

Bảo vệ bản quyền ảnh số và ứng dụng

Học viên: Lâm Mạnh Tuyên
chuyên ngành Hệ thống thông tin,
khoa Công nghệ thông tin
email lamtuyen85@gmail.com

Giáo viên hướng dẫn: PGS.TS. Trịnh Nhật Tiến
Cơ quan công tác: Khoa Công nghệ thông tin – Trường
Đại học Công nghệ - Đại học Quốc gia Hà Nội
Email tientn@vnu.edu.vn

Từ khóa: Watermarking, Intellectual Property Right.

GIỚI THIỆU BÀI TOÁN

Một trong những sự kiện công nghệ lớn của hai thập kỉ trước đó là sự thâm nhập của dữ liệu đa phương tiện vào mọi khía cạnh của đời sống. Dữ liệu số có thể lưu trữ dễ dàng với chất lượng cao, và nó có thể được xử lý trên máy tính một cách dễ dàng. Hơn thế nữa, dữ liệu số có thể được truyền một cách nhanh và rẻ thông qua mạng truyền thông mà không bị suy giảm chất lượng. “Dữ liệu số đa phương tiện” có những lợi thế quan trọng như: bản sao của dữ liệu đa phương tiện (âm thanh số, hình ảnh, tín hiệu video ...) không sai khác với bản gốc và dễ dàng chỉnh sửa, bản sao của dữ liệu đa phương tiện có tính “trung thực” cao (giống y hệt so với bản gốc). Cùng với sự phát triển của Internet quá trình phân phối các sản phẩm kỹ thuật số trở nên dễ dàng và nhanh chóng, nhưng chính điều đó lại làm cho “quyền sở hữu trí tuệ” (IPR- Intellectual Property Right) bị đe dọa hơn bao giờ hết, bởi khả năng sao chép không bị giới hạn. Một trong những giải pháp được đưa ra để bảo vệ “quyền sở hữu trí tuệ” là để hạn chế truy cập dữ liệu bằng cách sử dụng một số kỹ thuật mã hóa. Tuy nhiên kỹ thuật mã hóa không cung cấp phương thức bảo vệ sản phẩm một cách “toàn diện”. Đồng thời, quá trình mã hóa và giải mã cũng gây ra những trở ngại trong quá trình phân phối và xử lý dữ liệu. Có một giải pháp tốt hơn cho vấn đề trên, đó là giấu những “dữ liệu về quyền sở hữu”(ownership data) vào trong các dữ liệu đa phương tiện, sau đó có thể trích xuất những dữ liệu này để chứng minh quyền sở hữu sản phẩm [E9].

Hiện nay, vấn đề bảo vệ quyền tác giả có những tác động tài chính lớn và có tầm quan trọng đặc biệt, do vậy việc xây dựng và ứng dụng các thuật toán để ngăn chặn việc sao chép bất hợp pháp nội dung sản phẩm đa phương tiện là thực sự cần thiết.

Giấu tin nói chung hay thủy vân nói riêng là một lĩnh vực rộng lớn, trong luận văn này đi sâu tìm

hiều một số giải pháp bảo vệ bản quyền dữ liệu đa phương tiện nói chung và bảo vệ bản quyền ảnh số nói riêng bằng kỹ thuật thủy vân số. Từ đó có thể tìm hiểu để lựa chọn phương pháp thủy vân phù hợp với từng ứng dụng cụ thể.

Hiện nay, ảnh số là loại dữ liệu phổ biến và thu hút được nhiều sự quan tâm và nghiên cứu. Cùng với sự phát triển của Internet vấn đề bảo vệ bản quyền ảnh số ngày càng trở nên quan trọng. Thông tin được số hóa có thể dễ dàng sao chép mà không làm giảm chất lượng và hỗ trợ phân phối một cách hiệu quả. Do tính dễ sao chép, phát tán và thậm chí là chỉnh sửa, nên kẻ gian có thể xâm phạm bản quyền của chủ sở hữu thực sự. Việc giải quyết bài toán về bảo vệ quyền là yêu cầu cơ bản của các dịch vụ đa phương tiện hiện tại cũng như trong tương lai.

2. NỘI DUNG LUẬN VĂN

CHƯƠNG 1 – VẤN ĐỀ BẢO VỆ BẢN QUYỀN ẢNH SỐ

- A. Khái niệm và thuộc tính ảnh số.
- B. Biểu diễn ảnh số.
- C. Bản quyền và các quy định.
- D. Bảo vệ bản quyền ảnh số.

Trong chương này, luận văn đề cập tới khái niệm cùng những thuộc tính của ảnh số, vấn đề vi phạm bản quyền, bảo vệ bản quyền. Đồng thời cũng tập trung nghiên cứu các bài toán đặt ra trong bảo vệ bản quyền ảnh số và đề xuất các giải pháp phù hợp để giải quyết từng bài toán.

Bản quyền tác giả liên quan nhiều đến khía cạnh đạo đức, kinh tế. Việc vi phạm bản quyền có thể do hành vi cố tình nhằm mưu lợi hoặc cũng có thể do vô tình, nếu không hiểu biết đầy đủ về bản quyền tác giả, về sở hữu trí tuệ, nhiều người không nhận thức được tác hại của việc vi phạm bản quyền.

Mặc dù đã có nhiều quy định về bảo vệ bản quyền và đã có những chuyển biến tích cực trong việc thực thi quyền tác giả, nhưng bấy nhiêu vẫn còn chưa đủ. Những hành vi xâm hại quyền tác giả diễn ra tràn lan, tinh vi và công khai trước sự xót xa, bất lực của các chủ sở hữu. Đặc biệt với dữ liệu số chẳng hạn như ảnh số với nhiều định dạng thì vấn đề bảo vệ bản quyền lại càng trở nên khó khăn hơn.

Thủy vân không phải là một kỹ thuật mới. Nó là một nhánh của kỹ thuật ẩn giấu tin đã tồn tại vài trăm năm trước. Ẩn giấu tin là một kỹ thuật sử dụng cho việc truyền các thông tin mật. Thông điệp được truyền ở đây là một bí mật mà sự tồn tại của nó là chỉ được biết đến bởi các bên liên quan trong giao tiếp [E5, 6, 7].

