Journal of Science and Technology
ISSN: 2456-5660 Volume 8, Issue 12 (Dec -2023)
www.jst.org.in *DOI:https://doi.org/10.46243/jst.2023.v8.i12.pp208-218*

ELEVATING FILE SECURITY THROUGH ADVANCES MULTIPLE IMAGE STEGANOGRAPHY

Putta Srivani[1], B.Pallavi[2], B.Srija[2], T.Srinaina[2]

[1]Professor,[2]UG Students, Department of Cyber Security Engineering.
[1,2]Malla Reddy Engineering College for Women, Maisammaguda, Dhulapally, Kompally, Secunderabad-500100, Telangana, India.

To Cite this Article

Putta Srivani[1], B.Pallavi, B.Srija, T.Srinaina," ELEVATING FILE SECURITY THROUGH ADVANCES MULTIPLE IMAGE STEGANOGRAPHY" ***Journal of Science and Technology, Vol. 08, Issue 12 - Dec 2023, pp208-218***

Article Info

Received: 12-11-2023 Revised: 22 -11-2023 Accepted: 02-12-2023 Published: 12-12-2023

ABSTRACT

Background and History: In an age of increasing digital communication and data transfer, ensuring the security and privacy of sensitive information is paramount. Steganography, the art of hiding information within other data, has been used for centuries. In the digital realm, it plays a critical role in secure communication and information concealment. Traditional steganography methods often involve embedding information within a single image. While effective, this approach may be susceptible to detection, as single-image steganography can leave detectable traces, especially under sophisticated analysis. The primary challenge is to develop a robust system for multiple image steganography that can securely hide sensitive files within a set of images. This involves designing algorithms that distribute the information effectively across the images while maintaining imperceptibility and ensuring reliable extraction. Therefore, the rise of cyber threats and privacy concerns, there's a growing need for advanced techniques to protect sensitive files from unauthorized access or interception. Multiple image steganography, an emerging field, offers the potential for heightened security by spreading information across multiple images, making it even more challenging for potential adversaries to detect or extract. The project, "Elevating file security through advances in multiple image steganography," seeks to enhance file security by leveraging advanced techniques in multiple image steganography. By distributing the information across a set of images, this research endeavors to develop a system capable of securely concealing sensitive files. The algorithms utilized in this approach are designed to ensure imperceptibility and robustness against detection efforts. This advancement holds great promise for significantly improving the security of file transmission and storage, safeguarding critical information from unauthorized access or interception.

Keywords: Image Steganography, Security, Safeguarding.

1. INTRODUCTION

In today's digital era, safeguarding sensitive information during communication and data transfer is of utmost importance. Throughout history, the practice of steganography, which involves concealing information within other data, has been utilized to achieve this goal. As we transition to digital mediums, steganography plays a crucial role in ensuring secure communication and information concealment.

