**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**

**KHOA AN TOÀN THÔNG TIN**

****

**HỌC PHẦN: CÁC KỸ THUẬT GIẤU TIN**

**MÃ HỌC PHẦN: INT14102**

**Chủ đề: Giấu tin trong âm thanh**

**Lab: lsb-steghide-audio**

Sinh viên thực hiện: Hồ Phan Đức Anh

Mã sinh viên: B21DCAT024

Nhóm: 04

Giảng viên hướng dẫn: Đỗ Xuân Chợ

**HÀ NỘI 2025**

**Bài lab Các kỹ thuật giấu tin: lsb\_steghide\_audio**

1. **Mục đích**

Giúp sinh viên hiểu được thuật toán LSB và công cụ Steghide cùng cách kết hợp chúng để phục vụ giấu tin trong âm thanh.

1. **Yêu cầu đối với sinh viên**

Quen thuộc với hệ điều hành Linux và có kiến thức về kỹ thuật giấu tin.

1. **Nội dung lý thuyết**
   1. **Thuật toán LSB**

Phương pháp LSB (Least Significant Bit) là một kỹ thuật giấu tin trong âm thanh bằng cách thay thế các bit có trọng số thấp nhất trong mẫu âm thanh số bằng dữ liệu cần giấu. Do các bit này ít ảnh hưởng đến chất lượng âm thanh tổng thể, sự thay đổi của chúng thường không được thính giác con người nhận ra.



*Giá trị 8 bit của tín hiệu A = 218*



*Giá trị 8 bit của tín hiệu B = 219 sau khi giấu bit 1 vào LSB của A*

Khi giấu 1 bit mật vào mẫu dữ liệu thì độ lệch giá trị giữa mẫu dữ liệu gốc và dữ liệu mang tin tối đa là 1. Để tăng độ bền vững của kỹ thuật giấu này, ta có thể giấu nhiều lần chuỗi thông điệp mật hoặc điều chỉnh vị trí các bit cao hơn trong mỗi mẫu để giấu tin. Các kỹ thuật giấu dùng phương pháp điều chỉnh LSB thường chọn các bit từ vị trí 1 đến 3, tính từ bên phải sang trái

**Ưu điểm:**

* Đơn giản và hiệu quả: Dễ triển khai, cho phép giấu một lượng lớn dữ liệu mà không làm tăng kích thước tệp âm thanh.
* Khó phát hiện: Sự thay đổi ở các bit LSB thường không thể nhận biết được bằng thính giác con người.

**Nhược điểm:**

* Dễ bị tấn công: Các kỹ thuật nén mất dữ liệu hoặc chỉnh sửa âm thanh có thể làm mất hoặc hỏng thông tin được giấu.
* Thiếu tính bền vững: Do sự nhạy cảm với các biến đổi, phương pháp LSB không đảm bảo tính toàn vẹn của thông tin giấu khi tệp âm thanh bị chỉnh sửa hoặc nén.

Do đó, việc kết hợp giấu tin giữa phương pháp LSB với các thuật toán mã hóa như RSA và AES là hoàn toàn hợp lý và cần thiết.

**3.2 Công cụ steghide**

[Steghide](https://www.geeksforgeeks.org/how-to-install-steghide-tool-in-linux/) là một chương trình ẩn tin miễn phí cho phép bạn ẩn các tệp tin bí mật bên trong các tệp tin khác. Steghide hoạt động bằng cách nhúng dữ liệu ẩn của bạn vào tệp tin âm thanh, hình ảnh hoặc video. Đối với bất kỳ ai khác, tệp tin mang này sẽ trông và nghe có vẻ bình thường. Nhưng nó lại bí mật chứa tin nhắn hoặc tệp tin được mã hóa của bạn. Công cụ Steghide cho phép bạn dễ dàng nhúng thông tin ẩn của mình và trích xuất lại bằng mật khẩu. Điều này cung cấp một cách để truyền tin nhắn hoặc dữ liệu nhạy cảm một cách an toàn qua mạng công cộng hoặc bất kỳ hệ thống nào cần có quyền riêng tư.

