Equipment with new general education program, Volume 1, Issue 306(February 2024)
ISSN 1859 - 0810

Bảo vệ bản quyền và sự toàn vẹn ảnh số bằng kỹ thuật thuỷ vân thuận nghịch sử dụng phép biến đổi mở rộng hiệu

Tô Thị Mai Phương*, Đỗ Văn Hùng**

**ThS. Trường Cao đẳng Nghề Yên Bái, **ThS. Trường Cao đẳng Yên Bái*
Received: 10/01/2024; Accepted: 18/01/2024; Published: 22/01/2024

Abstract: *This article presents some digital watermarking schemes based on transformations that extend the effect of protecting copyright and digital image integrity using reversible watermarking techniques. This is a new research direction in the world, with scientific significance and practical application.*

Keywords: *Steganography and watermarking techniques based on effective scaling transformation*

1. Đặt vấn đề

Ngày nay, cùng với sự phát triển mạnh mẽ của công nghệ thông tin và truyền thông, mạng Internet đã trở thành một trong các phương tiện truyền tải, chia sẻ thông tin, tài liệu một cách thuận tiện, hiệu quả. Tuy nhiên, vấn nạn sao chép và sử dụng không hợp pháp dữ liệu số ngày một tăng. Từ đó, cần thiết phải có các giải pháp chống sao chép để hạn chế việc vi phạm bản quyền các sản phẩm dữ liệu số. Một trong những giải pháp hữu hiệu để bảo vệ bản quyền là kỹ thuật thủy vân số. Bài báo trình bày kỹ thuật giấu tin và thủy vân dựa trên phép biến đổi mở rộng hiệu. Đây là hướng nghiên cứu mới trên thế giới, có ý nghĩa khoa học và ứng dụng thực tiễn.

2. Nội dung nghiên cứu

2.1.Sơ lược về khái niệm kỹ thuật thủy vân số

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

2.2 Thuỷ vân thuận nghịch sử dụng phép biến đổi mở rộng hiệu

2.2.1 Bài toán về thủy vân bảo vệ bản quyền tác giả

Một thông tin nào đó mang ý nghĩa bản quyền được sở hữu của tác giả được gọi là thủy vân. Thông tin này sẽ được giấu vào ảnh I bằng thuật toán nhúng thủy vân. Ảnh sau khi giấu I' sẽ được phân phối trong môi trường. Trong quá trình đó có thể gặp các phép tấn công như: Nén JPEG, thay đổi kích thước… ảnh I' có thể bị biến đổi thành I*. Hãy xác định bản quyền tác giả đối với ảnh I*.

2.2.2. Phân tích và thiết kế hệ thống.

Bài toán trên được giải quyết bằng phương pháp thủy vân số thuận nghịch. Quá trình bảo vệ bản quyền và tách thủy vân để thu được hình ảnh gốc ban đầu được tiến hành qua các bước:

+ Chủ sở hữu bức ảnh số sẽ gửi các thông tin bí mật của mình cho hệ thống để tạo thủy vân và yêu cầu hệ thống nhúng thủy vân vào ảnh gốc của mình.

+ Hệ thống thủy vân tiến hành tạo và nhúng thủy vân cho chủ sở hữu. Sau khi nhúng thông tin, hệ thống sẽ gửi lại chủ sở hữu cả ảnh gốc và ảnh đã nhúng.

+ Khi có tranh chấp về vấn đề bản quyền, chủ sở hữu ảnh phải cung cấp ảnh có nghi ngờ sao chép trái phép cho hệ thống thủy vân để xác định nguồn gốc ảnh. Hệ thống thủy vân sẽ tách thủy vân từ ảnh nghi ngờ này. Sau đó, so sánh thủy vân nhận được với thủy vân mà chủ sở hữu cung cấp. Nếu hai thủy vân do hệ thống trích ra và thủy vân do chủ sở hữu cung cấp trùng nhau thì người này đúng là chủ sở hữu của tác phẩm, ngược lại chủ sở hữu trên là giả mạo và đã vi phạm sao chép sản phẩm không hợp pháp hoặc đã sửa đổi sản phẩm gốc thành tác phẩm của mình (nhái sản phẩm). Quá trình trích rút thông tin sẽ không yêu cầu chủ sở hữu cung cấp ảnh gốc, thêm nữa, sau khi trích thông tin ta thu được ảnh có các đặc tính giống như ảnh gốc.

