A Comprehensive Review on Advancements and Applications of Steganography

AFREEN S[1], DIVYASREE S[1], HARICHANDANA N[1], KHUSHI M[1]
[1] Computer Science and Engineering, Bangalore Institute of technology, Karnataka, (India)
Under the guidance of Prof. Nikitha K. S., Assistant Professor, Bangalore Institute of Technology

Abstract

Steganography, the art and science of concealing messages within other data, has a rich history spanning centuries. In this review paper, we delve into various aspects of steganography, exploring its techniques, detection methods, evaluation criteria, and practical applications. We analyze steganalysis techniques, discuss time-sensitive steganography, and examine historical cases illustrating the ingenuity and effectiveness of covert communication methods. Through this comprehensive examination, we aim to provide insights into the evolving landscape of steganography and its significance in contemporary digital communication.

Keywords: Steganography, Concealing messages, Steganalysis, Covert communication, Cryptography, Digital watermarking, Text steganography, Image steganography, Audio steganography, Clandestine communication methods, Blind steganalysis, Time-sensitive steganography.

I. Introduction[1]

Steganography, derived from the Greek words "steganos" (meaning concealed) and "graphein" (meaning writing), has long been employed as a clandestine communication technique. By embedding secret messages within seemingly innocuous carriers, steganography facilitates covert communication while evading detection. Over the years, steganographic methods have evolved from ancient practices such as invisible ink and hidden compartments to sophisticated digital techniques leveraging multimedia files and cryptographic algorithms.

In this review paper, we embark on a journey through the multifaceted realm of steganography. We explore the fundamental principles underlying steganographic techniques, investigate strategies for detecting hidden messages, and assess the efficacy of different steganographic algorithms. Additionally, we examine the interplay between steganography and steganalysis, shedding light on the cat-and-mouse game between concealment and detection.

Through a nuanced analysis of historical cases and contemporary advancements, we aim to elucidate the enduring relevance of steganography in modern information security. As digital communication continues to proliferate across diverse domains, understanding the principles and applications of steganography becomes increasingly vital.

Thus, this review seeks to provide a comprehensive overview of steganography, bridging the gap between historical precedents and cutting-edge innovations in covert communication.

2. History[2]

Few instances of historical incidents on steganography:

1. Harpagus' Hare Message:
- Harpagus hid a message inside a hare's body and sent it with a messenger pretending to be a hunter.
- Demonstrates the use of animals to conceal messages in ancient times.

2. Histaieus' Tattooed Message:
- Histaieus shaved the head of a trusted slave, tattooed the message on his head, and waited for his hair to grow back before sending him.
- Shows the extreme lengths to which people went to hide messages, even using human bodies as carriers.

3. Demeratus' Wax Tablets:
- Demeratus concealed a message under wax writing tablets by removing the wax, writing on the wood, and re-covering it with wax.
- Illustrates a clever method of hiding messages in plain sight, relying on the recipient to uncover the hidden message.

4. Aeneas' Astrogal:
- Aeneas invented the astrogal, a ball or cube with drilled holes representing letters, to pass thread through for spelling out messages.
- A creative and intricate method of secret communication, resembling a toy to avoid suspicion.

5. Invisible Ink and Pin Pricks:
- Germans used invisible ink and pin pricks above letters in innocuous messages, requiring heating or careful inspection to reveal the hidden message.
- Demonstrates the use of hidden markings and substances to convey covert information, even in modern times.

6. Porta's Dog Message:
- Giovanni Batista Porta suggested feeding a message to a dog and killing the dog to retrieve the message.
- Shows a more extreme and brutal method of retrieving hidden messages, indicating the lengths to which people went for secrecy.

2.1 Past

The Greeks used steganography and cryptography to convey secret messages, with examples dating back to 440 B.C. They used methods like hiding messages in wax or tattooing messengers. Romans used invisible ink for privacy, and the British used microdots in newspapers to hide messages effectively. Ancient emperors used null ciphers, and books like "Polygraphie" and "Steganographia" discussed cryptographic and steganographic methods. Americans used code talkers in World War II, and modern steganography methods are

exemplified by the prisoners' problem, as explained by Simmons.

2.2 Present

Steganography has evolved into a digital form, offering security and anonymity in internet communication. It is categorized into spatial and transform domains, with various techniques like watermarking and fingerprinting used to hide secrets in multimedia files. Algorithms such as LSB and OPAP have been developed for practical implementation. Steganography employs mathematics and engineering disciplines like matrix and information theory. Applications include protecting intellectual property, preventing piracy, and authentication of documents.