Traditionally, steganography focused on embedding information within a single image. While effective, this approach has its drawbacks, as it can be susceptible to detection, especially under sophisticated analysis. The challenge at hand is to develop a robust system for multiple image steganography that can securely hide sensitive files within a collection of images. This entails designing algorithms that efficiently distribute the information across the images while maintaining imperceptibility and ensuring reliable extraction. The increasing prevalence of cyber threats and privacy concerns underscores the need for advanced techniques to protect sensitive files from unauthorized access or interception. Multiple image steganography, an emerging field, offers the potential for heightened security by dispersing information across multiple images. This makes it even more challenging for potential adversaries to detect or extract the concealed data. The project, titled "Elevating file security through advances in multiple image steganography," aims to enhance file security by leveraging advanced techniques in multiple image steganography. The goal is to develop a system capable of securely concealing sensitive files by distributing information across a set of images. The algorithms employed in this approach are specifically designed to ensure imperceptibility and robustness against detection efforts. This advancement holds great promise for significantly improving the security of file transmission and storage, safeguarding critical information from unauthorized access or interception. In the current era of digital communication and data transfer, the protection of sensitive information is a critical concern. Steganography, a practice with historical roots, involves concealing data within other information and has become increasingly relevant in the digital landscape for ensuring secure communication and information protection. Traditional steganography methods have typically focused on embedding information within a single image. While effective, this approach is not fool-proof and can be vulnerable to detection, particularly under sophisticated analysis. The primary challenge lies in developing a robust system for multiple image steganography, where sensitive files can be securely hidden within a group of images. This task requires the creation of algorithms that can distribute information effectively across these images while maintaining imperceptibility and enabling reliable extraction. The growing prevalence of cyber threats and concerns about privacy highlight the necessity for advanced techniques to safeguard sensitive files from unauthorized access or interception. Multiple image steganography, an emerging field, offers the potential for enhanced security by dispersing information across several images. This complexity makes it considerably more challenging for potential adversaries to detect or extract concealed data. The objective of the project, titled "Elevating file security through advances in multiple image steganography," is to improve file security by harnessing advanced techniques in multiple image steganography. The aim is to create a system capable of securely concealing sensitive files by distributing information across a set of images. The algorithms employed in this approach are meticulously designed to ensure imperceptibility and robustness against detection efforts. This advancement holds significant promise for enhancing the security of file transmission and storage, protecting critical information from unauthorized access or interception.

2. LITERATURE SURVEY

B. Sultan,et.al[1] In this project The success of deep learning based steganography has shifted focus of researchers from traditional steganography approaches to deep learning based steganography. Various deep steganographic models have been developed for improved security, capacity and invisibility. In this work a multi-data deep learning steganography model has been developed using a well known deep learning model called Generative Adversarial Networks (GAN) more specifically using deep convolutional Generative Adversarial Networks (DCGAN). The model is capable of hiding two different messages, meant for two different receivers, inside a single cover image. The proposed model consists of four networks namely Generator, Steganalyzer Extractor1 and Extractor2 network. The Generator hides two secret messages inside one cover image which are extracted using two different

extractors. The Steganalyzer network differentiates between the cover and stego images generated by the generator network. The experiment has been carried out on CelebA dataset. Two commonly used distortion metrics Peak signal-to-Noise ratio (PSNR) and Structural Similarity Index Metric (SSIM) are used for measuring the distortion in the stego image The results of experimentation show that the stego images generated have good imperceptibility and high extraction rates.

X. Liao,et.al[2] In this project With the coming era of cloud technology, cloud storage is an emerging technology to store massive digital images, which provides steganography a new fashion to embed secret information into massive images. Specifically, a resourceful steganographer could embed a set of secret information into multiple images adaptively, and share these images in cloud storage with the receiver, instead of traditional single image steganography. Nevertheless, it is still an open issue how to allocate embedding payload among a sequence of images for security performance enhancement. This article formulates adaptive payload distribution in multiple images steganography based on image texture features and provides the theoretical security analysis from the steganalyst's point of view. Two payload distribution strategies based on image texture complexity and distortion distribution are designed and discussed, respectively. The proposed strategies can be employed together with these state-of-the-art single image steganographic algorithms. The comparisons of the security performance against the modern universal pooled steganalysis are given. Furthermore, this article compares the per image detectability of these multiple images steganographic schemes against the modern single image steganalyzer. Extensive experimental results show that the proposed payload distribution strategies could obtain better security performance.

M. Srivastava,et.al[3] In this project Image Steganography is the artwork of concealing mystery data within the image such that the hacker will now no longer be capable of discover the records within inside the stego images. This is a useful approach to secure our sensitive information. Security has continually been a main difficulty from last many years to existing days. The topic of interest to researchers has long been the development of secure technologies for sending data to anyone other than the recipient without revealing it. Therefore, from nowadays, researchers have evolved many strategies to meet the steady transfer of information and steganography is one in all them. In this paper, we work on two techniques for hiding information in the image. First, we do analysis on LSB for storing information bit. As the technique is known to all, the attacker will be able to easily reveal the information, this makes image steganography unsecured. Secondly, R-Color Channel encoding with RSA set of rules for offering extra protection to information in addition to our information hiding approach. The proposed approach makes use of a red color channel for hiding information bits and the following bits for RGB pixel values of the original image. This paper presents the performance analysis of two most popular algorithms, LSB and RSA along with image steganography.

