MỤC LỤC

CHƯƠNG 1: TỔNG QUAN VỀ XÁC THỰC ĐIỆN TỬ

1.1 Khái niệm xác thực

1.1.1 Xác thực theo nghĩa thông thường

Xác thực là một chứng thực một cái gì đó (hoặc một người nào đó) đáng tin cậy, có nghĩa là, những lời khai báo do người đó đưa ra hoặc về vật đó là sự thật.

Xác thực một đối tượng còn có nghĩa là công nhận nguồn gốc (provenance) của đối tượng, trong khi, xác thực một người thường bao gồm việc thẩm tra nhận dạng họ. Việc xác thực thường phụ thuộc vào một hoặc nhiều nhân tố xác thực (authentication factors) để minh chứng cụ thể.

1.1.2 Xác thực điện tử

Xác thực trong an ninh máy tính là một quy trình nhằm cố gắng xác minh nhận dạng số (digital identity) của phần truyền gửi thông tin (sender) trong giao thông liên lạc chẳng hạn như một yêu cầu đăng nhập. Phần gửi cần phải xác thực có thể là một người dùng một máy tính, bản thân một máy tính hoặc một chương trình máy tính (computer program).

Ngược lại sự tin cậy mù quáng (blind credential) hoàn toàn không thiết lập sự đòi hỏi nhận dạng, song chỉ thiết lập quyền hoặc địa vị hẹp hòi của người dùng hoặc của chương trình ứng dụng mà thôi.

Trong một mạng lưới tín nhiệm, việc "xác thực" là một cách để đảm bảo rằng người dùng chính là người mà họ nói họ là, và người dùng hiện đang thi hành những chức năng trong một hệ thống, trên thực tế, chính là người đã được ủy quyền để làm những việc đó.

1.2 Phân loại xác thực điện tử

1.2.1 Xác thực dữ liệu

1). Xác thực thông điệp (Message Authentication)

2). Xác thực giao dịch (Transaction Authentication)

3). Xác thực khóa (Key Authentication)

4). Xác thực nguồn gốc dữ liệu (Source của Data)

5). Xác thực bảo đảm toàn vẹn dữ liệu (Data Integrity)

1.2.2 Xác thực thực thể

1). Xác thực dựa vào thực thể: Biết cái gì (Something Known)

2). Xác thực dựa vào thực thể: Sở hữu cái gì (Something Possessed)

3). Xác thực dựa vào thực thể: Thừa hưởng cái gì (Something Inherent)

1.3 Xác thực dữ liệu

1.3.1 Xác thực thông điệp

Khái niệm

Xác thực thông điệp hay ***Xác thực tính nguyên bản*** của dữ liệu (Data Origin Authentication) là một kiểu ***xác thực đảm bảo một thực thể*** được chứng thực là **nguồn gốc thực sự** tạo ra dữ liệu này ở một thời điểm nào đó.

Xác thực thông điệp bao hàm cả **tính toàn vẹn dữ liệu**, nhưng ***không đảm bảo*** tính duy nhất và sự phù hợp về thời gian của nó.

1.3.1.1 Các phương pháp xác thực thông điệp

1.3.1.1.1 Xác thực thông điệp bằng chữ kí số

Ý tưởng chính của phương pháp xác thực bằng chữ ký số

1/. An gửi cho Thu cặp tin (X, Y), trong đó X là bản tin, Y là chữ ký số của bản tin X. Tức là $Y = Sig_k (X)$, Sig_k là thuật toán ký với khóa k.

2/. Khi nhận được (X, Y), Thu tiến hành kiểm tra chữ ký bằng thuật toán Ver

(X,Y). Nếu Ver_k (X, Y) = đúng thì Thu chắc chắn rằng X được bảo toàn.

Có hai khả năng:

+ An sử dụng chữ ký khôi phục được thông điệp gốc (chữ ký RSA).

+ An sử dụng chữ ký không khôi phục được thông điệp gốc (chữ ký ELGAMAL, chữ ký DSS).

1.3.1.1.2 Xác thực thông điệp bằng hàm băm

Ý tưởng chính của phương pháp xác thực bằng hàm băm

1/. A gửi cho B cặp tin (X, Y), trong đó X là bản tin, Y là đại diện bản tin X, tức là Y= h(X), h là hàm băm.

2/. Khi nhận được (X, Y), B tính lại h(X) = Z.

Nếu Z = Y, thì B chắc chắn rằng X được bảo toàn, không bị sửa đổi trên đường truyền.

Các hàm băm được sử dụng là:

- Hàm băm MD4.
- Hàm băm MD5.
- Hàm băm Secure Hash Standard (SHS).
- Hàm băm SHA.

1.3.1.1.3 Xác thực thông điệp bằng mã xác thực

Định nghĩa mã xác thực thông điệp

Mã xác thực là một bộ 4 (S, A, K, E) thoả mãn các điều kiện sau :

1 S là tập hữu hạn các trạng thái nguồn có thể.

2 A là tập hợp các nhãn xác thực có thể.

3 K là một tập hữu hạn các khoá có thể (không gian khoá).

4 Với mỗi $k \in K$ có một quy tắc xác thực $e_k : S \rightarrow A$.

Tập bản tin được xác định bằng $M = S \rightarrow A$.

Ý tưởng chính của phương pháp xác thực bằng mã xác thực

Chú ý một trạng thái nguồn tương đương với một bản rõ. Một bản tin gồm bản rõ với một nhãn xác thực kèm theo, một cách chính xác hơn có thể coi đó là một bản tin đã được xác nhận. Một quy tắc xác thực không nhất thiết phải là hàm đơn ánh.

Để phát thông báo (đã được kí). An và Thu phải tuân theo giao thức sau. Trước tiên họ phải chọn một khoá ngẫu nhiên $k \in K$. Điều này được thực hiện một cách bí mật như trong hệ mật khoá bí mật. Sau đó giả sử rằng An muốn gửi một trạng thái nguồn $s \in S$ cho Thu trên kênh không an toàn, An sẽ tính $a = e_k(s)$ và gửi bản tin (s, a) cho Thu. Khi nhận được (s, a) Thu tính $a' = e_K(s)$. Nếu $a = a'$ thì Thu chấp nhận bản tin là xác thực, ngược lại Thu sẽ loại bỏ nó.

1.3.2 Xác thực giao dịch

Khái niệm

Xác thực giao dịch là ***Xác thực thông điệp*** cộng thêm việc **đảm bảo tính duy nhất** (Uniqueness) và sự phù hợp về **thời gian** (Timeliness) của nó.

Xác thực giao dịch liên quan đến việc sử dụng các tham số thời gian (**TVB-** Time Variant Parameters).

Transaction Authentication = Message Authentication + TVB

Xác thực giao dịch "mạnh hơn" Xác thực thông điệp.

1.3.3 Xác thực khóa

+ Xác thực không tường minh khóa (Implicit Key Authentication):

Một bên được đảm bảo rằng chỉ có bên thứ hai (và có thể có thêm các bên tin cậy-Trusted Parties) là ***có thể*** truy cập được khóa mật.

+ ***Khẳng định (Xác nhận) khóa (Key Confirmation):***

Một bên được đảm bảo rằng bên thứ hai ***chắc chắn*** đã sở hữu khóa mật.

+ ***Xác thực tường minh khóa (Explicit Key Authentication)***

Bao gồm cả 2 yếu tố trên, nó chứng tỏ được định danh của bên có khóa đã cho.

Chú ý:

Xác thực khóa tập trung vào định danh bên thứ hai có thể truy cập khóa hơn là giá trị của khóa. Khẳng định khóa lại tập trung vào giá trị của khóa.

Ta gọi ngắn gọn Explicit Key Authentication là Key Authentication.

Chú ý:

Xác thực dữ liệu đã bao gồm tính toàn vẹn dữ liệu. Ngược lại thì không.

+ Đảm bảo xác thực nguồn gốc dữ liệu➔ phải đảm bảo tính toàn vẹn dữ liệu.

+ Đảm bảo tính toàn vẹn dữ liệu ➔không đảm bảo xác thực nguồn gốc dữ liệu.

1.3.4 Xác thực nguồn gốc dữ liệu

Công cụ: Dùng chữ ký số, hàm băm, thủy vân ký.

1.3.5 Xác thực bảo đảm toàn vẹn dữ liệu

Công cụ: Dùng chữ ký số, hàm băm, thủy vân ký, mã xác thực.

