

**ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN & TRUYỀN THÔNG**



NGUYỄN CAO THẮNG

**NGHIÊN CỨU, TÌM HIỂU
KỸ THUẬT GIẤU TIN MẬT VÀ ỨNG DỤNG**

LUẬN VĂN THẠC SĨ CÔNG NGHỆ THÔNG TIN

Thái Nguyên - 2020

**ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN & TRUYỀN THÔNG**



NGUYỄN CAO THẮNG

**NGHIÊN CỨU, TÌM HIỂU
KỸ THUẬT GIẤU TIN MẬT VÀ ỨNG DỤNG**

Ngành: Công nghệ thông tin

Chuyên ngành: Khoa học máy tính

Mã số: 848 0101

LUẬN VĂN THẠC SĨ CÔNG NGHỆ THÔNG TIN

NGƯỜI HƯỚNG DẪN KHOA HỌC: TS. HỒ VĂN CANH

Thái Nguyên - 2020

LỜI CAM ĐOAN

Học viên xin cam đoan luận văn này là công trình nghiên cứu thực sự của bản thân, dưới sự hướng dẫn khoa học của TS. Hồ Văn Canh.

Các số liệu, kết quả trong luận văn là trung thực và chưa từng được công bố dưới bất cứ hình thức nào. Tất cả các nội dung tham khảo, kế thừa của các tác giả khác đều được trích dẫn đầy đủ.

Em xin chịu trách nhiệm về nghiên cứu của mình.

Tác giả

Nguyễn Cao Thắng

LỜI CẢM ƠN

Học viên trân trọng cảm ơn sự quan tâm, tạo điều kiện và động viên của Lãnh đạo Đại học Công nghệ thông tin & Truyền thông, Đại học Thái Nguyên, các thầy cô Khoa Đào tạo sau đại học, các khoa đào tạo và các quý phòng ban Học viện trong suốt thời gian qua.

Học viên xin bày tỏ sự biết ơn sâu sắc tới TS. Hồ Văn Canh đã nhiệt tình định hướng, bồi dưỡng, hướng dẫn học viên thực hiện các nội dung khoa học trong suốt quá trình nghiên cứu, thực hiện luận văn.

Xin chân thành cảm ơn sự động viên, giúp đỡ to lớn từ phía Cơ quan đơn vị, đồng nghiệp và gia đình đã hỗ trợ học viên trong suốt quá trình triển khai các nội dung nghiên cứu.

Mặc dù học viên đã rất cố gắng, tuy nhiên, luận văn không tránh khỏi những thiếu sót. Học viên kính mong nhận được sự đóng góp từ phía Cơ sở đào tạo, quý thầy cô, các nhà khoa học để tiếp tục hoàn thiện và tạo cơ sở cho những nghiên cứu tiếp theo.

Xin trân trọng cảm ơn!