G. Benedict,et.al[4] In this project 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.

S. Mukhopadhyay,et.al[5] In this The paper proposes a scheme for achieving steganography with multiple encrypted monochromatic images with keys obtained from a synchronized system of

semiconductor lasers. The key selection scheme for steganography determines the robustness of the application. It is in this area that steganography may benefit from the properties of chaos synchronization. The encryption principle of the new algorithm is analyzed quantitatively by various statistical tests. The cover image used in the technique is also obtained from the visual representation of the chaotic sequences. This new scheme enjoys the benefit of added security, high key space, high embedding capacity, imperceptibility and robustness of the hidden information in conjunction with Least Significant Bit (LSB) based substitution. The result is important from the perspective of introducing a mechanism to multiplex and simultaneously transmit multiple images.

A. S. Ansari,et.al[6] This paper presents an image Steganography algorithm that can work for cover images of multiple formats. Having a single algorithm for multiple image types provides several advantages. For example, we can apply uniform security policies across all image formats, we can adaptively select the most suitable cover image based on data length, network bandwidth and allowable distortions, etc. We present our algorithm based on the abstract concept of image components that can be adapted for JPEG, Bitmap, TIFF and PNG cover images. To the best of our knowledge, the proposed algorithm is the first Steganography algorithm that can work for multiple cover image formats. In addition, we have utilized concepts like capacity pre-estimation, adaptive partition schemes and data spreading to embed secret data with enhanced security. The proposed method is tested for robustness against Steganalysis with favorable results. Moreover, comparative results for the proposed algorithm are very promising for three different cover image formats.

P. Grandhe,et.al[7] In this project Communicating online without fearing third-party interventions is becoming a challenge in the modern world. Especially the sectors like the military, and government organizations or private companies sharing sensitive information. They invest a lot of effort and cost into obtaining the advancement of safe communication techniques. Image processing encryption techniques using various algorithms promote security over communication channels and using different analysis methods make the tool stand out in providing security to the information. In today's world, there are various steganographic mechanisms that convert the secret message into stego medium and send it across various communication channels. Using algorithms like Blind Hide promotes the security of the message along with using multiple analysis methods that will further improve the tool in giving out information of encoded accuracy, size of stego of the secret message. The aim is to generate a tool that will give out a benchmark value of how precisely the message is stored in the cover file. Using Stego and bulk analysis the information about the presence of the stego medium in the message can be known to the user. All these analysis methods make the tool more enhanced and secure.

R. Joshi,et.al[8] in this There are advances in data stealth and forgery with the rise of technology and advances in data transmission. This arises the need for better and developed methods for data transmission. Data Transmission is an essential task in the current era, and equally important is the secure and safe information of that data. In the paper, batch steganography is used to secure data transmission from one end to the other. Often a password can be used for encoding the payload into the cover image. Here the data is encrypted using hashing and encryption techniques, SHA-256 and AES. The passwords used for encryption have been used after the logical operation XOR. Thus, the information has been encrypted twice using the XORed password for first and second input password for the next time. It increases the security of the data and makes the decryption almost impossible without knowing both the passwords and the encryption method. The encoded data is then embedded within the pixels of the original image using the LSB method. This prevents data theft and any possibilities of Man-in-the-Middle attacks since the time required for decrypting the data is drastically high without the knowledge of the inputs and the techniques used.

