NGHIÊN CỨU XÂY DỰNG PHƯƠNG PHÁP KẾT HỢP ẨN MÃ VỚI MẬT MÃ KHÔNG SỬA VẬT PHỦ

Trần Thị Xuyên, Đặng Xuân Bảo*, Hoàng Thu Phương, Nguyễn Thị Hồng Hà
Học viện Kỹ thuật Mật mã

TÓM TẮT

Ngày nay việc sử dụng đa phương tiện để trao đổi thông tin đã trở nên phổ biến. Vì thế, vấn đề đảm bảo an toàn trong quá trình truyền tin rất quan trọng, đặc biệt là các thông tin bí mật. Có hai cách phổ biến được dùng để bảo vệ tính bí mật cho các thông tin cần trao đổi đó là sử dụng các thuật toán mã hóa và ẩn mã. Thuật toán mã hóa giúp biến bản rõ thành bản mã và nếu không biết khóa thì không thể giải mã được. Trong khi đó, ẩn mã lại giấu đi sự tồn tại của thông điệp vào vật phủ khác, nên kẻ tấn công không nghi ngờ có sự trao đổi thông tin bí mật giữa các bên. Để nâng cao độ an toàn, có nhiều phương pháp sử dụng cả ẩn mã và mật mã, theo đó thông điệp thường được mã hóa rồi mới nhúng vào vật phủ. Nhưng trong cách này, vật ẩn mã cũng thay đổi so với vật phủ ban đầu nên có thể bị phát hiện khi phân tích lược đồ histogram hoặc giá trị PSNR. Chính vì vậy dung lượng nhúng thường không nhiều để đảm bảo yêu cầu về độ trong suốt. Bài báo này sẽ giới thiệu một phương pháp kết hợp ẩn mã với mật mã không những nâng cao được dung lượng nhúng mà còn không hề thay đổi vật phủ.

Từ khóa: *Ẩn mã; mật mã; vật phủ; histogram; PSNR*

Ngày nhận bài: 21/3/2019;Ngày hoàn thiện: 11/4/2019;Ngày duyệt đăng: 07/5/2019

A PROPOSED METHOD COMBINING STEGANOGRAPHY AND CRYPTOGRAPHY WITHOUT MODIFYING THE COVER OBJECT

Tran Thi Xuyen, Dang Xuan Bao*, Hoang Thu Phuong, Nguyen Thi Hong Ha
Academy of Cryptography Techniques

ABSTRACT

Recent, it is very popular to use multimedia to communicate in digital age. Thus, protecting transfered data, especially confidential information, is an interested issue. Two methods to protect confidential data are encryption and steganography. Encryption algorithm converts a plaintext to a ciphertext and everyone only can decrypt it by the secret key. While steganography hides message into a cover object, this helps to protect the existence of message from attacker. To increasing security level, there are many methods combining steganography and cryptography to embed ciphertext into the cover object. However, we can detect the difference between the stego object and the cover by analyzing histogram or PSNR value and embedded capacity is limited, which affects to imperceptibility. In this paper, we propose a new method combining steganography and cryptography to enhance embedded capacity without modifying the cover object.

