H}(C_i*S_i)}{\sum_{i=1}^{W*H}(C_i)^2})$

B. Embedding capacity (EC): This metric reflects the maximum number of secret bits that can be hidden per pixel of the cover media [12]. It is expected that a good cover media should have a high EC while ensuring imperceptibility and other evaluation metrics. Embedding capacity can also be referred to as embedding payload.

C. Security/undetectability: This is another important metric in digital steganography; all steganographic methods may sometimes suffer from different forms of steganalysis detection attacks as attackers always strive for novel ways of detecting the presence of secret bits in the stego-image. There are various methods of steganalysis methods that will play a prominent role in the retrieval of secret bits within cover objects, including (i) Visual steganalysis, (ii) Standard steganalysis, and (iii) Non-standard steganalysis [15].

D. Robustness: This metric is ideally measured in the transform domain; however, different steganographic schemes in the spatial domain are being considered recently when designing a scheme. Robustness is the ability of stego-images to retain the secret data even when subjected to sharpening, rotations, cropping, blurring, scaling, and noise addition [3,6].

E. Computational complexity: In steganographic techniques, computational complexity refers to the efficiency of algorithms used for the embedding and extraction stages of the process in terms of operation and time. Algorithms with low computational complexity are mostly preferred, such as the spatial domain-based methods. However, some methods that are based on machine learning require high computational ability because the embedding step is done using artificial intelligence algorithms [16].

2.2 Types of Steganography

Steganographic methods as mentioned previously can be categorized into six types based on the nature of the cover objects; these are text steganography, image steganography, audio steganography, video steganography, DNA steganography, and network steganography [4,12,13]. The following sub-section illustrates the six types in details.

A. Text Steganography

This type of steganography refers to the use of text files as the cover for secret data; the process may involve altering the text in terms of its format, wording, or generation of random character sequences to create readable texts. Data embedment into texts can be done using different methods, such as the format-based method, random and statistical generation, as well as the linguistic method. Several scholars have reported text steganography in various research efforts as reviewed below.

Al-Nofaie et al. [17] reported the embedment of secret data using Kashida and spaces between words. This method inserts Kashida between characters that can be connected if the secret bit is 1. Two whitespaces are also introduced between words if the secret bit is 1 before moving to the next word. If the secret bit is 0, nothing is added between words. The use of two white spaces which may elicit suspicion about an alteration to the text is the major disadvantage of this method.

Al-Nofaie et al. [18] further extended the capacity of the early method by introducing the insertion of 2 consecutive Kashida between connected characters when the secret bit is 1. Two pseudo-spaces are added between characters that are not connected. With this method, the capacity is increased as both the connected and unconnected characters are used to insert Kashida and ZWNJ to conceal the secret data. However, a major disadvantage of this method is that the insertion of several Kashida in one word may elicit suspicions since it is not a common practice in Arabic texts.

Alhusban [19] suggested an approach to secret its embedment via the insertion of Kashida between letters (pointed or un-pointed letters). During the embedding process, two tables are used to determine how to add Kashida in 4 possible combinations of a pair of secret bits (00, 01, 10, 11). The rules defined in the first table govern the first half of words in the cover text, while the rules in the second table govern the second half of words. However, the hiding of secret bits in this method depends on the insertion of Kashida between characters that are not connected, meaning that most of the unconnected characters cannot be used. Furthermore, this method overlooks many characters as their nature implies that they cannot match a case for Kashida insertion. Hence, this method has a payload of < 2 %.

An embedment method that hides secret data within Urdu cover text has been presented by Abbasi et al. [20]; this method relies on the Urdu letters in a cover text for hiding secret bits using the Unicode Standard. The product of the embedding process in this technique is imperceptible as it is not visibly different from the corresponding cover text. However, the problem of this method is the low payload (< 0.80%) due to the use of only isolated letters for secret data embedment.

B. Image steganography

In this type of steganography, secret data is hidden in the image as a cover object. Images are used in this process as a cover source due to the number of bits in the images' digital representation. Images can be used in three different ways as cover objects to hide information; these are spatial domain, frequency domain, and adaptive domain.

Various studies have used images as cover objects to hide secret data; for instance, Yang et al. [21] proposed contrast enhancement of medical images which had hidden data inside them. The proposed method could hide the data into a smooth region of images with improvement in the visual quality of the stego-image. The prime step of the proposed method was the use of the histogram shifting method for hiding information in the texture area of the image and the use of a contrast enhancement method for improving the visual quality of the image. The authors compared the proposed method with the other reversible data hiding method that also used histogram shifting. The authors used the peak signal to noise ratio as an objective parameter. From the results, it was clear that the proposed method performed better in comparison to the other methods.

Punidha et al. [22] used the concept of integer wavelet transform for sending audio speech signals through the steganography technique. The authors used the well-known Haar wavelet method with the integer wavelet transform for hiding secret messages. The authors used various objective parameters, such as signal-to-noise ratio, MSE, PSNR, and structural similarity index to evaluate the performance of the proposed method. The LL band of wavelet was used to store the data inside the image while the Daubechies method, along with the Haar, was used for comparison purposes. The algorithm with the Daubechies method performed better in comparison to the Haar wavelet method.

Vardhan et al. [23] proposed a reversible steganography technique that was based on the wavelet transform. They used the integer wavelet transform method on the encrypted digital images. The authors also performed mapping of integers with the cumulative density functions. Further, they used the sub-band of the encrypted image to store the secret message inside the cover image. The authors used the concept of histogram shifting for performing the steganography. The proposed method was compared with the other known steganography methods like logistic mapping and least significant methods. From the results, it was clear that the proposed method outperformed the other methods.

Yin et al. [24] performed steganography using reversible data hiding. The study performed steganography in encrypted digital images with the classification permutation. The permutation method used the XOR encryption and then data was embedded into the most significant bit of the encrypted image. With this approach, the visual quality of the recovered original image was very good. The authors compared the proposed algorithm with the other known methods of reversible data hiding like the Zhang method and Wu method. With the results, it was shown that the proposed method showed lossless recovery of the original image even when the embedding rate was higher.

Manikandan et al. [25] used the concept of encryption for obtaining the image and message from the stego image using the reversible data hiding technique. The authors performed the research on medical digital images. They saved the data of patients into the concerned medical images of the same patient and the advantage of it was that there was no need of sending patient data into another file. The main aim of the proposed method was to get good data embedding capacity and the method should have a low bit error rate in comparison to other methods. In the encryption mechanism, the authors used three keys to share data between sender and receiver. From the results, it was shown that the proposed method had good embedding capacity and took less time of execution.

