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

LUẬN ÁN TIẾN SĨ KỸ THUẬT

HÀ NỘI - 2019

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

LUẬN ÁN TIẾN SĨ KỸ THUẬT

NGƯỜI HƯỚNG DẪN KHOA HỌC:

GS.TSKH ĐỖ TRUNG TÁ

HÀ NỘI, 2019

LỜI CAM ĐOAN

Tôi xin cam đoan đây là công trình nghiên cứu do tôi thực hiện. Các số liệu và kết quả trình bày trong luận án là trung thực, chưa được công bố bởi bất kỳ luận án nào hay ở bất kỳ công trình nào khác.

Tác giả

Lê Hải Triều

LỜI CẢM ƠN

Luận án Tiến sĩ này được thực hiện tại Học viện Công nghệ bưu chính viễn thông dưới sự hướng dẫn khoa học của GS.TSKH Đỗ Trung Tá. Tôi xin trân trọng cảm ơn Lãnh đạo Học viện Công nghệ bưu chính viễn thông, Hội đồng Khoa học, Hội đồng Tiến sĩ của Học viện vì đã tạo điều kiện để luận án được thực hiện và hoàn thành chương trình nghiên cứu của mình.

Tôi xin bày tỏ lòng biết ơn sâu sắc tới GS.TSKH Đỗ Trung Tá về định hướng khoa học, thường xuyên góp ý, tạo điều kiện thuận lợi trong suốt quá trình nghiên cứu hoàn thành cuốn luận án. Xin chân thành cảm ơn các thầy cô ở Khoa Đào tạo Sau đại học, khoa Kỹ thuật Viễn thông 1 và và các nhà khoa học thuộc Học viện Công nghệ bưu chính viễn thông, các nhà khoa học trong và ngoài Ngành Công an, các tác giả đồng công bố, các tác giả có tài liệu đã trích dẫn trong luận án về sự hỗ trợ, hợp tác có hiệu quả trong suốt quá trình nghiên cứu khoa học của mình. Tôi xin được chân thành cảm ơn TS Hồ Văn Canh, TS Hoàng Trọng Minh vì những chỉ dẫn về học thuật hóa, kết nối giữa lý luận với kết quả thực nghiệm thời gian thực.

Tôi xin gửi lời cảm ơn tới Lãnh đạo Viện Kỹ thuật điện tử và cơ khí nghiệp vụ, Tổng cục IV, Bộ Công an (trước đây) nay là Viện Khoa học và công nghệ, sự biết ơn đối với gia đình, bạn bè thân thiết, các đồng nghiệp vì đã tạo nhiều điều kiện thuận lợi trong suốt quá trình học tập, liên tục động viên để duy trì nghị lực, sự cảm thông, chia sẻ về thời gian lẫn công việc và các khía cạnh khác của cuộc sống trong suốt quá trình để hoàn thành luận án.

Hà Nội, tháng 7 năm 2019

Tác giả

Lê Hải Triều

MỤC LỤC

DANH MỤC CÁC CHỮ VIẾT TẮT

Từ viết tắt	Nghĩ tiếng Anh	Nghĩa tiếng Việt
AES	Advanced Encryption Standard	Tiêu chuẩn mã hóa tiên tiến
BEB	Binary Exponential Back-off	Thuật toán tính toán khoảng thời gian chờ khi có xung đột
BMP	Windows Bitmap	Định dạng ảnh bitmap của hệ điều hành Windows
CIA	Central Intelligence Agency	Cơ quan tình báo trung ương
CPU	Central Processing Unit	Bộ xử lý trung tâm
CSMA/CA	Carrier Sence Multi Access/Collision Avoidance	Giao thức đa truy cập/tránh va chạm
DCT	Discrete Cosine Transform	Biến đổi cô-sin rời rạc
DES	Data Encryption Standard	Tiêu chuẩn mã hóa dữ liệu
DFT	Discrete Fourier Transform	Biến đổi Fu-ri-ê rời rạc
DSSS	Direction Sequence Spread Spectrum	Trải phổ chuỗi trực tiếp
DWT	Discrete Wavelet Transform	Biến đổi sóng con rời rạc
EIED	Exponential Increase Exponential Decrease	Thuật toán backoff tăng giảm hàm mũ
FH	Frequency Hopping Spread Spectrum	Trải phổ nhảy tần
GIF	Graphics Interchange Format	Định dạng trao đổi hình ảnh
IEEE	Institute of Electrical and Electronics Engineers	Viện kỹ nghệ Điện và Điện tử
JPEG	Joint Photographic Experts Group	Định dạng của Nhóm chuyên gia nhiếp ảnh
LSB	Least Significant Bit	Bit có trọng số nhỏ nhất

MAC	Media Access Control	Điều khiển truy nhập đa phương tiện
MD	Message-Digest algorithm 5	giải thuật Tiêu hóa tin 5
MSB	Most Significant Bit	Bit có trọng số cao nhất
OFDM	Orthogonal frequency-division multiplexing	Ghép kênh phân chia theo tần số trực giao
PNG	Portable Network Graphics	Định dạng chuyển đổi mạng lưới đồ hóa
PSRN	Pick Signal-to-Noise Ratio	Tỷ số tín hiệu trên tạp âm
QIM	Quantization Index Modulation	Điều chỉnh hệ số lượng tử
RC5	Rivest Cipher 5	Mật mã Rivest
RGB	Red-Green-Blue	Đỏ-Xanh da trời-Xanh lá
RF	Radio Frequency	Tần số vô tuyến
RSA	Ron Rivest, Adi Shamir và Len Adleman	Thuật toán mã hóa công khai
SDR	Software Defined Radio	Vô tuyến định nghĩa bằng phần mềm
SHA	Secure Hash Algorithm	thuật giải băm an toàn
SS	Spread Spectrum	Trải phổ
TTL	Time to Live	Thời gian sống của gói tin
WSN	Wireless Sensor Network	Mạng cảm biến không dây

DANH MỤC HÌNH VẼ

DANH MỤC BẢNG BIỂU

MỞ ĐẦU

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.

Hiện nay, việc bảo mật và xác thực thông tin bằng kỹ thuật mật mã đã đáp ứng được các yêu cầu của người sử dụng nói chung và các yêu cầu về bảo mật không ngặt nghèo trong các môi trường phổ thông. Tuy nhiên các kỹ thuật mật mã không bảo mật được địa chỉ người gửi và người nhận thông tin. Do đó, kẻ tấn công có thể sử dụng các kỹ thuật tấn công vào các giao thức mật mã (tức là tấn công vào tiền mã hóa hoặc hậu mã dịch) mà không cần chặn bắt và giải bản mã mà vẫn có thể đọc được bản rõ tương ứng. Ngoài ra, yêu cầu về xác thực và bảo vệ bản quyền số ứng dụng trong môi trường an ninh quốc gia đòi hỏi phải nghiên cứu kỹ thuật giấu tin nói chung…; Trong luận NCS không đi sâu phân tích vấn đề không chỉ bảo vệ thông tin mật mà còn phải bảo vệ bí mật cho cả người gửi và người nhận thông tin đó. Do đó, các nhà khoa học đã công khai giới thiệu nhiều công trình nghiên cứu về kỹ thuật giấu tin trong đa phương tiện như giấu tin trong ảnh kỹ thuật số (còn được gọi là ảnh số), trong âm thanh, trong video, trong các văn bản và giấu tin ngay trong các phần mềm máy tính,... Trong số đó, giấu tin trong ảnh kỹ thuật số được quan tâm nghiên cứu nhiều nhất **[**1**]**, **[**2**]**. Tùy theo yêu cầu ứng dụng cụ thể, người ta chia kỹ thuật giấu thông tin trong đối tượng đa phương tiện làm hai hướng nghiên cứu

chính, đó là nghiên cứu về kỹ thuật giấu tin mật (Steganography[1]) và kỹ thuật Thủy vân số (Digital Watermarking[2]) như trong hình 1.1 **[**3**]**, **[**4**]**, **[**5**]**

Ở Việt Nam, kỹ thuật giấu tin mật và thủy vân số đã được nghiên cứu đầu tiên vào khoảng năm 2001 bởi GS, TSKH Nguyễn Xuân Huy và cộng sự. Từ đó, đến nay đã có nhiều Công trình khoa học về lĩnh vực này đã được công bố **[**2**]**. Ngoài ra, có nhiều nghiên cứu khác như Luận án TS của NCS Đào Thị Hồng Vân "Vấn đề bảo đảm an toàn thông tin trong môi trường Web sử dụng kỹ thuật mật mã" (năm 2012 tại Viện KH&CN Quân sự), luận án TS của NCS Đỗ Văn Tuấn "Kỹ thuật thủy vân số và mật mã học trong xác thực, bảo vệ bản quyền dữ liệu đa phương tiện" (năm 2015 tại Đại học Bách khoa Hà Nội),…; Luận án TS của NCS Chu Minh Yên "Nghiên cứu, xây dựng hạ tầng cơ sở khóa công khai cho khu vực an ninh quốc phòng" (năm 2012, Viện KH&CN Quân sự); Luận án TS của NCS Nguyễn Văn Tảo "Nghiên cứu một số kỹ thuật giấu tin và ứng dụng" (năm 2009, Viện CNTT)

Đối với hướng nghiên cứu thứ nhất, kỹ thuật giấu tin mật được dựa trên hình thức nhúng thông tin mật cần truyền đi vào một đối tượng được truyền đi (được gọi là **"**vật mang tin"). Yêu cầu cơ bản của Steganography là giấu được càng nhiều thông tin càng tốt nhưng phải đảm bảo tính "vô hình" của ảnh gốc, nghĩa là những kẻ tấn công khó có thể phát hiện ra sự có mặt của thông tin chứa trong ảnh gốc. Nguồn gốc của Steganography là ghép của từ Steganos (bao bọc) và Graphia (bản viết) có nghĩa là **"**bảo vệ bản viết" **[**3**]** , **[**6**]**.

Hướng nghiên cứu thứ hai của giấu thông tin là kỹ thuật watermark. Kỹ thuật watermark lại yêu cầu tính bền vững của thông tin chứa trong ảnh gốc. Watermark là một quá trình nhúng dữ liệu gọi là watermark (thủy vân) hoặc chữ ký số (digital signature) hoặc thẻ (tag) hoặc nhãn (title) vào một đối tượng đa phương tiện (ảnh số, âm thanh số, video số, văn bản) mà watermark có thể được phát hiện hoặc trích lại sau đó nhằm mục đích xác thực nguồn gốc của đối tượng đa phương tiện đó **[**3**]**.

[1] Thuật ngữ Steganography hoặc gọi là "giấu tin" được sử dụng trong toàn bộ luận án này.
[2] Thuật ngữ Digital Watermarking hoặc Watermark hoặc gọi là "thuỷ vân số" được sử dụng trong toàn bộ luận án này.

Từ đó, bài toán nghiên cứu các phương pháp bảo mật thông tin giấu trong đa phương tiện chính là một ngành mật mã học trong lĩnh vực an toàn thông tin. Kỹ thuật giấu tin (bao gồm cả Steganography và Digital Watermaking) là những công cụ hiệu quả đối với vấn đề bảo mật thông tin trên mạng viễn thông ngoài mật mã học. Vấn đề là phải chủ động tạo ra các sản phẩm bảo mật thông tin giấu trong đa phương tiện và kiểm soát cũng như bảo đảm độ an toàn của sản phẩm nghiên cứu.

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*"**.

Nội dung nghiên cứu của luận án còn nhằm ứng dụng để phục vụ cho công tác thông tin liên lạc bí mật nghiệp vụ. Từ việc xác định tầm quan trọng của bảo mật thông tin giấu trong ảnh số khi truyền thông, luận án đã nghiên cứu, xây dựng và công bố thuật toán giấu tin mật trong ảnh số, thỏa thuận trao đổi khóa bí mật, đồng thời phân tích và đánh giá khả năng bảo mật đường truyền vô tuyến cho ảnh số khi bị tấn công để có sự lựa chọn đúng đắn theo các thuật toán khác nhau.

Việc nghiên cứu này không chỉ mở rộng đa dạng hoá các phương thức bảo mật để nâng cao hiệu quả khai thác, ứng dụng và sử dụng ảnh số trong truyền thông, mà còn hỗ trợ cho thông tin liên lạc bí mật thông qua truyền ảnh số phục vụ công tác nghiệp vụ an ninh - quốc phòng.

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

B.1. Mục tiêu và phạm vi nghiên cứu

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

- Nghiên cứu về kỹ thuật giấu tin và trao đổi khóa bí mật. Từ đó 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.

- Nghiên cứu một số vấn đề về bảo mật ảnh số có đánh dấu watermark và hiệu suất mạng khi bị tấn công. Từ đó đề xuất lựa chọn phương pháp đánh dấu bảo mật watermark nào tốt nhất cho cả hiệu năng lỗi và xác suất tìm thấy đánh dấu bảo mật

watermark, cũng như đánh giá hiệu suất xử lý của các thuật toán back-off khác nhau trên mạng vô tuyến khi bị tấn công trong điều kiện thông thường.

- Ứng dụng nội dung nghiên cứu trên vào thiết bị thông tin liên lạc bí mật nghiệp vụ bằng hình ảnh.

B.2. Đối tượng nghiên cứu

Đối tượng nghiên cứu ở đây 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...

B.3. Phương pháp nghiên cứu

Trên cơ sở mục tiêu, đối tượng và phạm vi nghiên cứu, phương pháp nghiên cứu được sử dụng trong luận án là 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.

B.4. Nội dung nghiên cứu

Từ các phân tích trên, trong phạm vi của đề tài, luận án tập trung vào giải quyết các vấn đề sau:

- Thứ nhất xây dựng thuật toán giấu tin mật trong ảnh số

- Thứ hai là đưa ra thuật toán sinh số giả ngẫu nhiên phục vụ thỏa thuận trao đổi khóa bí mật;

- Thứ ba là xây dựng thuật toán đánh giá độ an toàn của hệ thống mật mã và giấu tin trong ảnh số.

- Thứ tư là nghiên cứu, đánh giá hiệu năng lỗi và xác suất tìm thấy watermark nhúng trong ảnh số khi bị tấn công.

- Thứ năm là đánh giá ảnh hưởng của thuật toán back-off đến hiệu suất mạng khi bị tấn công thông thường.

- Thứ sáu trên cơ sở các nhiệm vụ nghiên cứu trên, luận án đề xuất ứng dụng vào hệ thống liên lạc nghiệp vụ.

C. Bố cục luận án

Luận án được tổ chức thành 4 chương với nội dung chính như sau

- Phần mở đầu

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

Chương 1 trình bày tổng quan những vấn đề cần nghiên cứu của luận án. 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 truyền tin vô tuyến khi giấu thông tin trong ảnh số. Đó là những vấn đề nghiên cứu đặt ra để các chương tiếp theo giải quyết.*

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

Chương 2 giải quyết bài toán giấu tin mật và thỏa thuận trao đổi khóa bí mật. Thứ nhất *đối với 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 [T4]*. 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 [T5]*. Thứ ba, *từ các nghiên cứu về phương pháp đánh giá độ an toàn hệ thống mật mã và giấu tin, luận án đề xuất 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 [T3]*.

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

Chương ba giải quyết bài toán đánh giá khả năng bảo mật ảnh số thông qua xác suất tìm thấy wartermark đã được đánh dấu và hiệu suất mạng lớp MAC của

IEEE 802.11 khi bị tấn công. Thứ nhất *nghiên cứu và đánh giá so sánh hiệu năng lỗi của ảnh JPEG/JPEG2000 [T2] đã đánh dấu bảo mật bằng watermark khi truyền trên mạng vô tuyến, từ đó đề xuất lựa chọn phương pháp đánh dấu bảo mật watermark nào tốt nhất cho cả vấn đề hiệu năng lỗi cũng như xác suất tìm thấy đánh dấu bảo mật watermark [T6].* Thứ hai *dựa trên việc hiệu suất lớp MAC của mạng IEEE 802.11 bị hạ xuống do các cuộc tấn công thông thường, luận án xây dựng mô hình trạng thái thuật toán Back-off, mô hình trạng thái kênh, các tham số hiệu suất gồm 3 tham số: lưu lượng truyền tải, xác suất rớt gói và độ trễ truy cập. Từ đó, luận án đánh giá hiệu suất xử lý của các thuật toán back-off khác nhau trong điều kiện thông thường [T7].*

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

Từ các kết quả đã đạt được trong chương 2 và chương 3, chương 4 luận án ứng dụng nội dung nghiên cứu vào hệ thống thông tin liên lạc bí mật nghiệp vụ. 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). Hệ thống thông tin liên lạc bí mật được sử dụng để trao đổi bản tin giấu trong ảnh số cho nhau phục vụ cho công tác nghiệp vụ [T1].

Kết luận và phụ lục: *Trong* 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. Phần* phụ lục *là kết quả thử nghiệm đánh giá đối với hệ thống thiết bị thông tin liên lạc bí mật.*

Các đề xuất mới trong luận án đều được chứng minh, phân tích lý thuyết và thực nghiệm, mô phỏng. Những kết quả chính của luận án được công bố trên 09 công trình.

CHƯƠNG 1. TỔNG QUAN VỀ VẤN ĐỀ NGHIÊN CỨU

Tóm tắt: *Chương này trình bày tổng quan những vấn đề nghiên cứu của luận án. 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 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

Dựa trên kỹ thuật ta có thể phân loại bảo mật thông tin thành hai nhóm: nhóm thứ nhất là bảo mật thông tin bằng các kỹ thuật phần cứng và nhóm thứ hai là giải pháp bằng phần mềm thông qua các thuật toán bảo mật. Luận án này tập trung vào nhóm giải pháp thứ 2. Để đảm bảo an toàn dữ liệu một cách hiệu quả nhằm chống các khả năng tấn công hoặc các rủi ro, sự cố ngẫu nhiên/cố ý có thể xảy ra trong quá trình truyền tin nói chung, việc phòng chống và xác định chính xác các nguy cơ có thể làm ảnh hưởng đến dữ liệu là vô cùng quan trọng [**1**], [**6**].

Theo NCS, một số vấn đề liên quan đến an toàn, bảo mật thông tin được đề cập dưới đây

** An toàn đối với việc bảo vệ thông tin gồm:*

- Tính bí mật: đảm bảo thông tin/dữ liệu trao đổi không bị lộ hoặc bị khám phá bởi những kẻ tấn công.

- Tính xác thực: Đảm bảo thông tin/dữ liệu trao đổi không bị mạo danh giữa người gửi và người nhận.

- Tính toàn vẹn: Đảm bảo thông tin/dữ liệu trao đổi không bị thay đổi hoặc bị phá hủy bởi những kẻ tấn công.

- Tính sẵn sàng: Đảm bảo những người nhận và người gửi hợp pháp không bị từ chối truy nhập một cách không chính đáng tới thông tin/dữ liệu trao đổi.

** Nguy cơ mất an toàn thông tin gồm:*

- Rò rỉ thông tin: Thông tin/dữ liệu bị lộ hoặc bị khám phá từ chính người được phép.

- Vi phạm tính toàn vẹn: Tính toàn vẹn của thông tin/dữ liệu bị phá hủy/ảnh hưởng thông qua việc tạo, thay đổi trái phép hay phá hoại thông tin/dữ liệu đó.

- Từ chối dịch vụ: Việc truy nhập thông tin/dữ liệu bị cản trở một cách có chủ đích.

- Sử dụng trái phép: Thông tin/dữ liệu được sử dụng bởi kẻ tấn công hoặc theo cách không được phép.

** Các dịch vụ an toàn thông tin gồm:*

- Dịch vụ giữ bí mật: Bảo vệ chống lại thông tin bị lộ hoặc bị khám phá do các kẻ tấn công.

- Dịch vụ xác thực: Cung cấp việc đảm bảo về định danh của thông tin/dữ liệu đó.

- Dịch vụ toàn vẹn dữ liệu: Bảo vệ chống lại thông tin/dữ liệu bị thay đổi, xoá, hoặc thay thế trái phép.

- Dịch vụ chống chối bỏ: Bảo vệ chống lại một nhóm trao đổi truyền thông từ chối một cách không đúng khi trao đổi xảy ra.

- Dịch vụ điều khiển truy nhập: Bảo vệ chống lại việc sử dụng hoặc thao tác trái phép trên các tài nguyên.

** Các hình thức tấn công thông tin trên đường truyền:*

- Tấn công chủ động (*Active*) có một số hình thức như sau: Ngăn chặn thông tin, sửa đổi thông tin và chèn thông tin giả; Trong đó *Ngăn chặn thông tin* là Thông tin/dữ liệu bị phá hủy, không sẵn sàng phục vụ hoặc không sử dụng được. Đây là hình thức tấn công làm mất khả năng sẵn sàng phục vụ của thông tin/dữ liệu. *Sửa đổi thông tin* là kẻ tấn công truy nhập, chỉnh sửa thông tin/dữ liệu trên đường truyền. Đây là hình thức tấn công lên tính toàn vẹn của thông tin/dữ liệu. *Chèn thông tin giả* là kẻ tấn công chèn thông tin/dữ liệu giả vào hệ thống. Đây là hình thức tấn công lên tính xác thực của thông tin/dữ liệu. Mục đích của các hình thức tấn công chủ động này là cho người nhận nhận được những thông tin đã bị sai

lệch,bị sửa đổi, thậm chí không nhận được dữ liệu gửi hoặc thời gian nhận bị trễ để phục vụ ý đồ khác nhau.

- Tấn công bị động (*Passive*) hay còn gọi là "nghe trộm" thông tin trên đường truyền: Kẻ tấn công có thể truy nhập tới thông tin/dữ liệu. Đây là hình thức tấn công vào tính bí mật của thông tin/dữ liệu. Kẻ tấn công biết được thông tin về người gửi và người nhận nhờ vào việc "nghe trộm" thông tin chứa trong gói tin truyền trên truyền dẫn. Đối với hình thức này, kẻ tấn công có thể kiểm tra được tần số trao đổi, số lượng gói tin truyền đi và độ dài của gói tin này. Tuy nhiên, với hành động trên, thông thường với mục đích giải mã thông tin, sao chép, đánh cắp nội dung thông tin (ví dụ như mật khẩu, thông tin cá nhân của ngân hàng…) chứ không làm ảnh hưởng nguy hại về mặt vật lý đối với dữ liệu hay làm sai lệch nội dung dữ liệu.

Từ những vấn đề nêu trên, đặt ra cho luận án cần nghiên cứu và giải quyết là *bảo mật thông tin* để chống lại tấn công *bị động* và *đánh giá khả năng an toàn của hệ thống* phục vụ chống lại các tấn công chủ động lên đường truyền.

1.2. Bảo mật thông tin giấu trong ảnh số

1.2.1. Khái nhiệm và phân loại bảo mật thông tin giấu trong đa phương tiện

Để bảo vệ thông tin dữ liệu trên đường truyền, ngoài an toàn thông tin về mặt vật lý, vấn đề an toàn và bảo mật thông tin là nhiệm vụ đóng vai trò quan trọng, rất nặng nề và thường xuyên cập nhật, thay đổi liên tục để đáp ứng yêu cầu thực tế.

Khái niệm về giấu tin có rất nhiều, tuy nhiên trong phạm vi nghiên cứu, luận án sử dụng khái niệm "Giấu thông tin" là kỹ thuật giấu một lượng thông tin số nào đó vào một đối tượng dữ liệu đa phương tiện khác (dữ liệu số - "vật mang tin") [**7**] [**8**].

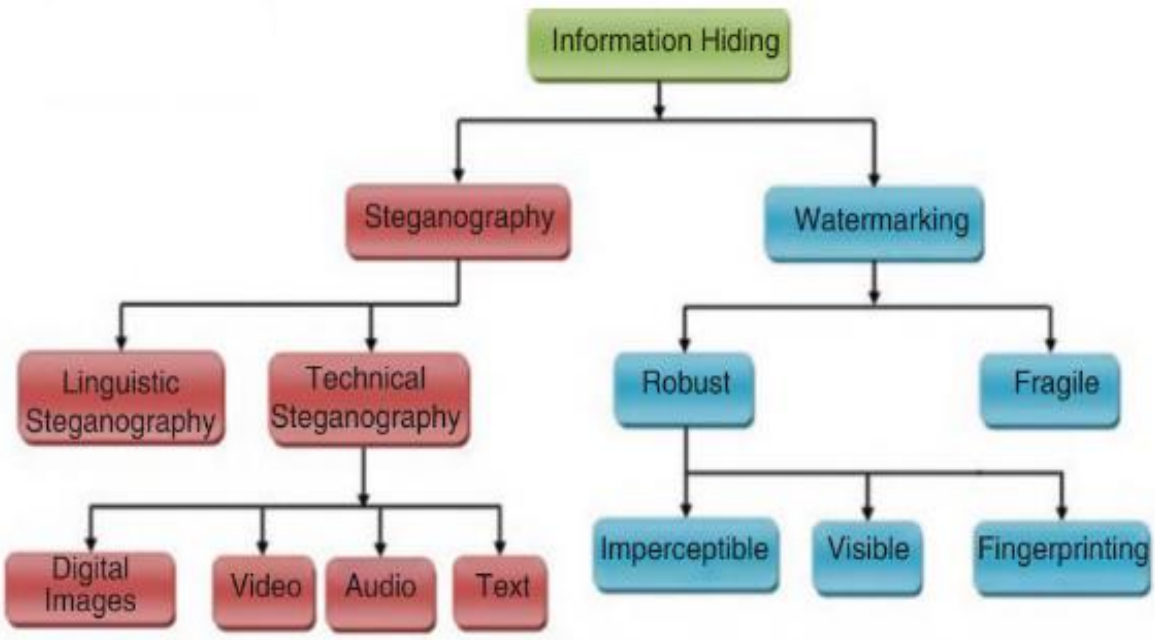
Sự khác nhau giữa mã hóa và giấu thông tin là ở chỗ các thông tin được mã hóa hiện rõ đối với người truy xuất, còn thông tin được giấu tin trong một "vật mang tin" thì không hiện rõ với người truy xuất do tính chất ẩn (invisible) của thông tin được giấu.

Như đã trình bày trong phần mở đầu, có hai hướng nghiên cứu chính về kỹ thuật giấu thông tin, một là Giấu tin mật (Steganography) nhằm bảo mật dữ liệu được đem giấu vào "vật mang tin" và hai là Thủy vân số (Digital watermarking) nhằm bảo vệ chính "vật mang tin" [**9**], [**10**], [**3**], [**11**], [**12**].

Mục tiêu của kỹ thuật giấu tin mật giải quyết là lượng thông tin giấu được nhiều nhất và ít bị phát hiện nhất.

Kỹ thuật watermark là kỹ thuật đánh dấu vào đối tượng "vật mang tin" nhằm bảo vệ nó, phát hiện việc thay đổi hay chỉnh sửa, "tấn công" có chủ ý "vật mang tin", hoặc đơn giản là thay thế bằng 1 "vật mang tin" giả mạo.

Theo [**11**] ta có sơ đồ phân loại các kỹ thuật giấu tin như hình 1.1 dưới đây



Hình 1.1. Phân loại kỹ thuật giấu thông tin

Mục đích của giấu tin mật là không chỉ nhúng những "thông tin quan trọng" cần trao đổi giữa người gửi và người nhận mà còn bí mật được cả địa chỉ của người gửi và nhận thông tin đó.

Còn watermark là nhúng dữ liệu số vào "vật mang tin" nhằm mục đích bảo vệ "vật mang tin" với mục đích là bảo vệ bản quyền số . Việc nhúng dữ liệu số như

vậy vào "vật mang tin" sẽ làm giảm chất lượng của ảnh số, nhưng đó là cách đánh dấu nhằm phát hiện sự tấn công làm thay đổi từ bên thứ 3 lên "vật mang tin". Có 2 kỹ thuật cơ bản trong watermark là thủy vân dễ vỡ (Fragile Watermarking) và thủy vân bền vững (Robust Watermarking). Thủy vân bền vững nhằm mục đích bảo đảm dấu thủy vân bền vững trước các tấn công nhằm loại bỏ dấu thủy vân trên "vật mang tin"; còn thủy vân dễ vỡ nhằm mục đích xác định tính chân thực, tính toàn vẹn của "vật mang tin" khi bị tấn công [**13**].

Việc bảo mật thông tin bằng kỹ thuật giấu tin mật (Steganography) nhằm mục đích bảo đảm tính "vô hình"của thông tin được giấu trong "vật mang tin" (an toàn thông tin). Để bảo vệ và xác thực "vật mang tin" nhận được sau quá trình trao đổi, cần phải sử dụng kỹ thuật thủy vân số (Digital Watermarking). Tuy nhiên, các kỹ thuật giấu tin mật nói trên mới bảo đảm cho bản tin mật và "vật mang tin" mà chưa thể bảo đảm bảo mật được nơi gửi và nơi nhận tin do tính chất của công tác liên lạc bí mật nghiệp vụ.

Về mô hình hóa, để bảo mật đầu cuối và đường truyền nhằm bảo vệ thông tin được an toàn, bản rõ M cần được mã hóa trước khi truyền. Việc mã hóa thông điệp M cần có một khóa mã - K. Nếu khóa K được sinh tại nơi gửi thì nó phải được gửi thông qua một kênh an toàn tới nơi nhận hoặc có thể một bên thứ ba sinh khóa - K và chuyển một cách an toàn tới cả hai nơi (nơi gửi và nơi nhận). Với thông điệp M và khóa mã K, thuật toán mã E sẽ tạo ra bản mã theo

$$M' = E_k(M) \tag{1.1}$$

Khi dữ liệu đã được mã hóa, trước khi truyền đi, chúng được chia thành các gói tin nhỏ và truyền đi nhiều hướng khác nhau dựa vào các nút của hệ thống mạng.

Kẻ tấn công có thể "nghe trộm" thông tin trên đường truyền và chặn thu các gói tin nhằm đánh cắp thông tin. Do vậy việc chia nhỏ các gói tin trong khi truyền cũng là một bước quan trọng làm giảm rủi ro truyền tin và mất dữ liệu trên mạng. Các gói tin sau khi lưu thông trên mạng một khoảng thời gian t sẽ quy định về thời gian sống của gói tin (Time to Live - TTL).

Ngoải ra trong quá trình truyền tin có thể số lượng gói tin đến đích không đủ nhưng dựa vào các thuật toán ta có thể khôi phục những gói tin bị hỏng và tiến hành ghép nối các gói tin sau đó là nhiệm vụ giải mã. Tại nơi nhận với thông điệp mã M' và khóa mã K, thuật toán giải mã D sẽ tạo ra thông điệp M

$$M = D_k(M') \quad (1.2)$$

Trong trường hợp kẻ tấn công thu được dữ liệu ở dạng mã M nhưng không có khóa K, thì bên nhận sẽ khôi phục M hoặc khóa K (với giả thiết kẻ tấn công đã biết thuật toán mã E và thuật toán giải mã D). Trong trường hợp chỉ quan tâm đến nội dung thông điệp, thì bên nhận sẽ khôi phục thông điệp M bằng việc sinh ra một ước lượng M^R' của M^R. Tuy nhiên thường kẻ tấn công mong muốn tìm ra khóa K để giải mã các thông báo tiếp theo, bằng cách sinh ra một khóa ước lượng K' của K. Độ bảo mật của mật mã khóa bí mật nằm ở khóa K, là thước đo mức độ khó khăn của việc tìm ra thông báo rõ khi biết bản mã.

Như vậy không gian khóa đóng vai trò cốt lõi để bảo đảm bí mật cho thông tin được mã hóa. Hiện nay trên thế giới có rất nhiều thuật toán, phương pháp mã hóa khác nhau [**14**]. Tuy nhiên tùy theo mục đích và điều kiện người ta áp dụng các phương pháp mã hóa khác nhau. Một số phương pháp mã hóa được trình bày dưới đây.

Mã hóa dạng khối DES (Data Encryption Standard) được đưa vào sử dụng bắt đầu từ năm 1977 bởi NIST - Viện tiêu chuẩn và công nghệ Quốc gia Mỹ và được sử dụng ngày càng phổ biến trên toàn thế giới và được coi là tương đối an toàn. DES sử dụng mã khối dữ liệu với mỗi khối là 64 bít. Năm 1999 DES được thay bằng phiên bản nâng cấp cao hơn như 3DES. Đến tháng 5/2005 NIST đã bãi bỏ tiêu chuẩn 3DES và được thay bằng AES.

Đặc biệt là tiêu chuẩn mã nâng cao AES (Andvanced Encryption Standard) do Rijndael và Joan Daemen công bố năm 1998 và được công bố tiêu chuẩn 2001 với kích thước khối dữ liệu 128 bít và độ dài khóa có thể thay đổi 128, 192 hoặc 256 bít. Ta có thể thấy không gian khóa của DES gồm 256 phần tử trong lúc đó không gian khóa của AES là 2^{128} hoặc lớn hơn.

Dạng mã hóa khác đó là RC5 (Rivert Cipher 5), đây là dạng mã hóa hiện đại đã được đăng ký bản quyền của RSADSI. RC5 có nhiều kích thước khóa và dữ liệu khác nhau và đặc biệt không có vòng lặp. RC5 được đánh giá là an toàn và dễ dàng cài đặt trên nhiều bộ vi xử lý phần cứng khác nhau. Phiên bản tiêu chuẩn hiện nay là RC5-32/12/16 [**15**], [**16**].

Ngày nay trong lĩnh vực thương mại, người ta sử dụng mật mã khóa công khai và mã hóa khóa bí mật để phục vụ thỏa thuận trao đổi khóa. Trong luận án TS "Hệ tiêu chuẩn tham số an toàn cho hệ mật RSA và ứng dụng" của tác giả Hoàng Văn Thức (2011) [**17**] *cũng đã đánh giá chung về Hệ mật khóa công khai RSA và các đề xuất độ dài khóa; Vấn đề rất quan trọng là phải có 1 kênh truyền an toàn để trao đổi khóa bí mật. Hiện tại NCS chưa tìm thấy đánh giá về mặt lý thuyết độ an toàn của các hệ mật mã khóa công mà chỉ có một số đánh giá mang tính thực hành thông qua mô phỏng. Trong thực tế công tác liên lạc bí mật nghiệp vụ, trước tiên phải bảo mật được nơi gửi và nơi nhận cũng như phát hiện xem quá trình liên lạc bí mật có bị tấn công hay không?*.

Năm 2007 Chính phủ đã ban hành tiêu chuẩn mật mã quốc gia để đánh giá độ an toàn khóa mã như "Hệ tiêu chuẩn đánh giá khóa mã", TCVN 7817-3:2007 [**18**] *khuyến cáo 7 cơ chế thỏa thuận khóa bí mật, 6 cơ chế vận chuyển khóa bí mật và 3 cơ chế vận chuyển khóa công khai. Việc áp dụng các tiêu chuẩn này được thực hiện dưới sự hướng dẫn và giám sát của các cơ quan chuyên ngành như Ban Cơ yếu Chính phủ* [**19**]. *Trong thực tế các tiêu chuẩn thuật toán nói trên ít khi áp dụng vào lĩnh vực liên quan đến công tác liên lạc bí mật nghiệp vụ của ngành Công an. Các hệ tiêu chuẩn mật mã quốc gia mới được áp dụng vào việc mã hóa bản tin mật trước khi đưa vào giấu tin, do vậy trong luận án NCS coi như các bản tin mật cần giấu đã được mã hóa nội dung trước khi áp dụng thuật toán giấu tin được đề xuất*.

Kỹ thuật giấu tin mật đã giải quyết được những vấn đề nêu trên, tuy nhiên vấn đề đặt ra ở đây là thuật toán giấu tin có đạt yêu cầu đặt ra hay không? Những yêu cầu cần phải giải quyết đó là:

- Lượng thông tin M giấu được trong ảnh có đủ lớn?

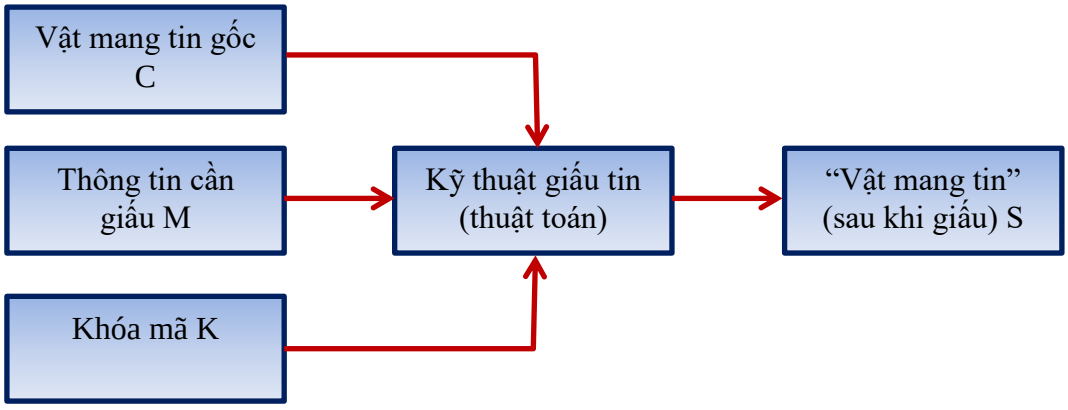
- Sự thay đổi ảnh giấu tin S so với ảnh gốc C?

- Trước khi được giấu, thông điệp đó cần phải được mã hóa bằng thuật toán mã hóa nào đó.

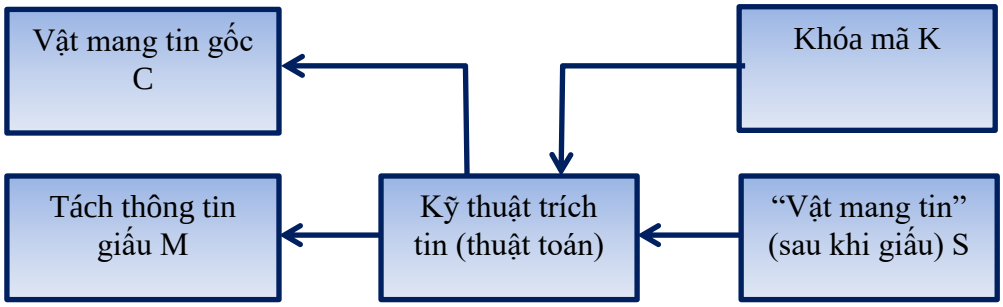
Việc tạo ra một chuỗi dãy bit giả ngẫu nhiên tuần hoàn có chu kỳ cực đại là rất cần thiết trong thỏa thuận trao đổi khóa bí mật. Cùng với đó, dãy bit giả ngẫu nhiên này được XOR với dãy bit của thông điệp được mã hóa sẽ tạo ra bản mã mới sau đó mới giấu vào ảnh số. Đó cũng chính là một trong những mục tiêu của luận án: tạo ra dãy giả ngẫu nhiên có chu kỳ cực đại nhằm phục vụ trao đổi khóa bí mật và phục vụ mã hóa thông điệp khi giấu vào ảnh số.

1.2.2. Sơ đồ giấu tin tổng quát trong dữ liệu đa phương tiện

Sơ đồ giấu thông tin tổng quát gồm quá trình giấu tin và quá trình trích tin [**20**]. Khái quát quá trình giấu tin và trích tin như 2 sơ đồ trong hình 1.2 và 1.3 dưới đây. Trên hình 1.2 ngoài thông tin cần giấu M và vật mang tin gốc C, mỗi thuật toán nhúng tin đều được trang bị khóa mã K để nâng cao sự an toàn cho hệ thống. Vì trong các ứng dụng truyền thông tin, thông thường các "vật mang tin" S đều bị công khai. Do vậy việc sử dụng hệ thống trao đổi khóa bí mật trong thuật toán giấu tin rất quan trọng, ngoài việc bảo mật, nó còn phục vụ cho việc trích tin.



Hình 1. 2. Sơ đồ giấu tin



Hình 1. 3. Sơ đồ trích tin

Sau khi nhúng tin, "vật mang tin" S được truyền trên các hệ thống thông tin có thể bí mật hoặc công cộng. Ở phía người nhận, thủ tục trích tin được trình bày trong hình 1.3. Đối với người dùng hợp lệ, ngoài việc trích tin để nhận được thông tin M, người nhận còn phải kiểm tra xem tính xác thực và toàn vẹn của "vật mang tin" S xem có bị tấn công hay không?

Như đã trình bày ở trên, giấu tin là phương pháp nhúng thông điệp M vào vật mang tin gốc C để nhận được đối tượng S. Khi nhúng M vào C, các kỹ thuật giấu tin thường phải biến đổi theo một thuật toán nào đó để nhận được S. Do vậy, giữa S và C bao giờ cũng có sự sai khác nhất định. Sự sai khác này có thể được phát hiện bằng các chương trình, hoặc bằng hệ thống thị giác đối với dữ liệu dạng hình ảnh, hoặc bằng hệ thống thính giác đối với dữ liệu âm thanh. Thuật toán có tính che giấu càng cao thì càng khó phát hiện. Nói cách khác, sự sai khác giữa vật mang tin gốc C và "vật mang tin" S càng ít thi tính che giấu càng cao.

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

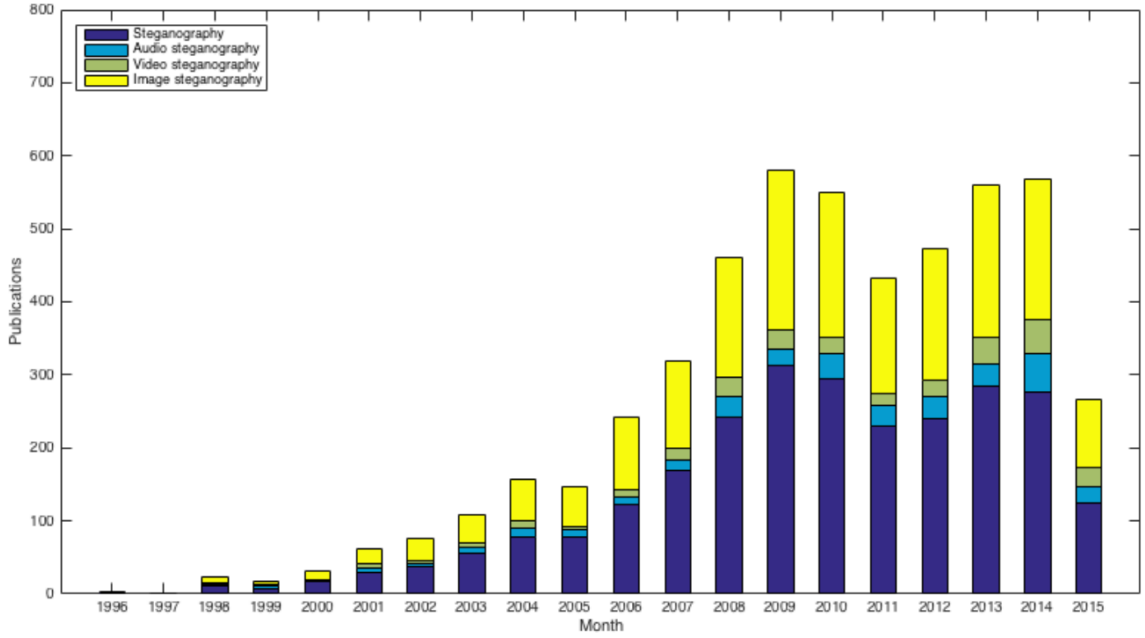
1.2.3.1. Khái niệm và nghiên cứu liên quan

Theo quan điểm của nghiên cứu sinh: Giấu tin mật trong ảnh số (còn gọi là thông tin giấu trong ảnh số) có nghĩa là Thông tin sẽ được giấu cùng với dữ liệu ảnh nhưng chất lượng ảnh ít thay đổi và không ai biết được đằng sau ảnh đó có chưa thông tin hay không [**21**], [**3**], [**22**], [**23**]. Ngày nay, khi ảnh số đã được sử dụng rất phổ biến, thì giấu thông tin trong ảnh đã đem lại rất nhiều những ứng dụng quan trọng trên nhiều lĩnh vực trong đời sống xã hội. Một đặc điểm của giấu thông tin

trong ảnh đó là thông tin được giấu trong ảnh một cách vô hình, nó như là một cách mà truyền thông tin mật cho nhau mà người khác không thể biết được bởi sau khi giấu thông tin thì chất lượng ảnh gần như không thay đổi đặc biệt đối với ảnh mầu hay ảnh xám.