Z. Wang,et.al[9] In this paper, a more accurate image steganography method is proposed, where a multi-level feature fusion procedure based on GAN is designed. Firstly, convolution and pooling operations are added to the network for feature extraction. Then, short links are used to fuse multi-level feature information. Finally, the stego image is generated by confrontation learning between discriminator and generator. Experimental results show that the proposed method has higher steganalysis security under the detection of high-dimensional feature steganalysis and neural network steganalysis. Comprehensive experiments show that the performance of the proposed method is better than ASDL-GAN and UT-GAN.

3. PROPOSED SYSTEM

Pixel Value Differencing (PVD) in Multiple Image Steganography

Introduction:

- Pixel Value Differencing (PVD) is an innovative approach to steganography that operates in the spatial domain of images. While PVD is commonly applied to single images, its extension to multiple image steganography introduces new dimensions of security and capacity. The fundamental concept of PVD revolves around manipulating the pixel values of multiple images to embed hidden information.
- Pixel Value Differencing:
  In PVD, the difference between the pixel values of adjacent pixels is utilized for data embedding. By carefully adjusting these differences, information can be hidden without significantly altering the visual appearance of the images.
- Spatial Domain Embedding:
  PVD operates in the spatial domain, making it resilient to frequency-based attacks. Unlike frequency domain techniques that might be susceptible to transforms, PVD directly modifies pixel values for data concealment.

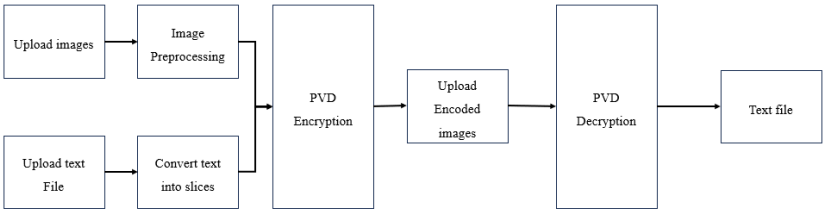


Figure 1: Architecture diagram of multiple image steganography

Multiple Image Steganography:

The extension of PVD to multiple images involves distributing hidden information across a set of images. This approach enhances security by dispersing the embedded data, making it more challenging for adversaries to detect or extract the complete message.

- Embedding Process:
  The embedding process in PVD-based multiple image steganography follows a series of steps:
- Image Preparation:

Select a set of cover images for embedding. These images act as carriers for different segments of the hidden message.

- Data Slicing:
  Divide the hidden message into segments corresponding to the number of selected cover images. Each segment is then embedded into the respective image.
- PVD Embedding:
  Apply the PVD algorithm to each image, adjusting pixel values based on the differences between adjacent pixels. The differences are manipulated to represent the hidden message.
- Secure Key Integration:
  Integrate a secure key into the embedding process to enhance security. The key determines how the pixel value differences are adjusted, and without it, extracting the hidden information becomes extremely challenging.
- Extraction Process:
  The extraction process is designed to retrieve the hidden message from the stego images:
- **Image Selection:**
  Choose the stego images containing segments of the hidden message.
- PVD Extraction:
  Apply the PVD algorithm in reverse to extract the differences between pixel values.
- Data Reconstruction:
  Reconstruct the hidden message segments from the extracted differences.
- Secure Key Utilization:
  Use the secure key during the extraction process to ensure accurate retrieval of the hidden information.

4. RESULTS AND DISCUSSION

4.1 Implementation description

- Tkinter Main Window Setup:

  The script initializes the main Tkinter window with a title and dimensions, serving as the GUI interface.

- Global Variables and PVD Object Initialization:

  Global variables (image_path and text_path) store paths for the selected image folder and text file. An instance of the pvd_lib class is created to handle PVD operations.

- Text Slicing Function (sliceText):

  Reads a binary text file and divides its content into blocks.Iterates through images in a specified folder, returning a list of text blocks and corresponding image file paths.

- PVD Encoding Function (PVDEncoding):

  Writes the sliced text message to a temporary file ("data.txt"). Creates a folder for encoded images if it doesn't exist. Utilizes the pvd_embed method from the pvd_obj instance to perform PVD encoding on each image.

