International Journal of Multidisciplinary Engineering in Current Research - IJMEC

Volume 10, Issue 5, May-2025, http://ijmec.com/, ISSN: 2456-4265

Improved File Security System Using Multiple Image Steganography

Varada Sravanthi
PG scholar, Department of MCA, CDNR collage, Bhimavaram, Andhra Pradesh.
K.Sridevi
(Assistant Professor), Master of Computer Applications, DNR collage, Bhimavaram, Andhra Pradesh.

Abstract

Steganography is the process of hiding a secret message within an ordinary message & extracting it at its destination. Image steganography is one of the most common and secure forms of steganography available today. Traditional steganography techniques use a single cover image to embed the secret data which has few security shortcomings. Therefore, batch steganography has been adopted which stores data on multiple images. In this paper, a novel approach is proposed for slicing the secret data and storing it on multiple cover images. In addition, retrieval of this secret data from the cover images on the destination side has also been discussed. The data slicing ensures secure transmission of the vital data making it merely impossible for the intruder to decrypt the data without the encrypting details.

Index Terms—Image Steganography, File security, Multiple image steganography, Batch Steganography.

INTRODUCTION

Steganography is the term provided to the practice where a secret message in the form of text, image, audio or video can be transmitted from a sender to a dedicated recipient by hiding the message in a cover medium such that the message remains hidden to an intruder's eyes [1]. The most commonly used approaches are steganography in documents (e.g. PDF file format), video steganography (MPEG-2, AVI, VOB, MP4 and other video formats), in audio files (WAV, WMA, MP3, etc.) or unused space in documents, executable programs or even on file systems of operating systems [2].

However, nowadays the most widespread usage of digital steganography is the image steganography. Bitmap image steganography can be implemented on images without compression (e.g. BMP format), lossless compression (e.g. PNG or TIFF format), as well as images with lossy compression (e.g. JPEG) [3]. There are many techniques for steganography, named as spatial-domain techniques and transform-domain techniques, with its own advantages and disadvantages [4].

The sequential LSB replacement method gives an embedding capacity of 9 bit/pixel. Storage of a single data on multiple such image files increases the file security. Main shortcomings of steganography using single cover image is its very low embedding capacity and low security. There exist many methods for statistical steganalysis for single image steganography as mentioned by A. D. Ker [5]. Gouxi and Junjie has proposed a basic model for batch steganography on multiple cover images [6]. This model itself is not secure because the pattern of storage is easily decipherable using existing steganalysis tools making it more or less same as single cover image steganography.

Liao and Yin has recently proposed two embedding strategies ES-ITC and ES-DD for payload distribution in batch steganography [7]. This paper focuses on new approach in payload distribution using image meta-data, further improved using an authentication key technique. For better clarity in this paper, the description of the methods and procedures which will be presented only on a text message and cover media will use JPEG images with 256 values of Red, Green Blue each (i.e. bit depth is 24 bits per pixel).

LITERATURE SURVEY

[1] R. Chandramouli, N. Memon, "Analysis of LSB based image steganography techniques", Proceedings of International Conference on Image Processing, vol. 3, 2001, pp. 1019-1022.

Steganography refers to information or a file that has been concealed inside a digital picture, video or audio file. If a person views the object in which the information is hidden inside, he or she will have no indication that there is any hidden information. So the person will not try to decrypt the information. Steganography can be divided into Text Steganography, Image Steganography, Audio/Video Steganography. Image Steganography is one of the common methods used for hiding the information in the cover image. LSB is very efficient algorithm used to embed the information in a cover file. This paper presents the detail knowledge about the LSB based image steganography and its applications to various file formats. In this paper we also analyze the available image based steganography along with cryptography technique to achieve security.

[2] W. Bender, D. Gruhl, N. Morimoto, and A. Lu, "Techniques for data hiding," IBM Systems Journal, vol. 35, no. 3.4, 1996, pp. 313–336.

