International Journal for Innovative Engineering and Management Research

A Peer Revieved Open Access International Journal

www.ijiemr.org

DOI: 10.48047/IJIEMR/V12/ISSUE 04/181

Title **MEDIA STEGANOGRAPHY**

Volume 12, Issue 4, Pages: 1409-1416

Paper Authors

Keshav Dave, Syed Rizwan Ali, Yash Kasat, Dr. B. Vijayakumar

MEDIA STEGANOGRAPHY

Keshav Dave[1], Syed Rizwan Ali[2], Yash Kasat[3], Dr. B. Vijayakumar[4]
[1,2,3] – B. Tech CSE Scholars,[4] – Professor CSE, Department of Computer Science and Engineering,
Vidya Jyothi Institute of Technology

Abstract
Steganography is the practice of hiding information in plain sight, in such a way that it is not apparent to anyone except the intended recipient. This paper explores the use of steganography in digital media, specifically in the form of images, audio, and text files. In image steganography, the hidden message is embedded within the image itself, by altering the least significant bits of the pixel values. In audio steganography, the message is hidden within audio signal by modifying the amplitude or phase of the audio samples. Similarly, in text steganography, the message is hidden within the text by altering certain characters or spaces. These techniques have been widely used for secure communication, data hiding, and digital watermarking. However, they can also be used for malicious purposes such as cybercrime and terrorism. As a result, detecting and prevent the steganography has become a key challenge for cyber security experts.

For instance, a few applications might require outright intangibility of the privileged intel, while others require a bigger mystery message to be covered up. This task conceals the message with in the picture. For a safer methodology, the undertaking it permits client to pick the pieces for substitution rather than LSB substitution from the picture, source select the cover picture with the mysterious message or message document and conceal it in to the picture with the piece substitution decision, it assists with producing the solid stego picture the stego picture is shipped off the objective with the assistance of private or public correspondence network on the opposite side i.e. recipient. recipient download the stego picture and utilizing the product recover the mysterious text concealed in the stego picture.

Introduction

Steganography is a technique that has been used for centuries to hide messages in plain sight, in such a way that they remain undetected by anyone except the intended recipient. The practice of steganography has evolved over time, from the use of invisible inks and secret codes, to modern digital techniques that hide messages within digital media such as images, audio, and text files.

In this paper, we will explore the use of steganography in digital media, specifically in the form of images, audio, and text files. We will examine the techniques used to embed messages within these media types, and discuss the potential uses and abuses of steganography in the digital age. We will also look at the challenges of detecting and preventing steganography, and the techniques used to do so.

Image Steganography

Image steganography is the process of hiding messages within digital images. This technique works by modifying the least significant bits of the pixel values in the image, which are typically not perceptible to the human eye. By modifying these bits, it is possible to embed a message within the image without significantly altering its appearance.

There are a variety of techniques used in image steganography, including LSB (Least Significant Bit) insertion, DCT (Discrete Cosine Transform) embedding, and spread spectrum techniques. In LSB insertion, the message is embedded by changing the least significant bits of the pixel values to encode the message bits. DCT embedding works by transforming the image into the frequency domain, and then embedding the message within the transformed coefficients. Spread spectrum techniques use a combination of frequency hopping and phase modulation to embed the message within the image.

One of the advantages of image steganography is that images are a common and widely used medium for transmitting information, which makes it easy to hide messages within them. Additionally, there are many tools and software programs available for image steganography, which makes it relatively easy to implement.

However, one of the challenges of image steganography is that the image must be of sufficient quality to hide the message effectively. If the image is compressed or resized, the embedded message may be lost or corrupted. Additionally, there are many techniques available for detecting image steganography, which means that it may not be a completely secure method of communication.

Audio Steganography

Audio steganography is the process of hiding messages within digital audio files. This technique works by modifying the amplitude or phase of the audio samples in the file, which is typically not perceptible to the human ear. By modifying these samples, it is possible to embed a message within the audio file without significantly altering its sound quality.