Chức năng nhận ảnh gốc: Các điểm ảnh trong tệp ảnh gốc gồm 3 thành phần màu: G,R và B. Ứng dụng duyệt qua toàn bộ ảnh gốc để nhận các điểm ảnh.

Chức năng nhúng thủy vân

Thủy vân là chuỗi ký tự/file văn bản: Chứa các thông tin bản quyền như tên tác giả, số chứng minh

thư, mã số bản quyền… Khi nhúng mỗi ký tự này sẽ chuyển thành mã ASCII tương ứng, sau đó đổi mã này thành chuỗi bít để đưa vào ảnh cần nhúng. Nếu so với ảnh đa cấp xám thì mỗi ký tự tương đương với một điểm ảnh. Nếu so với ảnh 24 bít mầu thì mỗi điểm ảnh tương đương với 3 ký tự. Vì thế thủy vân là ký tự thì lượng thông tin nhúng được sẽ rất nhiều.

Thủy vân là một ảnh: Ảnh này có thể là một logo đặc trưng cho công ty hoặc là dấu vân tay đặc trưng cho một cá nhân. Ảnh thủy vân phải có kích thước nhỏ hơn nhiều so với ảnh gốc.

Nếu ảnh thủy vân là ảnh đen trắng thì việc tạo thủy vân chỉ đơn thuần nhặt ra từng điểm ảnh để nhúng vào các khối ảnh. Nếu ảnh có kích thước MxN thì chuỗi nhị phân biểu diễn cho ảnh nhị phân cần nhúng có độ dài là MxN bít.

Nếu ảnh thủy vân là ảnh đa cấp xám: Lấy giá trị của từng điểm ảnh theo cách duyệt ảnh từ trên xuống dưới, từ trái qua phải xếp thành chuỗi số biểu diễn cho thủy vân cần nhúng. Mỗi số trong dãy số trên lại được chuyển thành một dãy 8 bit nhị phân. Vậy nếu ảnh có kích thước MxN thì dãy thủy vân biểu diễn cho ảnh thủy vân có kích thước là MxNx8 bits.

Nếu ảnh thủy vân là ảnh 24 bits màu, mỗi thành phần mầu R, G, B chiếm 1 byte nhớ. Khi đó có 2 cách tạo thủy vân:

Chức năng trích thủy vân

Từ các khối ảnh (16x16) có thủy vân ta sẽ lấy ra được một số bit thủy vân. Ghép các bít này lại với nhau để được dãy bit. Thực hiện cắt từng đoạn 8 bit một của dãy bit này để thu được mã ASCII của ký tự hoặc giá trị mức xám của một điểm ảnh.

Với mục đích xác thực thông tin thì yêu cầu của hệ thống phải là thủy vân dễ vỡ. Khi đó chỉ việc so sánh thủy vân tách được từ ảnh nghi ngờ với thủy vân gốc mà chủ sở hữu đang có, nếu không giống nhau thì có nghĩa là tác phẩm đã bị sửa chữa thông tin trái phép, không phải là sản phẩm nguyên bản của tác giả.Với mục đích bảo vệ bản quyền thì yêu cầu của hệ thống phải là thủy vân bền vững. Nghĩa là dù sản phẩm có bị sửa chữa theo một hình thức nào đó (do các đối tượng nhái lại từ bản gốc) thì thủy vân vẫn được bảo vệ. Do đó, tác giả có thể trích thủy vân từ bản nghi ngờ ăn cắp bản quyền để chứng minh rằng đây là tác phẩm của mình đã bị chỉnh sửa (bản nhái lại).

