Journal of educational equipment: Applied research, Volume 2, Issue 311 (April 2024)
ISSN 1859 - 0810

Nghiên cứu Kỹ thuật giấu ảnh trong ảnh sử dụng phương pháp LSB cải tiến phục vụ dạy học ngành Công nghệ thông tin ở Trường Đại học Hải Phòng

Hoàng Trần Hiếu

ThS. Trường Đại học Hải Phòng

Received: 25/3/2024; Accepted: 29/3/2024; Published: 03/4/2024

Abstract: *The information hiding techniques arose to satisfy the need for covert communication. Steganography is an extremely useful method for covert information transmission. Steganography is the data hiding technique which allows hiding secret message or image within a larger image or messagesuch that the hidden message oran image is undetectable. This paper proposes an image hiding steganographic method, of hiding an image within a cover image. This steganographic method aimsto minimize the visually aphương pháparent and statistical differences between the coverimage and a stego image withincrease in the size of the payload. The proposed algorithm uses the binary codes which is the binary representation of pixels inside the image. This algorithm make use of least significant bit (LSB) technique, which is a popular technique in steganography ,in which least significant bits of cover are altered by secret data bits. The proposed method incorporate randomization algorithm which improvethe security of LSB scheme. The bits of the secret image are embedded in random pixels of the cover image and these random pixels are generated by RC4 algorithm.The system enhances the security of the LSB technique by randomly dispersing the bits of secret image in the cover image which makes it harder for unauthorized people to extract the original image. Since all the secret image bits are embedded in the cover image the exact secret image can be regenerated from the stego-image and thereby the image quality is preserved by the system. Thus the proposed system implements steganography for images, with an improvement in both security and image quality.*

Keywords: *Data hiding, Steganography, LSB encoding, Image Steganography, Randomization, RC4 Algorithm.*

1. Đặt vấn đề

Bảo mật trong giao tiếp vẫn là một vấn đề quan trọng trong bảo mật thông tin. Truyền dữ liệu an toàn rất cần thiết trong nhiều lĩnh vực ngày nay. Một số giải pháp về phần cứng và phần mềm đã được đề xuất và thực hiện cho thông tin bảo mật cái mà hạn chế việc truy cập trái phép, tiết lộ và sử dụng những thông tin cá nhân vv..Giấu dữ liệu là một công nghệ phổ biến để bảo mật thông tin. Giấu dữ liệu là một công nghệ (CN) giấu thông tin vào trong một nội dung mà không bị phát hiện. Đánh dấu, mật mã và giấu tin là 3 CN phổ biến để giấu dữ liệu.

Đánh dấu là quá trình giấu tin kĩ thuật số trong một tín hiệu truyền thông, nới thông tin ẩn không cần chứa nội dung liên quan đến tín hiệu truyền thông. Hình mờ kĩ thuật số có thể được sử dụng để xác minh tính xác thực hoặc tính toàn vẹn của tín hiệu truyền thông và cũng thể hiện danh tính của chủ sở hữu của nó. Dễ thấy nó được sử dụng để theo dõi vi phạm bản quyền và trong chứng thực tiền giấy.Cả CN giấu và kĩ thuật đánh dấu sử dụng kĩ thuật giấu để nhúng dữ liệu bí mật tring tín hiệu ồn nhưng ưu tiên khác nhau.CN giấu ưu tiên cung cấp khả năng không để bị phát hiện của người dung,trong khi kĩ thuật đánh dấu cố gắng kiểm soát .

Mật mã là một kĩ thuật phổ biến được sử dụng để đảm bảo thông tin được truyền đi k có sự góp mặt của bên thứ 3.Mật mã đồng nghĩa với việc mã hóa,liên quan đến việc chuyển đổi thông tin từ một mã có thể đọc được đến mã vô nghĩa.Một kĩ thuật giải mã đặc biệt sẽ được yêu cầu giải mã hoặc khôi phục lại thông tin ban đầu từ một mẩu mã.Nguồn của một mật mã chỉ chia sẻ mã với người nhận, do đó tránh việc xâm nhập của bên thứ 3.

CN giấu thông tin là PP không giấu thông tin sao cho đối phương không phát hiện ra được bằng mắt thường. Mật mã cho phép chuyển thông tin thành vô nghĩa,trong khi đó giấu tin là thông tin cần giấu sẽ được giấu đi.Giấu tin liên quan đến bất kì quy trình giấu tin nào hoặc thông tin bên trong dữ liệu khác.

