BỘ THÔNG TIN VÀ TRUYỀN THÔNG
HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

LÊ HẢI TRIỀU

NGHIÊN CỨU PHƯƠNG PHÁP BẢO MẬT THÔNG TIN GIẤU TRONG ẢNH SỐ

Chuyên ngành: Kỹ thuật viễn thông
Mã số: 9.52.02.08

TÓM TẮT LUẬN ÁN TIẾN SĨ KỸ THUẬT

HÀ NỘI – 2019

Công trình được hoàn thành tại Học viện Công nghệ Bưu chính Viễn thông, Bộ Thông tin và Truyền thông

Người hướng dẫn khoa học: GS, TSKH Đỗ Trung Tá

Phản biện 1:……
……
……

Phản biện 2:……
……
……

Phản biện 3:……
……
……

Luận án được bảo vệ trước Hội đồng chấm luận án tại Học viện Công nghệ Bưu chính Viễn thông.

Vào hồi: …… giờ …… ngày …… tháng …… năm ……

Có thể tìm hiểu thêm Luận án tại:
- Thư viện Quốc gia;
- Thư viện Học viện Công nghệ Bưu chính Viễn thông

A. Tính cấp thiết của đề tài

Sự phát triển bùng nổ của Internet đã tạo điều kiện cho các loại hình tấn công trái phép vào các hệ thống truyền tin cả về chiều rộng (trên quy mô toàn thế giới) lẫn chiều sâu (can thiệp vào hệ thống truyền tin). Mỗi ngày, các hệ thống truyền tin phải đối phó với hàng trăm đợt tấn công và gây ra những vấn đề tổn hại nghiêm trọng cả về nội dung và hạ tầng truyền dẫn. Vấn đề bảo vệ thông tin bằng mật mã đã và đang được nhiều quốc gia trên thế giới đặc biệt quan tâm, trong đó có rất nhiều các nghiên cứu tạo ra các chuẩn bảo mật, các hệ mật và giải pháp bảo mật chống lại tấn công cho hệ thống truyền tin. Theo quan điểm mật mã và yêu cầu thực tế, chúng ta không thể sử dụng các sản phẩm bảo mật thông tin của nước ngoài để bảo mật thông tin trên mạng thuộc phạm vi bí mật Nhà nước.

Xuất phát từ nhu cầu thực tế đó, nghiên cứu sinh đã lựa chọn luận án **"*Nghiên cứu phương pháp bảo mật thông tin giấu trong ảnh số*"**.

B. Mục tiêu, đối tượng, phạm vi và nhiệm vụ nghiên cứu

** Mục tiêu và phạm vi nghiên cứu của luận án như sau:*

Thứ nhất: Đề xuất thuật toán giấu tin mới trong ảnh số và trao đổi khóa bí mật bằng sinh số giả ngẫu nhiên và đánh giá độ an toàn của hệ thống mật mã và giấu tin trong ảnh số; *Thứ hai:* Nghiên cứu một số vấn đề về bảo mật ảnh số có đánh dấu watermark và hiệu suất mạng khi bị tấn công trong điều kiện thông thường. *Thứ ba:* Ứng dụng nội dung nghiên cứu trên vào thiết bị nghiệp vụ trong thông tin liên lạc bí mật bằng hình ảnh.

* *Đối tượng nghiên cứu:* gồm ảnh số, bảo mật thông tin giấu trong ảnh số và các yếu tố ảnh hưởng đến bảo mật mạng vô tuyến trong quá trình truyền ảnh số khi bị tấn công...

* *Phương pháp nghiên cứu:* thông qua một số cơ sở lý thuyết toán học, dựa trên các mô hình đề xuất để phân tích, đánh giá kết hợp với các thuật toán, công cụ thống kê và một số kết quả về đại số. Ngoài ra, luận án còn sử dụng phương pháp thực nghiệm, mô phỏng số nhằm đánh giá giải pháp đề xuất.

* *Nội dung nghiên cứu:* Thứ nhất *xây dựng thuật toán giấu tin mật trong ảnh số*; Thứ hai *xây dựng thuật toán sinh số giả ngẫu nhiên phục vụ thỏa thuận trao đổi khóa bí mật*; Thứ ba *xây dựng thuật toán đánh giá độ an toàn của hệ thống mật mã và giấu tin trong ảnh số;* Thứ tư *nghiên cứu, đánh giá hiệu năng lỗi và xác suất tìm thấy watermark nhúng trong ảnh số khi bị tấn công*; Thứ năm *đánh giá ảnh hưởng của thuật toán back-off đến hiệu suất mạng khi bị tấn công*; Thứ sáu *ứng dụng vào hệ thống liên lạc bí mật*.

C. Bố cục luận án gồm 4 chương

- Chương 1. Tổng quan về vấn đề nghiên cứu.

Thứ nhất *tổng quan về bảo mật khi truyền dữ liệu trên mạng viễn thông [T2].* Thứ hai *giới thiệu về giấu tin trong đa phương tiện và giấu tin trong ảnh số.* Thứ ba *là watermark và các nghiên cứu liên quan, từ đó phân tích, đánh giá khả năng an toàn bảo mật của mạng vô tuyến khi giấu thông tin trong ảnh số.*

- Chương 2. Bảo mật thông tin giấu trong ảnh số và trao đổi khóa bí mật.

Thứ nhất *luận án đề xuất thuật toán mã khóa khối 5 bit hiệu quả và đơn giản [T4],[T6].* Thứ hai *luận án đề xuất thuật toán sinh số giả ngẫu nhiên có chu kỳ cực đại bằng phương pháp đồng dư tuyến tính [T7].* Thứ ba*, luận án đề xuất thuật toán đánh giá độ an toàn của hệ thống sinh bít giả ngẫu nhiên tùy ý và sinh dãy giả ngẫu nhiên chữ cái latinh và đối với kỹ thuật giấu tin mật [T3].*

- Chương 3. Bảo mật ảnh số có đánh dấu watermark và hiệu suất mạng khi bị tấn công.

Thứ nhất *nghiên cứu và đánh giá so sánh hiệu năng lỗi của ảnh JPEG/JPEG2000 đã đánh dấu bảo mật bằng watermar khi truyền trên mạng vô tuyến, đề xuất phương pháp đánh dấu bảo mật watermark nào tốt nhất [T5],[T8].* Thứ hai *luận án đánh giá hiệu suất xử lý của các thuật toán back-off khác nhau trong điều kiện thông thường trên lớp MAC của IEEE 802.11 khi bị tấn công qua các mô hình đề xuất để đánh giá trạng thái thuật toán Back-off và trạng thái kênh và một số tham số [T9].*

- Chương 4. Xây dựng hệ thống thông tin liên lạc bí mật thông qua truyền ảnh số

Hệ thống này ứng dụng kỹ thuật giấu tin mật bằng thuật toán mã hóa và có trao đổi khóa bí mật vào ảnh số (chương 2) và đánh dấu bảo mật watermark lên ảnh số đó (chương 3)[T1].

