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

HOÀNG THỊ THÚY DIỆU

PHƯƠNG PHÁP THỦY VÂN DỄ VỠ KHÓA CÔNG KHAI ỨNG DỤNG TRONG BÀI TOÁN CHỐNG GIẢ MẠO VĂN BẰNG

LUẬN VĂN THẠC SỸ KHOA HỌC MÁY TÍNH

Thái Nguyên - 2014

LỜI CAM ĐOAN

Tôi xin cam đoan

Những nội dung trong luận văn này là do tôi thực hiện dưới sự chỉ đạo trực tiếp của thầy giáo PGS.TS Phạm Văn Ất.

Mọi tham khảo dùng trong luận văn đều được trích dẫn rõ ràng tên tác giả, tên công trình, thời gian, địa điểm công bố.

Mọi sao chép không hợp lệ, vi phạm qui chế đào tạo, hay gian trá tôi xin chịu hoàn toàn trách nhiệm.

Học viên

Hoàng Thị Thúy Diệu

LỜI CẢM ƠN

Lời đầu tiên, em xin gửi lời biết ơn sâu sắc đến PGS.TS Phạm Văn Ất người đã tận tình hướng dẫn, chỉ bảo, giúp đỡ em trong suốt quá trình làm luận văn.

Em cũng xin gửi lời cảm ơn đến các thầy cô giáo trường Đại học Công nghệ thông tin và Truyền thông - Đại học Thái Nguyên, các thầy cô Viện Công nghệ thông tin đã truyền đạt những kiến thức và giúp đỡ em trong suốt quá trình học của mình.

Tôi cũng xin gửi lời cảm ơn tới Ban giám hiệu trường Cao đẳng Cộng đồng Bắc Kạn đã tạo điều kiện thuận lợi cho tôi tham gia khóa học và trong suốt quá trình hoàn thành luận văn.

Và cuối cùng tôi xin gửi lời cảm ơn tới các đồng nghiệp, gia đình và bạn bè những người đã ủng hộ, động viên tạo mọi điều kiện giúp đỡ để tôi có được kết quả như ngày hôm nay.

Thái Nguyên, tháng 7 năm 2014

Học viên

Hoàng Thị Thuý Diệu

MỤC LỤC

TRANG PHỤ BÌA……i
LỜI CAM ĐOAN ii
LỜI CẢM ƠN iii
MỤC LỤC iv
DANH MỤC CÁC BẢNG vii
DANH MỤC CÁC HÌNH viii
MỞ ĐẦU 1
Chương 1 3
TỔNG QUAN VỀ CÁC KỸ THUẬT GIẤU TIN 3
1.1. Khái niệm giấu tin 3
1.2. Lịch sử giấu tin 4
1.3. Phân loại các kỹ thuật giấu tin 6
1.4. Ứng dụng của kỹ thuật giấu tin 6
1.5. Một số hướng tiếp cận giấu tin trong ảnh 8
1.5.1. Giấu tin trên miền không gian ảnh 8
1.5.2. Giấu tin trên miền tần số 8
1.6. Cấu trúc tệp ảnh bitmap 9
1.6.1. Cấu trúc và nội dung của Bitmap File Header 10
1.6.2. Cấu trúc và nội dung của Bitmap Info 10
1.6.3. Cấu trúc và nội dung của Color Palette 11
1.6.4. Bitmap Data 11
1.7. Một số định nghĩa 11
1.8. Thuật toán giấu tin Wu-Lee 13
1.8.1. Thuật toán nhúng tin 13
1.8.2. Phân tích thuật toán 15