Năm 2012, báo chí đã được các cơ quan điều tra tiết lộ thông tin tên trùm khủng bố quốc tế Osma BinLaDen đã sử dụng cách thức giấu tin trong bức ảnh để mã hóa tốt hơn nhằm mục đích trao đổi, ra lệnh cho cấp dưới. Ngoài ra, chúng còn dùng quyển kinh thánh được viết bằng tiếng Anh nhằm chuyển các bản khóa và giải mã để phục vụ liên lạc bí mật. Cục tình báo trung ương Mĩ (CIA) và các cơ quan an ninh quốc tế đã bị qua mặt về vấn đề này. Sau khi được công bố, việc nghiên cứu các vấn đề liên quan đến giấu thông tin trong ảnh và phát hiện ảnh giấu tin ngày càng được quan tâm trên toàn thế giới không chỉ với các cơ quan đặc biệt mà còn cả các nhà mật mã học.

Có khá nhiều công trình nghiên cứu về kỹ thuật giấu tin trong ảnh đã được công bố trên IEEE. Hình 1.4 [**24**] thống kê từ năm 1996 đến năm 9/2015 số lượng nghiên cứu được công bố về steganography (giấu tin mật) là 1855 công trình.

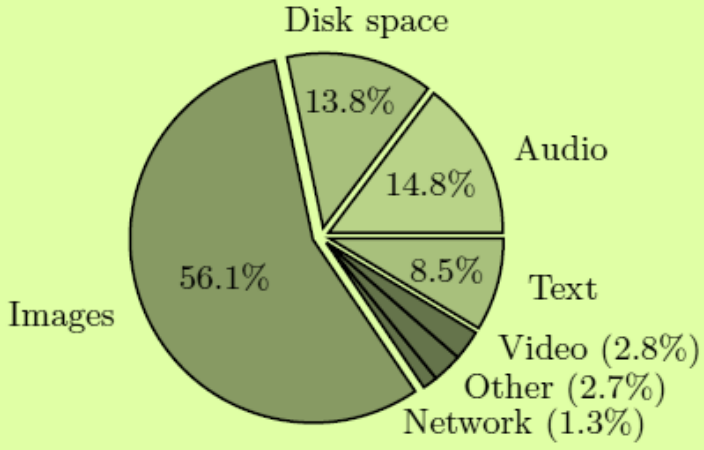


Hình 1. 4. Số lượng nghiên cứu về Steganography và các dạng giấu tin trong ảnh, video, audio được IEEE xuất bản từ năm 1996 đến năm 2015.

Những thông tin trong hình 1.5 và 1.8 [**12**] mặc dù đã cũ (do các tài liệu mà luận án tham khảo chỉ cập nhập đến năm 2007-2008) so với thời điểm thực hiện nội dung nghiên cứu của mình, tuy nhiên vì nhiều lý do khác nhau, những số liệu thống kê về nghiên cứu bảo mật thường ít được công bố trên các phương tiện thông tin. Ngoài ra, các thuật toán giấu tin cũng như các kỹ thuật watermark đều không được công bố rộng rãi vì lý do nhạy cảm cũng như các ứng dụng của nó đối với an ninh thương mại điện tử, đặc biệt là quốc phòng-an ninh. Luận án cũng chưa tìm thấy các thống kê về nghiên cứu này ở các mốc thời gian những năm gần đây.

Từ các hình 1.4, 1.5 và 1.8 cho thấy tỷ lệ giữa giấu tin giữa các định dạng đa phương tiện là khác nhau, trong đó, giấu tin trong ảnh chiếm tỷ lệ lớn nhất. Giấu tin trong ảnh được sử dụng nhiều nhất vì các lý do như dễ thực hiện nhất, tỷ lệ giấu được nhiều thông tin nhất và hiện nay ảnh số được sử dụng nhiều nhất trên mạng viễn thông nói chung. Ngoài ra giấu thông tin trong ảnh chiếm tỉ lệ lớn nhất trong các chương trình ứng dụng, các phần mềm, do lượng thông tin được trao đổi bằng ảnh là rất lớn.

Cover type	Count
Audio	445
Disk space	416
Images	1689
Network	39
Other files	81
Text	255
Video	86

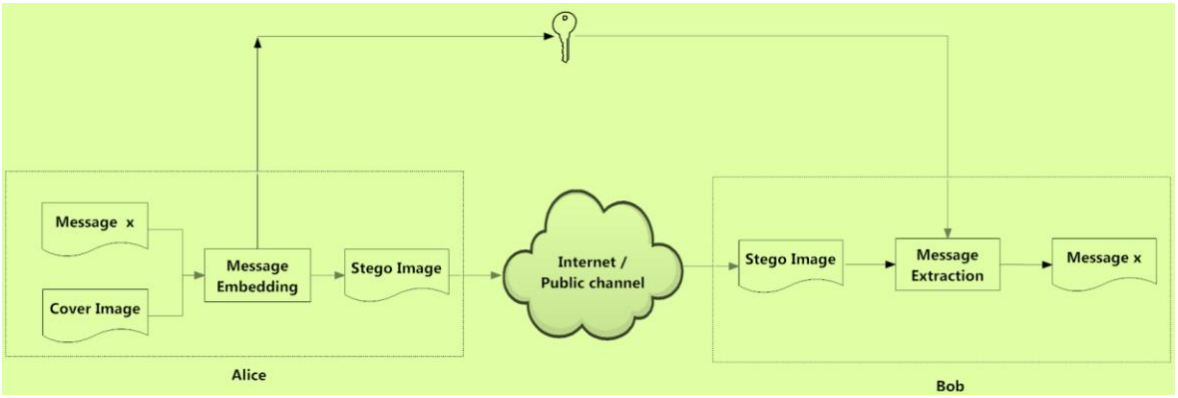


Hình 1. 5. Tỷ lệ và số lượng các ứng dụng giấu dữ liệu trong dữ liệu đa phương tiện năm 2008.

Giấu tin trong ảnh gồm hai giai đoạn: nhúng thông tin vào ảnh gốc và tách thông tin đã giấu. Để tăng cường độ an toàn cho thông tin đem giấu, thường thì

trước khi giấu thông tin có thể được mã hóa bằng kỹ thuật mã hóa nào đó [**3**], [**25**]. Trong quá trình tách tin, người ta thực hiện các bước ngược lại.

Theo [**11**], đối với dữ liệu hình ảnh, tính che giấu của phương pháp giấu tin có thể được đánh giá thông qua chất lượng ảnh chứa tin so với ảnh gốc bằng hệ số PSNR (Peak Signal-to-Noise Ratio). Lược đồ nào có giá trị PSNR càng lớn thì chất lượng ảnh càng cao (tính che giấu càng cao). Theo [**24**] ta có sơ đồ quá trình giấu tin điển hình như hình 1.6 sau.



Hình 1. 6. Sơ đồ quá trình giấu tin trong ảnh

Một số phép biến đổi được sử dụng chủ yếu trong quá trình giấu tin và tách tin như sau: các phép biến đổi cosine, wavelet, fourier rời rạc.

Để nâng cao tính bền vững, các thuật toán giấu tin thường biến đổi ảnh số từ miền không gian sang một miền biểu diễn mới (miền biến đổi), hay còn gọi là miền tần số và lựa chọn những đặc trưng thích hợp để nhúng tin, sau đó dùng phép biến đổi ngược tương ứng để chuyển dữ liệu từ miền biến dổi về miền không gian. Một số phép biến đổi thường được sử dụng như: DCT và DWT, NMF (Non-negative Matrix Factorization) [**26**], SVD (Singular Value Decomposition) và phép biến đổi QR. Nhóm kĩ thuật này sử dụng một phương pháp biến đổi trực giao nào đó, chẳng hạn như Cosine rời rạc, hay Fourier… để chuyển miền không gian ảnh sang miền tần số. Thuỷ vân sẽ được nhúng trong miền không gian tần số của ảnh theo kĩ thuật trải phổ trong truyền thông. Đây là kĩ thuật phổ biến nhất với nhiều thuật toán và

được hứa hẹn là một phương pháp tốt giải quyết vấn đề đảm bảo hai thuộc tính quan trọng của thuỷ vân sau khi giấu.

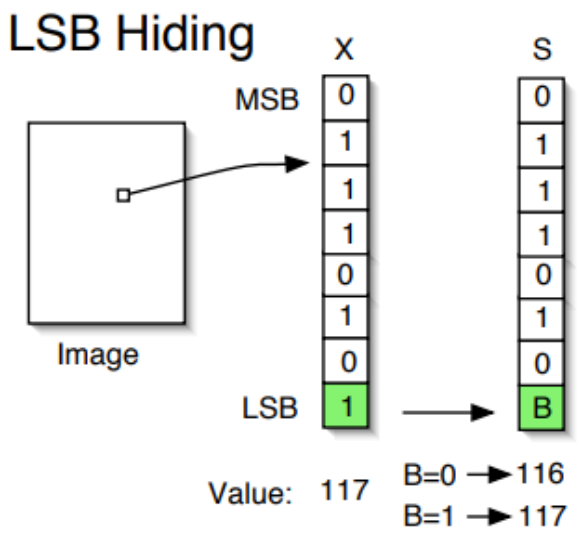
Biến đổi cosine rời rạc được thực hiện theo chuẩn nén ảnh JPEG, miền dữ liệu pixel của ảnh được chia thành các miền nhỏ (thường là kích cỡ 8x8 hoặc 16x16 pixel) sử dụng phép biến cosine rời rạc được các hệ số cosine [**27**], thông tin thường được giấu vào các hệ số cosine có giá trị lớn nhất hoặc nằm ở miền tần số giữa như các kỹ thuật giấu [**28**], [**29**].

Biến đổi wavelet rời rạc, sử dụng phép biến đổi wavelet rời rạc biển đổi miền dữ liệu pixel thành bốn băng tần mới LL, LH, HL, HH. Các giá trị trên bốn băng tần này gọi là các hệ số wavelet. Theo nhận định của những nhà giấu tin thì khi có thay đổi nhỏ các hệ số wavelet trên hai băng tần cao LH và HL (một số kỹ thuật giấu sử dụng cả băng tần HH) sẽ ít ảnh hưởng đến chất lượng trực quan của ảnh ban đầu như các kỹ thuật giấu [**27**], [**30**].

1.2.3.2. Giấu tin trên LSB

Các kỹ thuật giấu tin trong ảnh [**31**] phổ biến nhất hiện nay là kỹ thuật giấu tin trên LSB (Least Significant Bit) vì thay đổi trên bit LSB ít ảnh hưởng đến chất lượng ảnh theo khả năng cảm nhận của con người. Đây là phương pháp thay thế các bit thông tin vào bit LSB của điểm ảnh [**27**], và là hướng tiếp cận của luận án đối với nội dung nghiên cứu về giấu tin trong ảnh số. Kỹ thuật LSB được mô tả như ở hình vẽ 1.7 [**4**] dưới đây.

Trong một điểm ảnh của ảnh 8-bit cấp độ xám có thể biểu diễn dưới dạng chuỗi nhị phân 8 bit (giả sử điểm ảnh p có giá trị 236 có thể biểu diễn thành chuỗi nhị phân 8 bit là “11101100”) thì 7 bit liên tiếp đầu tiên (là chuỗi bit “1110110”) gọi là các bit MSBs (Most Significant Bit) có ý nghĩa quan trọng nhất đối với điểm ảnh, còn bit cuối cùng (bit “0”) gọi là bit LSB vì có ảnh hưởng ít nhất đến sự thể hiện của điểm ảnh. Do vậy, việc thay đổi giá trị của bit LSB (từ “0” sang “1” hay từ “1” sang “0”) không làm ảnh hưởng nhiều đến chất lượng của ảnh.



Hình 1. 7. Giấu tin vào bit LSB, lúc này giá trị điểm ảnh từ 1 thành 0

Vi dụ, xem xét một bức ảnh đa mức xám 8-bit, mỗi điểm ảnh (pixel) chứa một byte giá trị xám. Giả sử rằng, 8 điểm ảnh đầu tiên của ảnh gốc có giá trị sau:

10010111 10001100 11010010 01001010 00100110 01000011 00010101 01010111

Các bit LSB đã được tô đậm, màu đỏ. Để giấu chữ A có giá trị nhị phân là **01000001** vào ảnh trên, chúng ta cần thay thể các LSB của các điểm ảnh và giá trị mới của ảnh trên là:

10010110 10001101 11010010 01001010 00100110 01000010 00010100 01010111

Nhìn vào ví dụ trên ta thấy rằng trong 8 điểm ảnh đầu tiên, chỉ có điểm ảnh thứ 1,2,6,7 (màu xanh) là thay đổi từ 0 sang 1 hoặc ngược lại, các điểm ảnh còn lại 3,4,5,8 (màu đỏ) trùng với giá trị nhị phân chữ A nên không bị thay đổi.

Ví dụ, trong ảnh 24 bit màu, mỗi màu được biểu diễn bởi 24 bit tương ứng với ba màu RGB, mỗi màu chiếm 1 byte [**32**]. Người ta sử dụng một tính chất của mắt người là sự cảm nhận về màu B (Blue) kém sơn so với màu RG, vì thế ta thường chọn bit cuối cùng trong 8 bit biểu diễn màu B của mỗi điểm ảnh để giấu tin. Thay đổi bít cuối cùng trong 8 bit biểu diễn màu B chỉ làm giá trị biểu diễn màu B tăng hoặc giảm đi 1 đơn vị. Do vậy các bit ít quan trọng nhất trong trường hợp này là bit thứ 24 của mỗi điểm ảnh. Một số thuật toán muốn giấu nhiều hơn và chất lượng ảnh thấp hơn có thể sử dụng bit cuối cùng của mỗi byte biểu diễn mỗi màu RGB làm bit

ít quan trọng nhất. Trong trường hợp này thì mỗi điểm ảnh sẽ chọn ra được 3 bit LSB. Tuy nhiên phương pháp này cũng có nhiều hạn chế như không đảm bảo tính bền vững của thủy vân đối với các thao tác như quay hay nén ảnh JPEG chẳng hạn.

Hiện nay kỹ thuật giấu tin trên LSB vẫn tiếp tục được ưa chuộng và sử dụng phổ biến nhất vì nó rất đơn giản và có khả năng giấu được nhiều thông tin. Mỗi điểm ảnh có thể nhúng được một bit thông tin, do đó tỉ lệ nhúng lớn nhất là một bit thông tin trên một điểm ảnh (hay độ dài bit thông tin có thể nhúng bằng số điểm ảnh của ảnh).

1.2.3.3. Một số phương pháp giấu tin mật khác

a. Một số phương pháp giấu tin khác của LSB

- *Phương pháp tăng giảm LSB:* bít thông tin sẽ được so sánh với bit LSB của điểm ảnh được chọn (có thể tuần tự hoặc ngẫu nhiên). Nếu bit thông tin cùng giá trị với bit LSB của điểm ảnh cần giấu thì coi như sẽ giấu 1 bit thông tin đó vào điểm ảnh này, ngược lại bit LSB sẽ được XOR với 1 để cùng giá trị với bit thông tin đó [**2**].

- *Phương pháp đồng chẵn lẻ:* trong phương pháp này, người ta chia miền không gian ảnh thành nhiều khối bằng nhau, bit thông tin được giấu vào từng khối theo nguyên tắc số bit 1 của khối LSB là lẻ nếu bit thông tin cần giấu là 1 và ngược lại, số bit 0 của khối LSB là chẵn nếu bit thông tin cần giấu là 0. Trường hợp không trùng, ta thay đổi giá trị LCB đó để bảo đảm "đồng chẵn lẻ" với bit thông tin cần giấu [**33**].

- *Kết hợp các phương pháp giấu LSB khác nhau:* phương pháp tuần tự (bit LSB được chọn để giấu thông tin có thể chọn theo thứ tự tuần tự), phương pháp ngẫu nhiên (bit LSB được chọn để giấu thông tin có thể chọn theo thứ tự ngẫu nhiên), phương pháp tăng giảm (bit LSB được chọn sẽ giữ nguyên nếu trùng với bit thông tin, và ngược lại bit LSB đó sẽ tăng/giảm 1 để trùng với bit thông tin), phương pháp đồng chẵn lẻ) cùng với một số thao tác nào đó nhằm nang cao hiệu quả an toàn cho thông tin được giấu. Các phương pháp đều nhằm bảo đảm cho kỹ thuật giấu tin trong miền không gian không bị phá vỡ trước các phép tấn công hình học [**2**].

- *Phương pháp giấu tin theo hình thức chèn nhiễu SS:* Dữ liệu đem giấu sẽ được điều biến thành một chuỗi tín hiệu mang thông tin theo một hệ số bền vững α, sau đó được chèn vào dữ liệu ảnh gốc. Điển hình là phương pháp của J.Cox, ảnh gốc sẽ được biến đổi Cosine và chọn ra một lượng hệ số DCT [**34**] [**35**]. Theo J.Cox, các biểu thức hiệu chỉnh này cho phép giấu thông tin bền vững trong ảnh trước các tấn công nhiễu và một số phép biến đổi hình học.

- *Phương pháp giấu tin điều chỉnh hệ số lượng tử QIM:* là một phương pháp giấu khá phổ biến do Chen và Wornell giới thiệu [**36**], mặc dù kỹ thuật giấu hơi phức tạp và khả năng giấu thấp hơn kỹ thuật giấu LSB, nhưng cũng giống như kỹ thuật giấu SS, QIM làm cho thông tin có thể bền vững trước các tấn công hình học và nhiễu. Có nhiều phương pháp giấu tin đề xuất theo hình thức giấu này.

- *Ngoài ra còn có Kỹ thuật mở rộng sai phân DE (Difference Expansion):* do Tian đưa ra (2002) [**37**], đây là kỹ thuật giấu tin dựa trên mở rộng hệ số sai phân của điểm ảnh dữ liệu ảnh được tính sai phân theo biểu thức (2.15), thông tin được giấu trên LSB của các hệ số sai phân sau khi được mở rộng. Năm 2003, W.Ni và cộng sự đề xuất kỹ thuật giấu thuận nghịch dựa trên dịch chuyển biểu đồ tần suất gọi là NSAS [**38**].

Hiện nay, có rất nhiều phương pháp giấu tin khác đã và đang được các nhà khoa học trên thế giới tiếp tục nghiên cứu, cải tiến.

b. Thuật toán giấu tin kinh điển của Wu-Lee và thuật toán CPT

+ Năm 1998, M. Y. Wu và J. H. Lee đề xuất thuật toán giấu tin Wu-Lee theo khối [**39**], trong đó một ảnh nhị phân dùng làm môi trường giấu tin được chia thành các khối đều nhau, mỗi khối là một ma trận nhị phân. Thông tin mật là một bít mật được giấu vào mỗi khối này bằng cách thay đổi nhiều nhất một bit của khối. Kỹ thuật giấu thông tin trong ảnh đen trắng do M.Y.Wu và J.H.Lee vẫn dựa trên tư tưởng giấu một bit thông tin vào một khối ảnh gốc nhưng đã khắc phục được phần nào những tồn tại của mã hóa khối bằng cách đưa thêm khoá K cho việc giấu tin và đưa thêm các điều kiện để đảo bit trong mỗi khối, theo điều kiện đó các khối ảnh gốc toàn màu đen hoặc toàn màu trắng sẽ không được sử dụng để giấu tin. Quá trình

biến đổi khối ảnh F thành F’ để giấu 1 bit b được thực hiện theo công thức SUM(K^F’) mod 2 = b; Công thức này cũng được sử dụng cho quá trình tách, lấy tin đã giấu. Đánh giá về thuật toán giấu tin Wu-Lee là chỉ có thể giấu được 1 bit thông tin vào một khối m×n bit và cũng chỉ thay đổi tối đa 1 bit, ngoài ra khả năng bảo mật không tốt.

+ Kỹ thuật giấu tin của Chen-Pan-Tseng [**40**] sử dụng một ma trận khoá K và một ma trận trọng số W trong quá trình giấu và tách thông tin. Quá trình biến đổi khối ảnh (ma trận nhị phân) F thành F’ kích thước m×n để giấu dãy r bit thông tin $b_1b_2\ldots b_r$ được thực hiện sao cho: $SUM((F' \oplus K) \otimes W) \equiv b_1b_2...b_r \pmod{2^r}$. Công thức trên được sử dụng để tách chuỗi bit đã giấu $b_1b_2...b_r$ từ khối ảnh F’. Thuật toán CPT cho phép giấu giấu được tối đa r = log2(mn+1) bit dữ liệu vào khối ảnh kích thước m×n (với $2^r < m \times n$) bằng cách chỉ thay đổi nhiều nhất 2 bit trong khối ảnh gốc. Một số thử nghiệm về đánh giá thuật toán CPT cho thấy nếu độ lớn bản tin nhỏ cho giá trị PSRN trung bình đạt được khá cao và hiệu quả tốt; tuy nhiên khi khi tăng độ lớn bản tin, giá trị PSRN sẽ giảm và nhiễu tăng; Khả năng của giấu tin phụ thuộc vào việc chọn khóa K và ma trận trọng số W, Khả năng bảo mật của thuật toán CPT cao hơn so với thuật toán WL. Ngoài ra việc trao đổi/phân phối khóa là vấn đề quan trọng mà các thuật toán trên không đề cập đến.

- Một số nghiên cứu liên quan: Luận án tiến sỹ Huỳnh Bá Diệu (2017) “Một số kỹ thuật giấu thông tin trong âm thanh số” [**41**], luận án tiến sỹ Nguyễn Hải Thanh (2012) “Nghiên cứu phát triển các thuật toán giấu tin trong ảnh và ứng dụng trong mã đàn hồi” cũng đề xuất cải tiến thuật toán CPT. Ngoài ra, Yu-Chee Tseng; Hsiang-Kuang Pan (2001) [**40**]; Hioki Hirohisa (2003) đã đề xuất một thuật toán CPT cải tiến nhằm tăng chất lượng ảnh có giấu tin. Ahmed Al-Jaber và Khair Eddin Sabri (2005) có đề xuất một phương pháp giấu 4 bít trong khối ma trận nhị phân 5×5 mà không sử dụng ma trận trọng số như trong phương pháp CPT. Ở Việt Nam cũng có nhiều công trình nghiên cứu về giấu tin mật đã được các nhóm của Học viện Kỹ thuật Quân sự (Đào Thanh Tĩnh), Viện CNTT - Viện Khoa học và Công nghệ Việt Nam (Nguyễn Xuân Huy), Trường Đại học Giao thông Vận tải (Phạm

Văn Ất), Trường Đại học Công nghệ - Đại học Quốc gia Hà Nội (Trịnh Nhật Tiến) [**2**], Vũ Bá Đình, Nguyễn Xuân Huy, Đào Thanh Tĩnh (2002) "Đánh giá khả năng giấu dữ liệu trong bản đồ số" [**42**], Vũ Văn Tâm, Phan Trọng Hanh (2014) "Một phương pháp mới nhúng dữ liệu vào tín hiệu audio" [**43**], Bùi Văn Tân (2012) "Nâng cao hiệu quả giấu tin trong ảnh nhị phân", [**44**]….

=> Từ 2 thuật toán WL, CPT và một số thuật toán cải tiến khác, NCS nhận thấy chủ yếu là các thuật toán cải tiến từ mã khối. Từ năm 2000 đến nay đã có rất nhiều nghiên cứu để đưa ra cải tiến các thuật toán WL, CPT. Hơn nữa, WL và CPT vừa phức tạp lại vừa không giấu được nhiều thông tin mật là yêu cầu cần có của các kỹ thuật giấu tin mật (Steganography). NCS nhận thấy tài liệu [**4**] là sách chuyên khảo tương đối tổng quát nhất về giấu tin trong đa phương tiện gồm các nguyên tắc, các thuật toán và ứng dụng.

=> Từ 2 thuật toán WL, CPT và một số thuật toán cải tiến khác đã có nhiều nghiên cứu nhằm mục đích ngược lại là phát hiện ảnh có giấu tin. Hai hướng nghiên cứu về phát hiện ảnh có giấu tin dựa trên các thuật toán giấu tin như đã trình bày ở trên là: thuật toán phát hiện mù (blind steganalysis) và thuật toán phát hiện có ràng buộc (constraint steganalysis) [**2**]. Trong thực tiễn, phát hiện ảnh có giấu tin có 2 ý nghĩa: thứ nhất phục vụ đắc lực cho an ninh quốc phòng, thứ 2 nâng cấp và thúc đẩy các nghiên cứu mới về kỹ thuật giấu tin trong ảnh tốt hơn.

Do vậy NCS không lựa chọn hai thuật toán WL, CPT để cải tiến mà sử dụng các thuật toán cơ bản [**4**] và đề xuất cách giải quyết của mình.

1.2.3.4. Tính chất kỹ thuật giấu tin

Các kỹ thuật giấu tin đều có một số tính chất (khả năng) chung giống nhau như: khả năng nhúng tin, khả năng che giấu (tính ẩn) và khả năng bảo mật [**12**], [**45**].

a. Khả năng nhúng tin

Khả năng nhúng tin của một thuật toán giấu tin là số bít dữ liệu có thể nhúng được trên một đơn vị dữ liệu môi trường. Thuật toán nào nhúng được nhiều dữ liệu hơn thì có khả năng nhúng tin cao hơn và ngược lại. Khả năng nhúng tin là một

trong những tính chất quan trọng nhất của kỹ thuật giấu tin. Thường người ta đo khả năng giấu tin bởi tỷ lệ giấu tin , tức là tỷ số giữa các bít thông tin giấu được so với số lượng các LSB của ảnh mà không làm ảnh hưởng đáng kể chất lượng của ảnh.

b. Khả năng che giấu (tính ẩn)

Hệ số PSNR được dùng để tính toán khả năng che giấu của thuật toán giấu tin [**46**]. Giá trị PSNR càng lớn, khả năng che giấu càng cao và ngược lại. Hệ số PSNR giữa ảnh mang tin S (Steago) so với ảnh gốc C (Cover) kích thước m x n được tính theo công thức (1.3) dưới đây.

$$\text{PSNR} = 20\log_{10}(\text{MAX}/\text{sqrt}(\text{MSE})) \quad (1.3)$$

Còn tham số MSE được tính như sau:

$$MSE = \frac{1}{mn}\sum_{i=1}^{m}\sum_{j=1}^{n}[C(i,j) - S(i,j)]^2 \quad (1.4)$$

Trong đó, MAX là giá trị cực đại của điểm ảnh và MSE là sai số bình phương trung bình. Giá trị PSNR tính theo đơn vị decibel (dB).

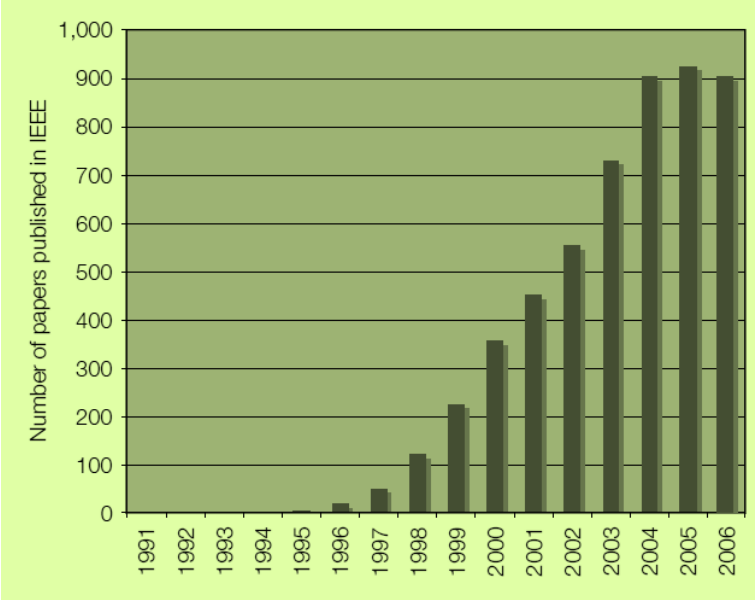
Đối với một thuật toán giấu tin, khả năng nhúng tin và khả năng che giấu có quan hệ mật thiết với nhau. Đối với mỗi thuật toán giấu tin, khi tăng dữ liệu nhúng thường làm giảm chất lượng ảnh chứa tin. Do vậy, tùy thuộc vào từng trường hợp, các thuật toán giấu tin đưa ra những giải pháp khác nhau nhằm cân bằng hai tính chất này.

c. Tính bảo mật

Tương tự như các hệ mật mã, các thuật toán giấu tin thường được công khai khi ứng dụng. Do đó, sự an toàn của phương pháp giấu tin phụ thuộc vào độ khó của việc phát hiện ảnh có chứa thông tin mật hay không. Mỗi khi thu được các ảnh số, làm thế nào để phát hiện được trong các ảnh đó, ảnh nào nghi có chứa thông tin ẩn? Đối với các hệ thống thông tin liên lạc bí mật, khi sử dụng các thuật toán giấu tin chúng ta cần bảo mật được các thuật toán giấu tin đó để bảo đảm ảnh chứa tin mật không bị phát hiện và không thể tách thông tin đã giấu ra khỏi ảnh đó khi bị tấn công trên đường tuyền.

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

1.2.4.1. Khái niệm và nghiên cứu liên quan



Hình 1. 8. Nghiên cứu về Steganography và Digital Watermark được IEEE công bố từ 1991 đến 2006

Trái với giấu tin mật trong ảnh số đã trình bày trong 1.2.3, kỹ thuật watermark là những kỹ thuật giấu tin được dùng để bảo vệ đối tượng chứa thông tin giấu; có nghĩa là nó được dùng để bảo vệ "vật mang tin" S. Hình 1.8 cung cấp thông tin các nghiên cứu được công bố trên IEEE từ năm 1991 đến 2006 về Steganography và Digital Watermark [**12**]. Thủy vân (Watermark) là một kỹ thuật nổi tiếng được dùng để bảo vệ và đánh dấu bảo mật trong thông tin kỹ thuật số, đã được khai thác thành công trong lĩnh vực âm nhạc và lưu trữ dữ liệu video, ảnh số và truyền thông.

Kỹ thuật thủy vân số được định nghĩa như là một quá trình chèn (nhúng) thông tin "đánh dấu" và dữ liệu đa phương tiện nhằm mục đích chính là bản quyền sản phẩm đa phương tiện. Việc nhúng dấu watermark vào các dữ liệu đa phương tiện có thể làm giảm chất lượng của "vật mang tin" S nhưng nó chính là "dấu vết" nhằm xách định tính xác thực của "vật mang tin" S hoặc dùng để chứng minh bản quyền của "vật mang tin" giữa người gửi và người nhận.

Việc đánh dấu bảo mật watermark nhằm bảo đảm an toàn cho "vật mang tin" mặc dù thuật toán thực hiện là công khai. Việc trao đổi khoá bí mật được thông qua nhiều hình thức trao đổi khoá khác nhau nhưng trong luận án này không đề cập đến.

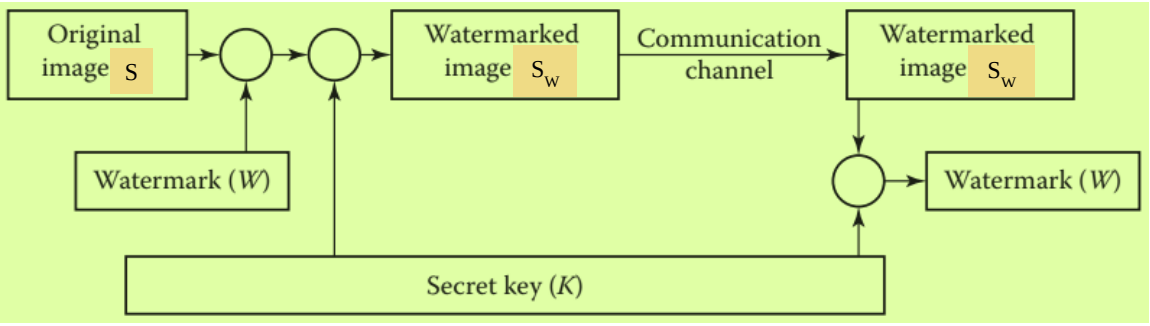
Đối với thủy vân số (Digital Watermark), trong phạm vi của luận án, NCS chỉ ứng dụng các kỹ thuật hiện có này đưa vào ảnh số là "vật mang tin" làm công cụ đánh giá và phân tích hiệu năng chống lại tấn công, tính xác thực mà không đặt vấn đề nghiên cứu. Mỗi một phương pháp giấu tin tốt trên ảnh số có thể được sử dụng nhằm đánh giá ưu nhược điểm để từ đó hỗ trợ, tham khảo cho việc nghiên cứu giấu tin trên các định dạng đa phương tiện khác như âm thanh, video…

Một bộ watermark có các thành phần chính: 1. "Vật mang tin" S trước khi nhúng thủy vân số; 2. Thành phần watermark W; 3. Hàm nhúng E và 4. Khoá k. Từ các thành phần này, chúng ta có phương trình biểu diễn "vật mang tin" S sau khi được đánh dấu bảo mật watermark là

$$S_w = E_k\{S,W\} \tag{1.5}$$

Vật mang tin S_w đủ lớn để thực hiện các hoạt động xử lý tín hiệu số như lọc số, nén tín hiệu số, truyền thông số… Thứ nhất, S_w được hiểu là để bảo đảm khả năng trích xuất watermark ngược lại từ thông tin nhận được. Thứ 2, yêu cầu về sự "tàng hình" của thủy vân số, tức là hệ thống sẽ vẫn hoạt động bình thường khi đưa vào tín hiệu S hay tín hiệu S_w. Ngữ cảnh kỹ thuật ở đây là việc đưa thêm S_w vào hệ thống sẽ không yêu cầu phải thay đổi, bổ sung hay điều chỉnh phần cứng hoặc phần mềm.

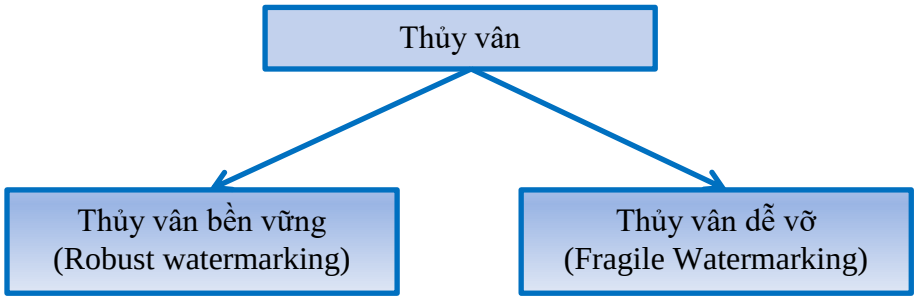
Theo [**3**], ta có sơ đồ tổng quát quá trình watermark như trong hình 1.9 sau.



Hình 1. 9. Sơ đồ tổng quát watermark

1.2.4.2. Phân loại

Kỹ thuật watermark được [**47**] chia thành 2 nhóm như sau:



Hình 1. 10. Phân loại thủy vân số

Thuỷ vân "dễ vỡ" (fragile matermaking) là kỹ thuật nhúng watermark vào trong ảnh sao cho khi truyền ảnh đó trên môi trường công cộng. Nếu có bất cứ một phép biến đổi nào làm thay đổi ảnh gốc đã được đánh dấu thủy vân thì ảnh nhận được sẽ không còn nguyên vẹn so với ảnh nhúng watermark ban đầu (dễ vỡ). Các kỹ thuật watermark có tính chất này được sử dụng trong các ứng dụng nhận thực thông tin và phát hiện xuyên tạc thông tin. Thủy vân dễ vỡ yêu cầu dấu thủy vân phải nhạy cảm (dễ bị biến đổi) trước sự tấn công trên dữ liệu thủy vân. Do vậy, thủy vân dễ vỡ thường được ứng dụng trong xác thực tính toàn vẹn của sản phẩm chứa dấu thủy vân trên các môi trường trao đổi không an toàn. Để xác thực tính toàn vẹn của các sản phẩm chứa dấu thủy vân, thuật toán xác thực thường so sánh sự sai khác giữa dấu thủy vân trích được (W') với dấu thủy vân gốc (W). Nếu có sự sai khác giữa W và W' thì kết luận sản phẩm chứa dấu thủy vân đã bị tấn công, nếu trái lại thì kết luận sản phẩm chưa bị tấn công (toàn vẹn). Ngoài xác thực tính toàn vẹn, một số kỹ thuật thủy vân dễ vỡ còn có khả năng định vị các vùng dữ liệu bị tấn công, mục đích việc định vị này còn giúp cho việc dự đoán được mục đích tấn công của bên thứ 3.

Ngược lại, với kỹ thuật thủy vân dễ vỡ là **kỹ thuật thủy vân bền vững** (robust watermarking). Các kỹ thuật thủy vân bền vững thường được ứng dụng trong các ứng dụng bảo vệ bản quyền. Trong những ứng dụng đó, watermark đóng vai trò là thông tin sở hữu của người chủ hợp pháp. Dấu watermark được nhúng trong ảnh số

như một hình thức dán tem bản quyền. Trong trường hợp như thế, watermark phải tồn tại bền vững cùng với ảnh số nhằm chống việc tẩy xoá, làm giả hay biến đổi phá huỷ dấu watermark. Thủy vân bền vững yêu cầu dấu thủy vân phải ít bị biến đổi (bền vững) trước sự tấn công trên sản phẩm chứa dấu thủy vân, hoặc trong trường hợp loại bỏ được dấu thủy vân thì sản phẩm sau khi bị tấn công cũng không còn giá trị sử dụng. Do vậy, những lược đồ thủy vân bền vững thường được ứng dụng trong bài toán bảo vệ bản quyền. Theo [**48**] các phép tấn công phổ biến nhằm loại bỏ dấu thủy vân đối với ảnh số là nén JPEG, thêm nhiễu, lọc, xoay, cắt xén, làm mờ, thay đổi kích thước, thay đổi cường độ sáng, thay đổi độ tương phản.

Do vậy, đối với loại thủy vân này, tính bền vững và tính che giấu được quan tâm hơn so với các tính chất còn lại của phương pháp giấu tin.

Thủy vân bền vững lại được chia thành hai loại là thủy vân ẩn và thủy vân hiện. Watermark hiện là loại watermark được hiển thị ngay trên sản phẩm đa phương tiện và người dùng có thể nhìn thấy được. Các dấu watermark hiện trên ảnh dưới dạng chìm, mờ hoặc trong suốt để không gây ảnh hưởng đến chất lượng ảnh gốc. Đối với watermark hiện, thông tin bản quyền được hiển thị ngay trên sản phẩm. Còn đối với watermark ẩn thì cũng giống như giấu tin, bằng mắt thường không thể nhìn thấy dấu thủy vân. Trong vấn đề bảo vệ bản quyền, watermark ẩn được dùng vào việc phát hiện sản phẩm đa phương tiện bị đánh cắp hoặc đánh tráo. Người chủ sở hữu hợp pháp sẽ chỉ ra bằng chứng là watermark ẩn đã được nhúng trong sản phẩm đa phương tiện bị đánh cắp đó hoặc bị đánh tráo.

Luận án "Nghiên cứu phương pháp bảo mật thông tin được giấu trong ảnh số" nhằm giải quyết vấn đề: là bảo mật nơi gửi và nơi nhận bản (kẻ tấn công bị động sẽ tìm cách thu lấy bản rõ trước khi mã hóa và sau khi mã dịch nếu chúng biết được nơi gửi và nơi nhận bản mã. và đánh giá khả năng an toàn của hệ thống phục vụ chống lại các tấn công chủ động lên đường truyền (ảnh giấu tin được bảo vệ bằng thủy vân số bền vững). Trong phần tổng quan (mục 1.1) NCS có trình bày về 2 hình thức tấn công là tấn công chủ động (Active) và tấn công bị động (Passive). Việc lựa chọn thủy vân số chính là kiểm chứng việc bản tin hình ảnh nhận được có bị tấn

công chủ động dẫn đến sửa đổi hay chèn thông tin giả; ngoài ra đối phương có thể gây nhiễu đường truyền để gây trễ (quá giờ hẹn) hoặc thậm chí làm cho 2 bên không nhận được thông tin cần trao đổi bí mật [**49**]*? Ngoài ra hiện nay thủy vân ẩn bền vững được quan tâm nghiên cứu nhiều nhất nhờ ứng dụng của nó trong bảo vệ ảnh số. Trong phạm vi nghiên cứu, luận án không đặt vấn đề nghiên cứu mới đối với thủy vân số mà chỉ ứng dụng kỹ thuật thủy vân số để tập trung đánh giá khả năng an toàn của hệ thống khi bị tấn công. Do vậy luận án lựa chọn thủy vân hiển bền vững để thực hiện việc mô phỏng đánh giá trong chương 3, cũng như thử nghiệm trong chương 4. Khối S_w trong hình 1.11 nhằm mục đích nói trên.*

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

1.3.1. Đánh giá hiệu suất xử lý ảnh có đánh dấu watermark

Các mạng cảm biến không dây (WSNs) đóng vai trò then chốt trong quá trình phát triển của Internet vạn vật (IoT). Trong đó, đặc biệt là các mạng cảm biến ảnh không dây (Wireless Image Sensor Networks: WSN) có hàng loạt ứng dụng trong cả an ninh-quốc phòng và dân sự đã và đang thu hút rất nhiều hướng nghiên cứu gần đây. Tương tự như các hạ tầng truyền thông, vấn đề an ninh mạng luôn được đề cao trong các mạng cảm biến WSNs. Cụ thể, một số kỹ thuật bảo mật về nhận thực đã được đề xuất, trong đó kỹ thuật đánh dấu bảo mật watermark được coi là cách tiếp cận đầy hứa hẹn cho các loại mạng này do tính phổ biến và đơn giản khi sử dụng.

Những năm gần đây, các mạng cảm biến không dây được xem như phần quan trọng trong thời đại của kết nối vận vật qua Internet. Chúng có ý nghĩa lớn trong việc truyền thông tin đa dịch vụ cho nhiều ứng dụng khác nhau. Trong đó, mạng cảm biến ảnh không dây WSN, nơi các nút được trang bị các camera thu nhỏ để cung cấp các thông tin dưới dạng hình ảnh là một công nghệ đầy hứa hẹn cho dự báo, theo dõi, giám sát hoặc các ứng dụng yêu cầu an toàn. Bên cạnh những lợi ích hiện hữu, WSN phải đối mặt với nhiều thách thức như thời gian hoạt động, hiệu năng mạng do hạn chế về băng thông, năng lượng hay bảo mật [**50**].

Trong nhiều ứng dụng dựa trên nén và truyền ảnh, kỹ thuật nén là giải pháp nhằm tối ưu quá trình xử lý ảnh độc lập. Theo đó, tiêu chuẩn nén JPEG hoặc JPEG2000 [**51**] là một trong những kỹ thuật phổ biến được sử dụng trong WSNs do tính tiện lợi và hiệu quả [**52**], [**53**]. Kể từ đó, liên tiếp những nghiên cứu tập trung vào khảo sát độ phức tạp các thuật toán biến đổi, đảm bảo năng lượng hoặc hiệu năng mạng cho các môi trường ứng dụng cụ thể.

Từ khía cạnh an ninh, tài nguyên hạn chế để xử lý bảo mật trong WSNs là một thách thức cố hữu. Do đó, 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 [**54**], [**55**].

Qua tìm hiểu, NCS chưa tìm thấy nghiên cứu nào đánh giá đồng thời cả hai nội dung: so sánh hiệu năng lỗi khi dùng các thuật toán biến đổi khác nhau và đánh giá xác suất phát hiện watermark đối với vấn đề an ninh bảo mật trong mạng WSN khi bị tấn công.

Từ đó, cần phải có đánh giá trên cơ sở xem xét và so sánh hiệu năng lỗi trên JPEG/JPEG2000 và kỹ thuật watermark dựa trên biến đổi trong miền tần số là biến đổi Cosin rời rạc (DCT) và biến đổi Wavelet rời rạc (DWT) cho mạng cảm biến ảnh không dây điển hình. Thứ hai, xác suất phát hiện watermark tại nút đích được tính toán trong hai phương thức nêu trên nhằm đề xuất phương thức đánh dấu bảo mật watermark tốt nhất dựa trên kết quả được đưa ra bằng mô phỏng số.