Kết luận: *Luận án tóm tắt các kết quả nghiên cứu chính đã đạt được, nêu các đóng góp mới và đề xuất hướng nghiên cứu tiếp theo.*

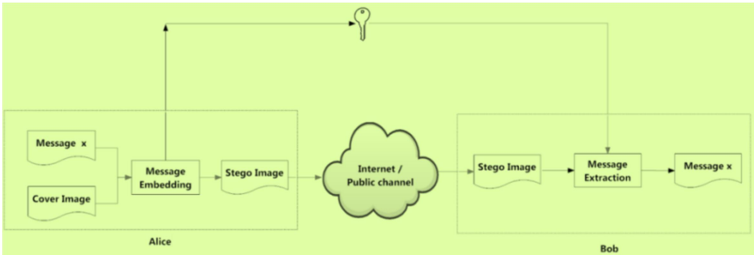
CHƯƠNG 1. TỔNG QUAN VỀ VẤN ĐỀ NGHIÊN CỨU

Tóm tắt: *Thứ nhất tổng quan về bảo mật khi truyền dữ liệu trên mạng viễn thông. Thứ hai giới thiệu về giấu tin trong đa phương tiện và giấu tin trong ảnh số. Thứ ba là watermark và các nghiên cứu liên quan, từ đó phân tích và đánh giá khả năng an toàn bảo mật của hệ thống khi giấu thông tin trong ảnh số.*

1.1. Một số vấn đề về an ninh, an toàn và bảo mật thông tin trên mạng viễn thông

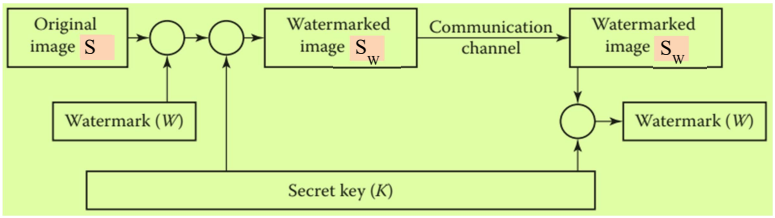
1.2. Bảo mật thông tin giấu trong ảnh số

1.2.3. Kỹ thuật giấu tin mật trong ảnh số và nghiên cứu liên quan



Hình 1. 7. Sơ đồ quá trình giấu tin trong ảnh

1.2.5. Kỹ thuật đánh dấu watermark và nghiên cứu liên quan



Hình 1. 10. Sơ đồ tổng quát watermark (Digital Watermarking)

1.3. Đánh giá khả năng an toàn của hệ thống khi bị tấn công

1.3.1. Đánh giá hiệu suất bảo mật ảnh có đánh dấu watermark

Đánh dấu bảo mật watermark được xem là một cách tiếp cận đầy hứa hẹn cho việc đảm bảo nhận thực, bảo mật và bảo vệ bản quyền kỹ thuật số nhờ việc xử lý đơn giản so hơn với những tiếp cận thông thường. Qua những tìm hiểu của NCS, chưa có một nghiên cứu đầy đủ nào trước đây nhằm so sánh hiệu năng lỗi khi dùng các thuật toán biến đổi khác nhau cũng như việc đánh giá xác suất phát hiện watermark là vấn đề quan trọng đối với an ninh bảo mật trong mạng WSN khi bị tấn công.

1.3.2. Đánh giá độ an toàn của kỹ thuật watermark trong truyền ảnh số trên mạng viễn thông

Trong phạm vi nghiên cứu của mình, luận án chỉ tập trung vào giải quyết vấn đề đánh giá độ an toàn và hiệu năng chống lại các tấn công kỹ thuật watermark đối với ảnh số.

1.3.3. Đánh giá hiệu suất xử lý xung đột lên mạng khi bị tấn công

Khi mạng IEEE 802.11 bị tấn công, từ một nút bình thường do quá trình back-off nút đó trở thành nút lỗi sẽ dẫn đến hạ hiệu suất hoạt động mạng ngay từ lớp vật lý (lớp MAC). Do đó, việc đóng băng back-off đối với các nút lỗi là vấn đề mấu chốt ảnh hưởng đến hiệu suất mạng. Trong các nghiên cứu trước đây chưa xem xét đồng thời cả vấn đề đóng băng back-off và thuật toán EIED để có đánh giá đầy đủ. Theo tìm hiểu của NCS, việc đánh giá hiệu suất xử lý của các thuật toán back-off khác nhau thông qua phân tích các tham số *lưu lượng truy cập, tỷ lệ rớt gói tin hay độ trễ* của lớp MAC trong 802.11 cũng chưa được đề cập đến trong các nghiên cứu gần đây.

1.5. Kết luận chương 1

Thứ nhất: Nghiên cứu tổng quan về an ninh an toàn và bảo mật trong truyền ảnh số trên mạng vô tuyến; *Thứ hai:* Tìm hiểu về các giấu tin mật trong ảnh số và trao đổi khóa bí mật; *Thứ ba:* Tìm hiểu về digital watermarking và nghiên cứu liên quan; *Thứ tư:* Đánh giá hiệu năng lỗi khi bị tấn công trên mạng IEEE 802.11 lớp MAC có đánh dấu watermark.

CHƯƠNG 2. BẢO MẬT THÔNG TIN GIẤU TRONG ẢNH SỐ VÀ TRAO ĐỔI KHÓA BÍ MẬT

Tóm tắt: *Chương này nghiên cứu về kỹ thuật giấu tin trong ảnh số, kỹ thuật trao đổi khóa bí mật và đánh giá chất lượng hệ thống mật mã cũng như giấu tin [T3],[T4],[T5].*

2.1. Thuật toán giấu tin mật trong ảnh số

2.1.3. Thuật toán giấu tin ban đầu và thuật toán cải tiến trước đây

2.1.3.1. Thuật toán giấu tin ban đầu

Thuật toán giấu tin này khá đơn giản. Tuy nhiên trong thực tế độ dài l(m) của bản tin thường bé hơn độ dài l(c) của ảnh môi trường, hơn nữa việc giấu tin lại tuần tự nên kẻ tấn công lợi dụng các nhược điểm này để có thể phát hiện được ảnh có giấu dữ liệu bên trong đó hay không bằng phân tích thống kê cấp 2 (bằng mô hình markov ẩn).

2.1.3.2. Thuật toán cải tiến trước đây đối với thuật toán giấu tin ban đầu

Thuật toán cải tiến (2.1.3.2) đã được trình bày ở trên cũng như nhiều thuật toán giấu tin khác đã được công bố rất khó chống lại được các phương pháp phát hiện bằng thuật toán thống kê cấp 1 hoặc cấp 2 nếu như tỷ lệ số bit LSB của ảnh số bị thay đổi lớn hơn 30% trên tổng số bit LSB của ảnh.

2.1.4. Thuật toán giấu tin mới dựa trên mã hóa khối 5 bit

2.1.4.3. Xây dựng bộ mã cho 26 ký tự La tinh (a, b, c,...,z)

Trước khi xây dựng thuật toán giấu tin mới, ta xây dựng một ma trận H có cấp 5x31 như trong bảng 2.3 dưới đây. Trong đó, Ma trận H được sử dụng dựa trên cơ sở bộ mã sửa sai Hamming trong thông tin liên lạc số. Ý nghĩa của việc xây dựng ma trận H chính là chỉ làm thay đổi 1 bít (nhúng 1 bít) đối với độ dài từ mã là 5 bít, nhằm giảm tỷ lệ nhúng tin xuống nhưng đồng thời tăng được lượng tin giấu nhiều hơn.

Bảng 2. 3. Ma trận H 5 x31

1	0	0	0	0	1	0	0	1	0	1	1	0	0	1	1	1	1	1	0	0	0	1	1	0	1	1	1	0	1	0
0	1	0	0	0	0	1	0	0	1	0	1	1	0	0	1	1	1	1	1	0	0	0	1	1	0	1	1	1	0	1
0	0	1	0	0	1	0	1	1	0	0	1	1	1	1	1	0	0	0	1	1	0	1	1	1	0	1	0	1	0	0
0	0	0	1	0	0	1	0	1	1	0	0	1	1	1	1	1	0	0	0	1	1	0	1	1	1	0	1	0	1	0
0	0	0	0	1	0	0	1	0	1	1	0	0	1	1	1	1	1	0	0	0	1	1	0	1	1	1	0	1	0	1

2.1.4.4. Đề xuất thuật toán giấu tin mới

Đầu vào:

+ Bản bản tin $m=m_1m_{2...}m_{l(m)}$ với $m_i \in \{0,1\}$ $i=1,2,..,l_{(m)}$

+ Ảnh cover $C=C_1C_2,\ldots C_{l(c)}$ với $C_i \in \{0,1\}$; $i=1,2,..,l_{(c)}$

Đầu ra:

+ Ảnh Stego S đã giấu tin, ta ký hiệu S=C(m)

Bước 1: Mã hóa bản tin m với thuật toán DES với khóa ở bảng 2.2 và kết quả ta nhận được bản mã $y=E_{DES}(m) = y_1y_2,\ldots,y_{l(m)}y_i \in \{0,1\}$ $i=1,2,..,l_{(m)}$.