Trong giấu tin, một thông điệp bí mật được giấu và môi trường giấu tin không có sự liên quan và nó chỉ nhằm mục đích gửi thông tin bí mật tới những thành viên khác. Trái ngược với điều này, trong thủy vân thông tin được giấu là có liên quan tới môi trường giấu tin theo một nghĩa nào đó.

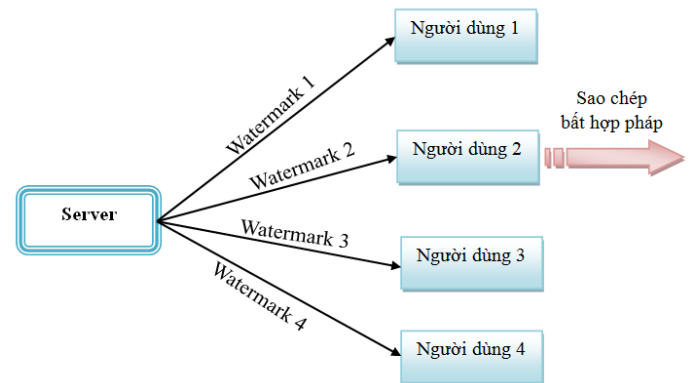
Phương pháp giấu tin nói chung không có tính bền vững, tức thông tin được giấu không thể khôi phục được sau khi xử lý. Trái với giấu tin, thủy vân có tính bền vững chống lại các cuộc tấn công. Ngay cả khi biết sự tồn tại của thủy vân thì kẻ tấn công cũng khó có thể phá hủy thủy vân, thậm chí thuật toán thủy vân được công khai. Chính vì vậy nên thủy vân thường được sử dụng trong một số lĩnh vực

Bảo vệ bản quyền: kỹ thuật thủy vân số có thể được sử dụng để xác định và bảo vệ bản quyền tác giả. Thông tin về bản quyền được nhúng vào trong các dữ liệu đa phương tiện để xác định chủ sở hữu bản quyền.

Chống sao chép: dữ liệu số có thể được nhúng thủy vân để chỉ ra rằng không thể nhân bản bất hợp pháp nội dung. Sau đó, các thiết bị có khả năng sao chép có thể phát hiện ra thủy vân và ngăn chặn sao chép trái phép nội dung.

Theo dõi và lần “vết”: kỹ thuật thủy vân số có thể được sử dụng để theo dõi việc sử dụng nội dung dữ liệu số. Mỗi bản sao của dữ liệu số có thể được nhúng thủy vân đặc biệt và duy nhất để xác thực người dùng có thẩm quyền sử dụng nội dung. Thủy vân này có thể được sử dụng để phát hiện nhân bản bất hợp pháp của nội dung và xác định những người dùng nào đã sao chép nội dung bất hợp pháp. Kỹ

thuật thủy vân được sử dụng để theo dõi được gọi là vân tay (fingerprinting). Hình 1.8 cho thấy cách thủy vân có thể được sử dụng để theo dõi và lần vết.



Hình 1 Kỹ thuật thủy vân áp dụng cho lần vết sử dụng nội dung

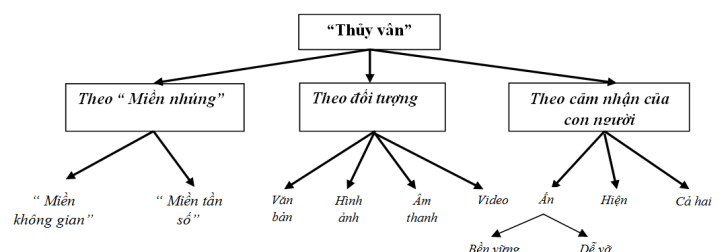
CHƯƠNG 2 – KỸ THUẬT THỦY VÂN

E. Tổng quan về thủy vân: Khái niệm, lịch sử, phân loại, cấu trúc, đặc tính và tiêu chuẩn.

F. Kỹ thuật thủy vân trên ảnh: kỹ thuật thủy vân trên miền không gian và miền tần số.

Chương này giới thiệu tổng quan về kỹ thuật thủy vân và thủy vân trên ảnh số. Các vấn đề cơ bản của kỹ thuật “thủy vân số”. Các yêu cầu và cấu trúc của hệ thống “thủy vân” điển hình được nghiên cứu. Đồng thời xem xét các thuộc tính quan trọng nhất của hệ thống “thủy vân” và đánh giá sơ bộ thông số của các thuật toán thủy vân. Các hình thức tấn công trên ảnh đã thủy vân và các giải pháp khắc phục

Thủy vân và kỹ thuật thủy vân tùy theo từng tiêu chí phân loại mà có thể được chia thành nhiều loại khác nhau. Một trong những tiêu chí để phân loại là “miền nhúng” là nơi chứa thủy vân Ví dụ, thủy vân có thể được thực hiện trong “miền không gian”. Một khả năng khác là thủy vân trong “miền tần số”. Trong hình 2 trình bày khái quát một số loại thủy vân khác nhau.



Hình 2.3: Các loại kỹ thuật thủy vân

Hệ thống thủy vân bao gồm ít nhất hai quy trình sau:

- Quy trình nhúng thủy vân (watermark).
- Quy trình phát hiện / trích xuất thủy vân.

Ngoài ra tùy từng hệ thống thủy vân, còn có thêm một số các quy trình khác. Các quy trình có thể được xem xét một cách riêng biệt, được mô tả trong phần sau.