Dhande et al. [26] proposed a reversible steganography method that was based on an encryption mechanism. The main utilization of the proposed algorithm was for the gray scale digital images which could hide the images in the cover image with the help of a suitable encryption mechanism. The authors used two keys for performing steganography. One key was used for hiding the data and another for encrypting the data. The authors used the advanced encryption standard method for performing the encryption in the digital images while the least significant method of steganography was used to get the accuracy and efficiency in the proposed approach.

Marella et al. [27] utilized the well-known least significant method for secret data hiding in the human faces. Authors tried to store the message into the various texture features of the human face, like eye, nose, and mouth. First, the authors tried to find the maximum region available out of various texture features of the face. Then, they tried to save the secret messages in those free spaces. Authors first used encryption to encrypt the message which had to be hidden in the image. From the results, it was shown that the proposed algorithm could store the data in the facial features of the human face, and it was not easy to detect the presence of some hidden data inside the digitally encrypted image.

Benedict et al. [28] enhanced the file security with the help of multiple image steganography. In this paper, the authors proposed a way to store various images inside a single cover digital image. The authors used the image sequential hashing concept in which it was difficult for an intruder to judge whether the given pixel belongs to a given image or another image. The authors used the ZIP file format to compress the file. They used the file size of the image before and after steganography and the execution time of the algorithm as objective parameters. The study showed that after performing steganography, the size of the final stego-image was comparable to the original image.

Elharrouss et al. [29] utilized k-least significant bit of cover image to perform steganography. Authors stored one image inside the other cover image. First, at the sending side, the most significant bit was selected which could be stored in the cover image, and in this way, a complete secret image was hidden in the cover image. On the decoding side, the authors used the concept of region detection. Here, an algorithm is used to search the various regions where the data of the secret image was hidden. Peak signal to noise ratio was used as an objective parameter. The proposed algorithm however performed below the expected level.

Rafiqi et al. [30] proposed an image steganography technique that was based on the use of the Grey Scale Co-occurrence Matrix. The authors used the well-known principal component analysis to detect edges so that information can be stored in them. Authors performed encryption on text data before hiding it into the cover image. Various objective parameters like peak signal to noise ratio, mean square error, and entropy were used for the performance evaluation of the proposed algorithm. From the experiments, it was clear that the value of peak signal to noise ratio and mean square error was better in comparison to other methods.

C. Audio steganography

Audio signals are used in this method as the cover to hide secret data; this embedment alters the binary sequence of the used audio file. This is a more difficult task when compared to image and text steganography. Audio steganography can be done using different methods such as least significant bit encoding, parity encoding, phase coding, and spread spectrum. This method hides the data in WAV, AU, and even MP3 sound files. The following discussions explained different methods of audio steganography.

R. Indrayani, H. A. Nugroho, and R. Hidayat, [31] Least significant bit (LSB) are one of the classical methods commonly used for steganography audio. Because of its simplicity, many researchers have been interested to develop it. This investigation aims to determine the maximum limit of adding bits and its effects on audio quality based on the modified LSB method consisting of LSB+1, LSB+2, and LSB+3. Then, this method is evaluated by counting steganography capacity, peak signal to noise ratio (PSNR), and bit error rate (BER) values. Evaluation results show that LSB+3 has the best performance by obtaining the maximum bit of steganography capacity and acceptable PSNR value.

Datta & Bandyopadhyay [32] stated that the embedment of secret “data in the same LSB position of consecutive samples help intruders to easily extract the hidden information. So, they proposed the introduction of a robust audio steganography technique for hiding secret data in multiple layers of randomly chosen LSB and in non-consecutive samples to improve the robustness and strength of the process. They solved the problem of data hiding at non-contiguous sample locations which causes loss of the capacity of stego audio by proposing the hiding of three bits in a target sample. They also increased the capacity by using “6 bits ASCII representation of the secret message” rather than 7. To evaluate the proposed technique, the authors embedded texts of different payloads in the cover audio and made comparisons with the other embedding methods in terms of capacity and” quality.

Al-Bayati & Al-Jarrah [33] presented the DuoHide as a model for hiding secret data in multimedia files irrespective of the type. The file is processed in an uncompressed form and “divided between two cover images of similar sizes. Before hiding the file in the multimedia file, the media is first split into two parts, one part containing the most significant half-bytes and the other containing the least significant half-bytes. Both parts are hidden in 2 RGB cover images (uncompressed) using a least significant 4-bit replacement method. The two stego images produced are transmitted via different channels to keep them from being intercepted by an adversary. The secret file is extracted by combining the LSB half-bytes from the two stego files, in this way, the extracted file shares close similarity with the original secret file in terms of structure and content. The evaluation of the proposed DuoHide system on public multimedia files of different sizes showed that there was a clear and visible difference between the cover and stego images even at the highest embedding ratio.” Hence, the proposed DuoHide model can ensure better security of the secret data because even if an attacker succeeded in intercepting one of the stego images, the information will still be incomplete since the attacker has not captured the other set of data from the other half-byte bits. The use of a pair of stego files also reduces the size of the required stego file by 50%; this avoids the issues surrounding the transmission of large files that cannot be compressed further. The performance of the DuoHide system, in terms of security, can be enhanced by randomizing the storage locations within the 2 stego images.

Sharma & Thakur [34] noted that in the present scenario of extensive mediums for communication technologies, it has always been a challenging task to ensure the confidentiality of the sensitive information that is transmitted over a secured channel. They also noted that amongst various reliable and efficient techniques to secretly exchange information, audio steganography is considered very promising. The study then proposed a Random Key Indexing method to replace the LSBs of the carrier audio with a secret message. The bit replacement is guided by a primary key that is provided by TTP (Trusted Third Party) and a secondary key that will be generated at the encoder end during the embedding process and is supplied to the decoder end. The proposed method also uses message retrieval code that adds another layer of protection to the process. The method is successfully tested on various 32-bit & 16-bit stereo wave files with different payloads. The SNR dB values came out in the range of 139 dB to 142 dB for 32-bit and 67 dB to 85 dB for 16-bit stereo files. The Bit Error Rate (BER) was in the range of 0.23 to 0.32 % for 32-bit and 0.018 to 0.028 % for 16-bit files.