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 không đi sâu vào khai thác các thuật toán mới dành cho watermark và coi đó là kỹ thuật bảo mật dành cho truyền ảnh trên các mạng vô tuyến. Do đã có nhiều công trình phát triển theo hướng tiếp cận này [**12**] nên luận án chỉ tập trung vào giải quyết vấn đề đánh giá độ an toàn cũng như hiệu năng chống lại các tấn công kỹ thuật watermark đối với ảnh số.

Hiện nay hệ số PSNR được sử dụng làm phương pháp đánh giá độ an toàn về khả năng che giấu (tính ẩn) trước sự cảm nhận của con người giữa ảnh gốc và ảnh sau khi giấu tin [**12**]. Theo cách tiếp cận này, cảm nhận của con người được chia làm năm mức độ khác nhau. Trên mỗi mức, chất lượng ảnh sẽ được tính theo PSNR, sau đó tùy vào giá trị tính được mà ảnh sẽ được đánh giá là thuộc vào ngưỡng nào. Công thức (1.3) và (1.4) đã trình bày về cách tính toán về chất lượng ảnh. Chất lượng PSNR được ánh xạ vào thang đo đánh giá bình quân MOS (Mean Opinion Score) theo thông số cho trong bảng dưới đây [**56**].

Bảng 1. 1. Mối quan hệ giữa các giá trị PSNR và MOS

PSRN (dB)	MOS
>37	5 (Rất tốt)
31 -37	4 (Tốt)
25-31	3 (Trung bình)
20-25	2 (Tồi)
<20	1 (Rất tồi)

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

Như chúng ta đã biết, do IEEE 802.11 [**57**] là tiêu chuẩn sử dụng chung nên phải có phương án để xử lý hiện tượng xung đột do bị tấn công từ bên trong hoặc bên ngoài. Đối với một mạng vô tuyến bất kỳ không có cách nào để bên gửi có thể phát hiện được đã có sự xung đột nói trên xảy ra. Vì lý do này, lớp vật lý (MAC) của IEEE 802.11 đã sử dụng giao thức CSMA/CA (Carier sense multiple access/collision avoidance - giao thức đa truy cập/tránh va chạm) để xử lý xung đột. Giao thức CSMA/CA này sử dụng thuật toán Binary Exponential Back-off (BED) để cân bằng truy nhập mạng tránh khả năng xung đột giữa các trạm dùng chung đường truyền (sóng vô tuyến).

Khoảng thời gian ngay sau khi đường truyền đang bắt đầu truyền gói tin (*khoảng thời gian bận*) là khoảng thời gian dễ xảy ra xung đột nhất, nhất là trong

môi trường có nhiều người sử dụng. Khi đó các nút mạng phải đợi đến khi đường truyền rảnh và sẽ thử truyền dữ liệu lại tại cùng một thời điểm. Khi đường truyền rảnh, thuật toán back-off sẽ điều chỉnh để trì hoãn việc truyền dữ liệu của nút mạng, hạn chế tối đa khả năng xảy ra xung đột giữa các nút mạng. Từ đó để nâng cao hiệu suất mạng, một số thuật toán back-off thay thế đã được đề xuất. Một trong số các thuật toán back-off đó là thuật toán EIED (Exponential Increase Exponential Decrease-EIED) đã được đề xuất để thay thế cho thuật toán BEB do nhiều trường hợp đạt hiệu quả về xử lý hiệu suất mạng tốt hơn [**58**], [**59**].

Khi mạng IEEE 802.11 bị tấn công (thông thường hoặc thông minh) từ bên trong hoặc bên ngoài, từ một nút mạng 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 (MAC). Do đó, việc đóng băng back-off đối với các nút lỗi chính 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 hiệu suất xử lý của thuật toán EIED để có đánh giá đầy đủ. Ngoài ra, trong các nghiên cứu [**60**], [**61**], [**62**], [**59**] liên quan, 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 IEEE 802.11 chưa được đề cập đến.

Từ đó NCS đặt vấn đề nghiên cứu và đề xuất mô hình mới về các trạng thái back-off, mô hình kênh và các tham số *lưu lượng truy cập, tỷ lệ rớt gói tin hay độ trễ*, từ đó đánh giá hiệu suất xử lý của thuật toán cũng như việc đóng băng back-off với trường hợp tồn tại các nút lỗi của lớp MAC mạng IEEE 802.11 trong xử lý đa truy nhập bằng thuật toán BEB hoặc EIED khi bị tấn công. Một vấn đề nữa là dựa trên mô hình phân tích đối với thuật toán EIED nhằm loại bỏ các tác động của nút lỗi dựa trên các tham số *lưu lượng truy cập, tỷ lệ rớt gói tin hay độ trễ* đối với lớp MAC của IEEE 802.11.

1.4. Các vấn đề luận án cần giải quyết

Những vấn đề chính cần giải quyết của luận án gồm:

Thứ nhất: Dựa vào phương pháp thay thế bit LSB của mỗi điểm ảnh đã được tìm hiểu trong các kỹ thuật giấu tin mật, luận án cần giải quyết vấn đề sau:

- *Thuật toán giấu tin mật trong ảnh số bằng mã hóa khối 5 bit.*

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

- *Thuật toán đánh giá độ an toàn thông tin được giấu trong ảnh số.*

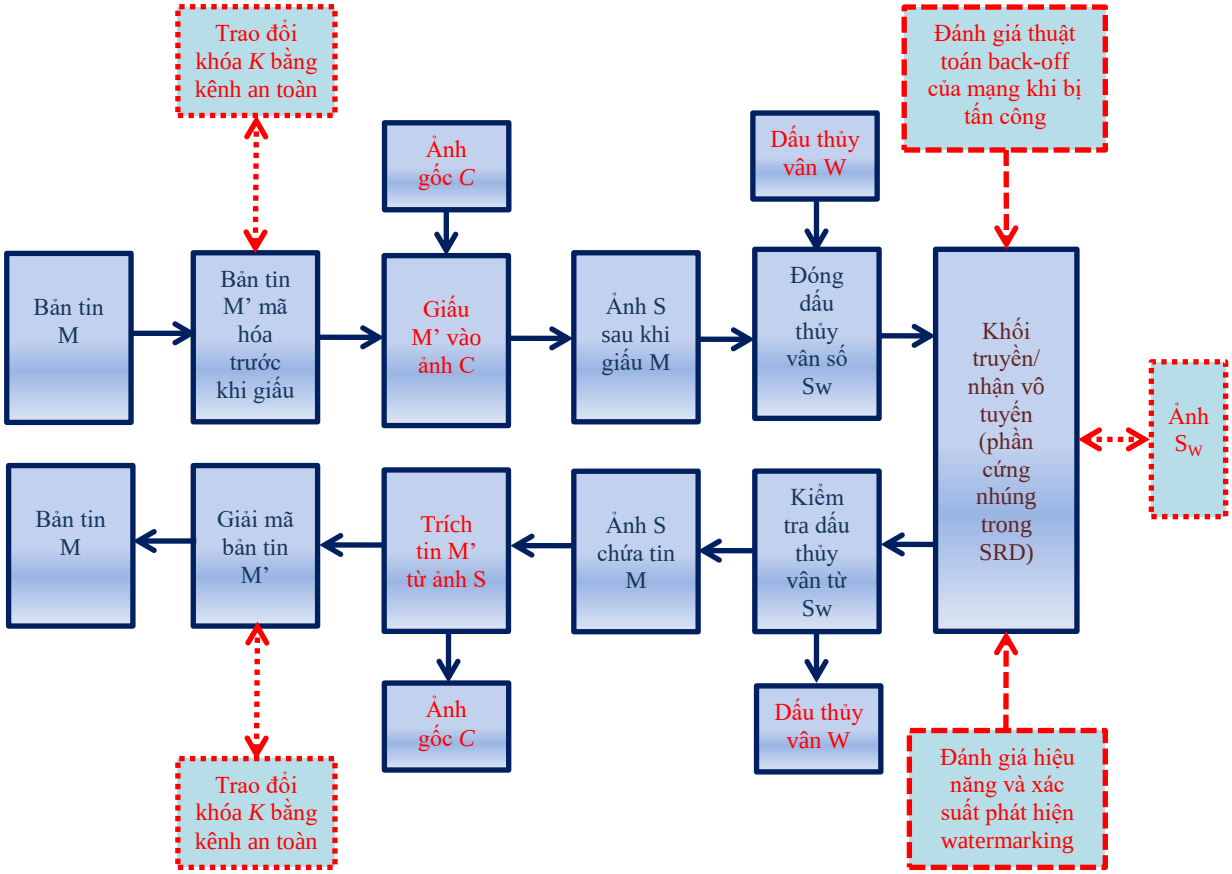
Thứ hai: Qua nghiên cứu vấn đề về bảo mật ảnh số được đánh dấu watermark bằng phương pháp nào là hiệu quả nhất cũng như hiệu suất mạng ảnh hưởng khi bị tấn công, luận án cần giải quyết nội dung sau:

- *Xây dựng mô hình phân tích và đưa ra đánh giá hiệu năng lỗi. Xây dựng thuật toán đánh giá xác suất tìm thấy watermark theo các tham số khác nhau.*

- *Xây dựng mô hình phân tích mới đối với mạng IEEE 802.11 trên lớp MAC sử dụng các thuật toán back-off. Đánh giá hiệu suất các thuật toán back-off khác nhau theo cách tấn công thông thường.*

Thứ ba: Ứng dụng các nghiên cứu ở trên vào hệ thống thông tin liên lạc bí mật phục vụ công tác. Điều này có ý nghĩa thiết thực trong thực tiễn, góp phần làm đa dạng các phương thức liên lạc nghiệp vụ.

Từ các nội dung đã phân tích ở trên, luận án xây dựng sơ đồ tổng quan về hướng tiếp cận và các vấn đề cần giải quyết đối với nghiên cứu một số phương pháp bảo mật thông tin giấu trong ảnh số được biểu diễn trong hình 1.11 dưới đây.



Hình 1. 11. Sơ đồ bảo mật/giải mật thông tin giấu trên ảnh số trong hệ thống thông tin liên lạc bí mật

1.5. Nguồn ảnh dùng để thử nghiệm

Việc lựa chọn nguồn cơ sở dữ liệu ảnh để thử nghiệm trong luận án theo các yêu cầu về độ tin cậy, số lượng ảnh lớn, nội dung đa dạng, do tổ chức có uy tín cung cấp. NCS lựa chọn tập ảnh thử nghiệm từ hai nguồn dưới đây gồm hơn 1000 ảnh, trước khi thử nghiệm được chuyển sang định dạng 24bit và kích thước ảnh phù hợp

- Đại học Washington, khoa Khoa học và kỹ thuật máy tính

http://imagedatabase.cs.washington.edu/groundtruth/

- Đại học Nam California, Viện Xử lý ảnh và tín hiệu

http://sipi.usc.edu/database/database.php

1.6. Kết luận chương 1

Trên cơ sở tìm hiểu tổng quan về các vấn đề nghiên cứu, chương 1 của luận án đã đạt được một số kết quả như sau:

- Nghiên cứu tổng quan về an ninh an toàn và bảo mật trong truyền ảnh số trên mạng vô tuyến

- Tìm hiểu về phương pháp giấu tin mật trong ảnh số và trao đổi khóa bí mật.

- Tìm hiểu về thủy vân số (digital watermarking) và nghiên cứu liên quan.

- Đánh giá hiệu năng lỗi khi bị tấn công trên mạng IEEE 802.11 lớp MAC có đánh dấu watermark.

Qua đó luận án đặt ra 2 bài toán cần giải quyết với các chương tiếp theo

- ***Bài toán 1:*** xây dựng một thuật toán giấu tin mật trong ảnh số và thỏa thuận trao đổi khóa bí mật bằng sinh số giả ngẫu nhiên. Sau đó đánh giá độ an toàn của các thuật toán nói trên đối với hệ thống (*trình bày trong chương 2*).

- ***Bài toán 2:*** đánh giá khả năng bảo mật của hệ thống khi bị tấn công lên ảnh số có đánh dấu watermark và hạ hiệu suất mạng (*trình bày trong chương 3*).

Từ nội dung trên, luận án ứng dụng vào việc xây dựng hệ thống thông tin liên lạc bằng bản tin hình ảnh có bảo mật (*trình bày trong chương 4*).

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

Tóm tắt: *Chương 2 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. 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 [T4]. 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 [T5]. Thứ ba, từ các nghiên cứu về phương pháp đánh giá độ an toàn hệ thống mật mã và giấu tin, luận án đè 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 [T3].*

2.1. Thuật toán giấu tin mật trong ảnh số

Kỹ thuật giấu tin (còn gọi là bảo mật thông tin được giấu) trong trong ảnh số yêu cầu cần thiết đối với sự phát triển của kỹ thuật mật mã. Trong nghiên cứu này luận án tập trung tìm hiểu về kỹ thuật giấu tin mật trong ảnh kỹ thuật số. Từ thuật toán giấu tin đã được công bố và thuật toán đã cải tiến của nó trước đây, luận án trình bày một thuật toán giấu tin mật mới có hiệu quả cao hơn.

2.1.1. Đặt vấn đề

Đã có nhiều thuật toán giấu tin vào ảnh kỹ thuật số được giới thiệu, nhưng phổ biến nhất và được ứng dụng rộng rãi nhất là các thuật toán chèn các thông tin ẩn vào các bit có ý nghĩa thấp nhất (Least Significant Bit - LSB) trong phần dữ liệu ảnh của ảnh kỹ thuật số. Hiện nay người ta thấy rằng không chỉ những bit LSB mà cả những bit mLSB (Với m=1,2) [**63**] của phần dữ liệu ảnh cũng không làm thay đổi đáng kể mà mắt thường khó có thể cảm nhận được. Tuy nhiên việc phát hiện ảnh có chứa

thông tin ẩn bằng thuật toán thống kê cấp 1 hoặc cấp 2 lại tỏ ra rất hiệu quả [**6**], [**1**], [**2**].

Kích cỡ dữ liệu ẩn: Khi muốn nhúng (ẩn) một văn bản hoặc 1 file dữ liệu số nào đó vào một file ảnh gốc ban đầu, trước hết ta cần đảm bảo rằng chất lượng và kích cỡ của file ảnh đó không bị thay đổi. Vì vậy độ dài tối đa của thông tin ẩn so với độ dài của các LSB [**64**]. [**65**] của một file dữ liệu ảnh là:

$$L_{max} \approx 12,5\% L_{LSB} \quad (2.1)$$

Trong đó L_{max} là độ dài tối đa của dữ liệu ẩn và L_{LSB} là độ dài các LSB của file dữ liệu ảnh. Tức là tối đa một điểm ảnh 8 bit chỉ được thay đổi 1 bit (1/8 = 12,5). Nếu tính tất cả các bit của 1 file dữ liệu ảnh thì độ dài $L_{max} \approx 100\%$ L_{BMP} (không vượt quá 100% dữ liệu ảnh của ảnh).

Xác định vị trí dữ liệu ẩn: Mỗi khi muốn đặt các bit thông tin ẩn vào một file ảnh, vấn đề đầu tiên là phải xem đặt thông tin ẩn bắt đầu từ vị trí nào của file dữ liệu ảnh là tốt nhất. Để tăng độ bảo mật cho dữ liệu ẩn thì dữ liệu ẩn này nên được bắt đầu chèn vào phần dữ liệu ảnh tại một vị trí ngẫu nhiên liên quan đến mật khẩu:

$$f(x) = f(C_1, C_2, .. C_n) \quad (2.2)$$

trong đó $(C_1, C_2, .., Cn)$ là một dãy con của dãy ký tự của mật khẩu độ dài n.

Thông thường người ta mã hóa bản tin trước khi nhúng vào ảnh số. Việc mã hóa này nhằm đảm báo độ an toàn cao hơn cho bản tin cần giấu, đặc biệt đối với những thông tin liên quan đến an ninh - quốc phòng v.v... Khi đó cho dù đối phương có thể phát hiện được bản tin giấu vẫn còn một lớp mã hoá bảo vệ nó [**5**].

2.1.2. Đánh giá khả năng giấu tin mật trong ảnh số

2.1.2.1. Đánh giá khả năng giấu tin trong ảnh

Nhiều nghiên cứu đã cho thấy việc giấu tin trong ảnh đen trắng đem lại hiệu quả thấp vì việc biến đổi một điểm ảnh từ đen (0) sang trắng (1) hoặc ngược lại từ trắng sang đen rất dễ tạo ra nhiễu của ảnh và do đó người ta dễ phát hiện được bằng thị giác của con người. Hơn nữa, tỷ lệ giấu trong ảnh đen trắng rất thấp. Chẳng hạn, một bức ảnh đen trắng kích cỡ 300x300 pixels chỉ có hơn 1KB. Trong khi đó một ảnh 24 màu với kích cỡ tương tự có thể giấu được tới 200KB. Ngoài ra, ảnh đen

trắng hiện nay ít được sử dụng, thay vào đó là ảnh màu, đa cấp xám. Để chọn ảnh màu, đa mức xám làm ảnh môi trường cho việc giấu tin, ta cần quan tâm đến các bit có ý nghĩa thấp nhất được ký hiệu là LSB, vì khi LSB bị thay đổi thì màu sắc của ảnh đó không thay đổi đáng kể so với màu sắc của ảnh ban đầu. Nhưng làm thế nào để xác định được LSB của mỗi điểm ảnh? Việc xác định LSB của mỗi điểm ảnh trong một bức ảnh phụ thuộc vào định dạng của ảnh đó và số bit màu dành cho mỗi điểm ảnh đó.

Đối với ảnh 16 bit màu hoặc 24 bit màu thì việc xác định LSB tương đối đơn giản. Riêng ảnh đa mức xám thì bảng màu của nó đã được sắp xếp sẵn. Trong các ảnh đó những cặp màu trong bảng màu có chỉ số chênh lệch càng ít thì càng giống nhau. Vì vậy, đối với ảnh đa mức xám LSB của mỗi điểm ảnh là bit cuối cùng của điểm ảnh đó [**32**].

Quá trình tách LSB của các điểm ảnh đa mức xám để tạo thành ảnh thứ cấp các bit này bằng thuật toán như thuật toán giấu tin trong ảnh đen trắng sẽ làm cho chỉ số màu của mỗi điểm màu thay đổi tăng hoặc giảm đi một đơn vị (hình 1.7). Do đó điểm ảnh mới sẽ có độ sáng tối của ô màu liền trước hoặc sau ô màu của điểm ảnh của điểm ảnh môi trường (ảnh gốc). Bằng mắt thường người ta khó phát hiện được sự thay đổi này. Thực nghiệm chỉ ra rằng, ngay cả khi ta đảo toàn bộ LSB của tất cả điểm dữ liệu ảnh trong một ảnh 8 bit đa cấp xám thì cũng không gây ra sự khác nhau nhiều [**65**], [**66**].

a. Đối với ảnh số 8 bit màu

Những ảnh thuộc loại này gồm ảnh 16 màu (4 bit màu) và ảnh 256 màu (8 bit màu). Khác với ảnh đa mức xám ảnh màu với số bit màu bé hơn hoặc bằng 8 không phải luôn luôn được sắp xếp bảng màu. Những màu ở liền kề nhau có thể rất khác nhau. Chẳng hạn, màu đen và màu trắng có thể được sắp xếp kề nhau trong bảng màu. Do đó việc xác định LSB là rất khó khăn. Nếu ta làm như đối với ảnh đa mức xám, tức là vẫn lấy bit cuối cùng của mỗi điểm ảnh để tạo thành ảnh thứ cấp thì mỗi thay đổi 0 sang 1 hoặc 1 sang 0 trên ảnh thứ cấp thì có thể làm cho màu của ảnh môi

trường và màu tương ứng của ảnh kết quả sẽ khác nhau rất xa đến mức mắt thường có thể phân biệt được, dù rằng chỉ số màu của chúng chỉ tăng giảm đi 1 bit mà thôi.

Nhưng làm thế nào để biết được màu nào đã được dùng màu nào không được dùng đến? Để trả lời câu hỏi này trước hết ta phải duyệt toàn bộ các màu trong bảng màu và đánh dấu những màu có chỉ số xuất hiện trong dữ liệu ảnh đó là những màu đã được dùng. Giả sử có một màu C không dùng đến. Với mỗi điểm màu A khi tìm được màu B có sử dụng trong bảng màu để sắp cạnh A mà giá trị S(A,B) vẫn còn lớn hơn một ngưỡng nào đó thì ta sẽ chèn ô màu C vào giữa A và B đồng thời đổi lại màu của ô C sao cho giống màu A và B nhất có thể.

Trường hợp số màu được sử dụng bé hơn hoặc bằng 8 (đối với ảnh 256) hay bé hơn hoặc bằng 4 (đối với ảnh 16 màu) thì việc sắp xếp lại bảng màu theo thuật toán trên cho ta kết quả giấu tin rất tốt.

b. Đối với ảnh 16 bit màu

Ảnh 16 bit màu trong thực tế chỉ sử dụng 15 bit cho mỗi điểm ảnh trong đó 5 bit biểu diễn cường độ tương đối của màu đỏ (Red); 5 bit biểu diễn cường độ tương đối của màu xanh lam (Green) và 5 bit biểu diễn cường độ tương đối của màu xanh lơ(blue). 3 bit còn lại không được dùng đến đó là bit cao nhất của byte thứ hai trong mỗi cặp 2 byte biểu diễn một điểm ảnh. Đó chính là LSB của ảnh 16 bit màu. Tuy nhiên ta chỉ lấy những bit này để tạo thành ảnh thứ cấp thì lượng thông tin giấu được sẽ không nhiều. Để tăng tỷ lệ tin giấu đối với ảnh 16 bit màu, ta có thể lấy được nhiều hơn 1 bit của mỗi điểm ảnh.

c. Đối với ảnh 24 bit màu

Ảnh 24 bit màu sử dụng 3 byte cho mỗi điểm ảnh, trong đó, mỗi byte biểu diễn một thành phần trong cấu trúc RGB. Trong mỗi byte, các bit càng thấp càng ít ảnh hướng tới màu sắc của mỗi điểm ảnh. Vì vậy đối với ảnh 24 bit, 3 bit cuối cùng của 3 byte của mỗi điểm ảnh chính là LSB của điểm ảnh đó. Bằng kết quả thực nghiệm cho thấy: Việc thay đổi toàn bộ các bit cuối cùng của mỗi byte trong phần dữ liệu ảnh 24 bít màu cũng không ảnh hưởng đến ảnh gốc [**2**], [**65**].

2.1.2.2. Nhận xét

Một giá trị màu thông thường là một véc-tơ 3 thành phần trong không gian màu RGB [**32**]. Trong đó các màu đỏ (R-Red), xanh lá cây (Green-G), xanh da trời (Blue-B) là những màu nguyên thủy (primary - màu gốc). Mỗi màu trong không gian màu có được chính là tổ hợp của các màu nguyên thủy đó. Như vậy một véc-tơ trong không gian RGB mô tả cường độ của các thành phần R, G, B đó.

Một không gian màu khác cũng được đề cập đến là Y, C_b, C_r. Nó phân biệt giữa độ sáng Y và 2 thành phần sáng tươi (C_b, C_r). Ở đây Y là thành phần sáng (chrominance) của một màu, còn C_b, $C_r$thì phân biệt mức độ màu. Một véc-tơ màu trong không gian màu RGB có thể được chuyển đổi thành Y, C_b, Cr bởi hệ thức sau:

$$\begin{aligned} Y &= 0.299R + 0.587G + 0.114B \\ C_b &= 0,492(B - Y) = - 0,147R - 0,289G + 0,346B \\ C_r &= 0,877(R - Y) = 0,615R - 0,515G - 0,100B \end{aligned} \quad (2.3)$$

Do trong ảnh đa mức xám, bảng màu đã được sắp sẵn và với mỗi điểm ảnh thì bit cuối cùng là LSB của điểm ảnh (gồm 8 bít) đó. Cho nên ta dễ dàng thực hiện việc giấu tin. Do vậy trong phần tiếp theo, luận án chỉ đề cập đến ảnh 24 bit màu.

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 [4]

a. Các tham số đầu vào:

Các ký hiệu: Gọi m là bức thông điệp cần giấu sau khi chuyển sang dãy bít bởi bộ mã ASCII mở rộng, ta được có các thông số đầu vào như sau:

* Cho $m = m_1m_2 ...m_{l(m)}$với $m_i \in \{0,1\}$; i= 1,2,...,l(m) và l(m) là độ dài số bít biểu diễn của thông điệp m.

* Cho $C = C_1C_2...C_{l(c)}$ với $C_i \in \{0, 1\}$; i= 1,2,...,l(c), là ảnh được dùng để giấu thông điệp m.

* Cho $S = S_1S_2...S_{l(c)}$ là ảnh Giấu tin đã được giấu thông điệp m.

b. Thuật toán giấu tin:

Quá trình thực hiện được trình bày trong thuật toán sau:

```
Input: m, C
Output: S
For i=1, 2, 3, ..., l(c), do:
  Si← Ci
end for
for i = 1, 2, 3, ..., l(m), do
  compute index Ji, where to store the i_th message bit:
  Sji← Cji ⇆ mi
end for.
```

c. Thuật toán trích chọn.

```
for i = 1, 2, ..., l(m),
  compute index Ji, where the i_th message bit is store,
  mi ← LSB (Sji),
end for.
```

d. Nhận xét

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 đối với thuật toán giấu tin ban đầu [4]

a. Tham số đầu vào

Để khắc phục nhược điểm của thuật toán giấu tin ban đầu người ta đã đưa ra thuật toán cải tiến được gọi là "Phương pháp khoảng ngẫu nhiên".

Giả sử hai người A và B trước lúc liên lạc với nhau họ thống nhất dùng một khóa K, được gọi là mầm khóa (key seed). Từ mầm khóa K, người ta thống nhất sinh ra một dãy giả ngẫu nhiên (pseudo-random sequence) $k_1,k_2,k_3,..,k_l(m)$ với l(m) là độ dài bản thông báo m, quy ra bit và đặt như sau:

$j_1 = k_1$

$j_i = j_{i-1} + k_i$ $i \geq 2$ tham gia vào việc truyền thông tin.

Từ đó, thuật toán cải tiến trước đây cho thuật toán ban đầu thực hiện như sau:

b. Thuật toán giấu:

```
For i=1,2,3,…l(c)  do
  Si← Ci
end for
Generate random sequence ki, using key seed K,
  ji ← ki
for i = 1, 2, ..., l(m), do
  Sj← Cj ⇆ mi
  ji ← ji-1 + ki
end for.
```

c. Thuật toán trích chọn.

```
Generate random sequence ki, using key seed K,
  ji ← ki
for i = 1, 2, ..., l(m), do
  mi← LSB (si)
  ji ← ji-1 + ki
end for.
```

d. Nhận xét.

Thuật toán cải tiến trước đây 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 do tỷ lệ số bit LSB của ảnh số bị thay đổi lớn hơn 30% trên tổng số bit LSB của ảnh [**64**], [**67**].

Nhưng nếu vậy thì lượng thông tin giấu được vào một ảnh lại không đủ lớn khi kích cỡ ảnh nhỏ. Câu hỏi đặt ra ở đây là: cần phải nghiên cứu và đề xuất một thuật toán giấu tin mật mới sao cho tỷ lệ các bit LSB của ảnh C ban đầu bị thay đổi ít nhất nhưng lại giấu được lượng thông tin càng nhiều càng tốt?

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

Qua phần 2.1.3, cho thấy người ta không thể đồng thời cực tiểu hóa yêu cầu thứ nhất (giảm thiểu số lượng bit LSB của dữ liệu ảnh số bị thay đổi) và tăng tùy ý yêu cầu thứ 2 (tăng tối đa lượng thông tin giấu được vào ảnh số). Để giảm thiểu sự thay đổi các bit LSB của ảnh môi trường sao cho tỷ lệ các bit bị thay đổi so với tổng số bit LSB dưới 10% để chống lại các tấn công bằng các thuật toán thống kê cấp 1 hoặc cấp 2 (theo mô hình Markov ẩn) và bảo đảm được lượng thông tin cần giấu đủ lớn cân bằng với yêu cần thực tế.

Để giấu được nhiều thông tin vào 1 ảnh số mà không làm thay đổi đáng kể đến các LSB của dữ liệu ảnh và đảm bảo bí mật, nghiên cứu sinh bổ sung thêm một lớp mật mã cho thông tin đó, nhằm cân bằng tỷ lệ bit LSB giấu tin đủ nhỏ nhưng lượng thông tin giấu được đủ lớn. Trong nội dung nghiên cứu của mình, luận án xây dựng một bộ mã 5 bit dùng cho thuật toán mới được đề xuất.

2.1.4.1. Một số kiến thức toán học bổ trợ

Ta ký hiệu GF(q)[x] là tập hợp tất cả đa thức cấp n tùy ý p(x), với

$$p(x) = a_0 + a_1x + a_2x^2 + ... + x^n$$

Trong đó $a_i \in GF(q)$ i = 0, 1, ..., n-1 ; q là số nguyên tố.

Ta có các định nghĩa sau đây:

a. Định nghĩa 1: Đa thức $f(x) \in GF(q)[x]$ được gọi là bất khả qui (irreducible) trong trường GF(q) nếu f(x) không thể phân tích được thành tích các đa thức cấp nhỏ hơn cấp của f(x) trong trường GF(q).

- *Ví dụ 1:* Đa thức $f(x) = x^2 + x + 1$ là đa thức bất khả quy trong trường GF(2).

b. Định nghĩa 2: Đa thức nguyên thủy (primitive polynomial). Một đa thức bất khả quy $p(x) \in GF(p)[x]$ có cấp m được gọi là đa thức nguyên thủy nếu số nguyên dương bé nhất n mà $x^n - 1$ chia hết cho p(x) là $n = p^m - 1$.

- *Ví dụ 2:* Đa thức $p(x) = x^3 + x + 1$ là đa thức nguyên thủy trong trường GF(2) vì nó là đa thức bất khả qui và số nguyên dương n bé nhất mà $2^n - 1$ chia hết cho $x^3 + x + 1$ là $n = 2^3 - 1 = 7$.

Thật vậy, $x^7 - 1 = (x^3 + x + 1)(x^4 + x^2 + x - 1)$ và không có một n' < 7 mà $x^{n'} - 1$ chia hết cho $x^3 + x + 1$.

Ta có các định lý sau đây:

c. Định lý 1: Có $\emptyset\ (2^n - 1)/n$ đa thức nguyên thủy cấp n trong trường GF(2). Điều này được chứng minh trong [**68**], trong đó $\varnothing$(n) là hàm Phi-Ơle,

d. Định lý 2: Mọi nghiệm $\{\alpha_j\}$ của một đa thức nguyên thủy cấp m trong trường GF(p)[x] đều có cấp p^m-1. Điều này được chứng minh trong [**69**], [**68**].

2.1.4.2. Bộ mã Hamming

Người ta đã chứng minh được rằng [**68**], [**5**] , một bộ mã Hamming trên trường GF(2) thỏa mãn các điều kiện:

+ Độ dài $n = 2^m - 1$

+ Số các ký hiệu mang thông tin là $k = 2^m - m - 1$

+ Số các ký hiệu kiểm tra chẵn lẻ là $m = n - k$

Khi đó, khả năng sửa sai của bộ mã là t = 1.

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

Vận dụng một số kết quả ở trên, luận án xây dựng bộ mã 26 chữ cái La tinh như sau: Giả sử $p(x) \in GF(2)[x]$ là một đa thức nguyên thủy cấp 5 trên trường GF(2). Lúc đó, ta biết rằng [**68**] sẽ có $\emptyset\ (2^5 - 1)/5$ đa thức nguyên thủy có cấp 5. Một trong những đa thức nguyên thủy cấp 5 trong trường GF(2) là $p(x) = x^5 + x^2 + 1$.

Gọi α là một nghiệm của p(x), tức là $p(\alpha) = 0$ hay $\alpha^5 + \alpha^2 + 1 = 0$.

Từ đó suy ra:

$$\alpha^5 = \alpha^2 + 1 \qquad (2.4)$$

Trong không gian véc tơ nghiệm của đa thức p(x) có cấp 5, tức là có cực đại 5 véc tơ độc lập tuyến tính. 5 véc tơ này sẽ tạo thành một cơ sở của không gian nghiệm. Bằng cách trực chuẩn hóa cơ sở này, nhận được một cơ sở của không gian nghiệm của (2.4) là:

α^0 = 1 0 0 0 0

$\alpha^1 = 0\ 1\ 0\ 0\ 0$

$\alpha^2 = 0\ 0\ 1\ 0\ 0$

$\alpha^3 = 0\ 0\ 0\ 1\ 0$

$\alpha^4 = 0\ 0\ 0\ 0\ 1$

Từ (2.4) ta có $\alpha^5 = 1\ 0\ 1\ 0\ 0$, tiếp tục $\alpha^6 = \alpha^3 + \alpha = \alpha^3 + \alpha^1 = 0\ 0\ 0\ 1\ 0 + 0\ 1\ 0\ 0\ 0 = 0\ 1\ 0\ 1\ 0$, .v.v.

Cuối cùng ta đã xây dựng bộ mã trong Bảng 2.1 sau đây

Bảng 2. 1. Bộ mã 5 bit

10000	**01011**	**11000**	**11010**
01000	**10001**	**01100**	**01101**
00100	**11100**	**00110**	**10010**
00010	**01110**	**00011**	**01001**
00001	**00111**	**10101**	
10100	**10111**	**11110**	
01010	**11111**	**01111**	
00101	**11011**	**10011**	
10110	**11001**	**11101**	

Nếu thêm vectơ 00000 vào bảng trên ta sẽ có bộ mã nhị phân gồm 32 từ mã. Với bộ mã này, ta lập tương ứng với 25 chữ cái Latinh (trừ chữ z) vì z có xác suất xuất hiện rất bé trong các bản tin (tỷ lệ khoảng 0,5%) nên ta sẽ sử dụng từ mã đó vào mục đích khác. Từ Bảng 2.1, ta tiếp tục xây dựng bảng 2.2 là bảng mã chữ cái tương ứng với bộ mã của bảng 2.1.

Bảng 2. 2. Bộ mã chữ cái 5 bit

TT	Kí tự	Từ mã	TT	Kí tự	Từ mã
0	**Ông**	**00000**	**16**	**p**	**11111**
1	**a**	**10000**	**17**	**q**	**11011**
2	**b**	**01000**	**18**	**r**	**11001**
3	**c**	**00100**	**19**	**s**	**11000**
4	**d**	**00010**	**20**	**t**	**01100**

5	**e**	**00001**	**21**	**u**	**00110**
6	**f**	**10100**	**22**	**v**	**00011**
7	**g**	**01010**	**23**	**w**	**10101**
8	**h**	**00101**	**24**	**x**	**11110**
9	**i**	**10110**	**25**	**y**	**01111**
10	**j**	**01011**	**26**	**(khóa mã), .**	**10011**
11	**k**	**10001**	**27**	**y/c**	**11101**
12	**l**	**11100**	**28**	**K/g**	**11010**
13	**m**	**01110**	**29**	**tr/lời**	**01101**
14	**n**	**00111**	**30**	**Gấp**	**10010**
15	**o**	**10111**	**31**	**Người nhận**	**01001**

Chú ý: Từ mã “10011” được dùng ở 2 chế độ là báo khóa cho nơi nhận biết trong trường hợp bản thông báo cần mã hóa trước lúc nhúng tin. Nếu không mã hóa thì từ mã này thay vì dấu “.” (stop). Để chống lại việc phát hiện từ khóa, mỗi khi cần dùng nó để mã hóa (DES, hoặc AES hoặc bất cứ khóa mã nào) thì qui định nhóm “10011” xuất hiện đầu tiên (hoặc cuối cùng) sẽ là báo khóa và còn lại là dùng vì dấu “.” (stop).

Ví dụ: Thông báo "K/g Ông Lê Văn Thành” (dùng bộ gõ unicode “K/g Ông Lee Vawn Thanhf”) thì bộ mã tương ứng là:

11010 00000 11100 00001 00001 00011 10000 10101 00111 01100 00101 10000 00111 00101 10100 10011.

Như vậy nếu viết đầy đủ thì sẽ là: “Kinhs guiwr OOng Lee Vawn Thanhf”. Riêng việc xây dựng bộ mã như trên đã giảm được 3 lần so với dùng bộ mã ASCII mở rộng như các thuật toán giấu tin đã được công bố cho đến nay [**2**].

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. Theo 2.1.4.2 về xây dựng bộ mã Hamming, ý nghĩa của việc xây dựng ma trận H chính là chỉ làm sai 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

Trên cơ sở kết quả đã được trình bày ở trên, ta xây dựng được thuật toán giấu tin mới như sau:

Đầu vào:

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

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

Đầu ra:

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

Sau đây là các bước tiến hành:

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

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 gốc C và trích chọn các LSB của các điểm ảnh có hệ số bắt đầu từ i_0 = 1,2,…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

$C_0 = C_0(1)\ C_0(2)\ \ldots.\ C_0\ ([\frac{l(c)}{31}])$ $[\frac{l(c)}{31}]$ là phần nguyên

Bước 4: Chia bản mã y thành từng khối, mỗi khối 5 bit và được kết quả là:

$Y = y(1)\ y(2)\ \ldots.\ (y[\frac{l(m)}{5}] + 1)$

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 thứ cấp C_1 vào đúng vị trí ban đầu như khi ta trích chọn C_0. Cuối cùng ta nhận được ảnh giấu tin S.

2.1.4.5. Ví dụ

Đầu vào: Bản tin m cần giấu "K/g Ông x" và ảnh gốc C.

Đầu ra: Bản tin m và ảnh C được khôi phục.

a. Quá trình giấu:

M="K/g Ông x"<-> 11010 00000 11110 = (m1,m2,m3) (bảng 2.2). Giả sử có 3 dãy LSB của ảnh C là (với giả thiết khởi điểm giấu là i_0=1):

$C_0(1)$=010011 00111 01000 11010 11100 10001

$C_0(2)$=100110 10100 01101 10000 10100 11010

$C_0(3)$=101110 10110 00111 10101 01101 10010

Ta có:

$y_1^T=m_1^T \oplus HC_0^T(1)=(11010)^T \oplus HC_0^T(1)=(11010)^T \oplus (11010)^T \oplus (01111)^T=(\mathbf{10101})^T$

Tồn tại y_1^T trùng với cột thứ 23 của ma trận H (bảng 2.3), ta thực hiện đảo bit của $C_0(1)$ tại vị trí 23 và ta có:

$C_0'(1)$= 010011 00111 01000 11010 1**0**100 10001

$y_2^T=m_2^T \oplus HC_0^T(2)=m_2^T \oplus HC_0^T(2)=(00000)^T \oplus HC_0^T(2)=(00000)^T \oplus (11010)^T \oplus (01010)^T=(\mathbf{01010})^T$

Tiếp tục tồn tại y_7^Tcột thứ 7 của H vậy thành phần thứ 7 của $C_0(2)$ được đảo bit và do đó ta nhận được:

C_0'(2)= 100110 **0**0100 01101 10000 10100 11010

Tương tự, vị trí cột 22 của C_0(3) được đảo bít:

C_0'(3)=101110 10110 00111 10101 **1**1101 10010

Đó là ảnh thứ cấp của ảnh giấu tin S đã giấu thông báo M= "K/g ông X". Sau khi trả lại các LSB tương ứng của ảnh gốc C, ta nhận được ảnh giấu tin S.

b. Quá trình trích chọn:

Đầu vào : ảnh Giấu tin S

Đầu ra: Bản tin M và ảnh C được khôi phục.

Tính $m_i^T = HC_0'(i)$ với i=1,2,3

Ta nhận được 11010 0000 11110↔"K/g Ông x".

2.1.5. Nhận xét và đánh giá

2.1.5.1. Kết quả thực nghiệm so sánh giữa thuật toán giấu tin 5 bit và thuật toán cải tiến cũ trước đây

Một số kết quả so sánh giữa thuật toán giấu tin 5 bit đề xuất mới (mục 2.1.4) và thuật toán giấu tin cải tiến cũ (2.1.3) theo kích thước ảnh không đổi/thay đổi, độ dài bản tin thay đổi/không đổi và tỷ lệ PSRN tương ứng.

Bảng 2. 4. So sánh độ dài bản tin giấu được trong ảnh giữa hai thuật toán

STT	***Kích thước ảnh không đổi***	***Số bit giấu tin thay đổi (bit)***	***Độ dài bản tin giấu của thuật toán giấu tin 5 bit mới (ký tự)***	***Độ dài bản tin giấu của thuật toán giấu tin cải tiến cũ (ký tự)***
1	*768⊗512*	*5190*	***1038***	*649*
2	*768⊗512*	*10380*	***2076***	*1298*
3	*768⊗512*	*15570*	***3114***	*1946*
4	*768⊗512*	*20760*	***4152***	*2595*
5	*768⊗512*	*25950*	***5190***	*3244*

6	768⊗512	31140	**6228**	3893
7	768⊗512	36330	**7266**	4541
8	768⊗512	41520	**8304**	5190
9	768⊗512	62280	**12456**	7785
10	768⊗512	98610	**19722**	12326

- Đánh giá: Cùng số bit, thuật toán 5 bit đề xuất giấu được bản tin có độ dài lớn hơn khoảng 60% lần so với thuật toán cải tiến cũ

Bảng 2. 5. 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 cải tiến 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

- Đánh giá: Với độ dài bản tin không thay đổi, kích thước ảnh thay đổi từ nhỏ đến lớn, tỷ số PSRN của thuật toán 5bit mới cao hơn nhiều so với tiêu chuẩn là 37dB (thấp nhất là 54,01dB, cao nhất lên đến 71.12dB) và cao hơn tương ứng so với thuật toán cải tiến trước đây; Ngoài ra, với các ảnh kích thước nhỏ (từ ảnh 1 đến ảnh 6), tỷ số PSRN của thuật toán cải tiến cũ đều dưới mức 37dB.

Bảng 2. 6. So sánh PSRN giữa hai thuật toán khi độ dài bản tin thay đổi và kích thước ảnh không đổi

STT	Kích thước ảnh không đổi (pixel)	Độ dài bản tin giấu thay đổi (ký tự)	Tỷ số PSRN của thuật toán giấu tin 5 bit mới (dB)	Tỷ số PSRN của thuật toán giấu tin cải tiến cũ (dB)
1	768⊗512	1038	**72,64**	72,59
2	768⊗512	2076	**69,66**	67,65
3	768⊗512	3114	**67,93**	65,97
4	768⊗512	4152	**66,68**	64,72
5	768⊗512	5190	**65,71**	63,73
6	768⊗512	6228	**64,91**	62,94
7	768⊗512	7266	**64,26**	62,31
8	768⊗512	8304	**63,67**	61,70
9	768⊗512	12456	**61,91**	59,94
10	768⊗512	19722	**59,90**	57,92

- Đánh giá: Với độ dài bản tin thay đổi từ nhỏ đến lớn, kích thước ảnh không thay đổi, tỷ số PSRN của thuật toán mới cao hơn so với thuật toán cũ.

2.1.5.2. Nhận xét

Thuật toán giấu tin được trình bày trong phần 2.1.4 trên có ưu điểm là đơn giản cho việc nhúng và trích chọn, ngoài ra lượng thông tin giấu được lớn nhưng các LSB thay đổi ít nhất. Trong phần trình bày trên tỷ lệ nhúng khoảng 3,2% (≈1/31). Nếu tỷ lệ nhúng dưới 10% thì mọi phương pháp dò tìm bằng các thuật toán thống kê đều cho hiệu quả rất hạn chế. Đây là tỷ lệ cho phép chống lại các thuật toán tấn công thông kê cấp 1 và cấp 2, các thuật toán tấn công phát hiện mù trên LSB của miền không gian, thuật toán phát hiện có ràng buộc [**67**] và các thuật toán tấn công đã được công bố trong [**70**], [**64**]. Có thể cải tiến thuật toán này để giảm tỷ lệ làm thay đổi ảnh gốc hơn.