1.4 Xác thực thực thể

Xác thực thực thể (hay Định danh thực thể) là xác thực định danh của một đối tượng tham gia giao thức truyền tin.

Thực thể hay đối tượng có thể là người dùng, thiết bị đầu cuối,…Tức là: Một thực thể được xác thực bằng định danh của nó đối với thực thể thứ hai trong một giao thức, và bên thứ hai đã thực sự tham gia vào giao thức.

1.4.1 Xác thực dựa vào thực thể: Biết cái gì (Something Known)

Chẳng hạn, mật khẩu, mật khẩu ngữ (pass phrase) hoặc số định danh cá nhân (personal identification number - PIN). Định danh cá nhân (PIN- Personal Identifier Number) thường gắn với **Something Possessed** để tăng tính bảo mật.

Chú ý:

"Biết cái gì" được dùng trong ***Giao thức định danh,*** đó là ***cơ chế hỏi – đáp*** (Challenge-Response):

Một thực thể (Claimant) chứng tỏ định danh của nó đối với thực thể khác (Verifier) bằng các biểu lộ hiểu biết về một thông tin mật liên quan nào đó cho Verifier, mà không bộc lộ bí mật của nó cho Verifier trong suốt giao thức.

Cơ chế đó gọi là ***"Chứng minh không tiết lộ thông tin".***

Trong cơ chế hỏi – đáp thường dùng một người được uỷ quyền có tín nhiệm TA (Trusted Autherity) để tạo các tham số chung, các thuật toán ký, kiểm tra chữ ký và các chuỗi định danh, dấu xác nhận cho các bên tham gia.

1.4.1.1. Xác thực dựa trên User name và Password

Sự kết hợp của tên người dùng và mật khẩu là cách xác thực cơ bản nhất. Với kiểu xác thực này, chứng từ ủy nhiệm người dùng được đối chiếu với chứng từ được lưu trữ trên cơ sở dữ liệu hệ thống, nếu trùng khớp tên người dùng và mật khẩu, thì người dùng được xác thực và nếu không người dùng bị cấm truy cập. Phương thức này không an toàn lắm vì chứng từ xác nhận người dùng được gửi đi xác thực trong tình trạng "plain text", tức là không được mã hóa và có thể bị tóm trên đường truyền.

1.4.1.2. Giao thức Chứng thực bắt tay thách thức - Challenge Handshake Authentication Protocol (CHAP)

Giao thức Chứng thực "Bắt tay Thách thức" cũng là mô hình xác thực dựa trên tên người dùng/ mật khẩu. Khi người dùng cố gắng đăng nhập, server đảm nhiệm vai trò xác thực sẽ gửi một thông điệp thử thách (challenge message) trở lại máy tính người dùng. Lúc này máy tính người dùng sẽ phản hồi lại tên người dùng và mật khẩu được mã hóa. Server xác thực sẽ so sánh phiên bản xác thực người dùng được lưu giữ với phiên bản mã hóa vừa nhận. Nếu trùng khớp, người dùng sẽ

được xác thực. Bản thân mật khẩu không bao giờ được gửi qua mạng. Phương thức CHAP thường được sử dụng khi người dùng đăng nhập vào các "remote servers" của công ty chẳng hạn như RAS server. Dữ liệu chứa mật khẩu được mã hóa gọi là mật khẩu băm (hash password).

1.4.2 Xác thực dựa vào thực thể: Sở hữu cái gì (Something Possessed)

Ví dụ như sở hữu **khóa bí mật để ký điện tử.** Ví dụ như sở hữu thẻ từ (Magnetic-striped Card), thẻ tín dụng (Credit Card), thẻ thông minh (Smart Card), chứng minh thư (ID card), chứng chỉ an ninh (security token), chứng chỉ phần mềm (software token) hoặc điện thoại di động (cell phone).

1.4.2.1 Phương pháp xác thực Kerberos (Kerberos authentication)

Là phương pháp dùng một Server trung tâm để kiểm tra việc xác thực người dùng và cấp phát thẻ thông hành (service tickets) để người dùng có thể truy cập vào tài nguyên. Kerberos là một phương thức rất an toàn trong xác thực bởi vì dùng cấp độ mã hóa rất mạnh. Kerberos cũng dựa trên độ chính xác của thời gian xác thực giữa Server và máy khách, do đó cần đảm bảo có một "time server" hoặc "authenticating servers" được đồng bộ thời gian từ các "Internet time server". Kerberos là nền tảng xác thực chính của nhiều OS như Unix, Windows.

1.4.2.2 Phương pháp Tokens

Là phương tiện vật lý như các thẻ thông minh (smart cards) hoặc thẻ đeo của nhân viên (ID badges) chứa thông tin xác thực. Tokens có thể lưu trữ số nhận dạng cá nhân - personal identification numbers (PINs), thông tin về người dùng, hoặc mật khẩu.

Các thông tin trên token chỉ có thể được đọc và xử lý bởi các thiết bị đặc dụng, ví dụ như thẻ smart card được đọc bởi đầu đọc smart card gắn trên máy tính, sau đó thông tin này được gửi đến " authenticating server". Tokens chứa chuỗi text hoặc giá trị số duy nhất thông thường mỗi giá trị này chỉ sử dụng một lần.

Ví dụ về Smart cards:

Smart cards là ví dụ điển hình về xác thực tokens (token - based authentication). Một smart card là một thẻ nhựa có gắn một chip máy tính lưu trữ các loại thông tin điện tử khác nhau. Nội dung thông tin của card được đọc với một thiết bị đặc biệt.

1.4.3 Xác thực dựa vào thực thể: Thừa hưởng cái gì (Something Inherent)

Chẳng hạn, vết lăn tay hoặc mẫu hình võng mạc mắt, chuỗi ADN. (có đủ loại định nghĩa về cái nào là cái thích hợp và đầy đủ), mẫu hình về giọng nói (cũng có vài định nghĩa ở đây), sự xác minh chữ ký, tín hiệu sinh điện đặc hữu do cơ thể sống tạo sinh (unique bio-electric signals), hoặc những biệt danh sinh trắc (biometric identifier).

Phương pháp Biometrics (phương pháp nhận dạng sinh trắc học)

Mô hình xác thực dựa trên đặc điểm sinh học của từng cá nhân:

+ Quét dấu vân tay (fingerprint scanner).

+ Quét võng mạc mắt (retinal scanner).

+ Nhận dạng giọng nói (voice-recognition).

+ Nhận dạng khuôn mặt (facerecognition).

Vì nhận dạng sinh trắc học hiện rất tốn kém chi phí khi triển khai nên chưa được sử dụng rộng rãi như các phương thức xác thực khác.

Trong lịch sử, vết lăn tay là một phương pháp xác minh đáng tin nhất, song trong những vụ kiện tòa án (court cases) gần đây ở Mỹ và ở nhiều nơi khác, người ta đã có nhiều nghi ngờ về tính đáng tin cậy của dấu lăn tay. Những phương pháp sinh trắc khác được coi là khả quan hơn (quét võng mạng mắt và quét vết lăn tay là vài ví dụ), song có những bằng chứng chỉ ra rằng những phương pháp này, trên thực tế, dễ bị giả mạo.

CHƯƠNG 2: TỔNG QUAN VỀ THỦY VÂN SỐ

2.1 Giấu tin

2.1.1 Định nghĩa giấu tin

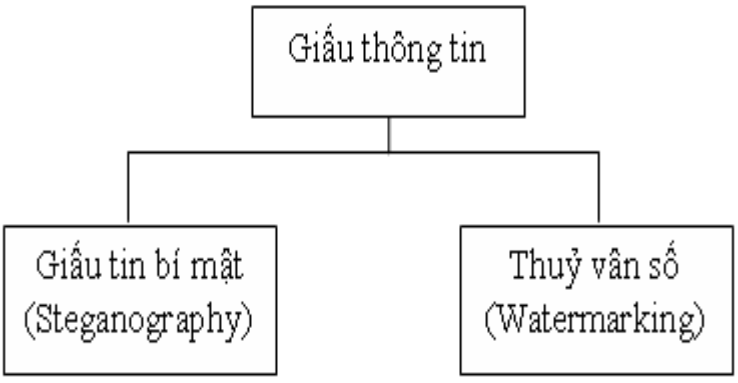
Giấu tin là một kỹ thuật giấu hoặc nhúng một lượng thông tin số nào đó vào trong một đối tượng dữ liệu số khác (giấu tin nhiều khi không phải là hành động giấu cụ thể mà chỉ mang ý nghĩa quy ước).

