



IMAGE STEGANOGRAPHY USING MACHINE LEARNING

¹KR Anirudh Yadav, ²Ravishankar, ³Abdulla Nishal, ⁴Aravind Nayak, ⁵Shreya Shetty, ⁶Suresha D

^{1,2,3}Student, ⁴Assistant Professor, ⁵Assistant Professor, ⁶Professor

^{1,2,3,4,5,6} COMPUTER SCIENCE AND ENGINEERING,

^{1,2,3,4,5,6} Srinivas Institute of Technology Mangaluru, India

Abstract : Image steganography concerns itself with the hiding of secret message information within digital images; hence, it is a covert communication technique. Cryptography scrambles the plaintext into an unreadable format, while steganography goes one step farther, hiding the plaintext's very existence. The interest of the project involves using the Least Significant Bit method in embedding hidden messages within images; pixel values are changed only at the very least possible, such that no conspicuous difference appears in the overall view of the image. The report highlights various theoretical aspects of image steganography, describes the methodology adopted in the implementation, and discusses security factors that must be taken into account. The report stresses the merits of the LSB approach in terms of simplicity, high capacity, and less degradation to visual quality of the image. The encoding and decoding of hidden messages have been implemented in Python using OpenCV and several other supporting libraries. A range of tests was conducted to evaluate the performance of the system regarding data capacity, security, and integrity of the image. The results confirm that LSB-based image steganography can effectively secure information that is sensitive to the maximum degree while maintaining almost the same appearance of the carrier image.

I. INTRODUCTION

The protection of important data has emerged as an extreme necessity in modern digital times. Steganography stands as an intriguing security method along with encryption since it enables hiding information within regular-looking data files. The detection of protected content becomes improbable through steganography because this method embeds secrets within unnoticeable data. The main focus of this initiative employs Image Steganography methods to blend secret data directly into digital pictures so they escape human observation. Digital image usage for communication and information transfer has led to a substantial rise in the need for embedded data protection. Steganography proves advantageous to law and business sectors alongside government institutions because secure transmission of important information remains necessary. This method selects images for hiding data instead of traditional encryption because it preserves both data confidentiality and ensures communication stays undetectable to unauthorized parties.

II. LITERATURE SURVEY

1) Jessica Fridrich (1999)

In the paper, various data hiding methodologies for digital images are studied. Jessica Fridrich is one of the pre-eminent researchers in the field of steganography. She investigated several techniques of image data hiding, concentrating principally on the LSB technique. In her work, she showed that electronic images could conceal secret texts while remaining imperceptibly altered to an observer; the relationship between that and the steganography's possibility of decrypting the information was also considered.

2) Neil F. Johnson and Sushil Jajodia (1998)

The research studies the practice of simple visual steganography through study of the least significant bit embedding approach. Through their overview, Johnson and Jajodia explained in detail how to effectively implement LSB insertion to achieve steganography. The authors outlined weaknesses of fundamental LSB techniques for steganography, including exposure during image processing, and recommended security strengthening by using encryption and randomization methods.

3) Petitcolas, Anderson, and Kuhn (1999)

A Survey on Information Hiding becomes the focus of this research paper. The study by this research team represents one of the most frequently referenced publications about steganography and information hiding methods. The researchers examined LSB-based steganography while informing stakeholders about simple techniques getting detected by statistical analysis. Reportedly, the researchers pointed out that LSB provides simple implementation, but robust secure steganographic systems require redundancy and encryption for maximum protection.

4) Berghel and O'Gorman (1996)

"The Protection of Ownership Rights Using Digital Watermarking Systems" represents the main topic of this research paper. The study by Berghel and O'Gorman centered on watermarked recognition, but their research recognized that these findings advanced steganographic techniques by demonstrating invisible and secure data implementation. The researchers made contributions to strengthen LSB steganographic methods based on their findings of resisting common attacks.

III. METHODOLOGY

Image Steganography Using Machine Learning

The implementation of machine learning-based image steganography consists of five essential stages that start with data preparation followed by model design and embedding process before moving to extraction process and ending with performance evaluation. The step-by-step instructions are presented through the following caption:

1. Problem Definition

The system training goal aims to develop intelligence for embedding secret messages within images with optimal distortion levels by learning crucial embedding patterns through machine learning models to make steganalysis detection practically difficult.

2. Dataset Preparation

A collection of standard digital images called Cover Images is obtained from CIFAR-10 and ImageNet alongside self-generated database. Recorded secret information includes randomly produced binary data, small images or texts embedded within cover images. The learning process demands pairs of two elements consisting of cover images matched with secret messages during the training phase.