Ngoài ra, trong thuật toán này, ma trận H có thể được mở rộng, chẳng hạn ma trận H có thể có kích cỡ 8 x 255 và như vậy tỷ lệ nhúng (số bit của các pixel bị đảo) còn bé hơn nữa mà vẫn đảm bảo lượng thông tin nhúng là khá lớn (có thể xuống cỡ 0,004). Trong phạm vi nghiên cứu này luận án chỉ dừng lại ở kích cỡ ma trận H là 5 x 31 để bảo đảm cân đối giữa tốc độ tính toán và độ phức tạp của thuật toán. Hiện nay, luận án đang tiếp tục nghiên cứu ma trận H với kích cỡ 6x63 để giảm tỷ lệ tin giấu xuống dưới 1,5%.

2.1.5.3. Đánh giá

Đánh giá sự khác nhau giữa thuật toán giấu tin mật mới với một số thuật toán đã được công bố, ta có.

- Thuật toán mới sử dụng bộ mã 5 bít trên cơ sở bộ mã Hamming trên trường GF(2) với độ dài từ mã là $n = 2^m-1$, ở đây NCS chọn $m = 5$ và do đó $n = 2^5-1 = 31$.

- Trong các thuật toán giấu tin mật đã được công bố, người ta sử dụng bộ mã ASCII mở rộng là 8 bít. Điều này có nghĩa là, cứ mỗi ký tự của bản thông báo cần nhúng sẽ gồm 8 bít.

Giả sử có một thông báo mật cần giấu gồm 100 ký tự La tinh. Như vậy thuật toán giấu phải làm thay đổi là 100.8 = 800 LSB của dữ liệu ảnh gốc. Thuật toán đề xuất sử dụng bộ mã 5 bít nên chỉ có 100.5 = 500 LSB. Hơn nữa, thuật toán mới chỉ giấu các ký tự bản thông báo theo "đại diện", điều này có nghĩa là mỗi ký tự gồm 5 bít ta chỉ cần giấu một bít làm đại diện cho cả 5 bít đó. Vì vậy, bản thông báo gồm 100 ký tự, thuật toán giấu mới chỉ làm thay đổi nhiều nhất là 100 LSB của dữ liệu ảnh gốc. Từ đó, thuật toán mới đã làm giảm được tỷ lệ giấu gấp ít nhất là 8 lần. Kết quả này làm giảm thiểu được khả năng tấn công của đối phương bằng các thuật toán thống kê toán học cấp một hặc cấp hai.

- Việc sử dụng từ mã 5 bít sẽ mã hết toàn bộ 26 ký tự Latinh và dư ra 6 từ mã khác sẽ được dùng cho ký hiệu điều khiển hoặc để mã hóa một số từ thường dùng trong các thông báo chuyên ngành.

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

Trong nội dung nghiên cứu này luận án đề xuất phương pháp sinh dãy số giả ngẫu nhiên có chu kỳ cực đại bằng phương pháp đồng dư tuyến tính với mục đích trao đổi khóa bí mật. Mục đích trao đổi khóa này để tăng tính hiệu quả và đơn giản sử dụng trong liên lạc bí mật. Khóa tạo ra có chu kỳ cực đại, không có chu kỳ con bằng phương pháp đồng dư tuyến tính. Việc tạo ra dãy giả ngẫu nhiên có chu kỳ cực đại (m dãy) còn có ý nghĩa để mã hóa thông tin trước lúc nhúng vào ảnh số và cũng ứng dụng đối với dấu watermark vào ảnh trước khi gửi đi [**71**], [**72**], [**73**], [**74**].

2.2.1. Đặt vấn đề

Việc sinh số ngẫu nhiên có nhiều ý nghĩa trong thực tiễn, đặc biệt trong lĩnh vực bảo mật thông tin, chẳng hạn các khóa mã đòi hỏi phải được chọn một cách ngẫu nhiên, nhằm chống lại các tấn công vét cạn [**75**], [**76**], [**77**].

Hiện nay, một hệ mật mã được cho là an toàn nếu không gian khóa là đủ lớn và việc chọn khóa trong đó phải là ngẫu nhiên theo nghĩa độc lập, đồng xác suất [**78**], [**79**], [**80**]. Tuy nhiên, việc sinh số hoàn toàn ngẫu nhiên bằng các thuật toán là rất khó khăn, tốn kém [**74**], [**81**].

Nội dung này luận án trình bày thuật toán sinh số giả ngẫu nhiên bằng phương pháp đồng dư tuyến tính, dãy số được tạo ra tuần hoàn, có chu kỳ cực đại và không tồn tại chu kỳ con trong khoảng chu kỳ cực đại đó.

2.2.2. Đặt bài toán

Xét phương trình đồng dư tuyến tính [3] có dạng sau:

$$ax \equiv b \bmod n \tag{2.5}$$

[3] Phương trình đồng dư dạng $ax \equiv b \ (mod\ m)$ được gọi là phương trình đồng dư tuyến tính với a,b,m là các số đã biết x_o là một nghiệm của phương trình khi và chỉ khi $ax_o \equiv b \ (mod\ m)$. Nếu x_o là một nghiệm của phương trình thì các phần tử thuộc lớp x_o cũng là nghiệm [**81**].

với *a,b,n* là các tham số nguyên, trong đó n≥2

Để giải phương trình (2.5) ta áp dụng các định lý sau:

2.2.2.1. Định lý 1

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

i) Phương trình (2.5) có *d* nghiệm phân biệt nếu *b* chia hết cho *d* (ký hiệu *d*|*b*).

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

Để chứng minh Định lý 1 ta áp dụng bổ đề sau:

a. Bổ đề: Cho trước 2 số nguyên không âm *a* và *n (với n≥2)* khi đó *a* là khả đảo theo mod *n* nếu và chỉ nếu gcd*(a,n)*=1, tức là *a* và *n* nguyên tố cùng nhau.

b. Chứng minh bổ đề:

Thật vậy, giả sử ngược lại rằng gcd*(a,n)=d, d>1* và có tồn tại một $b \in (0,n)$ sao cho *ab* mod *n* = 1 hay viết cách khác $ab \equiv 1 \bmod n$.

Từ gcd*(a,n)=d* suy ra $a = a_1 d$; $n = n_1 d$; trong đó a_1 và n_1 là hai số nguyên nào đó. Vậy từ (2.5) có thể viết thành các phương trình sau:

$$a_1 db \equiv 1 \bmod n_1 d \tag{2.6}$$

$$\text{hay } ba_1 d = 1 + kn_1 d \tag{2.7}$$

với k là số nguyên nào đó.

Từ (2.5) suy ra $ba_1 d - kn_1 d = 1$ hay $d(ba_1 - kn_1) = 1$

Điều này là không xảy ra nếu *d>1*, nó chỉ xảy ra khi và chỉ khi *d=1* vì $(ba_1 - kn_1)$ là một số nguyên. Vậy bổ đề là đúng.

c. Chứng minh Định lý 1

**** 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 (2.6) ta suy ra phương trình:

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

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 phương trình (2.5) có *d* nghiệm phân biệt là:

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

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 mod *n*.

Trường hợp 1 được giải quyết.

**** Trường hợp 2:*** vô nghiệm nếu *b* không chia hết cho *d* (ký 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 $R \le m$, 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) có thể được viết như sau:

$$a_1 d x_0 \equiv b\ mod\ (n_1 d) \qquad (2.10)$$

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:

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

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≥2, trong đó p là một ước của m;

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

a. Ví dụ

Xét $x_0=3$, a=13, b=7 và m=105. Ta có $(b,m)=(7,105)=1$; $a-1=12$ là bội của 2,3,4,6 (trường hợp này $p=2$); $a-1=12$ là bội của 4; nhưng $m=105$ không phải là bội của 4.

b. Chứng minh Định lý 2

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.

2.2.3. Một số ví dụ chứng minh

Các định lý trên là cơ sở lý thuyết để ta xây dựng dãy giả ngẫu nhiên với chu kỳ lớn tùy ý. Sau đây là hai ví dụ có tính chất thực hành.

2.2.3.1. Ví dụ 1

Cho $y_0 = 3; a = 7; b = 5; m = 27$

Khi đó áp dụng công thức $y_{n+1} = ay_n + b \bmod m = 7y_n + 5 \bmod 27$ ta có:

Bảng 2. 7. Kết quả tính toán giá trị y để xây dựng dãy giả ngẫu nhiên

n	y_n	ay_n	$y_{n+1} = ay_n + b \bmod m$
0	3	21	26
1	26	182	25
2	25	175	18
3	18	126	23
4	23	161	4
5	4	28	6
6	6	42	20
7	20	140	10
8	10	70	21
9	21	147	17
10	17	119	16
11	16	112	9
12	9	63	14
13	14	98	22
14	22	154	24
15	24	168	11
16	11	77	1
17	1	7	12
18	12	84	8
19	8	56	7
20	7	49	0
21	0	0	5
22	5	35	13
23	13	91	15
24	15	105	2
25	2	14	19
26	19	133	3
27	3	21	26

Nếu đổi sang chữ cái với 0 = A, 1 = B,.., 25 = Z thì sẽ được dãy: ZSXEG UKVRQ JOWYL BMIHA FNCTD (số 26 tương ứng với số 0)

2.2.3.2. Ví dụ 2

Cho $y_0 = 3; a = 13; b = 3; m = 1024$

Như vậy các tham số y_0, a, b, m thỏa mãn 3 điều kiện của Định lý 2 ở trên:

- Điều kiện (i): $(b,m)=(3,1024)=1$;
- Điều kiện (ii): $a-1=12=3.4$, ở đây $p=2$
- Điều kiện (iii): $a-1=12=3.4$ là bội của 4 mà m=1024=4.256 là bội của 4.

Khi đó áp dụng công thức $y_{n+1} = ay_n + b \bmod m$ ta có:

Bảng 2. 8. Kết quả tính toán giá trị y để xây dựng dãy giả ngẫu nhiên

n	y_n	ay_n	$y_{n+1} = ay_n + b \bmod m$
0	3	39	42
1	42	546	549
2	549	7137	996
3	996	12948	663
4	663	8619	430
5	430	5590	473
6	473	6149	8
7	8	104	107
8	107	1391	370
9	370	4810	717
10	717	9321	108
11	108	1404	383
12	383	4979	886
13	886	11518	257
14	257	3341	272
15	272	3536	467
16	467	6071	954

17	954	12402	117
18	117	1521	500
19	500	6500	359
20	359	4667	574
21	574	7462	297
22	297	3861	792
23	792	10296	59
24	59	767	770
25	770	10010	797
26	797	10361	124
27	124	1612	591
28	591	7683	518
29	518	6734	593
30	593	7709	544
31	544	7072	931
32	931	12103	842
33	842	10946	709
34	709	9217	4

Lấy các số đầu tiên của dãy ta được: 4, 5, 9, 6, 4, 4, 8, 1, 3, 7, 1, 3, 8, 2, 2, 4, 9, 1, 5, 3, 5, 2, 7, 5, 7, 7, 1, 5, 5, 5, 5, 9, 8, 7, 4.

Chuyển sang dạng ký tự với bảng mã quy định như trong Ví dụ 1 ta được chuỗi: EFJGE EIBDH BDICC EJBFD FCHFH HBFFF FJIHE ….

2.2.4. Nhận xét và đánh giá

Từ công thức $x_{n+1} = ax_n + b \ mod \ m$ ta tìm công thức truy hồi như sau:

$x_1 = ax_0 + b \ mod \ m$

$x_2 = ax_1 + b \ mod \ m = a(ax_0 + b \ mod \ m) + b \ mod \ m$

$x_2 = a^2x_0 + (a+1)b \ mod \ m$

$x_3 = ax_2 + b \bmod m = a(a^2x_0 + (a+1)b \bmod m) + b \bmod m$

$x_3 = a^3x_0 + (a^2 + a + 1)b \bmod m$

....

$$x_{n+1} = a^n x_0(a^{n-1} + a^{n-2} + .. + a^1 + 1)b \bmod m \quad (2.14)$$

Việc tạo dãy số giả ngẫu nhiên vừa được trình bày trong nghiên cứu có một số ưu điểm như sau:

- Chu kỳ R của dãy được kiểm soát nếu thực hiện đúng giả thiết của Định lý 2.

- Việc trao đổi khóa rất đơn giản, chỉ là 4 tham số x_0,a,b,m. Tùy theo yêu cầu của ứng dụng để chọn số *m* cho phù hợp. Hơn nữa thuật toán sinh dãy giả ngẫu nhiên rất đơn giản chỉ áp dụng theo công thức (2.14). Đây là công thức truy hồi để tìm dãy $\{x_n\}$ với n≥2.

- Trường hợp muốn chuyển sang dãy bit giả ngẫu nhiên, ta chú ý đến số tự nhiên đầu tiên của các số trong dãy: số lẻ được gán cho số 1 và chẵn được gắn cho số 0.

Ví dụ: 81, 15, 27, 31, 24,… ⇔ 01010……

Nội dung nghiên cứu có ý nghĩa thực tiễn cho an ninh quốc phòng. Thuật toán này được sử dụng cho việc trao đổi khóa mật mã phục vụ đối với thuật toán 5 bít trong mục 2.1.4 trước bằng hệ mật mã khóa công khai.

Trong hướng nghiên cứu tiếp theo, nhằm đảm bảo an toàn các tham số x_0 , a, b, m trong thuật toán nêu trên luận án sẽ cứng hóa và đưa vào thử nghiệm trên các hệ thống truyền ảnh số nghiệp vụ.

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

Để bảo mật những thông tin quan trọng, bên cạnh ứng dụng kỹ thuật mật mã, người ta sử dụng kết hợp kỹ thuật ẩn giấu thông tin (steganography) nhằm bổ sung cho những khiếm khuyết, tồn tại của hệ thống thông tin được bảo mật **[**82**]**. Với 2 nội dung nghiên cứu trong 2.1 và 2.2 về thuật toán giấu tin mật và thuật toán sinh số giả ngẫu nhiên có chu kỳ cực đại bằng phương pháp đồng dư tuyến tính, cần phải đặt ra vấn đề giải quyết là đánh giá độ an toàn của các thuật toán nói trên.

Bài toán đặt ra: cần có phương pháp tin cậy để đánh giá mức độ an toàn về mặt thực hành cho các hệ thống giấu tin mật có trao đổi khóa bí mật trong ảnh số nói

trên. Dựa vào một số phương pháp đánh giá trước đây, luận án đề xuất một số thuật toán đánh giá độ an toàn đối với hệ thống mật mã giấu tin trong ảnh số.

2.3.1. Đặt vấn đề

Trong nội dung nghiên cứu này, luận án tập trung xây dựng đánh giá mức độ an toàn thông tin đối với hệ thống mật mã và hệ thống kỹ thuật giấu tin trong ảnh số. Trong đó đối với hệ mật mã, nghiên cứu tập trung vào phương pháp đánh giá độ an toàn thông qua chất lượng của dãy giả ngẫu nhiên được sinh ra. Nghĩa là các bit của dãy được thiết bị sinh tạo ra là độc lập và có phân bố xác suất đồng đều và dãy đó gần với dãy ngẫu nhiên. Hiện nay đã có nhiều tiêu chuẩn đánh giá dãy ngẫu nhiên do thiết bị sinh tạo ra **[**75**]**, **[**83**]**, **[**84**]**, **[**85**]**, **[**86**]**.

Còn đối với thuật toán giấu tin, việc đánh giá "khó cảm nhận bằng mắt thường" hoặc "không thể phát hiện bằng phương pháp thống kê" đã được Cachin đưa ra khái niệm về phương pháp đánh giá độ an toàn hoàn hảo **[**7**]**. Tuy nhiên đây là khái niệm đứng từ quan điểm lý thuyết, trong thực tế rất khó thực hiện. Do vậy luận án sử dụng các lý thuyết khác để thực hiện việc đánh giá độ an toàn này theo hướng đơn giản và dễ thực hiện hơn.

2.3.2. Cơ sở lý thuyết

2.3.2.1. Một số bổ đề lý thuyết thông tin

a. Bổ đề A.1 **[**16**]**

Cho f và g là hai hàm số thực, không âm xác định và khả tích đối với độ đo μ_ hữu hạn nào đó trên miền X và thỏa mãn điều kiện tích phân $\int_X (f-g)d\mu \geq 0$. Khi đó ta có tích phân:

$$\int_X f.log\frac{f}{g}d\mu \geq 0 \qquad (2.15)$$

Và nó chỉ bằng 0 khi và chỉ khi $f = g$, μ_ hầu khắp nơi trên X

Chứng minh: Ta chứng minh cho trường hợp f và g là những hàm rời rạc

Giả sử có 2 chuỗi số thực, không âm, hội tụ

$\sum_{i\geq 1} a_i$ và $\sum_{i\geq 1} b_i$; $a_i, b_i \geq 0$ sao cho $(\sum a_i \sum b_i) \geq 0$.

Khi đó, ta sẽ chứng minh rằng $\sum a_i log \frac{a_i}{b_i} \geq 0$ hoặc tương đương

$$\sum a_i log \frac{b_i}{a_i} \leq 0 \qquad (2.16)$$

Trong đó, log là hàm logarit được chọn cơ số tùy ý. Để đơn giản, ta lấy logarit theo cơ số e. Giả sử $x \in [1,1+\varepsilon]$

Bằng khai triển Talor, ta có:

$lnx = \ln\big((x-1)+1\big) = (x-1) - (x-1)^2(2y^2)^{-1}$, trong đó $y \in (1,x)$

Từ đó,

$\sum a_i log \frac{b_i}{a_i} = (\sum b_i - \sum a_i) - \sum a_i (b_i - a_i)^2 (2y^2)^{-1} \leq 0$ với $y_i^2 \in b_i^2, a_i^2$

Điều phải chứng minh.

b. Bổ đề A.2:

Cơ sở đánh giá độ an toàn của một Hệ thống thông tin có bảo mật

Cho $f_1, f_2, \ldots f_n$ với n≥2 là hàm mật độ xác suất trên không gian *X*. Ký hiệu tập hợp G={ $f_1, f_2, \ldots f_n$ }; Giả sử *h* là hàm nào đó trong *G*. Khi đó:

i) Nếu $\int_X hlog \frac{f_i}{f_j} d\mu(x) > 0$ đối với mọi j ≠ i thì $h = f_i$, μ_hầu khắp nơi trên *X*

ii) Nếu có tồn tại một j ≠ i: $\int_X hlog \frac{f_i}{f_j} d\mu(x) < 0$ thì $h \neq f_i$, μ_hầu khắp nơi trên *X*

iii) Nếu $\int_X hlog \frac{f_i}{f_j} d\mu(x) = 0$ $i \neq j$ thì chưa có kết luận.

Trường hợp đặc biệt, nhưng rất quan trọng là *n=2*. Khi đó

$\int_X hlog \frac{f_1}{f_2} d\mu > 0 \Leftrightarrow h = f_1$,

trái lại $\int_X hlog \frac{f_1}{f_2} d\mu < 0$ thì $h = f_2$

Nếu $\int_X hlog \frac{f_1}{f_2} d\mu = 0$ thì chưa có kết luận

Trong đó, hàm logarit được lấy theo cơ số tùy ý. Chứng minh bổ đề A.2 cho trường hợp *n=2*.

Thật vậy, giả sử h ≠ f_1 và $\int_X hlog \frac{f_1}{f_2} d\mu > 0$.

Do G={f_1 , f_2} và $h \in G$, nên $h = f_2$. Khi đó $\int_X f_2 log \frac{f_1}{f_2} d\mu > 0$ hay $\int_X f_2 log \frac{f_2}{f_1} < 0$

Kết quả này trái với bổ đề A.1. Vậy $h=f_1$, μ_hầu khắp nơi trong X

Trường hợp $\int_X h log \frac{f_1}{f_2} d\mu < 0$ được chứng minh tương tự.

Cuối cùng nếu $\int_X h log \frac{f_1}{f_2} d\mu = 0$, lúc đó $f_1 \approx f_2$ trên X nên ta không thể kết luận được.

2.3.2.2. Một số cơ sở lý thuyết xác xuất và thống kê

a. Bổ đề B.1:

Cho hai đại lượng X_1, X_2 độc lập có hàm mật độ lần lượt là $P_1(.)$ và $P_2(.)$ trên không gian S. Đặt $\eta = X_1 + X_2$

Khi đó, đại lượng ngẫu nhiên η có hàm mật độ là

$$p_\eta(x) = \int_S P_1(y) P_2(x-y) dy \qquad (2.17)$$

Chứng minh này đã được trình bày trong [**87**]

b. Hệ quả B.2

Cho X_1, X_2 là hai đại lượng ngẫu nhiên, độc lập, rời rạc: X_1 nhận các giá trị $x_1, x_2, .., x_k$ với xác suất tương ứng là $p_1, p_2, .., p_k$; $(p_i = (X_1 = x_i), i = 1, .., k)$

X_2 nhận các giá trị $x_1, x_2, .., x_k$ với các xác suất tương ứng là $q_1, q_2, .., q_k (q_i = p(X_2 = x_i) i = 1,2, .., k)$

Đặt $Z = X_1 + X_2$. Khi đó, đại lượng ngẫu nhiên Z sẽ nhận các giá trị $Z_1, Z_2, .., Z_k$ với xác suất tương ứng là:

$r_j = p(Z_j) = \sum_{i=1}^{K} p_i q_{j-i}$ với $p_i = p(X_1 = X_i)$; $q_{j-i} = p(X_2 = Z_j - x_i); j = 1,2, .. k$

b. Hệ quả B.3

Cho hai đại lượng ngẫu nhiên X_1, X_2 thỏa mãn các điều kiện của Hệ quả B.2. Nếu một trong hai (chẳng hạn X_1) đại lượng ngẫu nhiên đó có phân bố đều $P_1 = P_2 = \cdots P_k = \frac{1}{2}$. Đại lượng ngẫu nhiên Z cũng có phân bố đều, nghĩa là $r_1 = r_2 =$

$\cdots r_k = \frac{1}{k}$. Chứng minh. Thật vậy, áp dụng kết quả của Hệ quả B.2, ta có với *j=1,2,..,k,*

$$r_j = \sum_{i=1}^{k} p_i q_{j-i} = \sum_{i=1}^{k} p(X_1 = x_i) p(X_2 = Z_j - x_i) = \frac{1}{k} \sum_{i=1}^{k} p(Z_2 = Z_j - x_i) = \frac{1}{k}$$

Hệ quả được chứng minh.

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 ra. Đầu ra đó có thể là dãy các chữ cái latinh, dãy số tự nhiên hoặc dãy nhị phân. Việc đánh giá này liên quan đến bài toán kiểm định các giả thuyết thống kê toán học. 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 độc lập có phân bố xác suất đều.

Trái lại:

H_1: Hệ thống đó sinh dãy giả ngẫu nhiên độc lập nhưng có phân bố không đều.

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 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.

Trong bất cứ một quyết định chiến lược nào, ta đều mắc phải hai sai lầm: Sai lầm xảy ra khi H_0 đúng, nhưng ta lại quyết định bác bỏ nó, được gọi là xác suất sai lầm loại một và được ký hiệu là α ($0 \leq \alpha \leq 1$) và xác suất sai lầm loại hai được ký hiệu là β là sai lầm xẩy ra khi chấp nhận giả thuyết H_0 sai *($0 \leq \beta \leq 1$)* .

Trong thực tế không có quyết định nào lại cực tiểu hóa đồng thời cả hai sai lầm loại 1 và loại 2. Do đó một quyết định được cho là tối ưu nếu cố định xác suất sai lầm loại một α cho trước và cực tiểu hóa sai lầm loại hai β. Bài toán đó đã được

nghiên cứu nhiều trong lý thuyết kiểm định giả thuyết thống kê và không phải là mục tiêu của nghiên cứu này. Nội dung nghiên cứu này chỉ đánh giá mức độ an toàn của hệ thống mật mã dựa trên cơ sở xích markov hữu hạn trạng thái.

Để đánh giá chất lượng của các bản mã do hệ thống sinh tạo ra, ta sẽ đánh giá chất lượng các dãy giả ngẫu nhiên được dùng để mã hóa các bản thông báo một dãy dãy giả ngẫu nhiên được sinh từ hệ thống nào đó được coi là tốt nếu các thành phần của dãy đó là độc lập và có phân bố đều.

Như vậy, một dãy giả ngẫu nhiên hoàn toàn độc lập và có phân bố đều là dãy thuộc xích markov với ma trận chuyển trạng thái là $P = (P_{ij})_{mxm}$ trong đó *m* là số trạng thái khác nhau của xích. Trường hợp đặc biệt nhưng quan trọng là *m=26* (tương ứng với 26 chữ cái la tinh) và $P_{ij} = \frac{1}{26}$ đối với mọi *i,j=1,2,..,26*. Như vậy, *P* là ma trận vuông cấp 26 x 26 với các phần tử bằng nhau và bằng $\frac{1}{26}$

Còn một dãy giả ngẫu nhiên được cho là tồi nếu đó chính là mẫu bản rõ thuộc một ngôn ngữ tự nhiên nào đó (để đơn giản, ta giả thiết đó là ngôn ngữ Tiếng Anh. Như vậy, trong trường hợp này một bản mã chữ cái, tương ứng với 2 bản rõ Tiếng Anh tùy ý cộng với nhau theo modulo 26.

Như vậy, bài toán kiểm định giả thuyết H_0 và theo dõi đối thuyết H_1 như sau:

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 $q_1 = (q_{ij})_{26x26}$, trong đó q_{ij} cho trước hoặc ước lượng được bằng phương pháp thống kê toán học.

Ở đây luận án sử dụng phương pháp cực đại hợp lý (*maximal likelihood estimation*). Trong thực hành, ta lấy mẫu khoảng 10000 chữ cái la tinh. Vì vậy, để đơn giản cho tính toán, trong thực hành ta lấy $p_{ij} = \frac{10000}{26^2} \approx 14,79$ đối với mọi *i,j=1,2,..,26*. Còn $(q_{ij})_{26x26}$ đã được tính toán và cho kết quả trong Bảng 2.4 là Ma trận P_0 được cho ở (2.14) ước lượng bộ đôi móc xích tiếng Anh.

Bảng 2. 9. Ước lượng bộ đôi móc xích tiếng Anh P_0

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	4	21	29	53	2	11	31	4	33	4	6	65	23	171	2	14		87	77	127	7	25	8	1	9	1
B	13				56				8	2		23			11			15	4	2	13				15	
C	33		7	1	71			36	18		10	9	1		51	3		10		29	11				3	
D	41	16	10	5	66	18	3	9	59		1	4	15	6	16	4		21	18	53	21	5	15		3	
E	88	20	58	126	57	41	20	16	51	1	4	56	57	154	35	7	6	194	153	66	9	26	31	13	5	
F	19	3	5	1	19	21	1	3	30	2		11	1		52			26	8	49	7	3	3		2	
G	21	4	3	2	35	1	3	15	18			6	1	4	21	1	1	23	9	21	9		5		1	
H		1	4		271	5	1	6	58				3	2	44	1		3	12	18	6		5		3	
I	40	7	53	24	25	9	11	3			2	38	26	212	58	2	1	46	82	120	1	3		4		3
J	3				5				1						46						3					
K	2				11				13					2	2				6	2	1		2		1	
L	46	2	5	12	65	7	5	2	44	1	1	54	2	2	26	1	1	2	16	23	9		1		34	
M	52	14	1		67			3	1				7	1	17	9	1	2	12	3	8		1		2	
N	42	10	48	126	63	19	107	12	32	1	6	6	9	7	54	7	1	7	47	132	6	5	14		13	
O	7	12	14	17	5	97	3	5	14			19	2	136	13	3		95	23	42	58	16	28		4	1
P	19	1			37			4	8			15	1		28	9		33	14	7	6					
Q																					17					
R	86	8	16	24	177	4	8	8	78	1	10	6	26	16	60	4		24	38	56	6	11	4		29	
S	66	9	17	9	76	13	1	47	78	3		8	11	12	58	7	6	9	48	121	35	1	28		4	
T	59	23	7	1	79	6	2	332	133	1		14	10	6	79	7		51	50	56	21	3	30		25	
U	12	5	9	6	9	1	6		9		1	20	5	31	2	5		48	40	31		3			1	
V	7				77				29						5										3	
W	38	1	1		39			33	36			4	1	8	15				4	2			1			
X	1		2			1			3						1	5				4			1			
Y	15	5	4	2	7	12	2	6	10			3	7	5	20	8		4	16	31			5			
Z	1				4																					

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 ε=*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 [**67**], ta có:

Cho dãy nhị phân $X = x_0x_1 \dots x_{n-1}$, độ dài *n*

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

Bước 2: Đặt $A(d) = \sum_{i=0}^{n-d-1}(x_i \oplus x_{i+d})$.

Bước 3: 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)*.

Bước 4: Nếu lấy α = 0,05 (xác suất sai lầm loại 1). Khi đó tra bảng phân phối chuẩn ta xác định được ngưỡng $t_\alpha = 1{,}6449$ [**67**]. 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,

Bước 5: 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 $G = \left(g_{ij}\right)_{26x26}$

Bước 3: Tính $H = \left(h_{ij}\right)_{26x26}$. Trong đó, $h_{ij} = \left[Klog\frac{0{,}0015n}{g_{ij}}\right]$; *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 được kết quả là ma trận *Q*

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

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 [**88**].

Cho Ω là một hệ thống giấu tin mật. $P_S(.)$ 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 [53] 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 $D(P_c \,||P_s) = 0$ 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 $D(P_c \,||P_s) \leq \varepsilon$ với $\varepsilon \geq 0$ thì thuật toán giấu tin cho trước có độ an toàn ε, trong đó ε là một số thực dương cho trước.

Hệ thống Ω được gọi là có độ an toàn hoàn hảo (perfect secutity) nếu $\varepsilon=0$.Trong đó Vì $D(P_c \,||P_s) = 0 \Leftrightarrow$ phân bố xác suất của ảnh giấu tin S bằng phân bố xác suất của ảnh gốc C tương ứng, tức là kẻ tấn công không phân biệt được đâu là ảnh gốc C và đâu là ảnh có chứa thông tin mật (ảnh stego S). Tuy nhiên trong thực tế điều này không xảy ra, vì nếu như vậy thì ảnh giấu tin và ảnh gốc hoàn toàn giống nhau, tức là $P_S(.) = P_C(.)$ (bổ đề A.1 và A.2). Vì vậy người ta thường chọn độ an toàn ε bảo đảm sự thay đổi giữa ảnh gốc C và ảnh giấu tin S là nhỏ nhất mà mắt người không thể cảm nhận được.

Từ (2.15), ta thấy rằng để thực hiện đánh giá độ an toàn của thuật toán giấu tin rất khó thực hiện trong thực tế. Do đó người ta thường chọn phương pháp đánh giá độ an toàn của thuật toán giấu tin theo cách tiếp cận bằng cảm nhận của mắt người thông qua tham số PSRN trong bảng 1.1. Để từ đó chọn sao cho giá trị của PSRN tính toán được có giá trị > 37 dB ở mức 5.

Trong nghiên cứu của mình, luận án tiếp cận phương pháp đánh giá của [**87**] nhưng giải quyết dựa theo các định lý và bổ đề sau đây

a. Định lý 3.1: Có tồn tại một hệ thống steganography có mức an toàn hoàn hảo.

Chứng minh: Cho *C* là tập hợp tất cả các dãy nhị phân có độ dài *n*, P_c là phân bố xác suất đều trên *C* và lấy $m \in C$ là một bản tin rõ (message). Bây giờ người gửi lấy ngẫu nhiên $c \in C$ rồi tính $s = c \oplus m$. Theo bổ đề B.1 và hệ quả B.2 ta có $P_s(.)=P_c(.)$ và do đó theo bổ đề A.1 và A.2 ta suy ra $D(P_c \,||P_s) = 0$.

Hệ thống steganography nêu trên rất đơn giản nhưng thường không dùng trong thực tế vì như vậy A và B trao đổi dãy ngẫu nhiên cho nhau (chứ không phải bản rõ).

b. Định lý 3.2: Cho Ω là một hệ thống steganography có độ an toàn ε chống lại các tấn công bị động, β là xác suất mà kẻ tấn công không phát hiện ảnh chứa thông điệp ẩn và α là xác suất để kẻ tấn công phát hiện sai ảnh có chứa thông điệp sẽ thỏa mãn: $d(\alpha,\beta) \leq \varepsilon$, trong đó $d(\alpha,\beta) = \alpha log_2 \frac{\alpha}{1-\beta} + (1-\alpha) log_2 \frac{1-\alpha}{\beta}$ với ($0 \leq \alpha, \beta < 1$)

Đặc biệt, nếu α=0, khi đó $\beta \geq 2^{-\varepsilon}$

Chứng minh xem [55 [**87**]

b. Bổ đề 3.3: Giả sử *X,Y* là đại lượng ngẫu nhiên được xác định trên tập *S* với phân bố xác suất lần lượt là $P_X(.)$và $P_Y(.)$; *f* là một ánh xạ $f: S \to T$

Khi đó, $D(P_{T_0} /\!/ P_{T_1}) \leq D(P_X /\!/ P_Y)$, trong đó P_{T_0} và P_{T_1} ký hiệu là các phân bố xác suất của *f(X)* và *f(Y)*

Chứng minh xem [**87**]

Từ định lý 3.1 và 3.2 cùng các kết quả trong 3.3, lấy ε=0,05 và α=0 thì $\beta \geq 2^{-0,05} = \frac{1}{2^{0,05}} \approx 0,966$. Nghĩa là hệ thống an toàn với $\varepsilon=0,05$ thì kẻ tấn công khó có thể dò tìm ảnh chứa thông tin ẩn (xác suất ≥ 97%).

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

Cho *C* là ảnh gốc, còn *S* là ảnh giấu tin 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 gốc *C* và *n* bit LSB của ảnh giấu tin *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 $\{c_1c_2 \dots c_n\}$ và $\{s_1s_2 \dots s_n\}$ 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 thì hệ thống không đáng tin cậy.

2.3.5. Nhận xét và đánh giá

2.3.5.1. Kết quả thử nghiệm của thuật toán trên

Bảng 2. 10. Kết quả Sai phân D(P_c//P_s) 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

Đánh giá: Các kết quả tính toán cho thấy giá trị sai phân Kullback – Leibler D tính được từ thuật toán trong 2.4.3.2 để đánh giá độ an toàn của thuật toán giấu tin 5 bit trong 2.1.4 cho kết quả luôn nhỏ hơn ε = 0,05 (trong điều kiện cụ thể tính toán của luận án) với độ an toàn lên đến trên 98% (tương đương ε = 0,03), vượt mức tối thiểu là 95% (tương đương ε = 0,07).

2.3.5.2. Đánh giá

Dựa trên các kết quả nghiên cứu và xây dựng thuật toán ở trên, cùng với kết quả thử nghiệm, nghiên cứu đã đánh giá mức độ an toàn thông tin đối với hệ thống mật mã và hệ thống kỹ thuật giấu tin trong ảnh số.

Trong đó, đánh giá độ an toàn của hệ thống mật mã dựa vào hệ thống sinh bit giả ngẫu nhiên tùy ý và hệ thống dãy giả ngẫu nhiên dựa trên chữ cái latinh; đối với hệ thống giấu tin mật trong truyền ảnh số, nghiên cứu đã giới thiệu và thử nghiệm trên phân tích về độ an toàn hoàn hảo với các tỷ lệ nhận dạng được thông điệp ẩn có hay không trong ảnh số.

2.4. Kết luận chương 2

Trong chương 2, luận án đã giải quyết ba vấn đề thông qua các nghiên cứu đã được tính toán và chứng minh bằng các ví dụ minh họa rõ ràng.

- 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 [T4].

- 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 [T5].

- Từ các nghiên cứu về phương pháp đánh giá độ an toàn hệ thống mật mã và giấu tin, luận án đã giới thiệu các thuật toán đánh giá độ an toàn đối với 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 [T3].

Hai nội dung nghiên cứu liên quan đến vấn đề bảo mật trong truyền ảnh số là xác suất tìm thấy watermark được đánh dấu trong ảnh số và hiệu suất mạng IEEE 802.11 theo các thuật toán back-off khi bị tấn công thông thường được giải quyết trong chương 3.

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

Tóm tắt: *Mục tiêu chương 3 giải quyết hai vấn đề. Thứ nhất nghiên cứu và 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 để đưa ra lựa chọn phương pháp đánh dấu bảo mật nào đạt hiệu quả nhất khi truyền trên mạng vô tuyến [T6]. Thứ hai, dựa vào các kết quả mô phỏng số cùng với xây dựng mô hình kênh, mô hình thuật toán back-off và các tham số lưu lượng truyền tải, xác suất rớt gói tin và độ trễ truy cập của lớp MAC trong mạng IEEE 802.11, nhằm 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 [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

Trong nội dung này, luận án trình bày một số đánh giá so sánh về hiệu năng lỗi (*Error Performance*) khi sử dụng các kỹ thuật xử lý ảnh theo chuẩn JPEG / JPEG2000 được đánh dấu bảo mật watermark trong môi trường mạng cảm biến ảnh không dây [**89**]. Ngoài ra, luận án cũng trình bày một số phương pháp biến đổi để tìm ra xác suất phát hiện watermark ở phía nhận để xem xét khả năng ảnh số có bị tấn công hay không. Kết quả số được đưa ra nhằm kiểm chứng các phương pháp biến đổi nói trên, từ đó đề xuất phương thức lựa chọn kỹ thuật đánh dấu bảo mật watermark trên ảnh số tốt nhất khi truyền trên mạng cảm biến ảnh không dây WSN.

3.1.1. Một số nghiên cứu liên quan

Kỹ thuật đánh dấu bảo mật watermark là phương pháp bảo mật nhằm cung cấp một số khả năng như phát hiện làm giả, xác thực dữ liệu sở hữu, hiện nay đã được sử dụng rộng rãi trong nhiều ứng dụng an ninh-quốc phòng. Với việc đánh dấu bảo

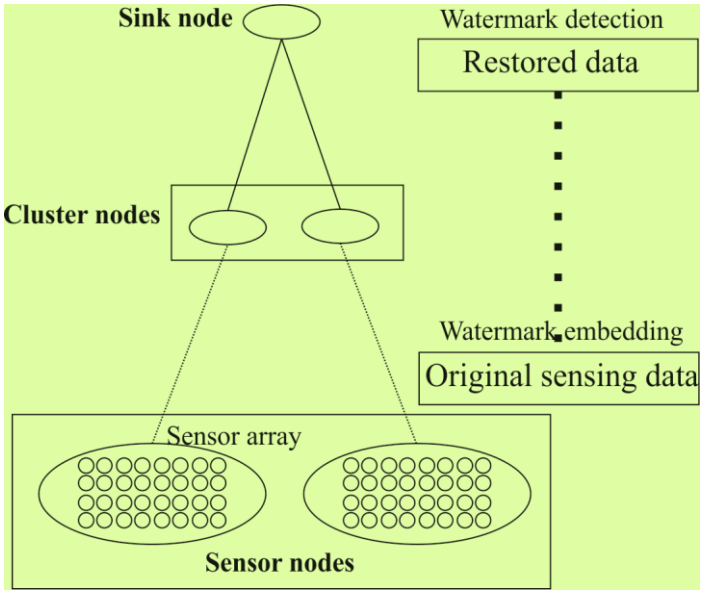
mật watermark vào ảnh, người ta có thể phát hiện hoặc trích dấu watermark nhằm bảo đảm khả năng nhận thực của nó.

Một số mạng WSNs sử dụng ảnh số như là dữ liệu cảm nhận được để truyền trực tiếp thông qua mạng WSN tới nút đích [**90**], [**50**], [**52**], [**53**]. Có nhiều loại watermark (ảnh logo, binary hoặc text [**91**]) được chèn vào ảnh số ban đầu nhằm mục đích đánh dấu bảo mật an toàn. Kỹ thuật đánh dấu bảo mật watermark không chỉ ý nghĩa đối với mục đích nhận thực mà còn đảm bảo dữ liệu trong truyền dẫn [**50**], [**92**]. Nghiên cứu [**93**] sử dụng biến đổi DCT để đánh dấu bảo mật watermark đối với ảnh số cảm nhận được. Nghiên cứu trong [**94**] đã đề cập tới hiệu năng lỗi của JPEG và kỹ thuật nhận thực trong mạng cảm biến không dây dựa trên biến đổi DCT nhưng chưa xem xét tới vấn đề an ninh của mạng khi bị tấn công. Kết quả nghiên cứu trong [**95**], [**96**] mới đề xuất cơ chế tính toán xác suất tìm thấy watermark tại nút đích dựa vào biến đổi DCT chứ không so sánh với biến đổi khác.

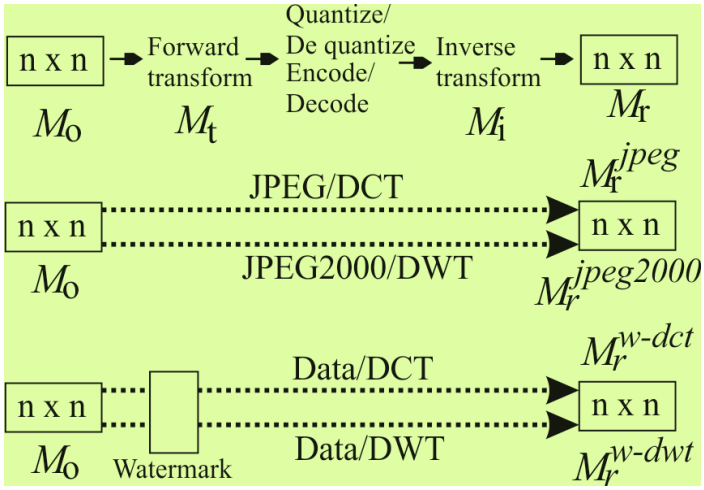
Từ các phân tích trên, luận án nhận thấy cả vấn đề hiệu năng lỗi (Error Performance) và xác suất phát hiện đánh dấu bảo mật watermark đối với hai phương thức biến đổi DCT và DWT đều chưa được nghiên cứu nào đề cập và xem xét đầy đủ. Do vậy luận án tập trung vào so sánh các thông số hiệu năng lỗi với các cơ chế biến đổi khác nhau đối với kỹ thuật đánh dấu bảo mật watermark được sử dụng WSN như sai số trung bình tuyệt đối (Mean Absolute Error - MAE), giá trị trung bình quân phương (Mean Square Error - MSE) và tỷ số công suất tín hiệu trên tạp âm đỉnh (Peak Signal-to Noise Ratio - PSNR).

3.1.2. Các giả định và mô hình thực tế

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).



Hình 3. 1. Mô hình cảm biến hình ảnh không dây đề xuất.



Hình 3. 2. Các kịch bản xử lý ảnh.

Trong đó:

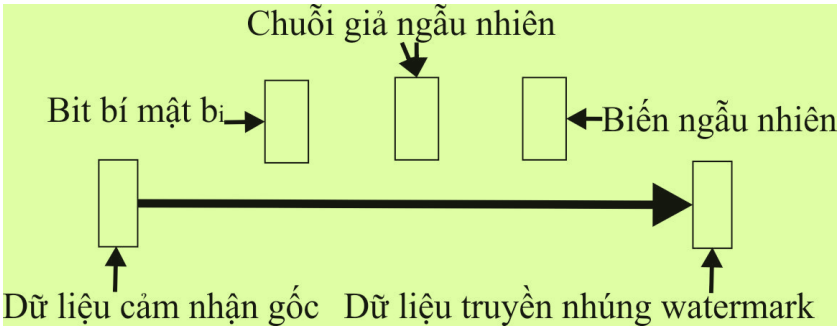
- Ma trận M_O là ma trận điểm ảnh ban đầu
- Ma trận M_t là ma trận chuyển đổi theo từng phương pháp DCT/DWT
- Ma trận M_i là ma trận chuyển đổi ngược
- Ma trận M_r là ma trận điểm ảnh nhận được

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 (*Error Performance*) trong quá trình xử lý được trình bày như hình 3.2.

Một nút cảm biến chứa một ma trận cảm biến điểm ảnh (mảng cảm biến) và mỗi giá trị cảm nhận được phản ánh qua cường độ điểm ảnh. Để đánh giá hiệu năng lỗi, luận án đề xuất xem xét hai khả năng thông tin được truyền tải. Thứ nhất, thông tin cảm nhận của mỗi cảm biến được đánh dấu bảo mật watermark trước khi gửi đến nút cụm. Tại nút cụm, nơi quản lý một tập hợp các nút cảm biến, có nhiệm vụ nén các dữ liệu nhận được và định tuyến tới nút đích. Thứ hai, nút cảm biến gửi dữ liệu đến nút đích mà không nhúng watermark.