Chức năng kiểm tra: Kiểm tra tính bền vững của các thuật toán thủy vân. Với chức năng này người sử dụng có thể kiểm tra xem thuật toán mình chọn có thể chống lại những biến đổi tấn công như: nén, nhiễu, tăng giảm độ sáng...từ đó có thể lựa chọn giải pháp hợp lý cho thuật toán nhúng thủy vân. Kẻ vi phạm bản quyền có thể dùng các tấn công trái phép để làm biến đổi thủy vân. Nếu sau khi tấn công chất lượng ảnh thấp, không còn giá trị thương mại thì thuật toán thành công về khía cạnh bền vững.

Chức năng thu nhận lại ảnh gốc: Trong quá trình trích rút thông tin thủy vân, hệ thống cũng sửa đổi lại các giá trị hệ số DE tương ứng, tiếp đến sử dụng DE nghịch để chuyển đổi hệ số từ ảnh thủy vân về ảnh gốc. Do phép biến đổi DE là thuận nghịch nên ta sẽ thu được giá trị thật của ảnh gốc

2.2.3. Mô hình thử nghiệm

2.2.3.1. Modul nhúng thủy vân.

Giao diện của modul này được trình bày trong Hình 2.1. Các cửa sổ lệnh bao gồm:

- Mở ảnh gốc: Chọn mục „Mở ảnh" để mở một file ảnh cần nhúng thủy vân. Ảnh gốc sẽ hiện ra bên trái của cửa sổ ứng dụng.

Hình 2.1. Giao diện thực hiện mở ảnh gốc

- Tạo thủy vân: Thủy vân là một chuỗi ký tự nhập trực tiếp vào tệp tin. Người sử dụng nhập trực tiếp chuỗi thủy vân vào thanh Tệp tin như Hình 2.2

Hình 2.2. Giao diện thực hiện nhập tệp tin

Sau khi nhập xong thủy vân, chọn mã hóa để chuyển thủy vân thành dạng nhị phân bằng cách nhấn vào nút Mã hóa.

- Nhúng thủy vân: Chọn mục "Nhúng" để bắt đầu quá trình nhúng. Các bước chính trong quá trình này bao gồm ● Nhận các khối (16x16) điểm ảnh của ảnh gốc và lưu vào 3 mảng tương ứng với 3 thành phần màu G,R và B.

● Chuyển đổi các giá trị của 3 mảng trên sang giá trị đa cấp xám ứng với 3 mảng Y,U và V.

● Biến đổi DE thuận trên các giá trị đa cấp xám của mảng Y.

● Chuyển đổi chuỗi ký tự thủy vân sang chuỗi các

bit, mỗi ký tự tương ứng 8 bit.

● Sử dụng thuật toán DE để thay đổi giá trị các phần tử của ảnh

● Chuyển đổi DE nghịch để nhận các giá trị đa cấp xám Y mới.

- Tạo ảnh thủy vân: Sau khi biến đổi DE nghịch ở bước trên, ta đưa từng điểm ảnh (đã biến đổi) vào một khung ảnh (pictureBox) trên cửa sổ ứng dụng. Ảnh đã nhúng thủy vân nằm bên phải cửa sổ ứng dụng và mã hóa tệp tin. Quá trình này được trình bày trong Hình 2.3.

Hình 2.3. Giao diện thực hiện nhúng thủy vân

Đánh giá: Vì chương trình xử lý với ảnh 24 bit mầu, nghĩa là chỉ có một thành phần R hoặc G hoặc B tham gia nhúng thủy vân nên khả năng "lộ" của ảnh rất thấp và mắt thường khó nhìn thấy được.

Chương trình tính hệ số PNSR để đánh giá sự khác nhau của ảnh. Hệ số PNSR = 37.8791db >= 30 là chấp nhận được.