Động lực chính của giấu tin là không để phát hiện thông tin và đảm bảo truyền tải thông tin một cách an toàn. Kỹ thuật giấu tin của Hy Lạp được định nghĩa là viết tắt.CN giấu tin được sử dụng trong thời Hy Lạp cổ đại xưa,bằng cách xăm một mẩu tin bí mật lên đầu của một sứ giả và để tóc mọc lại trc khi đưa anh ta qua lãnh thổ của kẻ thù. Một trong những cách phổ biến và đơn giản để tiếp cận ảnh giấu là PP chèn ít bit nhất có thể (LSB). Kĩ thuật LSB này có thê sử dụng để giấu ảnh bên trong một ảnh khác.Điều này liên quan đến việc thay thế LSB của các điểm ảnh với bit của ảnh bí mật. Do đó hình ảnh được ẩn bên trong một ảnh khác bằng cách thay đổi LSB của ảnh gốc. Sự thay đổi LSB không làm ảnh hưởng đến ảnh gốc và do đó nó sẽ không lộ thông tin được giấu bên trong ảnh.

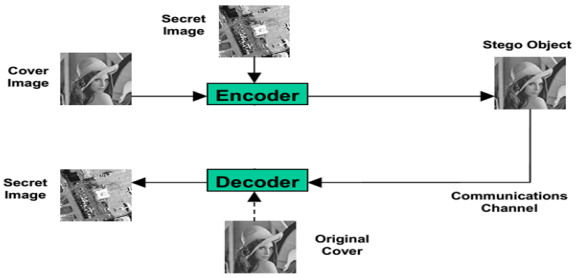
2. Nội dung nghiên cứu

2.1 Hệ thống đã tồn tại

Hình ảnh được biểu diễn bằng các cường độ ánh sang khác nhau, có nghĩa là được đại diện bởi những điểm ảnh của hình ảnh và điểm ảnh biểu diễn cho 1 con số. Do đó hình ảnh là một bảng điểm ảnh có giá trị khác nhau tại khu vực khác nhau.Ảnh kĩ thuật số thường được biểu diễn bởi 24 bit hoặc 8 bit, tức là 24 bit hoặc 8 bit để sử dụng biểu diễn 1 điểm ảnh. Hình ảnh 24 bit là hình ảnh màu thực và chúng có thể giấu được nhiều thông tin hơn. Tuy nhiên, hình ảnh 24 bit thường có kích thước lớn và không phổ biến,và nó sẽ thu hút sự chú ý khi được truyền đi qua mạng.Nên nhìn chung ảnh 8 bit như GIF được sử dụng để giấu thông tin, môi điểm ảnh biểu diễn bởi 1 byte đơn.Nên mỗi điểm ảnh có thể có giá trị từ 0 đến 255 và thể hiện được 256 màu sắc.

Thuật toán LSB (Least Significant Bit) thực hiện trên việc xác định các bit ít quan trọng nhất của bức ảnh để thay thế bằng các bit thông tin cần giấu. Bit ít quan trọng của một bứ ảnh là bit có ảnh hưởng ít nhất tới việc quyết định tới màu của một điểm ảnh, vì vậy khi ta thay đổi bit ít quan trọng của một điểm ảnh thì màu của mỗi điểm ảnh mới sẽ tương đối gần với điểm ảnh cũ. Như vậy, kỹ thuật tách bit trong xử lý ảnh được sử dụng rất nhiều trong quy định giấu tin. Việc xác định LSB của mỗi điểm ảnh trong một bức ảnh phụ thuộc vào định dạng ảnh và số bit màu dành cho mỗi điểm của ảnh đó.

PP LSB sẽ thay thế bit ít quan trọng nhất, thường là bit cuối của mỗi mẫu dữ liệu bằng một bit thông tin mật. Như vậy trên mỗi pixel của một ảnh BMP 24bit có thể giấu từ một đến 3 bit mật. Quá trình mã hóa (Encode) và giải mã (Decode)



Quá trình mã hóa:

Đầu tiên chúng ta chuyển ảnh gốc và ảnh bí mật sang dạng nhị phân.

Duyệt các pixel trong cả ảnh gốc và ảnh bí mật, đọc các giá trị RGB của từng pixel một.

Thay LSB của từng giá trị RGB. Cứ ba bit của ảnh bí mật được giấu vào trong ba bit LSB cuối cùng của ảnh gốc. Do đó ba bit cuối ảnh gốc được thay thế bởi bit của ảnh bí mật.

Quá trình giải mã:

Duyệt từng pixel của bức ảnh nhận được.