Bước 2: Tạo ảnh thứ cấp $C_0 = x_{i0}, x_{i0+1},\ldots x_{i0+l(c)}$. $x_i \in \{0,1\}$, $i=i_0,\ldots.,i_{0+l(c)}$ bằng cách quy ước chọn 1 chỉ số i_0 nào đó của pixel dữ liệu ảnh cover C và trích chọn các LSB của các điểm ảnh có hệ số bắt đầu từ $i_0 = 1,2,\ldots l$ (người gửi và người nhận thống nhất trước).

Bước 3: Chia C_0 thành từng block, mỗi block gồm 31 bít, tính từ khởi điểm x_{i0}, ta được $C_0 = C_0(1)\ C_0(2)\ ....\ C_0\ ([\frac{l(c)}{31}])$ $[\frac{l(c)}{31}]$ là phần nguyên

Bước 4: Chia căn bản mã y thành từng khối, mỗi khối 5 bit và được kết quả là: $Y = y(1)\ y(2)\ ....\ (y[\frac{l(m)}{5}] + 1)$

Bước 5: Với i = 1, 2, ..., [l(m)/5] + 1, thực hiện $Z^T(i) = y^T(i) \oplus HC^T(i)$ (trong đó C^T là véc tơ chuyển vị của véc tơ C, H là ma trận được sử dụng dựa trên cơ sở bộ mã sửa sai Hamming trong thông tin liên lạc số, bảng 2.3).

Bước 6: Với i = 1, 2, ... ,[l(m)] + 1;Tìm trong ma trận H, nếu tồn tại j_0, với $j_0 = 1, 2, ..., 31$ sao cho $y^T(i)= h_{j0}$ thì ta thực hiện đảo bit của véc tơ $C_0(i)$ tại vị trí j_0: $X'_{j0} = X_{j0} + 1$ và thay X'_{j0} vào vị trí của X_{j0} của véc tơ $C_0(i)$. Sau khi thay X'_{j0} ta có $C_0(i) = X'_0(i)$, với $X_0(i) + 1$, ..., $X_0(i) + 31$.

Nếu không tồn tại j_0 sao cho $y^T(i)= h_{j0}$ thì bỏ qua và quay lại Bước 5.

Bước 7: Ảnh thứ cấp mà ta đã thực hiện trên ký hiệu là C_1.

Bước 8: Trả lại ảnh thức cấp C_1 vào đúng vị trí ban đầu như khi ta trích chọn C_0. Cuối cùng ta nhận được ảnh Stego S.

2.1.4.5. Kết quả đánh giá so sánh thuật toán mới và thuật toán cũ

Bảng 2. 1. So sánh PSRN giữa hai thuật toán khi độ dài bản tin không đổi và kích thước ảnh thay đổi

STT	*Kích thước ảnh thay đổi*	*Độ dài bản tin giấu không đổi (ký tự)*	*Tỷ số PSRN của thuật toán giấu tin 5 bit mới (dB)*	*Tỷ số PSRN của thuật toán giấu tin cũ (dB)*
1	*100⊗100*	*1946*	***54,01***	***32,50***
2	*300⊗168*	*1946*	***60,98***	***35,98***
3	*275⊗183*	*1946*	***61,00***	***36,10***
4	*183⊗276*	*1946*	***61,02***	***36,81***
5	*268⊗175*	*1946*	***61,03***	***36,88***
6	*255⊗255*	*1946*	***61,15***	***36,94***
7	*600⊗401*	*1946*	***68,74***	*40,34*
8	*706⊗504*	*1946*	***69,92***	*42,38*
9	*768⊗512*	*1946*	***69,96***	*42,46*
10	*816⊗616*	*1946*	***71,12***	*43,13*

2.2. Thuật toán sinh số giả ngẫu nhiên có chu kỳ cực đại bằng phương pháp đồng dư tuyến tính

2.2.2. Đặt bài toán

Xét phương trình đồng dư tuyến tính có dạng sau:

$$ax \equiv b \bmod n \qquad (2.5)$$

với a,b,n là các tham số nguyên, trong đó $n \geq 2$

Để giải phương trình (2.3) ta áp dụng các định lý sau:

2.2.2.1. Định lý 1

Gọi gcd*(a,n)=d≥1* hàm trả về ước số chung lớn nhất của *a* và *n:*

a) (2.5) có *d* nghiệm phân biệt nếu *b* chia hết cho *d* (k/hiệu *d|b*).

b) (2.5) vô nghiệm nếu *b* không chia hết cho *d* (ký hiệu $d \nmid b$).

**** Trường hợp 1:*** có *d* nghiệm phân biệt nếu *b* chia hết cho *d* (ký hiệu *d|b*), có thể viết như sau gcd*(a,n)=d* nếu *b|d*.

Khi đó phương trình (2.5) có thể viết lại như sau:

$$a_1 dx \equiv b_1 d \bmod n_1 d \tag{2.8}$$

với a_1, b_1, n_1 là những số nguyên nào đó.

Áp dụng bổ đề trên của phép toán đồng dư từ (2.5) ta suy ra:

$$a_1 x = b_1 \bmod n_1 \tag{2.9}$$

Do $\gcd(a_1, n_1) = 1$ (vì gcd*(a,n)=d*) nên theo bổ đề 1 có tồn tại $a_1^{-1} mod\ n_1$, mà

$x_0 = a_1^{-1} mod\ n_1$là nghiệm duy nhất của phương trình (2.9) với $0 \le x_0 \le n_1$

Vì *d=1+1+..+1* nên (2.5) có *d* nghiệm phân biệt là:

$x_j = \left[\left(b/d\right)x^* + j\left(n/d\right)\right] mod\ n$, với $x^* = \left(a/d\right) mod \left(n/d\right) = a_1^{-1} mod\ n$

Như vậy ta có *d* giá trị của *x với* $x = x_0 + jn_1 mod\ n$; *(j=0,1,2,...,d-1)* là nghiệm của phương trình (2.5) và chúng khác nhau theo modulo n. Trường hợp 1 được giải quyết.

**** Trường hợp 2:*** vô nghiệm nếu *b* không chia hết cho *d* (k/hiệu $d \nmid b$)

Theo Định lý 1 ta sẽ xây dựng dãy số giả ngẫu nhiên. Bài toán đặt ra hãy xây dựng dãy giả ngẫu nhiên $\{x_n\}, n \ge 0$ sao cho chu kỳ của dãy là lớn nhất có thể, tức là $\{x_n\}$ là m dãy. Ta có dãy $x_{n+1} \equiv (ax_n + b) mod\ m$, trong đó x_0, a, b, m cho trước sao cho $m > \max\{x_0, a, b\}$. Rõ ràng dãy $\{x_n\}, n \ge 0$ phụ thuộc vào 4 tham số a, b, x_0, m. Dãy này

tuần hoàn và cho chu kỳ $R \leq m$, tùy thuộc vào việc chọn a,b và x_0. Mục tiêu của bài toán là hãy xác định các tham số a,b và x_0 để $R=m$.

Chứng minh trường hợp 2 như sau: Theo trường hợp 1, nếu b chia hết cho d, thì có thể viết lại d = gcd (a,n).