- PVD Decoding Function (PVDDecoding):

  Iterates through encoded images in a specified folder.Uses the pvd_extract method

from the pvd_obj instance to perform PVD decoding on each image.Concatenates the extracted data from each image to reconstruct the original hidden text.

— Upload Image Function (uploadImage):

Opens a file dialog allowing the user to select an image folder.Displays the selected image folder path in the GUI.Upload Text Function (uploadText):Opens a file dialog allowing the user to select a text file.Displays the selected text file path in the GUI.Slices the text and performs PVD encoding on each image in the selected image folder.

— Extract Text Function (ExtractText):

Opens a file dialog allowing the user to select a folder containing encoded images.Displays the selected folder path in the GUI. Performs PVD decoding on each encoded image in the selected folder. Concatenates the extracted text from each image to reveal the original hidden message.

— GUI Elements:

Labels, entry widgets, buttons, and a text box create a user-friendly interface. Labels provide information or titles for various sections.Entry widgets allow users to input or display information.Buttons trigger specific actions when clicked.A text box displays information, messages, or the extracted text.

— Tkinter Main Loop:

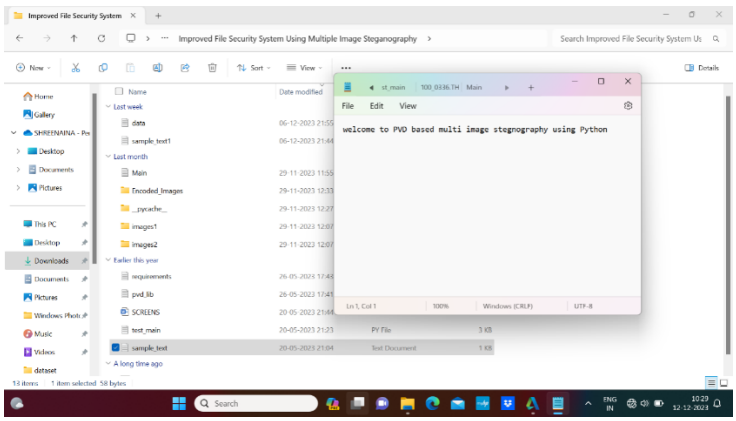
Initiates the Tkinter event loop, allowing the GUI to respond to user interactions and run the application.

4.2 Results and description

Improved File Security System Using Multiple Image Steganography

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.

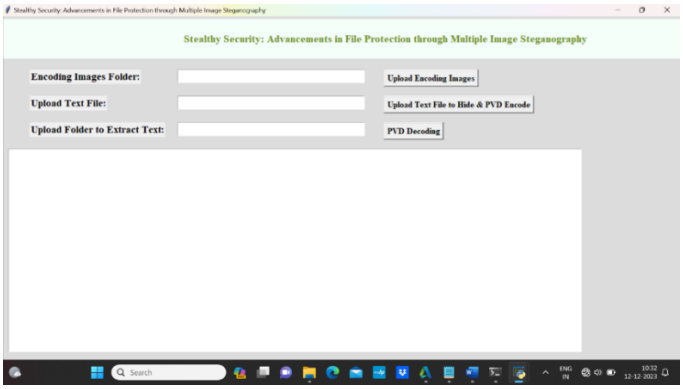
To embed text we are using below sample text file