1.8.3. Thí dụ minh họa thuật toán nhúng tin Wu-Lee 16
1.8.4. Một số nhận xét về thuật toán Wu-Lee 17
1.9. Thuật toán Chen – Pan – Tseng 18
1.9.1. Ý tưởng 18
1.9.2. Thuật toán nhúng tin CPT 18
1.9.3. Chứng minh tính đúng đắn của thuật toán 20
1.9.4. Một số thí dụ minh họa thuật toán CPT 22
1.9.5. Phân tích thuật toán 25
1.10. Thuật toán giấu tin THA 26
1.10.1. Thuật toán nhúng tin 26
1.10.2. Ví dụ minh hoạ 27
Chương 2 29
MỘT SỐ LƯỢC ĐỒ THỦY VÂN DỄ VỠ KHÓA CÔNG KHAI 29
2.1. Thủy vân trên ảnh số 29
2.2. Phân loại thủy vân 30
2.3. Giới thiệu về hàm băm 31
2.3.1. Định nghĩa hàm băm 31
2.3.2. Đặc tính của hàm băm 31
2.3.3. Tính chất của hàm băm 32
2.3.4. Một số hàm băm phổ biến 33
2.3.5. Tiêu chuẩn của một hàm băm tốt 35
2.3.6. Ứng dụng của hàm băm 36
2.4. Hệ mật mã khóa công khai 36
2.4.1. Mã khóa công khai 37
2.4.2. Sơ đồ mã khóa công khai 37
2.4.3. Các đặc trưng của khóa công khai 38
2.4.4. Ứng dụng khóa công khai 38

2.4.5. Tính an toàn của các sơ đồ khóa công khai 39
2.5. Hệ mã hóa RSA 39
2.5.1. Tạo khóa cho RSA 40
2.5.2. Sử dụng RSA 40
2.5.3. Ví dụ RSA 40
2.5.4. Sơ đồ chữ ký số RSA 41
2.6. Quản lý và phân phối khóa 42
2.7. Lược đồ thủy vân dễ vỡ khóa công khai trên ảnh nhị phân 43
2.7.1. Thuật toán nhúng dấu thủy vân 44
2.7.2. Thuật toán xác thực tính toàn vẹn 44
2.7.3. Tấn công tính chẵn lẻ 45
2.8. Lược đồ thủy vân dễ vỡ khóa công khai trên ảnh mầu 46
2.8.1. Nhúng tin trên ảnh mầu bằng kỹ thuật chèn bit thấp 46
2.8.2. Thuật toán nhúng thủy vân 48
2.8.3. Thuật toán xác thực 49
Chương 3 51
ỨNG DỤNG THỦY VÂN DỄ VỠ KHOÁ CÔNG KHAI TRONG 51
BÀI TOÁN CHỐNG GIẢ MẠO VĂN BẰNG 51
3.1. Bài toán 51
3.2. Giải pháp 51
3.3. Mô hình xử lý của hệ thống 51
3.4. Kết quả thực nghiệm 53
KẾT LUẬN 58
TÀI LIỆU THAM KHẢO 59
I. Tiếng Việt 59
II. Tiếng Anh 59

DANH MỤC CÁC BẢNG

Bảng 1.1. Cấu trúc và nội dung của Bitmap File Header 10
Bảng 1.2. Cấu trúc và nội dung của Bitmap Info..... 10
Bảng 1.3. Cấu trúc và nội dung của Color Palette 11

DANH MỤC CÁC HÌNH

Hình 1.1. Mô hình giấu tin 3
Hình 1.2. Mô hình giải mã thông tin 4
Hình 1.3. Phân loại kỹ thuật giấu tin 6
Hình 1.4. Minh hoạ thuật toán nhúng tin của Wu-Lee 16
Hình 1.5. Minh hoạ giữa thay đổi ngẫu nhiên và thay đổi có định hướng 18
Hình 1.6. Minh hoạ thuật toán CPT trường hợp thay đổi 1 bit 222
Hình 1.7. Minh hoạ quá trình giải mã thông tin đã giấu 233
Hình 1.8. Thí dụ minh hoạ trường hợp thay đổi hai bit 25
Hình 2.1. Mô hình thủy vân số 29
Hình 2.2. Phân loại thủy vân theo mục đích ứng dụng 30
Hình 2.3. Sơ đồ mã khóa công khai 38
Hình 2.4. Mô hình thuật toán nhúng thủy vân 44
Hình 2.5. Mô hình xác thực tính toàn vẹn 45
Hình 3.1. Sơ đồ thủy vân ảnh bằng 52
Hình 3.2. Sơ đồ xác thực và định vị vùng giả mạo 53
Hình 3.3. Ảnh bằng gốc ..... **Error! Bookmark not defined.**
Hình 3.4. Ảnh bằng thủy vân 55
Hình 3.5 Ảnh bằng giả 56
Hình 3.6. Ảnh định vị vùng giả mạo 57

