Group Members: Margelino, Kristina Marie Lab No. 1

Hizola, Alfred Luis Date: April 10, 2025

Bellen, Aila Marie

Labrador, Windelyn

Git Repository Link: https://github.com/auchyoo/-IAS-CS121-Steganography-Tool.git

**Objective**

*Clearly state the objective of the lab. What is the purpose of this activity? What are you trying to achieve or learn?*

The objective of this activity is to develop a steganography tool using Python that allows users to securely encode and decode hidden messages within image and text files. The tool aims to demonstrate the practical use of information hiding techniques in the context of information assurance and security.

**Methodology**

*Describe the steps you followed in the lab. Include algorithms, data flow, or specific Spark transformations/actions if applicable. Use numbered or bullet points for clarity.*

1. Research and Design:
   * Studied basic steganography principles, particularly Least Significant Bit (LSB) for images and whitespace encoding for text.
   * Planned a modular design with clear separation of functionality for image and text steganography.
   * References:
     1. https://www.geeksforgeeks.org/image-based-steganography-using-python/
     2. https://www.geeksforgeeks.org/text-extraction-from-image-using-lsb-based-steganography/?ref=ml\_lbp
2. Implementation:
   * Used the Pillow library to handle image encoding/decoding.
   * Employed bit manipulation to modify the LSB of pixel values in image files.
   * Used spaces and tabs appended to lines in text files to represent binary data.
   * Developed a command-line menu system for user interaction and repetition of tasks.
3. Testing:
   * Encoded and decoded multiple messages using different file types.
   * Handled edge cases such as empty input, large messages, and invalid paths.

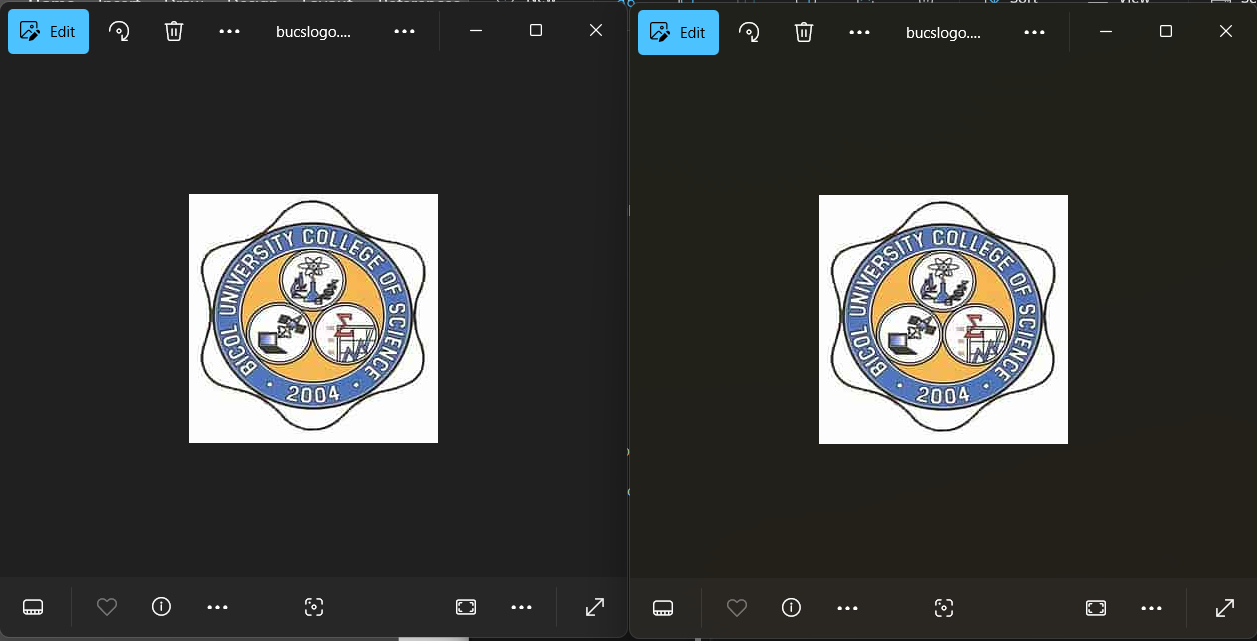
**Results & Analysis**

*Present the outcomes of your experiment. Use tables, graphs, or screenshots of results as needed. Provide a detailed analysis of the results, highlighting key findings.*

