|  |  |  |
| --- | --- | --- |
| ITE_LOGO1  **RAMON MAGSAYSAY MEMORIAL COLLEGES**  Office of the Program Director  INFORMATION TECHNOLOGY EDUCATION PROGRAM  General Santos City, Philippines | | |
| Document Type: | Document No. : **DAP–03-01- 29- E** | |
| T HESIS / CAPSTONE PROJECT REPORTS | Issue No.: SY20 | Revision No.: |
| Document Title: | Effective Date: June 01, 2017 | |
| Pre-Proposal Statement | Page of | |

# Pre-Proposal Statement Template

NOTE: 1 for each of the 3 to 5 titles chosen by the adviser (strictly word-processed)

|  |  |
| --- | --- |
| Project Title: | Confidential Documents Hiding in Audio for Regional Forensic Unit 12 using Audio Steganography and XOR Method |
| Proponents/Researchers: | John Lester Espinosa |
| Scope of the Study: | **The Scope of the Study are the following:**   * This study was conducted for the Regional Forensic Unit 12 to explore the use of audio steganography with the XOR method for securing confidential documents. * Only digital audio files were used as carriers for hiding and retrieving confidential documents in this study. * The security of the hidden documents was analyzed based on the effectiveness of the XOR method in preventing unauthorized access. * Tests were conducted on different audio formats and document types to evaluate compatibility and efficiency. * The system performance was measured based on accuracy, retrieval success, and the quality of the modified audio files. |
| Limitations of the Study: | **The Limitation of the Study are the following:**   * This study focuses only on audio steganography using XOR method and does not explore other steganographic techniques or encryption methods. * This study is limited to digital audio files as carriers for confidential documents and does not cover other media types like images or videos. * The study can only accept document files, especially common formats such as .doc files. * The study is designed for hiding sensitive documents through audio files, especially common formats such as WAV and MP3. * The effectiveness of the system is tested only under controlled conditions and may not account for real-world attacks or advanced steganalysis techniques. * The study does not address large-scale deployment or integration with existing forensic systems. |
| Project Design/Development Plan: | **Program Specification**   1. Encoding and Decoding  * Encode confidential documents within audio files using the XOR method * Decode and extract hidden documents from audio files. * Ensure secure storage and retrieval of confidential documents.  1. File Format Support  * Support various documents files formats (e.g., .doc). * Support multiple audio file formats (e.g., .wav, .mp3).  1. Performance and Optimization  * Maintain the quality of audio files after embedding data. * Optimize file size to reduce distortion in the audio. * Analyze system performance based on accuracy and efficiency.  1. User Experience  * Provide a user-friendly interface for easy encoding and decoding. * Allow users to verify the integrity of extracted documents.   **Software Specification**   1. IDE – Visual Studio Code / PyCharm / Jupyter Notebook 2. Graphical User Interface (GUI) – Tkinter, Kivy, or PyQt 3. Version Control – Git (for source code management) 4. Programming Language – Python 3.13   **Hardware Specification**   1. Processor - 11th Gen Intel(R) Core (TM) i5-1135G7 @ 2.40GHz, 2401 Mhz, 4 Core(s), 8 Logical Processor(s) 2. RAM – 16GB DDR4 3. Storage – 475GB SSD |