Do dó, giả thiết tồn tại một số nguyên x_0 thỏa mãn phương trình (2.5). Vì gcd$(a,n) = d > 1$, nên phương trình (2.5) được viết như sau:

$$a_1 d x_0 \equiv b \bmod (n_1 d) \tag{2.10}$$

Trong đó a_1, b_1 là những số nguyên. Từ đó ta suy ra: $a_1 d x_0 = b + k n_1 d$ với k là một số nguyên nào đó. Ta có:

$$a_1 d x_0 - k n_1 d = b, \text{ hay } (a_1 x_0 - k n_1) d = b \tag{2.11}$$

Suy ra $a_1 x_0 - k n_1 = b/d$ là số nguyên. Tuy nhiên do trường hợp 2 ta đã chọn b không chia hết cho d nên b/d không phải là số nguyên, trong khi đó, theo chứng minh trên, $a_1 x_0 - k n_1$ là một số nguyên.

Kết quả này mâu thuẫn với giả thiết trên. Vậy không tồn tại nghiệm nguyên x_0 thỏa mãn phương trình đồng dư (2.5). Trường hợp thứ 2 được chứng minh.

2.2.2.2. Định lý 2

Để dãy $\{x_n\}, n \geq 0$ được xác định trong (2.5) có chu kỳ $R=m$ phải thỏa mãn đồng thời 3 điều kiện sau:

i) $(b,m)=1$;

ii) $a-1$ là bội của p với mọi ước nguyên tố p của m với $p \geq 2$, trong đó p là một ước của m;

iii) $a-1$ là bội của 4 nếu m là bội của 4.

Ta xét phương trình đồng dư tuyến tính có dạng:

$$x \equiv ax+b \bmod m \tag{2.12}$$

$$\text{hay } (a-1)x \equiv -b \bmod m \tag{2.13}$$

Từ điều kiện (ii) ta suy ra rằng: $(a-1,m) = p > 1$

Trong lúc đó, theo (i) ta có: $(b,m) = 1 \neq p$

Từ đó (2.12) hoặc tương đương với (2.13) vô nghiệm với $x_n \neq x_{n+1}$ trong khoảng (0,m). Tức là không tồn tại một $n \geq 0$ sao cho: $x_n = (ax_n + b) mod\ m$ đối với $\forall n=1,2,...,m$. Định lý được chứng minh.

2.3. Phương pháp và thuật toán đánh giá độ an toàn hệ thống mật mã và giấu tin trong ảnh số

2.3.3. Phương pháp đánh giá độ an toàn của hệ thống mật mã

2.3.3.1. Phân tích độ an toàn của hệ thống mật mã

Để đánh giá độ an toàn của một hệ thống mật mã, ta cần đánh giá chất lượng của dãy giả ngẫu nhiên do hệ thống sinh (generator) tạo ra. Nội dung bài toán như sau: Giả sử trên cơ sở nào đó, người ta đưa ra hai giả thuyết thống kê đối lập nhau, lần lượt được ký hiệu là giả thuyết H_0 và đối thuyết H_1; H_0: Hệ thống sinh dãy giả ngẫu nhiên theo mô hình Markov với ma trận chuyển

$$P_0 = (\frac{1}{26})_{26x26} = (P_{ij})_{26x26} \quad (2.14)$$

H_1 Hệ thống sinh dãy giả ngẫu nhiên theo mô hình Markov $q_1 = (q_{ij})_{26x2}$, trong đó q_{ij} cho trước hoặc ước lượng được bằng phương pháp thống kê toán học. Để kiểm tra xem giả thuyết nào đúng trong hai giả thuyết đưa ra, ta lấy mẫu giả ngẫu nhiên $X = x_1, x_2, .., x_n$ ($n \geq 2$) rồi tính đặc trưng phân bố xác suất của X. Nếu đặc trưng đó có tương ứng với giả thuyết không (H_0) thì ta chấp nhận giả thuyết H_0 và do đó bác bỏ giả thuyết H_1. Ngược lại thì ta chấp nhận giả thuyết H_1 và bác bỏ giả thuyết H_0.

2.3.3.2. Xây dựng thuật toán đánh giá an toàn đối với hệ thống sinh bít giả ngẫu nhiên tùy ý

a. Thuật toán 1: Cho một dãy bít giả ngẫu nhiên được sinh từ hệ thống sinh nào đó: $X = x_1x_2 \dots x_n;\ x_i \in \{0,1\}; i = 1,2,..,n$. Vẫn chọn $\varepsilon=0,1$

Bước 1: Tính tần số bộ đôi móc xích của dãy *X* và nhận được kết quả

$$P = \begin{pmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{pmatrix}$$

Bước 2: Tính $Q = (q_{ij})_{2x2}$ trong đó $q_{ij} = \left[log_2 \frac{n}{4m_{ij}} \right]$

Bước 3: Tính $S(x) = \sum_1^2 \sum_1^2 \frac{n}{4} q_{ij}$

Bước 4: Nếu ε = 0,05 thì hệ thống có độ an toàn tốt với xác suất 97% và hệ thống dừng. Trái lại,

Bước 5: Hệ thống không an toàn và kết thúc

b. Thuật toán 2: Áp dụng định lý được cho trong [65], ta có:

Cho dãy nhị phân $X = x_0 x_1 \dots x_{n-1}$, độ dài *n*

Lấy và cố định số nguyên d: $1 \le d \le \left[n/2 \right]$ (phần nguyên của n/2)

Đặt $A(d) = \sum_{i=0}^{n-d-1} (x_i \oplus x_{i+d})$. Nếu n-d≥10,

ta có: $\lambda = \left. 2\left(A(d) - \frac{n-d}{2}\right) \right/ \sqrt{n-d}$ sẽ có phân bố xấp xỉ phân bố chuẩn *N(0,1)*.

Điều này có nghĩa là: Cho trước xác suất sai lầm loại 1, giả sử lấy α = 0,05. Khi đó tra bảng phân phối chuẩn ta xác định được ngưỡng$t_\alpha = 1{,}6449$ [65].

Khi đó nếu

$2\left(A(d) - \frac{n-d}{2}\right) < t_\alpha \sqrt{n-d} = 1{,}6449\sqrt{n-d}$ thì ta chấp nhận dãy *X* là tốt; trái lại thì ta coi dãy *X* được sinh ra từ bộ sinh là không tốt.

2.3.3.3. Xây dựng thuật toán đánh giá an toàn đối với hệ thống dãy giả ngẫu nhiên chữ cái Latinh

Xét trên bảng chữ cái La tinh $Z_{26} = \{a, b, c, .., z\}$ hay ={0,1,2,3,..,25}. Tiếp theo, lấy 2 mẫu văn bản tiếng Anh tùy ý một cách độc lập, mỗi mẫu *X, Y* có độ dài như nhau và bằng *n* (cỡ 10000 chữ cái) mà ta ký hiệu là

$$X = x_1, x_2, .., x_n$$

$$Y = y_1, y_2, .., y_n$$

Bước 1: Cộng $(x + y) mod 26 = Z = z_1, z_2, .., z_n$

Bước 2: Tính tần số bộ đôi móc xích của dãy *Z*, ta được kết quả $G = (g_{ij})_{26x26}$

Bước 3: Tính $H = (h_{ij})_{26x}$. Trong đó, $h_{ij} = \left[Klog\frac{0,0015}{g_{ij}}\right]$; *i , j =1,2,..,26*

Với *K* là một số nguyên dương nào đó (K≥1). Trong thực hành, ta chọn *K=10*. Mục đích chọn số *K* là làm tăng độ chính xác của kết luận, tức là giảm thiểu trường hợp $[logx] = 0$. Chẳng hạn lấy x = 1,2 và logarit là ln. Khi đó:

[ln1,2]=[0,1820]=0. Tuy nhiên [10ln1,2]=[1,820]=1

Bây giờ giả sử ta cần kiểm tra một dãy sinh $S = s_1 s_2 ... s_m$ với *m≥1;* $s_i \in \{a,b,..,z\}$; $i = \overline{1,m}$

Bước 1: Tính tần số bộ đôi móc xích của dãy *S*, ta nhận được kết quả là ma trận *Q*

$$Q = (q_{ij})_{26x26};\ q_{ij} \geq 0; i, j = 1,2,..,m$$

Bước 2: Tính vết $Tr(Q.H^T)$, trong đó H^T là ma trận chuyển vị của ma trận *H*

Bước 3: Nếu giá trị $Tr(Q.H^T) > 0$ thì dãy *S* được sinh ra từ bộ sinh dãy giả ngẫu nhiên nào đó là tốt.