2.1.2 Mục đích của giấu tin

Có 2 mục đích của giấu thông tin:

- Bảo mật cho những dữ liệu được giấu.
- Bảo đảm an toàn (bảo vệ bản quyền) cho chính các đối tượng chứa dữ liệu giấu trong đó.

Có thể thấy 2 mục đích này hoàn toàn trái ngược nhau và dần phát triển thành 2 lĩnh vực với những yêu cầu và tính chất khác nhau.



Hình 2.1. Hai lĩnh vực chính của kỹ thuật giấu thông tin.

Kỹ thuật giấu thông tin bí mật (Steganography): với mục đích đảm bảo tính an toàn và bảo mật thông tin tập trung vào các kỹ thuật giấu tin để có thể giấu được

nhiều thông tin nhất. Thông tin mật được giấu kỹ trong một đối tượng khác sao cho người khác không phát hiện được.

Kỹ thuật giấu thông tin theo kiểu đánh giấu (thủy vân) có mục đích là để bảo vệ bản quyền của đối tượng chứa thông tin thì lại tập trung đảm bảo một số các yêu cầu như đảm bảo tính bền vững… đây là ứng dụng cơ bản nhất của kỹ thuật thuỷ vân số.

2.2 Thủy vân số

Tạo thủy vân là một phương pháp nhúng một lượng thông tin nào đó vào trong dữ liệu đa phương tiện nhằm khẳng định bản quyền sở hữu hay phát hiện xuyên tạc thông tin.

2.2.1 Mục đích

Thủy vân số có thể được sử dụng cho một loạt các ứng dụng như:

Bảo vệ bản quyền tác giả (copyright protection): Đây là ứng dụng cơ bản nhất của kỹ thuật thuỷ vân số (digital watermarking) một dạng của phương pháp giấu tin. Một thông tin nào đó mang ý nghĩa quyền sở hữu tác giả (người ta gọi nó là thuỷ vân - watermark) sẽ được nhúng vào trong các sản phẩm, thuỷ vân đó chỉ một mình người chủ sở hữu hợp pháp các sản phẩm đó có và được dùng làm minh chứng cho bản quyền sản phẩm. Giả sử có một thành phẩm dữ liệu dạng đa phương tiện như ảnh, âm thanh, video và cần được lưu thông trên mạng. Để bảo vệ các sản phẩm, chống lại các hành vi lấy cắp hoặc làm nhái cần phải có một kỹ thuật để "dán tem bản quyền" vào sản phẩm này. Việc dán tem hay chính là việc nhúng thuỷ vân cần phải đảm bảo không để lại một ảnh hưởng lớn nào đến việc cảm nhận sản phẩm. Yêu cầu kỹ thuật đối với ứng dụng này là thuỷ vân phải tồn tại bền vững cùng với sản phẩm, muốn bỏ thuỷ vân này mà không được phép của người chủ sở hữu thì chỉ còn cách là phá huỷ sản phẩm.

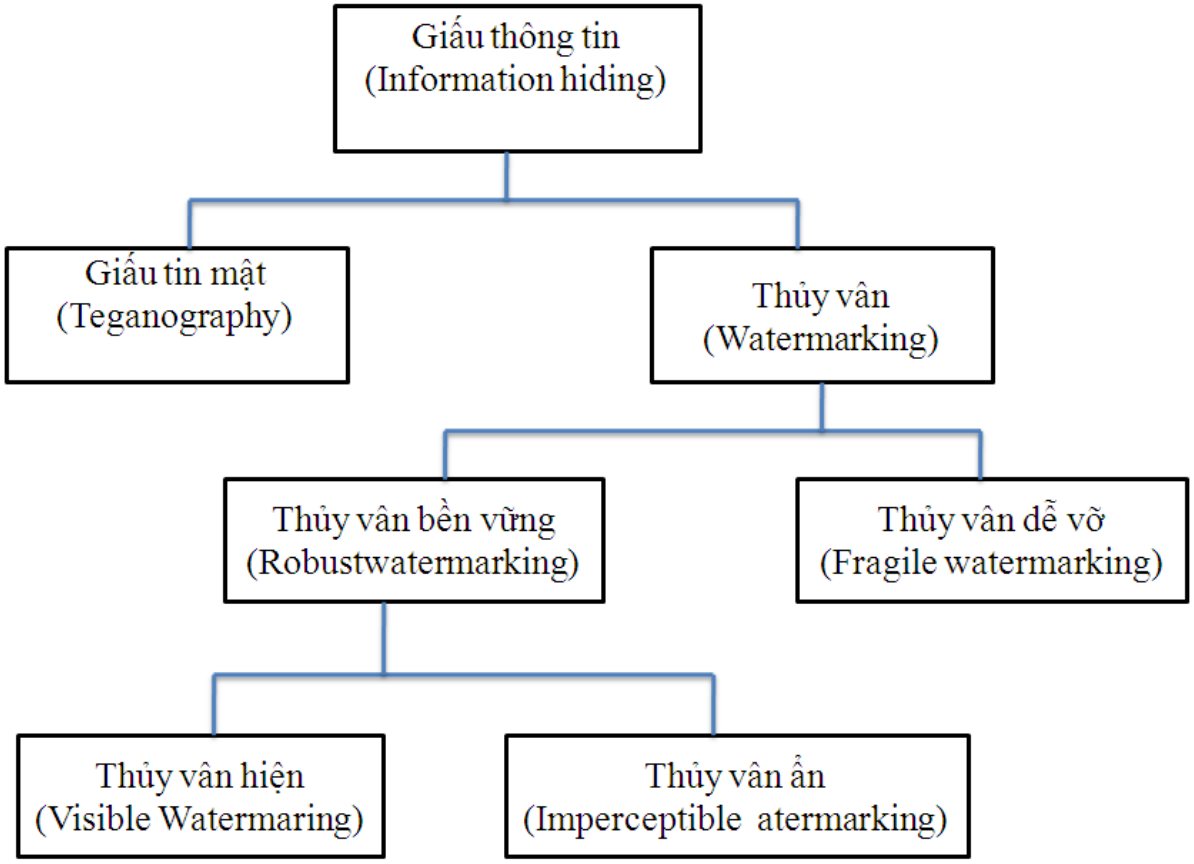
Nhận thực thông tin và phát hiện xuyên tạc thông tin (authentication and tamper detection): Một tập các thông tin sẽ được giấu trong phương tiện chứa sau đó được sử dụng để nhận biết xem dữ liệu trên phương tiện gốc đó có bị thay đổi hay không. Các thuỷ vân nên được ẩn để tránh được sự tò mò của kẻ thù, hơn nữa việc làm giả các thuỷ vân hợp lệ hay xuyên tạc thông tin nguồn cũng cần được xem xét. Trong các ứng dụng thực tế, người ta mong muốn tìm được vị trí bị xuyên tạc cũng như phân biệt được các thay đổi (ví dụ như phân biệt xem một đối tượng đa phương tiện chứa thông tin giấu đã bị thay đổi, xuyên tạc nội dung hay là chỉ bị nén mất dữ liệu). Yêu cầu chung đối với ứng dụng này là khả năng giấu thông tin cao và thuỷ vân không cần bền vững.

Giấu vân tay hay dán nhãn (fingerprinting or labeling): Thuỷ vân trong những ứng dụng này được sử dụng để nhận diện người gửi hay người nhận của một thông tin nào đó. Ví dụ như các vân khác nhau sẽ được nhúng vào các bản copy khác nhau của thông tin gốc trước khi chuyển cho nhiều người. Với những ứng dụng này thì yêu cầu là đảm bảo độ an toàn cao cho các thuỷ vân tránh sự xoá giấu vết trong khi phân phối.

Điều khiển sao chép (copy control): Các thuỷ vân trong những trường hợp này được sử dụng để điều khiển truy cập đối với các thông tin. Các thiết bị phát hiện ra thuỷ vân thường được gắn sẵn vào trong các hệ thống đọc ghi. Ví dụ như hệ thống quản lí sao chép DVD đã được ứng dụng ở Nhật. Các ứng dụng loại này cũng yêu cầu thuỷ vân phải được bảo đảm an toàn và cũng sử dụng phương pháp phát hiện thuỷ vân đã giấu mà không cần thông tin gốc.

2.2.2 Phân loại thủy vân

Thủy vân số đánh dấu vào đối tượng nhằm khẳng định bản quyền hay phát hiện xuyên tạc thông tin. Thủy vân số được phân thành hai loại là thủy vân bền vững và thủy vân dễ vỡ (Robustness and Fragileness).