3. Trends in Steganography

3.1 Origin of Steganography[4]

The origins of steganography trace back to ancient civilizations, notably the Greeks and Romans, who ingeniously concealed messages within everyday objects like hare corpses and wooden tablets coated with wax. As societies evolved, so did steganography, with advancements such as sympathetic inks and textual methods like acrostics gaining prominence during the Medieval Ages. The Renaissance introduced innovative techniques like hiding messages in hard-boiled eggs and using music scores as carriers. Subsequent eras, including the World Wars and the technological advancements of the 20th century, saw the development of more sophisticated steganographic methods, marking a continuous evolution in the art of covert communication.

3.2 Steganography and it’s relation to Cryptography[4][5]

Cryptography and steganography, often confused but fundamentally different, offer complementary approaches to information security. Cryptography aims to render messages unreadable to unauthorized recipients through encryption, relying on keys for decryption. However, encrypted messages still reveal the act of communication. In contrast, steganography conceals messages within carriers, making the exchange of information covert. By combining these technologies, communication can be not only challenging to detect but also decipher, offering heightened privacy. Steganography's ability to hide the existence of communication complements cryptography's focus on encoding message content, providing a robust defense against interception and decryption attempts.

3.3 Steganography v/s Digital Watermarking[6]

While both steganography and digital watermarking involve embedding hidden information into files, they serve distinct purposes and utilize different techniques. Digital watermarking primarily aims to assert ownership of intellectual property or ensure content integrity by inserting repetitive information into the carrier. Unlike steganography, the watermarking information may not always be hidden from viewers, and it's often designed to be removable while preserving the carrier file's integrity. Therefore, while related, steganography and digital watermarking employ different algorithms, serve different purposes,

and present varying levels of threat in terms of information security.

4. Types of Steganography

4.1 Based on Method[10]

Steganography plays a crucial role in securing various communication channels such as phone, fax, computer, and radio. There are three main types of steganography:

- **Pure Steganography:** Pure Steganography does not require the exchange of secret information before sending a message, relying solely on secrecy for security. It is defined by a quadruple (C, M, D, E), where C is the set of possible covers, M is the set of secret messages, and E is the embedding function. The extraction function D ensures that the hidden message can be retrieved from the cover. While Pure Steganography is preferred for its simplicity and lack of stego-key exchange, it offers no security if the embedding method is known to attackers.

- **Secret Key Steganography:** Secret key Steganography uses a secret key to embed a message into a cover, similar to a symmetric cipher. The receiver can extract the message using the same secret key. It is defined by a quintuple (C, M, K, DK, EK), where C is the set of covers, M is the set of secret messages, K is the set of secret keys, and EK is the embedding function.

- **Public Key Steganography:** Public key Steganography uses a public key to encrypt information before embedding it into a cover, ensuring that only the recipient with the corresponding private key can extract and decrypt the message. This approach eliminates the need for a prior exchange of secret keys between communication partners. The sender encrypts the message with the recipient's public key, embedding it in a channel known to the recipient. The receiver can then extract and decrypt the message using their private key, as long as both parties are using compatible cryptographic algorithms and embedding functions.

4.2 Based on Medium[1][3][7][8][9]

- **Text Steganography:** Text steganography involves hiding secret messages within text documents without altering the document's visible appearance. This technique uses various methods such as modifying whitespace, altering characters' case, or embedding messages in seemingly random data. Text steganography is often used to transmit covert information through seemingly innocent or routine communications, making detection difficult. It relies on the fact that the human eye may not detect subtle changes in text, especially in large volumes of data. Advanced techniques may use natural language processing to hide messages in grammatically correct sentences.

- **Image Steganography:** Image steganography involves hiding

secret data within an image file without altering its visual appearance significantly. This technique is used to securely transmit hidden information, such as text or another image, within the pixels of an image. The process typically involves encoding the secret data into the least significant bits of the pixel values. The recipient can extract the hidden information using the same steganographic algorithm and a secret key or password. Image steganography is commonly used for secure communication and digital watermarking.

- **Audio Steganography:** Audio Steganography is a technique used to hide secret information within audio files. It involves embedding the secret data into the audio signal in a way that is imperceptible to human listeners. This can be achieved by modifying certain properties of the audio signal, such as amplitude or frequency, to encode the hidden information. The process of embedding the data is typically reversible, allowing the hidden information to be extracted later. Audio steganography is often used for covert communication or for watermarking audio files to protect intellectual property.

5. Techniques of Steganography

5.1 Historical Techniques[5]

Steganography has a rich history of clandestine communication methods, predating the development of cryptographic systems. In ancient Greece, messages were cleverly concealed on wax tablets, appearing as ordinary tablets when covered in wax. Another method involved tattooing messages on messengers' bodies, hidden by the growth of their hair, as recounted by Herodotus during Persian invasion plans. During World War II, espionage agents utilized microdots to transmit information, embedding them in paper and disguising them as alphabetic characters or postage stamps. Velvalee Dickinson, a spy for the Japanese, concealed information within doll orders, earning her the moniker "Doll Woman." Additionally, the one-time pad cipher, theoretically unbreakable, allows for the hiding of messages within seemingly random data, providing a modern example of steganographic techniques.