Trái lại nếu $Tr(Q.H^T) < 0$ thì dãy *S* là không tốt và thuật toán dừng. Trường hợp $Tr(Q.H^T) = 0$ thì chưa có kết luận mà ta cần lấy tiếp mẫu *S* có độ dài lớn hơn *m* và tiếp tục quay về Bước 1.

Bước 4: Bổ sung thêm mẫu *s* thành *s'* để có độ dài *m'>m* và quay lại Bước 1.

2.3.4. Phương pháp đánh giá độ an toàn của kỹ thuật giấu tin

2.3.4.1. Độ an toàn của thuật toán giấu tin

Đặt *C* là tập các ảnh gốc *c*, *M* là tập thông tin cần giấu *m*, S tập các ảnh giấu tin s và K tập khóa giấu tin *k*. Một thuật toán giấu tin nói chung được biểu diễn theo quan hệ của (S_E, S_X). Trong đó S_E là thuật toán nhúng tin được biểu diễn C x M x K => S_E và S_X được trích tin theo S x K => M. Hàm nhúng tin S_E tạo ra tập S và hàm S_X trích thông tin M từ tập S bằng khóa K.

Cho Ω là một hệ thống giấu tin mật (Steganography). $P_S(.)$ là phân bố xác suất của tập ảnh giấu tin S khi gửi qua kênh công cộng và $P_C(.)$ là phân bố xác suất của ảnh gốc C.

Theo định nghĩa hệ thống Ω được gọi là an toàn nếu sai phân Kullback – Leibler giữa hàm mật độ xác xuất P_C và P_S theo $D(P_S \,||P_C) = 0$ theo (2.15), với D được tính theo công thức dưới đây:

$$D(P_C \,||P_S) = \sum_{c \in C} P_1\,(p) log \frac{P_C(c)}{P_S(c)} \qquad (2.15)$$

Khi $D(P_S \,||P_c) \leq \varepsilon$ với ε ≥ 0 thì thuật toán giấu tin cho trước có độ an toàn ε, trong đó ε là một số thực dương cho trước.

2.3.4.2. Xây dựng thuật toán đánh giá an toàn đối với hệ thống giấu tin mật

Cho C là ảnh cover, còn *S* là ảnh stego đã được giấu thông điệp với tỉ lệ nào đó và cho trước ε = 0,05

Bước 1: Trích chọn *n* bit LSB của ảnh cover *C* và *n* bit LSB của ảnh stego *S* tương ứng (cùng khởi điểm giấu). Ta nhận được kết quả lần lượt là:

$c_1 c_2 \dots c_n$ và $s_1 s_2 \dots s_n$; $c_i, s_i \in \{0,1\}, i = 1,2,..,n$

Bước 2: Tính tần số bộ đôi móc xích lần lượt của 2 dãy $\{c_1 c_2 \dots c_n\}$ và $\{s_1 s_2 \dots s_n\}$ ta được kết quả $P_c(x)$ và $P_s(x)$ như sau:

$$P_c = \begin{pmatrix} p_{11} & p_{12} \\ p_{21} & p_{22} \end{pmatrix} \quad P_s = \begin{pmatrix} q_{11} & q_{12} \\ q_{21} & q_{22} \end{pmatrix}$$

Bước 3: Tính

$$D(P_c \,//\, P_s) = \sum_{i=1}^{2}\sum_{j=1}^{2} P_c\,(i,j) log_2 \frac{P_c(i,j)}{P_s(i,j)}$$

Trong đó, $P_c(i,j) = p_{ij}; i,j = 1,2;\ P_s(i,j) = q_{ij}; i,j = 1,2$

Bước 4: Nếu $D(P_c \,//\, P_s) \leq 0{,}05$ thì hệ thống là đáng tin cậy với mức an toàn trên 95% và thuật toán dừng.

Bước 5: Nếu lớn hơn 0,05 hệ thống không đáng tin cậy.

2.4. Kết luận chương 2

Bảng 2. 2. Kết quả Sai phân D(Pc//Ps) đánh giá độ an toàn của thuật toán 2.1.4 theo kích thước ảnh không đổi/thay đổi tương ứng độ dài bản tin thay đổi/không đổi

STT	***Kích thước ảnh không đổi***	***Độ dài bản tin giấu thay đổi (ký tự)***	***Sai phân Kullback - Leibler D(P_C//P_S)***
1	*768⊗512*	*1038*	*0,000002082044841*
2	*768⊗512*	*2076*	*0,000006713339210*
3	*768⊗512*	*3114*	*0,000014087722528*
4	*768⊗512*	*4152*	*0,000026829523768*
5	*768⊗512*	*5190*	*0,000039290342406*
6	*768⊗512*	*6228*	*0,000055130897602*
7	*768⊗512*	*7266*	*0,000070708671449*
8	*768⊗512*	*8304*	*0,000085734489423*
9	*768⊗512*	*12456*	*0,000192297577694*
10	*768⊗512*	*19722*	*0,000750944583946*
STT	***Kích thước ảnh thay đổi***	***Độ dài bản tin giấu không đổi (ký tự)***	***Sai phân Kullback - Leibler D(P_C//P_S)***
1	*100⊗100*	*1946*	*0,0995662169714835*
2	*183⊗276*	*1946*	*0,0066124957907429*
3	*275⊗183*	*1946*	*0,0007075414552164*

4	*288⊗175*	*1946*	*0,0099152602771983*
5	*300⊗168*	*1946*	*0,0005286474040050*
6	*225⊗225*	*1946*	*0,0044478103637885*
7	*660⊗440*	*1946*	*0,0000020054366442*
8	*706⊗504*	*1946*	*0,0000094963145847*
9	*768⊗512*	*1946*	*0,0000064135151950*
10	*816⊗616*	*1946*	*0,0000061077702080*

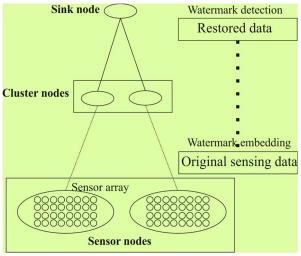
Thứ nhất: Đối với kỹ thuật giấu tin mật, luận án đề xuất thuật toán mã khóa khối 5 bit hiệu quả và đơn giản, bảo đảm cân đối giữa tốc độ tính toán và độ phức tạp của thuật toán. *Thứ hai:* Đối với hệ thống mật mã trao đổi khóa bí mật, luận án đề xuất thuật toán sinh số giả ngẫu nhiên có chu kỳ cực đại bằng phương pháp đồng dư tuyến tính. *Thứ ba:* Từ đó, luận án đề xuất các thuật toán đánh giá độ an toàn của hệ thống sinh bít giả ngẫu nhiên tùy ý, hệ thống sinh dãy giả ngẫu nhiên chữ cái latinh và đối với kỹ thuật giấu tin mật.