Hình 2.2. Phân loại các kĩ thuật giấu tin.

2.2.2.1 Thủy vân bền vững (Robustness)

Thường được ứng dụng trong các ứng dụng bảo vệ bản quyền. Thủy vân thường được nhúng trong sản phẩm như một hình thức dán tem bản quyền. Trong trường hợp này, thủy vân phải tồn tại bền vững cùng với sản phẩm nhằm chống lại việc tẩy xóa, làm giả hay biến đổi phá hủy thủy vân.

- **Thủy vân ẩn** (Imperceptible): Cũng giống như giấu tin, bằng mắt thường không thể nhìn thấy thủy vân.
- **Thủy vân hiện** (Visible)**:** Là loại thủy vân được hiện ngay trên sản phẩm và người dùng có thể nhìn thấy được.

2.2.2.2 Thủy vân dễ vỡ (Fragileness)

Là kĩ thuật nhúng thủy vân vào trong ảnh sao cho khi phân bố sản phẩm trong môi trường mở, nếu có bất cứ một phép biến đổi nào làm thay đổi đối tượng sản phẩm gốc, thì thủy vân đã được dấu trong đối tượng sẽ không còn nguyên vẹn như trước khi dấu nữa (dễ vỡ).

CHƯƠNG 3: PHƯƠNG PHÁP XÁC THỰC BẰNG THỦY VÂN SỐ

3.1 Mở đầu

Trong suốt thập kỷ qua chúng ta đã chứng kiến sự thống trị của phương tiện truyền thông kỹ thuật số. Trái ngược với kĩ thuật tương tự, dữ liệu kỹ thuật số thì dễ dàng thao tác hơn trong nhiều trường hợp. Trên thực tế kĩ thuật số cung cấp cho người sử dụng nhiều sự thích ứng chất lượng cao, nó tạo ra các bản sao hoàn hảo. Ngày nay, với sự bùng nổ của Internet các tài liệu có bản quyền bị sao chép và phân phối khắp mọi nơi trên thế giới với mức chi phí gần như bằng không. Vì vậy một vấn đề quan trọng của việc sao chép không được ủy quyền và phân phối của các phương tiện truyền thông kỹ thuật số được nêu ra. Cũng trong một số trường hợp vấn đề của tính xác thực và độ tin cậy đã được nêu ra (như trong y tế hoặc quân sự). Thủy vân số được tạo ra để chống lại với một số trong những vấn đề này.

Phim và các ngành công nghiệp ghi âm, cũng như ngành công nghiệp truyền thông nói chung, kinh tế bị thiệt hại rất lớn từ vi phạm bản quyền. Do đó, có một sự quan tâm ngày càng tăng trong những năm gần đây trong lĩnh vực thủy vân kỹ thuật số. Thủy vân ảnh kỹ thuật số là đại diện cho việc nhúng một tín hiệu bí mật, gọi là "thủy vân", trong một hình ảnh kỹ thuật số, để chứng minh quyền sở hữu, hoặc kiểm tra tính xác thực hoặc tính toàn vẹn của một hình ảnh nhất định. Một hình ảnh đã được thủy vân có thể chống đỡ các cuộc tấn công khác nhau (có hại hoặc không mong muốn) mà cuối cùng có thể phá hủy khả năng cảm nhận được thủy vân. Khi thủy vân vẫn còn có thể cảm nhận được sau một số cuộc tấn công, quá trình này được gọi là thủy vân bền vững. Thủy vân bền vững thường được sử dụng để kiểm soát bản quyền. ngược lại thủy vân dễ vỡ là trường hợp thủy vân

được nhúng vào một hình ảnh theo cách mà các thay đổi nhỏ của hình ảnh do một cuộc tấn công, sẽ làm cho các thủy vân không thể cảm nhận được. Thủy vân dễ vỡ thường được sử dụng cho kiểm tra tính xác thực, hoặc kiểm tra toàn vẹn.

Hiện nay hầu hết các chương trình thủy vân hoạt động chống lại các cuộc tấn công hình học một cách kém cỏi. Các cuộc tấn công hình học phổ biến nhất là xoay, lật, dịch, thay đổi tỷ lệ, thay đổi kích thước và cắt xén. Trong nhiều trường hợp để giải quyết các cuộc tấn công hình học, chương trình thủy vân sử dụng một số phương pháp đồng bộ hóa. Những phương pháp này thường cố gắng xác định các biến dạng hình học và hoán đổi chúng, trước khi phát hiện thủy vân được áp dụng. Việc xác định các biến cố hình học được thực hiện bằng cách kiểm tra một mẫu đăng kí nhúng cùng với các thủy vân trong ảnh lưu trữ. Tuy nhiên việc bổ sung các mẫu đăng ký để các dữ liệu mang thủy vân làm giảm tính chính xác của hình ảnh đã được thủy vân, cũng như năng lực của chương trình. Một điểm yếu của phương pháp này là thường tất cả những hình ảnh được thủy vân thì lại mang thủy vân cùng đăng ký. Một khi tìm thấy, các mẫu đăng ký có thể được gỡ bỏ từ tất cả các hình ảnh được thủy vân, do đó hạn chế tính có thể đảo ngược của bất kỳ biến dạng hình học nào. Ngoài ra những phương pháp này tăng đáng kể thời gian tính toán và trong một số trường hợp hoạt động kém.

Ngoài ra còn có chương trình thủy vân cố gắng đạt được sự bền vững để chống lại cá cuộc tấn công hình học, sử dụng các phép biến đổi, bất biến với một số các cuộc tấn công, và chức năng tương quan. Mặc dù các chương trình cho thấy kết quả tốt đối với việc quan tâm đến tính bền vững, nhưng chúng yêu cầu độ phức tạp tính toán cao trong quá trình nhúng cũng như trong quá trình trích lọc thủy vân.

3.2 Kỹ thuật thủy vân thuận nghịch dựa trên bảng biểu đồ histogram của hình ảnh

3.2.1 Giới thiệu

Kỹ thuật thủy vân thuận nghịch dựa trên biểu đồ histogram của hình ảnh (Reversible watermarking based on histogram-RWBH) do E. Chrysochos, V.Fotopoulos, AN Skodras, M. Xenos Hệ thống kỹ thuật số & Truyền thông Phòng thí nghiệm máy tính, Trường Khoa học và Công nghệ, Đại học Mở Hy Lạp đề xuất năm 2007.

Chương trình áp dụng kĩ thuật thủy vân có các tính năng sau đây:

- Thuận nghịch: hình ảnh thủy vân có thể được phục hồi hoàn toàn lại trạng thái ban đầu.
- Che dấu: để phát hiện thủy vân chỉ có hình ảnh đã được thủy vân là cần thiết.

  - Không đối xứng: một khóa công khai được sử dụng để phát hiện các thủy vân và một khóa bí mật được sử dụng để khôi phục lại hình ảnh đã được thủy vân.

  - Bền vững chống lại các cuộc tấn công hình học như xoay, lật, thay đổi tỷ lệ và thay đổi kích thước, cong vênh, chuyển dịch, bản vẽ, cũng như sự kết hợp của chúng.
- Multicast: một watermark chắc chắn có thể được nhúng nhiều lần để tăng tính bền vững.
- chi phí tính toán thấp.
- Áp dụng đối với hình ảnh rất nhỏ (xuống đến mức 16 x 16).
- Áp dụng đối với hình ảnh màu.
- hình ảnh thủy vân chất lượng tốt.

Nguyên tắc cơ bản của kĩ thuật này được dựa trên các hoán vị của các bảng biểu đồ, được lựa chọn trong các cặp, theo một quy tắc cụ thể. Để nhúng thủy vân một khóa là cần thiết. Đây là một số thực số mà chỉ rõ khu vực nơi mà thủy vân được nhúng. Khóa này cũng cần thiết cho việc phát hiện và trích lọc các thủy vân. Vì vậy nó được coi như là khoá công khai. Một khoá thứ hai, mà được coi như là khóa bí mật, được sử dụng cho việc khôi phục đầy đủ của hình ảnh.

3.2.2 Thuật toán nhúng thủy vân

Tham số quan trọng cần thiết nhất để nhúng thủy vân vào hình ảnh lưu trữ, là khóa công khai. Khóa này (như đã đề cập ở trên) là một số thực số mà xác định khu vực nơi mà thủy vân được nhúng. Phần nguyên (start) cho biết điểm của biểu đồ, nơi mà qui trình nhúng sẽ bắt đầu lựa chọn các cặp của bảng biểu đồ. Phần thập phân của nó, nhân với mười, định rõ khoảng cách tối thiểu mà một cặp giá trị của bảng biểu đồ có thể có. Chúng tôi sẽ quy định khoảng cách này là bước (step).