MỞ ĐẦU

Một trong những thành tựu quan trọng của những thập niên cuối thế kỷ XX, đầu thế kỷ XXI là sự ra đời, phát triển của mạng Internet. Mọi người đều có thể kết nối vào Internet để tìm kiếm thông tin một cách dễ dàng thông qua nhà cung cấp dịch vụ Internet. Người dùng có thể đọc thông tin mới nhất, tra cứu các thư viên số, tìm thông tin lĩnh vực mình quan tâm. Bên cạnh đó, các nhà cung cấp sản phẩm cũng sẵn sàng cung cấp dữ liệu của mình cho người dùng thông qua mạng.

Tuy nhiên việc phân phối một cách phổ biến các tài nguyên trên mạng hiện nay luôn gặp phải vấn nạn sao chép và sử dụng không hợp pháp. Kỹ thuật thủy vân hiện đang được xem là một trong những giải pháp quan trọng trong việc bảo vệ bản quyền và xác thực tính toàn vẹn của dữ liệu số.

Theo mục đích sử dụng của lược đồ thủy vân được chia thành hai nhóm chính là thủy vân dễ vỡ và thủy vân bền vững. Mặt khác, dựa vào việc sử dụng khóa cũng có thể chia thành hai loại là: thủy vân khóa bí mật và thủy vân khóa công khai. Đối với thủy vân khóa bí mật, do sử dụng chung khóa cho cả hai quá trình nên cần phải có công đoạn trao đổi khóa giữa người nhúng và người kiểm tra dấu thủy vân, điều này dẫn đến việc bảo mật khóa gặp phải khó khăn. Tuy nhiên hạn chế này không xuất hiện trong thuật toán thủy vân khóa công khai.

Nội dung luận văn tập trung vào việc nghiên cứu một số kỹ thuật giấu dữ liệu trong ảnh đã được công bố, một số lược đồ thủy vân dễ vỡ khóa công khai trên ảnh nhị phân và ảnh mầu; ứng dụng những kỹ thuật này trong bài toán chống giả mạo văn bằng.

Cấu trúc của luận văn

Dựa vào mục tiêu đã xác định, nội dung của luận văn sẽ được trình bày qua 3 chương như sau:

Chương I: Tổng quan về các kỹ thuật giấu tin

Chương II: Một số lược đồ thủy vân dễ vỡ khóa công khai

Chương III: Ứng dụng thuỷ vân dễ vỡ khoá công khai trong bài toán chống giả mạo văn bằng.

Do thời gian và trình độ còn hạn chế nên luận văn khó tránh khỏi những sai sót, kính mong nhận được sự đóng góp chỉ bảo của các thầy, cô giáo và các bạn đồng nghiệp.

Qua đây tôi xin cảm ơn thầy giáo PGS.TS Phạm Văn Ất và các thầy giáo trong Trường Đại học công nghệ thông tin và truyền thông – Đại học Thái Nguyên đã tận tình hướng dẫn tôi trong quá trình học tập cũng như trong thời gian nghiên cứu hoàn thiện luận văn này.

Thái Nguyên, tháng 7 năm 2014

Học viên thực hiện

Hoàng Thị Thúy Diệu