1). Tạo thủy vân

Thủy vân có thể là một hình ảnh dạng logo hay văn bản với độ dài cho trước. Thủy vân dạng ảnh có khả năng chống chịu trước các phép xử lý ảnh tốt hơn nhiều hơn so với thủy vân dạng ký tự. Thủy vân có thể được biến đổi (bằng mã hoá, chuyển đổi định dạng), trước khi giấu vào ảnh. Các thuật toán nhúng thủy vân dạng logo được gọi là thuật toán thủy vân hợp nhất ảnh (image-fusion). Thủy vân dạng ảnh có lợi ích là dễ dàng nhận biết về mặt trực giác và đưa ra một chứng minh đúng đắn về quyền sở hữu ảnh. Bình thường sẽ có một khoá bí mật K dùng để tăng tính bảo mật cho dữ liệu được nhúng. Do tính bền vững được đảm bảo hơn nên thủy vân dạng ảnh được sử dụng nhiều hơn.

Để tăng thêm tính an toàn và dung lượng, thì thủy vân trước khi nhúng vào ảnh mang có thể được mã hóa hay nén lại. Theo cơ chế này, đầu tiên thủy vân sẽ được nén lại để lượng dữ liệu thủy vân có thể tăng lên, sau đó được mã hóa để tăng tính bảo mật cho thông tin trước khi được giấu vào trong ảnh mang. Tuy nhiên, giải pháp này làm tăng độ phức tạp của bài toán phát hiện thủy vân.

2). Qui trình nhúng thủy vân

Hình 2.4 trình bày và giải thích quá trình nhúng thủy vân cho ảnh tĩnh. Trong đó, Ảnh gốc được kí hiệu bằng I , “thủy vân” được kí hiệu bởi W , hình ảnh chứa “thủy vân” là I_W và K là khóa nhúng. Hàm nhúng E_{MB} có đầu vào là ảnh gốc I , “thủy vân” W và khóa K và tạo ra một ảnh mới có chứa thủy vân mới thể hiện bằng I_W .

Khóa nhúng K là thực sự cần thiết cho việc nâng cao khả năng bảo mật của hệ thống “thủy vân”. Trước quá trình nhúng, hình ảnh gốc có thể được chuyển đổi sang miền tần số hoặc nhúng có thể được thực hiện biến đổi sang miền không gian.

Miền được chọn phụ thuộc vào việc lựa chọn kỹ thuật “thủy vân”. Nếu quá trình nhúng được thực hiện trong miền tần số, biến đổi nghịch đảo được áp dụng để thu được hình ảnh chứa “thủy vân”. Biểu thức toán học cho hàm nhúng có thể được thể hiện như sau:

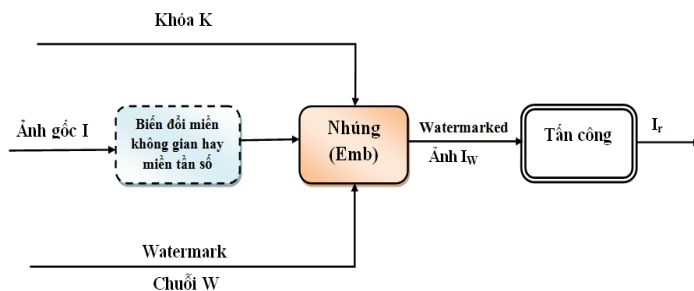
Đối với kỹ thuật biến đổi theo miền không gian:

$$E_{mb}(I, W, K) = I_W \quad (1.1)$$

Đối với kỹ thuật biến đổi theo miền tần số:

$$E_{mb}(f, W, K) = I_W \quad (1.2)$$

Trong đó f là vectơ hệ số cho phép biến đổi.



Hình 2.4 Quy trình nhúng thủy vân

Khi thu được hình ảnh chứa thủy vân và được lưu trữ hoặc truyền qua các kênh truyền thông thì có thể xảy ra các cuộc tấn công (hình ảnh I_r được tạo ra).

3). Trích xuất và tìm kiếm thủy vân

Hình 2.4 trình bày và giải thích quy trình phát hiện/trích xuất ảnh tĩnh. Một hàm phát hiện D_{tc} có đầu vào là hình ảnh I_r có chức năng xác định quyền sở hữu sản phẩm. Các hình ảnh I_r có thể chứa “thủy vân” hoặc không chứa “thủy vân”. Trong trường hợp tổng quát, hình ảnh có thể bị biến đổi. Hàm phát hiện có khả năng khôi phục “thủy vân” W_e từ bức ảnh hoặc kiểm tra có sự hiện diện của “thủy vân” W trong bức ảnh đã cho I_r hay không. Trong quá trình này hình ảnh gốc I cũng có thể được yêu cầu, phụ thuộc vào lược đồ “thủy vân” được lựa chọn.

Biểu thức toán học cho thủ tục trích xuất “mù” (blind extraction – trích xuất không sử dụng ảnh

gốc I) cụ thể như sau:

$$D_{tc}(I_r, K) = W \quad (1.3)$$

Biểu thức toán học cho thủ tục trích xuất “không mù” (*non-blind extraction* – trích xuất có sử dụng ảnh gốc I) cụ thể như sau:

$$D_{tc}(I_r, I, K) = W_e \quad (1.4)$$

Thuật toán phát hiện thủy vân “mù” có đầu ra là một giá trị nhị phân cho biết có sự hiện diện của “thủy vân” W hay không.

Trong lược đồ tách thủy vân phải được trích xuất một cách chính xác, nguyên mẫu. Lược đồ trích xuất “thủy vân” có thể chứng minh quyền sở hữu, trong khi lược đồ phát hiện “thủy vân” chỉ có thể xác nhận có sự hiện diện của thủy vân hay không.

Kỹ thuật thủy vân trên miền tần số sử dụng các phương pháp biến đổi như Cosine rời rạc, biến đổi Fourier rời rạc, biến đổi sóng con (wavelet)... để chuyển miền không gian ảnh sang miền tần số. Thủy vân sẽ được nhúng trong miền tần số của ảnh theo kỹ thuật trải phổ trong truyền thông, kỹ thuật này được đề xuất lần đầu tiên bởi Cox cùng cộng sự trong bài báo về "Thủy vân dựa trên trải phổ bảo vệ cho dữ liệu đa phương tiện" [E22], và đã được trích dẫn trong nhiều tài liệu (34.200 lần trích dẫn tính đến tháng 12 năm 2010). Đây là kỹ thuật phổ biến nhất với nhiều thuật toán được đề xuất và là phương pháp tốt giải quyết vấn đề về tính bền vững của thủy vân.