5.2 Major Modern Techniques[1][5][7]

Modern steganography emerged in 1985 with the rise of personal computers tackling classical steganography. It has since expanded with numerous 'stego' programs. Techniques include hiding messages in noisy images or sound files, concealing data within encrypted data blocks, chaffing and winnowing, invisible ink, null ciphers, embedding messages in tampered executable files, embedding pictures in videos, using imperceptible delays in network packets from keyboard inputs, content-aware steganography, BPCS-Steganography for large capacity embedding, and Blog-Steganography where messages are fragmented and added as comments in weblogs or social network platforms.

5.2.1 Text Steganography

- **Line-Shift Coding:** This method involves vertically shifting the positions of text lines within a document to encode information uniquely. Decoding may be done from either the format file or the bitmap image, particularly feasible when the original image has uniform line spacing.

- **Word-Shift Coding:** In this technique, the positions of words within text lines are horizontally shifted to encode the document uniquely. Decoding can be performed from the format file or the bitmap image, but the original image is necessary due to variable spacing between words, commonly used for text justification.

- **Feature Coding:** This approach alters selected text features within a document, such as vertical endlines (tops of letters like b, d, h, etc.), based on codewords. Decoding requires the original image, specifically noting changes in pixel dimensions at a given feature point.

5.2.2 Image Steganography

Hiding information within images through steganography has gained popularity, especially in online environments like the World Wide Web and newsgroups. While its practical use remains somewhat limited, various techniques enable the concealment of messages within images without altering their visible properties significantly. Here are some key methods:

- **Least Significant Bit (LSB) Embedding:** This straightforward approach involves embedding bits of a message directly into the least significant bit plane of the cover image. Since the changes are minimal and imperceptible to the human eye, LSB modification ensures effective hiding of information within the image. It's crucial to use lossless compression formats to prevent loss of hidden data during transformations.
  For example, the following grid can be considered as 3 pixels of a 24-bit color image, using 9 bytes of memory:
  (00100111 11101001 11001000)
  (00100111 11001000 11101001)
  (11001000 00100111 11101001)
  When the character A, which binary value equals 10000001, is inserted, the following grid results:
  (00100111 11101000 11001000)
  (00100110 11001000 11101000)
  (11001000 00100111 11101001)

Fig(a) Original picture [5]

Fig(b) Picture with a small text inserted using LSB [5]

- **Masking and Filtering:** Masking and filtering methods are commonly applied to 24-bit and grayscale images. They operate akin to watermarking physical paper, serving as digital counterparts. Masking involves altering the brightness of the masked portion. The smaller the change in brightness, the lower the likelihood of detection. While these methods may subtly change the image's visible properties, they are less susceptible to compression and other image processing compared to LSB modification.

Fig. Masking [15]

- **Discrete Cosine Transformations (DCT):** More complex than LSB embedding, this method involves modifying discrete cosine transformations used in JPEG compression. By manipulating DCT coefficients, data can be concealed within the image. This approach provides robust hiding capabilities, particularly suitable for images compressed using lossy algorithms like JPEG.
  For example[16], embedding the first chapter of The Hunting of the Snark in a JPEG using DCT.

Fig(a). The unmodified JPEG files.

Fig(b). Embedded image in a JPEG

5.2.3 Audio Steganography

Audio steganography involves embedding secret messages within digitized audio signals, subtly altering the binary sequence of the corresponding audio file. Here's an overview of some common methods:

- **LSB Coding:** In LSB coding, the least significant bit of the binary sequence of each sample in the digitized audio file is replaced with the binary equivalent of the secret message. This technique exploits the fact that small alterations in the least significant bit are imperceptible to human ears.
  For example,[7] if we want to hide the letter ‘A’ (binary equivalent 01100101) to an digitized audio file.

Sampled Audio Stream (16 bit)	‘A’ in binary	Audio stream with encoded message
1001 1000 0011 1100	**0**	1001 1000 0011 110**0**
1101 1011 0011 1000	**1**	1101 1011 0011 100**1**
1011 1100 0011 1101	**1**	1011 1100 0011 110**1**
1011 1111 0011 1100	**0**	1011 1111 0011 110**0**
1011 1010 0111 1111	**0**	1011 1010 0111 111**0**
1111 1000 0011 1100	**1**	1111 1000 0011 110**1**
1101 1100 0111 1000	**0**	1101 1100 0111 100**0**
1000 1000 0001 1111	**1**	1000 1000 0001 111**1**

Fig. The signal level comparisons between a WAV carrier file before (above) and after (below) the LSB coding is done[9]

- **Phase Coding:** Phase coding takes advantage of the fact that the Human Auditory System (HAS) is less sensitive to phase changes than to noise in audio signals. Secret message bits are encoded as phase shifts in the phase spectrum of the digital signal, achieving inaudible encoding in terms of signal-to-noise ratio.