Keywords: *Steganography; cryptography; cover image; histogram; PSNR.*

Received: 21/3/2019; Revised: 11/4/2019;Approved: 07 /5/2019

* Corresponding author: *Tel: 0964 101882, Email:dangxuanbao.attt@gmail.com*

1. Giới thiệu

Ngày nay, việc liên lạc trao đổi thông tin bằng các dữ liệu đa phương tiện thông qua mạng Internet đã trở nên rất phổ biến. Song song với những lợi ích về sự nhanh chóng, tiện dụng là sự mất an toàn thông tin. Người dùng mạng Internet luôn có những mối lo ngại về sự nghe lén, đánh cắp, sửa đổi thông tin một cách trái phép, virus hay sâu mạng, ... Chính vì thế việc đảm bảo an toàn thông tin trở thành nhu cầu cấp bách hơn bao giờ hết. Mật mã và ẩn mã là hai cách được sử dụng phổ biến nhất để nâng cao độ an toàn khi trao đổi thông tin trên mạng Internet. Các phương pháp mã hóa với hai nguyên lý chung là thay thế và xáo trộn [1] nhằm biến thông điệp dưới dạng bản rõ thành bản mã không có ý nghĩa. Các thuật toán mã hóa thường sử dụng các khóa bí mật hoặc khóa công khai để mã hóa. Đối với mã hóa khóa bí mật, bên gửi và bên nhận thống nhất trước một khóa và khóa này phải được giữ bí mật. Do đó kẻ tấn công nếu không biết khóa thì không thể đọc được nội dung thông tin đó. Còn với mã hóa khóa công khai, người gửi sẽ mã hóa bằng khóa công khai của người nhận và tất cả mọi người đều có thể biết khóa này. Tuy vậy không phải ai cũng giải mã được bản mã mà chỉ người nhận có khóa riêng mới có thể chuyển bản mã thành thông điệp rõ ban đầu. Một phương pháp khác cũng có tác dụng đảm bảo tính bí mật cho dữ liệu khi truyền trên mạng Internet là ẩn mã. Ẩn mã là một nghệ thuật che giấu và truyền dữ liệu qua các vật mang tin hoàn toàn vô hại [11, p.17]. Từ ẩn mã tiếng Anh là Steganography có nguồn gốc từ Hi Lạp, có nghĩa là cách viết được che phủ hoặc che giấu và bao gồm một loạt phương pháp giao tiếp bí mật mà che giấu sự tồn tại của thông điệp. Theo đó những vật được dùng để che giấu thông tin được gọi là vật gốc hay vật phủ, còn vật sau khi đã được nhúng tin vào được gọi là vật mang tin hay vật ẩn mã.

Có thể thấy rằng, khi sử dụng các phương pháp mật mã, dù kẻ tấn công không biết được nội dung thông tin đằng sau bản mã nhưng dễ dàng nghi ngờ về sự trao đổi thông tin bí mật, từ đó họ sẽ tìm mọi cách có thể để tấn công. Trong khi đó, các phương pháp ẩn mã cho phép che giấu sự tồn tại của thông điệp vào các dữ liệu đa phương tiện khác như các tệp ảnh số, video, âm thanh, văn bản [10, p.20]. Do đó các kỹ thuật này khiến kẻ tấn công không có những nghi vấn hay tò mò khi thông điệp bí mật được truyền đi. Nói chung các kỹ thuật ẩn mã thường thay thế các bit của vật phủ, chẳng hạn như các bit có trọng số thấp nhất (LSB) bằng các bit của thông điệp. Khi đó người nhận đã biết các vị trí nhúng thông tin và chỉ cần trích xuất các bit này để thu được thông điệp bí mật.

Với nhu cầu bảo vệ an toàn thông tin ngày càng nâng cao nên đã có rất nhiều nghiên cứu về sự kết hợp ẩn mã và mật mã, trong đó đa số các phương pháp đều hướng tới việc mã hóa thông điệp trước rồi sau đó nhúng bản mã nhận được vào vật phủ. Với cách này, kẻ tấn công muốn thu được thông điệp trước hết phải phá được thuật toán ẩn mã và trích xuất thông tin. Kế đó, anh ta lại phải tìm được khóa thích hợp để có thể giải mã được thông tin vừa trích xuất. Biện pháp này có nhược điểm là vật phủ vẫn bị thay đổi so với ban đầu. Chính vì vậy cần phải quan tâm tới việc lựa chọn vị trí nào để thay thế bít cũng như dung lượng nhúng sẽ bị hạn chế để đảm bảo rằng bằng các giác quan thông thường của con người không thể phát hiện ra sự biến đổi trong vật phủ. Cách tiếp cận này cũng cần phải kiểm tra lược đồ histogram của vật phủ so với vật ẩn mã cũng như giá trị PSNR để có thể tránh sự phát hiện có giấu tin. Ngoài ra, những phương pháp này cũng phải xem xét tới các phép phân tích khác, chẳng hạn như phân tích thống kê để có thể chống lại được các kiểu tấn công dạng này.