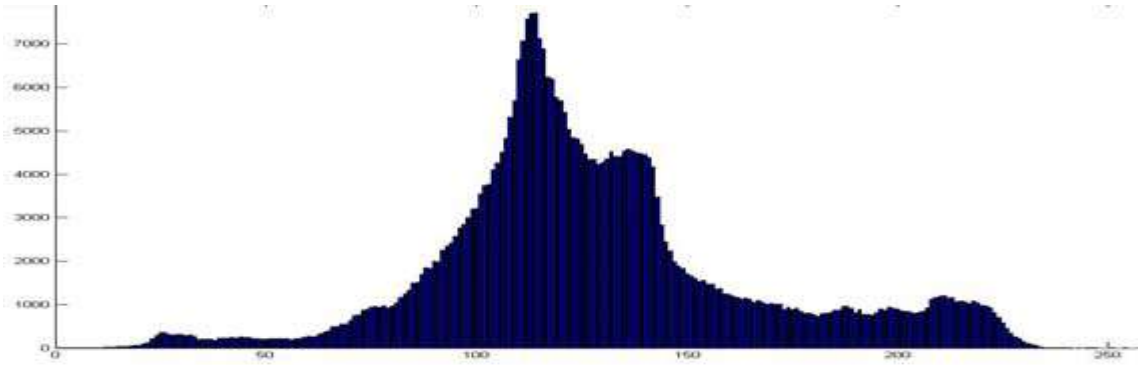
$$start = \text{public\_key div } 1$$

$$step = 10*(\text{public\_key mod } 1)$$

Các bước của thuật toán nhúng, để nhúng một thủy vân trong một hình ảnh xám như sau:

a. Các biểu đồ của hình ảnh lưu trữ được tính toán

b. *start* và *step* được tính toán đối với các khóa công khai.



Hình 3.1. Bảng biểu đồ lưu trữ và các cặp (a, b)

c. Cặp điểm đầu tiên (a, b) của các bảng biểu đồ được chọn theo start và step. Nếu các giá trị tương ứng của hist(a) và hist(b) bằng nhau, chúng ta loại cặp này và chúng ta tiếp tục với cặp kế tiếp.

d. Đối với mỗi cặp (a, b) và mỗi bit (w) của thủy vân tương ứng, các quy tắc sau đây được áp dụng. Nếu w bằng không thì sau đó các giá trị biểu đồ (hist(a), hist(b)) nên được xếp theo thứ tự tăng dần (tức hist(a)<hist(b)). Trong trường hợp ngược lại, tức là khi w bằng với một, các giá trị biểu đồ nên được xếp theo thứ tự giảm dần. (tức hist(a)>hist(b))

$$w=0 \rightarrow hist(a)<hist(b)$$

$$w=1 \rightarrow hist(a)>hist(b)$$

Nếu các giá trị của một cặp không theo thứ tự đúng theo quy tắc này, thì sau đó chúng được đổi chỗ, để thực hiện theo các quy tắc. Khi hai giá trị của biểu đồ được trao đổi thì chắc chắn rằng giá trị của các điểm ảnh tương ứng, với độ sáng a và b tương ứng, được đổi chổ lẫn nhau.

e. Các cặp (a, b) tiếp theo của bảng biểu đồ được chọn theo start và step cho việc nhúng bit (w) tiếp theo của các thủy vân. Các bước c và d của thuật toán được lặp lại cho đến khi tất cả các bit (w) của thủy vân đã được nhúng trong hình ảnh.

f. Các khóa bí mật, đó là cần thiết cho việc lưu trữ của hình ảnh, được tạo ra phù hợp với quy trình nhúng thủy vân. Đối với mỗi cặp (a, b) của bảng biểu đồ được lựa chọn, một bit (pk) của khóa riêng được tạo ra theo quy tắc này: nếu từ lúc đầu hist(a) và hist(b) xếp theo thứ tự tăng dần thì pk bằng không. Ngược lại, nếu ban đầu hist(a) và hist(b) xếp theo thứ tự giảm dần thì pk bằng một.

$$hist(a)<hist(b) \rightarrow pk=0$$

$$hist(a)>hist(b) \rightarrow pk=1$$

Trong trường hợp mà thuật toán đạt đến sự kết thúc của biểu đồ (tương ứng với một cường độ của 255), nó vẫn tiếp tục bắt đầu từ sự kết thúc của biểu đồ (tương ứng với một cường độ 0), với điều kiện là các cặp (a, b) không va chạm với một

cặp đã chọn trước đó. Để tránh những thủy vân đã được tạo ra trong hình ảnh, khoảng cách tối đa giữa a và b được thiết lập tới 9. Một trường hợp có thể phát sinh, là khi a là ở phần cuối của biểu đồ, trong khi b ở đầu biểu đồ. Trường hợp như vậy đã được đoán trước và bị cấm.

3.2.3 Thuật toán trích lọc thủy vân.

Các thông số cần thiết để trích lọc các thủy vân từ một hình ảnh có thể được đánh dấu, ngoại trừ từ chính hình ảnh đó, là khóa công khai và kích thước của thủy vân. Khóa công khai, như đã đề cập ở trên là một số thực số mà xác định vùng biểu đồ nơi mà thủy vân được nhúng. Chương trình không cần phải cho các hình ảnh ban đầu.

Các bước của thuật toán trích lọc thủy vân, để trích lọc thủy vân ra khỏi một hình ảnh màu xám ta làm như sau:

a. Các biểu đồ của hình ảnh đã được thủy vân được tính toán

b. start và step được tính toán đối với các khóa công khai.

c. Cặp (a, b) đầu tiên của bảng biểu đồ được chọn theo start và step. Nếu các giá trị tương ứng của biểu đồ hist(a) và hist(b) bằng nhau, cặp này bị loại bỏ và quá trình tiếp tục với cặp kế tiếp.

d. Mỗi cặp (a, b) tương ứng với chỉ một bit (w) của thủy vân. Các quy tắc sau đây được áp dụng. Nếu các giá trị của biểu đồ (hist(a), hist(b)) xếp theo thứ tự tăng dần thì w bằng không. Trong trường hợp ngược lại, nơi mà các giá trị biểu đồ nằm trong thứ tự giảm dần thì w bằng với một.

$$hist(a)<hist(b) \rightarrow w=0$$

$$hist(a)>hist(b) \rightarrow w=1$$

e. Các cặp (a, b) tiếp theo của bảng biểu đồ được chọn theo start và step để trích lọc bit (w) tiếp theo của thủy vân. Các bước c và d của thuật toán được lặp lại cho đến khi tất cả các bit (w) thủy vân được trích lọc. Nó là rất quan trọng cho quá

trình trích lọc, để chọn cùng các cặp (a, b) giống nhau, cái mà được chọn trong quá trình nhúng. Do đó sự lựa chọn của các cặp tiếp theo một cách chính xác các quy tắc tương tự với các thuật toán nhúng. Quy trình trích lọc thủy vân có thể thành công chỉ khi các cặp được chọn để trích lọc được chính xác giống như các cặp trước đó, chọn để nhúng.

3.2.4 Thuật toán khôi phục ảnh.

Để khôi phục lại hình ảnh đã thủy vân để trở thành hình ảnh ban đầu, cả hai khóa bí mật và khóa công khai là cần thiết. Khóa bí mật là khóa mà đã được tạo ra trong quá trình nhúng.

