

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

HOÀNG XUÂN LONG

NGHIÊN CỨU THUẬT TOÁN GIẤU TIN MẬT  
TRÊN MIỀN KHÔNG GIAN CỦA ẢNH BITMAP

LUẬN VĂN THẠC SĨ KHOA HỌC MÁY TÍNH

## LỜI CAM ĐOAN

Với mục đích nghiên cứu, tìm hiểu để nâng cao kiến thức và trình độ chuyên môn để áp dụng trong các bài toán cụ thể trong tương lai nên tôi đã làm luận văn này một cách nghiêm túc và hoàn toàn trung thực. Nội dung luận văn do tự tôi tìm hiểu và hoàn thành.

Trong luận văn, tôi có sử dụng tài liệu tham khảo của một số tác giả trong và ngoài nước để hoàn thành luận văn được nêu ở phần tài liệu tham khảo.

Tôi xin cam đoan và chịu trách nhiệm về nội dung, sự trung thực trong luận văn tốt nghiệp Thạc sỹ của mình.

*Thái Nguyên, tháng 6 năm 2015*

**Học viên**

**HOÀNG XUÂN LONG**

## LỜI CẢM ƠN

Những kiến thức căn bản trong luận văn này là kết quả của quá trình tự nghiên cứu trong quá trình công tác và hai năm học Thạc sỹ (2012 - 2014) tại Trường Đại học Công nghệ thông tin và Truyền thông Thái Nguyên. Dưới sự giảng dạy, đào tạo và dìu dắt trực tiếp của các thầy cô trong trường và Viện Công nghệ thông tin Việt Nam.

Tôi xin bày tỏ lời cảm ơn chân thành tới các thầy cô trong Khoa Công nghệ thông tin, Phòng Đào tạo, Phòng Công tác học sinh sinh viên, Phòng Đào tạo sau đại học Trường Đại học Công nghệ thông tin và Truyền thông Thái Nguyên, đã tạo điều kiện thuận lợi cho tôi trong thời gian học tập tại trường.

Tôi xin bày tỏ lòng biết ơn chân thành, lời cảm ơn sâu sắc nhất đối với thầy giáo **TS Hồ Văn Canh** đã trực tiếp hướng dẫn, định hướng cho tôi giải quyết các vấn đề trong luận văn.

Tôi cũng xin cảm ơn đến người thân, bạn bè và các bạn đồng môn lớp cao học khóa 11, đã ủng hộ và giúp đỡ tôi trong quá trình làm luận văn tốt nghiệp.

*Thái Nguyên, ngày 20 tháng 6 năm 2015*

**Học viên**

**Hoàng Xuân Long**

## Ý NGHĨA KHOA HỌC CỦA ĐỀ TÀI

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.

Mặt khác, luận văn cũng nghiên cứu và đề xuất một phương pháp mã hóa thông tin sử dụng ma trận trên kích thước  $8 \times 8$  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 đã xây dựng được chương trình giấu tin mật trên miền không gian ảnh bitmap ứng dụng một kỹ thuật giấu tin mới.

*Hướng nghiên cứu tiếp theo:* Để hoàn thiện hơn nữa chương trình giấu tin mật kết hợp với nén mã hóa, cần phải nghiên cứu giấu tin trong các loại ảnh khác như: JPEG, TIF, GIF,... Và trên các môi trường đa phương tiện khác.

## MỤC LỤC

LỜI CAM ĐOAN .....	i
LỜI CẢM ƠN .....	iii
Ý NGHĨA KHOA HỌC CỦA ĐỀ TÀI .....	iv
MỤC LỤC .....	v
DANH MỤC CHỮ CÁI VIẾT TẮT.....	vii
DANH MỤC CÁC BẢNG.....	viii
DANH MỤC CÁC HÌNH VẼ .....	ix
LỜI NÓI ĐẦU .....	1
CHƯƠNG 1: NGHIÊN CỨU TỔNG QUAN VỀ LĨNH VỰC GIẤU TIN .....	3
1.1. Tổng quan về giấu tin.....	3
1.1.1. Định nghĩa.....	3
1.1.2. Vài nét về lịch sử giấu tin.....	3
1.1.3. Mục đích của giấu tin.....	4
1.1.4. Mô hình kỹ thuật giấu thông tin cơ bản. ....	5
1.1.5. Phân loại giấu tin.....	7
1.2. Giấu tin trong ảnh.....	10
1.3. Tổng quan ảnh BITMAP (BMP). ....	11
1.3.1. Giới thiệu ảnh BITMAP (BMP). ....	11
1.3.2. Cấu trúc ảnh BITMAP (BMP). ....	12
CHƯƠNG 2: NGHIÊN CỨU, PHÂN TÍCH VÀ TÌM HIỂU MỘT SỐ THUẬT TOÁN GIẤU TIN .....	17
2.1. Các kỹ thuật giấu tin. ....	17
2.1.1. Kỹ thuật giấu tin LSB. ....	17
2.1.2. Kỹ thuật giấu tin theo khối bit.....	19
2.1.3. Kỹ thuật giấu tin Wu-Lee.....	20
2.1.4. Thuật toán Chen-Pan-Tseng.....	21