Một cách kết hợp ẩn mã và mật mã khác được Khalil Challita và Hikmat Farhat [4] giới thiệu vào năm 2011 với ý tưởng giấu thông tin nhưng không thay đổi vật phủ. Phương

pháp này áp dụng bài toán cây hậu tố tổng quát để tìm ra xâu con giống nhau dài nhất giữa vật phủ và thông điệp, từ đó xác định vị trí bắt đầu và kết thúc của xâu con rồi lưu các vị trí này vào một véc tơ, trong đó vật phủ đã được hai bên thống nhất với nhau từ trước. Thông tin được gửi cho bên nhận chính là véc tơ này và bên gửi sẽ dùng véc tơ nhận được để trích xuất thông điệp trong vật phủ đã biết. Kẻ tấn công dù có bắt được véc tơ mà hai bên trao đổi nhưng nếu không có vật phủ thì cũng không thể biết được nội dung thông điệp thực sự. Bài báo này, chúng tôi cũng dựa trên ý tưởng giấu thông điệp mà không sửa đổi vật phủ nhưng thay vì xác định xâu con giống nhau dài nhất giữa vật phủ và thông điệp thì chúng tôi sử dụng véc tơ nhị phân để lưu giá trị giống nhau và khác nhau giữa vật phủ và thông điệp, theo đó nếu bit của vật phủ và thông điệp giống nhau thì sẽ lưu giá trị 0, ngược lại lưu giá trị 1 vào véc tơ. Việc này được thực hiện rất đơn giản với phép toán XOR bit giữa thông điệp và ảnh phủ. Với phương pháp đề xuất này, chúng ta có thể giấu thông tin ở bất kì bít nào của vật phủ nên dung lượng nhúng sẽ tăng lên đáng kể so với các phương pháp khác. Véc tơ nhị phân này sẽ được gửi đi và chỉ có người nhận chủ định mới biết vật phủ thực sự để trích xuất thông điệp. Để tăng cường độ an toàn, véc tơ trước khi được gửi cho người nhận chúng tôi thực hiện mã hóa bằng một ánh xạ hỗn loạn. Bài báo bao gồm 5 phần, trong phần 2 chúng tôi sẽ tổng hợp giới thiệu một số nghiên cứu về các phương pháp kết hợp ẩn mã với mật mã. Phần 3 chúng tôi trình bày phương pháp đề xuất. Phân tích và đánh giá về độ an toàn của phương pháp đề xuất được trình bày trong phần 4. Kết luận cuối cùng được trình bày trong phần 5.

2. Các nghiên cứu liên quan

Mihir H Rajyaguru [1] đã đề xuất phương pháp kết hợp mật mã và ẩn mã. Thông điệp cần trao đổi được mã hóa bởi một khóa mà được tạo ra bởi một thiết bị sinh khóa ngẫu nhiên và sau đó được nhúng vào trong vật phủ.

Shamim Ahmed Laskar, Kattamanchi Hemachandran [2] đã đề xuất phương pháp giấu dữ liệu sử dụng kỹ thuật ẩn mã LSB và kết hợp với mã hóa chuyển vị. Thông điệp trước tiên được mã hóa bằng cách sắp xếp thành những ma trận cỡ $n \times n$ rồi lấy chuyển vị để được bản mã. Kết quả của quá trình mã hóa sẽ được nhúng vào vật phủ sử dụng kỹ thuật thay thế LSB.

Shailender Gupta, Ankur Goyal, Bharat Bhushan [3] đã đề xuất lược đồ ẩn mã cùng với mật mã để nâng cao độ an toàn. Ý tưởng của phương pháp này là trước tiên thông điệp được mã hóa bằng cách sử dụng thuật toán RSA hoặc Diffie Hellman và chuyển các giá trị ASCII đã được mã hóa này sang thành dạng nhị phân. Tiếp theo chuỗi nhị phân nhận được sẽ được nhúng vào ảnh phủ bằng phương pháp thay thế LSB.