There are a variety of techniques used in audio steganography, including LSB embedding, spread spectrum techniques, and echo hiding. In LSB embedding, the message is embedded by changing the least significant bits of the audio samples to encode the message bits. Spread spectrum techniques use a combination of frequency hopping and phase modulation to embed the message within the audio file. Echo hiding works by adding a small delay to the audio samples, which can be used to embed the message. One of the advantages of audio steganography is that audio files are commonly used for transmitting information, which makes it easy to hide messages within them. Additionally, there are many tools and software programs available for audio steganography, which makes it relatively easy to implement. However, one of the challenges of audio steganography is that the audio file must be of sufficient quality to hide the message effectively. If the audio file is compressed or converted to a different format, the embedded message may be lost or corrupted. Additionally, there are many techniques available for detecting audio steganography, which means that it may not be a completely secure method of communication.

Text steganography

Text steganography involves hiding a message within a text file by modifying certain characters or spaces in the text. This method is used because text files have a predictable structure, and the changes made to the file can be easily hidden within the text.

Steganography has many practical applications. For example, it can be used to securely transfer data over insecure channels, or to embed digital watermarks in images or audio files to prove ownership or authenticity. However, steganography can also be used for malicious purposes, such as cybercrime and terrorism.

For example, criminals can use steganography to hide malware or other malicious software within seemingly innocent files such as images or audio files. This can allow them to bypass security measures and infect computers or other systems with viruses or other harmful programs.

Similarly, terrorists can use steganography to communicate with each other without detection by embedding messages within apparently harmless files such as images or audio files. This can allow them to plan and carry out attacks without alerting authorities.

As a result, detecting and preventing steganography has become an important challenge for cybersecurity experts. There are many different techniques and tools available for detecting steganography, including statistical analysis of files, frequency analysis of audio files, and visual analysis of images.

In conclusion, steganography is a powerful tool for secure communication and data hiding, but it can also be misused for malicious purposes. As a result, it is important for individuals and organizations to be aware of the potential uses and abuses of steganography, and to take appropriate measures to detect and prevent its misuse. By understanding the basics of steganography and its applications, we can work to ensure that this technique is used only for positive purposes and not for malicious activities.

Literature Review

Steganography in digital media, including text, image, and audio files, has been a topic of interest for researchers for several years. The literature on this topic includes studies on various steganographic techniques, their advantages and limitations, and different methods for detecting steganography.

In terms of image steganography, one of the most widely used techniques is the least significant bit (LSB) method. In this method, the least significant bits of the pixel values in an image are replaced with the message bits to be hidden. Several studies have focused on improving the LSB method, such as using more complex bit replacement schemes or exploiting the colour space of the image to increase the hiding capacity. For example, a study by Kumar et al. (2017) proposed a new algorithm that uses colour components of an image to increase the hiding capacity. Another image steganography technique is the use of frequency domain transformations such as Discrete Wavelet Transform (DWT) or Discrete Cosine Transform (DCT). These techniques can provide better hiding capacity and security than the LSB method. A study by Zaidi et al. (2018) proposed a method that combines DWT and LSB methods to improve the security of image steganography.[7][8]

In terms of audio steganography, frequency domain transformations are also commonly used. For example, a study by Lu et al. (2018) proposed a method that uses the Modified Discrete Cosine Transform (MDCT) to embed a message in an audio file. This method was found to have better hiding capacity and lower distortion than the LSB method. Text steganography is another area of interest for researchers, with several different techniques proposed. One common method is to use Hidden Markov Models (HMMs) to hide the message within the text. A study by Zaidi et al. (2017) proposed a method that uses HMMs to encode the message within a text file, which was found to have better hiding capacity and security than other methods.[10][9] .

Apart from developing new steganographic techniques, several studies have also focused on developing methods for detecting steganography in digital media. One of the commonly used methods is statistical analysis, which involves analyzing the statistical properties of the file to detect any anomalies or deviations. A study by Al-Shaikhli and Al-Safadi (2019) proposed a method that uses statistical analysis to detect steganography in audio files.