2.2.3.2. Modul trích thủy vân và khôi phục

Giao diện của modul này có dạng như hình 2.4. Các bước trích thủy vân bao gồm:

- Mở ảnh đã thủy vân: Chọn mục "Mở ảnh" để mở một file đã nhúng thủy vân. Ảnh đã thủy vân sẽ hiện ra bên trái của cửa sổ ứng dụng

Hình 2.4. Giao diện thực hiện mở ảnh thủy vân

Chọn "Trích xuất" để bắt đầu quá trình trích thủy vân. Các bước trong quá trình này bao gồm:

● Nhận các khối (16x16) điểm ảnh của ảnh đã thủy vân và lưu vào 3 mảng tương ứng với 3 thành phần màu G,R và B.

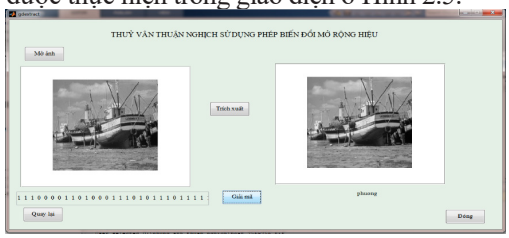
● Chuyển đổi các giá trị của 3 mảng trên sang giá trị đa cấp xám ứng với 3 mảng Y,U và V.

● Biến đổi DE thuận trên các giá trị đa cấp xám của mảng Y.

● Sử dụng thuật toán DE để xác định giá trị các bit đã nhúng tương ứng trong mỗi khối. Nối các bit này thành các chuỗi 8 bit và chuyển đổi sang mã ASCII để nhận được chuỗi ký tự thủy vân. Mục đích của thao tác này là để phục vụ việc chuyển đổi lại ảnh đã thủy vân trở lại ảnh có tính chất nguyên dạng ảnh gốc.

● Chuyển đổi DE nghịch để nhận các giá trị đa cấp xám Y mới.

- Khôi phục ảnh đã thủy vân về nguyên dạng ảnh gốc: Sau khi biến đổi nghịch ở bước trên. Ảnh nguyên dạng ảnh gốc nằm bên phải cửa sổ ứng dụng. Quá trình này được thực hiện trong giao diện ở Hình 2.5.



Hình 2.5. Giao diện thực hiện trích xuất ảnh thủy vân và khôi phục

Để tìm lại thủy vân, nhấn vào nút Giải mã sẽ thu được thủy vân gốc.

3. Kết luận

Bài báo tập trung xây dựng các lược đồ thủy vân bền vững dựa trên phương pháp thuận nghịch sử dụng phép biến đổi mở rộng hiệu.những đóng góp chính của bài báo bao gồm:1. Cài đặt các thuật toán trên phương pháp mở rộng hiệu; 2. Chương trình có khả năng thu nhận lại ảnh có tính chất tương đương ảnh gốc sau khi trích thủy vân, đánh giá tính bền vững của thủy vân qua một số phép tấn công đơn giản.

Tài liệu tham khảo

[1] C. W. Honsinger, P. Jones, M. Rabbani, J. C. Stoffel, "Lossless recover y of an original image containing embedded data", US Patent application, Docket no: 77102/e-d, 2001.

[2] Zhicheng Ni, Yun-Qing Shi, Nirwan Ansari, And Wei Su, "Reversible Data Hiding", Ieee Transactions On Circuits And Systems For Video Technology, Vol. 16, No.3 (2006) 354.

[3] J.H. Hwang, J. W. Kim, J. U. Choi, "A Reversible Watermarking Based On Histogram Shifting", Iwdw 2006, Lncs 4283 (2006) Pp. 384-361.

[4]. I..J. Cox, J. Kilian, T. Leighton, And T. Shamoon, A Secure, Robust Watermark For Multimedia, In Proc First Int. Workshop On Information Hiding, R. Anderson, Ed., No. 1174 In Lecture Notes In Computer Science, Pp. 185–206, May/June 1996.