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

Nguyễn Minh Họa

TÌM HIỂU THUỶ VÂN SỐ, MÃ HÓA DỰA TRÊN ĐỊNH DANH VÀ ỨNG DỤNG

Chuyên ngành : Khoa học máy tính
Mã số : 60 48 01

LUẬN VĂN THẠC SĨ KHOA HỌC MÁY TÍNH

NGƯỜI HƯỚNG DẪN KHOA HỌC
TS. Hồ Văn Hương

Thái Nguyên - 2015

LỜI CAM ĐOAN

Tôi xin cam đoan:

1. Những nội dung trong luận văn này là do tôi thực hiện dưới sự trực tiếp hướng dẫn của thầy giáo TS. Hồ Văn Hương.
2. 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.
3. Mọi sao chép không hợp lệ, vi phạm quy chế đào tạo, hay gian trá, tôi xin chịu hoàn toàn trách nhiệm.

Thái Nguyên, tháng năm 2015

Học viên

Nguyễn Minh Họa

LỜI CẢM ƠN

Tôi xin chân thành cảm ơn trường Đại học Công nghệ thông tin và Truyền thông – Đại học Thái nguyên, cùng tất cả các thầy giáo, cô giáo đã tận tình giảng dạy và giúp đỡ tôi trong suốt quá trình học tập, nghiên cứu.

Tôi xin bày tỏ lòng biết ơn sâu sắc đến thầy giáo TS. Hồ Văn Hương, người đã trực tiếp hướng dẫn và tạo mọi điều kiện thuận lợi giúp đỡ tôi trong quá trình thực hiện đề tài.

Tôi xin trân trọng cảm ơn Ban lãnh đạo, các đồng nghiệp đã ủng hộ và dành thời gian để giúp đỡ tôi hoàn thành luận văn này.

Tuy đã có nhiều cố gắng, nhưng chắc chắn luận văn của tôi còn có rất nhiều thiếu sót. Rất mong nhận được sự góp ý của thầy giáo, cô giáo và các bạn đồng nghiệp.

Xin chân thành cám ơn!

MỤC LỤC

DANH MỤC CÁC THUẬT NGỮ, CÁC CHỮ VIẾT TẮT

AES	Advanced Encryption Standard	Chuẩn mã hoá tiên tiến
ANSI	American National Standards Institude	Viện tiêu chuẩn quốc gia Mỹ
CA	Certification Authority	Nhà cung cấp chứng thực
CRL	Certificate Revocation List	Danh sách các chứng thực thu hồi
FIPS	Federal Information Processing Standard	Chuẩn xử lý thông tin liên bang
IDEA	International Data Encryption Algorithm	Thuật toán mã hoá dữ liệu quốc tế
ISO	International Organization for Standardization	Tổ chức tiêu chuẩn hoá quốc tế
NIST	National Institute of Standards and Technology	Viện quốc gia về chuẩn và công nghệ
PKI	Public Key Infrastructure	Cơ sở hạ tầng khoá công khai
RA	Registration Authority	Nhà quản lý đăng ký
RSA	Rivest-Shamir-Aldeman	
	Watermarking	Thủy vân số
	Fragile	Dễ vỡ
	Robust	bền vững
PSNR	Peak Signal to Noise Ratio	Tỷ số tín hiệu đỉnh trên nhiễu.
	perceptual insignificant	Trực giác
JPEG	Joint Photographic Experts Group	Phương pháp nén ảnh

DCT	Discrete Cosine Transform	Phép biến đổi cosine rời rạc
IMG	Image	Ảnh IMG.
	Run – Length	Nén loạt dài

DANH MỤC CÁC BẢNG

DANH MỤC CÁC HÌNH VẼ, ĐỒ THỊ

1. Lời mở đầu

Ngày nay, nhu cầu về bảo đảm an toàn thông tin trong lĩnh vực y học ngày càng tăng, nhằm phục vụ công tác chăm sóc sức khỏe của cộng đồng và bảo mật hồ sơ bệnh án khi người bệnh đến khám và chữa bệnh tại bệnh viện, như các bệnh mãn tính, ung thư, viêm gan, HIV... Sự phát triển của dữ liệu đa phương tiện đã hỗ trợ tích cực các hoạt động y học như chẩn đoán từ xa, chia sẻ thông tin y tế. Một trong các kỹ thuật cổ điển nhất để bảo vệ bản quyền tài liệu số hóa, thủy vân số vẫn có nhiều đặc tính phù hợp để bảo vệ dữ liệu E-Health. Nhúng thủy vân số về bản chất là việc chèn một thông điệp vào tài liệu số, thường ở dạng dữ liệu multimedia (ảnh, audio hoặc video).