Nhằm giảm mật độ phổ công suất tín hiệu tại tần số làm việc về gần với nhiễu nền để gây khó khăn cho kẻ tấn công, luận án sử dụng chuỗi trải phổ trực tiếp (DSSS) đối với dữ liệu watermark để thực hiện nhúng vào thông tin cảm nhận được từ cảm biến. Quá trình nhúng ảnh được trải trực tiếp trên dãy bit tín hiệu.

Sơ đồ khối của quá trình đánh dấu bảo mật watermark được thể hiện trên hình 3.3 dưới đây.



Hình 3. 3. Sơ đồ khối quá trình đánh dấu bảo mật watermark

Theo mô hình đề xuất, toàn bộ ma trận cảm biến được chia thành các khối nhỏ hơn với kích thước *n x n*. Mỗi khối sử dụng một chuỗi trải phổ khác nhau có độ dài *n x n* bit được sinh từ ma trận Hadamard nhằm đảm bảo tính trực giao (trải phổ DSSS). Các bit bí mật được đưa vào cùng với chuỗi giả ngẫu nhiên (mục 2.2) nhằm trộn lẫn khóa. Giá trị watermark được nhúng cũng là một chuỗi ngẫu nhiên sinh ra từ hàm Gauss có độ dài *n* bit. Vì vậy, dữ liệu truyền đi được bảo mật bằng khóa và tích của giá trị watermark nhúng với chuỗi giả ngẫu nhiên.

3.1.3. Các phương trình biến đổi

Biến đổi Cosin rời rạc là phương thức thông dụng đối với chuẩn JPEG. Một số ưu điểm của DCT như: (1) Phần lớn năng lượng tập trung ở thành phần tần số thấp. (2). Có khả năng giảm hiệu ứng chặn. Các ảnh được chia làm các thành phần tần số khác nhau bởi DCT. Bước lượng tử loại bỏ các tần số ít quan trọng và làm tăng mức độ hiệu quả trong việc nén và khôi phục tín hiệu mà không làm suy giảm nhiều nội dung của bức ảnh. Từ [**97**], phương trình biến đổi DCT được biểu diễn như sau

- *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,...,N-1* và *v = 0,...,N-1*

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

- *Phương trình biến đổi ngược*

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

Bước lượng tử tiếp theo nhằm giảm hầu hết các thành phần tần số cao sau khi biến đổi DCT về giá trị *0*. Sau khi lượng tử, ma trận điểm ảnh được quét zig-zag nhằm tối ưu việc nén dữ liệu.

Biến đổi Wavelet rời rạc của chuỗi tín hiệu có chiều dài giới hạn *x(n)* gồm N thành phần, được biểu diễn bởi ma trận *N* x *N*. Các hàm Wavelet được định nghĩa trên khoảng thời gian hữu hạn có giá trị trung bình *0*. Trong phương thức DWT, phương trình biến đổi có thể được thể hiện dưới ba phương trình biến đổi Wavelet 2 chiều dựa trên các biến đổi Wavelet 1 chiều như sau

$$\varphi(x,y) = \varphi(x)\varphi(y) \quad (3.3)$$

Với $\varphi(x)$ và $\varphi(y)$ là các hàm Wavelet 1 chiều.

Khi đó, hàm Wavelet được biểu diễn dưới các hàm Wavelet 1 chiều dưới đây

$$\begin{aligned} \Psi^H(x,y) &= \Psi(x)\,\Psi(y) \\ \Psi^V(x,y) &= \Psi(x)\,\Psi(y) \\ \Psi^D(x,y) &= \Psi(x)\,\Psi(y) \end{aligned} \quad (3.4)$$

Trong đó *H,V* và *D* tương ứng gọi là chiều ngang, chiều dọc và đường chéo Wavelet. Phương trình (3.3) và (3.4) có thể được biểu diễn bởi các hàm kết hợp tuyến tính của hai vector Wavelet

$$\begin{aligned} \varphi(x) &= \sum h_{\varphi}(n)\sqrt{2\varphi(2x-n)} \\ \Psi(x) &= \sum_n^n h_{\Psi}(n)\sqrt{2\,\Psi(2x-n)} \end{aligned} \tag{3.5}$$

Gọi $W_{\varphi}(j,m,n)$ và $W^{i}_{\psi}(j,m,n)$ với $i = H,V,D$ tương ứng là các hệ số đầu ra của biến đổi DWT tại mức *j*. Chuỗi các bộ lọc và giảm mẫu được hoạt động dựa trên tính toán $W^{H}_{\psi}(j,m,n)$. Hiệu năng lỗi được đánh giá bởi các tham số chính như MAE, MSE và PSNR như sau:

$$MAE = \frac{1}{G}\sum_{i=0}^{N-1}\sum_{j=0}^{N-1}|X(i,j) - Y(i,j)| \tag{3.6}$$

$$MSE = \frac{1}{G}\sum_{i=0}^{N-1}\sum_{j=0}^{N-1}[X(i,j) - Y(i,j)]^2 \tag{3.7}$$

$$PSNR = 10log_{10}\frac{255^2}{MSE}(dB) \tag{3.8}$$

Với giá trị của *G* phụ thuộc vào phương thức biến đổi.

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. Các 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.

Để khởi tạo ma trận M_0, luận án sử dụng hàm sinh Gauss để tạo các giá trị phần tử ứng với dữ liệu mà các cảm biến cảm nhận được. Không mất tính tổng quát, ma trận 8x8 được sử dụng đối với mọi trường hợp. Và các phần tử ma trận được tạo bằng cách lấy trung bình của 10.000 quá trình Gauss với các giá trị ngẫu nhiên theo

N(20,4). Bằng cách tương tự, độ lớn của luồng dữ liệu watermark cho mỗi nút được khởi tạo bằng hàm phân bố chuẩn với *N(7,1)*. Ta có

$$M_0 = \begin{pmatrix} 26 & 19 & 26 & 21 & 20 & 21 & 25 & 32 \\ 26 & 19 & 26 & 21 & 12 & 18 & 16 & 23 \\ 26 & 19 & 26 & 21 & 18 & 22 & 24 & 26 \\ 17 & 14 & 26 & 20 & 13 & 23 & 20 & 16 \\ 16 & 14 & 17 & 23 & 23 & 27 & 26 & 18 \\ 29 & 22 & 23 & 30 & 16 & 19 & 12 & 19 \\ 18 & 19 & 23 & 17 & 20 & 11 & 19 & 24 \\ 23 & 19 & 19 & 21 & 18 & 17 & 15 & 19 \end{pmatrix} \quad (3.9)$$

Tại nút đích, các ma trận khôi phục phụ thuộc vào các phương thức biến đổi sau:

$$M_r^{jpeg} = \begin{pmatrix} 23 & 21 & 19 & 18 & 19 & 22 & 26 & 28 \\ 18 & 18 & 18 & 18 & 19 & 20 & 22 & 23 \\ 15 & 16 & 17 & 19 & 19 & 19 & 18 & 18 \\ 15 & 17 & 20 & 22 & 22 & 20 & 19 & 17 \\ 19 & 20 & 23 & 25 & 25 & 22 & 19 & 17 \\ 23 & 23 & 24 & 24 & 24 & 22 & 20 & 19 \\ 24 & 23 & 21 & 20 & 19 & 19 & 19 & 19 \\ 24 & 22 & 18 & 15 & 14 & 15 & 17 & 18 \end{pmatrix}$$

$$M_r^{jpeg2000} = \begin{pmatrix} 22 & 23 & 22 & 20 & 18 & 18 & 24 & 30 \\ 21 & 22 & 22 & 16 & 14 & 16 & 18 & 22 \\ 13 & 17 & 20 & 15 & 15 & 21 & 23 & 24 \\ 14 & 17 & 22 & 20 & 20 & 21 & 21 & 18 \\ 16 & 14 & 18 & 23 & 23 & 26 & 24 & 19 \\ 26 & 23 & 22 & 29 & 29 & 16 & 15 & 14 \\ 18 & 20 & 22 & 17 & 17 & 14 & 17 & 22 \\ 20 & 20 & 20 & 17 & 17 & 14 & 15 & 21 \end{pmatrix}$$

$$M_r^{w-dct} = \begin{pmatrix} 24 & 22 & 22 & 21 & 20 & 23 & 25 & 27 \\ 22 & 22 & 21 & 20 & 19 & 19 & 19 & 20 \\ 15 & 16 & 18 & 19 & 20 & 22 & 22 & 22 \\ 20 & 21 & 22 & 21 & 20 & 18 & 15 & 14 \\ 16 & 17 & 20 & 22 & 23 & 24 & 23 & 23 \\ 23 & 23 & 23 & 23 & 21 & 19 & 17 & 17 \\ 19 & 19 & 19 & 19 & 19 & 20 & 21 & 22 \\ 20 & 19 & 17 & 16 & 15 & 16 & 16 & 18 \end{pmatrix}$$

$$M_r^{w-dwt} = \begin{pmatrix} 23 & 22 & 24 & 21 & 19 & 22 & 24 & 31 \\ 22 & 22 & 21 & 15 & 12 & 15 & 17 & 22 \\ 14 & 17 & 20 & 16 & 17 & 22 & 24 & 25 \\ 14 & 17 & 24 & 20 & 14 & 20 & 20 & 18 \\ 16 & 13 & 17 & 22 & 22 & 27 & 24 & 19 \\ 27 & 23 & 23 & 28 & 18 & 17 & 14 & 17 \\ 17 & 19 & 23 & 28 & 18 & 14 & 18 & 22 \\ 21 & 20 & 19 & 18 & 19 & 16 & 14 & 20 \end{pmatrix}$$

Ma trận lỗi được tính bằng hiệu số giữa ma trận M_r và M_0

$$M_e^{jpeg} = \begin{pmatrix} -3 & 2 & -7 & -3 & -1 & 1 & 1 & -4 \\ -2 & -6 & -3 & 3 & 7 & 2 & 6 & 0 \\ 1 & -1 & -4 & 4 & 1 & -3 & -6 & -8 \\ -2 & 3 & -6 & 2 & 9 & -3 & -2 & 0 \\ 3 & 6 & 6 & 2 & 2 & -5 & -7 & -1 \\ -6 & 1 & 1 & -6 & 8 & 3 & 8 & 0 \\ 6 & 4 & -2 & 3 & -1 & 8 & 0 & -5 \\ 1 & 3 & -1 & -6 & -4 & -2 & 2 & -1 \end{pmatrix}$$

$$M_e^{jpeg2000} = \begin{pmatrix} -4 & 4 & -4 & -1 & -2 & 0 & -1 & -2 \\ 1 & -2 & 1 & 1 & 2 & -2 & 2 & -1 \\ -1 & 0 & -1 & 0 & -3 & -1 & -1 & -2 \\ -3 & 3 & -4 & 0 & 3 & -2 & 1 & 2 \\ 0 & 0 & 1 & 0 & -1 & -1 & -2 & 1 \\ -3 & 1 & -1 & -1 & 1 & -3 & 3 & -5 \\ 0 & 1 & -1 & 0 & -3 & 3 & -2 & -2 \\ -3 & 1 & 1 & -4 & 2 & -3 & 0 & 2 \end{pmatrix}$$

$$M_e^{w-dct} = \begin{pmatrix} -2 & 3 & -4 & 0 & 1 & 2 & 0 & -5 \\ 2 & -2 & 0 & 5 & 7 & 1 & 3 & -3 \\ 1 & -1 & -3 & 4 & 2 & 0 & -2 & -4 \\ 3 & 7 & -4 & 1 & 7 & -5 & -5 & -2 \\ 0 & 3 & 3 & -1 & 0 & -4 & -3 & 5 \\ -6 & 1 & 0 & -7 & 5 & 0 & 5 & -2 \\ 1 & 0 & -4 & 2 & -1 & 9 & 2 & -2 \\ -3 & 0 & -2 & -5 & -3 & -1 & 1 & -1 \end{pmatrix}$$

$$M_e^{w-dwt} = \begin{pmatrix} -3 & 3 & -2 & 0 & -1 & 1 & -1 & -1 \\ 2 & -2 & 0 & 0 & 0 & -3 & 1 & -1 \\ 0 & 0 & -1 & 1 & -1 & 0 & 0 & -1 \\ -3 & 3 & -2 & 0 & 1 & -3 & 0 & 2 \\ 0 & -1 & 0 & -1 & -1 & 0 & -2 & 1 \\ -2 & 1 & 0 & -2 & 2 & -2 & 2 & -2 \\ -1 & 0 & -1 & 0 & -2 & 3 & -1 & -2 \\ -2 & 1 & 0 & -3 & 1 & -1 & -1 & 1 \end{pmatrix}$$

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

$$MAE_e^{jpeg} = 3.44;\ MSE_e^{jpeg} = 17.66;\ PSNR_e^{jpeg} = 35.57dB$$
$$MAE_e^{jpeg2000} = 3.44;\ MSE_e^{jpeg2000} = 17.66;\ PSNR_e^{jpeg2000} = 35.57dB$$
$$MAE_e^{w-dct} = 2.69;\ MSE_e^{w-dct} = 11.75;\ PSNR_e^{w-dct} = 37.43dB$$
$$MAE_e^{w-dwt} = 1.22;\ MSE_e^{w-dwt} = 2.44;\ PSNR_e^{w-dwt} = 44.26dB$$

Để phát hiện dữ liệu watermark, luận án sử dụng phương pháp dựa trên phép thử kiểm định (Hypothesis testing) được đề xuất trong [**95**]. Phương pháp Hypothesis testing như sau: *Các đặc trưng của mẫu được dùng để đánh giá xem 1 giả thuyết nào đó của 1 tổng thể là đúng hoặc sai. Việc tìm ra kết luận để chấp nhận hoặc bác bỏ giả thuyết đó được gọi là kiểm định giả thuyết. Giả sử tổng thể có tham số θ chưa biết. Với giá trị cụ thể θ_0 cho trước nào đó, ta nghi ngờ θ hiện nay không đúng, nên đưa ra giả thuyết*

+ Giả thuyết là H_0: $\theta = \theta_0$

+ Đối thuyết là H_1: $\theta \neq \theta_0$

- Nhiệm vụ của phương pháp kiểm định giả thuyết thống kê là: bằng thực nghiệm/mô phỏng (thông qua mẫu cụ thể) để kiểm tra tính đúng/sai của giả thuyết H_0.

- Từ mẫu cụ thể đó tính giá trị quan sát Z

- Kết luận: chấp nhận hay bác bỏ giả thuyết H_0.

Áp dụng vào phương pháp thử kiểm định trên đây sử dụng cho bài toán có phân bố Gausian của chuỗi bit dữ liệu mẫu và watermark (theo giải thiết ban đầu). Các đặc trưng thông kê cho các hệ số tương quan của H_1 (có sự hiện diện của watermark) và H_0 (không có watermark) được tính toán thông qua kỳ vọng và phương sai của chuỗi dữ liệu. Để đảm bảo mức bảo mật, watermark được phân bố trên toàn bộ miền giá trị của mẫu dữ liệu với hệ số tương quan tạo ra vế trái của công thức trên. Do giả thiết mẫu dữ liệu có phân bố gausian, nên hàm lỗi được xác định qua xác suất cảnh báo sai và phương sai của mẫu L. Xác suất cố định cảnh báo sai được sử dụng để tính ngưỡng cảnh báo theo tiêu chuẩn Neyman–Pearson,

từ đó nút nhận có thể phát hiện được có sự hiện diện của watermark hay không. Trong luận án này, H_0 và H_1 được tính toán như sau

H_0 : R = N, không xuất hiện watermark

H_1 : R = W + N, xuất hiện watermark

Với R tập các hệ số tương quan r_i; W là tập đầu ra của watermark b_i, N là tập chuỗi tín hiệu vào.

Bằng các đặc tính thống kê của hệ số tương quan dựa trên cách tiếp cận trên, phương trình (3.10) sau cho phép kiểm tra sự có mặt dữ liệu watermark ở phía thu. Ta có công thức tính lỗi như sau:

$$\sum_{i=1}^{L} b_i r_i \leq\geq erfc^{-1}(p_f)\sigma\sqrt{L} \tag{3.10}$$

Trong đó, r_i là hệ số tương quan, b_i là watermark bit, *erfc* là hàm lỗi bổ sung, p_f xác suất cố định cảnh báo sai và L là chiều dài của mẫu dữ liệu, $\sigma\sqrt{L}$ là phương sai của mẫu L.

Như đã giới thiệu ở phần trước, đánh dấu bảo mật watermark được nhúng vào mảng dữ liệu theo nguyên tắc trải phổ trực tiếp. Để thuận tiện, luận án sử dụng cùng chuỗi giả ngẫu nhiên cho mọi ma trận dữ liệu con. Tức là, sử dụng cùng mỗi chuỗi mã Walsh được tạo bởi ma trận Hadamard.

Trong mô hình đề xuất, nghiên cứu thực hiện trên các khối ảnh khác nhau với các kích thước 2x2, 4x4 và 8x8. Tại bước lượng tử trong DCT, các hệ số sau khi biến đổi được mã hóa sau khi áp dụng thuật toán K-largest coding. Ở đây, K phần tử lớn nhất trong ma trận sẽ được giữ lại và các phần tử còn lại được chuẩn hóa về 0 [**97**].

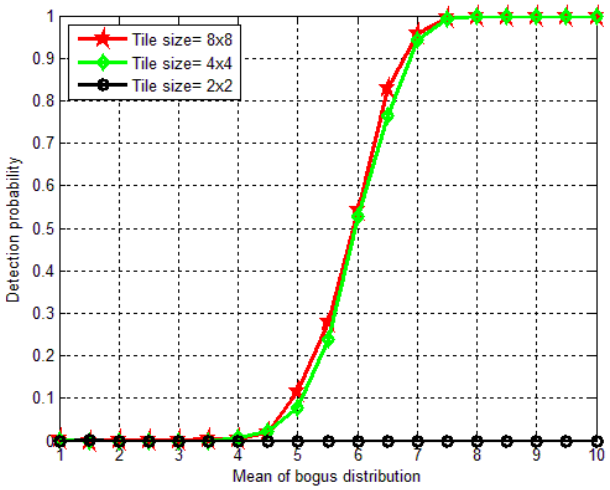
Tỷ số nén (Compress Ratio) được tính theo công thức (3.11) dưới đây.

$$CR = 1 - \frac{K}{N} \tag{3.11}$$

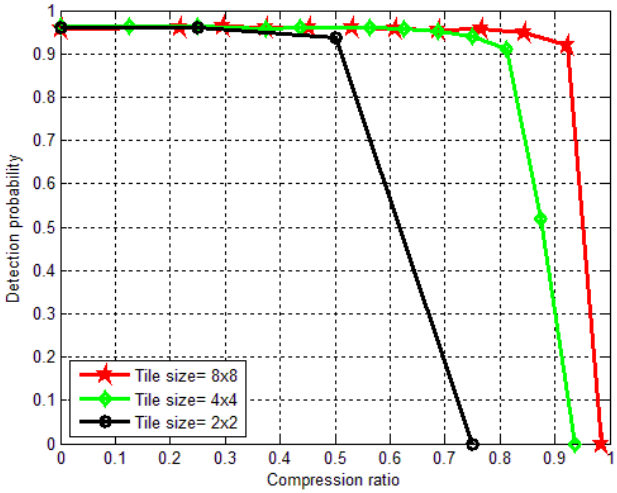
Với K là số cảm biến có độ lớn lớn nhất được giữ lại, N là số lượng cảm biến trong mỗi khối.

Để khảo sát ảnh hưởng của xác suất tìm thấy watermark p_f với các kích thước khối khác nhau thông qua biến đổi DCT, một số kết quả số được thể hiện dưới đây.

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 các 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.



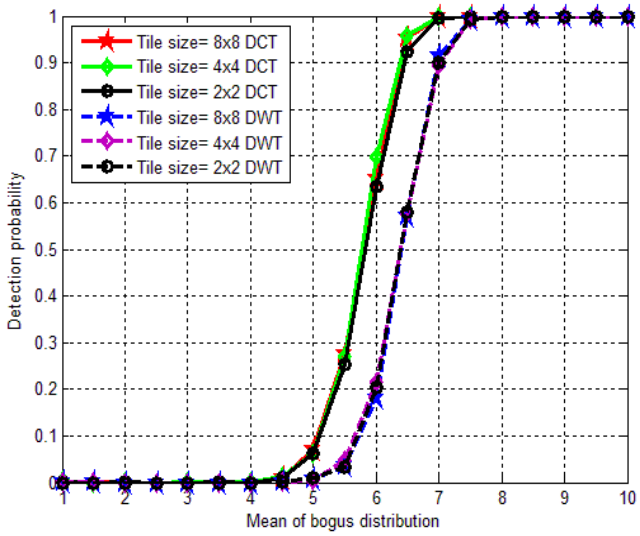
Hình 3. 4**.** Xác suất tìm thấy watermark với các độ lớn trung bình khác nhau.



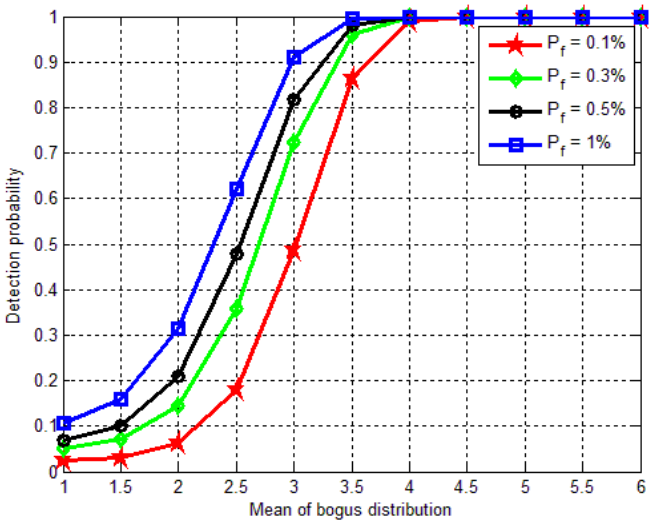
Hình 3. 5**.** Xác suất tìm thấy watermark với tỷ số nén thay đổi.

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.

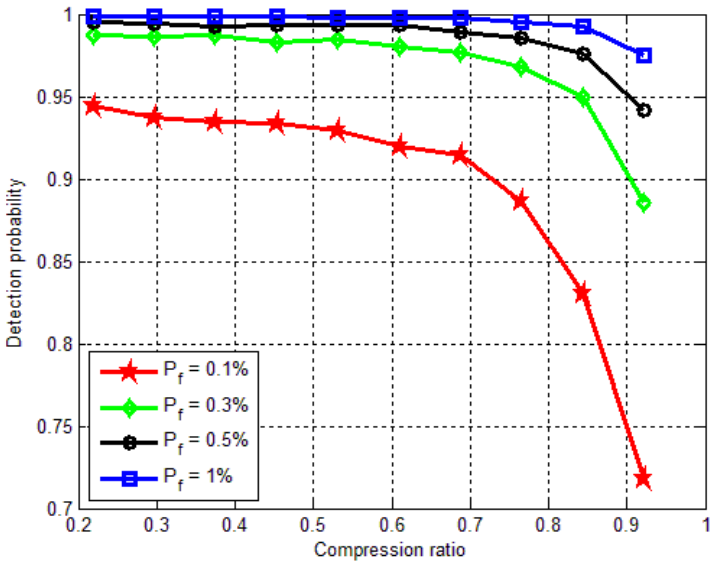


Hình 3. 6. Xác suất tìm thấy watermark với trường hợp DCT và DWT.



Hình 3. 7. Xác suất tìm thấy 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.

3.1.5. Nhận xét và đánh giá

Với kết quả nghiên cứu này ta có các nhận xét sau:

- Thứ nhất, đã cung cấp mô hình phân tích và kết quả số mô tả hiệu năng lỗi đối với mô hình phân tích đó trong quá trình xử lý ảnh theo chuẩn JPEG/JPEG2000 được quá trình đánh dấu bảo mật watermark vào dữ liệu cảm biến tương ứng. Nghiên cứu này tập trung vào các phương thức biến đổi khác nhau và so sánh mức độ hiệu quả giữa chúng.

- Thứ hai, từ xác suất tìm thấy watermark tại phía nhận thông qua mô phỏng số, ta thấy rằng, xác suất này phụ thuộc vào các tham số thay đổi như độ lớn watermark trung bình, xác suất cảnh báo sai, hệ số nén và kích thước ảnh cho đến cách chia khối cho từng ảnh.

- Từ đó, dựa trên kết quả có được, có thể đánh giá rằng bảo mật ảnh số có đánh dấu bằng watermark theo phương pháp DWT là lựa chọn tốt nhất cho cả vấn đề hiệu năng lỗi cũng như xác suất tìm thấy đánh dấu watermark.

- *Kết quả phân tích đánh giá so sánh nói trên cho mạng cảm biến không dây WISN hoàn toàn áp dụng vào các mạng thông tin vô tuyến khác. Trong thực tế, dù gửi/nhận ảnh số hay "vật mang tin" là đa phương tiện số (digital multimedia) nào khác thì mạng WISN hay mạng viễn thông khác chỉ là môi trường thông tin vô tuyến phục vụ truyền tải thông tin; Còn việc đánh dấu watermark hay giấu tin mật vào trong ảnh số đều được thực hiện trên hệ thống kỹ thuật số nào đó (máy tính, điện thoại hay thiết bị chuyên dụng,...) trước khi truyền đi. Nội dung nghiên cứu này nhằm phân tích hiệu năng lỗi trên ảnh số khi nhúng watermark, đồng thời lựa chọn được đánh dấu watermark theo phương pháp DWT khi ứng dụng là tối ưu.*

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

Hiện nay IEEE 802.11 là một trong những tiêu chuẩn về mạng vô tuyến được triển khai rộng rãi nhất trên thế giới, nó cung cấp rất nhiều ứng dụng cho cả mục đích thương mại lẫn an ninh-quốc phòng. Khi một mạng IEEE 802.11 bị tấn công thông thường hoặc tấn công thông minh nhằm hạ hiệu suất hoạt động của mạng sẽ dẫn đến việc các tham số *lưu lượng truy cập, tỷ lệ rớt gói tin và độ trễ* của IEEE 802.11 sẽ bị ảnh hưởng, kéo theo đó là vấn đề bảo mật cho đường truyền mạng cũng bị ảnh hưởng nghiêm trọng. Trong những năm gần đây, có nhiều nghiên cứu sử dụng phương pháp mô hình hóa để phân tích lỗi lớp MAC của IEEE 802.11 nhưng chỉ tập trung đánh giá khả năng xử lý của thuật toán Binary Exponential Back-off (theo hàm mũ nhị phân), tuy nhiên vấn đề đóng băng backoff (freezing back-off) trong thực tiễn cũng chưa được đề cập trong các mô hình nghiên cứu đó [**98**], [**99**], [**100**].

3.2.1. Một số nghiên cứu liên quan

Hiệu suất mạng của lớp MAC trong IEEE 802.11 luôn là mục tiêu được quan tâm của các nghiên cứu gần đây nhằm đánh giá và nâng cấp tiêu chuẩn IEEE. Để tiếp cận điều này, việc sử dụng mô hình phân tích là một phương pháp truyền thống do tính rõ ràng của nó. Tuy nhiên, độ chính xác và độ phức tạp của một mô hình phân tích phụ thuộc chủ yếu vào các mô hình giả định ban đầu có chính xác hay không. Mô hình tiêu biểu do Bianchi đề xuất [**61**] được bổ sung nhiều điều kiện hơn để bù cho tính đơn giản và độ chính xác như là vấn đề đóng băng back-off [**98**], [**99**], [**100**]. Tuy nhiên các nghiên cứu đó chỉ tập trung vào thuật toán Binary Exponential Back-off (BEB).

Từ đó thuật toán Exponential Increase Exponential Decrease back-off (EIED) đã được đề xuất với một số đặc điểm khác biệt. Kết quả mô phỏng số trong [**101**], [**60**] cho thấy rằng việc nâng cao lưu lượng truyền tải của mạng bão hòa IEEE 802.11 với thuật toán EIED back-off đã vượt qua thuật toán BEB back-off trong cùng một điều kiện. Nhưng đối với hiện tượng đóng băng back-off trong thuật toán EIED này chưa được nghiên cứu nào đề cập đến.

Ngoài ra lỗi xung đột lớp MAC trong IEEE 802.11 xuất hiện do các cuộc tấn công thông thường hoặc tấn công thông minh [**102**], từ đó dẫn đến việc thay đổi thuật toán back-off đã được trình bày trong nghiên cứu [**103**]. Theo tìm hiểu của nghiên cứu sinh, đã có nhiều đề xuất dựa vào chuỗi Markov [**99**] để xác thực thông số hiệu suất mạng đối với trường hợp có các nút lỗi [**62**], [**58**], [**25**]. Tuy nhiên, những mô hình này lại bỏ qua vấn đề đóng băng back-off mà chỉ kiểm tra dựa trên thuật toán BEB. Từ đó, luận án đề xuất mô hình phân tích mới nhằm bổ sung các thiếu sót trong các nghiên cứu trước đây [**61**], [**98**], [**99**], [**100**] đối với đánh giá hiệu suất mạng IEEE bị ảnh hưởng bởi các cuộc tấn công thông thường và thông minh về 3 tham số: lưu lượng truyền tải, xác suất rớt gói tin và độ trễ truy cập.

Từ phân tích trên, luận án xây dựng mô hình và tham số phục vụ đánh giá hiệu suất xử lý xung đột của các thuật toán back-off khác nhau lên mạng vô tuyến chống lại tấn công thông thường gồm:

- Mô hình trạng thái thuật toán back-off
- Mô hình trạng thái kênh
- Các tham số hiệu suất (*lưu lượng truy cập, tỷ lệ rớt gói tin và độ trễ*)

3.2.2. Các mô hình trạng thái dùng để đánh giá hiệu suất

a. Mô hình trạng thái thuật toán Back-off

Hãy xem xét một mạng vô tuyến IEEE 802.11 trạm đơn trong điều kiện lưu thông bão hòa. Mạng có chứa hai loại nút là nút bình thường (*normal node*) và nút lỗi (*misbehaviour node*) tuân theo thuật toán back-off. Gọi số lượng các nút trong mạng là *n* và số nút lỗi là *l*. Lớp MAC IEEE sử dụng thuật toán BEB hoặc EIED back-off đối với tất cả các nút bình thường.

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.

Trong đó τ_1 (*BEB*) là xác suất truyền của nút bình thường khi sử dụng thuật toán BEB, và τ_1 (*EIED*) đối với thuật toán EIED. Giả sử tất cả các kênh trong mạng làm việc bình thường và không có thiết bị đầu cuối bị lỗi.

Mô hình trạng thái back-off của một nút bình thường sử dụng thuật toán BEB được xác lập bằng chuỗi Markov 2 chiều trong [**98**], [**99**]. Gọi quá trình ngẫu nhiên biểu diễn cho giai đoạn back-off là *s*(*t*) và giá trị bộ đếm thời gian back-off là *b(t)*.

Giá trị $W = CW+1$ là giá trị của cửa sổ tranh chấp (*contention window*), m là giai đoạn back-off tối đa và R là giới hạn thử tối đa. Xác suất τ_1 (*BEB*) truyền của một nút bình thường được tính theo công thức sau:

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

Đối với thuật toán EIED được công bố trong [76], giá trị cửa sổ tranh chấp tăng và giảm theo hằng số r_I (tăng) và r_D (giảm). Trong nghiên cứu này, không mất tính tổng quát đối với các trường hợp phổ biến, luận án lựa chọn $r_I = r_D = 2$ như trong [**99**].

Đặt trạng thái (i^+, k) để biểu diễn nút truyền thành công và trạng thái (i^-, k) biểu rằng nút lỗi trong quá trình back-off khi đường truyền bị lỗi. Do các khe thời gian bất thường, ta có thể coi $W^+_i = W_i - 1$ là khe back-off nhàn rỗi đầu tiên sau khi truyền thành công.

Gọi $b_{j,k} = \lim_{t\to\infty} \Pr\{s(t) = j, b(t) = k\}$ là xác suất cố định của trạng thái back-off *(j, k)*. Xác xuất được này tính trong khoảng thời gian 1 nút bình thường truyền đi trong một khe thời gian nói chung bằng tổng của tất cả các trạng thái cố định với tham số k=0. Từ đó τ_1 (*EIED*) là xác suất truyền của nút bình thường khi sử dụng thuật toán EIED được tính theo công thức dưới đây.

$$\tau_1(EIED) = \sum_{i=0}^{m-1} b_{i^+,0} + \sum_{i=1}^{m} b_{i^-,0=\frac{1-x^{m+1}}{1-x} b_{0^+,0}}. \quad (3.13)$$

Với xác suất truyền đã cho của nút bình thường τ_1 và nút lỗi τ_2, ta có thể biểu diễn xác suất va chạm có điều kiện của một nút bình thường thông qua xác suất mà nút được gắn thẻ nhận được đường truyền có nguồn gốc từ ít nhất một trong các nút đang tranh chấp (contending nodes) như sau:

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

Trong các trường hợp phổ biến, một nút lỗi luôn được khởi tạo bởi 1 cửa sổ back-off nhỏ hơn so với cửa sổ khởi tạo của nút bình thường. Khi nút lỗi xuất hiện trong cửa sổ tranh chấp đã được cố định, kích thước cửa sổ tranh chấp không thay đổi trong suốt giai đoạn back-off. Đặt CW^* bằng kích thước cửa sổ tranh chấp của nút lỗi cộng thêm 1. Bộ đếm back-off của nút lỗi được lựa chọn ngẫu nhiên từ 0 đến CW^*-1. Xác suất truyền và xác suất và chạm của nút bình thường trong (3.12 và 3.14) biến thành xác suất truyền và xác xuất va chạm của nút lỗi τ_2 và p_2 như sau

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

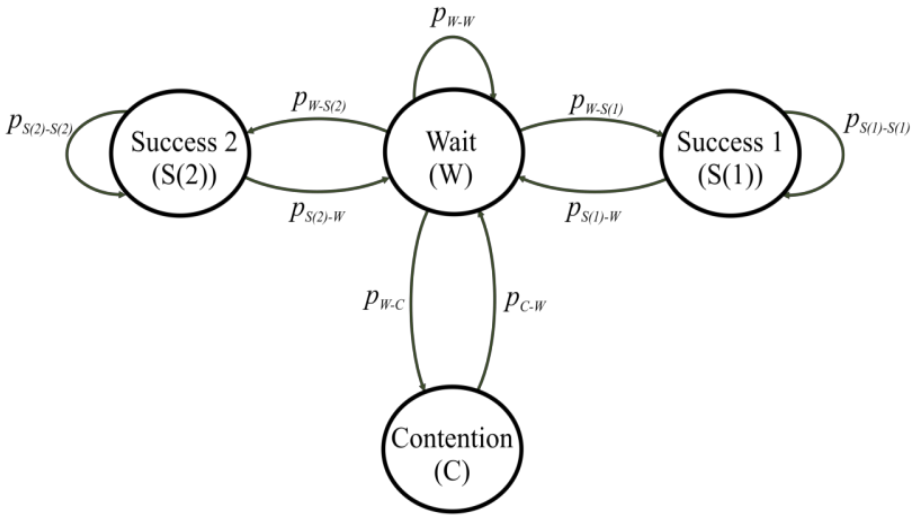
Xác suất va chạm của nút lỗi là

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

b. Mô hình trạng thái kênh

Luận án đề xuất mô hình trạng thái kênh lớp MAC của IEEE 802.11 theo cấu trúc đa kênh và được xây dựng trong hình 3.9. Mục đích của mô hình phân chia các trạng thái xung quanh nút bình thường và phân tích quá trình đóng băng back-off đối với núi lỗi xây dựng dựa chuỗi Markov.

Mô hình trong hình 3.9 có bốn trạng thái là: Chờ, Thành công 1, Thành công 2 và Tranh chấp. Trong đó trạng thái Chờ là trạng thái kênh ở trạng thái không hoạt động; trạng thái Thành công 1 là trạng thái kênh thể hiện sự truyền thành công của một nút bình thường; trạng thái Thành công 2 là trạng thái kênh thể hiện sự truyền thành công của một nút lỗi; và trạng thái Tranh chấp là trạng thái kênh thể hiện kênh trong quá trình va chạm.



Hình 3. 9. Mô hình trạng thái kênh.

Khả năng chuyển đổi các trạng thái được giải thích như dưới đây.

Chờ sang Chờ: đó là khả năng chuyển đổi từ trạng thái Chờ tới chính nó, ta có

$$p_{w-w} = (1-\tau_1)^{n-l}(1-\tau_2)^{l} \tag{3.17}$$

Chờ đến Thành công 1: Sau khi truyền thành công một nút bình thường kênh chuyển sang trạng thái bận.

$$p_{W-S(1)} = (n-l) \times [\tau_1(1-\tau_1)^{n-l-1}(1-\tau_2)^{l}] \tag{3.18}$$

Chờ đến Thành công 2: Sau khi một nút lỗi truy cập vào kênh và khởi tạo một truyền thành công. Ta có

$$p_{W-S(2)} = l \times [\tau_2(1-\tau_1)^{n-l}(1-\tau_2)^{l-1}] \quad (3.19)$$

Chờ đến Tranh chấp: Kênh đang trong tình trạng có va chạm do truyền đồng thời nhiều nút. Do vậy khả năng chuyển đổi trạng thái *Chờ* sang trạng thái *Tranh chấp* là:

$$p_{W-C} = 1 - p_{W-W} - p_{W-S(1)} - p_{W-S(2)} \quad (3.20)$$

Thành công 1 sang Thành công 1, Thành công 2 sang Thành công 2: Đó là sự kiện khi một nút truyền nhiều gói tin liên tiếp. Khả năng truyền mà một nút bình thường và một nút lỗi trích xuất bộ đếm thời gian back-off mới được tính theo công thức sau

$$p_{S(1)-S(1)} = \frac{1}{W_0}; \quad (3.21)$$

$$\text{và} \quad p_{S(2)-S(2)} = \frac{1}{CW^*}.$$

Xác suất trạng thái ổn định của chuỗi Markov được tính như sau:

$$\pi_W = \frac{1}{1 + p_{W-C} + p_{W-S(1)}/\left(1 - p_{S(1)-S(1)}\right) + p_{W-S(2)}/\left(1 - p_{S(2)-S(2)}\right)}$$

$$\pi_C = \pi_W \times p_{W-C};\ \pi_{S(1)} = \pi_W \times \frac{p_{W-S(1)}}{1-p_{S(1)-S(1)}};\ \pi_{S(2)} = \pi_W \times \frac{p_{W-S(2)}}{1-p_{S(2)-S(2)}} \quad (3.22)$$

Độ dài của khe thời gian trung bình được tính theo độ ổn định của mô hình trạng thái kênh là:

$$E[T] = \pi_W T_W + \pi_C T_C + \left(\pi_{S(1)} + \pi_{S(2)}\right) T_S. \quad (3.23)$$

Ở đây, T_S là thời gian trung bình kênh bận sau truyền thành công, T_C là thời gian trung bình kênh bận do mỗi trạm trong thời gian va chạm, và T_W là khoảng của một khe thời gian trống.

3.2.3. Các tham số hiệu suất

Trong phần này, ba tham số hiệu suất được tính toán là *phân tích lưu lượng truyền tải, xác suất rớt gói tin và phân tích trễ truy nhập* được tính toán như dưới đây.

Phân tích lưu lượng truyền tải: Lưu lượng truyền tải cực đại của một nút được định nghĩa là một phần của kênh bị chiếm dụng và truyền tải thành công các bít cần

truyền. Lưu lượng truyền tải thông thường của nút bình thường và nút lỗi có thể được biểu diễn theo các công thức sau:

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

Xác suất rớt gói tin: Xác suất rớt gói được định nghĩa là xác suất mà gói tin đó bị rớt khi đạt đến giới hạn thử tối đa (R) và được tính như sau:

$$P_{drop1} = p_1^{R+1}\ , P_{drop2} = p_2^{R+1}. \quad (3.25)$$

Phân tích độ trễ truy cập: Độ trễ của gói trung bình so với một gói đã truyền thành công được định nghĩa là khoảng thời gian từ thời điểm gói tin xếp ở đầu hàng lớp MAC đã sẵn sàng để được truyền đi cho đến khi có xác nhận đối với gói tin này là đã nhận được. Độ trễ gói của nút bình thường theo thuật toán BEB sử dụng trong nghiên cứu [**104**] và theo thuật toán EIED được tính bằng 2 công thức dưới đây.

$$T_{delay1}(BEB) = \sum_{j=0}^{R}\left(\frac{W_j+1}{2} \times \frac{p_1^j - p_1^{R+1}}{1-p_1^{R+1}}\right) \times E[T]; T_{delay1}(EIED) = \frac{\sum_{i=0}^{m} T_i \times d_i}{\sum_{i=0}^{m} d_i} \quad (3.26)$$

Trong đó, T_i là độ trễ trung bình khi một nút bình thường bắt đầu ở giai đoạn thứ *i* trong quá trình back-off, với hàm mật độ xác suất bằng d_i.

Ta có $d_0 = b_{0^+,0}, d_1 = b_{1^+,0}, \dots, d_{m-1} = b_{(m-1)^+,0}$ và $d_m = b_{m^-,0}$.

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

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

3.2.4. Kết quả mô phỏng và đánh giá

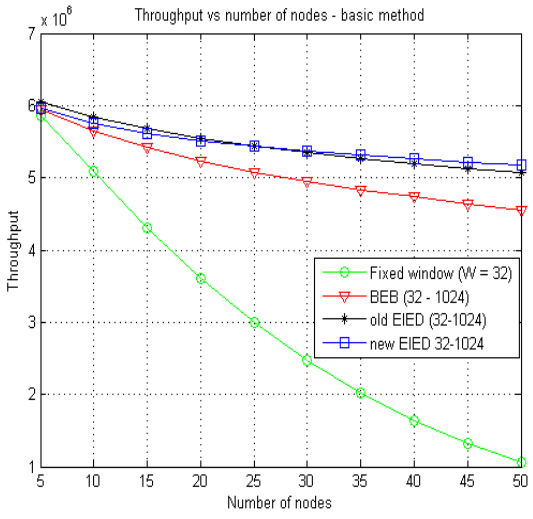
Để xác nhận hiệu suất mạng của hai thuật toán back-off BED và EIED cho cả nút bình thường lẫn nút lỗi trong mạng vô tuyến, ta sử dụng công cụ MATLAB để đánh giá các tham số *phân tích lưu lượng truyền tải, xác suất rớt gói tin và phân tích độ trễ truy cập*. Kết quả đánh giá được kiểm tra theo các thông số chuẩn của IEEE 802.11b [**57**].

Gọi L_{DATA} là độ dài trung bình của gói DATA, ta có $L_{DATA} = H + E[P]$, trong đó H là độ dài của tiêu đề (*header*), bao gồm tiêu đề vật lý và tiêu đề MAC. Thời lượng truyền của các gói DATA, ACK, RTS và CTS là: $T_{DATA} = L_{DATA} / R_{data}$; $T_{ACK} = L_{ACK} / R_{BASIC}$; $T_{RTS} = L_{RTS} R_{BASIC}$; $T_{CTS} = L_{CTS} / R_{BASIC}$. Khoảng thời gian của mỗi trạng thái ổn định là T_W ,T_S ,T_c được tham chiếu với mô hình đề xuất. Với mô hình cơ bản và mô hình RTS/CTS, ta có

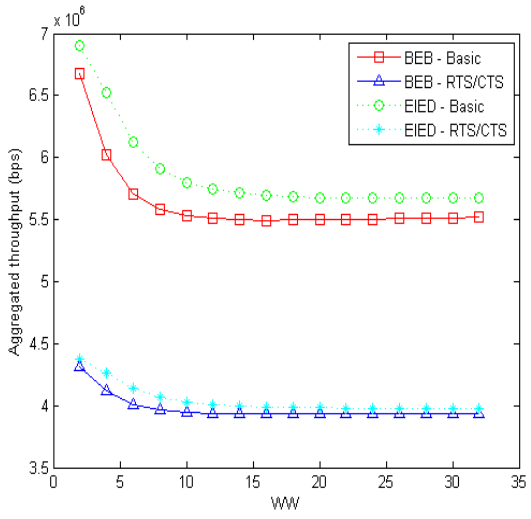
$$T_W = \sigma; T_C = T_{DATA} + SIFS + T_{ACK} + DIFS;\ T_S = T_{DATA} + SIFS + T_{ACK} + DIFS \quad (3.28)$$

$$T_W = \sigma; T_C = T_{RTS} + SIFS + T_{ACK} + SIFS; \\ T_S = T_{RTS} + SIFS + T_{CTS} + SIFS + T_{DATA} + SIFS + T_{ACK} + DIFS \quad (3.29)$$

Trước tiên, ta xem xét lưu lượng truyền tải mạng của tất cả các nút bình thường đối với ba thuật toán back-off khác nhau là Cửa sổ cố định (Fixed Windows), BEB và EIED theo sự thay đổi số lượng nút (Hình 3.10.a) và sự thay đổi giá trị cửa sổ tranh chấp theo 2 thuật toán BED và EIED với mô hình cơ bản và mô hình RTS/CTS (Hình 3.10.b).