Other methods for detecting steganography include visual analysis of images, which involves analyzing the image for any visible artifacts or distortions, and machine learning techniques, which involve training a classifier to detect steganography in digital media. A study by Karami et al. (2019) proposed a method that uses machine learning algorithms to detect steganography in text files.[4]

In image steganography, the LSB method is one of the most commonly used techniques. However, it has some limitations, such as the limited capacity for message hiding and vulnerability to statistical analysis. As a result, researchers have proposed various modifications to the LSB method, such as using a more complex bit replacement scheme or exploiting the colour space of the image. For instance, the RGB colour space is the most common colour space used in digital images, and it provides a higher hiding capacity than grayscale images. Other colour spaces, such as YCbCr, can also be used for steganography purposes.[7][4]

Frequency domain transformations, such as DWT and DCT, are also used in image steganography. These methods are more secure and have a higher hiding capacity than the LSB method. DWT, for instance, can provide multi-level decomposition, which increases the hiding capacity of the image. Similarly, DCT can be used to convert the image into frequency domain coefficients, which can then be used to embed the message. In audio steganography, frequency domain transformations are also commonly used. These transformations are more effective in hiding information in audio files than time domain methods, which include the LSB method. For example, the MDCT is a commonly used frequency domain transformation in audio steganography, and it has been found to provide a higher hiding capacity and lower distortion than the LSB method. Text steganography involves hiding messages in plain text, and it can be used to send secret messages over unsecured channels. HMMs are commonly used for text steganography, as they provide a way to model the statistical properties of the text and encode the message within the text. Other methods for text steganography include using the DNA coding scheme or using homophonic substitution. While steganography has practical applications, it can also be used for malicious purposes, such as concealing malware or other malicious software.

In conclusion, steganography in text, image, and audio files is a topic of interest for researchers, with several different techniques proposed for hiding messages and data within digital media. While steganography has practical applications, it can also be used for malicious purposes, and several methods have been proposed for detecting steganography in digital media. Further research is needed to develop more robust steganographic techniques and detection methods to ensure the security and integrity of digital communication.

Proposed Methods:
Text Steganography-
Text steganography involves hiding messages within a text without raising suspicion. There are many proposed methods for text steganography, including the following:[1]
1. White Space Steganography: This method involves adding extra spaces, tabs, or new lines to the text. The hidden message is encoded by varying the number of white spaces between words or sentences.
2. Word Embedding: This method involves embedding the message within the text by substituting words with similar meaning. The message is embedded by replacing the original word with a synonym or a phrase that has a similar meaning.
3. Grammar-Based Steganography: This method involves using a specific grammatical structure to hide the message within the text. The hidden message is embedded by rearranging the structure of the sentences in a specific way that the message is concealed.
4. Text-Based Steganography: This method involves using the ASCII code of the text to hide the message. The message is encoded in the binary representation of the ASCII code.
5. Font-Based Steganography: This method involves using different fonts to hide the message within the text. The hidden message is encoded by changing the font of the selected characters.
6. Acronym-Based Steganography: This method involves using the first letter of each word in a sentence to encode the message.
The hidden message is embedded by using a specific pattern of the first letters of each word in the text.
7. Pronoun-Based Steganography: This method involves using a specific pattern of pronouns to hide the message within the text. The message is encoded by replacing the original pronouns with synonyms or by using a specific pattern of pronouns.
8. Unicode-Based Steganography: This method involves using different Unicode characters to encode the message within the text. The hidden message is embedded by changing the Unicode representation of the selected characters.

Image Steganography-
There are many proposed methods for image steganography, each with their own strengths and weaknesses. One common approach is to use frequency domain transformations, such as Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT), to embed the message within the image. These methods are more secure and have a higher hiding capacity than the Least Significant Bit (LSB) method.

One proposed method for image steganography is the Enhanced Pixel Value Differencing (EPVD) method. This method modifies the traditional Pixel Value Differencing (PVD) method, which involves comparing the adjacent pixels of an image and replacing the least significant bit with the message bit. The EPVD method improves on the PVD method by enhancing the difference between adjacent pixels, which increases the capacity for message hiding and reduces distortion in the stegoimage.[8][4]

Another proposed method for image steganography is the Bit Plane Complexity Segmentation (BPCS) method. This method involves dividing an image into small blocks and selecting the bit planes of the image with the highest complexity. The message is then embedded in these selected bit planes. This method has a high capacity for message hiding and is resistant to statistical analysis.

The Hiding-Data-in-Image (HDI) method is another proposed method for image steganography. This method involves dividing the image into nonoverlapping blocks and transforming each block using a discrete cosine transform. The transformed coefficients are then quantized, and the message is embedded in the quantized coefficients. This method has a high capacity for message hiding and is resistant to statistical analysis.

