

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

NGUYỄN TRẦN HÙNG

**XÂY DỰNG LƯỢC ĐỒ THỦY VĂN BỀN VỮNG
KHÓA CÔNG KHAI SỬ DỤNG KỸ THUẬT
TRẢI PHỔ TRÊN MIỀN TÀN SỐ**

LUẬN VĂN THẠC SĨ KHOA HỌC MÁY TÍNH

THÁI NGUYÊN - 2016

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

NGUYỄN TRẦN HÙNG

**XÂY DỰNG LƯỢC ĐỒ THỦY VĂN BỀN VỮNG
KHÓA CÔNG KHAI SỬ DỤNG KỸ THUẬT
TRẢI PHỔ TRÊN MIỀN TÀN SỐ**

Chuyên ngành: Khoa học máy tính

Mã số: 60 48 01 01

Người hướng dẫn khoa học: PGS.TS. PHẠM VĂN ÁT

THÁI NGUYÊN - 2016

LỜI CAM ĐOAN

Tôi xin cam đoan kết quả tìm hiểu, nghiên cứu được trình bày trong luận văn được xây dựng từ kiến thức và kinh nghiệm thực tiễn của bản thân tôi dưới sự hướng dẫn tận tình của thầy giáo PGS.TS Phạm Văn Át. Những điều tôi viết trong luận văn là hoàn toàn trung thực, không vi phạm bất cứ điều gì trong luật sở hữu trí tuệ và pháp luật Việt Nam. Tất cả các tài liệu tham khảo đều có xuất xứ rõ ràng và được trích dẫn hợp pháp.

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

Tác giả luận văn

LỜI CẢM ƠN

Lời đầu tiên, tôi xin bày tỏ lòng biết ơn sâu sắc đến Ban Giám Hiệu, các thầy giáo, cô giáo Đại học Công nghệ Thông tin và Truyền thông Thái Nguyên đã giảng dạy và cung cấp cho tôi những kiến thức rất bổ ích trong thời gian học, giúp tôi có nền tảng tri thức để phục vụ nghiên cứu khoa học sau này.

Đặc biệt, tôi xin bày tỏ sự kính trọng và lòng biết ơn sâu sắc đến thầy giáo PGS-TS. Phạm Văn Át người đã tận tình hướng dẫn, chỉ bảo và giúp đỡ tôi trong suốt quá trình nghiên cứu và hoàn thành luận văn này.

Xin gửi lời cảm ơn tới gia đình, bạn bè, những người luôn quan tâm, động viên, khuyến khích và giúp đỡ tôi trong suốt quá trình học tập và hoàn thành luận văn.

MỤC LỤC

LỜI CAM ĐOAN	iii
LỜI CẢM ƠN	iv
MỤC LỤC	v
DANH MỤC CÁC KÍ HIỆU	vii
DANH MỤC HÌNH VẼ	viii
MỞ ĐẦU	1
CHƯƠNG I: TỔNG QUAN VỀ ẢNH SỐ, GIẤU TIN VÀ THỦY VÂN SỐ.....	3
1.1. Ảnh số	3
1.1.1. Khái niệm ảnh số	3
1.1.2. Phân loại ảnh số	3
1.1.3. Một số khái niệm liên quan đến điểm ảnh	4
1.1.4. Histogram của ảnh.....	5
1.1.5. Định dạng ảnh bitmap và ảnh Jpeg	5
1.1.6. Một số mô hình màu.....	8
1.2. Kỹ thuật giấu tin	10
1.2.1. Khái niệm giấu tin.....	10
1.2.2. Mô hình kỹ thuật giấu tin	10
1.2.3. Các kỹ thuật giấu tin trong ảnh	12
1.2.4. Một số thuật toán giấu tin trên ảnh nhị phân.	14
Thuật toán THA	21
1.3. Kỹ thuật thủy vân	23
1.3.1. Khái niệm thủy vân	23
1.3.2. Thủy vân khóa bí mật và thủy vân khóa công khai.	23
1.3.3. Phân loại các kỹ thuật thủy vân.....	24
1.3.4. Mô hình hệ thống thủy vân.....	25
1.3.5. Các tính chất của hệ thủy vân.....	27
1.3.6. Những tấn công trên hệ thủy vân	28
1.3.7. Đánh giá chất lượng ảnh trong thủy vân	29