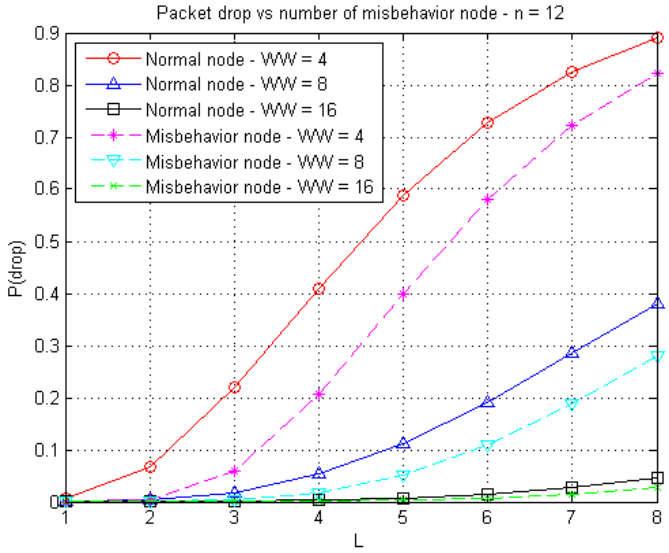
(a) Phân tích lưu lượng truyền tải mạng so với số nút mạng theo 3 thuật toán



(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

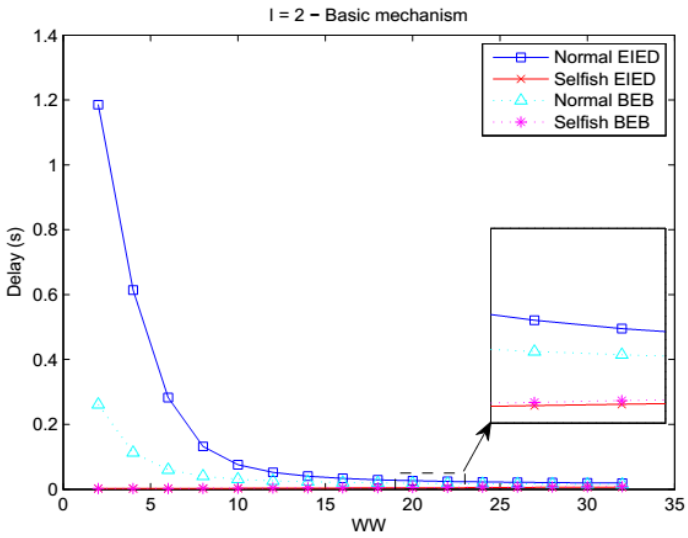
Hình 3. 10. Phân tích lưu lượng truyền tải mạng theo các thuật toán

Nhìn vào hình 3.10a, thuật toán back-off Cửa sổ cố định (Fixed Windows) có hiệu suất lưu lượng truyền tải là kém nhất khi tăng nhanh số lượng các nút. Trong khi đó thuật toán EIED có lưu lượng truyền tải tốt nhất và tốt hơn thuật toán BEB như đã được chứng minh trong [**101**], [**60**]. Còn trong hình 3.10b cho kết quả phân tích lưu lượng truyền tải mạng theo 2 thuật toán BED và EIED với mô hình cơ bản và mô hình RTS/CTS tương ứng với một nút lỗi trong mạng. Ta nhận thấy thuật toán EIED luôn cho kết quả tốt hơn so với thuật toán BEB với cả hai mô hình cơ bản và mô hình RTS/CTS. Tuy nhiên, trường hợp mạng theo mô hình RTS/CTS, lưu lượng truyền tải bị giảm là do nó đưa ra các thông báo điều khiển.



Hình 3. 11. Tỷ lệ rớt gói nút bình thường so với nút lỗi.

Hình 3.11 cho thấy tỷ lệ rớt gói tin đối với nút bình thường và nút lỗi khi số lượng nút lỗi thay đổi và kết hợp với các giá trị khác nhau của CW^*. Như đã thấy trong hình, tỷ lệ rớt gói tin của các nút bình thường luôn luôn cao hơn các nút lỗi với bất kỳ giá *trị* CW^* nào. Giá trị CW^* nhỏ nhất đưa ra tỷ lệ rớt gói lớn nhất. Tỷ lệ rớt gói tin sẽ tăng lên khi số nút lỗi tăng lên.



Hình 3. 12. Độ trễ của các nút bình thường và nút lỗi tương ứng với thuật toán BED và EIED.

Hình 3.12 cho thấy độ trễ giữa 2 thuật toán back-off khác nhau, một nút lỗi luôn giữ giá trị trễ nhỏ nhất so với tất cả các giá trị trong cửa sổ tranh chấp. Độ trễ của nút bình thường là rất cao so với giá trị rất nhỏ của cửa sổ tranh chấp vì xác suất chiếm kênh của nó rất thấp và hiệu suất của thuật toán BEB tốt hơn so với thuật toán EIED.

3.2.5. Nhận xét và đánh giá

Với kết quả này, luận án có hai nhận xét như sau:

- Thứ nhất, đề xuất một mô hình phân tích mới đối với lớp MAC của IEEE 802.11 bằng việc sử dụng các thuật toán EIED đã bao gồm xử lý hiện tượng đóng băng back-off.

- Thứ hai, dựa trên kết quả số về phân tích hiệu suất mạng theo các thuật toán back-off khác nhau với 3 tham số *lưu lượng truyền tải, xác suất rớt gói tin và độ trễ truy cập* đối với nút bình thường và nút lỗi để cho ra kết quả là khác nhau theo các tấn công thông thường.

Thông qua nghiên cứu này, luận án đánh giá được thuật toán EIED back-off có hiệu suất tốt hơn so với thuật toán BEB trong điều kiện thông thường. Tuy nhiên,

khi mạng tồn tại nút độc do ảnh hưởng của các tấn công thông thường, thì hiệu suất của mạng sử dụng thuật toán BEB back-off tốt hơn thuật toán EIED.

3.3. Kết luận chương 3

Chương 3 luận án tập trung giải quyết hai vấn đề sau

- Một là luận án 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.

- Hai là, 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.

Trong chương 4, luận án ứng dụng kết quả nghiên cứu vào nhiệm vụ thiết kế, chế tạo hệ thống thông tin liên lạc bí mật thông qua truyền ảnh số có bảo mật phục vụ công tác nghiệp vụ.

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. Hệ thống này ứng dụng kỹ thuật giấu tin mật bằng thuật toán mã hóa và có trao đổi khóa bí mật (chương 2) vào ảnh số sau đó đánh dấu watermark lên ảnh số đó (chương 3). Từ đó hoàn thiện hệ thống thông tin liên lạc bí mật vô tuyến để trao đổi bản tin hình ảnh trên cho nhau bằng bằng kỹ thuật trải phổ nhảy tần FHSS nhằm mở rộng các hình thức liên lạc mật trong một số công tác nghiệp vụ đặc biệt [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 rất quan trọng, do vậy đòi hỏi về tính năng - tác dụng đối với thiết bị rất cao. Các thiết bị do nước ngoài sản xuất có tính năng hiện đại, ứng dụng công nghệ cao, độ tin cậy tốt, khả năng bảo mật cao, nhưng ngược lại là vấn đề phụ thuộc và bị động về công nghệ, cũng như không thể bảo đảm yếu tố bí mật tuyệt đối trong các công tác nghiệp vụ. Từ nhu cầu của các đơn vị kỹ thuật nghiệp vụ, nghiên cứu sinh cùng nhóm cán bộ khoa học kỹ thuật của đơn vị đã ứng dụng hệ thống nhúng chế tạo thành công thiết bị thông tin liên lạc không dây có bảo mật, bước đầu đáp ứng với yêu cầu đặt ra. Ngoài việc đưa kết quả nghiên cứu của luận án vào thiết bị cụ thể còn có ý nghĩa thực tiễn rất lớn đó là nghiên cứu và ứng dụng đã được đi đôi với nhau.

Như chúng ta đã biết với xu thế phát triển chung, việc ứng dụng công nghệ nhúng trong thiết kế chế tạo các thiết bị điện tử, viễn thông nói chung cũng như thiết bị thông tin liên lạc không dây nói riêng hiện đang được sử dụng rộng rãi. Trong nghiên cứu này, luận án đã nghiên cứu, áp dụng các công nghệ kỹ thuật mới, hiện đại như: hệ thống điều khiển nhúng, kỹ thuật trải phổ nhảy tần, công nghệ

SDR, kỹ thuật mã hoá và giải mã chuẩn AES đối với thông tin liên lạc,... để thiết kế và chế tạo một bộ thiết bị thông tin liên lạc không dây, cùng với việc ứng dụng kỹ thuật giấu tin mật bằng thuật toán mã hóa và có trao đổi khóa bí mật (*chương 2*) vào ảnh số và đánh dấu watermark lên ảnh số đó (*chương 3*). Tại phía nhận, ảnh sẽ được tách dấu watermark và sau đó tách bản tin mật ra. Sản phẩm bước đầu đã đáp ứng được một số yêu cầu cơ bản về chỉ tiêu kỹ thuật, tính năng hoạt động của một hệ thống liên lạc không dây cũng như những yêu cầu riêng về tính bảo mật, nhỏ gọn, cơ động… [**105**], [**87**].

Mặc dù bài báo đầu tiên thiết kế hệ thống thông tin liên lạc vô tuyến bí mật từ năm 2011, đến nay đã 2019, nhưng trong thực tế, để triển khai được hoàn chỉnh hệ thống phần cứng và phần mềm truyền tin thôi cũng đòi hỏi rất nhiều thời gian để hoàn thiện. Sau khi hoàn thiện hệ thống phần cứng và phần mềm truyền tin, NCS mới tiếp tục nghiên cứu hoàn chỉnh phần bảo mật, mã hóa, tối ưu và thử nghiệm hệ thống. Trong thực tế công tác nghiệp vụ, việc thiết lập mạng vô tuyến truyền độc lập có bảo mật luôn phải chủ động thực hiện, các mạng viễn thông công cộng khác (như wifi, Internet, vệ tinh…) chỉ mang ý nghĩa dự phòng và phục vụ nhiệm vụ khác. Mỗi phiên liên lạc chỉ gửi/nhận 1 bản tin, do các vấn đề thời gian truyền tin và cự li truyền tin gần/xa liên quan chủ yếu đến kỹ thuật về phần cứng, nên NCS không đặt vấn đề giải quyết này trong luận án.

4.2. Giải pháp và công nghệ

a. Các yêu cầu chung đối với thiết bị

Đầu vào là ảnh số, sau đó bản tin text được mã hóa 5 bit, sinh khóa ngẫu nhiên 6 bit, đánh dấu watermark. Đầu nhận sẽ thực hiện ngược lại để giải mã và nhận bản tin text. Có thể truyền thông tin kỹ thuật số thu/phát một và hai chiều theo phương thức truyền thông không dây sóng ngắn RF, tốc độ cao.

Bản tin truyền giữa các thiết bị liên lạc là dữ liệu số có mã hóa AES, đáp ứng theo thời gian thực.

Có thể thiết lập mạng liên lạc đa kênh, giao thức truyền thông RF có độ bảo mật cao, khả năng chống nhiễu tốt, khoảng cách liên lạc từ 30 - 100m (có che chắn) và tới 400m (tầm nhìn thẳng). Lập trình hoạt động tự động, hoặc thao tác bằng tay đơn giản, nhanh chóng, thiết bị phải gọn nhẹ tiện lợi cho người sử dụng khi làm việc và di chuyển. Thiết bị có độ tin cậy cao, chi phí thấp hơn so với nhập ngoại, tiêu thụ ít năng lượng và ứng dụng công nghệ hiện đại.

b. Giải pháp và lựa chọn công nghệ phần cứng và phần mềm

Các thiết bị thông tin liên lạc không dây có bảo mật cần thiết kế là Hệ thống thông tin thu phát số, có mã/giải mã, các chế độ hoạt động lập trình được một cách linh hoạt, phần mềm điều khiển thực hiện đa nhiệm và có giao diện quen thuộc với trình độ người sử dụng. Do đó, nó hoàn toàn phù hợp với các đặc trưng cơ bản của hệ thống nhúng và việc ứng dụng hệ thống nhúng (Embedded System) để chế tạo thiết bị hoàn toàn có khả năng đáp ứng các yêu cầu đặt ra.

- Bộ xử lý trung tâm (CPU) của thiết bị là một máy tính nhúng mini, sử dụng hệ điều hành Window Embedded, phần mềm nhúng xử lý tín hiệu và điều khiển được lập trình bằng ngôn ngữ VisualC trên khối SDR.

- Kênh truyền dẫn dữ liệu số không dây liên lạc giữa các điểm trong nút mạng sử dụng kỹ thuật trải phổ với hệ thống sóng mang nhảy tần FHSS. Với các ưu điểm về tốc độ và băng thông, tính bảo mật cao trong các khung truyền dữ liệu và khả năng chống nhiễu trong thông tin trải phổ nhảy tần sẽ đảm bảo sự hoạt động ổn định, chính xác trong hệ thống thông tin vô tuyến giữa các thiết bị liên lạc.

- Băng tần số hoạt động được lựa chọn cho hệ thống là dải tần số 902 MHz – 928 MHz, tốc độ dữ liệu RF từ 1.200 đến 57.600bps số kênh làm việc FHSS là 7 hop với 25 tần số. Với yêu cầu về khoảng cách liên lạc, nên có thể giới hạn mức điều khiển công suất thu/phát trong khoảng 1 – 100mW tùy theo đặc điểm liên lạc.

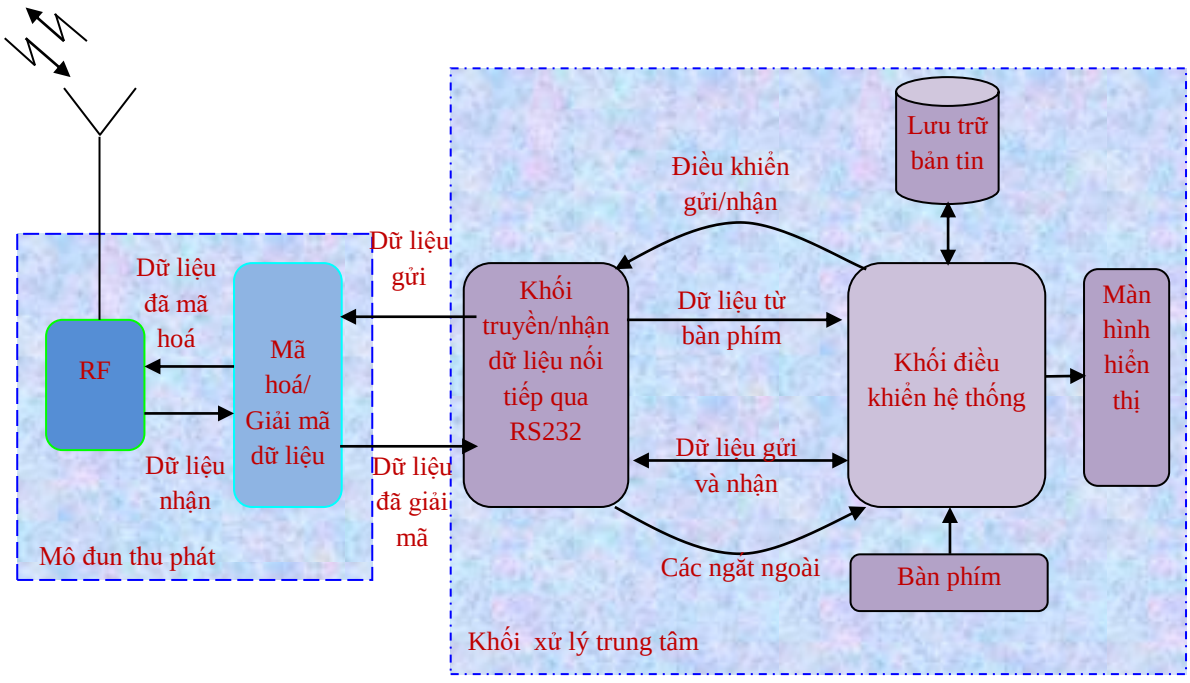
- Ứng dụng công nghệ SDR có ưu điểm là tốc độ lấy mẫu ADC/DAC cao (12 – 20Msa/s) để điều chế/giải điều chế tín hiệu với mục đích tăng khả năng làm việc thông qua thay đổi tần số bằng phần mềm.

- Xây dựng phần mềm điều khiển là chức năng rất quan trọng nhằm thực hiện nhiệm vụ mã hóa bản tin text theo thuật toán mã hóa khối 5 bit, sau đó tạo khóa giả ngẫu nhiên (trong phần ứng dụng vào thiết bị hiện tại, luận án chỉ mới sử dụng dãy giả ngẫu nhiên 6 bit) và sau đó đưa vào ảnh số đã được chọn từ đầu. Tiếp theo là quá trình chọn và đóng dấu watermark lên ảnh trước khi đưa đến khối truyền dữ liệu. Ngoài ra, phần mềm còn thực hiện mã hóa dữ liệu theo chuẩn AES 128 bit trước khi truyền tới mô đun RF điều này làm tăng khả năng bảo mật thông tin đáp ứng yêu cầu đặc thù hoạt động nghiệp vụ. Ngoài ra việc mã hóa/giải mã tín hiệu trên đường truyền theo tiêu chuẩn AES 128bit cũng được phần mềm thực hiện. Toàn bộ phần mềm được viết bằng ngôn ngữ lập trình Visual C.

Như vậy, các thành phần chính của thiết bị sẽ bao gồm hệ thống nhúng phần cứng kết hợp với mô-đun thu phát dữ liệu số không dây và phần mềm điều khiển, xử lý dữ liệu số cho các bản tin truyền thông, trong đó có đưa vào các kỹ thuật mã/giải mã đặc biệt (chương 2).

4.3. Triển khai hệ thống

a. Xây dựng sơ đồ khối hệ thống thu/phát



Hình 4. 1. Sơ đồ khối của hệ thống

Sơ đồ khối tổng quá của hệ thống như Hình 4.1. Có thể chia ra làm 2 khối chính: Khối xử lý trung tâm, khối thu phát không dây.

b. Nguyên lý hoạt động chung của hệ thống

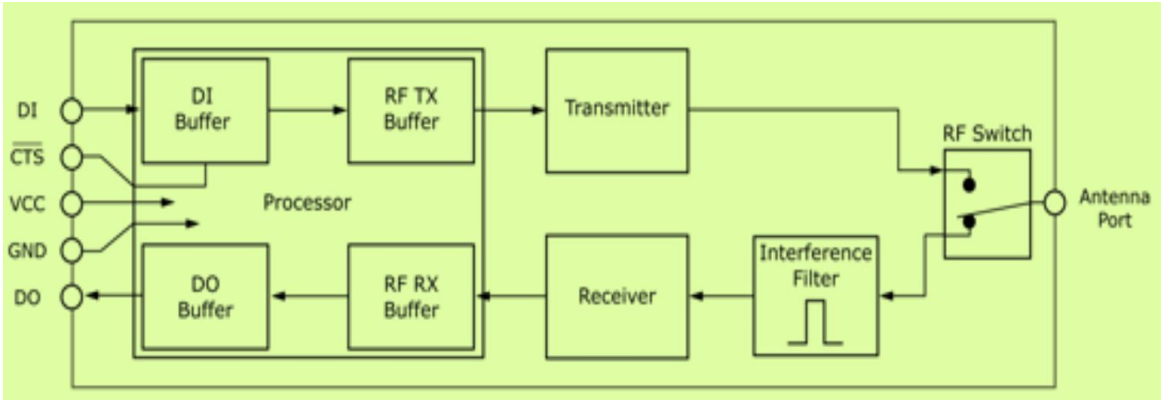
Tại trạm phát, dữ liệu hay bản tin truyền di được nhập vào thông qua bàn phím hoặc trên tệp dữ liệu có sẵn lưu trên hệ thống, sau đó được truyền tới khối giải mã/mã hóa dữ liệu thông qua đường truyền RS232. Tại khối này, dữ liệu được mã hóa theo chuẩn AES 128 bit để đảm bảo tính an toàn cho thông tin . Tiếp theo, dữ liệu được đưa tới khối thu/phát RF để truyền thông tin đi. Phía trạm thu, quá trình được thực hiện ngược lại. Sau khi dữ liệu đã nhận đủ, không bị lỗi, được giải mã thì kết quả sẽ được lữu trữ lên ổ cứng và hiển thị lên màn hình theo dõi. chỉ tiêu kỹ thuật chính của mô đun thu phát được thể hiện trong bảng 4.1 dưới đây.

Bảng 4. 1. Đặc điểm kỹ thuật mô đun RF

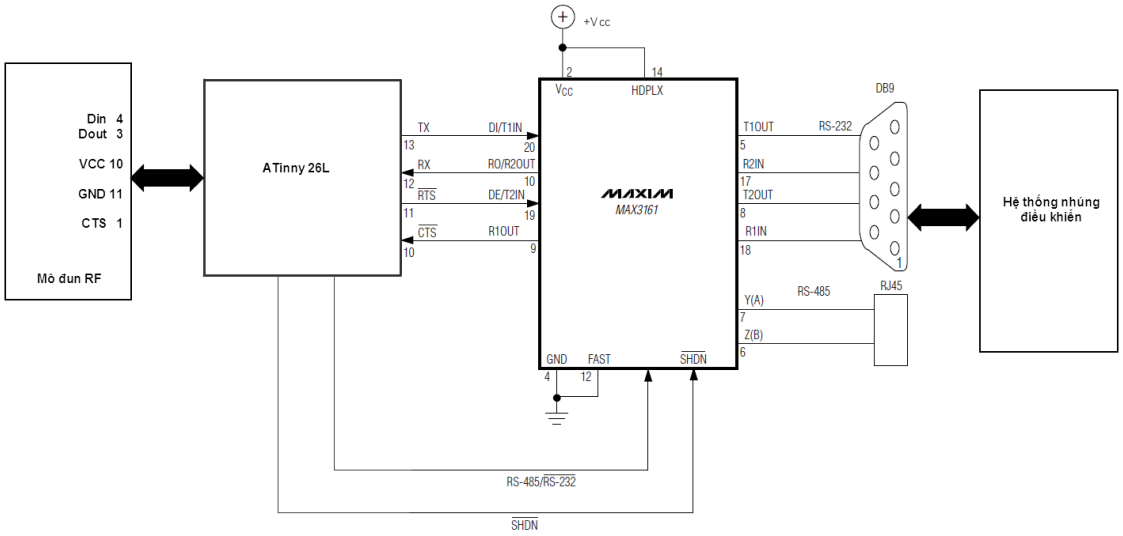
Đặc điểm	**Mô đun RF (900MHz)**
Công suất phát	100mW (20 dBm)
Phạm vi liên lạc có che khuất	<= 450m
Phạm vi liên lạc theo tầm nhìn thẳng	<= 7km
Tốc độ giao tiếp dữ liệu nối tiếp (*lập trình bằng phần mềm*)	1200 - 57600 bps
Tốc độ truyền dữ liệu	9600 - 19200 bps
Tốc độ dữ liệu RF	10000 - 20000 bps
Độ nhạy thu	-110 dBm (9600 bps) -107 dBm (19200 bps)
Dải tần số	910 - 917 MHz
Công nghệ trải phổ	FHSS
Mã hoá	AES 128 bit
Đánh địa chỉ	65535 trên 1 kênh

Khối xử lý trung tâm bao gồm 2 phần : mạch truyền/nhận dữ liệu nối tiếp qua RS232 và hệ thống nhúng mini làm chức năng điều khiển chế độ hoạt động toàn bộ hệ thống như: thiết lập chế độ, truyền nhận thông tin, mã hóa bảo mật, hiển thị, lưu trữ… Để thuận tiện cho quá trình thiết kế, rút gọn thời gian thực hiện, đáp ứng giải pháp công nghệ cũng như chỉ tiêu đặt ra, nhóm nghiên cứu đã chọn một máy tính mini làm hệ thống nhúng. Mạch giao tiếp truyền nhận dữ liệu sử dụng chip MAX3161 (dòng chíp được lập trình thu phát đa giao thức với các chân có thể lập trình tạo thành một giao tiếp gồm 2TX/2RX chuẩn RS-232 hoặc 1 cổng RS485/RS422 thông qua vi điều khiển ATiny26.

Sơ đồ chi tiết kết nối các khối như hình vẽ 4.2 dưới đây



(a) Mô đun RF



(b) Mạch khối truyền/nhận dữ liệu nối tiếp qua RS232

Hình 4. 2. Sơ đồ khối các mô đun

c. Khối điều khiển hệ thống

Khối điều khiển hoạt động của toàn bộ hệ thống được lập trình bằng ngôn ngữ Visual C chạy trên nền hệ điều hành Window nhúng giúp cho giao diện người dùng thuận tiện hơn. Các tác vụ như thiết lập cấu hình thiết bị, chế độ hoạt động, kiểm soát lỗi quá trình truyền dữ liệu, điều khiển các kết nối với thiết bị ngoại vi..., đều thực hiện đơn gian thông qua giao diện rất trực quan đơn giản. Điều này giúp tăng độ chính xác, tính bảo mật, tiết kiệm thời gian thao tác đảm bảo tính an toàn khi thực hiện các công tác nghiệp vụ khi dùng thiết bị này.

Phần mềm điều khiển cho hệ thống còn có một chức năng rất quan trọng đó là thực hiện nhiệm vụ mã hóa bản tin text theo thuật toán mã hóa khối 5 bit, sau đó tạo khóa giả ngẫu nhiên (trong phần ứng dụng vào thiết bị hiện tại, luận án chỉ mới sử dụng dãy giả ngẫu nhiên 6 bit) và sau đó đưa vào ảnh số đã được chọn từ đầu. Tiếp theo là quá trình chọn và đóng dấu watermark lên ảnh trước khi đưa đến khối truyền dữ liệu. Ngoài ra, phần mềm còn thực hiện mã hóa dữ liệu theo chuẩn AES 128 bit trước khi truyền tới mô đun RF điều này làm tăng khả năng bảo mật thông tin đáp ứng yêu cầu đặc thù hoạt động nghiệp vụ.

Kết quả nghiên cứu của chương 2 và 3 được thể hiện bằng phần mềm của hệ thống thông tin liên lạc bí mật. Hệ thống liên lạc bí mật có đầu vào là ảnh số làm vật mang tin (ảnh C). Việc đưa bản tin mật (bản tin M) vào hệ thống liên lạc được thực hiện trên thiết bị nhúng; Việc thực hiện giấu tin (theo thuật toán mục 2.1) cũng hoàn toàn thực hiện tự động bằng phần mềm, khóa K được tạo ngẫu nhiên cũng được tạo ra theo quy luật chuỗi giả ngẫu nhiên đồng dư tuyến tính; Sau khi giấu bản tin M trong ảnh C và khóa K, ảnh C trở thành ảnh S. Tiếp theo hệ thống sẽ thực hiện đánh tự tạo dấu thủy vân số (W) và đóng dấu vào ảnh S để trở thành ảnh S_w; cuối cùng ảnh S_w được đưa đến khối thu/phát truyền dữ liệu. Ảnh gửi đi và nhận được là ảnh đã được đánh dấu thủy vân số.

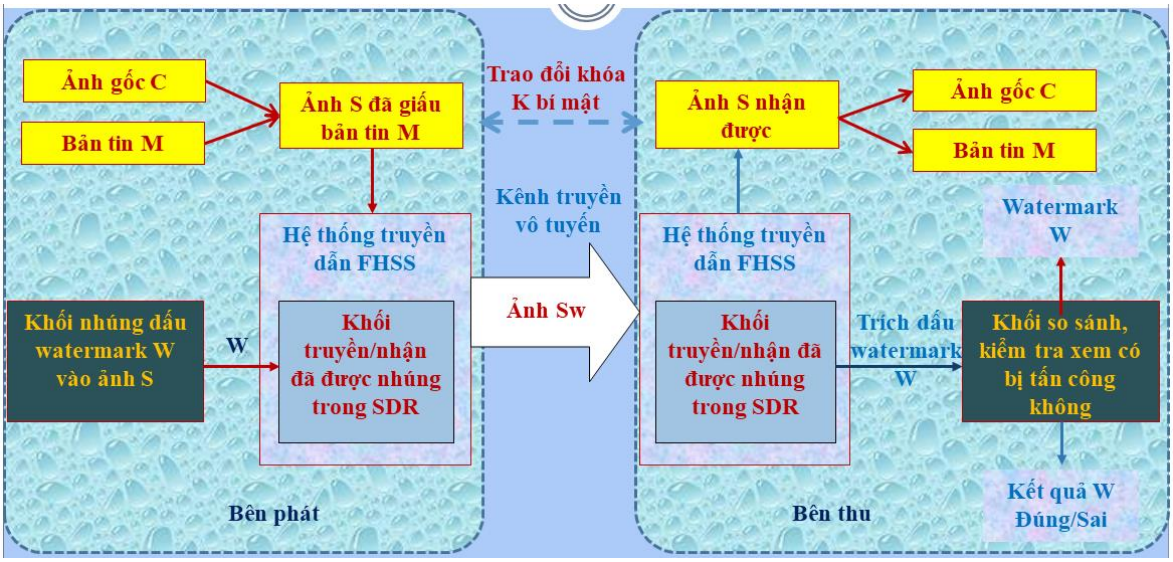
Việc thực hiện kiểm tra tách dấu thủy vân số và tách và giải mã bản tin giấu trong ảnh số nhận được theo quy trình ngược lại. Sau khi kiểm tra thủy vân số nhận được là giải mã bản tin để nhận được bản rõ. Do tại các đầu thu/phát của hệ thống

đều có chức năng giống nhau là gồm cả nhận và gửi bản tin mật (tương tự như 1 bộ tranceiver), nên NCS chỉ giới thiệu sơ đồ khối của một đầu hệ thống.

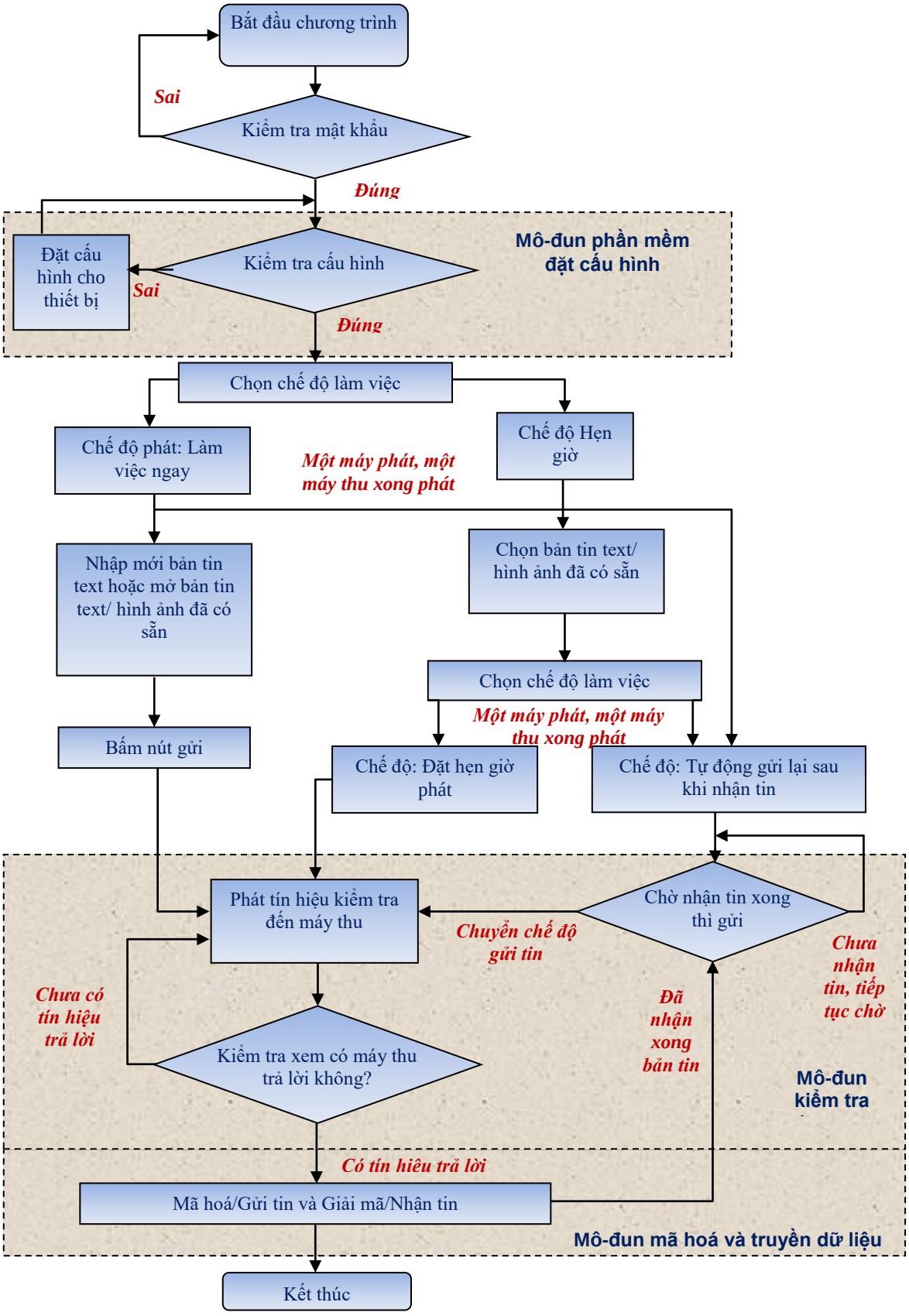
Việc kiểm tra khóa K cũng như dấu thủy vân số được thực hiện tự động, vì điều này cũng tương tự như việc thử ổ khóa. Không có kiểm tra khóa đúng rồi mới giải mã mà chương trình chỉ thực hiện 02 trường hợp:

- Nhập khóa để giải mã: Nếu giải mã được bản tin => Khóa đúng; ngược lại Nếu không giải mã được bản tin => Khóa sai!

Sơ đồ khối điều khiển hệ thống bằng phần mềm ứng dụng nội dung nghiên cứu được và lưu đồ chương trình điều khiển hệ thống được thể hiện trong hình 4.3 và hình 4.4 dưới đây.



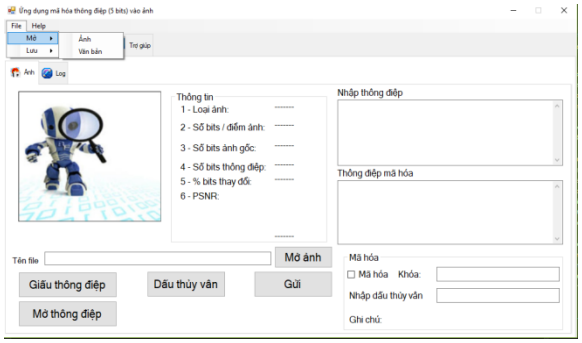
Hình 4. 3. Sơ đồ khối điều khiển hệ thống



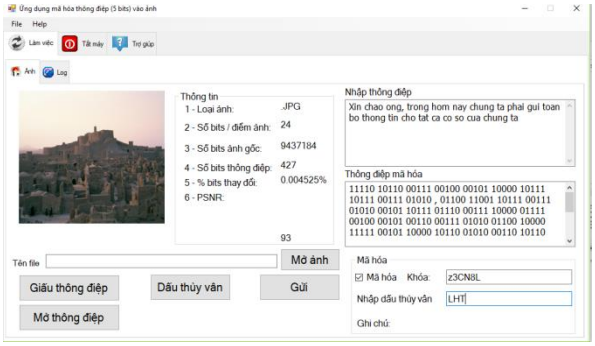
Hình 4. 4. Lưu đồ chương trình phần mềm điều khiển hệ thống

4.4. Kết quả thử nghiệm và đánh giá

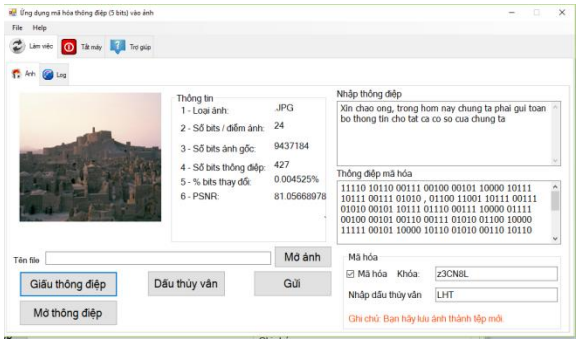
a. Một số giao diện chương trình điều khiển hệ thống



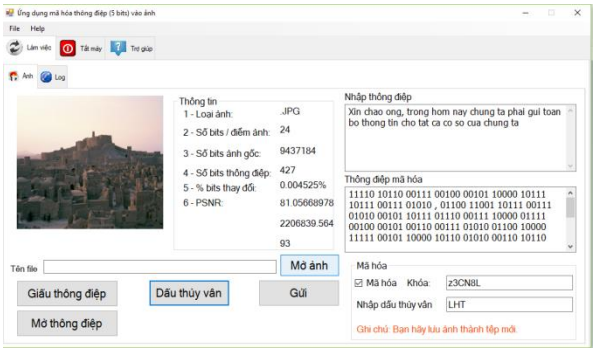
Hình 4. 5. Chọn ảnh C để giấu tin



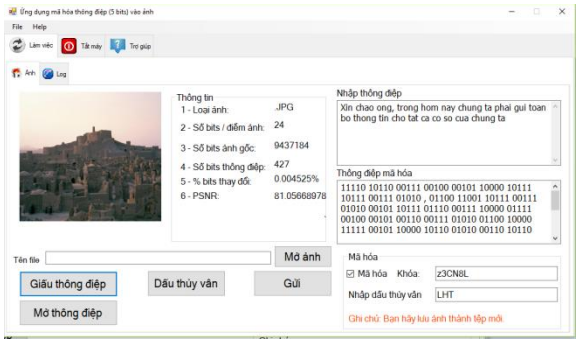
Hình 4. 6. Nhập bản tin M và sinh khóa K, dấu thủy vân W => Bản tin M'



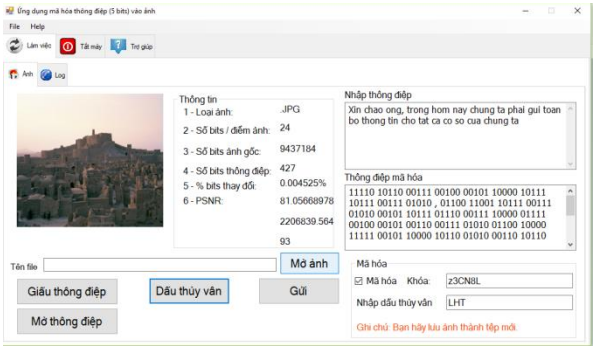
Hình 4. 7. Chọn giấu tin M vào ảnh C => ảnh S



Hình 4. 8. Đánh dấu thủy vân W lên ảnh S=> ảnh S_W



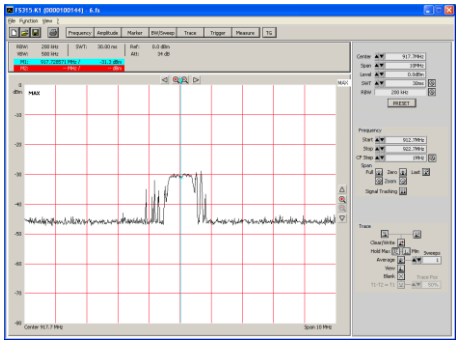
Hình 4. 9. Lưu ảnh S_W trước khi gửi



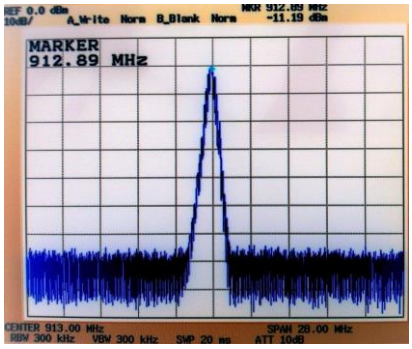
Hình 4. 10. Gửi ảnh S_W thành công

b. Kết quả về đo phổ

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.



Hình 4. 11. Phổ tần số tại 917.7MHz (kết quả đo trên máy phân tích phổ FS315 9kHz - 3GHz R&S)



Hình 4. 12. Phổ tần số tại 912.89MHz (kết quả đo trên máy phân tích phổ R3162 9kHz - 8GHz Advantest)

d. Kết quả đánh giá độ an toàn của hệ thống giấu tin

Các kết quả đánh giá độ an toàn của hệ thống đã được thể hiện bằng kết quả đánh giá độ an toàn của thuật toán giấu tin trong bảng 2.8 mục 2.3.5.1 với độ an toàn đạt trên 98% của hệ thống qua mỗi phiên liên lạc gửi và nhận thành công.

c. Đánh giá kết quả:

Thiết bị truyền ảnh có tính năng truyền bản tin ảnh số và bản tin text có mã hóa. Công nghệ sử dụng trong thiết bị là thu phát số OFDM, kỹ thuật trải phổ nhảy tần FHSS, với thiết kế là số kênh là 7 kênh và 25 tần số từ 902 MHz đến 928MHz. Việc chọn tần số 912 MHz và 917 MHz là ngẫu nhiên khi đo trên 2 thiết bị khác nhau. Thiết bị thứ nhất là máy phân tích phổ R&S FS315 tại đơn vị của NCS; thiết bị thứ hai là máy phân tích phổ Advantest R3162 tại Trung tâm Giám định chất lượng, Cục Tiêu chuẩn-Đo lường-Chất lượng, Bộ Quốc phòng ở các thời điểm khác nhau, nên cho kết quả đo khác nhau. Kết quả phổ tần của 2 tần số 1 đỉnh nhọn và 1 đỉnh phẳng là khi truyền bản tin text và bản tin hình ảnh. Bản tin text có dung lượng rất nhỏ, do vậy thời gian truyền rất ngắn và có phổ nhỏ; Bản tin ảnh số có dung lượng lớn và nhúng tin mật bên trong nên thời gian truyền lâu hơn, phổ rộng hơn. Việc lựa

chọn dải tần số 900 MHz cũng là một yếu tố hóa trang tần số trùng với dải tần số làm việc của mạng di động ở băng tần số GSM 900MHz để tăng tính bảo mật cho hệ thống.

d. Nhận xét kết quả thử nghiệm:

Thiết bị đã đáp ứng bước đầu các yêu cầu về thiết kế, lập trình, giao diện chương trình làm việc, vỏ máy…Chỉ tiêu kỹ thuật của thiết bị cơ bản đạt yêu cầu đặt ra. Khả năng liên lạc tốt khi di chuyển cùng chiều với vận tốc nhỏ hơn 30km/h và ngược chiều với vận tốc nhỏ hơn 25km/h. Đã hoá trang được cho sản phẩm vào các vỏ mẫu: vali xách tay, cặp tài liệu và túi xách đồ nghề. Trong phụ lục, luận án trình bày 3 kết quả thử nghiệm thiết bị với các tình huống thực hành khác nhau.