Ba công thức khác nhau được đề xuất bởi Cox cùng cộng sự cho việc nhúng thủy vân thường được sử dụng là:

$$f'(i) = f(i)(1 + \alpha w_i)$$

$$f'(i) = f(i) + \alpha w_i$$

$$f'(i) = f(i)e^{\alpha w_i}$$

Trong đó, $i = 1 \dots N$, thủy vân là một dãy số w_i độ dài N được nhúng vào một tập con các hệ số thích hợp các hệ số $f_1, f_2, \dots, f_N$ trong miền tần số của ảnh gốc. f' là giá trị các hệ số của ảnh mang chứa kết quả sau khi thay đổi để chứa thủy vân. α là hệ số năng lượng của thủy vân, hệ số này quyết định tính bền vững và vô hình của thủy vân.

Quá trình trích xuất thủy vân được tính bởi công thức sau:

$$w_i^* = \frac{f^*(i) - f(i)}{\alpha \cdot f(i)}$$

Trong đó, w^* là thủy vân tách được từ ảnh f^* đã trải qua các phép xử lý ảnh. Ta so sánh với thủy vân ban đầu bằng cách sử dụng tương quan chuẩn của dãy số làm thước đo

$$\delta = \frac{w^* \cdot w}{\|w\| \cdot \|w^*\|}$$

Nếu δ dương và gần 1 thì có thể kết luận ảnh ban đầu đã được nhúng thủy vân w . Một ngưỡng τ có thể được thiết lập hoặc bằng sự quan sát tương quan giữa các dãy ngẫu nhiên hoặc bằng cách phân tích. Một ngưỡng có thể chấp nhận được là

$$\tau = \frac{\alpha}{S \cdot N} \sum |f'|$$

Với S là độ lệch chuẩn (Độ lệch chuẩn đo tính biến động của giá trị mang tính thống kê. Nó cho thấy sự chênh lệch về giá trị của từng thời điểm giá so với giá trung bình, thường với ảnh số có giá trị là 2 hoặc 3). Hệ số năng lượng thủy vân α không nhất thiết phải là hằng số trên toàn bộ ảnh mà có thể biến thiên theo tính chất địa phương của tín hiệu. Ta có thể áp dụng mô hình HVS (*Human Visual System*) với các tính chất như hiệu ứng mặt nạ... để có thể tìm các hệ số thích hợp cho từng vùng ảnh, do đó có thể tăng thêm lượng tin được giấu và tăng chất lượng của phương pháp.

CHƯƠNG 3 - MỘT SỐ ỨNG DỤNG TRONG BẢO VỆ BẢN QUYỀN

G. Hệ thống xác thực trên máy ảnh kỹ thuật số.

H. Bảo vệ nhãn hiệu sản phẩm.

I. Một số ứng dụng khác của thủy vân

Thủy vân ảnh số được ứng dụng rộng rãi trong nhiều lĩnh vực. Tùy thuộc vào yêu cầu của từng ứng dụng cụ thể mà kỹ thuật thủy vân trên ảnh số khác nhau được sử dụng. Trong chương này sẽ tập trung vào ứng dụng các kỹ thuật thủy vân trên ảnh số trong một số các ứng dụng thực tế như: tăng cường tính phân lý cho ảnh số, bảo vệ bản nhãn hiệu sản

phẩm, phòng chống giả mạo chứng minh nhân dân/hộ chiếu cùng với một số ứng dụng khác.

Hình ảnh là một trong những công cụ hỗ trợ đắc lực cho các cơ quan thực thi pháp luật và có một vai trò pháp lý nhất định. Trước đây, hình ảnh thường được chụp bằng máy ảnh cơ sử dụng hệ thống cơ khí để điều khiển và việc ghi nhận hình ảnh dựa vào tác dụng của ánh sáng với hóa chất trên phim. Và chúng ta chỉ nhìn thấy kết quả cuối cùng sau khi cuộn phim đã được tráng rọi xong. Vì vậy mà việc chỉnh sửa hình ảnh là rất khó và cơ quan luật pháp xem hình ảnh về những cảnh phạm tội, cảnh về nạn nhân, hiện trường được chụp bằng máy ảnh cơ như bằng chứng vật lý hỗ trợ điều tra và kết tội [E30].

Tuy nhiên, với sự tiến bộ của khoa học công nghệ máy ảnh kỹ thuật số ra đời với nhiều ưu điểm và cũng tạo ra nhiều thay đổi. Hiện nay, máy ảnh số ngày càng trở nên phổ biến và được nhiều người sử dụng với chất lượng hình ảnh ngày càng được nâng cao. Đồng thời, với sự phát triển của Internet hình ảnh số có thể dễ dàng chia sẻ và tạo sự dễ dàng trong truy cập cơ sở dữ liệu. Mặt khác, nhờ vào các chương trình chỉnh sửa ảnh việc chỉnh sửa ảnh trở nên rất dễ dàng ngay cả đối với người nghiệp dư, tạo ra những bức giả mạo "hoàn hảo" tới mức "khó" có thể phân biệt được đâu là hình ảnh đã được chỉnh sửa

Nhãn hiệu hàng hóa là dấu hiệu nhận biết và làm nên giá trị thương hiệu. Nhãn hiệu là những dấu hiệu để phân biệt hàng hoá, dịch vụ của các cơ sở sản xuất, kinh doanh khác nhau.

Nhờ có nhãn hiệu nên người dùng có thể phân biệt hàng hoá, dịch vụ của chủ sở hữu nhãn hiệu với hàng hoá, dịch vụ của chủ thể khác. Tức là nhãn hiệu được tạo thành từ một hoặc một số yếu tố dễ nhận biết, dễ ghi nhớ hoặc từ nhiều yếu tố kết hợp thành một tổng thể dễ nhận biết, dễ ghi nhớ và dễ kiểm tra.