Các tác giả trong [9] đã đề xuất một phương pháp kết hợp ẩn mã với mật mã, đó là ẩn mã khóa công khai dựa trên sự so khớp. Đầu tiên, các tác giả sử dụng giao thức trao đổi khóa Diffie Hellman [12] để hai bên gửi và nhận có thể thống nhất được khóa bí mật dùng ẩn mã ở bước tiếp theo. Khóa này được dùng để lựa chọn điểm ảnh để giấu thông điệp. Phương pháp này sẽ giấu 8 bít thông điệp vào mỗi điểm ảnh được lựa chọn dựa trên việc so khớp giữa giá trị thông điệp và giá trị điểm ảnh theo thứ tự so sánh từ màu đỏ tới màu xanh lá cây và cuối cùng là màu xanh da trời. Một mảng được tạo ra để ghi lại kết quả so khớp giữa giá trị thông điệp và giá trị điểm ảnh. Có 4 trường hợp xảy ra tương ứng với 4 kết quả mà mảng vừa tạo có thể nhận giá trị. Bên gửi trước hết so sánh giá trị của thông điệp với màu đỏ (+/-7 (giá trị thập phân)), nếu bằng thì mảng nhận giá trị 0 (giá trị nhị phân là 00) và giá trị màu đỏ sẽ được gán thành 8 bít dữ liệu. Trường hợp 2, nếu giá trị thông điệp và giá trị màu đỏ không bằng nhau thì tiếp tục so sánh với giá trị màu xanh lá, nếu bằng (+/-7 (giá trị thập phân)) thì mảng nhận giá trị 1 (giá trị nhị phân là 01) và giá trị màu xanh lá cây sẽ được

gán thành 8 bít dữ liệu. Trường hợp 3, nếu giá trị thông điệp không bằng giá trị màu xanh lá thì tiếp tục so sánh với giá trị màu xanh da trời, nếu bằng (+/-7 (giá trị thập phân)) thì mảng nhận giá trị 2 (giá trị nhị phân là 10) và giá trị màu xanh da trời sẽ được gán thành 8 bít dữ liệu. Trường hợp cuối cùng, nếu giá trị thông điệp không bằng giá trị màu xanh da trời thì thực hiện nhúng tin bằng phương pháp LSB và mảng nhận giá trị 3 (giá trị nhị phân là 11). Và trong trường hợp cuối này 3 bít đầu tiên của thông điệp sẽ được nhúng vào 3 bít LSB của màu đỏ, 3 bít tiếp theo được nhúng vào 3 bít LSB của màu xanh lá cây và 2 bít cuối cùng được nhúng vào 2 bít LSB của màu xanh da trời. Có thể thấy đây là phương pháp cho phép nhúng được dung lượng khá lớn với 8 bít trên một điểm ảnh.

Trong [5] các tác giả đã đề xuất phương pháp ẩn mã dựa trên lý thuyết hỗn loạn trong miền không gian, theo đó ánh xạ hỗn loạn được dùng để mã hóa thông điệp bí mật rồi sau đó nhúng bản mã này vào ảnh phủ. Ở phương pháp này, tại mỗi giá trị điểm ảnh RGB thuật toán sẽ nhúng được 8 bít thông điệp, 3 bít đầu tiên sẽ được nhúng vào 3 bít LSB của màu đỏ (R), 3 bít tiếp theo sẽ được nhúng vào 3 bít LSB của màu xanh lá cây (G) và 2 bít còn lại được nhúng vào 2 bít LSB của màu xanh da trời (B). Lý thuyết hỗn loạn được áp dụng ở đây để tạo ra một chuỗi nhị phân từ chuỗi hỗn loạn vừa sinh ra thông qua giá trị trung bình của chuỗi gọi là ngưỡng. Chuỗi nhị phân này sẽ mã hóa thông điệp trước khi đem nhúng vào vật phủ bằng cách XOR với chuỗi thông điệp để được bản mã. Trong phương pháp này các tác giả cũng đề xuất chia thông điệp thành các phần nhỏ và mã hóa bằng các chuỗi hỗn loạn khác nhau (sử dụng các điều kiện khởi tạo khác nhau).

Trong [6] một phương pháp ẩn mã sử dụng hai ánh xạ hỗn loạn được đề xuất. Ánh xạ thứ nhất dùng để lựa chọn một cách hỗn độn vị trí của các điểm ảnh được dùng để nhúng thông điệp vào đó. Bằng cách này sẽ gia tăng độ an toàn vì khó có thể dự đoán ra thông điệp được nhúng ở đâu. Ánh xạ còn lại dùng để giấu thông điệp. Ngoài ra, các tác giả cũng đề xuất một số cách để làm tăng sự khó đoán cũng như tăng độ bền vững, chẳng hạn sử dụng ánh xạ hỗn loạn đầu tiên để xác định điều kiện khởi tạo cho ánh xạ hỗn loạn thứ hai.

