ĐẠI HỌC THÁI NGUYÊN

TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

NGUYỄN THỊ THANH XUÂN

NGHIÊN CỨU THUẬT TOÁN ẨN THÔNG TIN TRÊN ẢNH SỐ BẰNG KỸ THUẬT HOÁN VỊ HỆ SỐ VÀ ỨNG DỤNG TRONG BẢO MẬT DỮ LIỆU

LUẬN VĂN THẠC SĨ KHOA HỌC MÁY TÍNH

Thái Nguyên – 2013

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

Nguyễn Thị Thanh Xuân

NGHIÊN CỨU THUẬT TOÁN ẨN THÔNG TIN TRÊN ẢNH SỐ BẰNG KỸ THUẬT HOÁN VỊ HỆ SỐ VÀ ỨNG DỤNG TRONG BẢO MẬT DỮ LIỆU

Chuyên ngành: Khoa học máy tính

Mã số: 60.48.01

LUẬN VĂN THẠC SĨ KHOA HỌC MÁY TÍNH

NGƯỜI HƯỚNG DẪN KHOA HỌC

TS. NGUYỄN NGỌC CƯƠNG

Thái Nguyên – 2013

LỜI CẢM ƠN

Em xin được bày tỏ lòng biết ơn sâu sắc đến thầy TS. Nguyễn Ngọc Cương - Học viện An Ninh Nhân dân đã tận tình hướng dẫn, chỉ bảo và dành rất nhiều thời gian cho em trong suốt quá trình làm luận văn.

Em xin gửi lời cảm ơn chân thành đến các thầy cô giáo Trường Đại học Công nghệ Thông tin và Truyền Thông - Đại học Thái Nguyên, đã giảng dạy cung cấp, trang bị cho chúng em những kiến thức, chuyên ngành, chuyên môn chuyên sâu trong quá trình học tập tại trường cũng như quá trình làm luận văn này.

Cuối cùng em xin gửi lời cảm ơn sâu sắc nhất gia đình, bạn bè và các đồng nghiệp đã động viên, cổ vũ, tạo điều kiện cho em trong quá trình học tập cũng như thời gian làm luận văn; giúp em hoàn thành khóa học, luận văn theo qui định.

LỜI CAM ĐOAN

Tôi xin cam đoan luận văn là kết quả nghiên cứu của tôi, không sao chép của ai. Nội dung luận văn có tham khảo và sử dụng các tài liệu liên quan, các thông tin trong tài liệu được đăng tải trên các tạp chí và các trang website theo danh mục tài liệu của luận văn.

Tác giả luận văn

Nguyễn Thị Thanh Xuân

DANH MỤC CÁC HÌNH VẼ

DANH MỤC CÁC TỪ VIẾT TẮT

HVS	Hệ thống thị giác của con người
HAS	Hệ thống thính giác của con người
LSB	Kỹ thuật gài vào các bit có trọng số thấp
DCT	Biến đổi cosine rời rạc
DFT	Biến đổi Fourier rời rạc
DWT	Biến đổi wavelet
AES	Tiêu chuẩn mã hóa tiên tiến
DES	Tiêu chuẩn mã hóa dữ liệu

MỤC LỤC

MỞ ĐẦU

1. Đặt vấn đề

Cùng với sự bùng nổ của Internet và các phương tiện multimedia, những vấn nạn như ăn cắp bản quyền, xuyên tạc thông tin, truy nhập thông tin trái phép... cũng gia tăng, đòi hỏi phải không ngừng tìm các giải pháp mới, hữu hiệu cho an toàn và bảo mật thông tin. Một trong các giải pháp nhiều triển vọng là giấu tin (DataHiding), được nghiên cứu phát triển trong khoảng 10 năm gần đây.

Hiện nay nhiều ngành, nhiều đơn vị trên toàn quốc đã có hệ thống mạng nội bộ thông suốt các tỉnh thành trong cả nước. Hệ thống đảm bảo được các thông tin truyền đi trong mạng không bị lọt ra ngoài nhưng điểm yếu của hệ thống hiện tại chưa đạt được đó là tính cơ động. Việc sử dụng mạng internet dễ dàng hơn nhiều so với mạng nội bộ để truyền tin. Tuy nhiên internet có thể phát tán thông tin đi bất kỳ đâu trên thế giới. Đi kèm với việc truyền tin qua internet là những rủi ro về mất mát và sai lệch thông tin. Do đó bảo mật thông tin khi truyền trên internet là một vấn đề cấp thiết trong thực tế.

Bản chất của bảo mật thông tin là tìm cách để che giấu thông tin, có thể là mã hóa thông tin hoặc giấu thông tin trong các dữ liệu số khác. Mục đích đặt ra là thông tin được bảo mật chỉ có thể đọc được bởi đối tượng có quyền đọc thông tin đó. Một trong cách tiếp cận trong bảo mật thông tin đó là giấu tin có nghĩa là những thông tin số cần được bảo mật sẽ được người dùng giấu vào trong một đối tượng dữ liệu số khác (môi trường giấu tin) sao cho sự biến đổi của môi trường sau khi giấu tin là khó nhận biết, đồng thời người dùng có thể lấy lại được các thông tin đã giấu khi cần.