Nhãn hiệu gồm: Nhãn hiệu gắn vào sản phẩm, bao bì sản phẩm để phân biệt sản phẩm cùng loại của các cơ sở sản xuất khác nhau. Nhãn hiệu dịch vụ gắn vào phương tiện dịch vụ để phân biệt dịch vụ cùng loại của các cơ sở kinh doanh, dịch vụ khác nhau. Chẳng hạn như các quảng cáo trên mạng.

Bảo vệ nhãn hiệu sản phẩm chống hàng giả, hàng nhái lậu đã và đang là một thách thức lớn trong công cuộc đấu tranh bảo vệ thương hiệu bảo

vệ người tiêu dùng. Sự gia tăng của sự phức tạp của chuỗi cung ứng trong nền kinh tế toàn cầu ngày nay làm cho việc chứng thực nguồn gốc sản phẩm ngày càng khó khăn. Đồng thời, các sản phẩm từ thuốc tây, quần áo, điện thoại di động, mỹ phẩm đến cả thực phẩm ... đều bị làm giả, làm nhái với trình độ ngày càng tinh vi khiến người tiêu dùng khó phân biệt. Nạn hàng giả, hàng nhái đang vô cùng nhức nhối gây ra những vấn đề đặc biệt nghiêm trọng.

Bài toán cấp thiết đặt ra đó là người dùng làm thế nào để nhận diện được xuất xứ các mặt hàng trên thị trường, phân biệt được sản phẩm thật và giả.

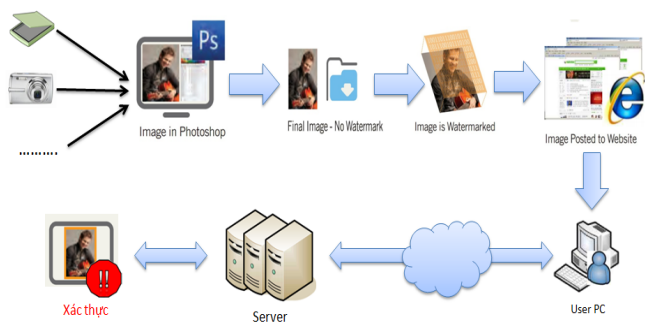
Có rất nhiều giải pháp đã được áp dụng và một trong những giải pháp thường được những nhà sản xuất sản phẩm sử dụng đó là sử dụng bao bì có những đặc trưng chống sao chép, giả mạo.

Xác thực trực tuyến

Với sự phát triển của mạng Internet, các loại điện thoại thông minh (Smart Phone) và cùng với sự phát triển của kỹ thuật thủy văn số làm cho quá trình chứng thực sản phẩm hàng hóa trở nên dễ dàng hơn, và tạo ra một chiều hướng mới cho việc bảo vệ nhãn hiệu quảng cáo và bao bì sản phẩm.

Bảo vệ nhãn hiệu quảng cáo.

Quảng bá thương hiệu sản phẩm là một bước quan trọng trong kinh doanh. Trong thời đại công nghệ số ngày nay, để quảng cáo sản phẩm nhà sản xuất, người kinh doanh thường tạo một bức ảnh về sản phẩm của mình và đưa nó lên nhiều trang web để quảng bá cho sản phẩm của mình. Để biết sản phẩm do đơn vị nào sản xuất và quảng cáo thì một thông cáo bản quyền "© 2011 Corporation X" thường được sử dụng. Tuy nhiên, kẻ xấu có thể làm sai lệch thông tin quảng cáo bằng việc chỉnh sửa bức ảnh quảng cáo hay thay đổi thông cáo bản quyền. Để giải quyết vấn đề này một kỹ thuật kết hợp thủy văn ẩn và thủy văn hiện được sử dụng, trong đó thủy văn hiện dùng để xác định nguồn gốc sản phẩm và thủy văn ẩn được sử dụng để xác thực tính tin cậy của thông tin quảng cáo thông qua việc xác thực trực tuyến theo như sơ đồ trong hình 3.



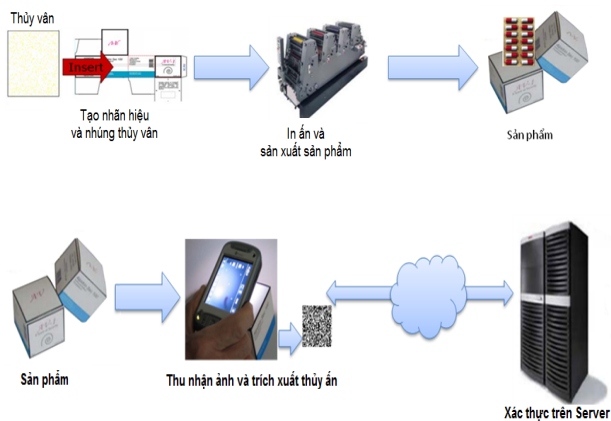
Hình 3 Sơ đồ bảo vệ hình ảnh quảng cáo trực tuyến

Theo sơ đồ trên, ảnh qua quá trình thu nhận ảnh từ các thiết bị như máy quét, máy ảnh số... sẽ được chỉnh sửa tạo ra bức ảnh cho sản phẩm cần quảng cáo. Sau đó thủy vân sẽ được nhúng trước khi đăng tải bức ảnh trên các trang web. Khi người dùng quan tâm tới một sản phẩm muốn xác thực thông tin về quảng cáo sẽ gửi yêu cầu xác thực thông tin trên server của nhà sản xuất, hay trung tâm kiểm soát việc đăng kí nhãn hiệu. Server sẽ tiến hành trích xuất thủy vân đối sánh và trả về thông tin cho người sử dụng.

Bảo vệ nhãn hiệu sản phẩm

Người dùng cuối có thể kiểm tra tính xác thực của sản phẩm mà họ muốn mua và các nhà sản xuất theo dõi và lần vết dựa trên các đặc trưng nhãn hiệu sản phẩm trên mạng hay đơn giản hơn thông qua một thiết bị hiện đang được sử dụng phổ biến là điện thoại di động.

