Al-Salam Journal for Engineering and Technology
Journal Homepage: http://journal.alsalam.edu.iq/index.php/ajest
e-IS S N: 2790-4822p-IS SN: 2958-0862

Survey steganography applications

Eng. Saad Nasser Al.Azzam [1], Dr. Abdelmageed Algamdi [2]

[1] Cyber Security Researcher, Faculty of Computing and Information Technology, University of Bisha Saudi Arabia

[2] Computer Science, Department of Computer and Information Systems, University of Bisha Saudi Arabia

*Corresponding Author: Eng. Saad Nasser Al.Azzam

DOI: https://doi.org/10.55145/ajest.2023.01.01.008
Received June 2022; Accepted September 2022; Available online November 2022

ABSTRACT: There are many and many ways that play an important role in terms of information security, including the most common method known as cryptography, which is changing/hiding the basic data according to a certain method to make it unreadable. Steganography is another art that aims to completely hide data to communicate between two parties unobtrusively to a third party, and this is known as steganography. Only the relevant persons are aware of this contact. The practice of steganography includes concealing a message inside a suitable carrier, such as a picture or an audio file, for example. Steganography is also known as cryptography. The carrier may then be delivered to the intended recipient with no one except the intended recipient being aware that it conceals a message. For instance, civil rights organizations in repressive countries may utilize this strategy to get their message out to the globe without raising suspicion at home. This is due to the fact that it is possible to use this strategy in private. In this piece, we've attempted to explain the many steps involved in using a "multimedia" file to create steganography (text, static image, audio, and video). Stainless is an emerging area of data science that tries to detect steganographic masks and, if possible, retrieve hidden communications. Stainless is an emerging industry. It's extremely similar to cryptanalysis, which is used in the field of cryptography. The technique has been around for quite some time, but it has only recently gained widespread notice because of its application to the secure transmission of digital information. The primary objective is to conceal the existence of the communication, as well as to prevent it from being read.

Keywords: Carrier, Privacy, Secrecy, Steganalysis, Steganography

1. INTRODUCTION

The original usage of the phrase "hidden writing" dates back to ancient Greece. Steganography That's why there's a field dedicated to researching different methods of information obfuscation. When compared to cryptography, whose goal is to make data unreadable to a third party, steganography's goal is to hide information from prying eyes [1]. Steganography is a method for hiding data in non-traditional media including images, sounds, texts, and even digital data transfers and films. When information is hidden inside another file, or "carrier," it is called a "stego carrier." To the human eye, it will seem quite similar to the illustration that appeared on the cover. It's not hard to see how steganography and cryptography are related. Encrypting messages in a manner that makes them unreadable is fundamental to the field of cryptography. However, steganography will obfuscate the message to the point that neither the sender nor the receiver will realize it exists [2]. Steganography refers to the technique of secretly inserting data into computer files. The steganographic coding in digital steganography may be hidden in the transport layer of any kind of digital file used in electronic communication, whether it a text file, an image file, a programmed file, or a protocol file [3]. The technology of steganography, on the other hand, has improved greatly in recent years, allowing users to hide enormous amounts of data inside audio and visual recordings. Information may be double protected using a combination of steganography and cryptography; first, it is encrypted, and then it is concealed, making it more difficult for an adversary to both discover the information and decode it.

The goal of this article is to present a security thesis that puts secrecy above privacy when it comes to different kinds of communication [4].

2. Implementation of Steganography

There are many different types of cover information that are capable of concealing secrets. The following equation offers a fairly generalized explanation of the many components that make up the steganographic process [5].

In this scenario, the file that we will use to conceal the hidden data, which may also be encrypted using the stego key, is referred to be the cover medium. The file that was produced as a consequence is known as the stego medium (and it will, of course, be of the same type as the cover medium file). Steganography may be implemented in one of these four ways:[6]

1. Using text.
2. Using images.
3. Using audio files.
4. Using video files.

3. Text Steganography

For text, there are three primary categories that may be used to classify steganography techniques for text: format-based, random and statistical creation, and linguistic approach. Methods that were based on formats took advantage of the actual text formatting of the document as a location to conceal information [7].

In most cases, this strategy involves making changes to the text that already exists in order to conceal the steganographic information. Some of the various format-based approaches that are utilized in text steganography include the insertion of spaces, the distribution of intentional misspellings across the text, and the scaling of the typefaces.