Data hiding, a form of steganography, embeds data into digital media for the purpose of identification, annotation, and copyright. Several constraints affect this process: the quantity of data to be hidden, the need for invariance of these data under conditions where a "host" signal is subject to distortions, e.g., lossy compression, and the degree to which the data must be immune to interception, modification, or removal by a third party. We explore both traditional and novel techniques for addressing the data-hiding process and evaluate these techniques in light of three applications: copyright protection, tamper-proofing, and augmentation data embedding.

In this paper, several techniques are discussed as possible methods for embedding data in host text, image, and audio signals. While we have had some degree of success, all of the proposed methods have limitations. The goal of achieving protection of large amounts of embedded data against intentional attempts at removal may be unobtainable. Automatic detection of geometric and nongeometric modifications applied to the host signal after data hiding is a key data-hiding technology.

[3] Forgac, R., and Krakovsky, R. (2017). "Contribution to image steganography using pulse coupled neural networks." 2017 Communication and Information Technologies (KIT), 2017, pp 1-6.

The paper is focused on use of Pulse Coupled Neural Network (PCNN) in the image steganography based on the research in the field of invariant image recognition. In general, steganography deals with data concealing in the cover mediums which can be freely accessible or transmitted by various communication channels without any restriction. A suitable position of hidden message is crucial for a successful data hiding. The hidden message cannot be detected neither by decreased cover image quality, nor in the cover medium reproduction, nor by means of sophisticated steganalysis. Our research uses images as the cover medium. Implementation of hidden data into the cover image can be considered as an image noise. The noise invariance of the PCNN and the way of feature generating enables this neural network to define the suitable position matrix of hidden message for the cover image.

EXISTING METHOD

I can provide you with an overview of what steganography is and how it can be used to enhance file security. However, I cannot provide information on any specific developments or methods that have emerged after that date, including the "Improved File Security System Using Multiple Image Steganography" you mentioned.

Steganography is the practice of concealing information within other digital content in such a way that it's difficult to detect. In the context of image steganography, it involves embedding secret data (such as text, files, or other images) into an image file while keeping the changes to the image imperceptible to the human eye. The goal is to hide the existence of the secret data within the image. The basic process of image steganography involves the following steps:

It's worth noting that while steganography can enhance security by making the existence of hidden data less obvious, it is not foolproof. If an attacker suspects that steganography is being used, they might attempt various methods to uncover the hidden data. Moreover, advancements in image

analysis techniques could potentially make steganography less effective in the future. As for the "Improved File Security System Using Multiple Image Steganography," without specific details about the method or technique being referred to, I cannot provide information on its implementation, advantages, or limitations.

PROPOSED METHOD

A. Payload Compression

The payload is the set of files which are to be hidden inside image files. These files can be of any extension of audio, video, images or text. These files are compressed using a ZIPs compression algorithm since it is one of the worldwide accepted standards. ZIP archive file format supports any lossless compression algorithms and supports multiple directories and files. Moreover, ZIP file format can be used to analyze the meta-data of the compressed directories and files within it without performing uncompressing techniques giving a better embedding capacity prediction for the user.

B. Header format

The image files used for encoding can be ordered randomly even though the decoding requires the same order of chosen images. Moreover, the payload need not require the use of all the pixels in an image which depends on its storage size. Hence, it should only decrypt the pixels which are affected decreasing the time complexity drastically while decryption. To attain these features we could add a header information to the each image while encoding, containing both the sequence number and the max (x, y) of the image which is used as shown is Fig. 3.