Công nghệ này bao gồm hai giai đoạn chính là tạo bao bì sản phẩm có chứa thủy vân và xử lý yêu cầu xác thực của người dùng được minh họa như hình dưới đây:



Hình 4 Quy trình tạo và xác thực thủy vân trên sản phẩm

Người tiêu dùng có thể dễ dàng kiểm tra tính xác thực của một sản phẩm thông qua ảnh chụp nhãn hiệu sản phẩm và gửi nó qua mạng hoặc e-mail trực tiếp từ điện thoại di động hay từ máy tính và nhận được kết quả kiểm tra.

Dữ liệu thủy vân được nhúng trong ảnh dễ dàng được trích xuất và xác thực khi có yêu cầu của người dùng người tiêu dùng. Tuy nhiên một vấn đề đặt ra là làm thế nào để đảm bảo tính bí mật của thủy vân, tức là chỉ nhà sản xuất mới có thể giải mã và xác thực thông tin về thủy vân. Phương pháp mã hóa thông thường (RSA, Elgamal...) có thể giải quyết được vấn đề trên nhưng lại gặp phải vấn đề về tỷ lệ sai dương do quá trình in và quét ảnh làm cho việc giải mã gặp nhiều khó khăn. Do vậy cần có một giải pháp sao cho vừa đảm bảo được tính bí mật của thủy vân lại vừa có thể đảm bảo tính bí mật, tức là có thể trích xuất thủy vân khi tỷ lệ lỗi bit cao.

Nghiên cứu vấn đề bảo vệ bản quyền ảnh số nói chung và vấn đề áp dụng kỹ thuật thủy vân cho ảnh số nói riêng, không chỉ hỗ trợ cho những ứng dụng đã nêu mà còn được ứng dụng trong nhiều lĩnh vực khác như bảo vệ dữ liệu y sinh học. Giấu tin trong ảnh với việc kết hợp thủy vân và nhiều kỹ thuật như trộn ảnh, hàm băm, mã hóa...góp phần nâng cao mức độ an toàn cho thông tin được giấu.

Liên kết thẻ vật lý, ảnh số và chip với kỹ thuật thủy vân

Một thẻ thông minh khi đến tay người sử dụng phải trải qua nhiều công đoạn với sự tham gia của nhiều nhân tố. Trước hết là quá trình sản xuất chip tại các nhà sản xuất. Tiếp theo là việc phát triển phần mềm tương ứng với các ứng dụng của sản phẩm tại các nhà sản xuất thẻ trước khi đến tay người sử dụng, thẻ được cá thể hóa tại các nhà cung cấp dịch vụ. Như vậy, khi xem xét vấn đề bảo mật của thẻ thông minh chúng ta phải xem xét đến tất cả các công đoạn, cũng như các nhân tố tham gia và môi trường của từng công đoạn.

Tần công hoàn toàn có thể thực hiện trên một chiếc thẻ được đánh giá là có độ an toàn cao khi người sử dụng không tự bảo vệ thẻ của mình (ví dụ làm lộ mã PIN), hay khi nhà cung cấp dịch vụ không đảm bảo độ an toàn các thông tin liên quan đến người sử dụng mà họ quản lý (ví dụ làm lộ CSDL của khách hàng). Ngay cả khi người sử dụng

và nhà cung cấp dịch vụ đã thắt chặt công tác bảo mật dữ liệu, thẻ thông minh vẫn có thể bị tấn công khi bản thân chiếc thẻ (phần cứng và phần mềm) không được bảo vệ. Như vậy, thẻ thông minh chỉ thực sự được bảo vệ khi mọi mắt xích trong vòng đời (life cycle) của thẻ đạt đến độ an toàn nhất định.

Tiến bộ của khoa học kỹ thuật làm tăng khả năng chứa dữ liệu trên thẻ ID. Một con chip tích hợp trong thẻ điện tử có thể thêm dữ liệu bổ sung thêm nhiều tính năng cho một thẻ điện tử, với các phương pháp như ký số, mã hóa có thể tăng cường bảo mật, chống lại thay đổi thông tin trên thẻ. Với các chip sử dụng các thuật toán bảo mật phức tạp có thể đảm bảo an toàn truy cập và tính toàn vẹn dữ liệu, tuy vậy công nghệ này không có nghĩa là có thể chống giả mạo hoàn toàn.

Với những kỹ thuật tinh vi, kẻ giả mạo có thể tấn công mô hình bảo mật của chip thông qua việc kết hợp các thành phần từ một số thẻ hợp lệ để tạo các tài liệu thẻ căn cước giả hay thay đổi các dữ liệu chứa trong chip. Một dạng tấn công khác là tác động tới chip và đầu đọc nhằm "phá vỡ" bảo mật các chip trên thẻ, hoặc vô hiệu hóa đầu đọc thẻ chip. Bởi vì chip là những thành phần bảo mật động và như vậy có một tỷ lệ thất bại thời gian thực, việc cố ý vô hiệu hóa thẻ hay đầu đọc làm sai lệch quyền hạn hợp pháp của thẻ hay chức năng của đầu đọc thẻ tạo thêm các quyền cho chủ thẻ không hợp lệ. Ví dụ như việc dùng tia laser chiếu vào mạch để mạch hoạt động không bình thường. Qua việc xử lý những kết quả không bình thường đó kẻ gian có thể dò được một số thông tin bí mật. Một mối đe dọa thực tế khác với các tổ chức phát hành thẻ và việc kiểm tra thẻ đó là, tội phạm có thể dễ dàng có được một thẻ trắng với một con chip hoàn chỉnh. Với thẻ trắng này cùng với các thiết bị đọc ghi thông tin chứa trên chip, kẻ giả mạo có thể dễ dàng kết hợp để tạo ra các thẻ hợp lệ (ví dụ từ các thẻ lấy cắp).