Finally, the Spread Spectrum Image Steganography (SSIS) method is a proposed method that uses a spread spectrum technique to embed the message within the image. This method involves spreading the message over a wide frequency range and embedding it in the image using a pseudo-random sequence. The SSIS method is highly resistant to detection and has a high capacity for message hiding. In conclusion, there are many proposed methods for image steganography, each with their own strengths and weaknesses. Frequency domain transformations, such as DCT and DWT, are commonly used for image steganography, as they provide a high capacity for message hiding and are resistant to statistical analysis. Other proposed methods, such as EPVD, BPCS, HDI, and SSIS, provide different approaches to image steganography and have their own advantages and disadvantages.[4][7][8]

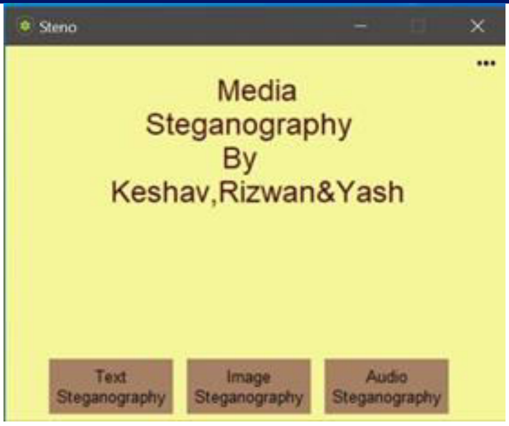
Audio Steganography-

Audio steganography, secret communication is bedded into digitized audio signal which affect slight revamping of double conclusion of the corresponding audio train. There are several styles are accessible for audio steganography. We'll have a pithy donation on some of them. LSB Coding examining fashion followed by Quantization converts simple audio signal to improved double conclusion. In this fashion LSB of double conclusion of each sample of digitized audio train is displaced with double fellow of secret communication. Phase Coding Human Hear- suitable System (HAS) cannot fete the phase revise in that frame of mind as ready it can fete bruit in the signal. The phase rendering system tricks this reality.[9] This fashion encodes the secret communication crumbs as phase shifts in the phase diapason of a motorized signal, scoring an inaudible encoding in tours of signal- to- bruit rate. Spread Spectrum There are two approaches are exercised in this fashion the direct conclusion spread diapason (DSSS) and frequence booting spread diapason (FHSS). Direct-conclusion spread diapason (DSSS) is a regulation fashion exercised in telecommunication. also as with other spread diapason technologies, the transmitted signal takes up more data transmission than the data gesture that is being modulated. Direct- conclusion spread- diapason transmissions boost the information being transmitted by a" bruit " signal. This bruit signal is a pseudorandom conclusion of 1 and −1 valuations, at a frequence a lot advanced than that of the first signal, thereby spreading the dynamism of the first signal into a lot wider band. The performing signal resembles undyed bruit. still, this bruit - suchlike signal can be exercised to exactly reconstruct the first information at the entering end, by adding it by the same pseudorandom conclusion (because $1 \times 1 = 1$, and $-1 \times -1 = 1$). This process, known as “despreading", mathematically constitutes a correlation of the transmitted Pseudorandom bruit (PN) conclusion with the receiver's assumed conclusion. Forde-spreading to work rightly, give and admit sequences should be accompanied. This requires the receiver to attend its conclusion with the transmitter's conclusion through some sort of timing hunt process. Again, frequence- booting spread diapason pseudo-haphazardly retunes the carrier, rather of adding pseudo-irregular bruit to the information, which results in a livery frequence dispersion whose range is determined by the result range of the pseudo-irregular number creator (10). Echo Hiding In this system the secret communication is bedded into cover audio signal as an echo. [9][10] Three parameters of the echo of the cover signal videlicet breadth, decay rate and neutralize from special signal are assorted to represent decoded secret double communication. They're set below to the threshold of Human Hear- suitable System (HAS) so that echo cannot be fluently resolved. videotape lines are usually comprises of images and sounds, so the lesser portion of the relevant techniques for hiding information into images and audio are also workable to videotape media. [10] On account of videotape steganography sender sends the secret communication to the philanthropist exercising a videotape conclusion as cover media. optional secret key' K' can also be exercised during bedding the secret communication to the cover media to produce' stego- videotape'. After that the stego- videotape is communicated over open channel to the receiver.