1.3.8. So sánh thủy văn tách được với thủy văn gốc.....	31
1.3.9. Ứng dụng của thủy văn số.....	32
CHƯƠNG II: THỦY VĂN BỀN VỮNG KHÓA CÔNG KHAI TRÊN MIỀN TẦN SỐ..	34
2.1. Một số lược đồ thủy văn trên miền tần số.....	34
2.2. Một số thuật toán thủy văn bền vững khóa công khai trên miền Cosine rời rạc (DCT).....	35
2.2.1. Phép biến đổi DCT.....	35
Phép biến đổi DCT 1 - D	36
Phép biến đổi IDCT 1 - D	36
Phép biến đổi DCT 2 - D	37
Phép biến đổi IDCT 2 - D	38
2.2.2. Miền DCT.....	39
2.3. Thuật toán R.Munir và thuật toán THLA	39
2.3.1. Thuật toán R.Munir.....	39
2.3.2. Thuật toán THLA	42
2.4. So sánh tính bền vững của thuật toán R.Munir và thuật toán THLA.....	45
CHƯƠNG III: CHƯƠNG TRÌNH THỬ NGHIỆM.....	48
3.1. Thủy văn và bản quyền tác giả	48
3.1.2 Phân tích bài toán.....	48
3.1.3 Phát biểu bài toán.....	48
3.1.4 Hướng giải quyết bài toán.....	49
3.2. Phần mềm thử nghiệm thủy văn bền vững trên miền DCT.....	49
3.2.1. Giao diện chính của chương trình	49
3.2.2 Thử nghiệm	51
3.2.3. Các hình thức tấn công	55
KẾT LUẬN.....	59
TÀI LIỆU THAM KHẢO	61

DANH MỤC CÁC KÍ HIỆU

CPT: Y.Chen, H.Pan, Y.Tseng

THA: ĐỖ VĂN TUẤN, TRẦN ĐĂNG HIÊN, PHẠM VĂN ÁT

THLA: ĐỖ VĂN TUẤN, TRẦN ĐĂNG HIÊN, CAO THỊ LUYÊN,
PHẠM VĂN ÁT

DANH MỤC HÌNH VẼ

Hình 1.1. Biểu diễn các điểm ảnh trong ảnh số	4
Hình 1.2. Biểu đồ histogram của ảnh đa cấp xám Lena	5
Hình 1.3. Cấu trúc tệp ảnh bitmap	6
Hình 1.4: Mô hình màu RGB	8
Hình 1.5: Mô hình màu YCbCr	9
Hình 1.6. Lược đồ của quá trình giấu tin	11
Hình 1.7. Lược đồ giải mã tin giấu	12
Hình 1.8. Phân loại các kỹ thuật thủy vân	24
Hình 1.9. Mô hình quá trình nhúng thủy vân.....	26
Hình 1.10. Mô hình quá trình tách và kiểm định thủy vân	27
Hình 2.1. Khối DCT kích thước 8×8	39
Hình 3.1. Giao diện thực hiện nhúng thủy vân	51
Hình 3.2: Các ảnh thử nghiệm	53
Hình 3.3 Giao diện so sánh hai phương pháp Munir và THLA	54
Hình 3.4 So sánh hệ số tương quan hai phương pháp Munir và THLA	55
Hình 3.5 Khẳng định bản quyền tác giả với phép tấn công Crop ảnh	56
Hình 3.6 Khẳng định bản quyền tác giả với phép tấn công làm nhiễu ảnh	57
Hình 3.7 Khẳng định bản quyền tác giả với phép tấn công xoay ảnh	57