However, according to what Bennett has said, such format-based tactics were successful in fooling the majority of human eyes, but they are no longer effective after computer technologies have been deployed. In random and statistical generation, the cover text is made based on the statistical features [8].

This approach is predicated on the sequential appearance of characters and words. The embedding of information to appear in a random series of characters is what is meant to be understood as "the concealment of information inside character sequences." This sequence has to provide the impression of being random so no one is able to intercept the message [9].

Another approach for character creation uses statistical features of word length and letter frequency to construct "words" (with no lexical meaning) that seem to have the same statistical qualities as real words in a particular language. The approach takes use of the correlation between word length and frequency of letters.

Words themselves may be utilized to conceal information, or a codebook with mappings between dictionary entries and bit sequences can be used [10].

The fourth kind is known as "linguistic method," and it involves not only taking into account the specific linguistic aspects of the text being written or modified, but also using the structure of the language itself to conceal meaning. Steganographic information may, in fact, be hidden inside the syntax of a language [11].

The sender and receiver agree ahead of time that the secret message will be encoded in the order of the succeeding words of the cover text, thus the sender gives the recipient a sequence of integer numbers (the Key). For instance, the cover may read, "A team of five guys joined today" from a sequence that goes "1, 1, 2, 3, 4, 2, 4." It follows that "Atfvoa" is the coded message. If there is a blank space in the decoded message, the corresponding "0" in the number series will show that.

If the number of characters in a word in the received cover text is fewer than the corresponding number in the series (Key), then the word will be skipped [12].

4. Image Steganography

The practise of concealing hidden messages inside digital images is now the one that sees the greatest use. This method of concealment uses steganography to take advantage of a limitation in the human visual system (HVS). When looking at a collection of color pixels, HVS is unable to recognize variations in the brightness of color vectors. The higher frequency side of the visual spectrum may be used to represent the individual pixels [13].

Characteristics such as "brightness" and "chroma" may be used to provide an idea of what an image looks like. Ones and zeros (or 1s and 0s) can be used to show each of these things in a digital format [14].

As an example, a bitmap with 24 bits will have 8 bits for each of the three-color values (red, green, and blue) that are included in each individual pixel. If we just examine blue, we will see that it may be represented by two distinct shades. It is quite unlikely that the human eye would be able to distinguish between the values 11111111 and 11111110 when comparing the blue intensity.

Therefore, if the only recipient of data is the human visual system (HVS), then the least significant bit (LSB) can be used for anything other than color information. This is because HVS is the only possible recipient of the data [15].

5. LSB Coding

The simplest method of hiding information inside an image file is to inject data using the least significant bit, or LSB. The least significant bit (LSB) of each byte included inside the cover picture might be written over using this approach, revealing the secret information [16].

If we are utilizing 24-bit color, the amount of change will be negligible, and it will be impossible for the human eye to tell the difference. As an example, let's say that we have three pixels that are next to one another, totaling nine bytes, and their RGB encoding is as follows:

10010101	00001101	11001001
10010110	00001111	11001010
10011111	00010000	11001011

Now let's pretend that we wish to "hide" the following 9 bits of data (the data to be hidden is typically compressed before it is hidden), which are: 101101101. When we put these 9 bits on top of the least significant bit (LSB) of the 9 bytes that came before them, we obtain the following (where the bits in bold have been altered):

10010101	00001100	11001001
10010111	00001110	11001011
10011111	00010000	11001011

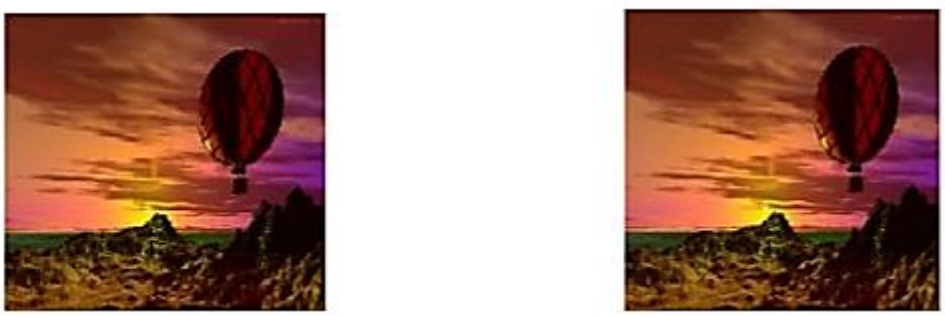

FIGURE 1. - (a) Original image; (b) Embedded image

Steganography is used on a still photograph as an example. The picture on the left is the original cover art, while the image on the right is a stego image created by inserting a text file inside the cover art [17].

