

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

TRẦN THẾ ANH

**NGHIÊN CỨU KỸ THUẬT LSB VÀ KẾT HỢP
THUẬT TOÁN RSA ĐỂ GIẤU TIN TRONG ẢNH**

LUẬN VĂN THẠC SĨ: KHOA HỌC MÁY TÍNH

THÁI NGUYÊN, NĂM 2015

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

TRẦN THẾ ANH

**NGHIÊN CỨU KỸ THUẬT LSB VÀ KẾT HỢP THUẬT
TOÁN RSA ĐỂ GIẤU TIN TRONG ẢNH**

Chuyên ngành: Khoa học máy tính

Mã số: 60 48 0101

LUẬN VĂN THẠC SĨ: KHOA HỌC MÁY TÍNH

HƯỚNG DẪN KHOA HỌC: TS. TRẦN ĐỨC SỰ

THÁI NGUYÊN, NĂM 2015

LỜI CAM ĐOAN

Tôi xin cam đoan luận văn “*Nghiên cứu kỹ thuật LSB và kết hợp thuật toán RSA để giấu tin trong ảnh*” 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 tháng năm 2015

Học viên

Trần Thế Anh

LỜI CẢM ƠN

Lời đầu tiên, tôi xin bày tỏ lòng biết ơn đến thầy TS Trần Đức Sự - Ban Cơ Yếu Chính Phủ, 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 tháng năm 2015

Trần Thế Anh

MỤC LỤC

	Trang
LỜI CAM ĐOAN	i
LỜI CẢM ƠN	ii
MỤC LỤC	iii
DANH MỤC CÁC HÌNH ẢNH	vii
DANH MỤC CÁC BẢNG BIỂU	viii
MỞ ĐẦU	1
CHƯƠNG 1. TỔNG QUAN VỀ ẨN MÃ VÀ ẢNH SỐ	5
1.1. Giới thiệu chung về ẩn mã	5
1.1.1. Khái niệm ẩn mã	6
1.1.2. Nguyên lý cơ bản của ẩn mã học	6
1.1.3. Ẩn mã thuần túy	8
1.2. Hệ mật mã RSA	9
1.2.1. Hệ thống mã hóa công khai.....	9
1.2.2. Hệ mật mã khóa công khai RSA.....	11
1.3. Độ an toàn và độ an toàn hoàn hảo trong ẩn mã.....	11
1.3.1. Độ an toàn của ẩn mã.....	11
1.3.2. Độ an toàn hoàn hảo trong ẩn mã	12
1.3.3. Độ an toàn hoàn hảo của một hệ ẩn mã	12
1.4. Ứng dụng của ẩn mã trong môi trường thực tế.....	13
1.5. Giới thiệu chung về ảnh số.....	14
1.5.1. Khái niệm ảnh số.....	14
1.5.2. Điểm ảnh	14
1.6. Các kỹ thuật giấu tin trong ảnh	16
1.6.1. Kỹ thuật giấu tin trên miền không gian ảnh.....	16
1.6.1.1. Kỹ thuật giấu tin trong khối bit	16

1.6.1.2. Kỹ thuật giấu tin thay thế các bit có trọng số thấp nhất	18
1.6.2. Kỹ thuật giấu tin trên miền tần số ảnh	19
1.7. Một số dạng tấn công trong môi trường ảnh số hóa	19
1.7.1. Tấn công trực quan.....	19
1.7.1.1. Tấn công trực quan dựa trên việc giấu và tìm kiếm tuần tự. 19	
1.7.1.2. Tấn công trực quan dựa trên việc giấu và tìm kiếm ngẫu nhiên.....	20
1.7.2. Tấn công cấu trúc.....	21
1.7.2.1. Tấn công cấu trúc trên dung lượng tập tin	21
1.7.2.2. Tấn công cấu trúc dựa trên việc ẩn mã bằng bảng màu	22
1.7.3. Tấn công thống kê.....	23
CHƯƠNG 2. KẾT HỢP KỸ THUẬT LSB VÀ THUẬT TOÁN RSA GIẤU TIN TRONG ẢNH BITMAP 24 BIT.....	24
2.1. Cấu trúc ảnh Bitmap.....	24
2.2. Kỹ thuật giấu tin LSB	28
2.2.1. Quá trình giấu tin	28
2.2.2. Quá trình tách tin.....	29
2.2.3. Đánh giá thuật toán	30
2.3. Mô hình sử dụng kỹ thuật LSB kết hợp thuật toán RSA để tăng độ an toàn cho việc giấu tin trong ảnh	31
2.3.1. Thuật toán mã hóa khóa công khai RSA	32
2.3.2. Mô hình giấu tin sử dụng kỹ thuật LSB kết hợp thuật toán RSA.....	36
2.4. Đánh giá mô hình sử dụng kỹ thuật LSB kết hợp thuật toán RSA.....	39
CHƯƠNG 3. TRIỂN KHAI CHƯƠNG TRÌNH THỬ NGHIỆM	42
3.1. Mục đích, yêu cầu	42
3.2. Yêu cầu về cấu hình hệ thống.....	42
3.3. Lựa chọn định dạng file ảnh trong thực nghiệm.....	42