Các bước của thuật toán khôi phục để lấy lại hình ảnh ban đầu, như sau:

a. Các biểu đồ của hình ảnh được thủy vân được tính toán.

b. Start và step được tính toán đối với các khóa công khai.

c. Cặp (a, b) đầu tiên của bảng biểu đồ được chọn theo start và step. Nếu các giá trị tương ứng của biểu đồ hist(a) và hist (b) bằng nhau, cặp này bị loại và thuật toán tiếp tục với cặp kế tiếp.

d. Đối với mỗi cặp (a, b) và mỗi bit (pk) của khóa bí mật tách riêng, các quy tắc sau đây được áp dụng. Nếu pk bằng không thì sau đó các giá trị biểu đồ(hist(a), hist(b)) xếp theo thứ tự tăng dần. Trong trường hợp ngược, nơi pk bằng một, các giá trị biểu đồ xếp theo thứ tự giảm dần.

$$pk=0 \rightarrow hist(a)<hist(b)$$

$$pk=1 \rightarrow hist(a)>hist(b)$$

Nếu các giá trị của một cặp không theo thứ tự đúng theo quy tắc này, thì sau đó chúng được đổi chỗ, để thực hiện theo các quy tắc. Khi hai giá trị của biểu đồ được trao đổi, các giá trị cường độ của các điểm ảnh tương ứng được đổi chỗ lẫn nhau.

e. Các cặp (a, b) tiếp theo của bảng biểu đồ được chọn theo start và step. Các bước c và d của thuật toán được lặp lại cho đến khi tất cả các bit (pk) của khóa bí mật được kiểm tra đối với biểu đồ. Nó là rất quan trọng cho quá trình khôi phục lại để chọn cùng một cặp (a, b), cái mà được chọn trong quá trình nhúng. Do đó sự lựa chọn của các cặp tiếp theo một cách chính xác các quy tắc tương tự với các thuật toán nhúng.

3.3 Áp dụng một số phương pháp tấn công hình học để kiểm tra độ bền vững

Tập dữ liệu ảnh gồm các hình ảnh PNG:

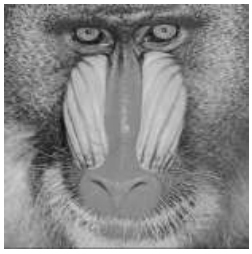
Bảng 3.1. Các hình ảnh thử nghiệm

Lena.png

Airplane. png

Perpper.png

Tiffany. png



Baboon. png

Beer. png

Sailboat. png

House. png

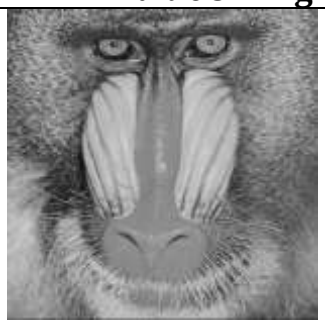
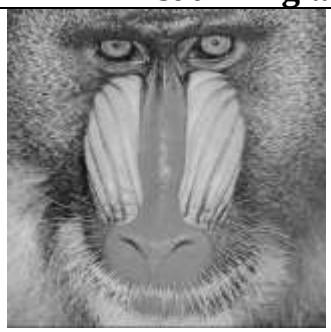
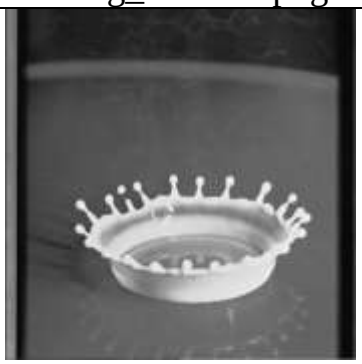
elaine.png

Anhstego.png

3.3.1 Đối với thuật toán nhúng thủy vân

Bảng 3.2. Các hình ảnh trước và sau khi thủy vân

Ảnh trước khi giấu	**Ảnh sau khi giấu**
anh_stego.png	nhung_anh_stego.png
 lena.png	 nhung_lena.png
 airplane. Png	 nhung_airplane.png
 peppers.png	 nhung_peppers.png

Ảnh trước khi giấu	Ảnh sau khi giấu
 baboon. Png	 nhung_baboon. png
 beer. png	 nhung_beer.png
 sailboat. png	 nhung_ailboat.png
 elaine.png	 nhung_elaine.png

Ảnh trước khi giấu	Ảnh sau khi giấu
 house.png	 nhung_house.png
 tiffany.png	 nhung_tiffany.png

Bảng 3.3 cho thấy rằng: PSNR của tất cả các ảnh đã được thủy vân ở trên đều từ mức 44.863 dB trở lên. Số lượng bit có thể nhúng giao động từ 1 bit đến 128 bit.

Bảng 3.3. Bảng tóm tắt kết quả thực nghiệm.

Ảnh vào	Khóa công khai	PSNR (dB)	Thông điệp	Ảnh ra
anh_stego.png(10x10)	12.1	63.3596	j	nhung_anh_stego.png
sailboat.png(512x512)	12.1	57.6653	Thanhanhvuct	nhung_sailboat.png
house.png(512x512)	12.5	48.700	Thuy van	nhung_house.png
beer.png(512x512)	12.1	61.4083	Copy right vmt10	nhung_beer.png
lena.png(512x512)	12.1	65.10.14	Copy right	nhung_lena.png
airplane.png(512x512)	12.1	70.9269	Copy right	nhung_ airplane.png
peppers.png(512x512)	12.1	661557	Copy right	nhung_peppers.png
elaine.png(512x512)	12.1	66.4548	Copy right	nhung_elaine.png
tiffany.png(512x512)	12.1	63.4598	Copy right	nhung_tiffany.png
baboon.png(512x512)	5.9	44.863	thanh	nhung_baboon.png

3.3.2 Đối với thuật toán trích lọc thủy vân

Với tập ảnh đã được nhúng thông điệp ở trên ta tiến hành trích lọc thủy vân, kết quả thực nghiệm như sau:

Bảng 3.4. Kết quả tóm tắt kết quả thực nghiệm với ảnh chưa bị biến đổi

Ảnh đã thủy vân	Khóa công khai	Thông điệp nhúng	Thông điệp trích lọc
nhung_anh_stego.png	12.1	j	j
nhung_sailboat.png	12.1	Thanhanhvuct	Thanhanhvuct
nhung_house.png	12.5	Thuy van	Thuy van
nhung_beer.png	12.1	Copy right vmt10	Copy right vmt10
nhung_lena.png	12.1	Copy right	Copy right
nhung_ airplane.png	12.1	Copy right	Copy right
nhung_peppers.png	12.1	Copy right	Copy right
nhung_elaine.png	12.1	Copy right	Copy right
nhung_tiffany.png	12.1	Copy right	Copy right
nhung_baboon.png	5.9	Thanh	thanh

Dựa vào Bảng 3.4 ta nhận thấy rằng khi ảnh chưa phải chịu bất kì một cuộc tấn công nào thì các thủy vân được lấy ra chính xác. Vấn đề đặt ra là khi ảnh đã được thủy vân bị tấn công (biến đổi) thì thủy vân còn được lấy ra chính xác hay không. Ta sẽ tiến hành tấn công vào 3 ảnh đã được nhúng thủy vân là: nhung_house.png, nhung_lena.png, nhung_baboon.png và trích lọc thủy vân của chúng kết quả thực nghiệm được thể hiện ở các bảng 3.5, bảng 3.6 và bảng 3.7.

Nhận xét:

Khi quan sát các bảng kết quả thực nghiệm(bảng 3.5, bảng 3.6 và bảng 3.7) trên ta thấy: thủy vân được lấy ra chính xác khi chịu các biến đổi xoay 90^0 , $180^{0,}$ 270^0 vì những biến đổi này không làm thay đổi bảng biểu đồ. Còn đối với các biến đổi còn lại như: xoay $15^0, 30^0, 45^0$, … thì thủy vân được lấy ra không còn chính xác nữa do bảng biểu đồ đã bị thay đổi.

+ Ảnh nhung_lena.png với thông điệp là”Copy right”:

Bảng 3.5 Kết quả thử nghiệm khi ảnh nhung_lena.png bị tấn công.

Các biến đổi đối với ảnh										Kết quả
Xoay ảnh						Tẩy	Làm mờ	Thay đổi tỉ lệ	Làm méo	
15^0	30^0	45^0	90^0	180^0	270^0					
x										½ðçðð
	x									-Đ$zÃ÷ü
		x								Àî= ò□±ü
			x							Copy right
				x						Copy right
					x					Copy right
						x				Copy rig(r
							x			ÿ\Ç:uö_#
								x		<htó÷O¶ý
									x	}Að>ÿà

+ **N**hung_house.png với thông điệp là”thuy van”:

Bảng 3.6 Kết quả thử nghiệm khi ảnh nhung_house_png bị tấn công.

Các biến đổi đối với ảnh										Kết quả
Xoay ảnh						Tẩy	Làm mờ	Thay đổi tỉ lệ	Làm méo	
15^0	30^0	45^0	90^0	180^0	270^0					
x										d□6!□6@□
	x									`□6(□□0□
		x								`□6□□
			x							thuy van
				x						thuy van
					x					thuy van
						x				tht¼□
							x			p 6@□
								x		Y 7b□
									x	H□6Q□¾□

+ nhung_baboon.png với thông điệp là “thanh”:

Bảng 3.7 Kết quả thứ nghiệm khi ảnh nhung_baboon.png bị tấn công.

