

NGHIÊN CỨU XÂY DỰNG MỘT PHƯƠNG PHÁP GIẤU TIN ĐƠN GIẢN, AN TOÀN

Học viên: Đỗ Minh Đức
Đơn vị công tác: Văn phòng Thường trực Ban Chỉ đạo về
Nhân quyền của Chính Phủ
Email: ducminhdo@gmail.com

GVHD: TS.Hồ Văn Canh
Đơn vị công tác: Bộ Công an
Email: hovancanh@gmail.com

Từ khóa: giấu tin, steganography, data hiding, steganalysis, phân tích giấu tin

1. GIỚI THIỆU BÀI TOÁN

Xuất phát từ thực tiễn và yêu cầu công tác của ngành công an, một mặt phải tìm hiểu phương pháp phân tích những thông tin bí mật, phương thức liên lạc mà đối tượng che giấu. Mặt khác, cũng phải nghiên cứu phương pháp bảo vệ kênh liên lạc phục vụ công tác nghiệp vụ của lực lượng bí mật. Luận văn đã đề ra mục tiêu cần giải quyết cụ thể như sau:

- Nghiên cứu giấu tin mật trong ảnh bitmap 24 bit màu;
- Trong trường hợp thuật toán giấu tin bị phá vỡ thì đối phương cũng không giải mã được tin mật.

2. NỘI DUNG LUẬN VĂN

Luận văn nghiên cứu một số phương pháp giấu tin trong môi trường ảnh, phân tích một số thuật toán giấu tin trong ảnh đen trắng, ảnh đa cấp xám và ảnh bitmap 24 bit màu; Nghiên cứu một số phương pháp phân tích ảnh có tin giấu; Đề xuất phương pháp mã hóa thông tin dựa trên lý thuyết đại số tuyến tính, sử dụng tính chất ma trận nghịch đảo để sinh khóa mã và khóa giải mã tin mật. Nghiên cứu xây dựng thuật toán giấu tin vào các bit LSB của ảnh bitmap 24 bit. Đề xuất tích hợp hệ giấu tin mật với phương pháp mã hóa sử dụng tiêu chuẩn mã hóa nâng cao AES để bảo đảm an toàn cao nhất cho thông điệp bí mật trong trường hợp thuật toán giấu tin bị tấn công.

Luận văn đã thực hiện xây dựng chương trình thử nghiệm giấu/tách tin mật kết hợp với mã hóa tin mật bằng phương pháp Rijndael. Đồng thời, thử nghiệm tấn công ảnh có tin giấu bằng phương pháp tăng cường bit LSB và phương pháp tấn công sử dụng tiêu chuẩn thống kê Khi bình phương.

3. KẾT LUẬN

Giấu tin là một lĩnh vực nghiên cứu rộng, môi trường giấu tin đa dạng, các phương pháp giấu tin trong môi trường ảnh chủ yếu tập trung nhiều vào việc giấu tin trong các bit có trọng số thấp. Luận văn này đã tìm hiểu, phân tích một số thuật toán giấu tin trong ảnh đen trắng, ảnh đa cấp xám và ảnh màu bitmap 24 bit. Đồng thời, luận văn cũng nghiên cứu một số phương pháp phân tích ảnh có tin giấu: phân tích trực quan, phân tích dựa trên tiêu chuẩn thống kê Khi bình phương, để làm cơ sở đánh giá thuật toán giấu tin đã đề xuất.

Mặt khác, luận văn cũng nghiên cứu và đề xuất một phương pháp mã hóa thông tin sử dụng ma trận trên kích thước 8×8 và tính chất nghịch đảo của ma trận để sinh khóa mã và khóa giải mã. Phương pháp này có ưu điểm, cho phép người nhận tin mật sử dụng tính chất ma trận nghịch đảo A^{-1} để mã hóa, gửi tin cho trung tâm mà không cần phải biết ma trận A .

Luận văn tập trung nghiên cứu khả năng bảo mật thông tin kể cả trong trường hợp thuật toán giấu tin bị phá vỡ, đối phương cũng không giải mã được tin mật. Đáp ứng mục tiêu đề ra, luận văn đã tìm hiểu tiêu chuẩn mã hóa hiện đại AES, áp dụng phương pháp mã hóa Rijndael để nâng cao tính bảo mật thông tin.

Luận văn đã xây dựng được chương trình giấu tin mật kết hợp mã hóa bằng phương pháp Rijndael (AES). Chương trình đã đáp ứng được yêu cầu đặt ra của bài toán.

Hướng nghiên cứu tiếp theo: Để hoàn thiện hơn nữa chương trình giấu tin mật kết hợp với mã hóa, cần phải nghiên cứu giấu tin trong các loại ảnh khác như: JPEG, TIF, GIF,... Và nghiên cứu tích hợp khả năng trao đổi khóa trên mạng an toàn, bí mật.