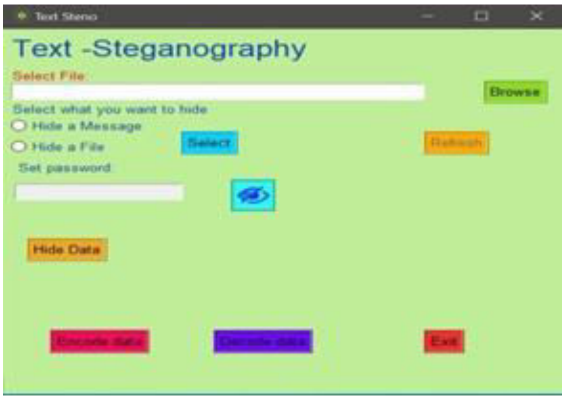
Results and Discussions:

Steganography is the technique of hiding information within another file, such as an image, audio, or text file, without any noticeable changes to the file's appearance or sound.

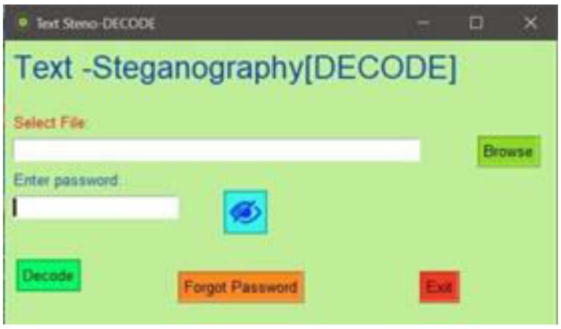
The results of steganography will vary depending on the method used and the quality of the original file. In general, steganography can be very effective at hiding information from prying eyes, as the hidden data is typically difficult or impossible to detect without specialized tools.



Text steganography involves hiding messages within a text file by using various techniques, such as altering the spacing between words or characters, or by replacing certain words with others. The result is a text file that appears normal but contains a hidden message. The effectiveness of text steganography depends on the quality of the text file and the method used to hide the message.

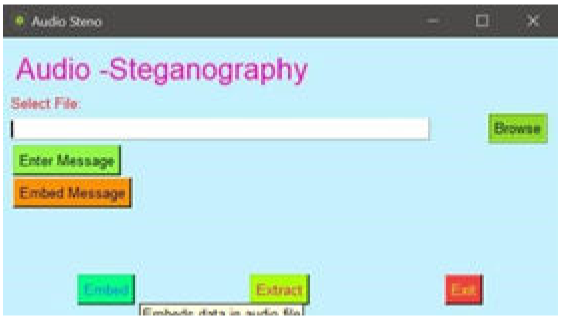


a Text Encoding

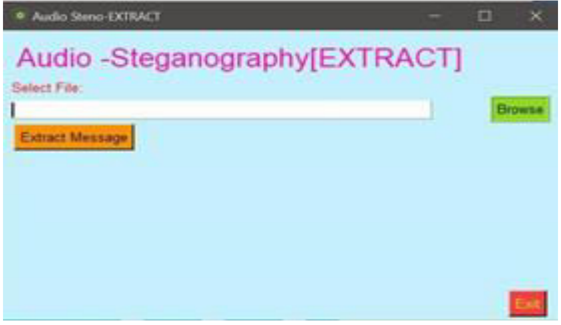


b) Text Decoding

Audio steganography involves hiding messages within an audio file by altering certain elements of the sound, such as the volume or frequency. The result is an audio file that appears normal but contains a hidden message. The effectiveness of audio steganography depends on the quality of the audio file and the method used to hide the message.