Như vậy, để đảm bảo an toàn trong quá trình sản xuất cũng như sử dụng thẻ thông minh thì không thể chỉ sử dụng một kỹ thuật, một phương pháp đơn lẻ nào mà đòi hỏi phải tạo lập nhiều lớp bảo vệ khác nhau cho thẻ thông minh (bảo vệ theo chiều sâu). Trong luận văn này tập trung tìm hiểu một lớp bảo vệ cho thẻ thông minh sử dụng kỹ thuật thủy vân nhằm góp phần hỗ trợ và nâng cao mức bảo mật tổng thể cho các loại thẻ thông minh có

hình ảnh của chủ sở hữu thẻ như chứng minh thư số, thẻ hộ chiếu...

Kỹ thuật thủy vân số có khả năng tạo ra một lớp bảo mật có hiệu quả với thuộc tính ẩn. Đồng thời đây cũng là kỹ thuật được sử dụng phổ biến với chi phí rẻ, được nghiên cứu và phát triển nhiều trong những năm qua nhằm mục đích chống giả mạo và bảo vệ bản quyền. Đặc trưng ẩn của thủy vân số có thể làm giảm tác động của các cuộc tấn công đã được thảo luận, khi sử dụng kết hợp với các tính năng bảo mật trên chip tạo ra loại thẻ thông minh có độ an toàn cao. Kỹ thuật thủy vân số cùng với thuộc tính ẩn tạo thành một cấu trúc bảo mật cao, kết hợp cả văn bản, đồ họa cùng với dữ liệu số được lưu trữ trên chip. Với phương pháp tiếp cận này giúp tăng cường tính toàn vẹn và bảo mật tổng thể của một tài liệu.

Kỹ thuật thủy vân số có thể sử dụng kỹ thuật trải phổ để ẩn các dữ liệu số trong thông số về độ chói của hình ảnh. Quá trình nhúng thủy vân có thể sử dụng kết hợp các kỹ thuật sửa lỗi và phát hiện lỗi để tăng thêm tính bền vững và tin cậy cho quá trình trích xuất thủy vân. Sau đó, thủy vân được nhúng dưới dạng chuỗi giả ngẫu nhiên giống như nhiễu theo kỹ thuật trải phổ.

Quá trình phát hiện bắt đầu bằng cách cải thiện tỷ lệ tín hiệu nhiễu (SNR-signal-to-noise ratio) của dữ liệu được nhúng trong ảnh số dựa trên các dữ liệu đặc biệt được nhúng trong hình ảnh. Sau khi đồng bộ hóa dựa trên các dữ liệu số được nhúng, hình ảnh được lấy mẫu để thu thập các giả ngẫu nhiên đã được nhúng. Từ chuỗi giả ngẫu nhiên thu được, thủy vân được giải mã và bất kỳ lỗi nào được phát hiện sẽ được sửa chữa. Quá trình phát hiện thủy vân không yêu cầu các hình ảnh ban đầu, được gọi là trích xuất mù. Chuỗi trải phổ giả ngẫu nhiên được điều khiển sử dụng một khóa bí mật. Các khóa khác nhau tùy theo tổ chức phát hành thẻ, tài liệu và quá trình đọc thẻ sử dụng một hệ thống quản lý khóa an toàn để cấp quyền truy cập. Chuỗi giả ngẫu nhiên làm cho thủy vân mạnh mẽ hơn trong việc chống lại các cuộc tấn công.

Quy trình tạo liên kết giữa thẻ vật lý, hình ảnh số chủ sở hữu thẻ và chip với kỹ thuật thủy vân. Trong đó: Các liên kết được tạo ra thông qua quá trình đồng bộ ảnh số và chip: sử dụng thủy vân để vờ nhúng số xê-ri của chip (hay thông tin định danh duy nhất của chip) vào trong hình ảnh được lưu trữ

trên chip để đảm bảo rằng hình ảnh và chip là nguyên mẫu không bị chỉnh sửa hay thay thế. Sau đó quá trình đồng bộ chip và ảnh in trên thẻ được thực hiện thông qua thủy vân bền vững nhúng số xê-ri của chip (hay thông tin định danh duy nhất của chip) vào ảnh in trên thẻ tạo ra liên kết thực sự có hiệu quả giữa chip với hình ảnh cho phép phát hiện ra khi ảnh bị thay thế. Cuối cùng đồng bộ ảnh in và thẻ vật lý được thực hiện: Những dữ liệu quan trọng từ thẻ vật lý vào trong ảnh in cho phép phát hiện ra ảnh và dữ liệu bị thay thế.

Theo nghiên cứu của tổ chức Digimarc (một trong những tổ chức đi đầu trong việc nghiên cứu các ứng dụng về thủy vân) khuyến cáo kết hợp thông tin mô tả ảnh, bản tóm tắt các thông tin ghi trên thẻ, chuỗi số xê-ri trên chip vật lý nên theo cùng cấu trúc có độ dài 96 bit để việc xác thực thực hiện nhanh và dễ dàng hơn

Kỹ thuật thủy vân bảo vệ bản quyền bản đồ số

Để thực hiện thủy vân trên bản đồ vectơ số cần chú ý tới các đặc điểm riêng có của loại dữ liệu này. Dữ liệu ảnh vectơ là sự biểu diễn thông thường không gian dữ liệu, tập hợp dữ liệu và thêm vào một vài dữ liệu được sử dụng như chỉ số, sự mô tả. Mô tả không gian dữ liệu, các vùng địa lý của bản đồ đối tượng mô tả đối tượng địa lý trong thế giới thực và luôn nắm lấy ba yếu tố địa lý cơ bản là điểm, đường và đa giác. Tất cả đối tượng bản đồ này đều được định dạng bởi các đỉnh có thứ tự. Không gian dữ liệu là một chuỗi các tọa độ của những đỉnh cơ sở này trong một hệ thống địa lý.