Trong [7] các tác giả giới thiệu một phương pháp truyền thông điệp an toàn bằng cách sử dụng mật mã kết hợp với ẩn mã. Bên gửi áp dụng hai thuật toán mật mã để mã hóa thông điệp bí mật. Trước tiên bên gửi mã hóa thông điệp bằng thuật toán mã hóa góc (agular encryption algorithm) để biến thông điệp thành một ảnh mã hóa bằng cách kết hợp thông điệp với ảnh phủ. Khóa của quá trình mã hóa này là ảnh phủ và điểm ảnh $P(x,y)$ ngẫu nhiên của ảnh phủ đó. Sau đó thuật toán biến đổi được sử dụng để kết hợp ảnh mã hóa nhận được với ảnh phủ ở trên để tạo ra một văn bản trung gian chính là bản mã của thông điệp ban đầu. Khóa của thuật toán biến đổi vẫn là ảnh phủ. Bản mã của thông điệp sau đó được giấu trong ảnh phủ sử dụng phương pháp ẩn mã LSB với một khóa bí mật. Các tác giả sử dụng thuật toán RSA để mã hóa khóa (gồm điểm ảnh và khóa dùng trong thuật toán LSB) và truyền khóa cho người nhận.

Dr. S. Bhargavi và cộng sự trong [8] đã đề xuất một kỹ thuật giấu dữ liệu bằng cách sử dụng một ánh xạ hỗn loạn để mã hóa thông điệp rồi giấu bản mã thu được vào ảnh. Ánh xạ hỗn loạn sinh ra một chuỗi các số thực, sau đó tính giá trị ngưỡng T là trung bình cộng của chuỗi số này để biến chuỗi số thực hỗn loạn thành chuỗi nhị phân, theo đó tại vị trí nào mà giá trị của số hạng trong chuỗi nhỏ hơn T thì bít ở vị trí đó bằng 0 và ngược lại. Quá trình mã hóa được thực hiện bằng cách XOR bít giữa thông điệp với chuỗi nhị phân vừa nhận được. Phương pháp này nhúng 8 bít thông điệp vào các LSB của một điểm ảnh, trong đó 3 bít đầu tiên được nhúng vào 3 LSB của thành phần màu đỏ, 3 bít tiếp theo được nhúng vào 3 LSB của thành phần màu xanh lá

cây và 2 bít còn lại được nhúng vào 2 LSB của thành phần màu xanh da trời. Có thể thấy dung lượng thông tin được giấu của phương pháp này khá lớn, bên cạnh đó việc cài đặt thuật toán cũng dễ dàng.

Có thể thấy các phương pháp trên đây cũng như hầu hết các phương pháp kết hợp ẩn mã với mật mã đều thực hiện mã hóa thông điệp cần trao đổi trước rồi nhúng bản mã của thông điệp vào vật phủ. Chính vì vậy quá trình nhúng thường làm thay đổi vật phủ và do đó sẽ ảnh hưởng tới chất lượng của vật phủ. Mặt khác để tăng dung lượng nhúng thì phải sử dụng nhiều bit của một điểm ảnh để thay bằng các bit của thông điệp. Do vậy cách kết hợp này sẽ phải cân bằng hai yêu cầu cơ bản của ẩn mã đó là dung lượng nhúng và việc khó cảm nhận sự thay đổi chất lượng ảnh bằng mắt thường. Challita,K. và Farhat [4] đã đề xuất một phương pháp ẩn mã kết hợp mật mã nhưng không hề thay đổi vật phủ. Trước tiên người gửi và người nhận thống nhất sử dụng một ảnh phủ để gửi thông điệp. Người gửi xác định các bit của thông điệp mà giống với các bit trong vật phủ rồi lưu lại những vị trí của chuỗi bit giống nhau này vào một véc tơ. Véc tơ này sau đó có thể được mã hóa rồi gửi cho bên nhận. Phía người nhận khi nhận được véc tơ thì đối chiếu vào ảnh phủ đã biết để trích xuất được thông tin thực sự mà người gửi muốn trao đổi. Các tác giả đã áp dụng bài toán tìm xâu con dài nhất sử dụng phương pháp cây hậu tố tổng quát để cải thiện độ phức tạp của thuật toán còn $O(nlogn)$. Trong bài báo này, chúng tôi đề xuất một giải pháp không sửa vật phủ, tuy nhiên so với [4] phương pháp này khá đơn giản và dễ dàng trong cài đặt thuật toán và độ phức tạp chỉ là tuyến tính.