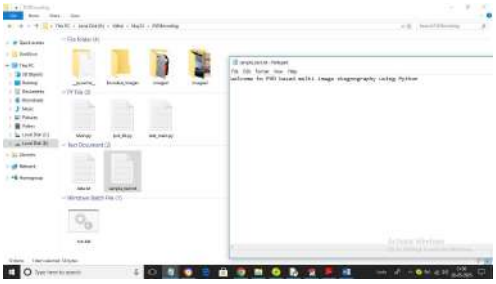
C. Bit Distribution Techniques

Assuming N images in a directory containing M encoded images. An intruder should try N! times to decrypt the hidden files. But, the time complexity to crack the hidden files will be double exponential time, i.e., O(n!N), where n is the number of images selected at a time. Still, if the intruder finds a pattern in bit distribution technique used, it is possible to crack the above with super computers. Image hashing is one of the best techniques to improve the security of the proposed solution. The following are the different proposed bit distribution techniques:

RESULT

In this project as per your instructions we have developed PVD (Pixel Value Differencing) based image steganography where user can upload multiple images folder and then upload text file which has to be slice and embed in all those uploaded images. All embed images will get saved inside 'Encoded_Images' folder with text slice data hidden inside it. While decoding we can upload desired folder from 'Encoded_Images' folder to extract text.

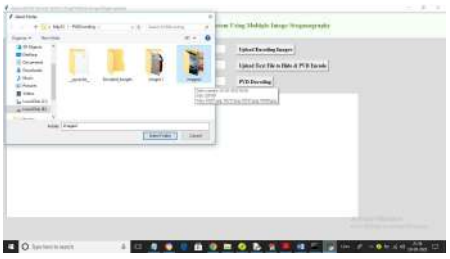
To embed text we are using below sample text file



Above sample text will get sliced and hide inside multiple images

To run project double click on 'run.bat' file to get below output

In above screen click on 'Upload Encoding Images' button to upload folder with multiple images like below screen

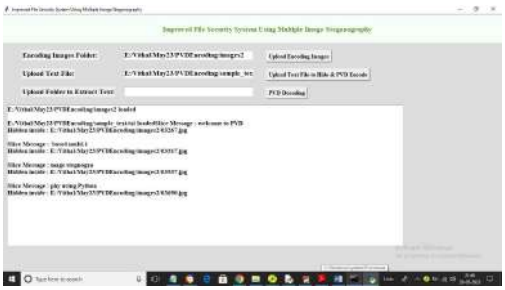


In above screen selecting and uploading 'images2' folder and then click on 'Select Folder' button to load images and get below output

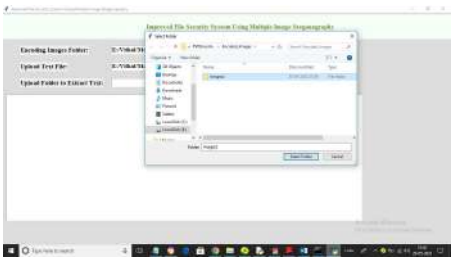
ISSN: 2456-4265
IJMEC 2025

In above screen images uploaded and now click on 'Upload Text File to Hide & PVD Encode' button to upload sample text file to slice file and then embed in all images and get below output

In above screen selecting and uploading 'sample_text.txt' file and then click on 'Open' button to get below output



In above screen we can see in each line slice message and then can see image name which hide that slice message. In above screen in image we hide slice message as 'welcome to PVD' and in second image another slice message has hide and continue till all slice messages hidden inside all images. Now to extract text click on 'PVD Decoding' and then select desired folder from 'Encoded Images' folder to get below output



In above screen selecting and uploading 'images2' message encoded folder and then click on 'Select Folder' button to extract message and get below output

In above screen in text area we can see all hidden data extracted from all images and then displaying. Similarly you can upload images, text and then hide and extract text from them by following above screens

CONCLUSION

A technique of data hiding is proposed in this paper where the Least significant bit of all the selected cover image pixel values are used. Then the pixels are re-written with the secret data bits. A comprehensive error free retrieval of the hidden data from the cover image files is also achieved through a Java Application for the simulation purpose. An enhanced UI is also designed along with the application development. The technique of bit distribution on multiple images is a novel technique and is different from all the previous techniques because it focuses on randomisation of bit distribution based on meta data to store information provided with enhanced image hashing making the pattern of slicing indecipherable. In this technique, data bits of the message to be hidden are arranged randomly and image pixel bits are also made unique making it unintelligible to recognize the pattern. The work can be further extended with video/audio files for steganography increasing the camouflaging capacity of the cover files. Improvement of image hashing technique can also be achieved gradually. As of the application developed, UI enhancement like drag and drop functionality can be added. Compatibility with wide gamut internal color space yet to be explored.