3. Design of Machine-Learning Model

A neural network referred to as an encoder exposes secret data points into cover images thus generating stego images without detectable visual changes from the original. The revealing network refers to Decoder as the component which recovers hidden secrets from stego images. When using GANs the discriminator works optionally to determine whether stego images resemble original images and this mechanism drives the encoder to generate high-quality steganographic artifacts.

4. Embedding Process (Training Phase)

The Encoder system combines both a given secret message and cover visual content as it operates. A stego image emerges from the process that embeds the secret data into it. The secret message retrieval process takes place through the Decoder by analyzing the stego image. With GAN applications the Discriminator develops the ability to distinguish cover images from their corresponding stego versions.

Loss Functions Used: The reconstruction loss evaluates the accuracy with which hidden messages can be retrieved from the stego image. Perceptual Loss protects the stego image from having visual distortions which would reveal the embedded information. The encoder receives an adversarial loss which aids in developing undetectable stego images when GANs are implemented. The combination of various weighted objectives results in the total loss measurement.

5. Extraction Process (Testing Phase)

The Decoder accepts stego images that have been trained for this purpose. The decoder software first receives stego images to recover hidden secret information. The evaluation process assesses both the exactness of message recovery and the closeness of stego image appearance to its source cover image.

IV. Architecture of the off-Image Steganography System:-

Encoder (Hiding Network) Input: Cover Image (normal image) Secret Data (text or binary bits) Function: The encoder embeds the secret data into the cover image. Through learning the modification process the system adapts pixel value alterations that result in imperceptible changes.

Typical Structure: Convolutional Layers: For feature extraction from images. Concatenation Layer: Combines cover image features and secret data. The nature of Stego images (images including hidden data) is reconstructed by this layer.

Output: The output stego image displays identical visual appearance to its cover image.

2. **Decoder (Revealing Network)** Input: The secret data exists inside Stego Image (a visual match to the cover image).

Function: The stego image passes through the decoder network which performs the dual task of both recovery and reconstruction of the hidden secret.

Typical Structure: The primary function of these layers during extraction is to detect embedded detection features. The dense layer helps restore hidden secret information.

Output: Recovered Secret Message (or recovered bits).

3. **Discriminator (optional, for GAN-based systems)** Input: Stego Image and/or Cover Image

Function: Within GAN framework the discriminator operates as a model that differentiates between stego images with secret data and cover images without hidden content. Through its design the encoder receives pressure to create stego images which are more difficult to discover.

Typical Structure: Convolutional Neural Networks (CNN) classifier. Output: A probability (Real vs Fake).

V. ARCHITECTURE OF THE IMAGE STEGANOGRAPHY SYSTEM:-

1. **Enhancing Robustness Against Attacks**

The research stream should concentrate on improving the durability of stego images against regular image processing attacks that involve compression (e.g. JPEG) along with resizing, cropping and filtering and incorporating noise addition. The survival capability of hidden data will remain intact when images undergo changes during both transmission and storage through robustness improvements.

2. **Integrating Advanced Machine Learning Models**

Advanced architectural models including Transformers with diffusion models should be investigated to optimize both feature detection and data concealing abilities. These models demonstrate higher data capacity and improved detection resistance against steganalytic inspection methods.

3. **Developing Adaptive Embedding Techniques**

Future systems should include dynamic embedding since their data-hiding capabilities will decide optimal image regions to use according to texture and edge patterns and complexity metrics. Adaptive data hiding techniques would be more difficult to detect because they offer improved stealth features to steganographic systems.

4. **Supporting Other Media Types**

The image steganography concepts studied in this research can be generalized to include audio and video as well as three-dimensional digital models. The implementation of multi-modal steganography would enable more secure communication through several digital platforms.

5. **Implementing Real-Time Steganography Systems**

Future system optimizations will allow developers to create steganographic systems capable of real-time operations that perform instant message embedding and extraction in live video communications and secure streaming.

VI. IMPACT ON SOCIETY

1. Enhanced Privacy and Confidentiality

People along with organizations maintain secure communication of sensitive messages through steganography systems that operate without detection. The technology serves privacy rights by giving users secure information sharing capabilities which help journalists and whistleblowers and activists when operating under repressive governments.