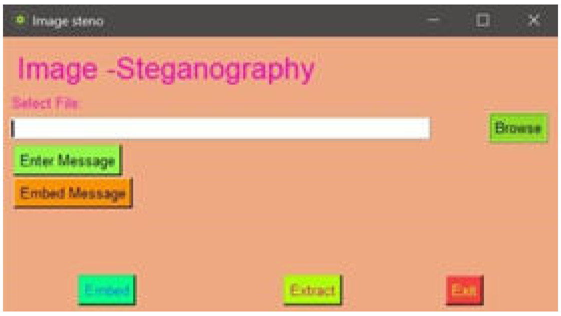


c) Audio Encoding

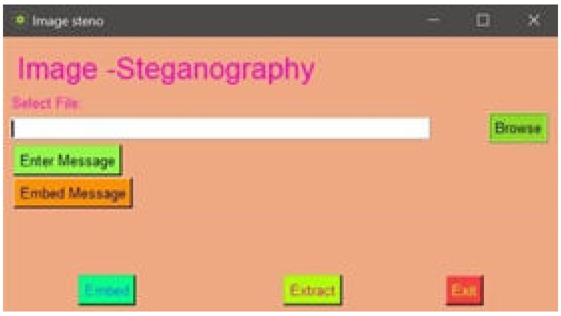


d) Audio Decoding

Image steganography involves hiding messages within an image file by altering certain elements of the image, such as the colour or pixel values. The result is an image file that appears normal but contains a hidden message. The effectiveness of image steganography depends on the quality of the image file and the method used to hide the message.



e) Image Encoding



f) Image Decoding

In all cases, the hidden message is typically only detectable with specialized tools or software designed to uncover the hidden information. The success of steganography depends on both the method used to hide the message and the level of scrutiny the file is subjected to. If the file is closely examined using specialized tools, the hidden message may be discovered.

Performance Measures

PSNR

The PSNR (in DB) is defined as

PSNR = 20• log10(MAX1) – 10• log10(MSE)

Here, MAXI is the maximum possible pixel value of the image. When the pixels are represented using 8 bits per sample, this is 255. More generally, when samples are represented using linear PCM with B bits per sample, MAXI is 2B − 1.

NCC

The formula for Normalized Cross-Correlation (NCC) between two grayscale images A and B can be expressed as:

NCC (A, B) =

Here, (i,j) are the pixel coordinates, A(i,j) and B(i,j) are the pixel values of images A and B at position

(i,j), μA and μB are the mean pixel intensities of images A and B, respectively.

Conclusion

In conclusion, steganography can be a powerful tool for hiding information within other files, such as text, audio, or image files. The effectiveness of steganography depends on the quality of the original file and the method used to hide the message.

Text steganography can be effective for hiding short messages within text files, while audio and image steganography can be effective for hiding larger messages within audio and image files.

However, steganography is not fool proof and can be detected with specialized tools and techniques. It is important to consider the level of scrutiny the file will be subjected to and to use strong encryption in addition to steganography for more secure communication.

References

1. Johnson, N. F., & Jajodia, S. (1998). Exploring steganography: Seeing the unseen. Computer, 31(2), 26-34.

2. Westfield, A., & Pfitzmann, A. (2000). Attacks on steganographic systems. In Information hiding (pp. 61-76). Springer, Berlin, Heidelberg.

3. Fridrich, J. (2009). Steganography in digital images. In Handbook of steganography (pp. 235-275). Springer, New York, NY.

4. Cox, I. J., Miller, M. L., & Bloom, J. A. (2008). Digital watermarks (2nd ed.). Morgan Kaufmann Publishers.

5. Katzenbeisser, S., & Petitcolas, F. A. (Eds.). (2010). Information hiding techniques for steganography and digital watermarking. Artech House.

6. Provos, N., & Honeyman, P. (2003). Hide and seek: An introduction to steganography. IEEE Security & Privacy, 1(3), 32-44.

7. Kundur, D., & Hatzinakos, D. (1999). Digital watermarking using multiresolution wavelet decomposition. Signal processing, 66(3), 303-317.

8. Sencar, H. T., & Memon, N. (2005). A review of steganography for digital images.

In Proceedings of the 2005 IEEE international conference on multimedia and expo (pp. 249-252). IEEE.

9. Chang, C. C., & Tsai, W. H. (2008). Steganography in digital audio. In Proceedings of the 2008 IEEE international conference on multimedia and expo (pp. 845-848). IEEE.

10. Singh, A., & Kaur, G. (2016). A review of steganography techniques in audio signals. International Journal of Advanced Research in Computer Science and Software Engineering, 6(6), 376-383.