Abdelsatir & Abushama [35] proposed a new spatial domain-based audio steganography method using a transparent LSB matching approach. The scheme was evaluated using standard algorithms and other audio steganography tools. The proposed scheme achieved better transparency rates than the comparative tools based on image LSB matching methods. The hidden information in the proposed method also left no evidence of steganography use during the subjective listening tests; hence, there was no detectable auditable noise in the host audio signal.

Binny & Koilakuntla [36] presented a steganographic method for text embedding in audio using LSB based algorithm. In this method, each audio sample is transformed into bits before embedding the text data. The first step of the embedding process is the conversion of the message character into the corresponding binary before using the proposed LSB-based algorithm to do the embedding; this improves the capacity of the stego system. The evaluation of the proposed algorithm was done using metrics like SNR values for different audio inputs.

Mandal et al [37] presented an audio steganographic method for hiding data in the LSB of the stereo-audio samples. In this method, the message bits are encoded into the cover audio files using stego-keys. The method was presented as an improvement on the security and imperceptibility of the LSB method for audio steganography.

The study by Marwa Tarek, & Wassim [38] proposed the encryption of secret messages using AES–128 before LSB embedment in the cover audio using a Logistic map-generated sequence. The performance of this scheme was evaluated using MSE, PSNR, waveform plots, and a hearing test.

Bit permutation of messages before steganography was proposed by Jayaram & Anupama [39]. A validation step was also introduced for a checksum at the receiver end to ensure the imperceptibility of the secret message or being intercepted by an attacker. The method was evaluated using MSE, PSNR, and a χ 2 calculation as performance metrics to determine the probability of message interception.

The combination of RSA and LSB for audio steganography was proposed by Gambhir, Ankit, & Sibaram Khara [40]. The authors only reported waveform plots as the metric for the performance evaluation of the method.

In [41], the use of LSB coding and encryption was proposed for hiding secret information in cover audio. The LSB method utilizes the parity of digital cover audio files while the encryption step uses XOR operation. Authors in [42] also developed two double-layer schemes for message security in which a cryptography layer is the first layer (uses AES–128) while the steganography layer is the second layer (uses LSB substitution). The method was evaluated using similar metrics as found in [38].

A mix of text encryption, audio encryption, and audio steganography was proposed by [43] for hiding secret data. A modified Vigenère cipher algorithm was first used for the encryption of the original text before LSB embedding the ciphertext in the cover audio. The “Blum Blum Shub pseudo-random number generator” is then used to perform transposition on the stego audio before transmitting the encrypted stego audio to the receiver. The evaluation of the scheme was done via the provision of the stego audio file that contains the encrypted text, waveforms of the original audio file, as well as the post-transposition encrypted stego audio file.

A multilayer security method that merged RSA cryptography with dual audio steganography was proposed by [44] for improving security levels. Another study by [45] presented a scheme for audio steganography in which the locations for data hiding are randomly selected to ensure they change with every new embedding process.

Authors in [46] also presented a scheme for audio steganography that relies on a random mechanism and the PKE algorithm for better security. Cryptography was also combined with steganography in the proposed approach.

D. Video Steganography

Video steganography is the use of digital video to hide any kind of data. This method is beneficial because of the possibility of hiding a large amount of data in a video file since a video file is a moving stream of sounds and images. So, video steganography can be seen as a hybridization of image and audio steganography. Video steganography can be done in two ways which include data embedment in uncompressed raw video and subsequent compression of the data, as well as direct data embedding into an already compressed data stream.

Cheddad et al. [47] coined the term "method of skin tone information concealment" to describe a video steganography technique based on the YCbCr color space. The Cr components are utilized to hide the hidden secret data to preserve the utilized skin area. The PSNR value served as the metric to determine the quality of video steganography, with the value ranging from 53.9535 dB to infinity (Inf: Stego image is identical to the original image) across all the tested databases. In addition, the embedding capacity (bits) ranged between 1368 and 3600 bits. The major problem of the suggested method is that the confidential message is only embedded in the Cr component of the skin.

A video steganography technique for secure communication has been proposed by Hanafy et al. [48]. This technique is used in the spatial domain. Furthermore, the secret data is divided into non-overlapping pieces and then hidden (using a secret key) within the video frames. The secret data is constantly randomized within each video frame to prevent an intruder from locating the exact location of the secret data. The data embedding process was accomplished by using the two least significant bits (LSB) from each RGB color channel to hide six bits in each pixel frame of the secret message. Confidential information is protected in this technique by utilizing a secret key. However, this approach conceals the hidden information by using the spatial domain. The video quality for different resolutions varied based on the PSNR for each cover. The PSNR value ranges from 51.57 to 53.58 dB when using text as the secret information; 50.44–65.56 dB when using an image; 50.86–59.3 dB when using audio; and 50.94–52.58 dB when using video as the secret message. The noise and compression levels are significantly reduced.

Tadiparthi et al. [49] proposed a steganography technique that uses animations as the cover object. The limited message is hidden in animation video frames in this method. This technique outperforms the two current algorithms (Gifshufe and Animated-Digital Invisible Ink Toolkit), which are discussed in this work. "The probability distribution of a secret message is dependent on a secret key, and the distribution of a secret message cannot be modified. This procedure also takes a long time to complete, making it more complicated. The proposed approach has a 2 percent average hiding capacity ratio.

Cetin et al. [50] describe two new steganographic methods that are based on similar and dissimilar histograms. The histogram rate is critical for distinguishing between these two concealment techniques, which are derived from each video frame. In addition, two new strategies are provided, namely frame-based and block-based procedures, to seek the critical characteristics, namely concealing data capacity (HDC) and the number of modified bits. In a comparable histogram approach, frame-based techniques fared better, whereas block-based techniques performed better in different histogram approaches.

Cheddad et al. [51] used skin tone recognition-based video steganography as an adaptive methodology in which the luminance component Y is extracted from an RGB color image. The proposed algorithm then separates the skin tones, which is then employed as a host to insert the encrypted data." The average PSNR of the resulting steganography was 41.9245 dB.

Mritha [52] proposed the use of a stego machine to create video steganography apps for hiding secret information. using the LSB alteration methodThe proposed embedding algorithm successfully hides text while keeping the visual quality of stego video. This strategy uses subtle changes to keep secret information out of the hands of illegal authorities.