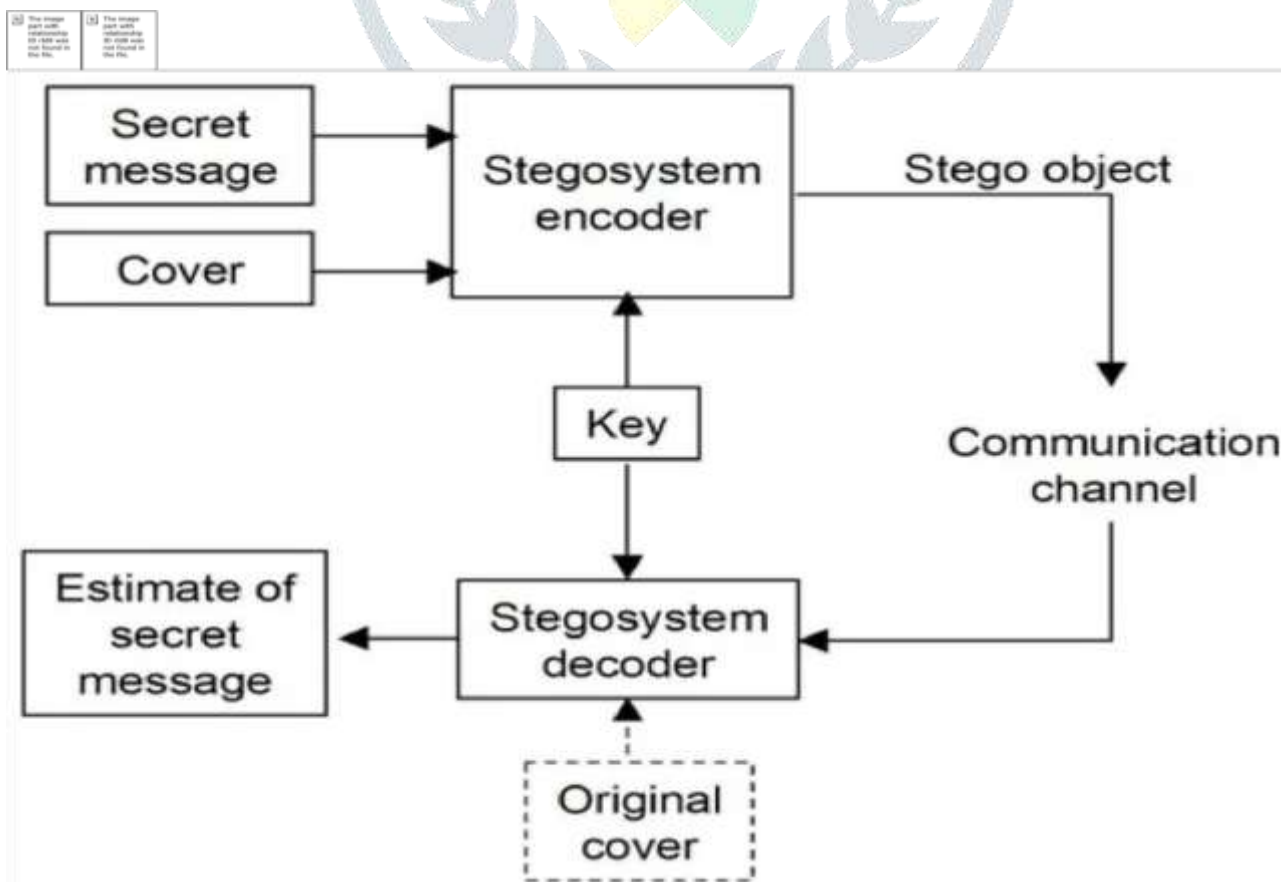
2. Secure Communication in Critical Fields