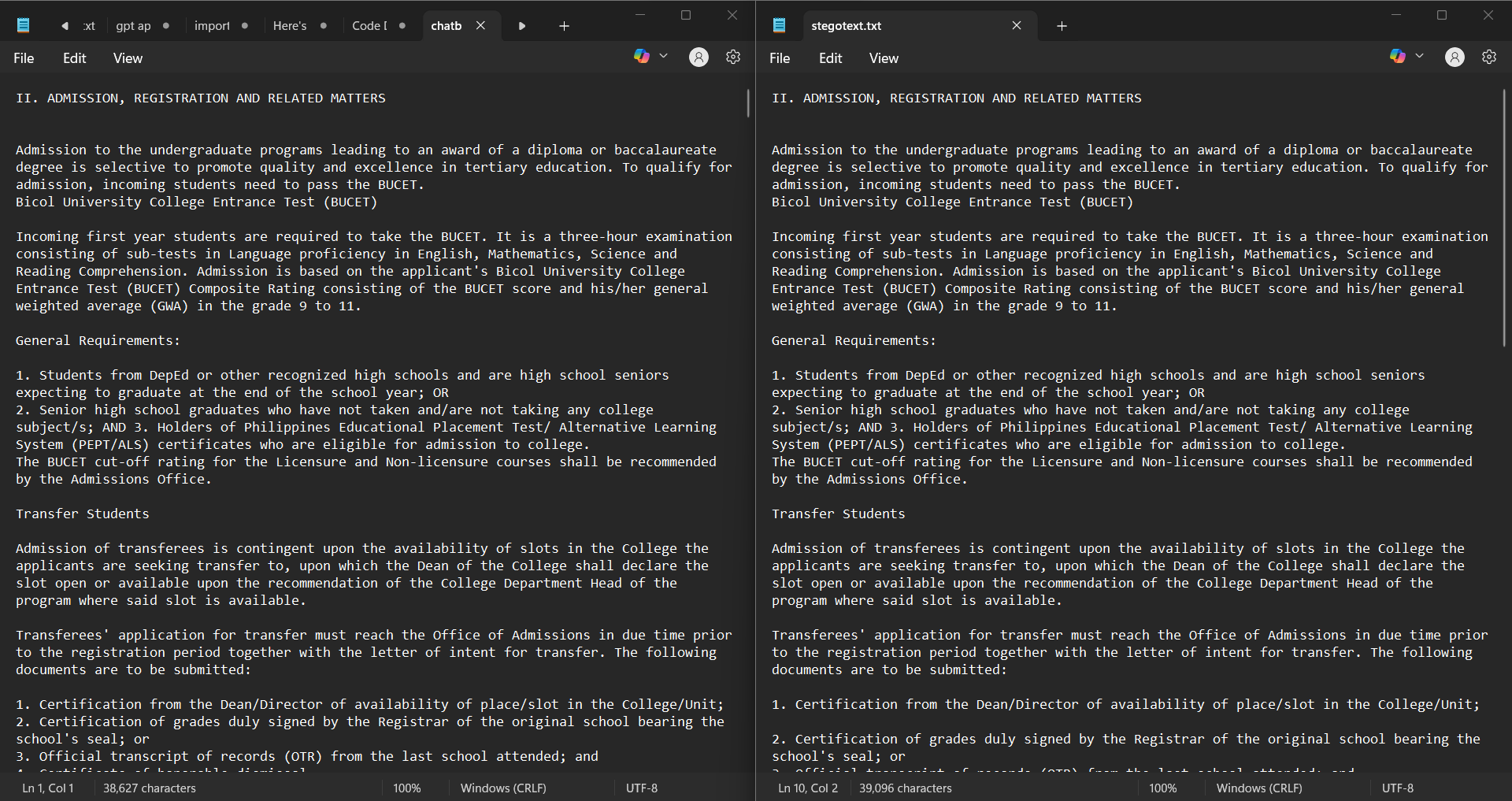
*[Results & Analysis] Image 1: Result of Program Execution. The program has successfully encoded and decoded the message in both image and text files.*