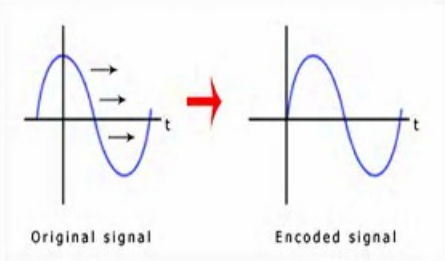


Fig. The signals before and after Phase coding procedure, [9]

- **Spread Spectrum:** Spread spectrum techniques encompass two approaches: direct sequence spread spectrum (DSSS) and frequency hopping spread spectrum (FHSS). DSSS multiplies the transmitted signal by a pseudorandom noise sequence, spreading the signal's energy over a wider bandwidth. FHSS, on the other hand, pseudo-randomly returns the carrier frequency, resulting in a uniform frequency distribution.

- **Echo Hiding:** Echo hiding involves embedding the secret message as an echo within the cover audio signal. Parameters such as amplitude, decay rate, and offset from the original signal are adjusted to represent the encoded binary message, ensuring that the echo remains below the threshold of human auditory perception.

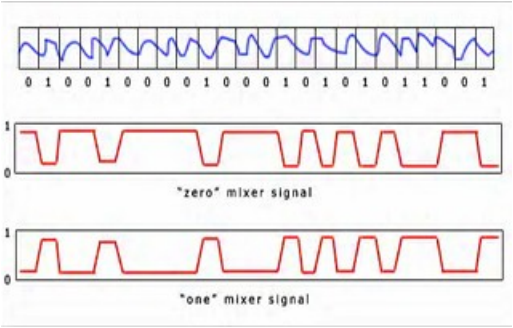


Fig. An example of echo hiding, [9]

6. Factors Affecting Steganography[10] [11][12]

Steganographic techniques involve embedding messages within covers, with various features characterizing their strengths and weaknesses. Here's a breakdown of key factors affecting the efficiency and effectiveness of steganography methods:

- **Capacity:** Capacity refers to the total number of bits successfully hidden and recovered by the steganographic system.
- **Robustness:** Robustness denotes the ability of embedded data to remain intact despite

transformations undergone by the stego-system, such as filtering, noise addition, and compression.

- **Undetectable:** An algorithm is considered undetectable if the image with the embedded message aligns with the source model, without making statistical changes to the carrier's noise component.
- **Invisibility (Perceptual Transparency):** Invisibility relies on properties of the human visual or audio system. Embedded information should be imperceptible to an average observer, without significant degradation in perceptual quality.
- **Security:** Security entails ensuring embedded information remains resistant to removal after discovery by an attacker, relying on the secrecy of the algorithm and the secret key.

Additional factors determining efficiency include:

- **Payload Capacity:** The amount of secret information that can be hidden in the cover source.
- **MSE (Mean Square Error):** Measures the average squared difference between a reference and distorted image.
- **PSNR (Peak Signal to Noise Ratio):** Measures the quality between the original and compressed image. Mean square error (MSE) and Peak Signal to Noise Ratio (PSNR) can also be used as metrics to measure the degree of imperceptibility:

$$MSE = [\Sigma^{M}_{i=1} \Sigma^{N}_{j=1} (f_{ij} - g_{ij})^2]MN$$
$$PSNR = 10 \log_{10}(L^2/MSE),$$

where M and N are the number of rows and number of columns respectively of the cover image, fij is the pixel value from the cover image, gij is the pixel value from the stego-image, and L is the peak signal value of the cover image (for 8-bit images, L=255).

- **SNR (Signal to Noise Ratio):** Compares the level of desired signal to background noise.

Metrics used to assess steganographic systems:

- **Entropy:** Perfect security is achieved when the statistics of cover and stego data are identical.
- **Correlation:** Determines the closeness between the original and stego-image, aiding in the detection of hidden data. Localization, that is detection of the presence of the hidden data relies on the use of cross correlation function RXY of two images X and Y:

$$R_{XY}(\alpha,\beta) = \sum_i \sum_j X(i,y)\, Y(i-\alpha, j-\beta)$$

7. Applications [11][13]

Steganography is used to hide data to prevent unauthorized access, with applications ranging from corporate espionage to protecting copyrights. It can be used for peaceful purposes, such as adding fictional elements to maps or protecting digital media from unauthorized use. However, it can also be misused by terrorists for covert communication and coordination of attacks. In the business world, steganography can be employed to hide sensitive information like chemical formulas or plans for inventions, while in the entertainment industry, it can be used to prevent unauthorized copying