A Hash-based LSB (HLSB) video steganography approach has been proposed by Dasgupta et al. [53]. The 8-bit confidential data is divided into three sections, each of which is hidden in the LSB of RGB cover frames. The [54] is to be dispersed in a manner that the chromatic impact of a blue pixel is greater on human eyes than the red and green pixels. As a result, stego video visual quality is not improved, but payload capacity can be increased. The PSNR value achieved using the HLSB approach is in the range of 42.66–45.67 dB, which is higher than that produced using the conventional LSB method. A data concealing method that uses LSB and byte randomization approach have been presented by Bhole et al. [54]. The first frame of a video sequence is utilized as an index frame in this method to control the data of various frames, while the remaining frames are used to hide the secret data. The LSB method was also implemented in this technique but being that implementation is in the spatial domain, it is the least resilient.

In LSB-based steganographic approaches with a reversible histogram transformation function were presented by Lou et al. [55]; this approach is resistant to statistical techniques such as Regular-Singular (RS) attacks and x2-detection.

Zhang et al. [56] employed BCH encoding-based embedding, which turns data into a block that can be used as a cover object. The different input block coefficients are altered to make the syndrome value null and hide the secret data. When compared to other methods, this method achieved a higher embedding capacity.

Moon et al. [57] used computer-based forensic methods to develop a technique for hiding secret data. confidential data is hidden in 4 LSB using this technique. The confidential data is encrypted in a video frame using a key that can be identified by both the sender and the receiver. A computer forensic method is used to determine the validity of the stego video. Because it uses the spatial domain, this technique is not resistant to noise, video compression, or signal processing. The implemented approach has a 12.5 percent average hiding capacity. Using histogram variation, Kelash et al. [58] developed a video steganography method. This method uses a constant histogram value as a threshold value to hide confidential data. The variations of the successive pixels were computed by partitioning the video frames into blocks. The sensitive information is encoded in the first three LSB of each pixel value. For using only the HCV value as the carrier object, the technique has a limited hiding capacity; the proposed method was evaluated and the achieved average PSNR value was 48.425 dB.

Paul et al. [59] proposed a steganographic method based on a video stream in which video frames are used as the hosts and the selection of the video frame is based on histogram variation and abrupt scene fluctuation. The secret information, after conversion, is hidden in the 3–3–2 LSBs of each pixel'. Even though the suddenly altered scene has a limited number of pixels, these randomized locations of the abruptly altered scene's pixel boost the security level of the stego image.

Dasgupta et al. [60] used a genetic algorithm (GA)-based optimized technique to increase the video quality and the security of the secret data of the steganogram. An objective function based on multi-parameters like MSE and HVS is the driving force behind the development.

The approach presented by [61] is not resistant against disturbances, signal processing, or compression because it uses the spatial (pixel) domain. The suggested method achieved an average payload of 8 bpp and a PSNR value of 38.453 dB. Instead of employing a whole frame, Khupse et al. [61] created a method that uses steganofage to hide data in the Region of Interest (ROI) frame. Human skin-tone detection was employed as a carrier object in this method to conceal the hidden information. The filling procedure and morphological dilation approach are utilized to remove the face region. Following that, the YCbCr frame is picked for the concealment step since it has a lower MSE. The Cb section of the video frame is picked to hide information in a frame. Because only a single frame is used for the data concealing stage in this technique, the payload is low. The stegnofage-based approach achieved an average PSNR value of 85.18 dB, and a payload of 2120 bits per video, which is considered low.

Ramalingam et al. [62] developed a video steganography system that uses an Enhanced Hidden Markov Model (EHMM) to improve the rate of recovering hidden information. The embedment and extraction operations are divided into two steps: (1) identification of the conditional states in the selected video frames; and (2) computation of transitions between conditional states in a sequence. By reducing the time to hide data by 3–50%, enhancing the security by 4–77%, and improving the rate of data retrieval by 22–77% at the base computational cost of 20–91%, the suggested technique is considered efficient in terms of performance. Mustafa et al. [63] developed a tracking-based video steganography algorithm by employing the Hamming code called Kanade–Lucas–Tomasi (KLT) (15, 11). The four stages of this strategy are as follows: (1) preprocessing of the secret message to produce an encoded message using Hamming code (15, 11); (2) detection of the face and its tracking over the selected video frames to establish the ROI; (3) embedment of the encoded secret message in ROI using the adaptive LSB substitution approach. To hide 3, 6, 9, and 12-bits of confidential data, the author used 1 to 4 LSBs respectively, of facial pixels; (4) extraction of the secret message from the RGB components of the face region for stego video execution.

Sun [64] developed a new information concealment method based on enhanced BPCS steganography. The general BPCS technique computes the difficulty level based on the black-and-white border of a selected area. BPCS steganography using DWT has also been demonstrated by Noda et al. [65]. The two coding methods used in the DWT domain are Motion-JPEG2000 and 3D set partitioning in hierarchical trees (SPIHT). This method divides the bit planes of the video and secret frames into 88 blocks. Then, the bit-plane blocks are selected based on the noise threshold value. The BPCS technique is used in the above techniques to hide secret data in quantized DWT; this is normally implemented on bit-plane blocks. The empirical evaluations showed that the performance of 3D SPIHT coding in terms of achieving a higher payload is better than that of Motion-JPEG2000 coding. However, this approach has several disadvantages, viz. different cover films do not contain sufficient noise like bit-plane blocks; it can be applied only in the wavelet-based compression domain; the complexity level is high compared to the spatial domain.

E. DNA Steganography

Kar et al. [66] devised a DNA-based technique for transmitting data hidden within a video file. The first step is the conversion of the video footage into image frames. Then, using the LSB substitution approach, random frames are selected for data embedment at random positions. “The steganographic video file demonstrated low degradation but achieved poor data hiding capacity and payload that was not equal to zero. Mumthas et al. [67] proposed combining RSA, Huffman encoding, 2D DCT steganography, and random DNA encryption to create a system with three levels of guaranteed security. The strategy was discovered to increase the quality of the steganographic system and decoding the codes, which was considerably more onerous when compared to other approaches.” A combination of cryptography and steganography concepts based on molecular biology concept was demonstrated by Hamed et al. [68]; the proposed method was well-secured and achieved a high payload capacity, preserved algorithm. The performance was satisfactory but there is a higher level of redundancy and increased message size which reduces scalability.

Mondal et al. [69] chaos-based steganographic technique that relies on random bit creation and DNA computation; this method produces random DNA sequences using a cross-coupled chaotic map. The secret DNA sequence was used to replace the LSB of the cover image pixels. The method performed admirably; however, it must send repeated data to the recipient to retrieve the secret message from stego-DNA.