Thái Nguyên, tháng năm 2020

Học viên

Nguyễn Cao Thắng

MỤC LỤC

LỜI CAM ĐOAN	i
LỜI CẢM ƠN	ii
MỤC LỤC	iii
DANH MỤC TỪ VIẾT TẮT	v
DANH MỤC HÌNH VẼ	vii
DANH MỤC BẢNG BIỂU	viii
MỞ ĐẦU	1
1. Tính cấp thiết của đề tài	1
2. Mục đích nghiên cứu	2
3. Đối tượng và phạm vi nghiên cứu	2
4. Phương pháp nghiên cứu	2
5. Bố cục luận văn	2
CHƯƠNG 1. TỔNG QUAN VỀ KỸ THUẬT GIẤU TIN	3
1.1 Giới thiệu chung về giấu thông tin	3
1.2 Lịch sử ẩn giấu thông tin	4
1.3 Các thành phần của hệ giấu tin	5
1.4 Phân loại các kỹ thuật giấu tin	6
1.5 Môi trường giấu tin	6
1.5.1 Giấu tin trong ảnh	6
1.5.2 Giấu tin trong audio	8
1.5.3 Giấu tin trong video	8
1.5.4 Giấu tin trong văn bản dạng text	9
1.6 Giấu tin trong ảnh số	9
1.6.1 Một số khái niệm	9
1.6.2 Mô hình kỹ thuật giấu tin, tách tin	10
1.7 Tính chất, đặc trưng giấu tin trong ảnh	11
1.7.1 Phương tiện chứa có dữ liệu tri giác tĩnh	11
1.7.2 Giấu tin phụ thuộc ảnh	11
1.7.3 Giấu tin lợi dụng khả năng thị giác của con người	12
1.7.4 Giấu tin không làm thay đổi kích thước ảnh	12
1.7.5 Đảm bảo chất lượng ảnh sau khi giấu tin	12
Kết luận Chương 1	13
CHƯƠNG 2. NGHIÊN CỨU MỘT SỐ KỸ THUẬT GIẤU TIN MẬT	
TRONG ẢNH SỐ	14
2.1 Ảnh số	14
2.1.1 Khái niệm chung	14

2.1.2 Phân loại ảnh.....	15
2.1.3 Các định dạng ảnh	15
2.2 Yêu cầu đối với giấu tin trong ảnh.....	18
2.2.1 Tính bảo mật	20
2.2.2 Tỷ lệ giấu tin	20
2.2.3 Tính bền vững	20
2.2.4 Độ phức tạp tính toán	20
2.3 Hai tiêu chí đánh giá giấu tin trong ảnh.....	21
2.4 Một số phương pháp giấu tin trong ảnh.....	21
2.4.1 Giấu tin mật vào các bit có trọng số thấp LSB.....	21
2.4.2 Giấu tin kiểu chèn nhiều và điều chỉnh hệ số lượng tử	24
2.4.3 Phương pháp giấu tin thuận nghịch	25
2.4.4 Các phương pháp giấu tin khác	26
2.5 Một số thuật toán giấu tin trong ảnh.....	27
2.5.1 Thuật toán giấu tin đơn giản	27
2.5.2 Thuật toán giấu tin VU- LEE.....	31
2.5.3 Thuật toán giấu tin Chen- Pan- Tseng (CPT)	36
2.5.4 Thuật toán Chen- Pan- Tseng cải tiến.....	45
2.6 Mã hóa thông tin.....	47
2.6.1 Sơ lược về lịch sử mật mã học.....	50
2.6.2 Các khái niệm cơ bản.....	51
2.6.3. Phân loại	53
Kết luận Chương 2	56
CHƯƠNG 3. NGHIÊN CỨU XÂY DỰNG GIẢI PHÁP KẾT HỢP MÃ	
HÓA VÀ KỸ THUẬT GIẤU THÔNG TIN TRÊN MÔI TRƯỜNG ẢNH.....	57
3.1 Mục đích yêu cầu.....	57
3.2 Giải pháp	57
3.3 Xây dựng chương trình.....	59
3.3.1 Lựa chọn phương pháp mã hóa	59
3.3.2 Giải thuật giấu tin	62
3.4 Cài đặt và thực nghiệm	64
3.4.1 Cài đặt.....	64
3.4.2 Thực nghiệm	65
3.5 Đề xuất áp dụng vào thực tiễn công tác lĩnh vực AN-QP	72
Kết luận chương 3	74
KẾT LUẬN VÀ KIẾN NGHỊ	75
DANH MỤC CÁC TÀI LIỆU THAM KHẢO	77