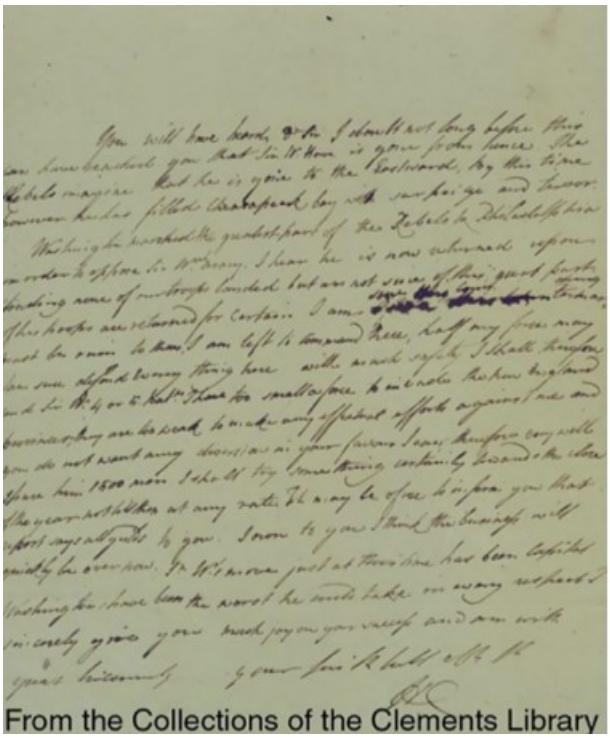
of DVDs. Other applications are as follows:

- Confidential Communication and Secret Data Storing
- Protection of Data Alteration
- Access Control System for Digital Content Distribution
- E-Commerce
- Media
- Database Systems.
- Digital watermarking

Real world Example: [6]

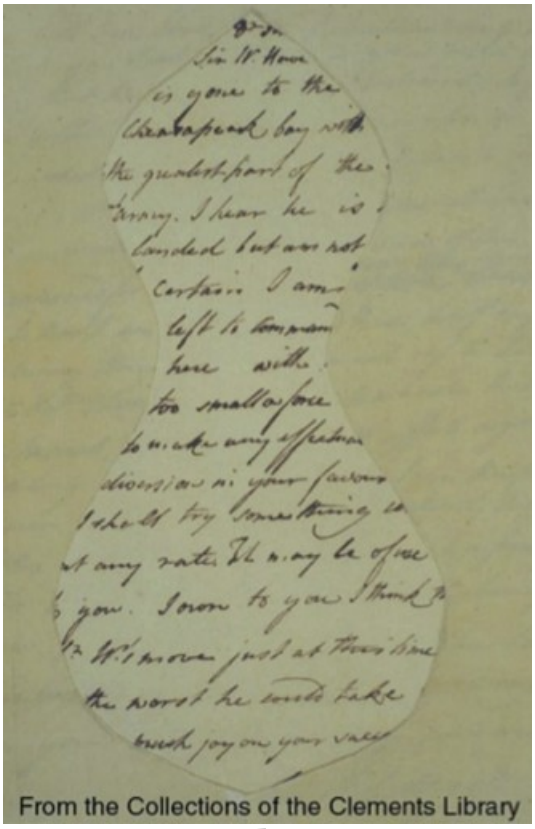
Concealment Ciphers:

Concealment ciphers are an old method of hiding messages. These types of ciphers hide a message openly in the carrier medium so that it can be recovered by anyone who knows the secret for how it was concealed. A grille cipher, for example, employs a template that reveals the message once applied to the original carrier. One well-known example is that of a letter written by British Lt. General Sir Henry Clinton to General John Burgoyne in August 1777.


From the Collections of the Clements Library

The text of the letter reads: You will have heard; Dr Sir I doubt not long before this can have reached you that Sir W. Howe is gone from hence. The Rebels imagine that he is gone to the Eastward. By this time, however, he has filled Chesapeak bay with surprise and terror. Washington marched the greater part of the Rebels to Philadelphia in order to oppose Sir Wm's. army. I hear he is now returned upon finding none of our troops landed but am not sure of this, great part of his troops is returned for certain. I am sure this countermarching must be ruin to them. I am left to command here, half of my force may I am sure defend everything here with much safety. I shall therefore send Sir W. 4 or 5 Bat [talion] ns. I have too small a force to invade the New England provinces; they are too weak to make any effectual efforts against me and you do not want any diversion in your favour. I can, therefore very well spare him 1500 men. I shall try something certainly towards the close of the year, not till then at any rate. It may be of use to inform you that the report says all yields to you. I owe it to you that I think the business will quickly be over now. Sr. W's move just at this time has been capital. Wahington's have been the worst he could take in every respect. sincerely give you much joy on your success and am with great Sincerity your [] HC.