6. Masking And Filtering

The majority of the time, procedures such as masking and filtering are used on pictures that are 24 bit and grayscale. They are sometimes employed as digital watermarks and conceal information in a manner that is analogous to how watermarks hide information on physical paper. Changing the brightness of the region that is going to be masked is required when masking photographs. The slighter the variation in brightness, the less likely it is that it will be picked up by the eye [18].

When it comes to compression, cropping, and some aspects of image processing, masking is a more reliable option than LSB insertion. Instead of just concealing the message in the "noise" level, masking methods include it in important portions of the cover picture. This makes it so that the concealed message is more of an essential part of the cover. Because of this, it is more suited than LSB for use with lossy JPEG pictures, for example [19].

7. Audio Steganography

The fallibility of the human hearing and visual senses is essential to the practise of steganography in its broadest sense. In audio steganography, the psychoacoustical masking phenomena of the human auditory system (HAS) are used for the purpose of hiding information.

The psychoacoustic or auditory masking feature makes a weak tone unperceivable when there is a loud tone in its temporal or spectral vicinity. This is because the two tones compete for attention. This trait is brought about by the fact that the HAS has a short differential range, despite the fact that its dynamic range spans 80 dB below the level of the ambient noise [20].

When the human ear is exposed to tone-or noise-like frequencies at greater levels, a phenomenon known as frequency masking may take place. This phenomenon causes the human ear to be unable to hear frequencies that are there but have a lower power level [21].

In addition, a faint pure tone will be obscured by wide-band noise if it comes within a band that is considered to be significant. The fact that low sounds cannot be heard makes this attribute useful for embedding information in a variety of different ways. Recent research has shown that it is possible to hide data in cover audio signals by adding tones that can't be heard [22].

A hidden message is inserted into a digitized audio signal via audio steganography, which results in a very minor change to the binary sequence of the audio file that corresponds to the hidden message. Below is a list and discussion of the many techniques that are often used in the process of audio steganography.

- LSB coding
- Parity coding
- Phase coding
- Spread spectrum
- Echo hiding

7.1 LSB Coding

A process called sampling is used to turn the analogue audio stream into a digital binary sequence. This is followed by a process called quantization.

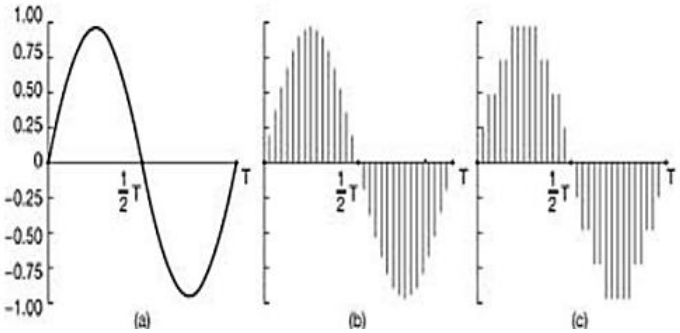

FIGURE 2. - LSB Coding

In this method, the least significant bit (LSB) of each sample in a digitised audio file is replaced with the binary equivalent of a secret message.

7.2 Parity Coding

Each bit of a secret message is encoded in the parity bit of a sample region using the method of parity coding, which partitions a signal into regions of samples rather than individual samples. It's an alternative to sampling the signal individually. If the selected region's parity bit does not match the secret bit that must be encoded, the algorithm will flip the least significant bit (LSB) of one of the samples in that region.

Therefore, the sender has a wider variety of encoding options for the secret bit, and fewer evident methods to alter the signal [23].

7.3 Phase coding

The Human Auditory System (HAS) is not as adept at identifying phase changes in an audio transmission as it is at identifying noise within the signal. This is taken advantage of by the phase coding approach. This method encodes the bits of a secret message as changes in the phase spectrum of a digital signal. This makes the signal-to-noise ratio too low to be heard [24].

7.4 Spread spectrum

Using the spread spectrum (SS) technique, audio steganography seeks to conceal information by dispersing it over the audio signal's frequency range. This is the same as a system that uses LSB coding where the message bits are spread randomly throughout the whole audio file.

The SS technique is similar to LSB coding in that it uses a code that is independent of the real signal to conceal information inside an audio file. The resulting signal uses more bandwidth than is necessary for transmission [25].