Đọc giá trị RGB, lấy các LSB của từng giá trị RGB, ta thu được các bit của ảnh bí mật.

Chuyển từ dạng nhị phân sang ảnh bí mật.

PP chèn ít bit LSB nhất là PP phổ biến và đơn giản cho giấu ảnh. CN này cho phép giấu thông tin bên trong ảnh bằng cách thay đổi LSB của ảnh gốc.Sự thay đổi LSB không làm thay đổi ảnh gốc và do đó người dung sẽ không thể biết được thông tin bí mật. Các PP hiện tại của giấu ảnh sử dụng LSB chỉ thay thế bit quan trọng nhất của mỗi điểm ảnh của ảnh gốc,một bit đơn được thay thế bởi mỗi điểm ảnh.Việc thay thế LSB cho phép giấu thông tin bên trong ảnh gốc chi tiết. Và khi đó nó thay đổi một chút và điểm ảnh mà không gây ra sự khác biệt về chất lượng của hình ảnh.

PP giấu dữ liệu 4 bit và 6 bit dựa vào PP LSB có thể sử dụng để phát triển dung lượng thông tin của ảnh gốc được sử dụng.Trong PP LSB một bit LSB được sửa đổi trong mỗi điểm ảnh và mỗi điểm ảnh biểu diễn với 8 bit,ảnh gốc yêu cầu lớn hơn 8 lần so với ảnh bí mật.PP 4 bit và 6 bit sửa đổi nhiều số bit LSB và do đó kích thước yêu cầu của ảnh gốc bị giảm bởi những PP này. Trong PP giấu dữ liệu 4 bit 4 bit cuối cùng của LSB của mỗi điểm ảnh gốc được thay thế bởi 4 bit MSB đầu tiên của ảnh bí mật,có nghĩa PP này nhúng 4 bit MSB của ảnh bí mật vào trong 4 bit LSB của ảnh gốc.

2.2. Hệ thống được áp dụng

Bài báo biểu diễn kĩ thuật giấu ảnh của 3 bit dựa vào kỹ thuật LSB. LSB có kích thước lớn thì ảnh gốc như một bất lợi. Ảnh gốc yêu cầu lớn hơn 8 lần so

với ảnh bí mật, PP giấu dữ liệu 4 bit và 6 bit vượt quá yêu cầu về kích thước này.Nhưng chất lượng thu được không được cung cấp bởi PP này. Một bất lợi lớn khác của PP này là vấn đề về sơ đồ tuần tự. Có vô số sơ đồ chi tiết giữa ảnh gốc và điểm ảnh của ảnh bí mật.Do tính đơn giản của PP này dẫn đến việc ng dung phát hiện ra có một vài thông tin sau ảnh gốc này, họ có thể dễ dàng thu thập LSB của ảnh bí mật.Đề xuất phương pháp 3 bit LSB là một giải pháp của vấn đề này.

2.2.1. PP giấu 3 bit dữ liệu của ảnh bí mật

3 bít dữ liệu bí mật được chia làm 3 lần. Mỗi 3 bit của ảnh bí mật được nhúng vào 3 bit LSB cuối cùng của ảnh gốc. Do đó 3 bit cuối ảnh gốc được thay thế bởi bit của ảnh bí mật.Sau đó với mỗi 8 bit của ảnh gốc 3 bit sẽ là thông tin bí mật. Hình 1 biểu diễn phương pháp giấu 3 bit dữ liệu.Khi đó tất cả bit của ảnh bí mật được nhúng vào ảnh gốc,ảnh bí mật có thể được lấy ra một cách chính xác nhất bởi phương pháp này.Công nghệ giấu 3 bit dl tránh được các vấn đề về sơ đồ tuần tự và tăng cường kỹ thuật LSB bằng cách kết hợp ngẫu nhiên với chèn LSB.Bằng cách này các bit hình ảnh bí mật sẽ được phân tán ngẫu nhiên vào các điểm ảnh gốc và do đó khiến người dung không thể phát hiện được thông tin giấu trong ảnh.