Thông tin bệnh học trong các hệ thống E-health được gửi tới cho các bác sỹ điều trị, phòng thí nghiệm, cơ quan điều tra nghiên cứu hoặc trung tâm tư vấn sức khỏe... Việc sử dụng hệ thống chăm sóc y tế điện tử mang lại các lợi ích trong việc truy cập, kiểm soát và chia sẻ thông tin y tế của người bệnh, tuy nhiên lại gây ra các nguy cơ xâm phạm tính bí mật và riêng tư tới các thông tin sức khỏe nhạy cảm của người bệnh như các bệnh mãn tính, ung thư, viêm gan B, HIV.... Các nghiên cứu liên quan về sử dụng thủy vân số ứng dụng trong y sinh học sẽ được trình bày, trên cơ sở đó, một mô hình đề xuất sử dụng thủy vân số kết hợp mã hóa truyền thông dựa trên định danh được trình bày. Phương pháp này giúp đảm bảo tính bí mật và riêng tư cho các thông tin dữ liệu cho người bệnh. Hiện nay, mới chỉ có một vài cách tiếp cận đối với bài toán thuỷ vân dữ liệu quan hệ được đề xuất. Tuy nhiên, những kỹ thuật này không bền vững trước các tấn công thông thường và các tấn công gây hại, vì vậy cần có một kỹ thuật thủy vân cơ sở dữ liệu quan hệ có độ bền vững cao hơn nhất là đối với các tấn công xoá, sửa và chèn các bản ghi.

Bằng cách sử dụng thủy vân, dữ liệu số sẽ bảo vệ khỏi sự sao chép bất hợp pháp. Thủy vân là một mẩu tin được ẩn trực tiếp trong dữ liệu số. Thủy

vân luôn gắn kết với dữ liệu số. Bằng trực quan thì khó có thể phát hiện được thủy vân trong dữ liệu chứa nhưng ta có thể tách được chúng bằng các chương trình có cài đặt thuật toán thủy vân. Thủy vân tách được từ dữ liệu số chính là bằng chứng kết luận dữ liệu số có bị xuyên tạc thông tin hay vi phạm bản quyền không.

Mã hóa dựa trên định danh (Indetity based encryption -IBE) hiện nay đang được xem là một công nghệ mật mã mới có nhiều thuận tiện trong thực thi ứng dụng so với các thuật toán khóa công khai khác. Đối với các hệ mật mã khóa công khai truyền thống, việc cài đặt là khó khăn và tốn kém, ứng dụng thành công nhất của công nghệ khóa công khai là việc sử dụng rộng rãi của SSL, nó yêu cầu tương tác tối thiểu với người sử dụng khi được dùng để xác thực máy chủ và mã hóa các truyền thông với máy chủ đó. Các ứng dụng mà yêu cầu người sử dụng quản lý hoặc sử dụng các khóa công khai thì không thành công được như vậy. IBE là một công nghệ mã hoá khoá công khai, cho phép một người sử dụng tính khoá công khai từ một chuỗi bất kỳ. Chuỗi này như là biểu diễn định danh của dạng nào đó và được sử dụng không chỉ như là một định danh để tính khoá công khai, mà còn có thể chứa thông tin về thời hạn hợp lệ của khoá để tránh cho một người sử dụng dùng mãi một khoá IBE hoặc để đảm bảo rằng người sử dụng sẽ nhận được các khoá khác nhau từ các hệ thống IBE khác nhau. Trong chuỗi này có chứa thông tin là duy nhất đối với mỗi cài đặt IBE cụ thể, chẳng hạn như URL mà định danh máy chủ được sử dụng trong cài đặt của các hệ thống IBE khác nhau. Khả năng tính được các khoá như mong muốn làm cho các hệ thống IBE có các tính chất khác với các tính chất của các hệ thống khoá công khai truyền thống, những tính chất này tạo ra các ưu thế thực hành đáng kể trong nhiều tình huống. Bởi vậy, có một số ít tình huống không thể giải quyết bài toán bất kỳ với các công nghệ khoá công khai truyền thống, nhưng lại có thể giải quyết được với IBE và sử