Syntactic Steganography for Document Leak Identification

Hardik Rajpal

October 12, 2023

1 Introduction

This project seeks to implement the principles of syntactic steganography for identification of the sources of leaks of confidential documents from a protected server. The security model is based on the following assumptions:

1. Each protected document is stored on the server in .DOCX format.
2. Each user has an identification number, known to the server.
3. The only way to access the documents is to request them from the server after authentication.

In addition to steganography, additional techniques are employed to futher complicate the task of leaking the documents, such as:

1. Ghostscript

2 References

1. Combat text selection
2. Combat text selection still