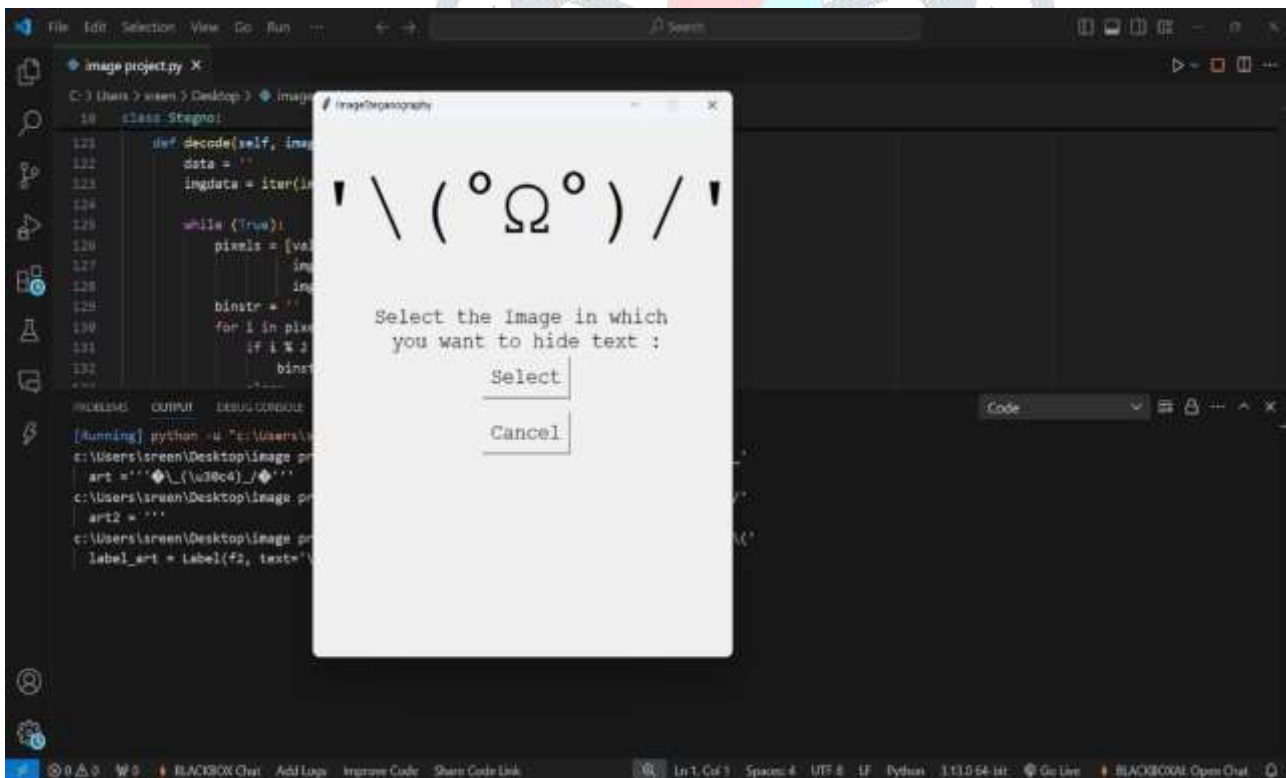
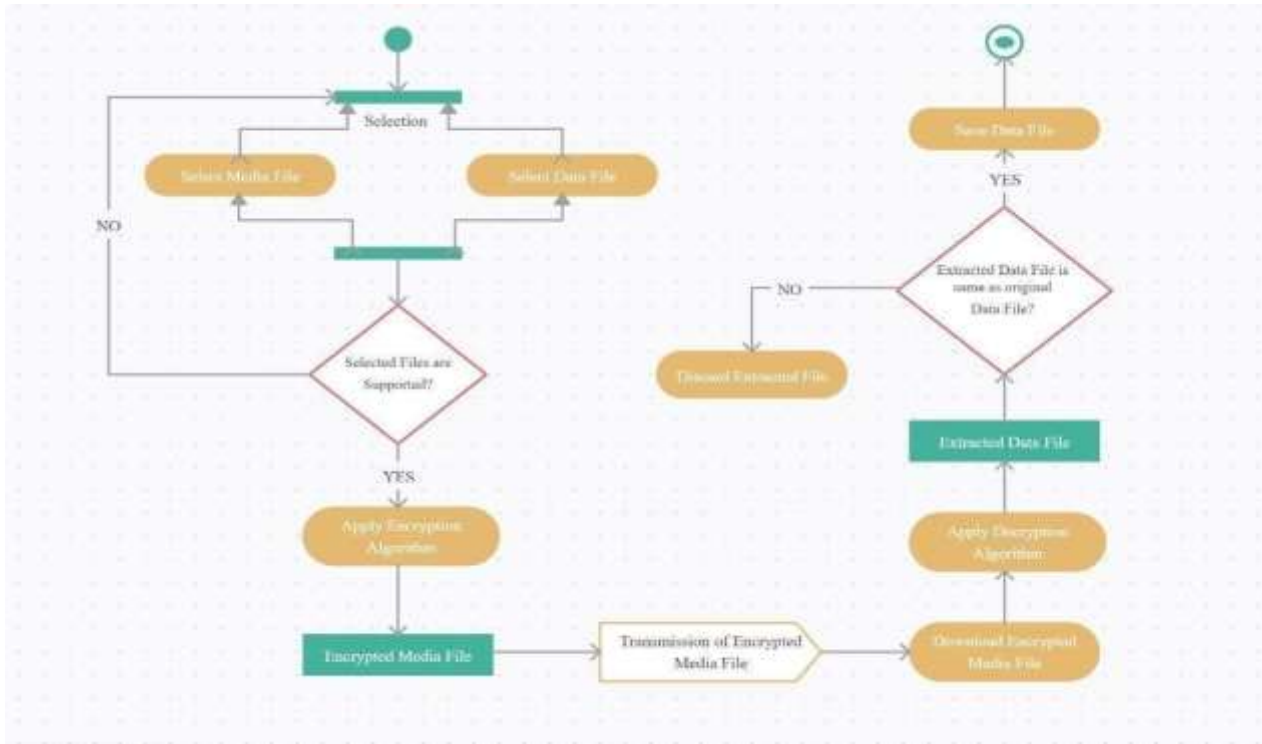
The defense industry together with government sectors and corporate organizations maintain absolute need for protecting their secret communications. Through the use of image steganography users can maintain secure classified information transfer which shields both personal information and national assets from digital espionage.