Công cụ này hoạt động dựa trên cơ chế thay đổi các bit ít quan trọng nhất (Least Significant Bits – LSB) trong dữ liệu của tệp chứa, cho phép nhúng thông tin một cách kín đáo mà không gây ảnh hưởng rõ rệt đến chất lượng hình ảnh hay âm thanh. Bên cạnh đó, Steghide còn hỗ trợ mã hóa dữ liệu bằng thuật toán AES khi người dùng cung cấp mật khẩu, giúp đảm bảo an toàn và bảo mật cho thông tin được ẩn giấu.  
 Ưu điểm chính của Steghide là nó có thể nhúng dữ liệu mà không làm giảm chất lượng hoặc kích thước tệp của tệp gốc. Điều này khiến việc phát hiện bất kỳ thông tin ẩn nào đã được thêm vào trở nên khó khăn.

**3.3 Ứng dụng trong bài lab**

Mục đích của bài lab là mô phỏng lại phương pháp LSB kết hợp với công cụ steghide. steghide giúp người dùng nhúng nội dung từ file văn bản vào một file âm thanh gốc, tạo thành file mới chứa dữ liệu đã được ẩn. File âm thanh sau khi được nhúng dữ liệu vẫn nghe giống như file gốc, khiến người ngoài khó nhận ra rằng bên trong có chứa thông tin bí mật. Sau khi tạo ra file âm thanh đã được ẩn dữ liệu, người dùng truyền file này qua mạng tới một máy khác mà không gây nghi ngờ, bởi vì dữ liệu được ngụy trang dưới dạng một file âm thanh thông thường. Trên máy nhận, file âm thanh này sẽ được lưu lại và sử dụng lại steghide để trích xuất thông tin đã bị giấu bên trong. Kết quả là nội dung ban đầu trong file ban đầu được khôi phục lại một cách đầy đủ.

**Nội dung thực hành**

Khởi động bài lab:

Vào terminal, gõ:

*labtainer -r lsb-steghide-audio*

(Chú ý: Sinh viên sử dụng mã sinh viên của mình để nhập thông tin email người thực hiện bài lab khi có yêu cầu, để sử dụng khi chấm điểm)

Sau khi khởi động xong hai terminal ảo sẽ xuất hiện, một cái là đại diện cho máy gửi dữ liệu, một cái là địa diện cho máy nhận dữ liệu

**Nhiệm vụ 1: Nhúng dữ liệu vào file âm thanh**

Trên terminal com1, thực hiện nhúng dữ liệu bí mật vào file âm thanh gốc

***steghide embed -cf input.wav -ef secret.txt -sf output.wav***

steghide sẽ yêu cầu bạn nhập mật khẩu để mã hóa nội dung nhúng.

Sau khi đã nhúng dữ liệu vào file âm thanh gốc, thực hiện so sánh đặc tính âm thanh trước và sau khi nhúng:

***sox input.wav output.wav -n stat***

Trên teminal com 2, thực hiện lắng nghe và lưu tệp dữ liệu bí mật

***ncat -l 4444 > file.tar.gz***

Sau đó trên terminal com 1, gửi tệp âm thanh đã nhúng qua mạng

***ncat --send-only 172.20.0.3 4444 < output.wav***

**Nhiệm vụ 2: Kiểm tra thông tin ẩn trong tệp**

Sau khi máy com2 nhận file âm thanh đã nhúng, kiểm tra xem trong file đó có chứa dữ liệu ẩn chưa

***steghide info output.wav***

steghide sẽ yêu cầu nhập mật khẩu dùng khi nhúng.

Nếu mật khẩu đúng, bạn sẽ thấy thông báo như:  
embedded file "secret.txt" – cho biết có dữ liệu và tên tệp được nhúng.

**Nhiệm vụ 3: Trích xuất dữ liệu và xem nội dung trong tệp ẩn**

Khi đã biết trong file output.wav chứa dữ liệu ẩn, thực hiện trích xuất dữ liệu

***steghide extract -sf output.wav***

Khi chạy, chương trình yêu cầu nhập mật khẩu.

Sau khi nhập đúng, tệp secret.txt sẽ được khôi phục về thư mục hiện tại

Xem nội dung trong file dữ liệu đã trích xuất

***cat secret.txt***

**Kết thúc bài lab:**

Kiểm tra checkwork:

*checkwork*

Trên terminal đầu tiên sử dụng câu lệnh sau để kết thúc bài lab:

*stoplab*