Tập hợp dữ liệu mô tả thuộc tính của đối tượng bản đồ như tên, loại, và một vài thông tin khác. Hiển nhiên, những thông tin được ghi lại bởi tập hợp dữ liệu rất quan trọng và không thể thay đổi tùy tiện, tương tự cho những dữ liệu được thêm vào đã kể ra ở trên. Không gian để thủy vân được quy định bởi không gian dữ liệu như tọa độ của các đỉnh. Một bản đồ vectơ bất kỳ đều có một dung sai rõ ràng, chúng đưa ra độ rộng tối đa cho sự làm méo tọa độ cho phép. Việc thay đổi giá trị tọa độ đứt khoát phải nhỏ hơn dung sai thì sẽ không làm suy giảm đi chất lượng của bản đồ.

Có nhiều thuật toán thủy vân đã được đề xuất và ý tưởng chung của thuật toán này là trích chọn tập dãy các đỉnh bản đồ vector, sau đó dãy này được biến đổi sang miền tần số bằng các phép biến đổi

DCT, DFT... Thông thường với bản đồ số biến đổi DFT thường được sử dụng do tính bền vững của nó với các phép biến đổi hình học. Sau khi thực hiện biến đổi DFT. Thủy vân có thể thực hiện trên phổ pha DFT bằng cách chia các pha của DFT theo kích thước bước lượng tử hóa. Thủy vân cũng có thể thực hiện trên phổ biên độ DFT bằng cách chia dãy các hệ số L sau khi đã biến đổi DCT hay DFT thành các dãy con có kích thước L_i và với mỗi dãy con L_i sẽ mang không quá một bit thông tin. Việc chọn các dãy con L_i để mang tin phụ vào kích thước của bản đồ và lượng thông tin thủy vân cần thiết sao cho lượng tin giấu dần trải trên toàn bản đồ.

KẾT LUẬN

Bảo vệ bản quyền ảnh số nói chung và bảo vệ nhãn hiệu sản phẩm nói riêng là vấn đề rất được quan tâm bởi không chỉ nhà sản xuất sản phẩm mà còn bởi cả người tiêu dùng. Đặc biệt, công nghệ ngày càng phát triển và các giao dịch thương mại điện tử ngày càng được áp dụng nhiều hơn, thì vấn đề bảo vệ bản quyền càng trở nên cấp thiết. Kỹ thuật thủy vân số là một trong những giải pháp có nhiều triển vọng trong việc giải quyết vấn đề quyền sở hữu, bảo vệ dữ liệu số khỏi sao chép bất hợp pháp và hỗ trợ lần vết thông tin.

Luận văn tập trung tìm hiểu các đặc trưng ảnh số và những vấn đề trong bảo vệ bản quyền ảnh số. Đồng thời, luận văn cũng nghiên cứu, tìm hiểu và đánh giá một số kỹ thuật thủy vân trên ảnh, tập trung chủ yếu vào các kỹ thuật thủy vân bền vững, tính ẩn và cho phép trích xuất thủy vân mà không cần tới ảnh gốc. Các kỹ thuật thủy vân trong miền không gian và trong miền tần số dựa các phép biến đổi DCT, DFT, DWT và lược đồ thủy vân kết hợp. Từ đó làm cơ sở để ứng dụng giải quyết một số vấn đề trong thực tiễn như: nâng cao tính pháp lý cho ảnh số, bảo vệ nhãn hiệu sản phẩm, tăng tính bảo mật cho thẻ thông minh và bảo vệ bản quyền bản đồ số. Bên cạnh đó, việc tìm hiểu kỹ thuật thủy vân trên ảnh số cũng hỗ trợ làm tăng mức độ an toàn trong lĩnh vực giấu tin bằng việc kết hợp nhiều kỹ thuật như trộn ảnh, mã hóa...bù đắp cho những hạn chế của kỹ thuật thủy vân.

Luận văn đã đạt được các kết quả chính sau:

1). Nghiên cứu tài liệu để tổng hợp lại các vấn đề:

Thực trạng vấn đề bảo vệ bản quyền ảnh số.

Kỹ thuật thủy vân trên ảnh số.

Một số ứng dụng trong bảo vệ bản quyền.

2). Xây dựng thử nghiệm chương trình với các chức năng sau:

Nhúng thủy vân vào một bức ảnh số.

Tách thủy vân trong ảnh đã được thủy vân.

Kiểm tra xác thực thông tin của bức ảnh.

Hỗ trợ giấu tin với nhiều định dạng khác nhau: văn bản, âm thanh, hình ảnh.

Hướng phát triển luận văn: nghiên cứu và xây dựng chương trình thủy vân trên tất cả định dạng ảnh đặc biệt là ảnh 3D. Đồng thời, tiếp tục nghiên cứu các phương pháp bảo vệ bản quyền trên nhiều lĩnh vực khác như văn bản, thẻ web, audio, video.

TÀI LIỆU THAM KHẢO

- [1] Trịnh Nhật Tiến, *Giáo trình An toàn dữ liệu*, 2008.
- [2] Nguyễn Quang Hoan, *Giáo trình xử lý ảnh*, Học viện bưu chính viễn thông, 2006.
- [3] Paul a. Blythe, *Biometric Authentication System For Secure Digital Cameras*, 2006
- [4] Josef Pauli, Natasa Terijza, *Robust Digital Image Watermarking Algorithms for Copyright Protection*, 2006.
- [5] VIKAS SAXENA, *A Novel Watermarking Scheme for JPEG Images*, 2007
- [6] Chaw Seeng Wo, *Digital Image Watermark Methods for Copyright Protection and Authentication*, March 2007 at Queensland University of Technology
- [7] V. Venkata Rama Prasad and Rama Kurupati, *Secure Image Watermarking in Frequency Domain using Arnold Scrambling and Filtering*, pp. 236–244 Volume3 2010.
- [8] Xavier Leroy, *Smart Card Security From a Programing Language and Static Analysis Perspective*, 2008
- [9] Card Logix, EvoLis, SCM Corporate, *Smart Card and Security Basics*, 2010
- [10] Yasser Dakroury, Ismail Abd El-ghafar and Ashraf Tammam, *Protecting GIS Data Using Cryptography and Digital Watermarking*, International Journal of Computer Science and Network Security, VOL.10 No.1, 2010