International Journal of Engineering and Techniques - Volume 10 Issue 2, March 2024

RESEARCH ARTICLE OPEN ACCESS

Steganography

Yaseen Shaikh
Computer Engineering, Parul University, India, yaseenshaikh1811@gmail.com

ABSTRACT:

The safeguarding of sensitive information has become increasingly integral to both professional and personal spheres of life. As a result, the secure storage and transmission of such confidential data have garnered significant interest from researchers worldwide. One method gaining traction in this domain is steganography, which involves concealing confidential information within seemingly innocuous digital media such as images, audio, and video.
In the realm of steganography, digital images stand out due to their widespread usage and accessibility. Therefore, this research endeavours to delve into the realm of digital image steganography, aiming to explore its implementation and implications thoroughly.

KEYWORDS: — Information security, Steganography

I. INTRODUCTION

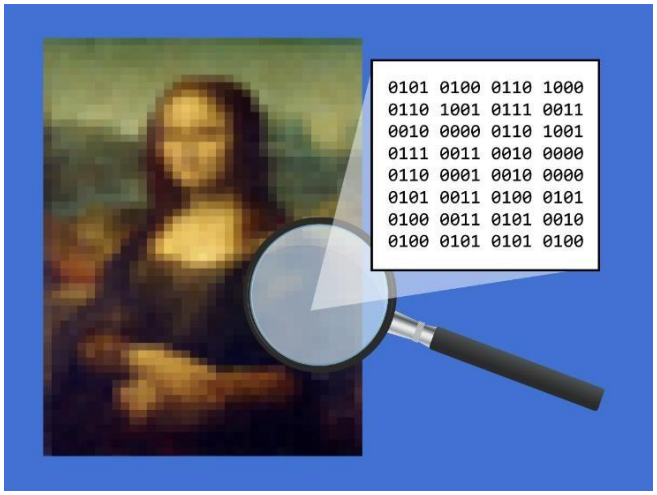
The rapid evolution of digital technology, particularly with the introduction of computers and internet technology, has sparked a transformative revolution, effectively shrinking the world into a digital village. However, this advancement also brings forth challenges, notably concerning the security of digital data. Illicit eavesdroppers continuously attempt to breach the security barriers protecting sensitive information. To counter such threats, numerous techniques have emerged to safeguard digital data. These include Cryptography, Steganography, Digital Watermarking, among others. Each technique offers unique approaches to securing data in the digital realm, providing layers of protection against unauthorized access and manipulation. Steganography is the practice of concealing communication in such a way that the existence of the communication itself remains hidden.

II. STEGANOGRAPHY

Steganography has ancient roots, with evidence of its practice dating back to early civilizations. In ancient times, secret messages were ingeniously concealed using various methods. For instance, wax tablets could be used to hide messages beneath a layer of wax, ensuring only the intended recipient could access the information. Additionally, some messages were tattooed onto the shaven heads of individuals, effectively camouflaging them from prying eyes. One notable historical account of steganography dates back to the writings of Herodotus. According to Herodotus, the Greek ruler Histiaeus employed a clever steganographic technique by tattooing a message onto the scalp of his most trusted slave. Once the slave's hair regrew, the message remained hidden from view, allowing the slave to carry the secret information undetected. This historical anecdote highlights the ingenuity and creativity employed in ancient steganographic practices. One of the most common uses of modern steganography in the digital world of

computers is to hide information from one file in the contents of another file. A common method is to manipulate the least significant bits of an image or audio file, replacing them with data extracted from a

text file. This alteration is done in a manner that minimizes any noticeable loss in image or audio quality, making it difficult for a casual observer to detect. For instance, an image shared on the internet, accessible to anyone worldwide, could clandestinely harbor a highly sensitive text message.



III. METHODS OF STEGANOGRAPHY:

In recent years, a multitude of steganography techniques have emerged, focusing on embedding concealed messages within multimedia objects. These techniques aim to hide information within images in a manner that remains imperceptible to the human eye. Common approaches include Least Significant Bit (LSB) manipulation, masking and filtering, and various transformation techniques. These methods enable the seamless integration of hidden data into images, ensuring that any alterations made to the image are virtually undetectable to observers.

The Least Significant Bit (LSB) insertion technique offers a straightforward method for embedding information within image files. In this approach, the bits of the message are directly inserted into the least significant bit plane of the cover image in a predetermined sequence. This modulation of the least significant bit typically results in changes that are imperceptible to the human eye due to their small amplitude. To increase the embedding capacity, some implementations utilize two or more least significant bits. However, this enhancement comes with trade-offs. While it boosts the capacity for embedding messages, it also heightens the risk of making the embedded message statistically detectable and degrades the fidelity of the image.