A Hyper-elliptic Curve Cryptography (HECC)-based steganographic method was created by Vijayakumar et al. [70] which provided a greater level of protection to image files and ensured the security of digital materials. A comparison of the method with the traditional method showed that the proposed method required about % 30% and 42 % more time to complete the encryption and decryption processes, respectively.

F. Network Steganography

Network steganography is the process of information embedment within the network control protocols that are employed for data transmission; such protocols include TCP, UDP, ICMP, etc. Some covert channels in the OSI model can also be used for steganography. For instance, information can be hidden in the TCP/IP packet header in some optional fields. Various tools are available today for steganography; the rest of this review will focus on the capabilities of some of the popular steganographic tools.

A new network voice-based steganography model was proposed by Huang & Tang [71] for covert communication space. The system uses a spatial model to solve the problem of packet loss by employing a quick-start retransmission technique. The communication parties can share the currently used hidden vector across a secret channel using the time and space negotiation mechanism. Data hiding is done using only some media packets in the senders’ media stream; the receiver is required to identify the streaming media that hosts the secret data, as well as the hidden vector used to hide the secret data [72]. The receiver can directly extract the hidden message upon identifying the hidden vector used in the streaming media packet. With this method, the problem of improving payload, imperceptibility, and synchronization efficiency was solved without impact on channel concealment.

An “information hiding technique was proposed by Gong [73] which was based on IP phone transcoding; this method compresses public information to have more space for data hiding. The first step is the analysis of the payload of the RTP protocol header before deciding whether to detect the voice of the user in the RTP packet or to encode the original voice. An appropriate codec is ten used for public encoding that will generate the voice stream that resembles the original voice in quality, but with a smaller payload. The voice stream is finally transcoded into the original payload field, while the remaining space is available for data hiding. Jiang et al. [74] developed a UDP-based VoIP communication scheme in which a prediction model is first established based on fractal interpolation for the determination of the suitability of the VoIP packet for data hiding. The original data will be retained if it is determined that the VoIP data is not suitable for data hiding. Else, the DEA of the variable embedding interval of the AES will first be hidden before encrypting the secret data using a block cipher. The data is later divided into multiple groups for embedding in the VoIP stream data packet. The actual network environment is then simulated with the Gilbert model to handle the issue of data packet losses. The evaluation showed that increases in the degree of packet loss cause a gradual decrease in the mean-variance of the voice quality metric (PESQ score) between the 'unembedded' voice samples and the 'embedded' voice samples, showing improvement in the security" of the secret data.

Lu et al. [75] came up with a network steganography scheme that relied on the UDP packet length via analysis of the UDP packets flow and other data files storage characteristics. In this method, some data packets are first sent by the sender. The secret data is sent with the data packet length because of the randomness of the packet length distribution [76]. Multiple IP addresses are then sent through the router. Some fake packets are also introduced to confuse the monitor and enhance the security of secret data transmission. This is done using random coding technology because it can simulate usual traffic better and overcome the problems of the present solutions.

Sabine & Wojciech [77] developed the StegVAD algorithm for improving the channel capacity without any impact on the quality of VoIP sessions. This method converts the "Voice Activity Detection (VAD)-activated VoIP stream of voice activity detection into a non-VAD VoIP stream." Then, the timestamp and sequence number during the silent period is increased to generate fake RTP packets by the encoder. This system achieved improved channel capacity, but the robustness and anti-detection performance were not adequate.

Deepika & Saravanan [78] presented a hash-based system for data hiding in which "voice stream is first obtained from the UDP protocol before constructing the hash array from the frame data. The hash array for each new frame must be updated. Then, the secret data is cut, followed by the selection of the appropriate bit position based on the hash function to embed the secret data. Upon full embedment of the secret data, the value of the hash array is set to 0. Then, the hash array and audio samples are sent as a VoIP frame to the receiver for subsequent extraction of the secret message using the hash array flag value. The algorithm performed well in undetectability, computational complexity, and voice quality on the side of the sender and receiver." The problem is the extra bandwidth taken by the hash array in the VoIP communication process.

3. STEGANALYSIS

The art and science of uncovering the secret bits hidden by steganography are known as steganalysis [12,4]. Steganography and steganalysis are always incompatible with one another. When an optimal steganographic scheme is created, steganalysis is created as a countermeasure to defeat or study the embedding processes [66]. If any steganalysis reveals the presence of hidden bits inside the embedded digital object, the basic aim of steganography is defeated. Detection assaults are conceivable in steganalysis, even though the "embedding methods are visually transparent to human eyes in image steganography. The introduction of ranges of visual artifacts by steganographic schemes during an embedding process causes some unusual variations in the features of the stego-image, such as imperceptibility. Such variations are exploited during steganalysis to detect the presence of secret data. There are two common methods for steganalysis which are passive and active steganalysis [58]. During passive steganalysis, the aim is to identify the presence or absence of the secret data or the embedding process, but in active steganalysis, it aims to either modify or recover the secret data; sometimes, the aim is to determine the secret data length. Literature evidence suggests the existence of both statistical and non-statistical methods of steganalysis; most of these methods are designed" for specific use while some are universal in their design.

Some of the employed test analysis and detection attacks used in literature to evaluate the security of new steganographic schemes are discussed in this section. Some of the basic analysis techniques are also detailed in this section.

1. Visual steganalysis: Steganographic methods are expected to exhibit some levels of perceptual invisibility. Some of the salient visual artifacts must be rendered invisible to the human eye after embedding. Hence, several visual quality metrics are used to determine the visual quality measures of a steganographic process and most of the ones used are MSE, PSNR, SSIM, Q index metrics.
2. Statistical steganalysis: The structural features of images are exploited here to detect unusual features that result from the steganographic method. Different statistical analysis methods are available, such as histogram analysis, sample pair analysis, bit plane analysis, etc. fr easy identification of the presence of secret bit and secret bit size estimation.
3. Non-structural steganalysis: Here, the cover image is modeled using a feature extractor

before estimating the level of "distortion between the cover and stego-image; this aids in detecting the location of the embedded secret data. In this method, feature set selection can be either steganographic-oriented or universal. The feature set is generally trained using a machine learning-based classifier in a manner that learns the feature variations between a stego-image and a larger dataset of the cover images. Subtractive pixel adjacency matrix (SPAM) and spatial rich model (SRM) are the common forms of non-structural steganalysis [33]. SVM is normally used as the steganalyzer while ensemble classifier can be trained via the supervised training method and used as the classifier." There are numerous feature-based steganalysis methods in the literature [38].