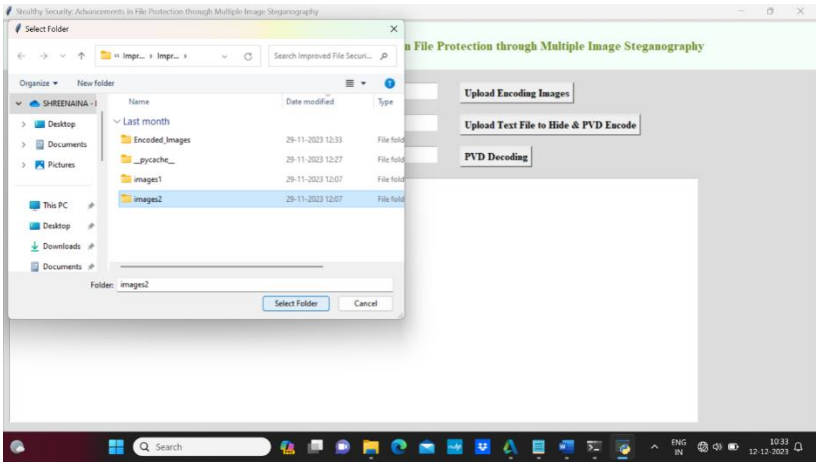
Above sample text will get sliced and hide inside multiple images

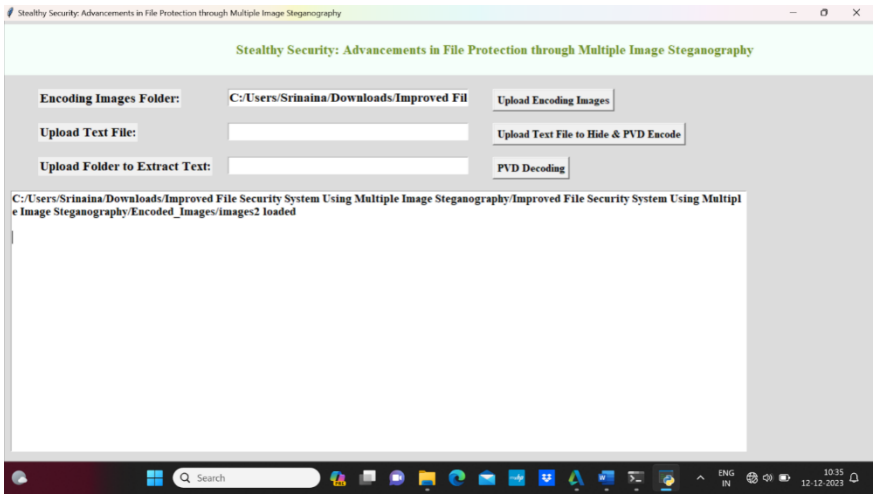
Journal of Science and Technology
ISSN: 2456-5660 Volume 8, Issue 12 (Dec -2023)
www.jst.org.in *DOI:https://doi.org/10.46243/jst.2023.v8.i12.pp208-218*

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



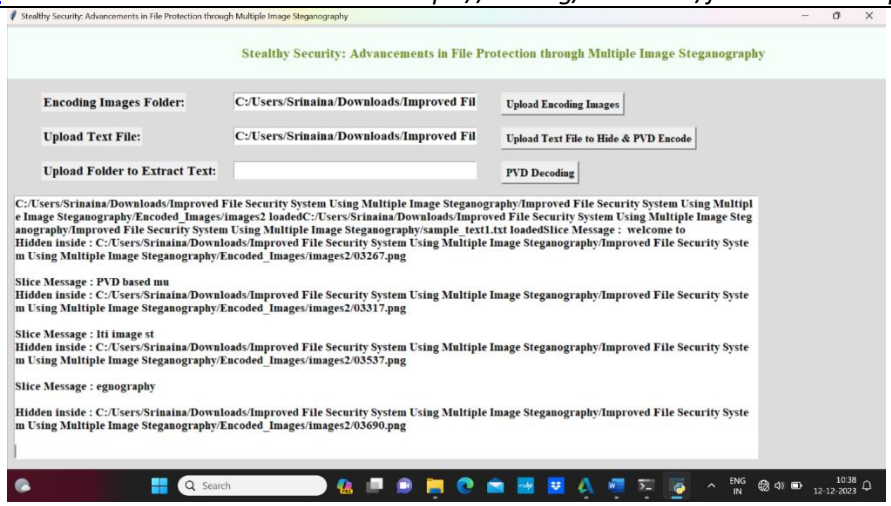
In above screen click on 'Upload Encoding Images' button to upload folder with multiple images like below screen