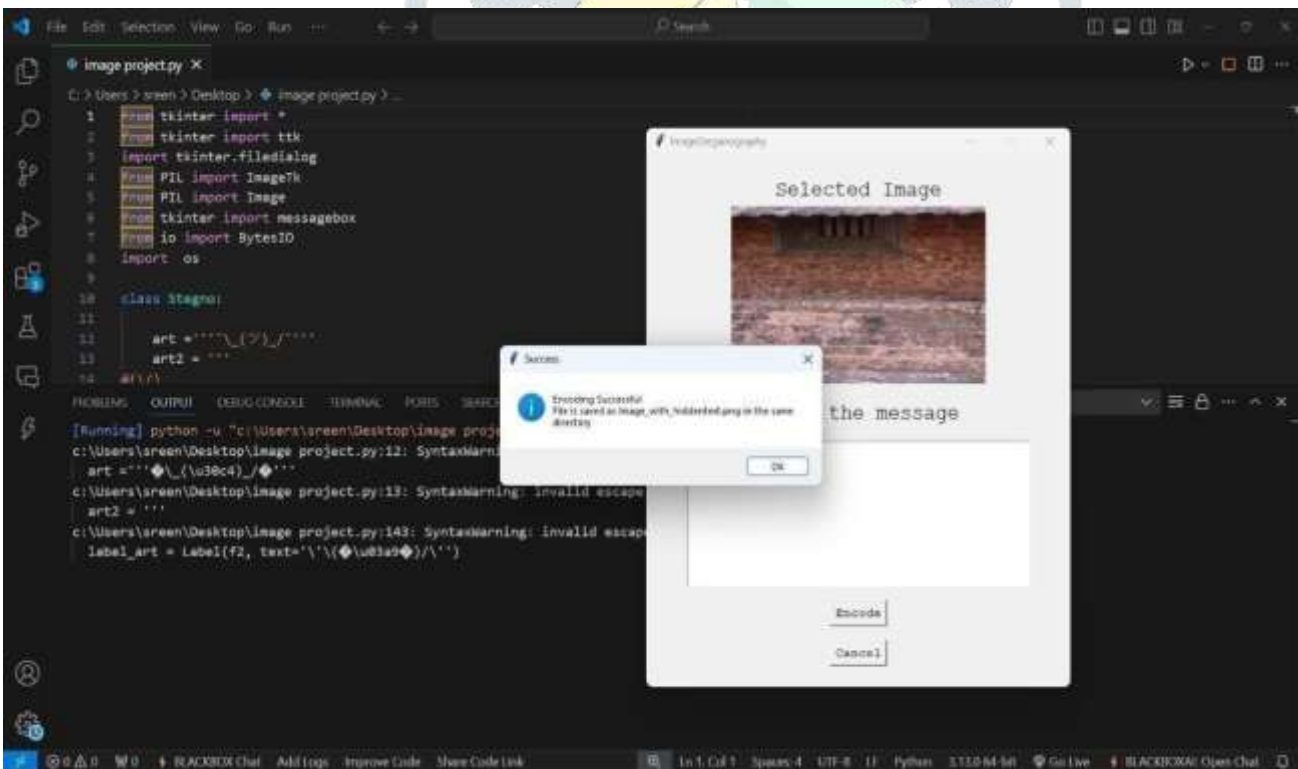
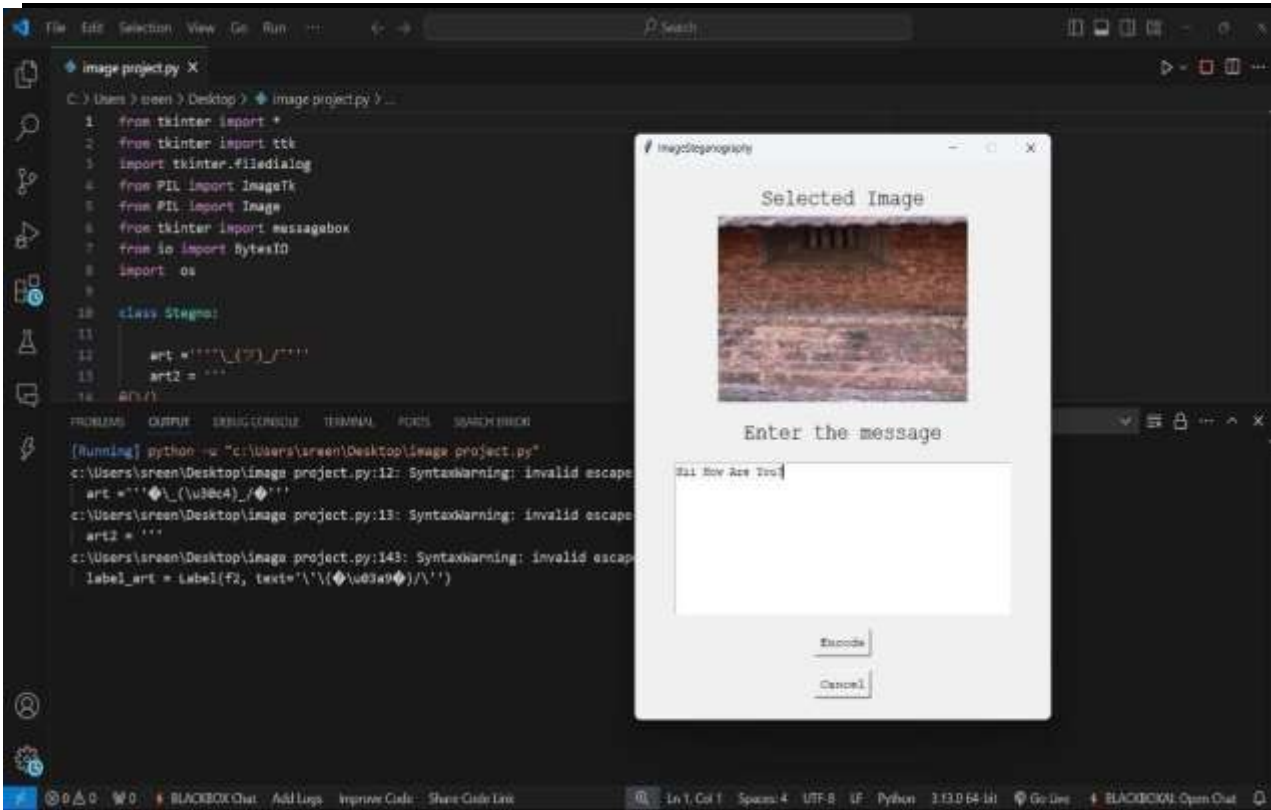
3. Preservation of Freedom of Expression