Another technique, Masking and filtering techniques, typically applied to 24-bit and grayscale images, operate by imprinting information onto an image, akin to paper watermarks. These techniques involve

analyzing the image and strategically embedding the information within significant areas, rather than simply concealing it within the image's noise level. This approach ensures that the hidden message

becomes an intrinsic part of the cover image, enhancing its integration and making it less susceptible to detection.

Transform techniques involve embedding messages by manipulating coefficients in a transform domain, such as the Discrete Fourier Transform or Wavelet Transform. These methods conceal messages in significant areas of the cover image, rendering them more resilient to detection or attacks. Transformations can be applied across the entire image, to specific blocks within the image, or through other variations, providing flexibility in implementation and enhancing the security of the embedded message.

Text Steganography:

Text steganography offers several techniques for concealing information within text files:

- Line-shift encoding
- Word-shift encoding
- Feature encoding

Line-shift encoding: In this method, text lines are shifted either up or down to encode the hidden information.

Word Shift Encoding: This method involves shifting words either from left to right or vice versa to encode the hidden information.

Feature Encoding: In this encoding technique, minor alterations are made to the shapes of characters to embed the hidden message.

Audio Steganography:

Audio steganography conceals secret messages within audio files of various formats.
Different methods for audio steganography include:

- Low-Bit Encoding
- Phase Coding
- Spread Spectrum

Low-Bit Encoding: In this coding method, data is stored in the least significant bit of images. Similarly, binary data can be concealed within the least significant bit of audio files.

Phase Coding: The phase coding method involves substituting the phase of an initial audio segment with a reference phase representing the data. This technique facilitates the embedding of information into audio files.

Spread Spectrum: When employing spread spectrum techniques, encoded data is distributed across as much of the frequency spectrum as feasible. This approach enhances the robustness and security of the hidden message within the audio file.

Image Steganography:

- Images are composed of individual dots known as pixels.
- Image files can be classified into two types: 8-bit and 24-bit per pixel.
- In these images, each pixel is assigned a color by blending different percentages of red, green, and blue (RGB).
- For each color component (red, green, and blue), the value ranges from 0 to 255.

Video Steganography:

Video steganography is a technique used to conceal files of any extension within a video file. However, this form of steganography is less common due to its complexity in implementation.

CONCLUSION:

In conclusion, steganography remains an intriguing field with diverse applications in digital communication, data security, and covert operations. Despite its ancient origins, steganography is continuously evolving, with ongoing research and development yielding new techniques and applications. As technology progresses, it becomes increasingly crucial to consider the ethical implications and challenges posed by steganography. Ensuring its responsible use in the digital age is essential for maintaining privacy, security, and ethical standards.

As we navigate the complexities of the digital age, it becomes increasingly imperative to grapple with the ethical dimensions and practical challenges posed by steganography. While this covert art holds immense potential for legitimate purposes such as secure communication and data protection, it also harbors the risk of misuse for illicit activities. Therefore, a nuanced understanding of steganography's ethical implications is essential for guiding its responsible use and safeguarding against potential abuses.

REFERENCES:

Cheddad A., Condell J., Curran K. & Kevitt P. (2010). Digital image steganography: Survey and analysis of current methods. Signal Processing, 90(3), 727-752.

Cheong S., Ling H. & Teh P. (2014). Secure encrypted steganography graphical password scheme for near field communication smartphone access control system. Expert Systems with Applications, 41(7), 3561-3568.

B. Dunbar. A detailed look at Steganographic Techniques and their use in an Open-Systems Environment, Sans Institute, 1(2002).

C. Christian. An Information-Theoretic Model for Steganography, Proceedings of 2nd Workshop on Information Hiding, MIT Laboratory for Computer Science, 1998.

Chiew K. & Pieprzyk J. (2010). Binary image steganographic techniques classification based on multi-class steganalysis. Information Security, Practice and Experience, 6047(1), 341-358.

Fridrich J., Goljan M., & Hogea D. (2012). New methodology for breaking steganographic techniques for JPEGs. Security and Watermarking of Multimedia Contents, 143(1), 83-97.

Kahn D., 1983. The Codebreakers. The Story of Secret Writing New York, Macmillan.