7.5 Echo Hiding

Echo concealing is a method for protecting sensitive data inside an audio file by superimposing a second echo on top of the original, discrete signal. Similar to the spread spectrum method, this one boasts a number of advantages, including a high data transmission rate and more robustness than the approaches that generate noise.

In the case of merely a single echo being returned from the original signal, only a single bit of information could be stored. Therefore, the source signal is segmented into blocks before being encoded. Following encoding, the signal is reconstructed by rearranging the blocks in their original arrangement [26].

8. Video Steganography

As video files are often made up of a collection of pictures and sounds, the methods discussed in regards to still photos and sound files may usually be used to video files as well. The DCT (Discrete Cosine Transform) technique is often used by programmes or people to disguise information inside videos [27].

DCT modifies each video frame just enough to make it unrecognizable to the naked eye. To be more exact, DCT changes the values of certain areas inside pictures, often by rounding them up. For instance, if a certain area of a picture has a value of 6.667, for instance, that number will be rounded up to 7 [28].

9. Applications

Every time you need to conceal information, steganography is your best option. While there are a variety of motivations for doing so, the overarching goal of hiding information is to ensure that no unauthorized parties learn of its existence. New methods make a secret message as difficult to detect as random noise.

No evidence exists to confirm the message, even if it is assumed to exist. In the corporate environment, steganography may be used to conceal sensitive information such as a new chemical formula or innovative blueprints. [29]

When employed for corporate espionage, steganography may be used to secretly transmit sensitive information like trade secrets [30].

Steganography may also be used by terrorists to hide their communications and coordinate attacks. While the above may seem sinister, the most apparent applications of steganography are in fields like espionage. However, it has many benign uses in the world today.

The earliest and simplest of these techniques is employed in mapmaking, when occasionally a little fictitious street is added to a map so that the creator may go after piracy. To prevent illegal resale, another tactic is to include fictitious names on mailing lists. Steganography in the form of a digital watermark is used more and more in modern applications to stop sensitive data from being copied without permission.

There are sometimes hidden messages in images that may be used to identify copies in CD photo collections. When used for DVDs, the method is much more successful since DVD recorders are purpose-built to identify and prevent the copying of protected DVDs [31].

10. Conclusion

be used to expose such deceptive approaches, but the first step is to understand that they exist. Furthermore, there are other advantageous applications for this kind of data concealment, such as watermarking or a safer centralized storage solution for things like passwords or key procedures. Any way you slice it, the technology is simple to implement and hard to spot.

It will be one step ahead if you take the time to get acquainted with all its features and capabilities. Several methods for concealing information in media such as text, images, and audio/video signals are addressed in this study. In this article, I have provided a high-level introduction of the interesting and rapidly developing field of computer security.

There is widespread concern among security experts about the potential risks posed by this technology to public and private sectors. With the advancement of computer processing power, this field is poised for explosive growth and will soon become widely used.

Numerous steganography tools exist, and they may be used on any kind of material, including text, audio, and visuals. There is active investigation into the most effective methods of detecting steganography in files, both by the government and by several commercial firms. Steganography will become commonplace in the same way that firewalls, virus scanners, and IDS/IPS are already common.

ACKNOWLEDGEMENT

Acknowledgements and Reference heading should be left justified, bold, with the first letter capitalized but have no numbers. Text below continues as normal.

CONFLICTS OF INTEREST

The authors declare no conflict of interest

REFERENCES

References should be in IEEE style.