4. RESEARCH DIRECTIONS

Image steganography faces the major problem of hiding secret bits in the cover image with minimum detectability, high security, robustness against alteration/interception, and high payload. Despite the research effort in this domain for some time now, it is still a problem to achieve the above-listed requirements. A major issue is relatedness between these attributes as the mutual relationship between steganographic properties entails that while enhancing some properties, others are adversely affected. This issue persists due to the lack of a practical solution to achieve these properties at once. Some of the proposed methods for improving the performance of the existing steganographic methods are given below:

1. Hybrid steganographic techniques: The combination of several steganographic methods into one method may improve data security and confuse specific steganalysis methods as the strengths of the combined methods will be exploited to address their weaknesses during the design of the hybrid method [22,40].
2. Merging of cryptography with steganography: This could add a layer of security to secret data as they will be encrypted first before embedding. An attacker may intercept the steganographic algorithm but will still have to contend with the cryptographic scheme to be able to recover the encrypted data [53].
3. Secured lightweight encryption-based steganographic techniques: As most of the existing steganographic techniques are prone to modern steganalysis, coupled with the high cost of secret data protection using the conventional encryption method, it has become necessary to design a lightweight encryption method that can protect secret data in a cost-efficient manner [27].
4. Additive noise distortion function reduction: This is another way of protecting the existing steganographic techniques from steganalysis. Most of the modern steganalysis methods deploy the method of computing the specific features of the cover and stego-images to determine their types. These distinctive features are mostly generated by additive noise in stego-images. Hence, there is a need to devise ways of minimizing this additive when designing new steganographic methods [57].
5. Merging of reversible and irreversible methods: This may improve payload and secret data security. Different reversible and non-reversible methods can recursively employ the same pixels at the same time, making it hard for the attacker to extract the secret data [12].
6. Location sensitive embedding: This is also called adaptive steganography; it has evolved recently as a way of improving payload, reducing distortion, and making a dynamic decision on special data during steganographic processes. However, this type of steganography needs more time to mature in the face of modern steganalysis [4].

5. CONCLUSION

This article reviewed several steganography techniques, focusing more on technical steganography and detailed classification. Digital steganography and its types were also discussed, as well as other review publications on steganography. A performance study of the existing digital steganography schemes was also performed based on the cover embedding techniques. Each of the reviewed schemes has some advantages and limitations. It can be concluded based on what the mentioned references indicated, the image steganography scheme will be more secure and more robust if the designed scheme is combined between spatial and frequency domain as well as preparing the secret text using a new encryption method to add a new level of security, also, the selecting image pixels should be in a Random way The most recent steganographic methods were reviewed and compared with most of the existing techniques based on their embedment and extraction processes. Considering the benefits and drawbacks of each of the reviewed methods, it is important to come up with a robust and efficient system that can perform well in terms of achieving a high payload, data embedding, and data reconstruction without much impact on data quality and data security.

REFERENCES

[1] RANDOM, STEGANOGRAPHY SCHEME USING TWO. "An Effective and Secure Digital image Steganography Scheme using Two Random Function and Chaotic Map." *Journal of Theoretical and Applied Information Technology* 98.01 (2020).

[2] ALRikabi, Haider TH, and Hussein Tuama Hazim. "Enhanced Data Security of Communication System Using Combined Encryption and Steganography." *International Journal of Interactive Mobile Technologies* 15.16 (2021).

[3] Dhawan, Sachin, and Rashmi Gupta. "Analysis of various data security techniques of steganography: A survey." *Information Security Journal: A Global Perspective* 30.2 (2021): 63-87.

[4] Kadhim, I. J., Premaratne, P., Vial, P. J., & Halloran, B. (2019). Comprehensive survey of image steganography: Techniques, Evaluations, and trends in future research. *Neurocomputing*, *335*, 299-326.

[5] Yang, Peng, Yingjie Lao, and Ping Li. "Robust Watermarking for Deep Neural Networks via Bi-Level Optimization." *Proceedings of the IEEE/CVF International Conference on Computer Vision*. 2021.

[6] Pirandola, Stefano, et al. "Advances in quantum cryptography." *Advances in Optics and Photonics* 12.4 (2020): 1012-1236.

[7] Saini, Ravi, Kamaldeep Joshi, and Rainu Nandal. "An Adapted Approach of Image Steganography Using Pixel Mutation and Bit Augmentation." *Smart Computing Techniques and Applications*. Springer, Singapore, 2021. 217-224.

[8] Mushenko, Alexey, Alexander Zolkin, and Aleksandr Yatsumira. "Steganography Analysis of Chaotic Carrier Signal Transmission with Non-linear Parametric Modulation." *2021 International Russian Automation Conference (RusAutoCon)*. IEEE, 2021.

[9] Alsaawy, Yazed, et al. "Double Steganography-New Algorithm for More Security." *2021 8th International Conference on Computing for Sustainable Global Development (INDIACom)*. IEEE, 2021.

[10] Taha, Mustafa Sabah, et al. "A Steganography Embedding Method Based on P single/P double and Huffman Coding." *2021 3rd International Cyber Resilience Conference (CRC)*. IEEE, 2021.

[11] AL-HALABI, YAHIA SABRI. "A SYMMETRIC KEY BASED STEGANOGRAPHY CALCULATION FOR ANCHORED INFORMATION." *Journal of Theoretical and Applied Information Technology* 98.01 (2020).

[12] Hussain, Mehdi, et al. "Image steganography in spatial domain: A survey." *Signal Processing: Image Communication* 65 (2018): 46-66.

[13] Taha, Mustafa Sabah, et al. "Information Hiding: A Tools for Securing Biometric Information." *Technology Reports of Kansai University* 62.04 (2020): 1383-1394.

[14] Wahab, Osama Fouad Abdel, et al. "Hiding Data Using Efficient Combination of RSA Cryptography, and Compression Steganography Techniques." *IEEE Access* 9 (2021): 31805-31815.

[15] ALRikabi, H. T., & Hazim, H. T. (2021). Enhanced Data Security of Communication System Using Combined Encryption and Steganography. *International Journal of Interactive Mobile Technologies*, *15*(16).

[16] AbdelWahab, Osama F., et al. "Efficient Combination of RSA Cryptography, Lossy, and Lossless Compression Steganography Techniques to Hide Data." *Procedia Computer Science* 182 (2021): 5-12.