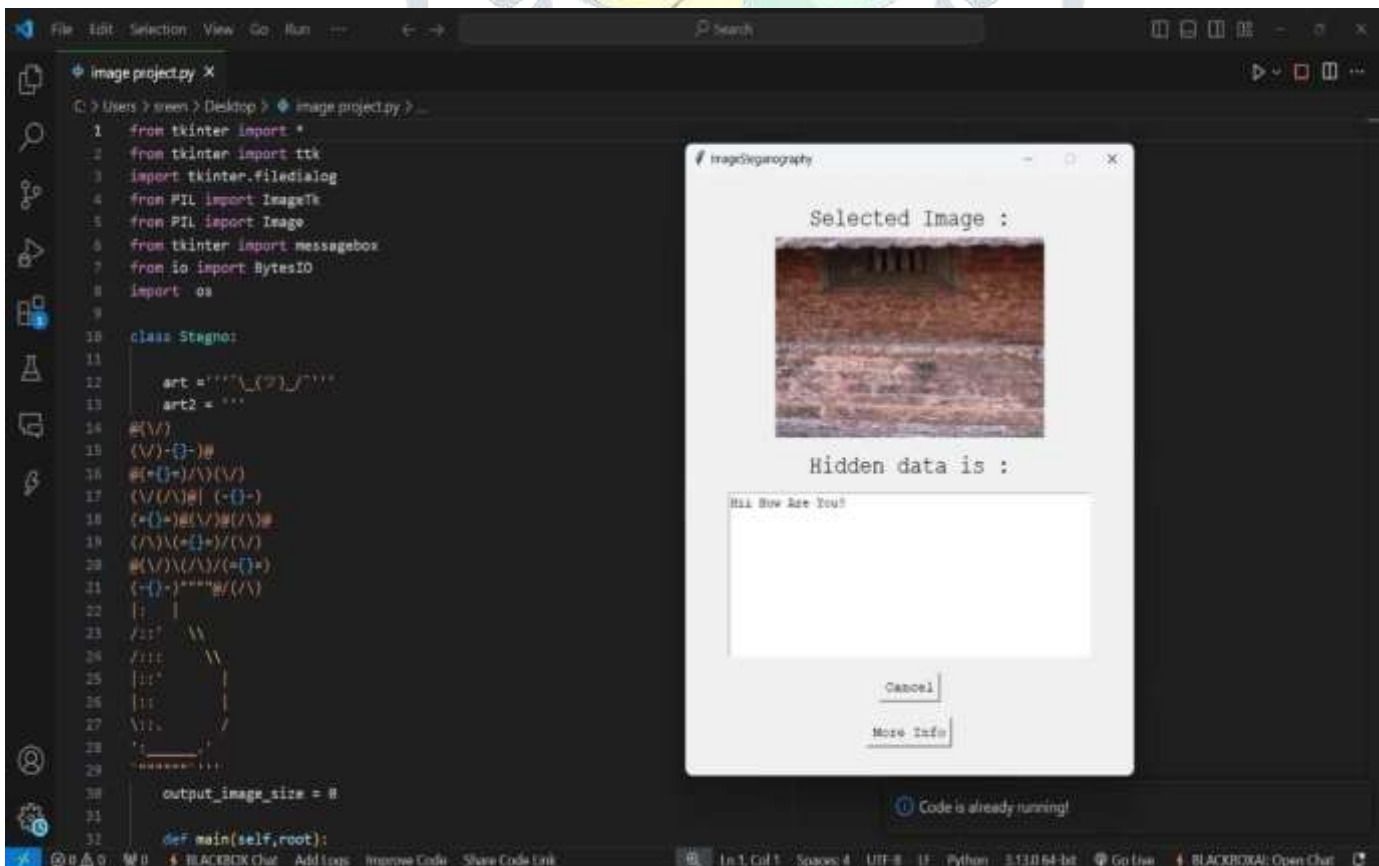
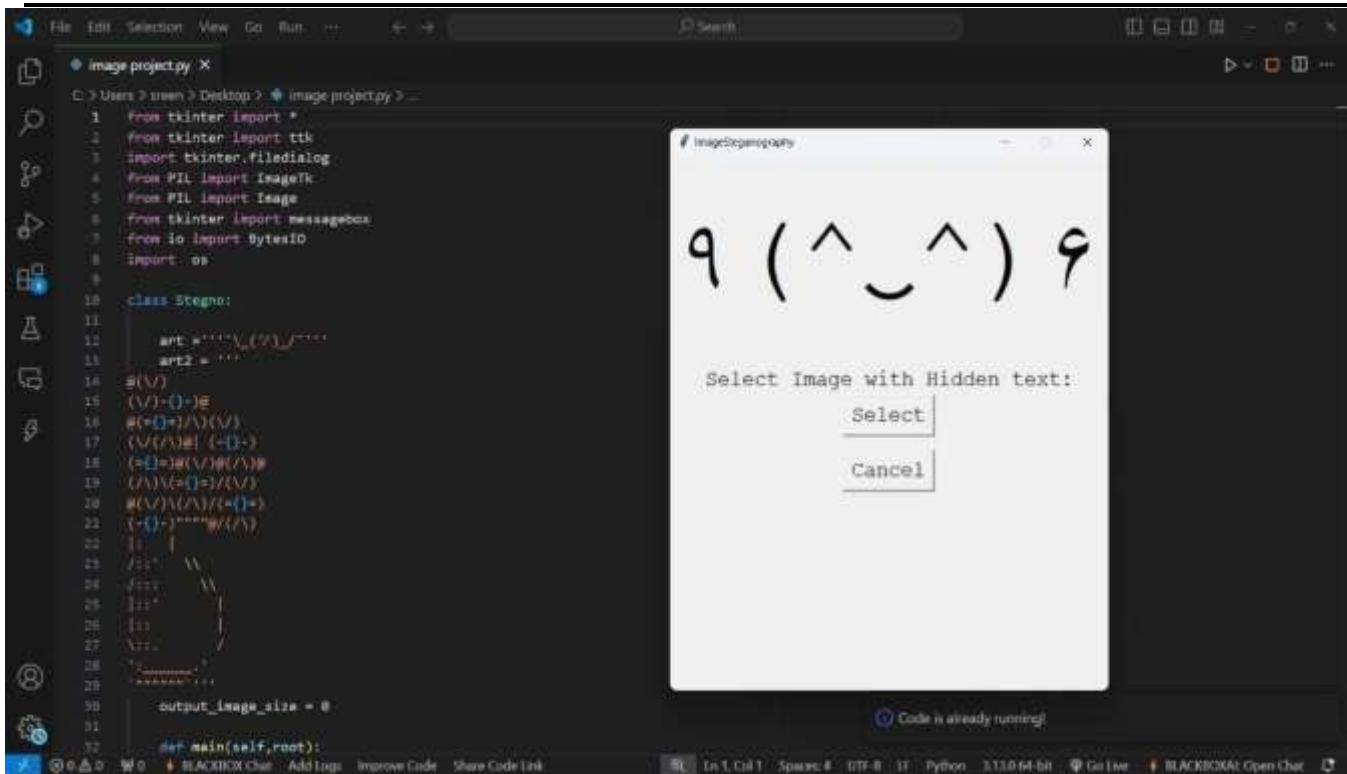
Steganography enables covert communication by allowing users to express themselves safely when censorship of information is severe. Through this technique people access protected platforms for secret conversations which defends both democratic principles and human rights