[1]. Kadhim, Inas Jawad, et al. "Comprehensive survey of image steganography: Techniques, Evaluations, and trends in future research." Neurocomputing 335 (2019): 299-326.
[2]. Yahya, Abid. "Steganography techniques." Steganography Techniques for Digital Images (2019): 9-42.
[3]. Wayner, P. Compression algorithms for real programmers. Morgan Kaufmann. 2000))
[4]. Taha, Mustafa Sabah, et al. "Combination of steganography and cryptography: A short survey." IOP conference series: materials science and engineering. Vol. 518. No. 5. IOP Publishing, 2019.
[5]. Muhammad, Mohd Hilal, et al. "Review on feature-based method performance in text steganography." Bulletin of Electrical Engineering and Informatics 10.1 (2021): 427-433.
[6]. Debnath, Sanghamitra, Manashee Kalita, and Swanirbhar Majumder. "A review on hardware implementation of steganography." 2017 Devices for Integrated Circuit (DevIC) (2017): 149-152.
[7]. Majeed, Mohammed Abdul, et al. "A review on text steganography techniques." Mathematics 9.21 (2021): 2829.
[8]. Narayana, V. Lakshman, and N. Ashok Kumar. "Different techniques for hiding the text information using text steganography techniques: A survey." Ingénierie des Systèmes d'Information 23.6 (2018).
[9]. Doshi, R., Jain, P., & Gupta, L. Steganography and its Applications in Security. International Journal of Modern Engineering Research (IJMER), 2(6), 4634-4638.2012)).
[10]. Ahvanooey, Milad Taleby, et al. "AITSteg: An innovative text steganography technique for hidden transmission of text message via social media." IEEE Access 6 (2018): 65981-65995.
[11]. Malik, Aruna, Geeta Sikka, and Harsh K. Verma. "A high capacity text steganography scheme based on LZW compression and color coding." Engineering Science and Technology, an International Journal 20.1 (2017): 72-79.

[12]. Luo, Yubo, and Yongfeng Huang. "Text steganography with high embedding rate: Using recurrent neural networks to generate chinese classic poetry." Proceedings of the 5th ACM workshop on information hiding and multimedia security. 2017.
[13]. Kadhim, Inas Jawad, et al. "Comprehensive survey of image steganography: Techniques, Evaluations, and trends in future research." Neurocomputing 335 (2019): 299-326.
[14]. Mandal, Pratap Chandra, et al. "Digital image steganography: A literature survey." Information Sciences (2022).
[15]. Hussain, Mehdi, et al. "Image steganography in spatial domain: A survey." Signal Processing: Image Communication 65 (2018): 46-66.
[16]. 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.
[17]. Bansal, Kriti, Aman Agrawal, and Nency Bansal. "A survey on steganography using least significant bit (lsb) embedding approach." 2020 4th International Conference on Trends in Electronics and Informatics (ICOEI)(48184). IEEE, 2020.
[18]. Din, Roshidi, and Alaa Jabbar Qasim. "Steganography analysis techniques applied to audio and image files." Bulletin of Electrical Engineering and Informatics 8.4 (2019): 1297-1302.
[19]. Kose, Joab, Oscar Bautista Chia, and Vashish Baboolal. "Review and Test of Steganography Techniques." arXiv preprint arXiv:2012.08460 (2020).
[20]. Dutta, Hrishikesh, et al. "An overview of digital audio steganography." IETE Technical Review 37.6 (2020): 632-650.

[21]. Mishra, Shilpi, et al. "Audio steganography techniques: A survey." Advances in Computer and Computational Sciences. Springer, Singapore, 2018. 581-589.
[22]. Dutta, H., Das, R. K., Nandi, S., & Prasanna, S. M. An overview of digital audio steganography. IETE Technical Review, 37(6), 632-650.2020))
[23]. Mishra, Shilpi, et al. "Audio steganography techniques: A survey." Advances in Computer and Computational Sciences. Springer, Singapore, 2018. 581-589.
[24]. Mishra, Shilpi, et al. "Audio steganography techniques: A survey." Advances in Computer and Computational Sciences. Springer, Singapore, 2018. 581-589.
[25]. Mishra, Shilpi, et al. "Audio steganography techniques: A survey." Advances in Computer and Computational Sciences. Springer, Singapore, 2018. 581-589.
[26]. Mishra, Shilpi, et al. "Audio steganography techniques: A survey." Advances in Computer and Computational Sciences. Springer, Singapore, 2018. 581-589.
[27]. Liu, Yunxia, et al. "Video steganography: A review." Neurocomputing 335 (2019): 238-250.
[28]. Kumar, V., & Muttoo, S. K. Principle of graph theoretic approach to digital steganography. In Proceedings of the 3rd National Conference (pp. 161-165).2009))
[29]. Baluja, Shumeet. "Hiding images in plain sight: Deep steganography." Advances in neural information processing systems 30 (2017).
[30]. Djebbar, F., Ayad, B., Meraim, K. A., & Hamam, H. Comparative study of digital audio steganography techniques. EURASIP Journal on Audio, Speech, and Music Processing, 2012(1), 1-16.2012)).
[31]. CHATURVEDI, A., KUMAR, V., & VERMA, P. Overview on Various Data Techniques Developed in Steganography and Cryptography to Secure Data. Changing Global Economic Scenario, 278.