[17] Al-Nofaie, Safia, Adnan Gutub, and Manal Al-Ghamdi. "Enhancing Arabic text steganography for personal usage utilizing pseudo-spaces." *Journal of King Saud University-Computer and Information Sciences* (2019).

[18] Al-Nofaie, Safia Meteb, Manal Mohammed Fattani, and Adnan Gutub. "Merging two steganography techniques adjusted to improve arabic text data security." *Journal of Computer Science & Computational Mathematics (JCSCM)* 6.3 (2016): 59-65.

[19] Ala'a, M., and Odeh Alnihoud. "AMeliorated KASHIDA-BASED APPROACH FOR ARABIC TEXT STEGANOGRAPHY." *Int. J. Comput. Sci. Inf. Technol.(IJCSIT)* 9.2 (2017).

[20] Abbasi, Aliya Tabassum, et al. "Urdu text steganography: Utilizing isolated letters." Australian Information Security Management Conference. Australia (2015).

[21] Yang, Yang, Weiming Zhang, and Nenghai Yu. "Improving visual quality of reversible data hiding in medical image with texture area contrast enhancement." *2015 international conference on intelligent information hiding*

and multimedia signal processing (IIH-MSP). IEEE, 2015.

[22] Punidha, R. "Integer wavelet transform based approach for high robustness of audio signal transmission." *International Journal of Pure and Applied Mathematics* 116.23 (2017): 295-304.

[23] Vardhan, M. Vishnu, B. Rama Krishna, and V. Thanikaiselvan. "IWT Based Data Hiding in Encrypted Images." *2018 Second International Conference on Electronics, Communication and Aerospace Technology (ICECA)*. IEEE, 2018.

[24] Yin, Bangxu, et al. "Separable reversible data hiding in encrypted image with classification permutation." *2017 IEEE Third International Conference on Multimedia Big Data (BigMM)*. IEEE, 2017.

[25] Manikandan, Vazhora Malayil, and Vedhanayagam Masilamani. "An improved reversible data hiding scheme through novel encryption." *2019 Conference on Next Generation Computing Applications (NextComp)*. IEEE, 2019.

[26] Dhande, Krutika, and Rutuja Channe. "A Brief Review on Reversible Data Hiding in Encrypted Image." *2019 International Conference on Communication and Signal Processing (ICCSP)*. IEEE, 2019.

[27] Marella, Pranay, Jeremy Straub, and Benjamin Bernard. "Development of a Facial Feature Based Image Steganography Technology." *2019 International Conference on Computational Science and Computational Intelligence (CSCI)*. IEEE, 2019.

[28] Benedict, Arnold Gabriel. "Improved file security system using multiple image steganography." *2019 International Conference on Data Science and Communication (IconDSC)*. IEEE, 2019

[29] Elharrouss, Omar, Noor Almaadeed, and Somaya Al-Maadeed. "An image steganography approach based on k-least significant bits (k-LSB)." *2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT)*. IEEE, 2020.

[30] Rafiqi, Abdul Yabar. "Features Analysis and Extraction Techniques for the Image Steganography." *Turkish Journal of Computer and Mathematics Education (TURCOMAT)* 12.8 (2021): 2103-2109.

[31] Indrayani, Rini, Hanung Adi Nugroho, and Risanuri Hidayat. "An evaluation of MP3 steganography based on modified LSB method." *2017 International Conference on Information Technology Systems and Innovation (ICITSI)*. IEEE, 2017.

[32] Datta, Biswajita, Prithwish Kumar Pal, and Samir Kumar Bandyopadhyay. "Multi-bit data hiding in randomly chosen LSB layers of an audio." *2016 International Conference on Information Technology (ICIT)*. IEEE, 2016.

[33] Al-Bayati, Marwa Tariq, and Mudhafar M. Al-Jarrah. "DuoHide: A Secure System for Hiding Multimedia Files in Dual Cover Images." *2016 9th International Conference on Developments in eSystems Engineering (DeSE)*. IEEE, 2016.

[34] Sharma, Vipul, and Ravinder Thakur. "LSB modification based audio steganography using trusted third party key indexing method." *2015 Third International Conference On Image Information Processing (ICIIP)*. IEEE, 2015.

[35] Abdelsatir, El-Tigani B., Narayan C. Debnath, and Hisham Abushama. "A multilayered scheme for transparent audio data hiding." *2015 IEEE/ACS 12th International Conference of Computer Systems and Applications (AICCSA)*. IEEE, 2015.

[36] Binny, Anu, and Maddulety Koilakuntla. "Hiding secret information using LSB based audio steganography." *2014 International Conference on Soft Computing and Machine Intelligence*. IEEE, 2014.

[37] Mandal, Ashis Kumar, et al. "An approach for enhancing message security in audio steganography." *16th Int'l Conf. Computer and Information Technology*. IEEE, 2014.

[38] Elkandoz, Marwa Tarek, and Wassim Alexan. "Logistic tan map based audio steganography." *2019 international conference on electrical and computing technologies and applications (ICECTA)*. IEEE, 2019.

[39] Jayaram, P., H. R. Ranganatha, and H. S. Anupama. "Information hiding using audio steganography–a survey." *The International Journal of Multimedia & Its Applications (IJMA) Vol* 3 (2011): 86-96.

[40] Gambhir, Ankit, and Sibaram Khara. "Integrating RSA cryptography & audio steganography." *2016 International Conference on Computing, Communication and Automation (ICCCA)*. IEEE, 2016.

[41] Kekre, H. B., et al. "Information hiding in audio signals." *International Journal of Computer Applications* 7.9 (2010): 14-19.

[42] Hussein, Reem, and Wassim Alexan. "Secure message embedding in audio." *2019 2nd International Conference on Computer Applications & Information Security (ICCAIS)*. IEEE, 2019.

[43] Elkandoz, Marwa Tarek, and Wassim Alexan. "Logistic tan map based audio steganography." *2019 international conference on electrical and computing technologies and applications (ICECTA)*. IEEE, 2019.

[44] Sinha, Nishith, Anirban Bhowmick, and B. Kishore. "Encrypted information hiding using audio steganography and audio cryptography." *International Journal of Computer Applications* 112.5 (2015).

[45] Bangera, Kripa N., et al. "Multilayer security using RSA cryptography and dual audio steganography." *2017 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT)*. IEEE, 2017.

[46] Rana, Lovey, and Saikat Banerjee. "Dual layer randomization in audio steganography using random byte position encoding." *International Journal of Engineering and Innovative Technology* 2.8 (2013).