CHƯƠNG 3. BẢO MẬT ẢNH SỐ CÓ ĐÁNH DẤU WATERMARK VÀ HIỆU SUẤT MẠNG KHI BỊ TẤN CÔNG

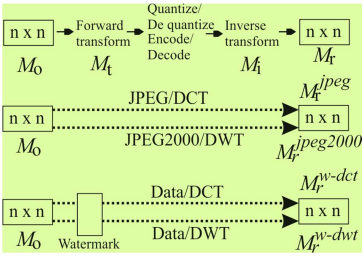
Tóm tắt: *Mục tiêu chương này giải quyết hai vấn đề. Thứ nhất xây dựng thuật toán đánh giá và so sánh về hiệu suất xử lý ảnh JPEG/JPEG2000 có đánh dấu bảo mật bằng watermark trong quá trình truyền ảnh số. Thứ hai, phân tích khả năng và đánh giá hiệu suất xử lý xung đột của các thuật toán back-off khác nhau lên mạng vô tuyến khi bị tấn công trong khi truyền ảnh số [T2][T6],[T7].*

3.1. Bảo mật ảnh số thông qua đánh giá và so sánh về hiệu suất xử lý ảnh JPEG/JPEG2000 có đánh dấu watermark

3.1.2. Các giả định và mô hình thực tế



Hình 3. 1. Mô hình WSN



Hình 3. 2. Các kịch bản xử lý ảnh

Trong đó:

- Ma trận M_O là ma trận điểm ảnh ban đầu
- Ma trận M_t là ma trận chuyển đổi theo từng DCT/DWT
- Ma trận M_i là ma trận chuyển đổi ngược
- Ma trận M_r là ma trận điểm ảnh nhận được

Xét cấu hình WSN điển hình được minh họa trong hình 3.1. Mạng bao gồm các nút cảm biến (sensing node), nút cụm (cluster node) và nút đích (sink node). Dựa trên biểu đồ mô tả quá trình xử lý ảnh như trên, một số kịch bản được thiết lập để đánh giá hiệu năng lỗi trong quá trình xử lý được trình bày như hình 3.2.

3.1.3. Các phương trình biến đổi

- *Phương trình biến đổi thuận*

$$Y(u,v) = \frac{2}{N}C(u)C(v) \times \sum_{x=0}^{N-1}\sum_{y=0}^{N-1} X(x,y)\cos\frac{\pi(2x+1)u}{2N}\cos\frac{\pi(2y+1)v}{2N} \quad (3.1)$$

Với $u = 0,\ldots,N-1$ và $v = 0,\ldots,N-1$

- Đối với ma trận 8x8, khi đó $N=8$ và $C(k) = \begin{cases} \frac{1}{\sqrt{2}} \text{ đối với } k = 0 \\ 1 \text{ còn lại} \end{cases}$

- *Phương trình biến đổi ngược*

$$(u,v) = \frac{2}{N}\sum_{x=0}^{N-1}\sum_{y=0}^{N-1} C(u)C(v)Y(x,y) \times \cos\frac{\pi(2x+1)u}{2N}\cos\frac{\pi(2y+1)v}{2N} \quad (3.2)$$

3.1.4. Kết quả mô phỏng và đánh giá

Để so sánh mức độ hiệu quả của các phép biến đổi dựa trên mô hình đề xuất, bốn trường hợp giả thiết bao gồm: (1) dữ liệu ảnh JPEG,

(2) dữ liệu ảnh JPEG2000, (3) dữ liệu đã được watermark sử dụng DCT, (4) dữ liệu đã được watermark sử dụng DWT. Dữ liệu ảnh được khởi tạo ngẫu nhiên bởi hàm Gauss, tương ứng với dữ liệu đầu vào M_0. Ngoài ra, dữ liệu watermark được trải phổ bởi chuỗi trải phổ trực tiếp DSSS trong quá trình truyền.

Gọi $M_r^{jpeg}, M_r^{jpeg2000}, M_r^{w-dct}, M_r^{w-dwt}$ và $M_e^{jpeg}, M_e^{jpeg2000}, M_e^{w-dct}, M_e^{w-dwt}$ tương ứng là ma trận dữ liệu được khôi phục tại phía thu và các ma trận lỗi của dữ liệu JPEG, JPEG2000, dữ liệu DCT watermark và dữ liệu DWT watermark.

Với kết quả tính toán toán ở trên, các tham số hiệu năng lỗi thu được như sau.

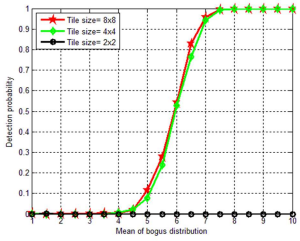
$$MAE_e^{jpeg} = 3.44;\ MSE_e^{jpeg} = 17.66;\ PSNR_e^{jpeg} = 35.57dB$$

$$MAE_e^{jpeg2000} = 3.44;\ MSE_e^{jpeg2000} = 17.66;\ PSNR_e^{jpeg2000} = 35.57dB$$

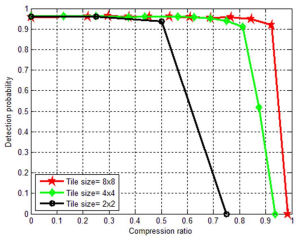
$$MAE_e^{w-dct} = 2.69;\ MSE_e^{w-dct} = 11.75;\ PSNR_e^{w-dct} = 37.43dB$$

$$MAE_e^{w-dwt} = 1.22;\ MSE_e^{w-dwt} = 2.44;\ PSNR_e^{w-dwt} = 44.26dB$$

Trong hình 3.4, với p_f =0,1% và CR = 75%, xác suất tìm thấy watermark đối với trường hợp 2x2 gần như bằng 0 với mọi giá trị trung bình của độ lớn watermark trong khi trường hợp còn lại xấp xỉ 95% khi giá trị trung bình của watermark bằng 7. Với tỷ số nén khác nhau, xác suất tìm thấy watermark đột ngột giảm về 0 như hình 3.5.

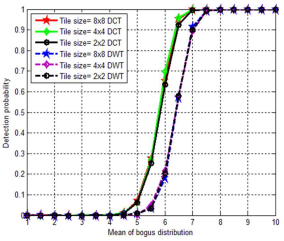


Hình 3.4. Xác suất tìm thấy watermark với các độ lớn trung bình khác nhau

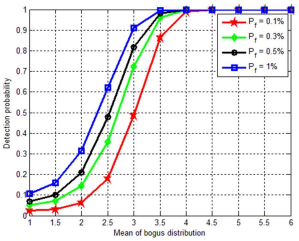


Hình 3.5. Xác suất tìm thấy watermark với tỷ số nén thay đổi

Để so sánh xác suất tìm thấy watermark cho hai phương thức biến đổi DCT và DWT, luận án thực hiện các độ lớn trung bình watermark khác nhau với cùng tỷ số nén. Kết quả hình 3.6 mô tả xác suất tìm thấy watermark gần như bằng nhau với các kích thước khác nhau trên cùng một phương thức biến đổi. Tuy nhiên, xác suất tìm thấy khi sử dụng biến đổi DCT lớn hơn.

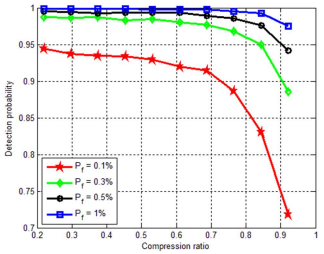


Hình 3.6. Xác suất tìm thấy watermark DCT và DWT



Hình 3.7. Xác suất tìm thấy watermark bị ảnh hưởng bởi xác suất cảnh báo cố định

Nhằm tăng tính ngẫu nhiên và đặc tính thống kê của luồng dữ liệu watermark, kích thước của mẫu ảnh được mở rộng lên 16x16. Và sử dụng các phương thức tương tự như các trường hợp đã xét ở trên với kích thước khối được chia theo chuẩn 8x8. Hình 3.7 cho thấy xác suất tìm thấy watermark tăng khi giá trị p_f tăng.