Dưới đây là một số đánh giá so sánh thiết bị hệ thống: so sánh giữa kết quả thực tế và yêu cầu đề ra Bảng 4.2, so sánh với thiết bị chuyên dụng có tính năng tương đương Bảng 4.3, Bảng 4.4.

Bảng 4. 2. So sánh kết quả đo, kiểm tra thiết bị thực tế với yêu cầu đã đặt ra

Chỉ tiêu	Chỉ tiêu kỹ thuật đạt được	Yêu cầu đặt ra
Dải tần số làm việc	902 - 928MHz	900Hz hoặc 2.4GHz
Số kênh làm việc	7 kênh 25 tần số	<=8 kênh
Công suất	100mW	<=60mW
Phạm vi liên lạc có che khuất	30 - 90m (liên lạc tốt trong 50m)	30 - 100m
Phạm vi liên lạc không che khuất	100 - 300m (liên lạc tốt trong <200m)	300 - 500m
Tốc độ dữ liệu RF	9,6 - 38,4Kbps	9,6kbps - 34.8Kbps
Mã hoá dữ liệu AES	Có	Có
Nguồn cung cấp	9VDC	3 - 12 VDC
Dòng tiêu thụ khi phát	60 - 75mA	<50mA
Dòng tiêu thụ khi thu	65 - 75mA	<60mA
Dòng chờ	25 - 30µA	<20µA

Bảng 4. 3. So sánh các chỉ tiêu kỹ thuật chính với thiết bị chuyên dụng

Các chỉ tiêu kỹ thuật chính	Thiết bị thiết kế	Thiết bị chuyên dụng
Dải tần số làm việc	902 - 928MHz	390 - 440MHz
Số kênh làm việc (FHSS)	7 kênh 25 tần số	44 kênh
Phạm vi liên lạc có che khuất	30 - 90m	30 - 600m
Phạm vi liên lạc không che khuất	100 - 300m	600 - 1000m
Phạm vi liên lạc tốt (có che khuất)	<50m	300m
Phạm vi liên lạc tốt (không có che khuất)	100 - 200m	600m
Tốc độ dữ liệu RF	9,6 - 38,4Kbps	9,6Kbps
Mã hoá dữ liệu AES 128bit	Có	Có
Nguồn cung cấp	9VDC, 1.1A	7.2VDC, 3.6Ah
Công suất	100mW	~465mW

Bảng 4. 4. So sánh một số tính năng cơ bản với thiết bị chuyên dụng

Một số tính năng cơ bản	Thiết bị thử nghiệm	Thiết bị chuyên dụng
Khả năng làm việc trực tiếp	Tích hợp hệ thống nhúng	Phải kết nối PC
Chế độ làm việc tức thời	Có	Có
Hẹn giờ gửi tin	Có	Có
Nhận tin xong thì gửi lại	Có	Có
Điều chỉnh cấu hình giao diện nối tiếp	Có	Không
Kiểm tra bản tin tại chỗ	Có	Không
Soạn thảo bản tin trực tiếp trên thiết bị	Có	Không
Sai số thời gian khi liên lạc	Tối đa 1h (*lập trình bằng phần mềm*)	Từ ±5ph đến ±30ph
Chức năng xoá khẩn cấp	Không (*Chưa thực hiện*)	Có
Điều chỉnh thiết kế và cấu hình	Có	Không

thiết bị		(*Mặc định của nhà SX*)
Dung lượng bản tin	Không hạn chế (*khuyến nghị bản tin < 100kb*)	2kb
Định dạng bản tin	Tất cả các loại định dạng	Text
Dung lượng và thời gian gửi tin	2k - 3s; 4k - 6s, 20k - 26s; 28k - 31s; 65k - 1ph12s; 70k - 1ph26s; 87k - 2ph33s;	2k - 6s
Khả năng lưu trữ	Không giới hạn	1 bản tin duy nhất
Thời gian chờ của ắc-qui	2h30ph	20h
Thời gian làm việc của ăc-qui máy phát	20ph - 1h20 (*phụ thuộc loại pin*)	3h

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 quả thuật toán giấu tin mục 2.1, sinh khóa K mục 2.2 và đánh giá độ an toàn của thuật toán 2.3 đã được đưa vào thực hiện trực tiếp trên hệ thống cho thấy nội dung nghiên cứu đã bám sát yêu cầu và đưa được vào ứng dụng trong thiết bị thực tế. Nội dung 3.1 và 3.2 mới được đánh giá trên bằng mô phỏng số. So sánh với thiết bị chuyên dụng đang được sử dụng, đối với phần mềm ứng dụng kết quả nghiên cứu cho thấy hoàn toàn khả thi sau khi hoàn thiện hệ thống;

Tuy nhiên trong thực tế thiết bị chuyên dụng chỉ vượt một số chỉ tiêu về phần cứng mà thôi. NCS cũng chưa có điều kiện thử nghiệm đối với các module phần cứng có công suất phát lớn hơn (khoảng từ 300 - 500mW hoặc 1W). Hiện nay hệ thống đã đạt được một số kết quả ban đầu và đang tiếp tục hoàn thiện để đưa vào sử dụng trong thực tế công tác của đơn vị.

KẾT LUẬN

Bài toán bảo mật thông tin giấu trong ảnh số là bài toán cấp thiết hiện nay trong lĩnh vực an toàn, bảo mật thông tin nói chung, lĩnh vực quốc phòng-an ninh nói riêng. Có nhiều hướng tiếp cận nghiên cứu về bảo mật thông tin giấu trong ảnh số, đòi hỏi phải được nghiên cứu một cách đa chiều, toàn diện. Từ các nghiên cứu đó, phạm vi ứng dụng của bài toán giấu tin sẽ được mở rộng và đa dạng hóa đối tượng ứng dụng trong các nhiệm vụ cụ thể.

Dựa trên phương pháp nghiên cứu được sử dụng như thông qua một số cơ sở lý thuyết toán học, xây dựng thuật toán và đề xuất mô hình thực hiện để phân tích, dánh giá kết hợp với các công cụ thống kê, toán học cũng như mô phỏng trên máy tính, các kết quả chính của luận án được trinh bày trong chương 2 và chương 3. Chương 4 đã hiện thực hóa nội dung nghiên cứu và ứng dụng cụ thể vào thiết bị nghiệp vụ, bước đầu đã đáp ứng một số tiêu chí cơ bản công tác nghiệp vụ.

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; Từ nghiên cứu về phương pháp đánh giá độ an toàn hệ thống mật mã và hệ thống giấu tin trong ảnh số, luận án đề xuất thuật toán thực hiện đánh giá độ an toàn toàn của hệ thống mật mã và giấu tin. Cụ thể là:*

- Đóng góp thứ nhất: Xây dựng thuật toán giấu tin mới sử dụng bộ mã 5 bít, trong khi các thuật toán giấu tin khác đã được công bố sử dụng bộ mã ASCII mở rộng là 8 bít. Nội dung này giải quyết 4 vấn đề. *Thứ nhất,* giảm tỷ lệ nhúng xuống khoảng 3,2% (≈1/31). Nếu tỷ lệ nhúng dưới 10% thì mọi phương pháp dò tìm bằng các thuật toán thống kê đều cho hiệu quả rất hạn chế. Với các thuật toán giấu tin

mật có tỷ lệ thay đổi bit LBS thấp khoảng 3% thì đây là tỷ lệ cho phép chống lại các thuật toán tấn công thông kê cấp 1 và cấp 2. *Thứ hai là* thuật toán giấu tin trên có ưu điểm là đơn giản cho việc nhúng và trích chọn, ngoài ra lượng thông tin giấu được lớn nhưng các LSB thay đổi ít hơn. *Thứ ba* là việc sử dụng bộ mã 5 bít trên cơ sở bộ mã Hamming, thuật toán đề xuất mới đã tăng được khả năng giấu tin lên gấp ít nhất là 8 lần so với các thuật toán khác. *Thứ tư,* việc sử dụng từ mã 5 bít sẽ mã hết toàn bộ 26 ký tự Latinh và 6 bít dư được dùng để mã hóa cho một số từ thường khác hoặc dùng cho ký hiệu điều khiển [T4]. Kết quả so sánh thuật toán đề xuất mới và thuật toán cũ đã được cho trong các bảng 2.4, 2.5 và 2.6.

- Đóng góp thứ hai: Xây dựng thuật toán sinh bit giả ngẫu nhiên mới có chu kỳ cực đại bằng phương pháp đồng dư tuyến tính, nhằm phục vụ trao đổi khóa bí mật cho việc giấu tin trong ảnh số. Ba ưu điểm trong thuật toán mới được thể hiện sau đây. *Thứ nhất,* chu kỳ R của dãy được kiểm soát nếu thực hiện đúng giả thiết của Định lý 2; *Thứ hai,* việc trao đổi khóa rất đơn giản, chỉ cần 4 tham số x_0,a,b,m (công thức 2.14). Tùy theo yêu cầu của ứng dụng để chọn m cho phù hợp. Đây là công thức truy hồi để tìm dãy $\{x_n\}$ với $n\geq 2$. *Thứ ba,* thuật toán này được sử dụng cho việc trao đổi khóa mật mã phục vụ đối với thuật toán 5 bít trong mục 2.1.4 trước bằng hệ mật mã khóa công khai và ứng dụng trực tiếp cho nội dung trong chương 4 cũng như trong quốc phòng-an ninh [T5].

- Đóng góp thứ ba: Từ các phương pháp đánh giá chất lượng giấu tin mật và sinh khóa giả ngẫu nhiên, luận án xây dựng thuật toán đánh giá độ an toàn bảo mật. *Thứ nhất,* để đánh giá chất lượng của các bản mã do hệ thống sinh tạo ra, ta sẽ đánh giá chất lượng các dãy giả ngẫu nhiên được dùng để mã hóa các bản thông báo một dãy dãy giả ngẫu nhiên được sinh từ hệ thống nào đó được coi là tốt nếu các thành phần của dãy đó là độc lập và có phân bố đều. Như vậy, một dãy giả ngẫu nhiên hoàn toàn độc lập và có phân bố đều là dãy thuộc xích markov với ma trận chuyển trạng thái là $P = (P_{ij})_{mxm}$ trong đó m là số trạng thái khác nhau của xích. Từ đó

luận án đề xuất xây dựng thuật toán đánh giá an toàn đối với hệ thống sinh bít giả ngẫu nhiên tùy ý và thuật toán đánh giá an toàn đối với hệ thống dãy giả ngẫu nhiên chữ cái Latinh. *Thứ hai,* đối với thuật toán giấu tin, trong thực tế việc đánh giá "khó cảm nhận bằng mắt thường" hoặc "không thể phát hiện bằng phương pháp thống kê" đã có khái niệm về phương pháp đánh giá độ an toàn hoàn hảo. Đối với một hệ thống giấu tin mật Ω, ta có $P_S(.)$ 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. 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). Trong thực tế để thực hiện điều này rất khó, do vậy luận án đề xuất thuật toán đánh giá hàm D dựa theo công thức (2.15) để giải quyết theo hướng đơn giản và hiệu quả hơn. Kết quả đánh giá sai phân D được cho trong bảng 2.8. [T3]

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, cụ thể là:*

- Đóng góp thứ tư: Trên cơ sở 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, luận án đã giải quyết 3 vấn đề. *Thứ nhất,* cung cấp mô hình phân tích và kết quả số mô tả hiệu năng lỗi cho mô hình đề xuất trong quá trình xử lý ảnh theo chuẩn JPEG/JPEG2000 [T2] và quá trình đánh dấu bảo mật watermark vào dữ liệu cảm biến tương ứng. Nghiên cứu này tập trung vào các phương thức biến đổi khác nhau và so sánh mức độ hiệu quả giữa chúng. *Thứ hai,* từ xác suất tìm thấy watermark tại phía nhận thông qua mô phỏng số, ta thấy rằng, xác suất này phụ thuộc vào các tham số thay đổi như độ lớn watermark trung bình, xác suất cảnh báo sai, hệ số nén và kích thước ảnh cho đến cách chia khối cho từng ảnh. *Thứ ba,* dựa trên kết quả có được, có thể đánh giá rằng bảo mật đối với ảnh số bằng đánh dấu

watermark theo phương pháp DWT là lựa chọn tốt nhất cho cả vấn đề hiệu năng lỗi cũng như xác suất tìm thấy dấu watermark [T6].

- Đóng góp thứ năm: Dựa trên việc hiệu suất mạng bị hạ xuống trong các cuộc tấn công thông thường, luận án xây dựng mô hình trạng thái thuật toán Back-off, mô hình trạng thái kênh, các tham số hiệu suất. Từ các mô hình đó, luận án đã giải quyết các vấn đề sau. *Thứ nhất*, đề xuất một mô hình phân tích mới đối với lớp MAC của IEEE 802.11 bằng việc sử dụng các thuật toán EIED đã bao gồm xử lý hiện tượng đóng băng back-off. *Thứ hai,* dựa trên kết quả số về phân tích hiệu suất mạng theo các thuật toán back-off khác nhau với 3 tham số *lưu lượng truyền tải, xác suất rớt gói tin và độ trễ truy cập* đối với nút bình thường và nút lỗi để cho ra kết quả là khác nhau theo các tấn công thông thường. *Thứ ba* là thông qua nghiên cứu này, luận án đánh giá được thuật toán EIED back-off có hiệu suất tốt hơn so với thuật toán BEB trong điều kiện thông thường. Tuy nhiên, khi mạng tồn tại nút độc do ảnh hưởng của các tấn công thông thường, thì hiệu suất của mạng sử dụng thuật toán BEB back-off tốt hơn thuật toán EIED. [T7]

A.3. *Dựa trên các nội dung đã nghiên cứu, luận án đã ứng dụng vào thiết bị thông tin liên lạc bí mật bản tin hình ảnh cụ thế phục vụ công tác nghiệp vụ.*

- Đóng góp thứ sáu: căn cứ vào yêu cầu thực tế công tác về việc xây dựng hệ thống thông tin liên lạc bí mật bản tin bằng hình ảnh có bảo mật dựa trên thu phát số, luận án đã thực nghiệm xây dựng hệ thống. *Thứ nhất* đưa nội dung về giấu tin mật bằng bộ mã 5 bit vào mã hóa bản tin và ứng dụng thuật toán sinh số giả ngẫu nhiên để phục vụ thỏa thuận trao đổi khóa bí mật; sau đó ứng dụng đánh dấu watermark lên ảnh số trước khi truyền. *Thứ hai* là xây dựng hệ thống sử dụng kỹ thuật trải phổ nhảy tần FHSS với 7 hop và 25 tần số trên nền tảng lập trình SDR trước khi đưa đến bộ thu/phát. Kết quả thử nghiệm được thể hiện trong các phụ lục kèm theo [T1].

B. Những nội dung nghiên cứu tiếp theo

Hiện nay các phương pháp bảo mật thông tin trong ảnh số nói riêng và trong sản phẩm đa phương tiện số trong liên lạc công khai và bí mật luôn được các nước trên thế giới, nhất là các cơ quan đặc biệt về quốc phòng - an ninh quan tâm, đầu tư nghiên cứu và phát triển. Mỗi kỹ thuật giấu tin mới lại có nhiều ưu điểm và ngày càng hiệu quả hơn.

Theo hướng này, trong thời gian tiếp theo nghiên cứu sinh sẽ tiếp tục phát triển các nội dung sau:

- 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 cũng như các thủ tục và hồ sơ công nhận liên quan để đưa vào sử dụng trong thực tế công tác.

DANH MỤC CÁC CÔNG TRÌNH ĐÃ CÔNG BỐ

[T1] 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.

[T2] 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.

[T3] 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.

[T4] 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.

[T5] 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 .

[T6] 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.

[T7] 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.

TÀI LIỆU THAM KHẢO

Tiếng Việt

[1] Phan Đình Diệu, *(2002), Lý thuyết mật mã và an toàn thông tin, NXB Đại học Quốc gia Hà Nội*.

[2] Hồ Thị Hương Thơm, *(2012) "Nghiên cứu một số kỹ thuật phát hiện ảnh giấu tin", Luận án tiến sỹ, Đại học Quốc gia Hà Nội, Hà Nội*.

[6] Hồ Văn Canh and Nguyễn Viết Thế , *(2010), Nhập môn Phân tích thông tin có bảo mật. NXB Thông tin và truyền thông*.

[17] Hoàng Văn Thức, *(2011), "Hệ tiêu chuẩn tham số an toàn cho hệ mật RSA và ứng dụng", luận án tiến sỹ, Viện KHCN Quân sự*.

[18] Ban Cơ yếu Chính phủ, *(2007), TCVN 7817-3:2007, Công nghệ thông tin - Kỹ thuật mật mã quản lý khoá - Phần 3: Các cơ chế sử dụng kỹ thuật không đối xứng, Bộ KH&CN*.

[19] Trần Đức Lịch, Nguyễn Văn Tú, Hồ Sỹ Tấn, *(4/2008), "Tiêu chuẩn quốc gia Việt Nam về Quản lý khóa", Tạp chí An toàn thông tin, Ban Cơ yếu Chính phủ, Hà Nội*.

[41] Huỳnh Bá Diệu, *(2017), "Một số kỹ thuật giấu thông tin trong âm thanh số", luận án tiến sĩ, Đại học Quốc gia Hà Nội*.

[42] Vũ Bá Đình, Nguyễn Xuân Huy, and Đào Thanh Tĩnh, *(2002) "Đánh giá khả năng giấu dữ liệu trong bản đồ số", Tạp chí Tin học và Điều khiển học, số 4, tr. 347-353.*

[43] Vũ Văn Tâm and Phan Trọng Hanh, *(8/2014), "Một phương pháp mới nhúng dữ liệu vào tín hiệu audio", Tạp chí Nghiên cứu khoa học và công nghệ quân sự, trang 58-64.*

[44] Bùi Văn Tân, *(2012) "Nâng cao hiệu quả giấu tin trong ảnh nhị phân", Tạp chí KH ĐHQG Hà Nội, số 28, trang 110-115.*

[49] Chu Hà, *(2004), "Tình báo vô tuyến điện tử", NXB Công an nhân dân*.

[51] Bộ TT&TT, *(2017), TCVN 11777-5:2017 (ISO/IEC 15444-5:2015), Công nghệ thông tin - Hệ thống mã hóa hình ảnh JPEG 2000 – Phần 5: Phần mềm tham chiếu, Bộ KH&CN*.

[105] Đỗ Xuân Tiến, *(1991), Kỹ thuật Vi xử lý, Học viện Kỹ thuật Quân sự, Hà Nội*.

Tiếng Anh

[3] Frank Y. Shih, *(2017), Digital Watermarking and Steganography: Fundamentals and Tecniques, Second Edition, CRC Press, New Jersey Institute of Technology, USA*.

[4] Jessica Fridrich, *(2009), Steganography in digital media: principles, algorithms, and applications, Cambridge University Press*.

[5] Fabien A. P. Petitcolas Stephan Katzenbeisser, *(2000), "Information Hiding Techniques for Steganography and Digital Watermarking", Artech House , Boston, London*.

[7] C.Cachin, *(1998), "An information - Theoretic Model for staganography", InD. Aucsmith, Edittor, Information Hidding, 2rd International Workshop, volume 1525 of LNCS, Springter, Newyork, pp 306-318*.

[8] I.Y. Soon B. Leia, *(2015), Perception-based audio watermarking scheme in the compressedbitstream. International Journal of Electronics and Communications (AEU), ELSEVIER, pp. 188-197*.

[9] A. Khan, A. Siddiqua, S. Munib, S.A. Malik, *(2014) A Recent Survey of Reversible Watermarking Techniques. Information Sciences, pp.251-272*.

[10] B. Smitha, K.A. Navas, *(2007) Spatial Domain - High Capacity Data Hiding in ROI Images. IEEE - ICSCN, MIT Campus, Anna University, Chennai, India, pp.528-533*.

[11] Abid Yahya, *(2018), Steganography Techniques for Digital Images, Springer, ISBN 978-3-319-78535-6, pp. 11*.

[12] Jessica Fridrich, Ton Kalker, Ingemar J.Cox, Matthew L. Miller, and Jeffrey A. Bloom, *(2008), Digital Watermarking and Steganography, Morgan Kaufmann Publishers, Second Edition, ISBN 978-0-12-372585-1*.

[13] R. Liu, T.Tan, *(2002) An SVD Based watermarking scheme for protecting rightful ownership. IEEE Transactions on Multimedia, Vol.4, pp. 121-128*.

[14] Olivien Billet Matthew Robshaw, *(2008), "New Stream Cipher Designs: The eSTREAM Finalists", Springer-Verlag Berlin, Heidelberg*.

[15] Kalendri, Maria; Pnevmatikatos, Dionisios and Papaefstathiou, Ioannis; Manifavas, Charalampos, *(2012),"Breaking The GSM A5/1 Cryptography. Algorithm with Rainbow Tables and High--end FPGAs", In proc. Of 22nd International Conference on Field-programmable Logic and Applications, pp.747-753*.

[16] Lano J., *(2006), "Cryptanalysis and Design of Synchronous Stream Ciphers" PhD thesis, Katholieke Universiteit Leuven, Faculteit Ingenieurswetenschappen, Department Elektrolechnik_ESAT*.

[20] M.Y. Wu, Y.H. Ho, J.H. Lee, *(2004) An iterative method of palette-based image steganography. Pattern Recognition Letters 2-5, pp. 301-309*.

[21] R. Chandramouli, M. Kharrazi and N. Memon, *(2004), "Image Steganography and Steganalysis: Concepts and Practice", international workshop on digital watermarking, No. 2, COREE, REPUBLIQUE DE , vol. 2939, pp. 35-49*.

[22] V.K. Sharma, V. Shrivastava, *(2012) A Steganography Algorithm For Hiding Image In Image By Improved Lsb Substitution By Minimizedetection. Journal of Theoretical and Applied Information Technology, pp. 1-8*.

[23] K. M. Sullivan, *(2005), Image steganalysis: Hunting and Escaping, Ph. D Thesis in Electrical and computer Engineering, University of California*.

[24] Feno Heriniaina R.1 , Xiaofeng Liao, *(2016), Pictographic steganography based on social networking websites, ACSIJ Andvances in Computer Science:*

an International Journal, Vol. 5, Issue 1, No 19, ISBN 2322-5157, pp. 142-150.

[25] C. I. Podilchuk and E. J. Delp, *(2001), "Digital watermarking: Algorithms and applications ", IEEE Signal Process. Mag., vol. 18 (4), pp. 33-34.*

[26] Tran Dang Hien, Do Van Tuan and Le Hung Son Pham Van At, *(2012) A Novel Algorithm for Nonnegative Matrix Factorization. Proceeding of The 16th Asia Pacific Symposium on Intelligent and Evolutionary Systems, 2012, Kyoto, Japan, p.117-123, ISBN978-4-9906692-0-.*

[27] Michiharu Hideki Noda and Takayuki Ishida, Kazumi Yamawaki, *(2009), "Performance improvement of JPEG2000 steganography using QIM", Journal of Communication and Computer, Volume 6 (l), USA.*

[28] H. C. Wu, N. I. Wu, C. S. Tsai, M. S. Hwang, *(2005), "Image Steganographic scheme based on pixel - value differencing and LSB replacement methods", IEE Proc.-Vis. Image Signal Process, Vol. 152, Issue 5, pp. 611-615.*

[29] Y. Wang, P. Moulin, *(2003), "Steganalysis of Block-DCT Image Steganography", Proc. IEEE Workshop on Statistical Signal Processing.*

[30] Xiaolong Li, Bin Yang and Tieyong Zeng Daofang Cheng, *(2009), "A Generalization of LSB Matching", IEEE signal processing letters, Vol. 16 (2), pp. 69-72.*

[31] P. M. Kumar, K. L. Shunmuganathan, *(2010), "A reversible high embedding capacity data hiding technique for hiding secret data in images ", International Journal of Computer Science and Information Security (IJCSIS), Vol.7 (3), pp. 109-115.*

[32] J.etal Foley, *(1990),"Computer Graphic: principles and practice". MA. Addison Wesley.*

[33] C.A.Stanley, *(2005), Pair of values and the chi-square attack, Department of Mathematics, Iowa State University.*

[34] I.J. Cox, J. Kilian, T. Leighton, T. Shamoon, *(1996) Secure spread spectrum*

watermarking for images, audio and video. Proc IEEE Internat. Conf. on Image Processing (ICIP'96) Vol. III, Lausanne, Swizerland, 16-19 September 1996, pp. 243-246.

[35] J. Kilian, T. Leighton, and T. Shamoon J. K I. Cox, *(1997), Secure spread spectrum watermarking for multimedia, IEEE Trans. on Image Processing, 6(12): pp.1673 - 1687*.

[36] B. Chen and G. Wornell, *(2001), Quantization index modulation: A class of provably good methods for digital watermarking and information embedding", IEEE Trans. Info. Theary, Vol. 47 (4), pp. 1423 - 1443*.

[37] J. Tian, *(2002), Reversible Watermarking by Difference Expansion, In Proc. of Workshop on Multimedia and Security, pp. 19 - 22*.

[38] Z., Shi, Y., Ansari, N., Su, W. Ni, *(2003), Reversible data hiding, Proc. ISCAS 2003, pp. 912 - 915*.

[39] J. Lee M. Wu, *(1998), A Novel Data Embedding Method for Two-Color Facsimile Images, Proceeding of International Symposium on Multimedia Information Processing, Taiwan*.

[40] Hsiang-Kuang Pan, Yu-Chee Tseng Yu-Yuan Chen, *(2000), A Secure Data Hiding Scheme for Two-Color Images, National Central University, Taiwan*.

[45] S.S. Bedi, S. Verma, G. Tomar, *(2010) An Adaptive Data Hiding Technique for Digital Image Authentication. International Journal of Computer Threory and Engineering, Vol. 2, No. 3, pp. 338 -344*.

[46] Joseph Raphael A., Sundaram V., *(2010), "Secured Communication through Hybrid Crypto-Steganography", International Journal of Computer Science and Information Security (IJCSIS), Vol. 8 (4), pp. 45-48*.

[47] S. Saha, D. Bhattacharyya, S.K. Bandyopadhayay, *(2010) Security on Fragile and Semi-Fragile Watermarking Authentication. International Journal of Computer Applications, Vol.3, No.4, pp. 23-27*.

[48] G. Bhatnagar, B. Raman, *(2009) A new robust reference watermarking scheme based on DWT-SVD. Computer Standards & Interfaces, pp. 1002-1013.*

[50] O. Gonçalves and D. Costa. De. Danilo, *(2015), A Survey of Image Security in Wireless Sensor Networks. Journal of Imaging, pp1, 4-30.*

[52] C. Chirstopoulos, and T. Ebrahimi A. Skordas, *(2001), The JPEG 2000 still image compression standard, IEEE Signal Processing Magazine, vol 5, pp 36-58.*

[53] Kemal Bicakci, Ruken Zilan, and Jose M. Barcelo-Ordinas Bulent Tavli, *(2012), A survey of visual sensor network platforms. Multimedia Tools Appl, vol 60, 3, pp. 689-726.*

[54] Y., Suying, Y., Jiangtao, X., Yu, Z and Ye C. Ping ping, *(2009), Copyright protection for digital image in wireless sensor network. In proceeding of 5th International conference on wireless communications, networking and mobile computing, pp.1-4.*

[55] Gwenaël Doërr and Teddy Furon Ingemar J. Cox, *(2006). Watermarking is not cryptography, digital watermarking. In Lecture Notes in Computer Science, 4283, 1-15.*

[56] Robert C., Stefan Winkler, and David S. Hands Streijl, *(2016), "Mean opinion score (MOS) revisited: methods and applications, limitations and alternatives.", Multimedia Systems Journal, Vol 22.2, pp. 213-227, Springer.*

[57] IEEE, *(2007), IEEE 802.11 standard, Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications.*

[58] Y. Shu, M. Li, O.W.W Yang C. Liu, *(2008), Delay Modeling and Analysis of IEEE 802.11 DCF with Selfish Nodes, in Procs. 4th International Conference on Wireless Communications Networking and Mobile Computing, pp. 1-4.*

[59] J. Choi, K. Kang, Y.C. Hu K.J. Park, *(2009), Malicious or Selfish? Analysis of Carrier Sense Misbehavior in IEEE 802.11 WLAN, Lecture Notes of the*

Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, 22, pp 351-362.

[60] Y. Li and A. Reznik C. Ye, *(2010), Performance Analysis of Exponential Increase Exponential Decrease Back-off Algorithm, Proc. IEEE Globecom, pp. 1-6*.

[61] G. Bianchi, *(2000), Performance analysis of the IEEE 802.11 distributed coordination function, IEEE J. Sel. Areas Commun. vol 18, pp. 535-547*.

[62] Y. Shu, W. Yang, O.W.W Yang C. Liu, *(2008), Throughput Modeling and Analysis of IEEE 802.11 DCF with Selfish Node, Proc. IEEE GLOBECOM, pp. 1-5*.

[63] A.D. Ker, *(2007),"Steganalysis of Embedding in Two Least-Significant Bits", IEEE Transactions on Information Forensics and Security 2,pp. 46-54*.

[64] Xiangyang Luo, Fenlin Liu Chunfang Yang, *(2009), "Embedding Ratio Estimating for Each Bit Plane of Image", Springer-Verlag Berlin Heidelberg*.

[65] E. Tang, and B. Liu M. Wu, *(2000), "Data Hiding in Digital Images", IEEE International Conference on Multimedia, Expo (ICME)*.

[66] S. A Pfitzmann and I. Stirand Moller, *(1996), "Computer Based Stenography: How It Works and Why Therefore Any Restrictions on Cryptography Are Nonsense At Best", In Information Hiding Notes in Computer Science, Springer, pp. 7-21*.

[67] Z. Duric, D. Richards Y. Kim, *(2007),"Modified matrix encoding technique for minimal distortion steganography", LNCS, vol. 4437, Springer, Heidelberg*.

[68] Stephen B. Wicker, *(2009),"Error Control Systems for Digital Communication and Storage", Prentice Hall - New Jersey*.

[69] Vasiliy Sachnev Rongyue Zhang, *(2009), Hyoung-Joong Kim Fast "BCH Syndrome Coding for Steganography",Lecture Notes in Computer Science, Volume 5806, CIST, Graduate School of Information Management and*

Security Korea University, Seoul, Korea, pp 48-58.

[70] A. Westfeld, *(2001), "High Capacity Despite Better Steganalysis (F5-A Steganographic Algorithm)", In: Moskowitz, I.S. (eds.): Information Hiding. 4th International Workshop. Lecture Notes in Computer Science, Vol.2137. Springer-Verlag, Berlin Heidelberg Ne*.

[71] Narendra S. Chaudhari Ashish Jain, *(2014), "Cryptanalytic Results on Knapsack Cryptosystem Using Binary Particle Swarm Optimization", International Conference on Computational Intelligence in Secuirty for Information System (CISIS 2014), Springer International Publishing, pp. 375-384.*

[72] S. Blackburn U. Baum, *(1995), "Clock-controlled pseudorandom generators on finite groups, pp 6-21, BPreneel, editor (LNSC 1008), Springer- Verlag.*

[73] J. L. Massey U. Maurer, *(1991), "Local Randomness in Pseudorandom Sequences", Journal of Cryptology: the journal of the International Association for Cryptologic Research Volume 4, Number 2.*

[74] C. P. Schnorr S. Micali, *(1991), "Efficient, perfect polynomial random number generators", Journal of Cryptology, v.3 n.3, p.157-172.*

[75] Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone, *(1999), "Handbook of Applied Cryptography", CRC Press: Boca Raton, New York, London, Tokyo.*

[76] D. L. Kreher and D.R. Stison, *(1999), "Combinatorial Algorithms: Generation Enumeration and Search", CRC Press.*

[77] Andreas Klein, *(2013), "Stream Ciphers", Springer London Heidelberg, New York Dordrecht.*

[78] R. Kohno and H. Imai H. Fukumasa, *(1994), "Design of pseudonoise sequences with good odd and even correlation properties for DS/CDMA", IEEE Journal on Selected Areas in Communications, Volume 12, Issue 5.*

[79] Daniel J. Bernstein, *(2008). The Salsa20 family of stream ciphers. In Matthew Robshaw and Olivier Billet, editors, New Stream Cipher Designs, volume 4986 of Lecture Notes in Computer Science, pages 84-97. Springer Berlin Heidelberg*.

[80] M. Blum and S. Micali, *(2006), "How to generate cryptographycally strong sequences of pseudorandom bits", SIAM Journal on Computing, Volume 13, Issue 4, pp. 850-864*.

[81] E. Bach, *(2005), "Realistic Analysis of some Randomized Algorithms", Journal of Computer and System Sciences*.

[82] Low S. H. and N. F. Maxemchuk, *(2008), "Performance Comparison of Two Text Marking Methods ", IEEE Journal on Selected Areas in Communications , Vol. 6, No 4.pp. 561-572*.

[83] Yiming Yang, Konstantin Salomatin, Jaime Carbonell Siddharth Gopal, *(2013), "Statistical Learning for File - Type Identification ", Institute for System Architecture Technishe Universtät Dresden 01002 Dresden , Germany*.

[84] Skitovich. V. P, *(1998), "Linear Forms of Indepent Radom Variables and The Normal Distribution Law", New York, London, Tokyo*.

[85] V. Vapnik, *(2005), "The Nature of Statistical Learning Theory ", Springer - Verlag, New York.*

[86] J. Xu, C. Lu, Ma, S. Zhang X. Cheng, *(2012), "A Dynamic Batch Sampling Mode for SVM Active Learning in Image Retrieval ", In Recent Advances in Computer Science and Information Engineering, Vol. 128 of Lecture Notes in Electrical Engineering*.

[87] Jim K. Omura, Robert A. Scholtz, Barry K. Levitt Marvin K. Simon, *(2015), "Spread Spectrum Communications Handbook", Mc Graw- Hill Inc.*

[88] L., and I.S. Moskowitz Chang, *(2007), "Critical Analysis of Security in Voices Hiding Techniques ", In Proceedings of the International Conference on*

Information and Communications Security, Vol. 1334 of Lecture Notes in Computer Science , Springer.

[89] A. Sharif, E. Chang V. Potdar, *(2009), Wireless sensor networks: A survey. In Proceedings of the IEEE AINA, pp. 636- 641*.

[90] Ibrahim Kamel and Lami Kaya Hussam Juma, *(2008), Watermarking sensor data for protecting the integrity. In International Conference on Innovations in Information Technology, pp. 598-602*.

[91] Jessica Fridrich and P.Miodrag, *(2003), Real-time watermarking techniques for sensor networks. Proceedings SPIE The International Society for optical Engineering, pp. 391-402*.

[92] Vidyasagar Potdar, and Jaipal Singh Bambang Harjito, *(2012), Watermarking technique for wireless multimedia sensor networks: a state of the art. In Proceedings of the CUBE International Information Technology Conference (CUBE '12). ACM, New York, NY, USA, pp. 832-840*.

[93] Yao S, Xu J, Zhang Y, and Chang Y. Yu P, *(2009), Copyright protection for digital image in wireless sensor network. In Proceedings of International Conference on Wireless Communications, Networking and Mobile Computing, Beijing, China, pp. 1-4*.

[94] Mohammad A S and Hesham E., *(2014), Error Performance of JPEG and Watermark Authentication Techniques in Wireless Sensor Network. International Journal of Security, Privacy and Trust Management (IJSPTM), 3(3), pp. 1-14*.

[95] Yonghe Liu, Sajal K. Das, Pradip De. Wei Zhang, *(2008), Secure data aggregation in wireless sensor networks: A watermark based authentication supportive approach. Pervasive and Mobile Computing journal, pp. 658-680*.

[96] Z. and B. Liu Wenjun, *(1999), A statistical watermark detection technique without using original images for resolving rightful ownerships of digital images. In IEEE Transactions on Image Processing, 8(11), pp. 1534-1548*.

[97] Rafael C. Gonzalez and Richard E. Wood, *(2007), "Filtering in the frequency domain," In Digital Image Processing, Prentice Hall, 3rdedition, ,pp 247-275*.

[98] G. Bianchi and Y. Xiao I. Tinnirello, *(2010), Refinements on IEEE 802.11 distributed coordination function modeling approaches", IEEE Trans. 59 pp. 1055-1067*.

[99] H. Chen, *(2011), Revisit of the Markov model of IEEE 802.11 DCF for an error-prone channel, IEEE Communications Letters, vol. 15 pp. 1278-1280*.

[100] Van-Kien Bui, Thi Nguyen Trong-Minh Hoang, *(2015), Analyzing Impacts of Physical Interference on a Transmission in IEEE 802.11 Mesh Networks, Pro. TSSA Int Conf*.

[101] Y. Peng, K. Long, S. Cheng, and J. Ma H. Wu, *(2002), Performance of reliable transport protocol over IEEE 802.11 WLAN: Analysis and enhancement, Proc. IEEE INFOCOM, 2 pp. 599-607*.

[102] C. Assi, A. Benslimane L. Guang, *(2008), MAC layer misbehavior in wireless networks: challenges and solutions, IEEE Wireless Communications, vol. 15 pp. 6-14*.

[103] N. Jaggi V.R. Giri, *(2010), MAC layer misbehavior effectiveness and collective aggressive reaction approach", 2010 IEEE Sarnoff Symposium, pp. 1-5*.

[104] A. C. Boucouvalas and V. Vitsas P. Chatzimisios, *(2003), IEEE 802.11 Packet Delay: A Finite Retry Limit Analysis, IEEE GLOBECOM, vol. 2, pp. 950-954*.

PHỤ LỤC 1. MỘT SỐ MÔ ĐUN PHẦN MỀM

Hàm tạo khóa giả ngẫu nhiên

```
public static string RandomKey(int length)
        {
            const string chars =
"ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789";
            return new string(Enumerable.Repeat(chars, length)
              .Select(s => s[random.Next(s.Length)]).ToArray());
        }
```

Hàm mã hóa thông điệp thuật toán 5bit

```
   private static string[] arrCumTu = new string[] { "y/c", "k/g", "tr/loi",
"gap", "nguoi nhan" };
        private static Dictionary<string, string> dicMaHoa = new
Dictionary<string, string>()
    {
        { "ong", "00000"},
        { "a", "10000"},
        { "b", "01000"},
        { "c", "00100"},
        { "d", "00010"},
        { "e", "00001"},
        { "f", "10100"},
        { "g", "01010"},
        { "h", "00101"},
        { "i", "10110"},
        { "j", "01011"},
        { "k", "10001"},
        { "l", "11100"},
        { "m", "01110"},
        { "n", "00111"},
        { "o", "10111"},
        { "p", "11111"},
        { "q", "11011"},
        { "r", "11001"},
        { "s", "11000"},
        { "t", "01100"},
        { "u", "00110"},
        { "v", "00011"},
        { "w", "10101"},
        { "x", "11110"},
        { "y", "01111"},
        { "y/c", "11101"},
        { "k/g", "11010"},
        { "tr/loi", "01101"},
        { "gap", "10010"},
        { "nguoi nhan", "01001"},
    };

        public static string MaHoaThongDiep(string text)
        {
            // text = text.Replace(" ", "*");
            text = text.Trim();
            text = text.ToLower();
```

```
            string tu;
            int len = arrCumTu.Length;
            string[] arrt = text.Split(' ');
            string textTemp = "";
            for (int i = 0; i < arrt.Length; i++)
            {
                if (arrt[i] == "ong")
                {
                    arrt[i] = dicMaHoa["ong"];
                }
                if (i > 0) textTemp += " ";
                textTemp += arrt[i];

            }

            for (int i = 0; i < len; i++)
            {
                tu = arrCumTu[i];
                textTemp = textTemp.Replace(tu, dicMaHoa[tu]);
            }

            foreach (char c in textTemp)
            {
                if (dicMaHoa.ContainsKey(c.ToString()))
                {
                    textTemp = textTemp.Replace(c.ToString(),
dicMaHoa[c.ToString()] + " ");
                }
            }
            textTemp = textTemp.Trim();
            return textTemp = textTemp.Replace("  ", " ");

        }
```

Hàm mã hóa và giải mã thông điệp

```
private static byte[] _salt =
Encoding.ASCII.GetBytes("jasdh7834y8hfeur73rsharks214");

        /// <summary>
        /// Encrypt the given string using AES.  The string can be decrypted
using
        /// DecryptStringAES().  The sharedSecret parameters must match.
        /// </summary>
        /// <param name="plainText">The text to encrypt.</param>
        /// <param name="sharedSecret">A password used to generate a key for
encryption.</param>
        public static string EncryptStringAES(string plainText, string
sharedSecret)
        {
            if (string.IsNullOrEmpty(plainText))
                throw new ArgumentNullException("plainText");
            if (string.IsNullOrEmpty(sharedSecret))
                throw new ArgumentNullException("sharedSecret");
```

```
            string outStr = null;                       // Encrypted string to
return
            RijndaelManaged aesAlg = null;              // RijndaelManaged
object used to encrypt the data.

            try
            {
                // generate the key from the shared secret and the salt
                Rfc2898DeriveBytes key = new Rfc2898DeriveBytes(sharedSecret,
_salt);

                // Create a RijndaelManaged object
                aesAlg = new RijndaelManaged();
                aesAlg.Key = key.GetBytes(aesAlg.KeySize / 8);

                // Create a decryptor to perform the stream transform.
                ICryptoTransform encryptor = aesAlg.CreateEncryptor(aesAlg.Key,
aesAlg.IV);

                // Create the streams used for encryption.
                using (MemoryStream msEncrypt = new MemoryStream())
                {
                    // prepend the IV
                    msEncrypt.Write(BitConverter.GetBytes(aesAlg.IV.Length), 0,
sizeof(int));
                    msEncrypt.Write(aesAlg.IV, 0, aesAlg.IV.Length);
                    using (CryptoStream csEncrypt = new CryptoStream(msEncrypt,
encryptor, CryptoStreamMode.Write))
                    {
                        using (StreamWriter swEncrypt = new
StreamWriter(csEncrypt))
                        {
                            //Write all data to the stream.
                            swEncrypt.Write(plainText);
                        }
                    }
                    outStr = Convert.ToBase64String(msEncrypt.ToArray());
                }
            }
            finally
            {
                // Clear the RijndaelManaged object.
                if (aesAlg != null)
                    aesAlg.Clear();
            }

            // Return the encrypted bytes from the memory stream.
            return outStr;
        }

        /// <summary>
        /// Decrypt the given string.  Assumes the string was encrypted using
        /// EncryptStringAES(), using an identical sharedSecret.
        /// </summary>
        /// <param name="cipherText">The text to decrypt.</param>
```

```
        /// <param name="sharedSecret">A password used to generate a key for
decryption.</param>
        public static string DecryptStringAES(string cipherText, string
sharedSecret)
        {
            if (string.IsNullOrEmpty(cipherText))
                throw new ArgumentNullException("cipherText");
            if (string.IsNullOrEmpty(sharedSecret))
                throw new ArgumentNullException("sharedSecret");

            // Declare the RijndaelManaged object
            // used to decrypt the data.
            RijndaelManaged aesAlg = null;

            // Declare the string used to hold
            // the decrypted text.
            string plaintext = null;

            try
            {
                // generate the key from the shared secret and the salt
                Rfc2898DeriveBytes key = new Rfc2898DeriveBytes(sharedSecret,
_salt);

                // Create the streams used for decryption.
                byte[] bytes = Convert.FromBase64String(cipherText);
                using (MemoryStream msDecrypt = new MemoryStream(bytes))
                {
                    // Create a RijndaelManaged object
                    // with the specified key and IV.
                    aesAlg = new RijndaelManaged();
                    aesAlg.Key = key.GetBytes(aesAlg.KeySize / 8);
                    // Get the initialization vector from the encrypted stream
                    aesAlg.IV = ReadByteArray(msDecrypt);
                    // Create a decrytor to perform the stream transform.
                    ICryptoTransform decryptor =
aesAlg.CreateDecryptor(aesAlg.Key, aesAlg.IV);
                    using (CryptoStream csDecrypt = new CryptoStream(msDecrypt,
decryptor, CryptoStreamMode.Read))
                    {
                        using (StreamReader srDecrypt = new
StreamReader(csDecrypt))

                            // Read the decrypted bytes from the decrypting
stream
                            // and place them in a string.
                            plaintext = srDecrypt.ReadToEnd();
                    }
                }
            }
            finally
            {
                // Clear the RijndaelManaged object.
                if (aesAlg != null)
                    aesAlg.Clear();
            }
```

```
            return plaintext;
        }
```

