ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

LÊ ANH DŨNG

GIẤU TIN TRONG FILE ÂM THANH BẰNG CÁC PHÉP BIẾN ĐỔI RỜI RẠC

LUẬN VĂN THẠC SỸ: KHOA HỌC MÁY TÍNH

THÁI NGUYÊN, NĂM 2015

ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

LÊ ANH DŨNG

GIẤU TIN TRONG FILE ÂM THANH BẰNG CÁC PHÉP BIẾN ĐỔI RỜI RẠC

Chuyên ngành: Khoa học máy tính
Mã số: 60 48 0101

LUẬN VĂN THẠC SỸ: KHOA HỌC MÁY TÍNH

HƯỚNG DẪN KHOA HỌC: **TS TRỊNH THANH LÂM**

THÁI NGUYÊN, NĂM 2015

LỜI CAM ĐOAN

Tôi xin cam đoan luận văn "*Giấu tin trong file âm thanh bằng các phép biến đổi rời rạc*" là sản phẩm của riêng cá nhân, không sao chép lại của người khác. Trong toàn bộ nội dung của luận văn, những điều được trình bày hoặc là của cá nhân hoặc là được tổng hợp, nghiên cứu từ nhiều nguồn tài liệu. Tất cả các tài liệu tham khảo đều có xuất xứ và trích dẫn rõ ràng.

Tôi xin hoàn toàn chịu trách nhiệm và chịu mọi hình thức kỷ luật theo quy định cho lời cam đoan của mình.

Thái Nguyên, ngày 15 tháng 05 năm 2015

Học viên

Lê Anh Dũng

LỜI CẢM ƠN

Lời đầu tiên, tôi xin bày tỏ lòng biết ơn đến thầy TS Trịnh Thanh Lâm - ĐHQG Hà Nội, người đã tận tình hướng dẫn, chỉ bảo và giúp đỡ tôi trong suốt quá trình nghiên cứu và hoàn thành luận văn này.

Tôi xin chân thành cảm ơn các thầy cô giáo trường Đại học Công nghệ Thông tin và Truyền thông - Đại học Thái Nguyên đã giảng dạy và cung cấp cho chúng tôi những kiến thức rất bổ ích trong thời gian học cao học, giúp tôi có nền tảng tri thức để phục vụ nghiên cứu khoa học sau này.

Tôi cũng xin cảm ơn Lãnh đạo và đồng nghiệp tại đơn vị đã tạo điều kiện và giúp đỡ tôi trong suốt quá trình nghiên cứu và hoàn thành luận văn. Tôi cũng xin bày tỏ lòng cảm ơn đến gia đình và bạn bè, những người luôn quan tâm, động viên và khuyến khích tôi trong quá trình học tập.

Thái Nguyên, ngày 15 tháng 05 năm 2015

Lê Anh Dũng

MỤC LỤC

Trang

DANH MỤC CÁC TỪ VIẾT TẮT TRONG LUẬN VĂN

AAC - Định dạng âm thanh chuẩn (*Advanced Audio Coding*)

A/D D/A - Biến đổi tương tự/số và ngược lại (*Analog/Digital*)

AIFF - Định dạng không mất thông tin (*Audio Interchange File Format*)

DCT - Phép biến đổi Cosin rời rạc (*Discrete Cosine Tranform*).

DES - Hệ mật mã chuẩn (*Data Encryption Standard*)

DSP - Xử lý tín hiệu kỹ thuật số (*Digital signal processing*)

FLAC - Nén âm thanh không mất dữ liệu (*Free Lossless Audio Codec*),

FT - Biến đổi Fourier (*Fourier Transform*)

HAS - Hệ thống thính giác (*Human Auditory system*)

HVS - Hệ thống thị giác (*Human Vision System*)

IDE - Môi trường phát triển tích hợp (*Integrated Development Environment*)

IFT - Biến đổi Fourier ngược (*Inverse Fourier Transform*)

LSB - Bít ít quan trọng nhất (*Least Significant Bít*)

MP3 - Định dạng nén âm thanh (*Movie Picture Experts Group-Layer 3*)

PCM - Điều biến mã xung (*Pulse Code Modulation*)

RSA - Mã hóa công khai RSA (*Rivest, Shamir và Adleman*)

WAV - Định dạng âm thanh dạng sóng (*Waveform Audio Format*)

WMA - Định dạng âm thanh của Microsoft (*Windows Media Audio*)

DANH MỤC CÁC HÌNH ẢNH

Trang

DANH MỤC CÁC BẢNG BIỂU

Trang

MỞ ĐẦU

1. Đặt vấn đề

Ngày nay, Internet là môi trường phổ biến cho việc trao đổi thông tin giữa các nhà cung cấp và người sử dụng. Do đó, vấn đề an toàn dữ liệu trên mạng luôn luôn là một thách thức đối với các nhà quản lý và các nhà nghiên cứu. Các thông tin trên Internet có thể dễ dàng bị làm giả mạo, sai lệch và bị đánh cắp bởi hacker trong quá trình truyền tải dữ liệu. Thông tin của cá nhân, tổ chức hoặc quốc gia đứng trước nguy cơ bị xâm nhập bất cứ lúc nào. Cùng với nó là vấn nạn ăn cắp bản quyền, xuyên tạc thông tin,... ngày càng gia tăng. Vì vậy, vấn đề đặt ra làm thế nào để đảm bảo được sự an toàn, và toàn vẹn thông tin trong quá trình truyền tải trên Internet. Hai giải pháp cho vấn đề này là mã hóa và giấu thông tin có vai trò quan trọng trong việc bảo vệ quá trình truyền tải thông tin mật. Sự xác thực và bản quyền trong môi trường trao đổi công cộng. Việc tìm giải pháp cho những vấn đề này giúp ta hiểu thêm về một công nghệ đang phát triển và còn tạo ra những cơ hội mới [1].

Trong những giải pháp đã và đang được triển khai thì giấu tin (Data Hiding) là một trong những giải pháp được các nhà nghiên cứu và phát triển coi đó là một hướng đi có nhiều triển vọng. Giấu thông tin là kỹ thuật nhúng một lượng thông tin số nào đó vào trong một đối tượng thông tin số khác mà các đối tượng đó thường là một tài liệu, hình ảnh, âm thanh hoặc video. Các kỹ thuật giấu tin có thể chia ra làm hai nhóm. Nhóm thứ nhất là các phương pháp che giấu thông tin trực tiếp. Nhóm này thường sử dụng các bít ít quan trọng nhất của một khối bít nhị phân được sửa đổi để giấu thông tin. Nhóm thứ hai lại che giấu thông tin thông qua các phép biến đổi chẳng hạn như phép biến đổi Cosin hay wavelet rời rạc được sử dụng rộng rãi [4].

Sau khi tiến hành nghiên cứu các tài liệu liên quan đến lĩnh vực giấu tin trong đa phương tiện và nhận thấy các kỹ thuật trên đều cho kết quả tốt với