Bảng 2.1: PP giấu 3 bit dữ liệu

Cover Image																							
Pixel 1								Pixel 2								Pixel 3							
1	0	0	1	0	1	1	0	1	0	1	1	1	0	0	1	0	1	1	0	0	1	1	0
					LSB+2	LSB+1	LSB																

Secret Image																							
Pixel 1								Pixel 2								Pixel 3							
1	0	1	0	1	0	0	1	1	0	1	0	1	1	0	1	0	1	0	0	1	1	0	1

Strgo Image																							
Pixel 1								Pixel 2								Pixel 3							
1	0	0	1	0	1	0	1	1	0	1	1	1	0	1	0	0	1	1	0	0	0	1	1

2.2.2. Kỹ thuật LSB ngẫu nhiên

Các kỹ thuật LSB là PP dễ dàng và trực tiếp giấu ảnh vào trong ảnh. Thông tin được nhúng bằng cách sử lập sơ đồ tuần tự. Tác giả áp dụng kỹ thuật ngẫu nhiên hóa để nâng cao tính bảo mật của PP LSB. PP này nhúng bit ảnh bí mật vào các điểm ảnh ngẫu nhiên của ảnh gốc. Và do đó nó cho phép vượt qua vấn đề về sơ đồ tuần tự và đảm bảo về hệ thống.Thuật toán RC4 được sử dụng để nhúng sự ngẫu nhiên này. Thuật toán RC4 tạo ra các điểm ảnh của hình ảnh gốc theo một thứ tự ngẫu nhiên và các bit ảnh bí mật được nhúng vào những điểm ảnh này theo thứ tự tương ứng. RC4 có cấu trúc đơn giản và được sử dụng rộng rãi. RC4 cũng cung cấp kế hoạch chính đơn giản và quá trình sản xuất đầu ra. Kể từ khi thông tin bí mật được nhúng ngẫu nhiên nó khó bị phát hiện hơn. Thuật toán này sử dụng một khóa stego trong quá trình nhúng và trích xuất thông tin bí mật. Khóa stego này có thể được có sẵn tại các máy thu bằng cách nhúng vào hình ảnh hoặc có thể cung cấp cho ng nhận. Trong trường hợp không có khóa stego rất khó để biết trình tự trong điểm ảnh gốc được sử dụng để nhúng. Do đó dựa trên RC4 ngẫu nhiên hệ thống bảo mật được cải thiệt hơn.

Các bước mô tả thuật toán RC4

Bước 1: Phân phối hình ảnh

Bước 2: Tạo mảng vị trí ảnh gốc cho khóa stego được chọn sử dụng thuật toán RC4

Bước 3: Thay thế LSB của điểm ảnh gốc trên màn hình trong trình tự tạo ra trong bước 2, với các dữ liệu giấu.Do đó PP đề xuất cung cấp cải thiện về an ninh và chất lượng

3. Kết luận

Kỹ thuật giấu ảnh là một CN hiệu quả được sử dụng để chuyển thông tin bí mật. Kĩ thuật này cho phép giấu ảnh bí mật bên trong một ảnh khác.Giấu ảnh là PP hiệu quả nhất để kẻ thù không phát hiện ra sự hiện diện của bí mật ẩn giấu.Kỹ thuật dựa vào bit LSB ít nhất là phổ biến và dễ dàng nhất cho nhúng thông tin trong ảnh.Chúng tôi trình bày PP LSB an toàn và mạnh hơn.Chúng tôi đề xuất một kỹ thuật che giấu hình ảnh cho phép giấu 1 ảnh trong 1 ảnh khác. Sử dụng PP giấu 3 bit dữ liệu để nâng cao chất lượng hình ảnh.Để tăng cường bảo mật,thứ tự điểm ảnh của ảnh gốc đã được chọn để nhúng ảnh bí mật phụ thuộc vào số ngẫu nhiên được tạo ra bởi RC4 sử dụng khóa stego. Ngay cả khi người sử dụng phát hiện ra thông tin bí mật cũng là một khó khăn để có thể phục hồi nó,bởi các bit được nhúng theo thứ tự ngẫu nhiên.Sự an toàn của hệ thống được đề xuất có thể được cải tiến hơn nữa bằng cách kết hợp mã hóa mật mã với hệ thống. Hình ảnh bí mật được ẩn có thể mã hóa trước khi thực hiện kỹ thuật LSB. Điều này có thể được xem xét trong tương lai.

Tài liệu tham khảo

1. Reena M Patel,D J Shah (2013) , *"Concealogram : Digital image in image using LSB insertion method", International journal of electronics and communication engineering & technology(IJECET).*

2. Nadeem Akhtar, Pragati Johri, Shahbaaz Khan (2013), *"Enhancing the security and quality of LSB based image steganography", 2013 5th International Conference on Computational Intelligence and Communication Networks.*

3. R. Chandramouli, N. Memon (2001), *"Analysis of LSB Based Image Steganography Techniques", IEEE phương pháp. 1019-1022.*