Clinton's letter was intended to be read by Burgoyne using a grille. Once the grille is applied, the letter reads:



Sir. W. Howe
is gone to the
Chesapeak bay with
the greatest part of the
army. I hear he is
landed but am not
certain. I am
left to command
here with
too small a force
to make any effectual
diversion in your favour.
I shall try something
at any rate. It may be of use
to you. I own to you I think
Sr W's move just at this time
the worst he could take.
Much joy on your success.

8. Detection and evaluation of Steganography[9]

8.1 Detection of Steganography

Detection of steganography involves looking for patterns or anomalies in the cover media that might indicate hidden information.

Text Steganography:

- Detection involves looking for patterns or alterations in the text, such as unusual language usage or excessive white space.

Image Steganography:

- Statistical analysis can reveal discrepancies or patterns indicating modifications in stego-images, particularly focusing on LSB alterations.
- Techniques such as frequency analysis or detecting statistical anomalies can aid in uncovering hidden messages.

Audio and Video Steganography:

- Statistical analysis can be applied to detect LSB modifications in audio files.
- Other detection methods include scanning for high, inaudible frequencies, odd distortions, or patterns in sounds.
- For video steganography, special code signs or gestures may be used, which are difficult to detect with computer systems.

8.2 Evaluation of Steganography

Evaluation of steganographic techniques is based on several criteria.

Text Steganography:

- The first-letter algorithm is not very secure, as knowledge of the system

used automatically reveals the secret.
- Evaluation criteria include imperceptibility, payload capacity, robustness against statistical attacks, and independence of file format.

Image Steganography:
- Imperceptibility is crucial, along with robustness against statistical attacks and image manipulation.
- Algorithms must be compatible with various file formats and produce unsuspicious files to avoid detection.

Audio Steganography:
- Evaluation factors include data transmission rate, bandwidth, robustness, and noise audibility.
- Selection of methods depends on the specific communication needs, ranging from simple LSB coding to more sophisticated techniques like phase coding or spread spectrum.

Video Steganography:
- Combined evaluations of image and audio steganography are applied.
- Consideration of the impact on video quality and security is essential to achieve secure communication.

9. Steganalysis[5][6][7][17]

Steganalysis is the process of detecting steganography by analyzing various parameters of a stego media to determine if it contains a hidden message. This process involves identifying suspected media, reducing the set of suspected information streams using statistical methods, and employing techniques such as visual detection to identify unusual patterns or degradation in the media. Steganalysis attacks aim to detect, extract, and destroy hidden objects in stego media, and they can vary based on the information available for analysis, including known carrier attacks, steganography-only attacks, known message attacks, and known steganography attacks. Steganalysis helps in detecting and stopping the use of steganographic techniques by comparing cover objects, stego objects, and portions of the stego-key.

In the case of Visual detection steganalysis technique a set of stego images are compared with original cover images and note the visible difference. The signature of the hidden message can be derived by comparing numerous images. Cropping or padding of image also is a visual clue of hidden message because some stego tool is cropping or padding blank spaces to fit the stego image into fixed size. Difference in file size between cover image and stego images, increase or decrease of unique colors in stego images can also be used in the Visual Detection steganalysis technique.

Steganography Attacks:
Steganographic attacks consist of detecting, extracting and destroying hidden objects of the stego media. Steganography attack is followed by steganalysis. There are several types of

attacks based on the information available for analysis.
Some of them are as follows: -

- **Known carrier attack:** The original cover media and stego media both are available for analysis. Steganography only attack: In this type of attack, only stego media is available for analysis.
- **Known message attack:** The hidden message is known in this case.
- **Known steganography attack:** The cover media, stego media as well as the steganography tool or algorithm, are known.
- **Chosen stego attack**: In this case, both the steganographic algorithm and stego medium (i.e. image) are known to the steganalyst. This type of attack may involve the steganalyst attempting to produce stego objects from cover objects in order to pair the seized stego medium. Theoretically, trying to create brand-new stego mediums to pair the seized one seems right, yet in practice it is extremely difficult to achieve, considering both the stego medium and the embedded information is not known.

Blind steganalysis:
Blind steganalysis techniques are more challenging but powerful than targeted approaches as they don't require knowledge of specific embedding procedures. Algorithms are designed to detect manipulations in suspected files, indicating potential steganography. Early techniques like IQM and wavelet-based statistics by Memon et al. and Farid aimed to identify communicative information in images. Fridrich et al. introduced a self-calibration technique for blind steganalysis, estimating the cover image from a suspected file. This allows for more generalized attacks and accurate determination of hidden messages without prior knowledge.

10. Limitations of Steganography[14]

The scheme proposed aims for unconditional covertness by using uncompressed digital video as cover text and encoding ciphertext at a low rate. The goal is to make attacks impossible by embedding ciphertext as the least significant bit of pixels based on a shared one-time pad. The proof of covertness would involve demonstrating that the warden cannot differentiate between raw cover text and stegotext without knowledge of the key, ensuring that the number of plausible embedded messages remains constant. The difficulty lies in the critical dependence on the model of the cover text.