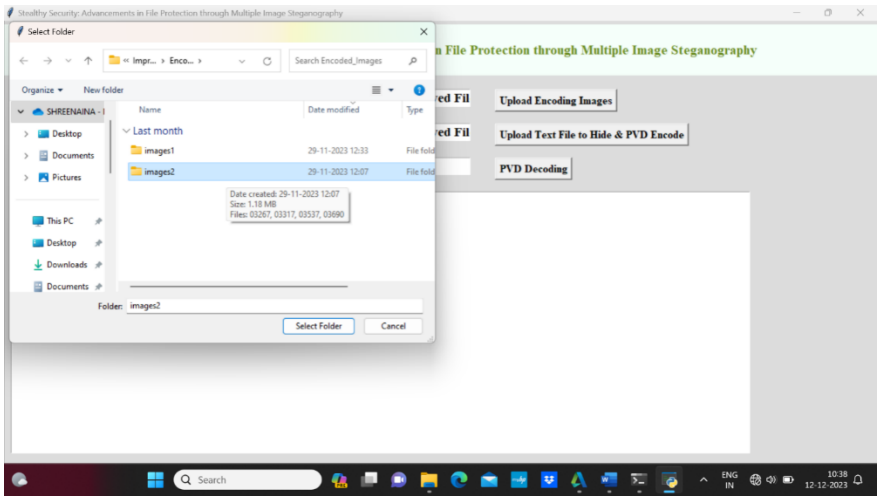


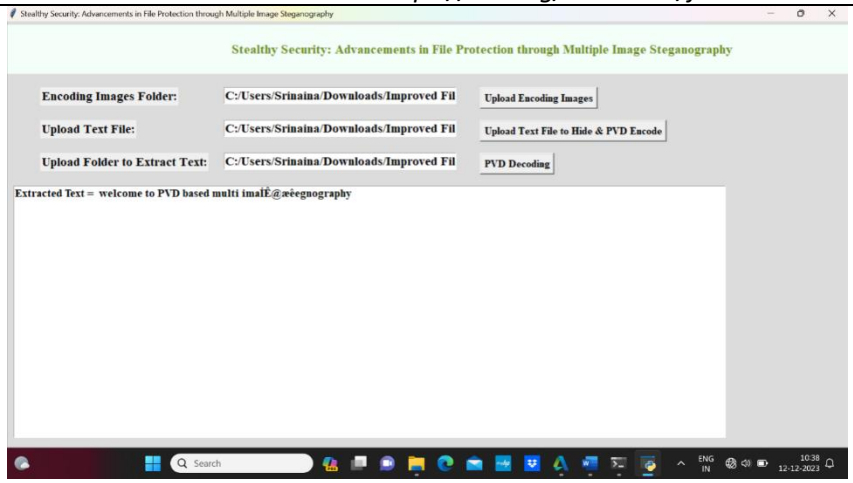
In above screen images uploaded and now click on 'Upload Text File to Hide & PVD Encode' button to upload sample text file to slice file and then embed in all images and get below output

Journal of Science and Technology
ISSN: 2456-5660 Volume 8, Issue 12 (Dec -2023)
www.jst.org.in *DOI:https://doi.org/10.46243/jst.2023.v8.i12.pp208-218*



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

5. CONCLUSION

multiple image steganography represents a significant advancement in the field of covert communication and secure data transmission. The technique of distributing hidden information across a series of images, coupled with the Pixel Value Differencing (PVD) algorithm, offers a potent combination of security, resilience, and imperceptibility. The strategic division of data, error-correction techniques, spread spectrum methods, and secret sharing schemes contribute to the robustness and reliability of the steganographic system.