Các biến đổi đối với ảnh										Kết quả
Xoay ảnh						Tẩy	Làm mờ	Thay đổi ti lệ	Làm méo	
15^0	30^0	45^0	90^0	180^0	270^0					
x										¸□à7
	x									¸□À7
		x								¸□à7
			x							thanh
				x						thanh
					x					thanh
						x				tl0Ù□
							x			°-□`
								x		□¸□□Ø
									x	□̧ø

3.3.3 Đối với thuật toán khôi phục ảnh gốc

Để khôi phục được ảnh ban đầu, ta chỉ cần ảnh đã thủy vân kèm theo hai khóa bí mật và công khai. Để đánh giá được ảnh khôi phục ta so sánh hai ma trận của ảnh khôi phục và ảnh gốc ban đầu. Ta tiến hành thử nghiệm với ảnh gốc là anh_stego.png, ảnh khôi phục là kp_anh_stego.png. Kết quả thực nghiệm như sau:

Bảng 3.8 kết quả thực nghiệm khôi phục ảnh

 anh_stego.png										 Kp_anh_stego.png									
110	115	108	100	97	101	107	111	109	107	110	115	108	100	97	101	107	111	109	107
109	117	111	103	100	105	111	115	112	108	109	117	111	103	100	105	106	115	112	108
108	117	114	106	103	108	116	118	116	111	108	117	114	111	103	108	116	118	116	111
100	111	112	106	106	110	115	117	115	111	100	111	112	106	106	110	115	117	115	111
93	105	108	107	108	110	114	115	114	112	93	105	108	107	108	110	114	115	114	112
83	94	101	105	109	109	109	109	110	110	83	94	101	105	109	109	109	109	110	110
73	81	89	99	105	105	103	102	102	101	73	81	89	99	105	105	103	102	102	101
64	69	80	92	101	102	100	97	94	92	64	69	80	92	101	102	100	97	94	92
60	60	71	84	95	98	95	91	86	80	60	60	71	84	95	98	95	91	86	80
61	59	69	82	91	93	90	85	78	71	61	59	69	82	91	93	90	85	78	71

3.4 Phương pháp xác thực bằng kĩ thuật RWBH

Giả sử có hai đối tượng A và B, A muốn gửi cho B một ảnh. Khi dữ liệu ảnh được truyền trên đường truyền, dữ liệu ảnh có thể sẽ bị các đối tượng xấu xuyên tạc, hoặc giả mạo. Ta sẽ tiến hành xác thực dữ liệu ảnh bằng cách áp dụng kĩ thuật RWBH ở phần sau.

3.4.1 phương pháp xác thực toàn vẹn dữ liệu bằng kĩ thuật RWBH

Khi truyền tải dữ liệu ảnh qua đường truyền, ảnh có thể bị xuyên tạc, để đảm bảo tính toàn vẹn của dữ liệu ảnh A và B sẽ thỏa thuận với nhau về thông điệp được nhúng trên ảnh. Lúc này A sẽ nhúng thông điệp Y (thông điệp đã thỏa thuận) trên toàn ảnh X để được X’ rồi gửi cho B cặp (X’, Y)

Khi B nhận được, B sẽ tiến hành tách thông điệp từ ảnh X’. Giả sử thông điệp tách được là Z. B sẽ so sánh Z và Y. Nếu Z trùng với Y thì ảnh không bị xuyên tạc. Ngược lại thì ảnh đã bị xuyên tạc.

Ví dụ 1: A muốn gửi cho B một ảnh có tên là “lena.png”, A sẽ nhúng thông điệp “tai lieu” (đã được thỏa thuận) trên toàn ảnh “lena.png” rồi gửi cho B. B sẽ tiến hành tách thông điệp và so sánh với thông điệp đã được thỏa thuận.

Ảnh trước khi nhúng Ảnh sau khi nhúng

Hình 3.2.ảnh lena.png trước và sau khi nhúng

Ở đây có hai trường hợp xảy ra:

Trường hợp 1: khi truyền trên đường truyền, ảnh không phải chịu bất cứ một cuộc tấn công hình học nào. Ta có kết quả của việc lấy và so sánh thông điệp theo chương trình thực hiện ***hình 3.3***

Hình 3.3 kết quả khi ảnh không phải chịu tấn công hình học

Trường hợp 2: khi truyền trên đường truyền, ảnh chịu một số cuộc tấn công hình học nào, giả sử ảnh bị xoay một góc bằng 30^0 (Hình 3.4), sau đó B sẽ tách thông điệp và so sánh, kết quả như ở *hình 3.5*

Hình 3.4 Ảnh nhúng thông điệp bị xoay 30^0

Hình 3.5 kết quả khi ảnh bị tấn công

Như vậy với kĩ thuật thủy vân thuận nghịch ta có thể áp dụng vào việc xác thực tính toàn vẹn dữ liệu ảnh.

3.4.2 phương pháp xác thực nguồn gốc dữ liệu bằng kĩ thuật RWBH

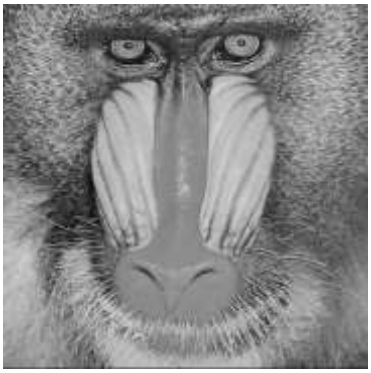
Giả sử A và B muốn gửi dữ liệu cho nhau. A và B đã thỏa thuận với nhau về cách xác thực nguồn gốc của dữ liệu ảnh bằng cách A sẽ nhúng một xâu kí tự lên ảnh. Để xác thực nguồn gốc dữ liệu ảnh A và B tiến hành như sau:

Trước tiên khi A muốn gửi cho B một ảnh, A sẽ tiến hành nhúng xâu kí tự (mà A đã thỏa thuận với B) lên ảnh muốn gửi.

Khi nhận được ảnh, B sẽ tiến hành tách xâu kí tự trên ảnh và so sánh với xâu kí tự của A mà hai bên đã thỏa thuận với nhau.

Nếu hai xâu kí tự là giống nhau thì ảnh đúng là nguồn gốc của A, nếu ngược lại thì ảnh không phải do A gửi.

Ví dụ 2: A tiến hành nhúng xâu kí tự: “CT1001_HPU” trên ảnh “baboon.png” (Hình 3.8) rồi gửi cho B. Khi nhận được, B tiến hành tách xâu kí tự trên ảnh “baboon.png” mà A đã gửi.

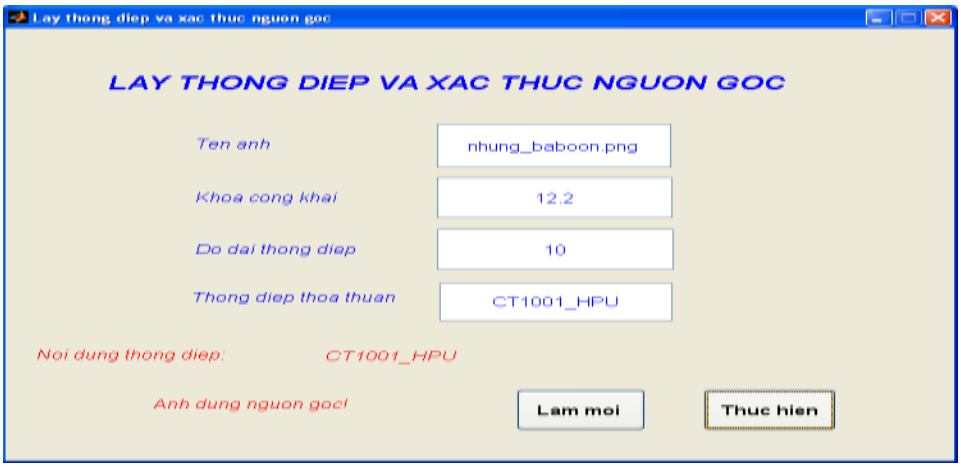


Hình 3.6 Ảnh sau khi A nhúng xâu kí tự

Giả sử sau khi tách được xâu kí tự Z, B sẽ so sánh Z và "CT1001_HPU". Nếu giống thì suy ra ảnh là do A gửi, ngược lại ảnh không phải do A gửi.