A. What If Perfect Compression Existed?

The existence of perfect compression poses a challenge for steganography, as it implies that any ciphertext message can be efficiently hidden in compressed data without detection. If perfect compression were achievable, steganography would be either trivial or impossible, depending on the efficiency of compression. This highlights the need to bridge the gap between information theory and steganography, suggesting that practical steganography becomes relevant only in cases where compression is inefficient.

B. Entropy

Entropy arguments are important in steganography, particularly when the embedded material is indistinguishable from random data. The entropy of the stegotext equals the entropy of the cover text plus the entropy of the embedded material. To ensure security against detection of embedded material, options include keeping the uncertainty in the opponent's measurement low or processing the material to reduce its entropy before embedding. However, the competence of the opponent in measuring entropy of the cover text is unknown, making security proofs challenging. Increasing the amount of stegotext given to the opponent may improve their ability to estimate the statistics of the cover text, potentially reducing the rate at which bits can be safely tweaked. Empirical evidence suggests that positive rates of ciphertext insertion are achievable in some channels.

C. Selection Channel

Inspired by Shannon's correction channel, using a shared one-time pad in steganography can be seen as a selection channel, where the pad determines which cover text bit is marked with the next ciphertext bit. This approach ensures that the number of plausible ciphertexts generated by trying all possible pads is large enough to prevent Willie, who is computationally unbounded, from accusing Alice of sending stegotext. The book cipher, which enciphers a message as pointers to words in a shared book, is another example of a selection channel, where security depends on the secrecy of the book and avoiding word reuse. A repetitive book or cover text with unusual statistics will have lower capacity for embedding messages securely.

D. The Power of Parity

In steganography systems that filter out locations where embedding would significantly affect relevant statistics, a selection channel approach suggests selecting a set of pixels using a one-time pad and embedding the ciphertext bit as their parity. This reduces the effect of the embedding process on statistics below a chosen threshold. The selection channel can be a pseudorandom number generator, allowing for the hiding of more bits in the cover text. However, there are limits to the amount of information that can be safely hidden based on the allowed set of cover texts and encoding rules.

11. Time Sensitive Steganography[6]

Time-sensitive steganography acknowledges that covert channels don't need to remain hidden indefinitely. While some researchers prioritize steganographic methods that are immune to various attacks, practitioners understand that most secret messages have a limited lifespan. Therefore, a steganographic method is considered adequate if it can keep the secret hidden long enough to achieve the communicators' objectives. Even a less effective steganographic method may serve its purpose if it can maintain secrecy for a duration longer than it takes for an adversary to detect and decode the covert channel.

In designing or selecting a steganographic method, practitioners consider time-sensitive criteria. The

chosen stego scheme should have usability and implementation criteria that satisfy the following equation:

TCRITICAL < TDETECT + TDECODE

Here, TCRITICAL represents the required lifetime of the covert channel, which can vary depending on the user's needs. For some scenarios, keeping the secret for a few days or weeks may be sufficient, while in others, maintaining secrecy for years or even decades may be necessary. The stego method must be robust enough so that the combined time to detect the covert channel (TDETECT) and the time to decode it (TDECODE) exceeds the critical lifetime required for the channel.

12. Future of Steganography[3]

Given the nascent nature of this technology, the scope of the business issues that are affected and the continuing impact of Moore's law on the power of computing it is difficult to predict with any certainty where we will be in 5 years. Nevertheless, the following predictions are presented as a reasonable set of possibilities:

- Steganographic techniques will become more common and increasingly sophisticated.
- Steganalysis tools will also become more complex but will typically be behind their steganographic counterparts.
- A stego process will be developed to embed Trojans, worms and viruses in media such as images or audio files and have they become active by viewing or listening to the files. In 2001, the Nimda worm demonstrated that it was possible to get a virus just by visiting an infected web site. In January of 2002, viruses were being delivered by Macromedia flash images. One day, merely viewing a bitmap image might cause a virus attack on your PC.
- Intrusion Detection Systems (IDS) will include images as part of their attack signatures.
- Anti-virus software will be developed with steganalytical capabilities to detect viruses in audio and image files.
- A strong tamper-resistant, economically viable digital watermark will be developed.

The person who develops the last item will undoubtedly become very rich. There is probably no better motivating factor for learning about Steganography.

It is hoped that Dual Steganography, Steganography along with Cryptography may be some of the future solutions for this above-mentioned problem.

Conclusion

In conclusion, our exploration of steganography illuminates its enduring significance as a clandestine communication tool. From ancient methods of concealing messages in wax tablets to modern digital techniques embedded within multimedia files, steganography has evolved to meet the changing demands of covert communication. Our review has delved into various facets of steganography, including its techniques, detection methods, evaluation criteria, and practical applications.

