Optimization of Steganography Techniques to Protect Important Information in Data Transmission

Zahra Kharisma Sangha[1], Heni Sulistiani[2]

[1]*Zahra Kharisma Sangha, information technology, Universitas Teknokrat Inodesia, Bandarlampung, Indonesia*

Article Information

Received: 15-11-2023
Revised: 30-11-2023
Published: 15-12-2023

Keywords
Social Media, Steganography, Cover File, Stego Image, LSB.

****Correspondence Email:***
zahra_kharisma_sangha@teknokrat.ac.id

Abstract

Currently, social media has become an immensely popular platform, enabling users to share content, provide feedback, and interact with each other. Despite its convenience, the use of social media, particularly in sharing photos and videos, is often vulnerable to misuse due to a lack of security. Media security is crucial to prevent potential risks and undesired consequences. One effective way to enhance security is by implementing steganography techniques. Steganography involves a series of methods to conceal secret messages within cover files, making them undetectable in stego images. This research summarizes the latest methods in steganography techniques, focusing on utilizing cover files as containers to store secret information. The research findings indicate that the most commonly used method is Least Significant Bit (LSB) due to its ease of implementation, allowing for further development and combination with other methods or techniques to enhance security in hiding secret information. The analysis also reveals that the LSB method produces a lower average error rate compared to other methods.

1. Introduction

In the rapidly evolving field of Information Technology and Communication, social media has become exceedingly popular and widely used. Social media encompasses a group of online communication channels utilized for content sharing, feedback, interaction, and collaboration within communities. Its capability to facilitate the sharing of photos, opinions, and events has transformed our way of life. However, the security issues arising from the lack of safeguards in sharing photos and videos on social media are prevalent. Data security and confidentiality are crucial aspects of information. With the rise of illegal information retrieval techniques, many attempt to access unauthorized information. Therefore, media security is vital to prevent undesirable incidents.

One method employed to enhance media security is through steganography techniques. Steganography is a security technology still in use today. Literally meaning "covered writing" from the Greek language, steganography aims to communicate and share information covertly. In steganography, one frequently used technique is the Least Significant Bit (LSB), where the last bit in the pixel of an image is altered. In a specific

study, the LSB Word-Hunt (LSB WH) method was employed, representing a new approach inspired by word-hunt puzzles. LSB WH primarily focuses on reducing the Expected Number of Modifications per Pixel (ENMPP) compared to other methods in the literature. The research results reveal that LSB has an ENMPP of approximately 0.315 for natural images with high pressure on the second and third most significant bits. The study also demonstrates the method's resilience against chi-square statistical attacks.

Another research applies multi-resolution wavelet and wavelet packet methods to decompose speech signals into three and two layers. In this study, histogram statistics, HMFD, and their combined moments are extracted and compared with classical MFCC features and 36-dimensional MFCC features to train SVM classified by tested script samples. Detection results are tested using LSB matching steganography from varying rates of increase in speech signals. The findings show that detection performance with HMFD is superior to histogram statistical moments. The HPM method with Wavelet Packet Decomposition (WPD) can effectively detect low-bit embedding (LSB) in speech steganography, with an accuracy of 60.8%, while the embedding rate is only 3%.

This research aims to compare several previous studies that have addressed steganography using various methods. The goal is to compare the quality and robustness of images produced by several spatial domain and transformation-based image steganography algorithms. This is achieved by applying Image Enhancement processes such as histogram equalization, contrast stretching, brightening, and gamma correction to the cover image before and after the message is embedded.

1.1 Literature Review

Cryptography Steganography is a technique used to conceal secret information within media such as images, videos, and audio signals. In image steganography, confidential information is hidden within the cover image, making it invisible to other users when viewing the image.

Steganography has two main techniques: spatial domain and transformation. One frequently used method in the spatial domain is the Least Significant Bit (LSB). This method is not overly complex and allows for the storage of a considerable amount of messages on the cover object. It is closely related to binary numbers 0 and 1, where the last bit in the image is altered to embed data. The results of steganography using the LSB method are almost indistinguishable from the original image.