Trường hợp 1: Ảnh không bị mạo danh, kết qủa (Hình3.7)

Trường hợp 2 : Ảnh bị mạo danh, hoặc bị tấn công bởi các phép biến đổi hình học (Hình 3.8), và kết quả sau khi tách và so sánh(Hình 3.9)



Hình 3.7 Kết quả khi ảnh không bị tấn công.

Hình 3.8 Ảnh nhúng chữ kí bị làm méo

Hình 3.9 kết quả sau khi tách và so sánh ảnh bị tấn công

3.5 Tổng kết chương

Chương 3 đã giới thiệu một kĩ thuật thủy vân là kĩ thuật RWBH. Kĩ thuật đó đã được áp dụng vào phương pháp xác thực tính toàn vẹn và xác thực nguồn gốc dữ liệu. Từ thuật toán của kĩ thuật thủy vân thuận nghịch và các kết quả thực nghiệm, ta có thể rút ra một số nhận xét sau:

Tính bền vững của thủy vân phụ thuộc vào tham số khoảng cách được sử dụng trong quá trình nhúng. Nếu như khoảng cách giữa các cặp của bảng biểu đồ tăng lên, thủy vân sẽ trở nên bền vững hơn. Điểm bất lợi là khi khoảng cách gia tăng thì khả năng giấu của ảnh giảm. Điều này có thể được cân đối nếu các thuật toán nhúng được phép thực hiện nhiều hơn một lần đi qua các giá trị biểu đồ, miễn là các cặp (a, b) đã được chọn được giữ lại nguyên vẹn.

Thuật toán thủy vân đã được mô tả ở trên có thể cũng được áp dụng cho trường hợp của các hình ảnh màu RGB. Bằng cách này thủy vân sẽ được nhúng ba lần, do đó đạt được cải thiện về tính bền vững.

Dung lượng tối đa của chương trình này là khá thấp, cụ thể là 128 bit, nhưng nó có thể tăng đến 384 bit, nếu sử dụng ba thành phần màu sắc. Nó có lợi thế, tuy nhiên, nó có thể được áp dụng cho hình ảnh rất nhỏ (xuống đến mức 16 x 16), với dung lượng giảm. chương trình có thể cung cấp lên đến 2.304 khóa công khai khác

nhau (256 cho các giá trị khác nhau cho start * 9 giá trị khác nhau cho step) cho hình ảnh màu xám và 12.230.590.464 khóa công khai khác nhau (2304^3) cho hình ảnh màu sắc.

CHƯƠNG 4: CÀI ĐẶT CHƯƠNG TRÌNH

4.1 Môi trường cài đặt

Cài đặt chương trình trên môi trường Matlab 7.5.0.342. Cầu hình máy tính tối thiểu để chạy chương trình: Hệ diều hành Windown XP hoặc các hệ điều hành tương tự, Chip PIII 500 trở lên, Ram từ 128, ổ cứng còn trống 400 Mb.

4.2 Giao diện và các chức năng của chương trình

Chương trình gồm những chức năng sau:

- Nhúng thông điệp.
- Lấy thông điệp.
- Tính PSNR.
- Khôi phục ảnh gốc.
- Thoát.

Hình 4.1 Giao diện chính của chương trình**.**

4.2.1 Nhúng thông điệp

+ Quá trình thực hiện:

- Nhập tên ảnh tiền hành nhúng thủy vân.
- Nhập khóa công khai.
- Nhập thông điệp.
- Nhập tên ảnh sau khi đã nhúng thông điệp.
- Nhấn nút thực hiện để bắt đầu công việc nhúng.

Hình 4.2.a Giao diện chức năng thực hiện nhúng.

+ Để tiến hành nhúng với các ảnh khác ta nhấn vào nút "Lam moi" để bắt đầu.

Hình 4.2.b Giao diện chức năng làm mới.

4.2.2 Lấy thông điệp

+ Quá trình thực hiện:

- Nhập tên ảnh đã được nhúng thủy vân .
- Nhập khóa công khai.
- Nhập độ dài của thông điệp.
- Nhấn nút thực hiện để bắt đầu Lấy.

Hình 4.3.a Giao diện chức năng lấy thông điệp đã nhúng.

+ Để tiến hành lấy thông điệp từ các ảnh khác ta nhấn vào nút "Lam moi" để bắt đầu.

Hình 4.3.b Giao diện chức năng làm mới.

4.2.3 Tính PSNR

+ Quá trình thực hiện:

- Nhập tên ảnh gốc.
- Nhập tên ảnh đã được nhúng thủy vân.
- Nhấn nút thực hiện.

Hình 4.4.a Giao diện chúc năng tính PSNR.

+ Để tiến hành tính PSNR của các cặp ảnh khác nhấn vào nút "Lam moi" để bắt đầu.

Hình 4.4.b Giao diện chúc năng làm mới để tính PSNR của ảnh khác.

4.2.4 Khôi phục ảnh

+ Quá trình khôi phục ảnh:

- Nhập tên ảnh đã được thủy vân.
- Nhập khóa công khai.
- Nhập khóa bí mật.
- Nhập tên ảnh sau khi phục hồi.
- Nhấn nút thực hiện.

Hình 4.5 a Giao diện chức năng khôi phục ảnh gốc

+ Để tiến hành khôi phục ảnh khác nhấn vào nút "Lam moi" để bắt đầu.

Hình 4.5.b Giao diện chức năng làm mới để khôi phục ảnh gốc khác.

KẾT LUẬN

Công nghệ xác thực nói chung và phương pháp xác thực bằng thủy vân số nói riêng hiện nay đang được rất nhiều các nhà khoa học nghiên cứu và phát triển. Nó đang trở thành xu hướng ngày nay khi mà công nghệ số, Internet đang bùng nổ trên toàn cầu.

Đồ án đã trình bày một số khái niệm về xác thực điện tử và một số nét về thủy vân số. Bên cạnh đó đồ án cũng giới thiệu một kĩ thuật thủy vân đó là "kĩ thuật thủy vân thuận nghịch dựa trên biểu đồ histogram của ảnh" và áp dụng nó vào việc xác thực nguồn gốc dữ liệu và xác thực tính toàn vẹn dữ liệu.

Với thuật toán nhúng thủy vân, tính bền vững của thủy vân được nhúng sẽ phụ thuộc vào khoảng cách của các cặp được chọn trên biểu đồ. Từ các kết quả thực nghiệm ta thấy rằng thủy vân được nhúng bởi kĩ thuật thủy vân thuật nghịch dựa trên biểu đồ histogram của ảnh, khi bị tấn công bởi các phép biến đổi hình học, cho thấy rằng chúng bền vững với một số phép biến đổi như xoay 90^0, 180^0, 270^0, nhưng lại bị tác động bởi phép dịch chuyển, co dãn, làm méo ảnh.

Do kiến thức còn hạn chế và thời gian nghiên cứu ngắn nên em chỉ tập trung vào nghiên cứu một kĩ thuật thủy vân đó là kĩ thuật thủy vân thuận nghịch dựa trên bảng biểu đồ của hình ảnh. Trong đồ án này không tránh khỏi những thiếu sót, vì vậy rất mong nhận được sự góp ý của các thầy, cô giáo và các bạn.

TÀI LIỆU THAM KHẢO

[1] Nguyễn Xuân Huy, Trần Quốc Dũng, Giáo trình giấu tin và thuỷ vân ảnh, Trung tâm thông tin tư liệu, TTKHTN - CN 2003

[2] Trần Thị Thu Hà, *Luận văn tốt nghiệp ngành Công nghệ thông tin*, năm 2009

[3] Mặc Như Hiển, Luận *văn tốt nghiệp ngành CNTT*, năm 2009

[4] Phạm Thị Thu Trang, *Luận văn tốt nghiệp ngành CNTT*, năm 2009

[5] Phạm Thị Quỳnh, *Luận văn tốt nghiệp ngành CNTT*, năm 2009

[6] Ingemar Cox, Jeffrey Bloom, Matthew Miller, Ton Kalker, Jessica Fridrich, *Digital Watermarking and Steganography*, Morgan Kaufmann, 2008

[7] Chrysochos E., Fotopoulos V., Skodras A., Xenos M., "Reversible Image Watermarking Based on Histogram Modification", 11th Panhellenic Conference on Informatics with international participation (PCI 2007), Vol. B, pp. 93-104, 18-20 May 2007, Patras, Greece.