We have discussed steganalysis techniques aimed at detecting hidden messages and evaluated the robustness of different steganographic algorithms. Additionally, we examined the concept of time-sensitive steganography, emphasizing the importance of balancing detection and decoding times with the critical lifetime of covert channels.

Throughout history, steganography has played a pivotal role in espionage, warfare, and clandestine communication. While some academic circles prioritize steganographic methods immune to detection, practitioners often recognize the pragmatic necessity of temporary concealment. As illustrated by historical cases, even rudimentary steganographic methods can serve their purpose if they effectively hold secrets for the required duration.

Looking ahead, steganography remains a dynamic field ripe for further exploration and innovation. As digital communication continues to evolve, so too will the techniques and tools employed in covert communication. By fostering a deeper understanding of steganography and its implications, we can better navigate the intricate landscape of information security and privacy in the digital age. Ultimately, our review underscores the enduring relevance of steganography as both an art and a science, shaping the contours of covert communication in an ever-changing world.

References

[1] Masoud Nosrati, Ronak Karimi, Mehdi Hariri, "*An introduction to steganography methods*", World Applied Programming, Vol (1), No (3), August 2011, 191-195.

[2] Kahn, D. (1996). *The history of steganography*. In: Anderson, R. (eds) Information Hiding. IH 1996. Lecture Notes in Computer Science, vol 1174. Springer, Berlin, Heidelberg.

[3] Amirtharajan, Rengarajan, and John Bosco Balaguru Rayappan. "*Steganography-time to time: A review*." Research Journal of Information Technology 5, no. 2 (2013): 53-66.

[4] Zielińska E, Mazurczyk W, Szczypiorski K (2014) *Trends in steganography*. Commun ACM 57(3):86–95.

[5] Jammi Ashok, Y.Raju, S.Munishankaraiah, K.Srinivas, "*STEGANOGRAPHY: AN OVERVIEW*", Jammi Ashok et. al. / International Journal of Engineering Science and Technology Vol. 2(10), 2010, 5985-5992.

[6] GARYC.KESSLER, CHET HOSMER, "*An Overview of Steganography*", Advances in Computers, VOL.83, ISSN:0065-2458/DOI:10.1016/B978-0-12-385510-7.00002-3.

[7] Das, Soumyendu, Subhendu Das, Bijoy Bandyopadhyay, and Sugata Sanyal. "*Steganography and Steganalysis: different approaches.*" arXiv preprint arXiv:*1111.3758* (2011) .

[8] Morkel, Tayana, Jan HP Eloff, and Martin S. Olivier. "*An overview of image steganography*." In *ISSA*, vol. 1, no. 2, pp. 1-11. 2005.

[9] Bandyopadhyay, Samir K., Debnath Bhattacharyya, Debashis Ganguly, Swarnendu Mukherjee, and Poulami Das. "*A tutorial review on steganography*." In International conference on contemporary computing, vol. 101, pp. 105-114. 2008.

[10] Zaidoon Kh. AL-Ani, A.A.Zaidan, B.B.Zaidan and Hamdan.O.Alanazi, "*Overview: Main Fundamentals for Steganography*", Journal Of Computing, Volume 2, Issue 3, March 2010, ISSN 2151-9617.

[11] Jasleen Kour, Deepankar Verma, "*Steganography Techniques –A Review Paper*", International Journal of Emerging Research in Management &Technology ISSN: 2278-9359 (Volume-3, Issue-5).

[12] Pramanik, Sabyasachi, and R. P. Singh. "*Role of steganography in security issues*." International Journal of Advance Research in Science and Engineering 6, no. 1 (2017): 1119-1124.

[13] Ronak Doshi, Pratik Jain, Lalit Gupta, "*Steganography and Its Applications in Security*", International Journal of Modern Engineering Research (IJMER), Vol.2, Issue.6, Nov-Dec. 2012 pp-4634-4638 ISSN: 2249-6645.

[14] Ross J. Anderson and Fabien A. P. Petitcolas, "*On the Limits of steganography*", IEEE Journal On Selected Areas in Communications, Vol. 16, No. 4, May 1998.

[15] Johnson, Neil F., and Sushil Jajodia. "*Exploring steganography: Seeing the unseen*." Computer 31, no. 2 (1998): 26-34.

[16] Provos, Niels, and Peter Honeyman. "*Hide and seek: An introduction to steganography*." IEEE security & privacy 1, no. 3 (2003): 32-44.

[17] Douglas, Mandy, Karen Bailey, Mark Leeney, and Kevin Curran. "*An overview of steganography techniques applied to the protection of biometric data*." Multimedia Tools and Applications 77, no. 13 (2018): 17333-17373.