In audio steganography, the secret message is inserted into the digital audio signal with slight changes in the binary sequence of the corresponding audio file. There are also techniques that use IP datagrams, where hidden data is embedded in TCP/IP-based network datagrams such as the internet. The goal of this approach is to make the hidden datagram undetectable by network observers like sniffers or Intrusion Detection Systems (IDS). The information to be concealed is placed in the IP header of the TCP/IP datagram.

In the overall approach to steganography, the objective is to effectively hide data without being detected by others.

2. Research Methods

This research utilizes a proposed steganography method using Fibonacci sequence to represent the cover image. In this method, the image is represented in a Fibonacci sequence, allowing an increase in the bit depth from 8-bit to 12-bit. The experimental results of this method are compared with other existing steganography methods, demonstrating that not only is this method capable of embedding secret data at a high rate, but it also produces stego images with high quality in terms of peak signal-to-noise ratio (PSNR).

3. Result and Discussion

Steganography, as a technique for securing confidential information, involves concealing data within media with the primary goal of avoiding detection. In comparison to cryptography, steganography takes a different approach, focusing more on information concealment than encryption. This research aims to develop new strategies for hiding secret information in various types of media, including images, audio, and videos. The proposed approach combines cryptography and steganography to enhance security. The message is encrypted

using the AES algorithm and SHA-2 hash key to prevent potential attacks. This method also modifies the LSB algorithm by adding a key to organize the non-sequential hiding process.

The research findings illuminate the efficacy of the proposed method in bolstering resilience and security. The embedded decryption key in the encrypted image leverages machine learning and nearest-centroid group techniques. Spatial domain reading of LSB-M complicates attacks, challenging the identification of scattered key bits throughout the image. Rigorous testing yields above-average MSE values, substantiating the incapacity of malicious entities to discern the presence of stego data in the image.

Steganography methods employing LZMA text compression facilitate the comprehensive concealment of text within an image. The Android application development presented facilitates .apk file transmission via WhatsApp, fortifying security through the amalgamation of steganography and LZMA compression. This application's paramount advantage lies in dual security provision, attributed to the utilization of the XOR LSB substitution method and an 8-bit random secret key initially XORed with RGB colors for enhanced data hiding security and sharing.

The utilization of the Arithmetic Coding algorithm for data compression and decompression, coupled with the SHA-256 hash function for authentication, is a pivotal component. The prototype named Ste-Chy seamlessly incorporates these techniques, resulting in the successful creation of an image acceptable to users with adequate quality, by hiding secret messages alongside the target image for secret authentication purposes. Larger secret messages achieve higher data compression ratios through data compression techniques.

Employing the histogram of oriented gradient (HOG) algorithm identifies the dominant edge direction in each 2x2 block of the cover image. Blocks of interest (BOIs) are adaptively determined based on the gradient and angle of the cover image. Subsequently, the PVD algorithm hides secret data in the dominant edge direction, while LSB substitution is employed on the remaining two pixels. Experiments confirm that this scheme provides high embedding capacity and better visual quality compared to other PVD and LSB methods [10]. In audio files, steganography as a cover utilizes Lifting Wavelet Transform (LWT) and Dynamic Key (DK) techniques combined with AES encryption. This technique employs frames as Dynamic Keys, encrypting secret data using AES with these Dynamic Keys, and subsequently embedding it in audio frames using LWT. The decryption process can be executed using the marked frame without requiring a manual key.

Additionally, filter operations are heavily contingent on the working color space, with substantial variations across different color spaces. Although not always apparent, this factor is crucial, particularly in high-quality color imaging. Initial processing is imperative for image embedding within the system, demanding considerable effort and testing to ensure success, exemplified in cases of concealing longer text messages and small image files in JPEG cover files for later transmission via Facebook.