3. Đề xuất phương pháp ẩn mã kết hợp mật mã không sửa vật phủ

Trong phương pháp này chúng tôi nhúng thông điệp theo cách không sửa vật phủ và lưu lại các giá trị 0/1 ứng với bít giống nhau và khác nhau giữa thông điệp và vật phủ vào một véc tơ, vị trí nhúng bắt đầu từ đầu vật phủ đã thỏa thuận trước. Véc tơ này sau đó sẽ được mã hóa sử dụng ánh xạ logistic để tăng cường tính bảo mật.

3.1 Ánh xạ logistic

Đặc tính nổi bật của các ánh xạ hỗn loạn là nhạy cảm với các điều kiện ban đầu, tức là chỉ cần thay đổi nhỏ trong các giá trị ban đầu thì các giá trị sinh ra sẽ hoàn toàn khác nhau. Chính vì vậy, chúng tôi lựa chọn sử dụng ánh xạ hỗn loạn được nêu trong tài liệu [5] để gia tăng sự an toàn khi kẻ tấn công khó có thể đoán được chuỗi hỗn loạn.

3.2 Phương pháp đề xuất

Trong bài báo này chúng tôi vẫn sử dụng ý tưởng hai bên gửi và nhận thống nhất trước vật phủ và bên nhận sẽ nhúng thông điệp mà không sửa vật phủ của Challita,K. và Farhat. Tuy nhiên thay vì tìm xâu con giống nhau dài nhất giữa vật phủ và thông điệp thì chúng tôi chỉ đơn thuần thực hiện phép XOR bit giữa véc tơ bít của thông điệp với véc tơ bít của ảnh. Theo đó, nếu bít thông điệp giống với bít của ảnh thì giá trị của véc tơ kết quả là 0, ngược lại nếu bít thông điệp khác bít của ảnh thì sẽ là 1. Véc tơ nhị phân nhận được sau khi nhúng hết thông điệp sẽ được mã hóa bằng ánh xạ hỗn loạn rồi mới gửi cho bên nhận. Người nhận biết được khóa bí mật là các tham số đầu vào của ánh xạ logistic sẽ giải mã véc tơ nhận được sau đó cùng với vật phủ đã thống nhất với người gửi để trích xuất được thông điệp ban đầu. Thậm chí chúng ta cũng có thể tăng cường bảo mật hơn nữa bằng cách sử dụng thêm một ánh xạ hỗn loạn để mã hóa thông điệp trước khi đem XOR với vật phủ và một ánh xạ hỗn loạn khác để lựa chọn ngẫu nhiên các điểm ảnh của vật phủ trước khi chuyển sang giá trị nhị phân để thực hiện XOR với thông điệp tuy nhiên lúc đó độ phức tạp của thuật toán lúc này không còn là tuyến tính nữa. Mô hình của thuật toán được đưa ra trong hình 1 dưới đây.

Thuật toán cụ thể của phương pháp này gồm hai quá trình sau:

1) Thuật toán nhúng

2) Thuật toán trích xuất

3.2.1 Thuật toán nhúng

Bước 1: Nhập ảnh mang tin và thông điệp cần giấu, chuyển ảnh mang tin và thông điệp sang dạng nhị phân kí hiệu lần lượt là c và m