A screenshot of a computer program

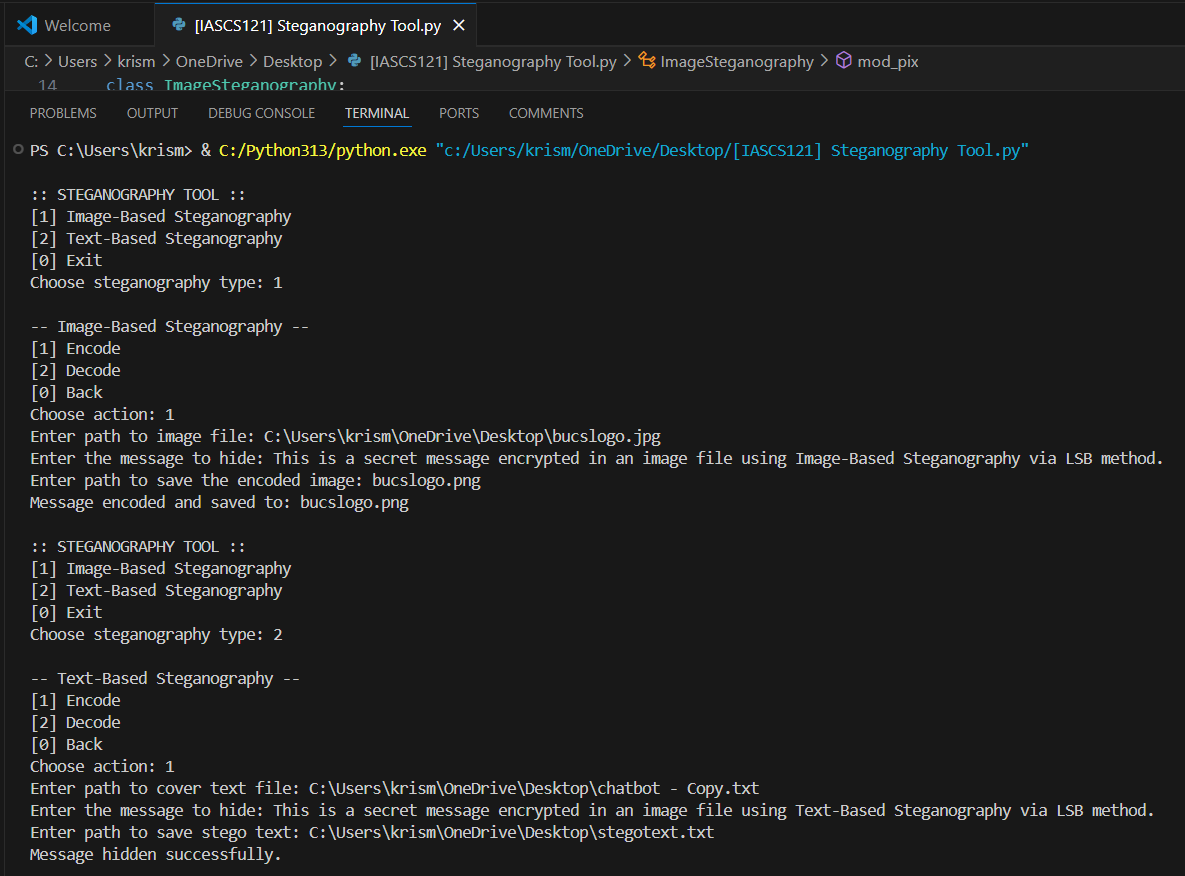
AI-generated content may be incorrect.



*[Results & Analysis] Image 2: No change in Image quality after Image-Based Encoding.*



*[Results & Analysis] Image 3: No change in text content after Text-Based Encoding.*



*[Results & Analysis] Image 4: The looped menu interface improved usability, allowing users to perform multiple actions without having to restart the program again.*

**Challenges & Solutions**

*Document any issues encountered during the lab and how you resolved them.*

* Challenge: Encountered permission errors when using directories.
* Solution: Added error handling and required full file path inputs for flexible access.
* Challenge: Image saving failed when the format string was incorrect.  
  Solution: Automatically detected and converted the file extension to the correct format.
* Challenge: Unexpected inputs could break the flow.  
  Solution: Implemented input checks and exception handling.

**Conclusion**

*Summarize the key takeaways from the lab. Did you meet the objectives? What did you learn about tools, techniques, or concepts?*

The steganography tool met its goal of providing a functional, beginner-friendly implementation of both image and text steganography. It showcased how simple encoding techniques can be applied to enhance message confidentiality. The project strengthened our understanding of steganography concepts and their real-world relevance to information assurance and digital security.