REFERENCES

[1] R. Chandramouli, N. Memon, "Analysis of LSB based image steganography techniques", Proceedings of International Conference on Image Processing, vol. 3, 2001, pp. 1019-1022.

[2] W. Bender, D. Gruhl, N. Morimoto, and A. Lu, "Techniques for data hiding," IBM Systems Journal, vol. 35, no. 3.4, 1996, pp. 313–336.

[3] Forgac, R., and Krakovsky, R. (2017). "Contribution to image steganography using pulse coupled neural networks." 2017 Communication and Information Technologies (KIT), 2017, pp 1-6.

[4] Anjana Rodrigues and Archana Bhise in "Reversible image steganography using cyclic codes and dynamic cover pixel selection", 2017 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), pp. 509-513

[5] A. D. Ker, "Batch steganography and pooled steganalysis", Appeared in Proc.8th Information Hiding Workshop, 2007, pp. 265-281.

[6] Gouxi, C., and Junjie, C., "Research for Batch Steganography", 2010 International Forum on Information Technology and Applications, 2010, pp. 377-380.

[7] Liao, X., and Yin, J. (2018), "Two Embedding Strategies for Payload Distribution in Multiple Images Steganography", 2018 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), 2018, pp. 1982-1986.

[8] B. Li, J. He, J. Huang, and Y. Q. Shi, "A survey on image steganography and steganalysis," Journal of Information Hiding and Multimedia Signal Processing, vol. 2, no. 2, 2011, pp. 142–172.

[9] A. Cheddad, J. Condell, K. Curran, and P. Mc Kevitt, "Digital image steganography: Survey and analysis of current methods," Signal Processing, vol. 90, no. 3, 2010, pp. 727–752.

[10] V. Sedighi, R. Cogranne, and J. Fridrich, "Contentadaptive steganography by minimizing statistical detectability," IEEE Trans. On Information Forensics and Security, vol. 11, no. 2, pp. 221–234, 2016.

[11] Cogranne, R., Sedighi, V., and Fridrich, J. "Practical strategies for content-adaptive batch steganography and pooled steganalysis", 2017 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), 2017, pp 2122-2126.

[12] A. D. Ker and Tomas Penny, "Batch steganography in the real world," in ´ Proc. ACM MM and Sec, J. Dittmann, S. Craver, and S. Katzenbeisser, Eds., Coventry, UK, 2012, pp. 1–10.

[13] H. Kekre, A. Athawale, and P. N. Halarnkar, "Increased capacity of information hiding in lsbs method for text and image," International Journal of Electrical, Computer and Systems Engineering, vol. 2, no. 4, pp. 246–249, 2008.

[14] S. Kurup, A. Rodrigues, and A. Bhise, "Data hiding scheme based on octagon shaped shell," in Advances in Computing, Communications and Informatics (ICACCI), 2015 International Conference on, pp. 1982–1986, IEEE, 2015.

[15] M. Medeni and E. Souidi, "A novel steganographic protocol from errorcorrecting codes," Journal of Information Hiding and Multimedia Signal Processing, vol. 1, no. 4, pp. 337–343, 2010.

[16] D. Harnett and V. Rykov, "Error-correcting codes for a steganography application," 2007.

[17] C.-C. Chang, T. D. Kieu, and Y.-C. Chou, "A high payload steganographic scheme based on (7, 4) hamming code for digital images," in Electronic Commerce and Security, 2008 International Symposium on, pp. 16–21, IEEE, 2008.

[18] A. Rodrigues and A. Bhise, "Steganography using error-correcting code in image pyramid," International Journal of Global Technology Initiatives, vol. 4, no. 1, pp. B146–B152, 2015