[47] Cheddad, Abbas, et al. "Skin tone based steganography in video files exploiting the YCbCr colour space." *2008 IEEE International Conference on Multimedia and Expo*. IEEE, 2008.

[48] Hanafy, Amr A., Gouda I. Salama, and Yahya Z. Mohasseb. "A secure covert communication model based on video steganography." *MILCOM 2008-2008 IEEE Military Communications Conference*. IEEE, 2008.

[49] Tadiparthi, Gopalakrishna Reddy, and Toshiyuki Sueyoshi. "A novel steganographic algorithm using animations as cover." *Decision Support Systems* 45.4 (2008): 937-948.

[50] Cetin, Ozdemir, and A. Turan Ozcerit. "A new steganography algorithm based on color histograms for data embedding into raw video streams." *computers & security* 28.7 (2009): 670-682.

[51] Cheddad, Abbas, et al. "A skin tone detection algorithm for an adaptive approach to steganography." *Signal Processing* 89.12 (2009): 2465-2478.

[52] dd

[53] Dasgupta, Kousik, J. K. Mandal, and Paramartha Dutta. "Hash based least significant bit technique for video steganography (HLSB)." *International Journal of Security, Privacy and Trust Management (IJSPTM)* 1.2 (2012): 1-11.

[54] Bhole, Ashish T., and Rachna Patel. "Steganography over video file using Random Byte Hiding and LSB technique." *2012 IEEE International Conference on Computational Intelligence and Computing Research*. IEEE, 2012.

[55] Lou, Der-Chyuan, and Chen-Hao Hu. "LSB steganographic method based on reversible histogram transformation function for resisting statistical steganalysis." *Information Sciences* 188 (2012): 346-358.

[56] Zhang, Rongyue, et al. "An efficient embedder for BCH coding for steganography." *IEEE Transactions on Information Theory* 58.12 (2012): 7272-7279.

[57] Moon, Sunil K., and Rajeshree D. Raut. "Analysis of secured video steganography using computer forensics technique for enhance data security." *2013 IEEE Second International Conference on Image Information Processing (ICIIP-2013)*. IEEE, 2013.

[58] Kelash, Hamdy M., et al. "Hiding data in video sequences using steganography algorithms." *2013 International Conference on ICT Convergence (ICTC)*. IEEE, 2013.

[59] Paul, Rahul, et al. "Hiding large amount of data using a new approach of video steganography." *Confluence 2013: The Next Generation Information Technology Summit (4th International Conference)*. IET, 2013.

[60] Dasgupta, Kousik, Jyotsna Kumar Mondal, and Paramartha Dutta. "Optimized video steganography using genetic algorithm (GA)." *Procedia Technology* 10 (2013): 131-137.

[61] Khupse, Sneha, and Nitin N. Patil. "An adaptive steganography technique for videos using Steganoflage." *2014 International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT)*. IEEE, 2014.

[62] Ramalingam, Mritha, and Nor Ashidi Mat Isa. "Fast retrieval of hidden data using enhanced hidden Markov model in video steganography." *Applied Soft Computing* 34 (2015): 744-757.

[63] Mstafa, Ramadhan J., and Khaled M. Elleithy. "A video steganography algorithm based on Kanade-Lucas-Tomasi tracking algorithm and error correcting codes." *Multimedia Tools and Applications* 75.17 (2016): 10311-10333.

[64] Sun, Shuliang. "A new information hiding method based on improved BPCS steganography." *Advances in Multimedia* 2015 (2015).

[65] Noda, Hideki, et al. "Application of BPCS steganography to wavelet compressed video." *2004 International Conference on*

Image Processing, 2004. ICIP'04.. Vol. 4. IEEE, 2004.

[66] Kar, Nirmalya, Kaushik Mandal, and Baby Bhattacharya. "Improved chaos-based video steganography using DNA alphabets." *ICT Express* 4.1 (2018): 6-13.

[67] Mumthas, S., and A. Lijiya. "Transform domain video steganography using RSA, random DNA encryption and Huffman encoding." *Procedia computer science* 115 (2017): 660-666.

[68] Hamed, Ghada, et al. "Hybrid, randomized and high capacity conservative mutations DNA-based steganography for large sized data." *Biosystems* 167 (2018): 47-61.

[69] Mondal, Bhaskar. "A Secure Steganographic Scheme Based on Chaotic Map and DNA Computing." *Micro-Electronics and Telecommunication Engineering*. Springer, Singapore, 2020. 545-554.

[70] Vijayakumar, P., V. Vijayalakshmi, and G. Zayaraz. "An improved level of security for dna steganography using hyperelliptic curve cryptography." *Wireless Personal Communications* 89.4 (2016): 1221-1242.

[71] Huang, YongFeng, and Shanyu Tang. "Covert voice over internet protocol communications based on spatial model." *Science China Technological Sciences* 59.1 (2016): 117-127.

[72] Peng, Bo, and Jie Yang. "An optimized algorithm based on generalized difference expansion method used for HEVC reversible video information hiding." *2017 IEEE 17th International Conference on Communication Technology (ICCT)*. IEEE, 2017.

[73] Wu, Zhijun, et al. "Steganography and Steganalysis in Voice over IP: A Review." *Sensors* 21.4 (2021): 1032.

[74] Jiang, Yijing, et al. "Covert voice over Internet protocol communications with packet loss based on fractal interpolation." *ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM)* 12.4 (2016): 1-20.

[75] Lu, Xiaorong, et al. "Concealed in the internet: A novel covert channel with normal traffic imitating." *2016 Intl IEEE Conferences on Ubiquitous Intelligence & Computing, Advanced and Trusted Computing, Scalable Computing and Communications, Cloud and Big Data Computing, Internet of People, and Smart World Congress (UIC/ATC/ScalCom/CBDCom/IoP/SmartWorld)*. IEEE, 2016.

[76] Anuradha, M., et al. "IoT enabled cancer prediction system to enhance the authentication and security using cloud computing." *Microprocessors and Microsystems* 80 (2021): 103301.

[77] GR, Manjula. "A Survey on Audio Stream Steganography Techniques." *Available at SSRN 3851209* (2021).

[78] Lei, Tim, Jeremy Straub, and Benjamin Bernard. "Lightweight Network Steganography for Distributed Electronic Warfare System Communications." *Advances in Security, Networks, and Internet of Things*. Springer, Cham, 2021. 437-447.