The application of steganography in images employing reversible logic based on Quantum Dot Cellular Automata (QCA) is a notable inclusion. The Feynman gate serves as a reversible encoder and decoder for image steganography. The nano communication circuit for image steganography, incorporating an encoder/decoder circuit utilizing QCA, shows lower quantum costs compared to conventional designs, with a 28.33% increase in area over the complementary metal-oxide-semiconductor circuit. The LSB method is employed for image steganography, with parameters such as signal-to-noise ratio (SNR), peak SNR, and mean squared error (MSE) evaluated. This research encompasses the development of multiphase encryption algorithms to augment data security. An Android application is constructed to test these algorithms, presenting validation results based on parameter evaluations encompassing time complexity, security, and data size.

In a forensic context, steganography often emerges, particularly in anti-forensic techniques. An application is developed to scan, hash, and analyze hidden information in images, videos, or audio files on Android devices, with mobile data connectivity facilitated via USB debug using ADB. Following data retrieval, the application executes hash functions on selected options to preserve data integrity. A scanning module is implemented to detect the presence of hidden data in Android device files. This application furnishes extraction buttons and

reports for further analysis and decision-making, substantiating its concept and enabling Forensic Investigators to scrutinize Android phones, ensuring the accessibility of potential evidence. The ensuing discussion spans various steganography techniques, the artifacts generated, and forensic investigation tools implemented to detect and extract steganography in mobile devices.

4. Conclusions

Building upon the previous discussion, the technique of steganography offers a diverse array of methods that can be applied across various platforms. Among these methods, the Least Significant Bit (LSB) technique has gained popularity over other options. The popularity of the LSB method is attributed to its simplicity in concealing information, leading to continuous advancements with the introduction of new elements and integration with other techniques, including cryptography. The advantage of LSB steganography lies in utilizing the last bit of each pixel to embed secret information, ensuring that the quality of the stego image remains optimal after concealment. Research utilizing the LSB steganography method has consistently demonstrated low error rates, reinforcing the effectiveness and reliability of this technique.

A recommendation is to maintain a focus on developing and implementing steganography methods that blend convenience and security. Integration with cryptographic techniques can be a smart approach to enhance the security level of hidden information. Furthermore, it is crucial to continually explore the potential development of other steganography methods to preserve the novelty and relevance of techniques in addressing increasingly complex information security challenges. A profound understanding of the strengths and weaknesses of each method can also aid in selecting the most appropriate one based on the specific needs of a given context or application.

5. References

Arun C, Murugan S. "Design of image steganography using LSB XOR substitution method." Proc 2017 IEEE Int Conf Commun Signal Process ICCSP 2017 2018;2018-Janua:674–7. DOI: 10.1109/ICCSP.2017.8286444.

Carneiro Tavares JR, Madeiro Bernardino Junior F. "Word-Hunt: A LSB Steganography Method with Low Expected Number of Modifications per Pixel." IEEE Lat Am Trans 2016;14:1058–64. DOI: 10.1109/TLA.2016.7437258.

Yang W, Tang S, Li M, Cheng Y, Zhou Z. "Steganalysis of low embedding rates LSB speech based on histogram moments in frequency domain." Chinese J Electron 2017;26:1254–60. DOI: 10.1049/cje.2017.09.026.

AL-Shaaby AA, AlKharobi T. "Cryptography and Steganography: New Approach." Trans Networks Commun 2017;5. DOI: 10.14738/tnc.56.3914.

Danuputri C, Mantoro T, Hardjianto M. "Data Security Using LSB Steganography and Vigenere Chiper in an Android Environment." Proc - 4th Int Conf Cyber Secur Cyber Warf Digit Forensics, CyberSec 2015 2016:22–7. DOI: 10.1109/CyberSec.2015.14.

Rehman A, Saba T, Mahmood T, Mehmood Z, Shah M, Anjum A. "Data hiding technique in steganography for information security using number theory." J Inf Sci 2019;45:767–78. DOI: 10.1177/0165551518816303.

Anwar M, Sarosa M, Rohadi E. "Audio steganography using lifting wavelet transform and dynamic key." Proceeding - 2019 Int Conf Artif Intell Inf Technol ICAIIT 2019 2019:133–7. DOI: 10.1109/ICAIIT.2019.8834579.