Bước 2: Véc tơ $v = c\ xor\ m$

Bước 3: Mã hóa véc tơ v sử dụng ánh xạ hỗn loạn

Bước 4: Gửi kết quả mã hóa cho người nhận

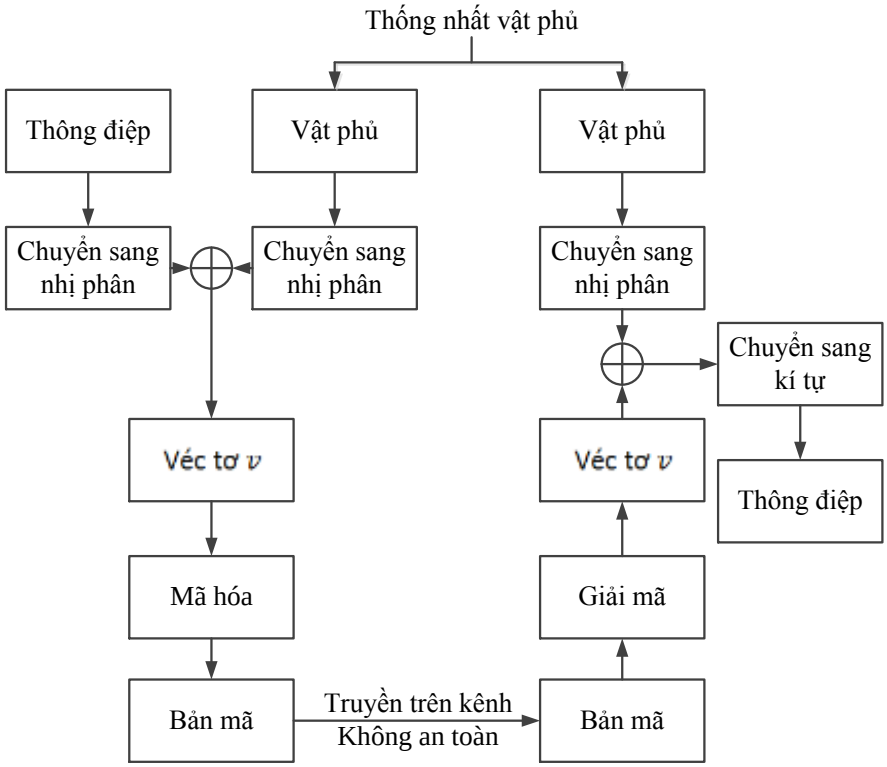
3.2.2 Thuật toán trích xuất

Bước 1: Giải mã để thu được véc tơ v sử dụng ánh xạ hỗn loạn

Bước 2: Chuyển ảnh phủ sang véc tơ nhị phân kí hiệu là c

Bước 3: Véc tơ $m = v\ xor\ c$

Bước 4: Chuyển véc tơ nhị phân m thành thông điệp.



Hình 1.*Mô hình kết hợp ẩn mã và mật mã không sửa vật phủ*

4. Phân tích và đánh giá

Thuật toán khá đơn giản trong việc thực hiện cũng như cài đặt với độ phức tạp tuyến tính. Việc thực hiện mã hóa sử dụng ánh xạ hỗn loạn trong bước 3 của quá trình nhúng tin làm tăng độ an toàn. Kẻ tấn công khi chặn bắt được véc tơ nhị phân sẽ chỉ giải mã được nếu như biết các tham số bí mật của hàm hỗn loạn mà hai bên đã sử dụng. Có thể thấy rằng, số lượng giá trị của các tham số bí mật này là vô hạn, do vậy đây cũng là một ưu điểm của việc đảm bảo an toàn dữ liệu khi dùng hàm hỗn loạn. Mặt khác, để biết được nội dung thực sự của thông điệp thì kẻ tấn công còn cần phải biết vật phủ tương ứng. Ngoài ra để tăng cường độ an toàn hơn nữa thì chúng ta hoàn toàn có thể lựa chọn các điểm ảnh một cách ngẫu nhiên rồi sau đó mới chuyển sang dạng nhị phân, thậm chí có thể thêm cả bước mã hóa thông điệp trước khi nhúng vào vật phủ. Rõ ràng với các biện pháp ẩn mã thông thường, để đạt được độ trong suốt thì cần phải hạn chế dung lượng thông điệp cần nhúng