Hình 3.8. Xác suất tìm thấy watermark với các p_f khác nhau.

Trong khi đó, với p_f=0,1%, xác suất đạt 75% và xấp xỉ 100% khi độ lớn watermark trung bình bằng 4. Hình 3.8 biểu diễn xác suất tìm

thấy watermark với các giá trị p_f khác nhau, trong đó xác suất càng giảm nếu tỷ số nén càng tăng nhưng vẫn luôn lớn hơn 70% ngay cả trường hợp tỷ số nén cao.

3.2. Phân tích và đánh giá hiệu suất xử lý xung đột của các thuật toán back-off khác nhau lên mạng vô tuyến khi bị tấn công

3.2.2. Mô hình trạng thái thuật toán Back-off

Gọi τ_1 , p_1 tương ứng là xác suất truyền và xác suất va chạm đối với nút bình thường, τ_2 , p_2 tương ứng là xác suất truyền và xác suất va chạm đối với nút lỗi.

$$\tau_1(BEB) = \frac{1-p_1^{R+1}}{1-p_1} \frac{2}{\sum_{i=0}^{R} p_1^i(2^iW+1) - (1-p_1^{R+1})} \quad (3.12)$$

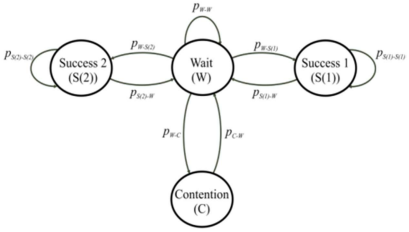
$$p_1 = 1-(1-\tau_1)^{n-l-1}(1-\tau_2)^l \quad (3.14)$$

$$\tau_2 = \frac{2}{(CW^*+1)-(1-p_2)} = \frac{2}{(CW^*+p_2)}. \quad (3.15)$$

$$p_2 = 1-(1-\tau_2)^{n-1}(1-\tau_2)^{l-1} \quad (3.16)$$

3.2.3. Mô hình trạng thái kênh

Mô hình trong hình 3.9 có bốn trạng thái là: Chờ, Thành công 1, Thành công 2 và Tranh chấp.



Hình 3.9. Mô hình trạng thái kênh.

3.2.4. Các tham số hiệu suất

Phân tích lưu lượng truyền tải:

$$Th_1 = \frac{\pi_{S(1)}}{n-l} \times \frac{E[P]}{E[T]}, Th_2 = \frac{\pi_{S(2)}}{l} \times \frac{E[P]}{E[T]}. \quad (3.24)$$

Xác suất rớt gói tin:

$$P_{drop1} = p_1^{R+1}, P_{dr} = p_2^{R+1}. \quad (3.25)$$

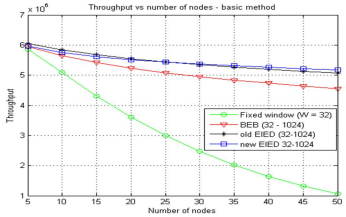
Phân tích độ trễ truy cập:

$$T_{dela}\ (BEB) = \sum_{j=0}^{R}\left(\frac{W_j+1}{2} \times \frac{p_1^j - p_1^{R+1}}{1-p_1^{R+1}}\right) \times E[T]; T_{delay}\ (EIED) = \frac{\sum_{i=0}^{m} T_i \times d_i}{\sum_{i=0}^{m} d_i} \quad (3.26)$$

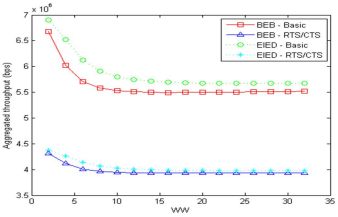
Đối với mỗi i, T_i và độ trễ gói của nút lỗi được tính như sau:

$$T_i = \sum_{j=0}^{R}\left(\frac{W_{\min(i+j,m)}+1}{2} \times \frac{p_1^j - p_1^{R+1}}{1-p_1^{R+1}}\right) \times E[T];\ T_{delay(2)} = \sum_{j=0}^{R}\left(\frac{WW+1}{2} \times \frac{p_2^j - p_2^{R+1}}{1-p_2^{R+1}}\right) \times E[T]. \quad (3.27)$$

3.2.5. Kết quả mô phỏng và đánh giá

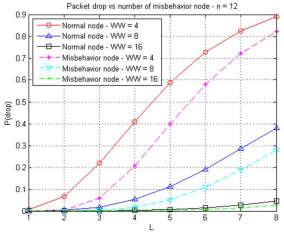


(a) Phân tích lưu lượng truyền tải mạng so với số nút mạng theo 3 thuật toán

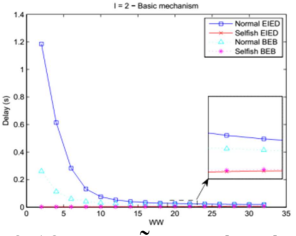


(b) Phân tích lưu lượng truyền tải mạng so với cửa sổ tranh chấp theo 2 thuật toán BED và EIED với mô hình cơ bản và mô hình RTS/CTS

Hình 3.10. Phân tích lưu lượng truyền tải mạng theo các thuật toán



Hình 3.11. Tỷ lệ rớt gói nút bình thường so với nút lỗi



Hình 3.12. Độ trễ của các nút bình thường và nút lỗi tương ứng với thuật toán BED và EIED

3.3. Kết luận chương 3

Thứ nhất, *đã xây dựng thuật toán đánh giá so sánh về hiệu suất xử lý ảnh có đánh dấu bảo mật bằng watermark trong quá trình*

truyền ảnh số để có thể lựa chọn phương pháp đánh dấu bảo mật DWT có hiệu quả nhất. Thứ hai, *dựa vào các kết quả mô phỏng số với 3 tham số lưu lượng truyền tải, xác suất rớt gói tin và độ trễ truy cập của lớp MAC trong mạng 802.11 theo các thuật toán back-off khác nhau, luận án đã phân tích khả năng và đánh giá hiệu suất xử lý xung đột của các thuật toán back-off khác nhau lên mạng vô tuyến khi bị tấn công trong khi truyền ảnh số để ứng dụng*.

CHƯƠNG 4. XÂY DỰNG HỆ THỐNG THÔNG TIN LIÊN LẠC BÍ MẬT THÔNG QUA TRUYỀN ẢNH SỐ

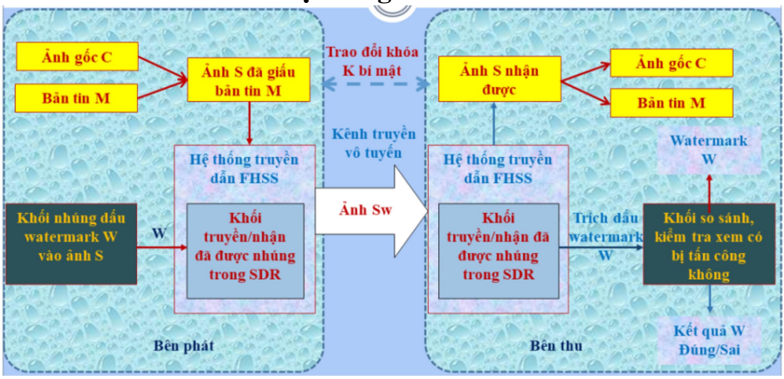
Tóm tắt: *Ứng dụng kết quả đã nghiên cứu trong chương 2 và 3, luận án đưa vào đề xuất và xây dựng một hệ thống thông tin liên lạc vô tuyến bí mật [T1].*

4.1. Giới thiệu chung

Xuất phát từ nhu cầu cần có một thiết bị liên lạc cơ động trong quá trình công tác có khả năng lập trình để hoạt động tự động với yêu cầu bảo mật bản tin liên lạc ứng dụng nội dung chương 2,3.