The incorporation of cryptography and encryption enhances the confidentiality of the concealed information, while authentication and watermarking techniques provide mechanisms for verifying the integrity of the images. Hybrid approaches, integrating various steganographic methods and security measures, offer adaptability and versatility to meet diverse security requirements.

REFERENCES

[1]. B. Sultan and M. A. Wani, "Multi-data Image Steganography using Generative Adversarial Networks," 2022 9th International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India, 2022, pp. 454-459, doi: 10.23919/INDIACom54597.2022.9763273.

[2]. X. Liao, J. Yin, M. Chen and Z. Qin, "Adaptive Payload Distribution in Multiple Images Steganography Based on Image Texture Features," in IEEE Transactions on Dependable and Secure Computing, vol. 19, no. 2, pp. 897-911, 1 March-April 2022, doi: 10.1109/TDSC.2020.3004708.

[3]. M. Srivastava, P. Dixit and S. Srivastava, "Data Hiding using Image Steganography," 2023 6th International Conference on Information Systems and Computer Networks (ISCON), Mathura, India, 2023, pp. 1-6, doi: 10.1109/ISCON57294.2023.10112069.

[4]. A. G. Benedict, "Improved File Security System Using Multiple Image Steganography," 2019 International Conference on Data Science and Communication (IconDSC), Bangalore, India, 2019, pp. 1-5, doi: 10.1109/IconDSC.2019.8816946.

[5]. S. Mukhopadhyay and H. Leung, "Multi Image Encryption and Steganography Based on Synchronization of Chaotic Lasers," 2013 IEEE International Conference on Systems,

Man, and Cybernetics, Manchester, UK, 2013, pp. 4403-4408, doi: 10.1109/SMC.2013.751.

[6]. A. S. Ansari, M. S. Mohammadi and M. T. Parvez, "A Multiple-Format Steganography Algorithm for Color Images," in IEEE Access, vol. 8, pp. 83926-83939, 2020, doi: 10.1109/ACCESS.2020.2991130.

[7]. P. Grandhe, A. M. Reddy, K. Chillapalli, K. Koppera, M. Thambabathula and L. P. Reddy Surasani, "Improving The Hiding Capacity of Image Steganography with Stego-Analysis," 2023 IEEE International Conference on Integrated Circuits and Communication Systems (ICICACS), Raichur, India, 2023, pp. 01-06, doi: 10.1109/ICICACS57338.2023.10100146.

[8]. R. Joshi, A. K. Bairwa, V. Soni and S. Joshi, "Data Security Using Multiple Image Steganography and Hybrid Data Encryption Techniques," 2022 International Conference for Advancement in Technology (ICONAT), Goa, India, 2022, pp. 1-7, doi: 10.1109/ICONAT53423.2022.9725949.

[9]. Z. Wang, Z. Zhang and J. Jiang, "Multi-Feature Fusion based Image Steganography using GAN," 2021 IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW), Wuhan, China, 2021, pp. 280-281, doi: 10.1109/ISSREW53611.2021.00079.

[10]. X. Zhao and H. Huang, "Research on Image Steganography Based on Multiple Expansion Generation Adversarial Network," 2021 IEEE 3rd International Conference on Frontiers Technology of Information and Computer (ICFTIC), Greenville, SC, USA, 2021, pp. 361-366, doi: 10.1109/ICFTIC54370.2021.9647204.

[11]. B. Wei, X. Duan and H. Nam, "Image Steganography with Deep Learning Networks," 2022 13th International Conference on Information and Communication Technology Convergence (ICTC), Jeju Island, Korea, Republic of, 2022, pp. 1371-1374, doi: 10.1109/ICTC55196.2022.9952432.

[12]. M. Liu, W. Luo, P. Zheng and J. Huang, "A New Adversarial Embedding Method for Enhancing Image Steganography," in IEEE Transactions on Information Forensics and Security, vol. 16, pp. 4621-4634, 2021, doi: 10.1109/TIFS.2021.3111748.