trong mỗi điểm ảnh. Tuy nhiên với thuật toán này chúng ta có thể tận dụng tất cả các bit của mỗi điểm ảnh mà không phải quan tâm tới sự thay đổi của biểu đồ histogram hay giá trị PSNR. Ví dụ, với một ảnh phủ có kích thước $m \times n$, trong đó mỗi điểm ảnh được biểu diễn dưới dạng 8 bit thì dung lượng của thông điệp có thể nhúng vào là $8 \times m \times n$. Tất nhiên thuật toán cũng tồn tại nhược điểm đó là, kẻ tấn công dễ dàng biết được độ dài của thông điệp, bên cạnh đó nếu như các kỹ thuật ẩn mã thường sẽ không gây sự tò mò trong việc truyền tin cho kẻ tấn công thì thuật toán của chúng tôi chưa giải quyết được vấn đề này vì thông điệp gửi đi là một véc tơ đã được mã hóa. Ngoài ra vấn đề thống nhất vật phủ trong thực tế cũng không phải là một điều đơn giản. Mặc dù vậy, bằng việc mã hóa véc tơ, chúng tôi đã giảm nguy cơ lộ thông tin ngay cả khi kẻ tấn công biết được vật phủ đã được sử dụng. Chính vì vậy độ an toàn của thuật toán nằm ở sự bí mật của vật phủ cũng như các tham số của hàm hỗn loạn.

5. Kết luận

Trong bài báo này chúng tôi đã đưa ra một thuật toán ẩn mã mới kết hợp với mật mã nhằm nâng cao độ an toàn trong quá trình truyền tin. Ưu điểm của phương pháp này là không biến đổi vật phủ, dung lượng nhúng lớn hơn rất nhiều so với hầu hết các phương pháp ẩn mã khác. Hơn nữa thuật toán khá đơn giản và độ phức tạp chỉ là tuyến tính. Tất nhiên thuật toán cũng tồn tại những nhược điểm nhất định như kẻ tấn công dễ phán đoán được độ dài của thông điệp, gây sự chú ý đối với kẻ tấn công hay khó khăn trong việc thống nhất vật phủ

TÀI LIỆU THAM KHẢO

[1]. M. H. Rajyaguru, "CRYSTOGRAPHY-Combination of Cryptography and Steganography With Rapidly Changing Keys", *Int. J. Emerg Technol Ad. Eng*, 2(10), pp. 329-332, 2012.

[2]. Shamim Ahmed Laskar, Kattamanchi Hemachandran, "High capacity data hiding using LSB steganography and encryption", *International Journal Database Management Systems*, Vol.4, N0.6, 2012.

[3]. S. Gupta, A. Goyal, & B. Bhushan, "Information hiding using least significant bit steganography and cryptography", *International Journal of Modern Education and Computer Science*, 4(6), pp. 27, 2012.

[4]. K. Challita, & H. Farhat, "Combining steganography and cryptography: new directions", *International Journal of New Computer Architectures and their Applications (IJNCAA)*, 1(1), pp. 199-208, 2011.

[5]. Debiprasad Bandyopadhyay, Kousik Dasgupta, J. K. Mandal, Paramartha Dutta, "A novel secure image steganography method based on chaos theory in spatial domain", *International Journal of Security, Privacy and Trust Management (IJSPTM)*, Vol 3, No 1, 2014.

[6]. Anoop Kurmar Tiwari, Ajay Rajpoot, K. K. Shukla, S. Karthikeyan, "A Robust Method for Image Steganography based on chaos theory", *International Journal of Computer Applications*, (0975 – 8887) Volume 113 – No. 4, 2015.

[7]. A. Aswathy Nair, Deepu Job (2014), "A Secure Dual Encryption Scheme Combined With Steganography", *International Journal of Engineering Trends and Technology (IJETT)*, Volume 13, Number 5, 2014.

[8]. Dr. S. Bhargavi, M. J. Shobha, T. N. Swetha, M. J. Pushpa, "An image steganography based on logistic chaotic map in spatial domain", *International Journal of Research In Science & Engineering*, Volume 1 Special Issue 2.

[9]. Mohammad Ahmad Alia, Abdelfatah A. Yahya, "Steganography LSB Match", *European Journal of Scientific Research*, ISSN 1450-216X Vol. 40 No. 2, pp.223-231, 2010.

[10]. Gregory Kipper, *Investigator's guide to steganography*, CRC Press, ISBN-10: 0-8493-2433-5, 2004.

[11]. Neil F. Johnson, Zoran Duric, and Sushil Jajodia, *Information hiding: Steganography and watermarking-Attacks and countermeasures*, Springer-Science+Business media, LLC, ISBN-13: 978-1-4613-6967-7.

[12]. William Stallings, *Cryptography and Network Security: principles and practices*, pearsons education, first Indian reprint, 2003.