2.1.5. Kỹ thuật giấu tin SES.....	24
2.2. Lý thuyết đại số và ứng dụng cải tiến kỹ thuật giấu tin LSB [2]:.....	29
2.2.1. Lý thuyết ma trận tam giác: .....	29
2.2.2. Lý thuyết về trường hữu hạn và không gian vector [6]. .....	35
2.2.3. Ứng dụng lý thuyết trên vào giấu tin. ....	42
CHƯƠNG 3: ỨNG DỤNG KỸ THUẬT GIẤU TIN MỚI XÂY DỰNG CHƯƠNG TRÌNH DEMO GIẤU TIN TRONG ẢNH BITMAP 24BIT .....	48
3.1. Xây dựng chương trình demo. ....	48
3.1.1. Môi trường thử nghiệm: .....	48
3.1.2. Tổ chức thực hiện chương trình: .....	48
3.1.3. Giao diện chương trình: .....	49
3.2. Ưu điểm & Nhược điểm.....	52
3.2.1. Ưu điểm.....	52
3.2.2. Nhược điểm.....	53
3.3. Lý thuyết độ trùng khớp.....	54
KẾT LUẬN .....	57
TÀI LIỆU THAM KHẢO.....	59

## **DANH MỤC CHỮ CÁI VIẾT TẮT**

BMP	Ảnh Bitmap
LSB	Least significant bit
SES	Steganography Evading analyses
RS	Regular Singular

**DANH MỤC CÁC BẢNG**

Bảng 1.1 Chi tiết khối bytes tiêu đề tập tin BMP. ....	13
Bảng 1.2 dưới đây miêu tả chi tiết khối bytes thông tin tập tin BMP. ....	14
Bảng 2.1 Bộ mã hóa.....	42
Bảng 2.2 Bảng chuyển đổi ký tự sang nhị phân. ....	46



**DANH MỤC CÁC HÌNH VẼ**

Hình 1.1: Hai lĩnh vực chính của kỹ thuật giấu thông tin.....	5
Hình 1.2: Lược đồ chung cho quá trình giấu tin.....	6
Hình 1.3: Lược đồ chung cho quá trình giải mã.....	7
Hình 1.4: Phân loại các kỹ thuật giấu tin. ....	9
Hình 2.1: Sơ đồ giấu tin SES. ....	26
Hình 2.2: Sơ đồ tách tin SES.....	28
Hình 3.1: Giao diện giới thiệu.....	50
Hình 3.2: Chương trình giấu tin .....	51
Hình 3.3: Ảnh gốc chưa giấu tin .....	52
Hình 3.4: Ảnh đã giấu tin.....	52

## LỜI NÓI ĐẦU

Trong những năm qua, chúng ta chứng kiến sự tiến bộ mạnh mẽ của khoa học - công nghệ nói chung và ngành Công nghệ thông tin nói riêng. Hưởng lợi từ những kết quả đó, không chỉ trong lĩnh vực dân sự, mà trong lĩnh vực An ninh - Quốc phòng, cũng tận dụng tối đa những thành tựu của ngành Công nghệ thông tin để phục vụ yêu cầu công tác. Cùng với sự phát triển mạnh mẽ của ngành khoa học công nghệ thông tin, internet đã trở thành một nhu cầu, phương tiện không thể thiếu đối với mọi người, việc truyền tin qua mạng ngày càng lớn. Tuy nhiên, với lượng thông tin được truyền qua mạng nhiều hơn thì nguy cơ dữ liệu bị truy cập trái phép cũng tăng lên vì vậy vấn đề bảo đảm an toàn và bảo mật thông tin cho dữ liệu truyền trên mạng là rất cần thiết.

Để đảm bảo an toàn và bí mật cho một thông điệp truyền đi người ta thường dùng phương pháp truyền thống là mã hóa thông điệp theo một qui tắc nào đó đã được thỏa thuận trước giữa người gửi và người nhận. Tuy nhiên, phương thức này thường gây sự chú ý của đối phương về tầm quan trọng của thông điệp. Thời gian gần đây đã xuất hiện một cách tiếp cận mới để truyền các thông điệp bí mật, đó là giấu các thông tin quan trọng trong những bức ảnh. Nhìn bề ngoài các bức ảnh có chứa thông tin cũng không có gì khác với các bức ảnh khác nên hạn chế được tầm kiểm soát của đối phương. Mặt khác, dù các bức ảnh đó bị phát hiện ra là có chứa thông tin trong đó thì với các khóa có độ bảo mật cao thì việc tìm được nội dung của thông tin đó cũng rất khó có thể thực hiện được.

Xét theo khía cạnh tổng quát thì giấu thông tin cũng là một hệ mã mật nhằm bảo đảm tính an toàn thông tin, nhưng phương pháp này ưu điểm là ở chỗ giảm được khả năng phát hiện được sự tồn tại của thông tin trong nguồn mang. Không giống như mã hóa thông tin là chống sự truy cập và sửa chữa một cách trái phép thông tin, mục tiêu của giấu thông tin là làm cho thông tin trộn lẫn với