MỞ ĐẦU

Hiện nay mạng Internet đã trở thành một trong các phương tiện truyền tải, chia sẻ thông tin, tài liệu một cách thuận tiện, hiệu quả. Tất cả mọi người ở mọi nơi, không phân biệt vị trí địa lý đều có thể kết nối vào Internet để tìm kiếm các thông tin cần thiết một cách dễ dàng. Thông qua mạng Internet, các nhà cung cấp sản phẩm có thể bán sản phẩm của mình cũng như sẵn sàng cung cấp dữ liệu, thông tin về các sản phẩm đó. Tuy nhiên việc quản lý và khai thác các thông tin này đôi khi không kiểm soát được do nạn sao chép bất hợp pháp, vi phạm bản quyền ngày một gia tăng. Vì vậy cần thiết phải có các giải pháp chống sao chép để hạn chế việc vi phạm bản quyền các sản phẩm dữ liệu số. Một trong những giải pháp hữu hiệu để bảo vệ bản quyền là kỹ thuật thủy vân số.

Thủy vân số dựa trên kết quả nghiên cứu của nhiều lĩnh vực khác nhau như: Mật mã học, kỹ thuật giấu tin, lý thuyết thống kê và xử lý tín hiệu số. Mục đích của phương pháp này là nhúng một lượng thông tin có ích được gọi là thủy vân vào các sản phẩm số. Dựa trên mục đích sử dụng, các lược đồ thủy vân được chia thành hai nhóm chính gồm thủy vân bền vững và thủy vân dễ vỡ. Thủy vân dễ vỡ được ứng dụng trong bài toán xác thực tính toàn vẹn dữ liệu số. Trong khi đó thủy vân bền vững được ứng dụng trong bài toán bảo vệ bản quyền đối với các sản phẩm số.

Gần đây đã có một số công trình nghiên cứu trong nước về thủy vân bền vững nhưng dựa vào khóa bí mật. Trong các công trình thủy vân khóa bí mật, người nhúng thủy vân và người trích thủy vân sử dụng chung một khóa bí mật. Điều này dẫn đến việc bảo mật công đoạn trao đổi khóa giữa người nhúng dấu thủy vân và người trích dấu thủy vân gặp phải những khó khăn. Để khắc phục vấn đề này một số nhà nghiên cứu chuyển hướng sang nghiên cứu phương pháp thủy vân bền vững khóa công khai. Phương pháp này, người

nhúng thủy vân sử dụng khóa bí mật, người trích thủy vân sử dụng khóa công khai. Đây là hướng nghiên cứu mới, có ý nghĩa khoa học và có nhiều ứng dụng trong thực tiễn. Vì vậy em chọn nghiên cứu đề tài: “***Xây dựng lược đồ thủy vân bền vững khóa công khai sử dụng kỹ thuật trải phổ trên miền tần số***”. Nội dung luận văn tập trung nghiên cứu, tìm hiểu một số kỹ thuật giấu tin, ảnh số và thủy vân bền vững trên ảnh số đã được công bố trên một số lược đồ thủy vân bền vững khóa công khai ứng dụng biến đổi Cosine rời rạc (DCT).

Cấu trúc của luận văn:

Ngoài phần mở đầu, phần kết luận, phần mục lục và tài liệu tham khảo.

Luận văn được bố cục gồm 3 chương, cụ thể như sau:

Chương I: Tổng quan về ảnh số, giấu tin và thủy vân số.

Chương II. Thủy vân bền vững khóa công khai trên miền tần số

Chương III: Chương trình thử nghiệm.

- Kết luận và những kiến nghị về hướng phát triển.

Mặc dù trong quá trình nghiên cứu và hoàn thành luận văn em đã rất nỗ lực và cố gắng. Tuy nhiên, do thời gian và trình độ còn hạn chế nên luận văn khó tránh khỏi những thiếu sót, kính mong nhận được sự đóng góp ý kiến, chỉ bảo của các thầy giáo, cô giáo và các bạn để luận văn hoàn thiện hơn.

Em xin trân trọng cảm ơn!