3.4. Sơ đồ chức năng chương trình	43
3.5. Sơ đồ hoạt động của chương trình	45
3.6. Thuật toán RSA, giấu tin và trích rút tin theo kỹ thuật đề xuất	48
3.6.1. Thuật toán RSA.....	48
3.6.1.1. Tạo khóa công khai và khóa bí mật.....	48
3.6.1.2. Thuật toán mã hóa	49
3.6.1.3. Thuật toán giải mã	49
3.6.2. Giấu tin.....	50
3.6.3. Trích rút.....	51
3.7. Kết quả thực nghiệm	52
3.7.1. Chức năng tạo khóa.....	52
3.7.2. Chức năng giấu thông tin	53
3.7.3. Chức năng trích rút tin mật	54
3.8. Đánh giá kết quả thực nghiệm	55
KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN	57
TÀI LIỆU THAM KHẢO.....	58
PHỤ LỤC	59

DANH MỤC CÁC TỪ VIẾT TẮT TRONG LUẬN VĂN

- BMP - Định dạng ảnh Bitmap (*Bitmap*)
- BPP - Số bit trên 1 pixel (*Bits per pixel*)
- CGA - Bộ điều hợp đồ họa màu (*Color Graphics Adapter*)
- CPT - Kỹ thuật giấu tin (*Cheng - Pan - Tseng*)
- DCT - Phép biến đổi Cosin rời rạc (*Discrete Cosine Transform*)
- DES - Hệ mật mã chuẩn (*Data Encryption Standard*)
- EGA - Bộ điều hợp đồ họa nâng cao (*Enhanced Graphics Adapter*)
- GIF - Định dạng ảnh Gif (*Graphics Interchange Format*)
- LSB - Bit có trọng số thấp nhất (*Least Significant Bit*)
- JPEG - Định dạng ảnh JPEG (*Join Photographic Experts Group*)
- RSA - Mã hóa công khai RSA (*Rivest, Shamir và Adleman*)
- SVGA - Bộ điều hợp đồ họa video cao cấp (*Super Video Graphics Adapter*)
- VGA - Bộ điều hợp đồ họa video (*Video Graphics Adapter*)
- WEP - Thuật toán mã hóa sử dụng trên mạng không dây (*Wired Equivalent Privacy*)

DANH MỤC CÁC HÌNH ẢNH

	Trang
Hình 1.1. Phân loại kỹ thuật giấu tin.....	6
Hình 1.2. Mô hình cơ bản của kỹ thuật giấu tin.....	7
Hình 1.3. Sơ đồ hệ thống mã hóa khóa công khai	11
Hình 2.1. Ảnh đen trắng	24
Hình 2.2. Ảnh đa mức xám	25
Hình 2.3. Ảnh màu	26
Hình 2.4. Ảnh trước và sau khi giấu tin bằng kỹ thuật LSB.....	30
Hình 2.5. Sơ đồ tạo khóa, mã hóa và giải mã RSA	34
Hình 2.6. Quá trình xử lý giấu thông điệp bí mật	37
Hình 2.7. Quá trình trích xuất thông điệp	38
Hình 3.1. Sơ đồ chức năng chương trình thử nghiệm.....	43
Hình 3.2. Sơ đồ hoạt động của quá trình giấu tin	45
Hình 3.3. Sơ đồ hoạt động của quá trình trích rút tin	47
Hình 3.4. Quá trình tạo khóa.....	53
Hình 3.5. Quá trình giấu tin của chương trình	54
Hình 3.6. Quá trình trích rút tin mật của chương trình	55

DANH MỤC CÁC BẢNG BIỂU

	Trang
Bảng 2.1. Ý nghĩa các trường trong vùng Bitmap Header	27
Bảng 2.2. Bảng số hóa thông tin cần giấu.....	29
Bảng 2.3. Bảng giá trị của bản mã và bản rõ	35
Bảng 3.1. Một số phần mềm giấu tin	42