DANH MỤC TỪ VIẾT TẮT

Ký hiệu, viết tắt		Ý nghĩa
AES	Advanced Encryption Standard	Tiêu chuẩn mã hóa tiên tiến
AN-QP		An ninh quốc phòng
CNSS	Committee on National Security Systems	Ủy ban hệ thống an ninh quốc gia
GCD	Greatest Common Divisor	Ước chung lớn nhất
HVS	Human Vision System	Kỹ thuật giấu tin phụ thuộc vào thị giác
HAS	Human Auditory System	Kỹ thuật giấu tin phụ thuộc vào thính giác
IT	Information Technology	Công nghệ thông tin
ISO	International Organization for Standardization	Tổ chức tiêu chuẩn hóa quốc tế
LSB	Least Significant Bit	Bit có trọng số bé nhất
MSB	Most Significant Bit	Bit có trọng số lớn nhất
NIST	National Institute of Science and Technology	Viện công nghệ và tiêu chuẩn quốc gia Hoa Kỳ
RSA	Rivest - Shamir - Adleman	Hệ mật mã RSA
CRT	Chinese Remainder Theorem	Định lý đồng dư Trung Hoa
$GF(P)$		Trường số hữu hạn P phần tử
$GF(2)$		Trường nhị phân
K		Tập hợp khóa mã
E		Thuật toán mã hóa

D		Thuật toán giải mã
P		Tập hợp các bản rõ
C		Tập hợp các bản mã
$\varphi(n)$		Hàm Phi_Ole
(p, q)		Cặp số nguyên tố p và q
n		Số nguyên dương bất kỳ
x		Văn bản rõ thuộc P
y		Bản mã thuộc C
k'		Thành phần khóa công khai
k''		Thành phần khóa bí mật
s		Số nguyên tố Mersenne
r		Số nguyên lẻ

DANH MỤC HÌNH VẼ

Hình 1.1: Sơ đồ phân loại các kỹ thuật giấu tin	6
Hình 1.2: Tỷ lệ phương tiện được lựa chọn để giấu tin	7
Hình 1.3: Kỹ thuật giấu tin công bố trong giai đoạn 1992- 2007	7
Hình 1.4: Sơ đồ giấu tin	10
Hình 1.5: Sơ đồ quá trình tách tin	11
Hình 2.1: Biểu đồ Histogram của ảnh ngọn nến.....	18
Hình 2.2: Minh họa giấu thông tin trong LSB của ảnh cấp xám 8 bit	22
Hình 2.3: Thay đổi bit	29
Hình 2.4: Ảnh trước và sau khi giấu các bit thông tin	35
Hình 2.5: Phân loại hệ mật	53
Hình 2.6: Sơ đồ mật mã đối xứng	54
Hình 2.7: Hệ thống mã khóa công khai.....	55
Hình 3.1: Mô hình giải pháp kết hợp mã hóa và ẩn giấu thông tin.....	59
Hình 3.2: File chạy chương trình	64
Hình 3.3: Giao diện chính chương trình	64
Hình 3.4: Quá trình nạp khóa công khai	65
Hình 3.5: Quá trình mã hóa bằng RSA và AES.....	66
Hình 3.6: Giao diện quá trình giấu tin	66
Hình 3.7: Chức năng tách dữ liệu từ ảnh	67
Hình 3.8: Quá trình giải mã thông điệp	68
Hình 3.7: Tập ảnh gốc	69

DANH MỤC BẢNG BIỂU

Bảng 2.1: Số hóa thông tin và ảnh gốc	22
Bảng 2.2: Khối bit ban đầu	29
Bảng 2.3: Bảng chân lý phép toán AND và XOR	32
Bảng 2.4: Mô tả quá trình đảo bit để giấu tin	34
Bảng 2.5: Ma trận trọng số W	37
Bảng 2.6: Chia ma trận ảnh theo thuật toán CPT	40
Bảng 2.7: Thực hiện phép XOR.....	40
Bảng 2.8: Thực hiện phép AND	41
Bảng 2.9: Bảng ghép khối ảnh theo thuật toán CPT	43
Bảng 2.10: Mô tả giải mã bản tin theo thuật toán CPT.....	47
Bảng 3.1: So sánh ảnh gốc và ảnh đã giấu tin.....	70