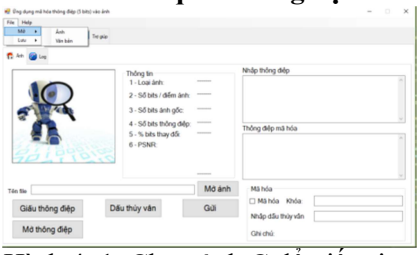
4.3. Triển khai hệ thống

4.3.3. Khối điều khiển hệ thống

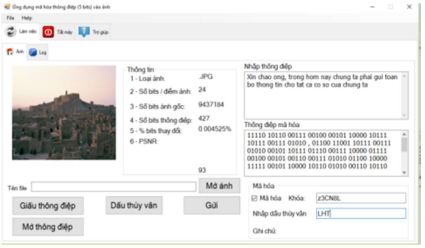


Hình 4.3. Sơ đồ khối điều khiển hệ thống

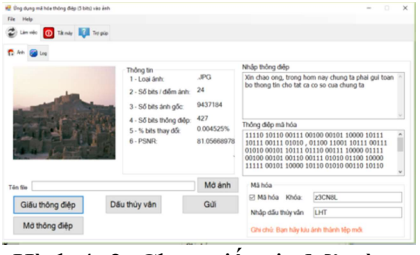
4.4. Kết quả thử nghiệm



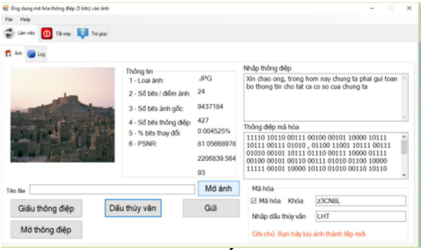
Hình 4. 1. Chọn ảnh C để giấu tin



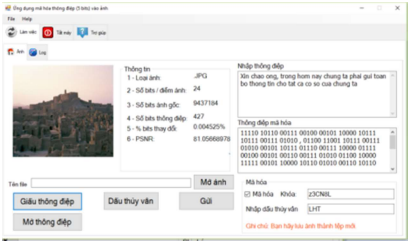
Hình 4. 2. Nhập bản tin M và sinh khóa K, dấu thủy vân W => Bản tin M'



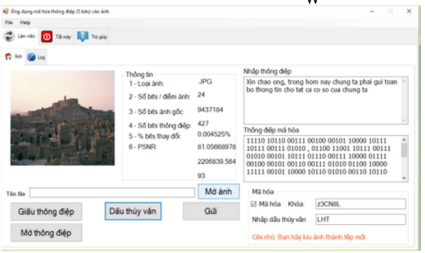
Hình 4. 3. Chọn giấu tin M' vào ảnh C => ảnh S



Hình 4. 4. Đánh dấu thủy vân W lên ảnh S=> ảnh S_W



Hình 4. 5. Lưu ảnh S_W trước khi gửi



Hình 4. 6. Gửi ảnh S_W thành công

Hệ thống sau khi thiết kế đã được đo đạc, thử nghiệm trong một số điều kiện khác nhau để kiểm tra về yêu cầu chất lượng, kỹ thuật cũng như yêu cầu đặc thù nghiệp vụ hay không trước khi được vào sử dụng. Một số kết quả thử nghiệm được trình bày trong phụ lục.

4.5. Kết luận chương 4

Việc thiết kế và tạo ra một hệ thống thiết bị thông tin liên lạc có bảo mật truyền ảnh số đã bổ sung giải quyết bài toán liên lạc mật phục vụ công tác nghiệp vụ và chứng minh cho tính khả thi của các kết quả đã được trong chương 2,3.

KẾT LUẬN

A. Các đóng góp chính của luận án

A.1. *Xây dựng các thuật toán giấu tin mật trong ảnh số từ các thuật toán giấu tin đã có và thuật toán đã cải tiến nhưng chưa hiệu quả với các tấn công thống kê cấp 1, cấp 2; xây dựng thuật toán trao đổi khóa khóa bí mật bằng phương pháp đồng dư tuyến tính; Luận còn đề xuất phương pháp và một số thuật toán đánh giá độ an toàn hệ thống mật mã và hệ thống giấu tin trong ảnh số.*

A.2. *Đánh giá độ an toàn bảo mật trong truyền ảnh số theo hai vấn đề là xác suất tìm thấy watermark được đánh dấu trong ảnh số và hiệu suất mạng IEEE 802.11 của các thuật toán back-off khi bị tấn công thông thường.*

A.3. *Dựa trên các nội dung đã nghiên cứu, luận án đã ứng dụng xây dựng hệ thống thông tin liên lạc bí mật thông qua truyền ảnh số.*

B. Những nội dung nghiên cứu tiếp theo: *Cải tiến thuật toán giấu tin mật nhằm đưa tỷ lệ giấu tin giảm xuống dưới 1%; Cứng hóa các tham số sinh số giả ngẫu nhiên nhằm tăng tốc độ xử lý cũng như độ an toàn cho khóa; Nghiên cứu về thuật toán đánh dấu bảo mật watermark trên đa phương tiện; Nâng cao hiệu suất mạng chống lại tấn công theo các phương thức đặc biệt; Hoàn thiện thiết bị nghiệp vụ để đưa vào sử dụng trong thực tế công tác.*

DANH MỤC CÁC CÔNG TRÌNH ĐÃ CÔNG BỐ

[1] Lê Hải Triều, Nguyễn Trung Trực, Nguyễn Đức Vinh, Nguyễn Thành Chung (11/2011), Ứng dụng hệ thống nhúng thiết kế chế tạo thiết bị thông tin liên lạc không dây, Hội nghị toàn quốc về Điều khiển và Tự động hoá – VCCA 2011, Hà Nội, trang 1-9.

[2] Lê Hải Triều, Nguyễn Trung Trực (12/2012), Nghiên cứu một số công cụ bảo mật trong truyền ảnh số của JPSEC, Kỷ yếu Hội thảo quốc gia lần thứ XV, Một số vấn đề chọn lọc của Công nghệ thông tin và truyền thông, Hà Nội, trang 1-9.

[3] Lê Hải Triều, Hồ Văn Canh (7/2016), "Kỹ thuật nhận dạng bản tin rõ", Tạp chí Khoa học giáo dục Kỹ thuật – Hậu cần, ISSN 2354-1008, trang 26-29,38.

[4] Lê Hải Triều, Hồ Văn Canh (2-3/2017) "Xây dựng thuật toán dấu tin mật trong truyền ảnh số", Tạp chí Khoa học Công nghệ Thông tin và truyền thông, trang 3-9.

[5] Lê Hải Triều, Trần Xuân Ban (6/2018) "Đề xuất thuật toán sinh số giả ngẫu nhiên có chu kỳ cực đại bằng phương pháp đồng dư tuyến tính", Tạp chí Nghiên cứu khoa học và công nghệ quân sự, trang 106-112 .

[6] L.H.Trieu, H.T.Minh, L.T.Nguyen, D.T.Trong (10/2016), A comparative evaluation for digital image watermarking techniques in wireless image sensor networks, Wireless Sensors (ICWiSE), 2016 IEEE Conference, IEEE Xplore (12/2017), pp 45-49.

[7] Trong MINH Hoang, Van KIEN Bui, Thanh TRA Nguyen, Hai TRIEU Le (3/2016), "A study on IEEE802.11 Mac Layer Misbehavior under Differen Back-off Algorithms", International Conference on Sustainable Enegy, Enviroment and Information Engineering (SEEIE 2016), Multimedia, Network security and Communications (MNSC2016), Thailand, pp. 362-368.