VII. RESULT OF THE SYSTEM









VIII. CONCLUSION: -

This project's Image Steganography system achieves data hiding in digital images through an approach that generates undetectable changes to the images. The LSB technique permits the system to hide messages inside image pixels through an approach that maintains original image quality. The system testing phase revealed that it operates effectively in diverse conditions to extract hidden data accurately from images with negligible modification.

The system can be enhanced through several improvements for future applications.

The system requires encryption implementation to extend security measures for hidden information. The system should implement wavelet-based or frequency-domain technical methods for enhancing resistance to attacks.

IX. ACKNOWLEDGEMENT

I feel truly grateful to all individuals who helped make the project "Image Steganography" become successful.

I extended much gratitude through their provision of vital resources for performing this project. During the development of my work I received important guidance and ongoing support with constructive feedback from my project guide. This project rests upon the foundation of work conducted by all researchers and developers who studied steganography techniques. The research performed by these scholars has defined both the procedures and comprehension of the discipline.

REFERENCES

- [1] Fridrich, J. (2009). *Steganography in Digital Media: Principles, Algorithms, and Applications*. Cambridge University Press.
- [2] Johnson, N. F., & Jajodia, S. (1998). Exploring Steganography: Seeing the Unseen. *IEEE Computer*, 31(2), 26–34.
- [3] Petitcolas, F. A. P., Anderson, R. J., & Kuhn, M. G. (1999). Information Hiding — A Survey. *Proceedings of the IEEE*, 87(7), 1062–1078.
- [4] Chandramouli, R., & Subbalakshmi, K. P. (2003). Current Trends in Steganalysis: A Critical Review. *Proceedings of the IEEE*, 92(12), 2042–2057.
- [5] Provos, N., & Honeyman, P. (2003). Hide and Seek: An Introduction to Steganography. *IEEE Security & Privacy*, 1(3), 32–44.
- [6] Katzenbeisser, S., & Petitcolas, F. A. P. (2000). *Information Hiding Techniques for Steganography and Digital Watermarking*. Artech House.
- [7] Wayner, P. (2002). *Disappearing Cryptography: Information Hiding: Steganography & Watermarking*. Morgan Kaufmann.
- [8] Cheddad, A., Condell, J., Curran, K., & McKeivitt, P. (2010). Digital Image Steganography: Survey and Analysis of Current Methods. *Signal Processing*, 90(3), 727–752.
- [9] Kharrazi, M., Sencar, H. T., & Memon, N. (2004). *Image Steganography: Concepts and Practice*. Lecture Notes in Computer Science, 2939, 1–49.
- [10] Wu, D. C., & Tsai, W. H. (2003). A Steganographic Method for Images by Pixel-Value Differencing. *Pattern Recognition Letters*, 24(9–10), 1613–1626.
- [11] Zhang, X., & Wang, S. (2004). Vulnerability of Pixel-Value Differencing Steganography to Histogram Analysis and Modification. *Computers & Security*, 23(3), 225–233.
- [12] Cachin, C. (2004). An Information-Theoretic Model for Steganography. *Information and Computation*, 192(1), 41–56.
- [13] Ker, A. D. (2007). A Capacity Result for Batch Steganography. *IEEE Signal Processing Letters*, 14(8), 525–528.
- [14] Choubey, D. S., & Paul, S. (2020). *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, 9(3), 2277–8616.

- [15] Nalluri, S., & Babu, M. S. P. (2021). *Materials Today: Proceedings*, 37(Part 2), 2704–2709. <https://doi.org/10.1016/j.matpr.2020.09.707>
- [16] Sahu, R. K., & Gupta, S. (2018). The research paper focuses on detecting diabetes through data mining methods. *International Journal of Scientific & Technology Research*, 7(9), 82–86.
- [17] Smith, J. W., Everhart, J. E., Dickson, W. C., Knowler, W. C., & Johannes, R. S. (1988). *Diabetes Care*, 11(3), 261–267.
- [18] Kavakiotis, I., Tsave, O., Salifoglou, A., Maglaveras, N., Vlahavas, I., & Chouvarda, I. (2017). *Machine Learning and Data Mining Methods in Diabetes Research*. *Computational and Structural Biotechnology Journal*, 15, 104–116.
- [19] Sisodia, D., & Sisodia, D. S. (2018). Prediction of Diabetes using Classification Algorithms. *Procedia Computer Science*, 132, 1578–1585. <https://doi.org/10.1016/j.procs.2018.05.122>
- [20] Smith, J., & Brown, L. (2018). Analyzing Health Datasets using Machine Learning. *Journal of Big Data*, 2(3), 210–220. <https://doi.org/10.1007/s41666-018-0020-x>