Hàm giấu thông điệp và trích thông điệp từ ảnh

```
  public enum State
        {
            Hiding,
            Filling_With_Zeros
        };

        public static Bitmap embedText(string text, Bitmap bmp)
        {
            // initially, we'll be hiding characters in the image
            State state = State.Hiding;

            // holds the index of the character that is being hidden
            int charIndex = 0;

            // holds the value of the character converted to integer
            int charValue = 0;

            // holds the index of the color element (R or G or B) that is
currently being processed
            long pixelElementIndex = 0;

            // holds the number of trailing zeros that have been added when
finishing the process
            int zeros = 0;
            int charcount = 0;
            // hold pixel elements
            int R = 0, G = 0, B = 0;
            //ghi thông điệp từ vị trí x
            int y= bmp.Height;
            int x = bmp.Width;
            // pass through the rows
            for (int i = 0; i < y; i++)
            {
                // pass through each row
                for (int j = 0; j < x; j++)
                {
                    // holds the pixel that is currently being processed
                    Color pixel = bmp.GetPixel(j, i);

                    // now, clear the least significant bit (LSB) from each
pixel element
                    R = pixel.R - pixel.R % 2;
                    G = pixel.G - pixel.G % 2;
                    B = pixel.B - pixel.B % 2;

                    // for each pixel, pass through its elements (RGB)
                    for (int n = 0; n < 3; n++)
                    {
                        // check if new 8 bits has been processed
                        if (pixelElementIndex % 8 == 0)
```

```
                        {
                            // check if the whole process has finished
                            // we can say that it's finished when 8 zeros are
added
                            if (state == State.Filling_With_Zeros && zeros ==
8)
                            {
                                // apply the last pixel on the image
                                // even if only a part of its elements have
been affected
                                if ((pixelElementIndex - 1) % 3 < 2)
                                {
                                    bmp.SetPixel(j, i, Color.FromArgb(R, G,
B));
                                }

                                // return the bitmap with the text hidden in
                                return bmp;
                            }

                            // check if all characters has been hidden
                            if (charIndex >= text.Length)
                            {
                                // start adding zeros to mark the end of the
text
                                state = State.Filling_With_Zeros;
                            }
                            else
                            {
                                // move to the next character and process again
                                charValue = text[charIndex++];
                            }
                        }

                        // check which pixel element has the turn to hide a bit
in its LSB
                        switch (pixelElementIndex % 3)
                        {
                            case 0:
                                {
                                    if (state == State.Hiding)
                                    {
                                        // the rightmost bit in the character
will be (charValue % 2)
                                        // to put this value instead of the LSB
of the pixel element
                                        // just add it to it
                                        // recall that the LSB of the pixel
element had been cleared
                                        // before this operation
                                        R += charValue % 2;

                                        // removes the added rightmost bit of
the character
                                        // such that next time we can reach the
next one
```

```
                                    charValue /= 2;
                                    charcount++;
                                }
                            } break;
                        case 1:
                            {
                                if (state == State.Hiding)
                                {
                                    G += charValue % 2;

                                    charValue /= 2;
                                    charcount++;
                                }
                            } break;
                        case 2:
                            {
                                if (state == State.Hiding)
                                {
                                    B += charValue % 2;

                                    charValue /= 2;
                                    charcount++;
                                }

                                bmp.SetPixel(j, i, Color.FromArgb(R, G,
B));
                            } break;
                    }

                    pixelElementIndex++;

                    if (state == State.Filling_With_Zeros)
                    {
                        // increment the value of zeros until it is 8
                        zeros++;
                    }
                }
            }
        }

        return bmp;
    }

    public static string extractText(Bitmap bmp)
    {
        int colorUnitIndex = 0;
        int charValue = 0;

        // holds the text that will be extracted from the image
        string extractedText = String.Empty;
        //ghi thông điệp từ vị trí y
        int y = bmp.Height;
        int x = bmp.Width;
        // pass through the rows
        for (int i = 0; i < y; i++)
        {
```

```
                // pass through each row
                for (int j = 0; j <x; j++)
                {
                    Color pixel = bmp.GetPixel(j, i);

                    // for each pixel, pass through its elements (RGB)
                    for (int n = 0; n < 3; n++)
                    {
                        switch (colorUnitIndex % 3)
                        {
                            case 0:
                                {
                                    // get the LSB from the pixel element (will
be pixel.R % 2)
                                    // then add one bit to the right of the
current character
                                    // this can be done by (charValue =
charValue * 2)
                                    // replace the added bit (which value is by
default 0) with
                                    // the LSB of the pixel element, simply by
addition
                                    charValue = charValue * 2 + pixel.R % 2;
                                } break;
                            case 1:
                                {
                                    charValue = charValue * 2 + pixel.G % 2;
                                } break;
                            case 2:
                                {
                                    charValue = charValue * 2 + pixel.B % 2;
                                } break;
                        }

                        colorUnitIndex++;

                        // if 8 bits has been added, then add the current
character to the result text
                        if (colorUnitIndex % 8 == 0)
                        {
                            // reverse? of course, since each time the process
happens on the right (for simplicity)
                            charValue = reverseBits(charValue);

                            // can only be 0 if it is the stop character (the 8
zeros)
                            if (charValue == 0)
                            {
                                return extractedText;
                            }

                            // convert the character value from int to char
                            char c = (char)charValue;

                            // add the current character to the result text
                            extractedText += c.ToString();
```

```
                    }
                }
            }
        }

        return extractedText;
    }

    public static int reverseBits(int n)
    {
        int result = 0;

        for (int i = 0; i < 8; i++)
        {
            result = result * 2 + n % 2;

            n /= 2;
        }

        return result;
    }
```

Hàm đánh dấu watermark vào ảnh

```
//đong dau thuy van
    private void AddTextToImage(string text)
    {
        if (bmp != null)
        {
            // ghi text từ 0 đến vị trí y
            int y = bmp.Height / 3;

            int x = bmp.Width / 3;
            Rectangle r = new Rectangle(x, y, bmp.Width, bmp.Height);
            StringFormat strFormat = new StringFormat();

            strFormat.Alignment = StringAlignment.Center;
            strFormat.LineAlignment = StringAlignment.Center;

            Graphics g = Graphics.FromImage(bmp);

            g.DrawString(text, new Font("Tahoma", 20), Brushes.Red, r,
strFormat);
        }
    }
```

PHỤ LỤC 2. MỘT SỐ KẾT QUẢ THỬ NGHIỆM

(trích biên bản thử nghiệm tại đơn vị công tác)

A. Kết quả thử nghiệm lần 1

Nội dung thử nghiệm: ***Thử nghiệm tần số và liên lạc có che khuất của thiết bị***

1. Các chỉ tiêu đặt ra của đề tài cần thử nghiệm lần 1:

- Dải tần số làm việc: 900MHz hoặc 2.4GHz
- Số kênh làm việc: <= 8 kênh
- Công suất máy phát: <=60mW
- Phạm vi liên lạc có che khuất: 30 - 100m
- Nguồn cung cấp: 3 - 12VDC
- Dòng tiêu thụ khi phát: <50mA
- Dòng tiêu thụ khi thu: <60mA

2. Kết quả thử nghiệm:

2.1 Các thiết bị sử dụng trong quá trình thử nghiệm:

- Máy phân tích phổ Rohde & Schwarz FS315 Spectrum Analyzer 9kHz … 3GHz
- Đồng hồ đo vạn năng FLUKE 8842A
- Đồng hồ đo HIOKI 3257-50
- Nguồn chuẩn HAMEG 7044
- Nguồn lập trình Agilent 6634B
- Máy hiện sóng HITACHI V-1565 100MHz

2.2. Điều kiện thử nghiệm

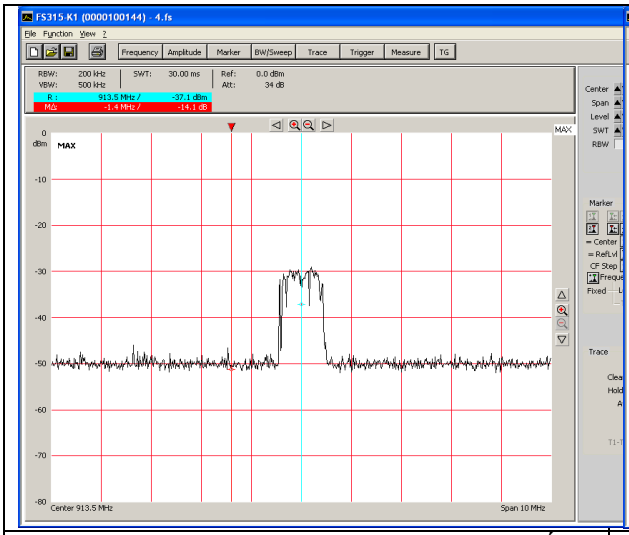
- Nguồn cung cấp cho mô-đun thu/phát: pin 9VDC (loại 6AM-6PI, Alkaline)
- Nguồn cung cấp cho mô-đun phát/thu: nguồn 9VDC, 1.1A
- Thử thu/phát một bản tin dung lượng 5kb, môi trường có che khuất, xuyên qua 4 buồng làm việc tại tầng 5 nhà đa năng, liên lạc giữa tầng 5 và tầng 4, từ buồng làm việc tầng 5 ra đến cổng ra vào 80 Trần Quốc Hoàn, khoảng cách từ 10m đến 110m.

2.3. Dòng tiêu thụ

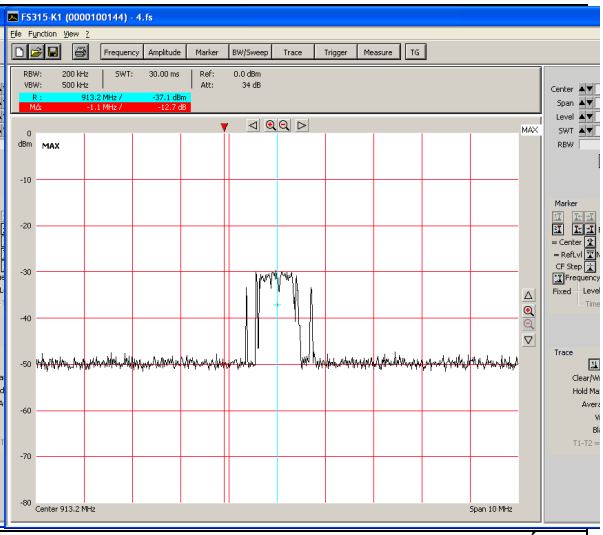
- Dòng tiêu thụ khi phát: 75mA
- Dòng tiêu thụ khi thu: 65mA

2.4. Kết quả: Thử nghiệm thiết bị trong phạm vi liên lạc có che khuất

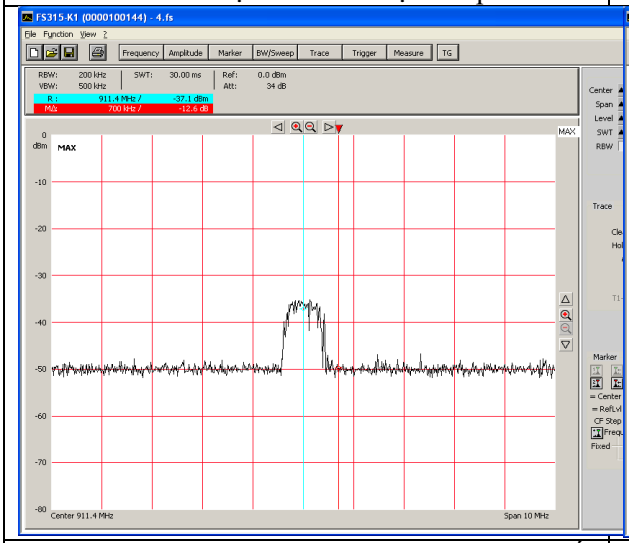
2.4.1. Thử nghiệm về khoảng cách liên lạc



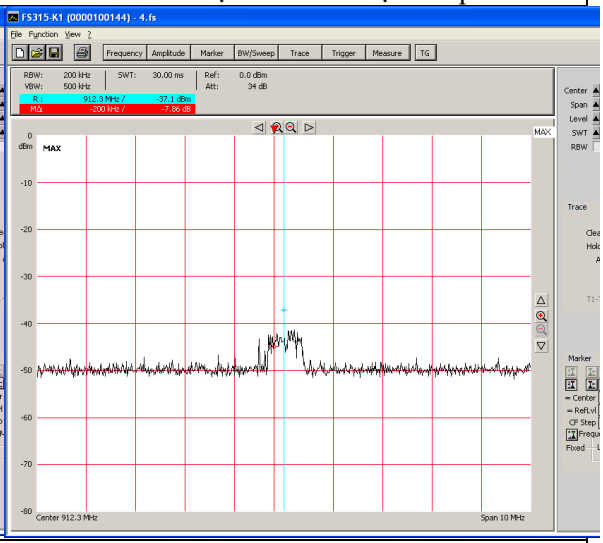
a. kh/cách liên lạc 10m: tín hiệu thu/phát tốt



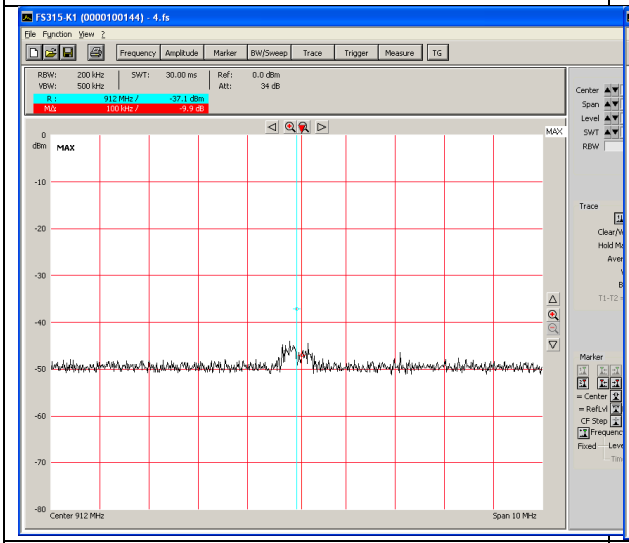
b. kh/cách liên lạc 30m: tín hiệu thu/phát tốt



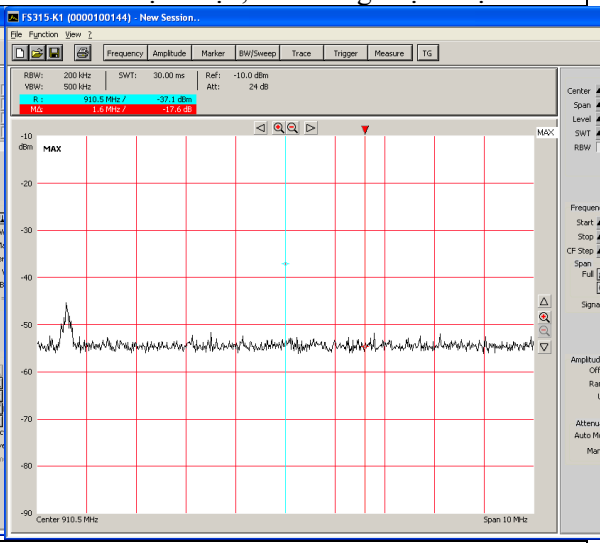
c. khoảng cách liên lạc 50m: tín hiệu thu/phát tốt



d. khoảng cách liên lạc 70m: tín hiệu thu/phát lúc nhận được, lúc không nhận được

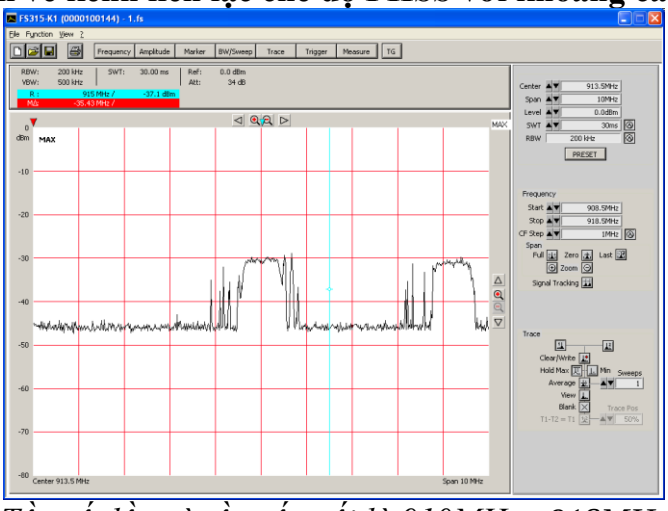


e. kh/cách liên lạc 90m: tín hiệu thu/phát kém



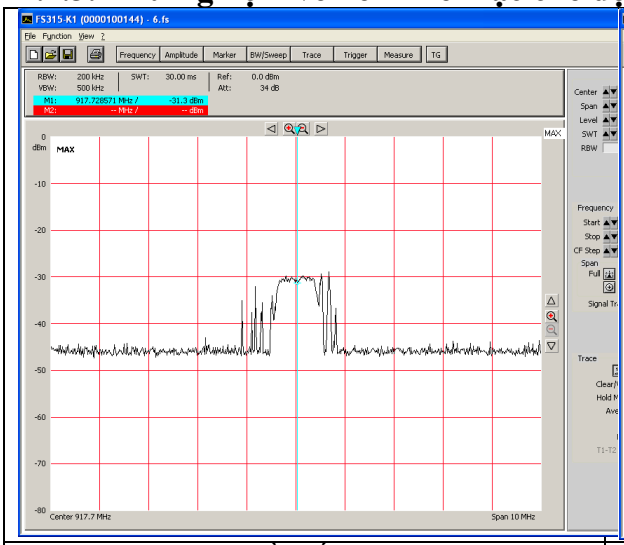
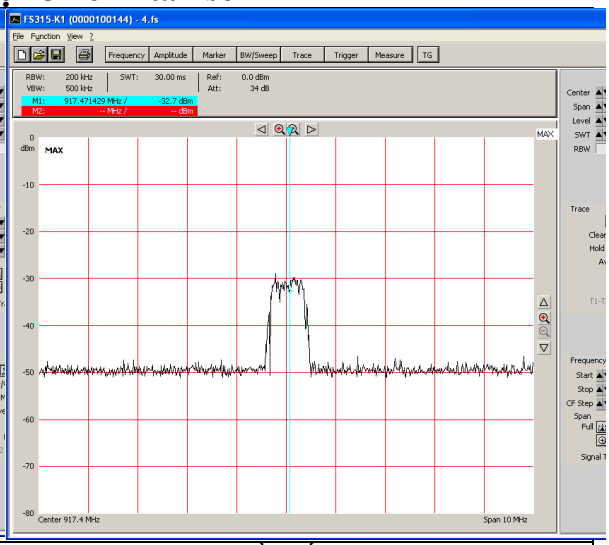
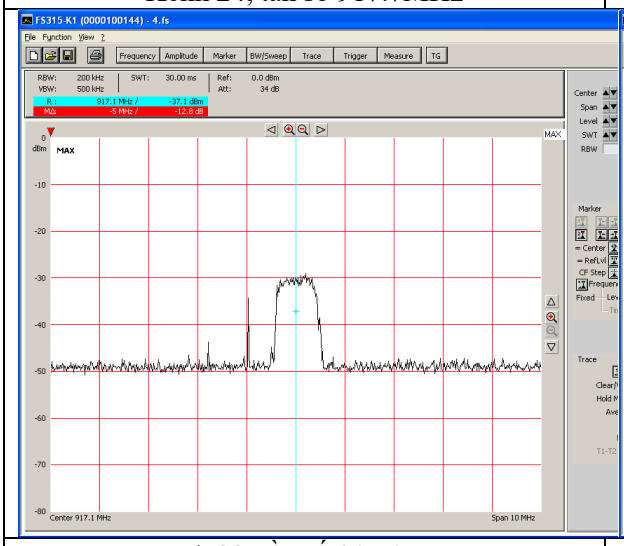
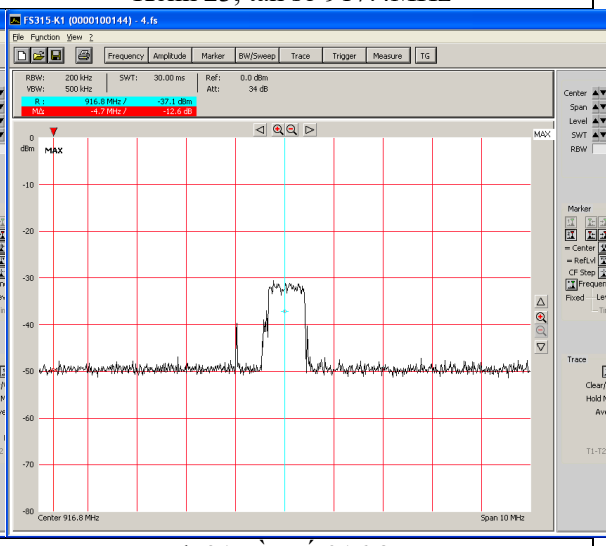
g. kh/cách liên lạc 110m: không liên lạc được

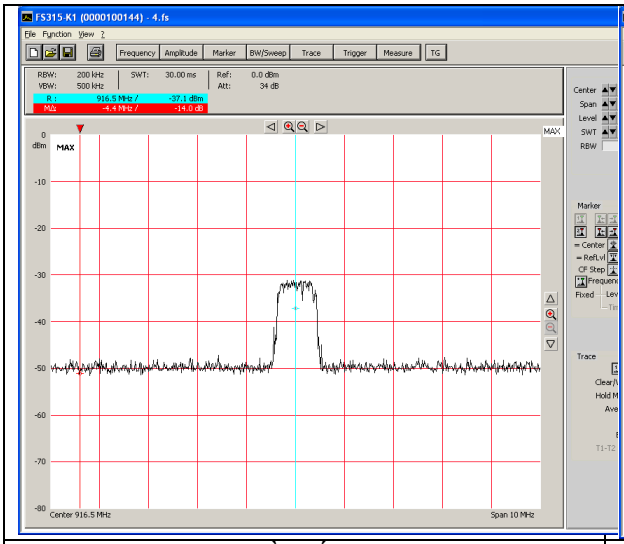
2.4.2. Thử nghiệm về kênh liên lạc chế độ FHSS với khoảng cách liên lạc 50m



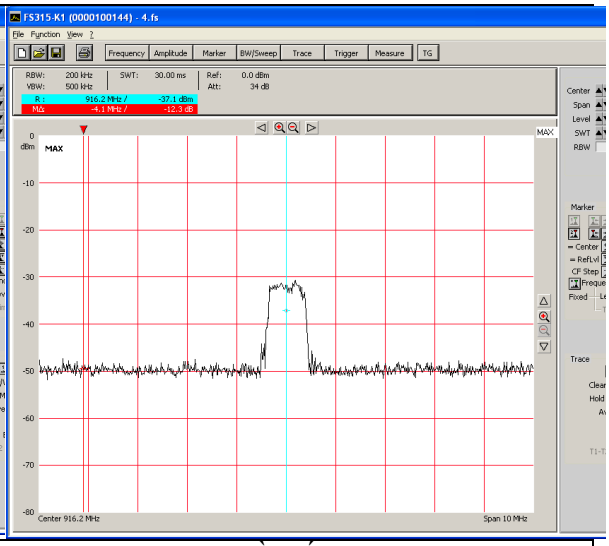
Tần số đầu và tần số cuối là 910MHz - 918MHz

2.4.3. Thử nghiệm về kênh liên lạc chế độ 25 kênh tần số

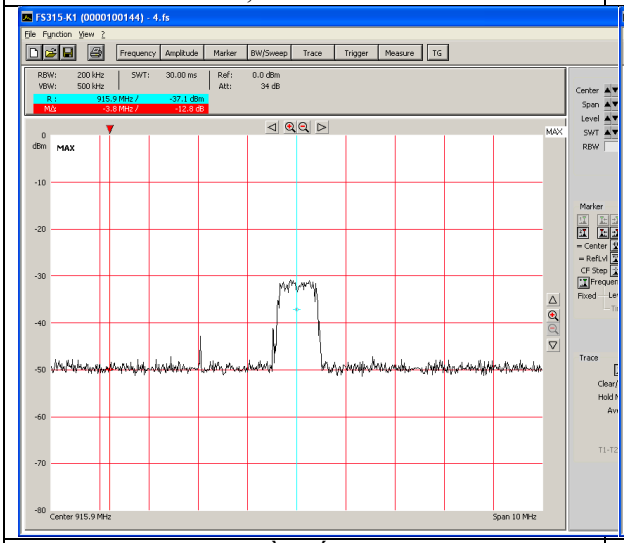
	
Kênh 24, tần số 917.7MHz	Kênh 23, tần số 917.4MHz
	
Kênh 22, tần số 917.1MHz	Kênh 21, tần số 916.8MHz



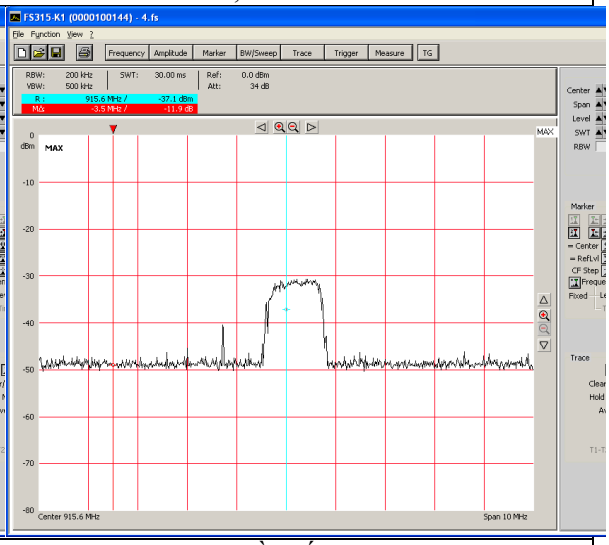
Kênh 20, tần số 916.5MHz



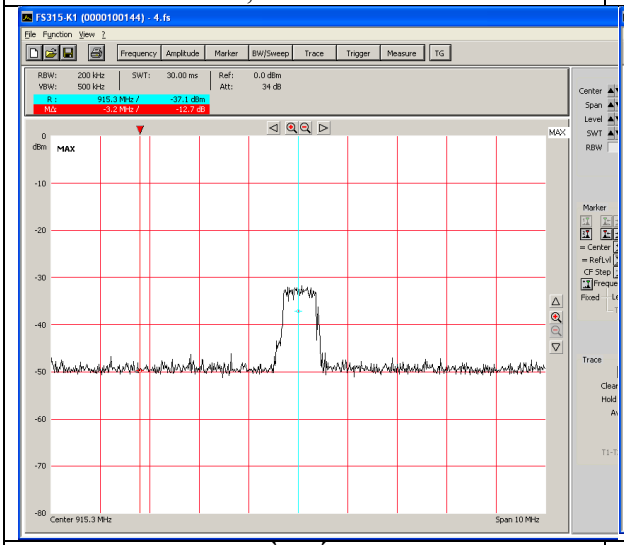
Kênh 19, tần số 916.2MHz



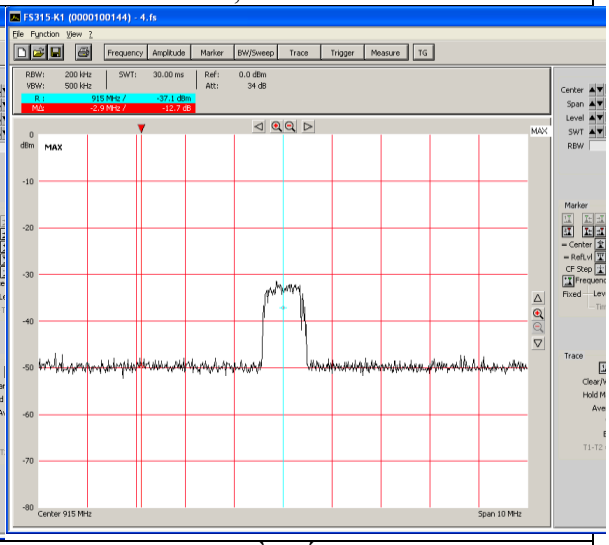
Kênh 18, tần số 915.9MHz



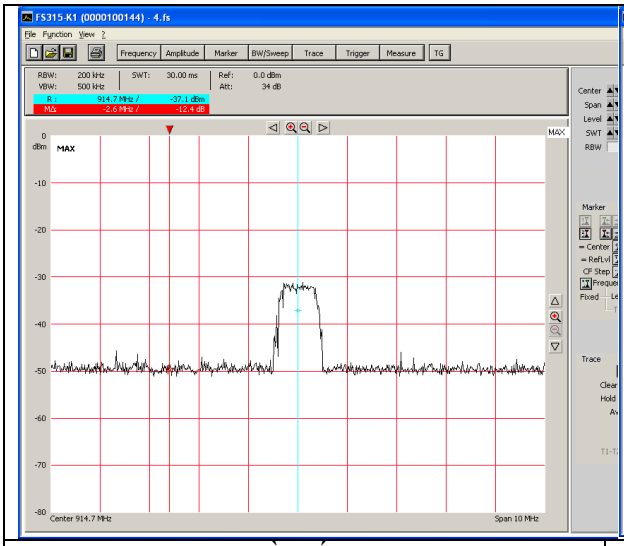
Kênh 17, tần số 915.6MHz



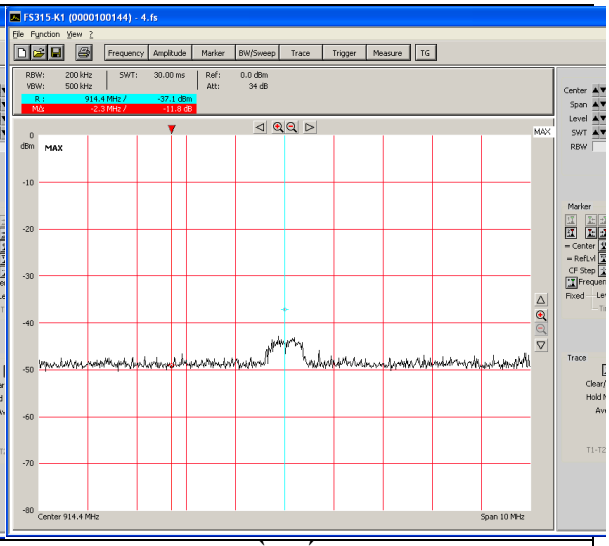
Kênh 16, tần số 915.3MHz



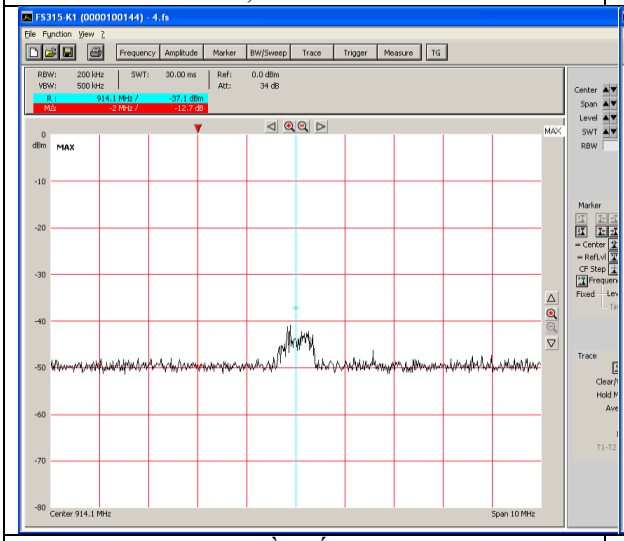
Kênh 15, tần số 915.0MHz



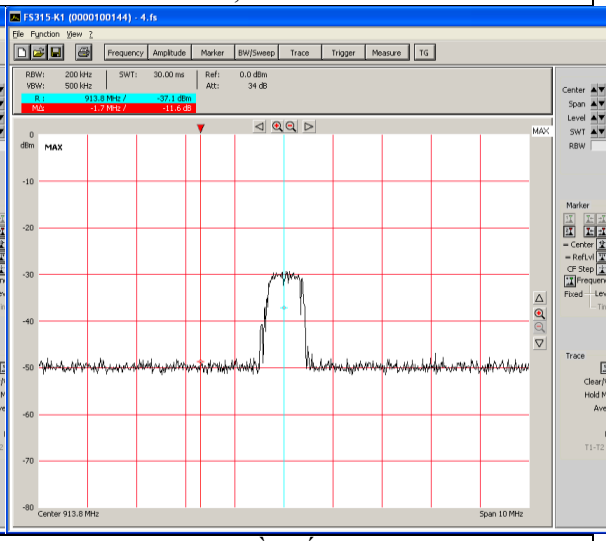
Kênh 14, tần số 914.7MHz



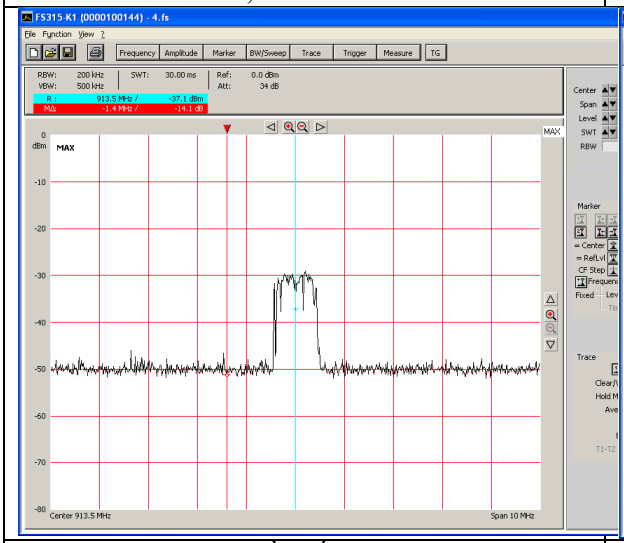
Kênh 13, tần số 914.4MHz



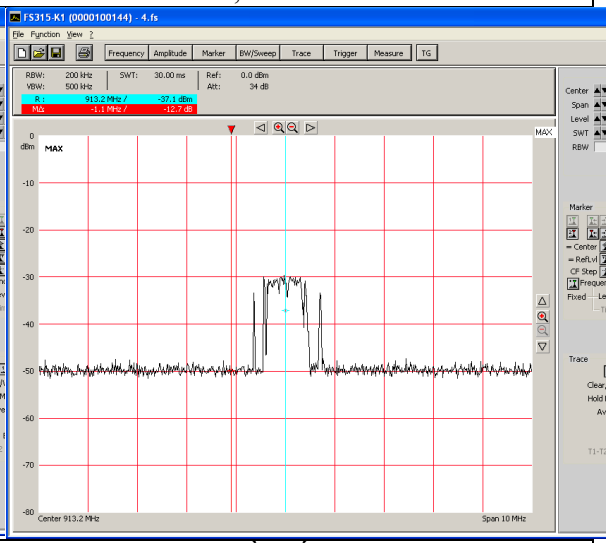
Kênh 12, tần số 914.1MHz



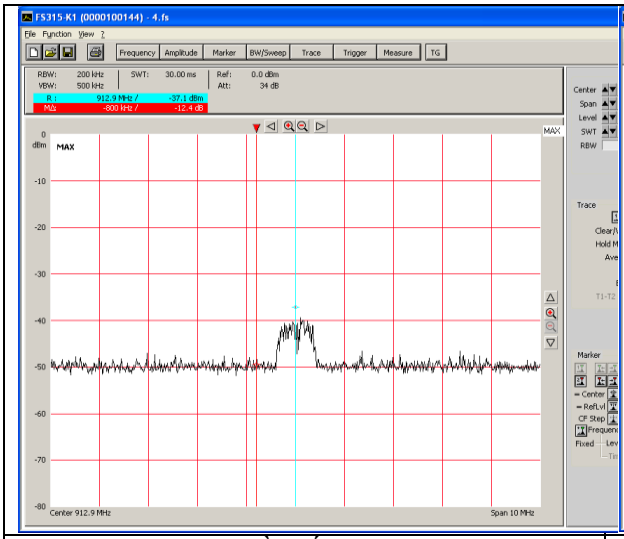
Kênh 11, tần số 913.8MHz



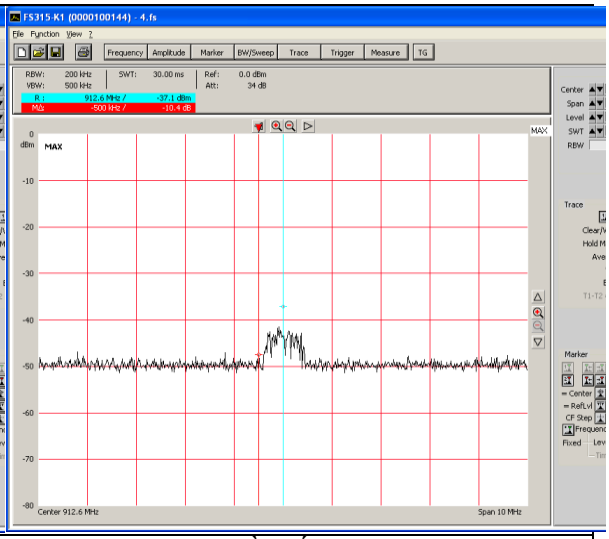
Kênh 10, tần số 913.5MHz



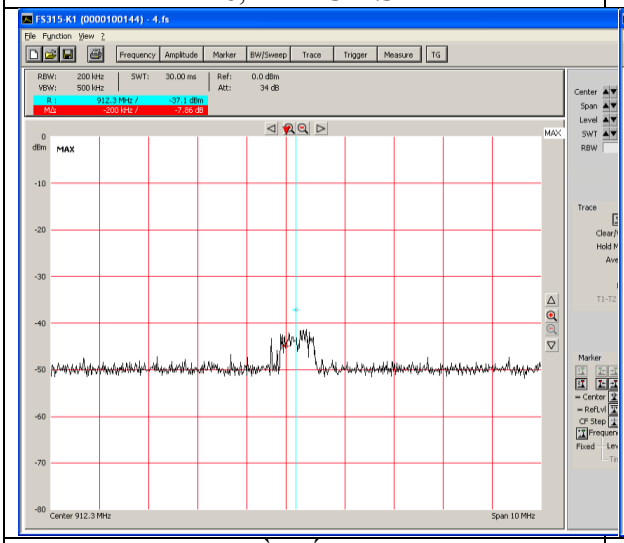
Kênh 9, tần số 913.2MHz



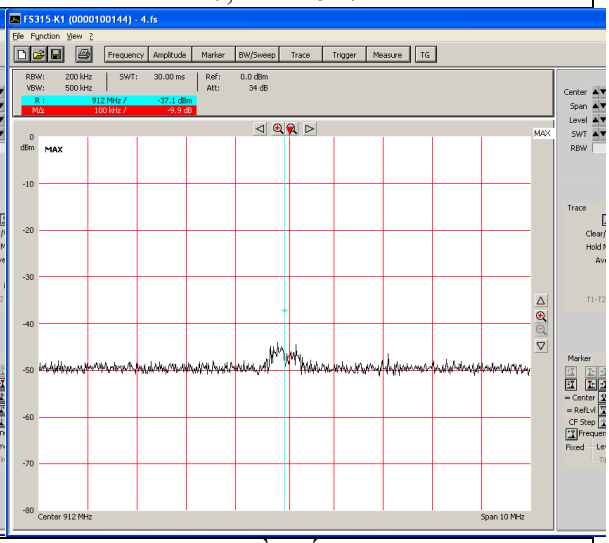
Kênh 8, tần số 912.9MHz



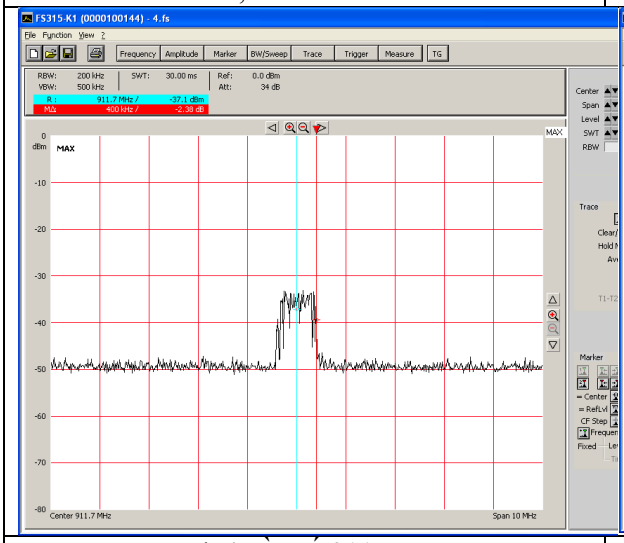
Kênh 7, tần số 917.4MHz



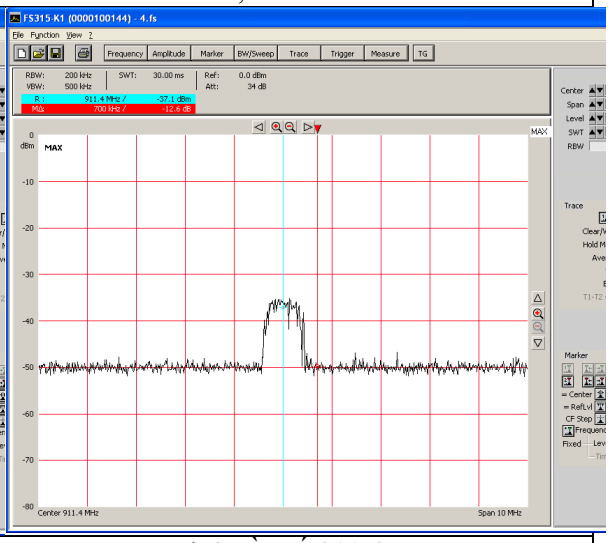
Kênh 6, tần số 912.3MHz



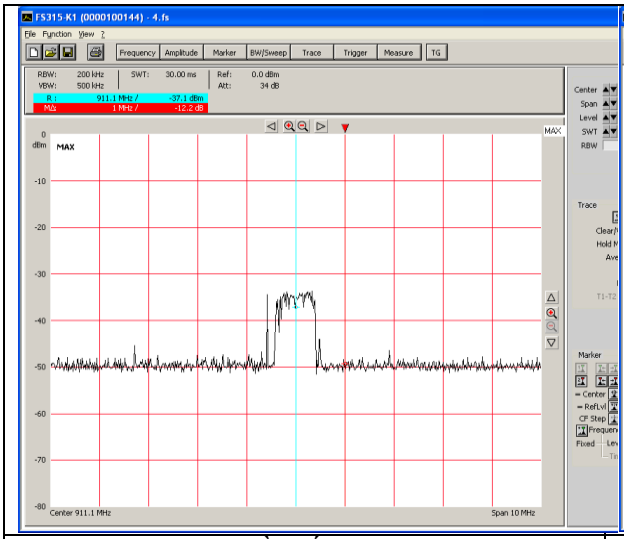
Kênh 5, tần số 912MHz



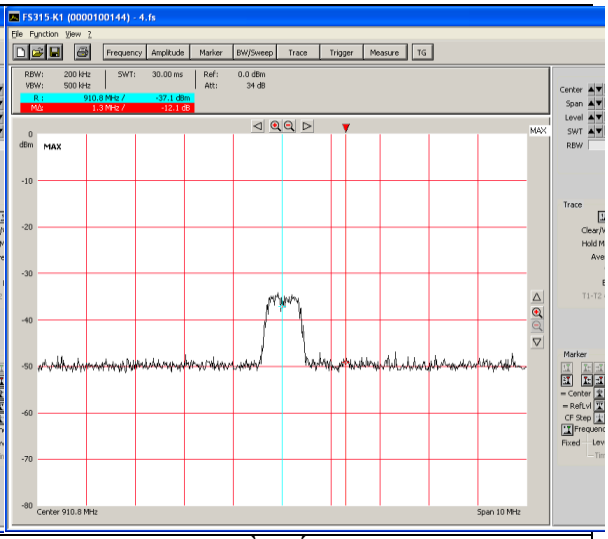
Kênh 4, tần số 911.7MHz



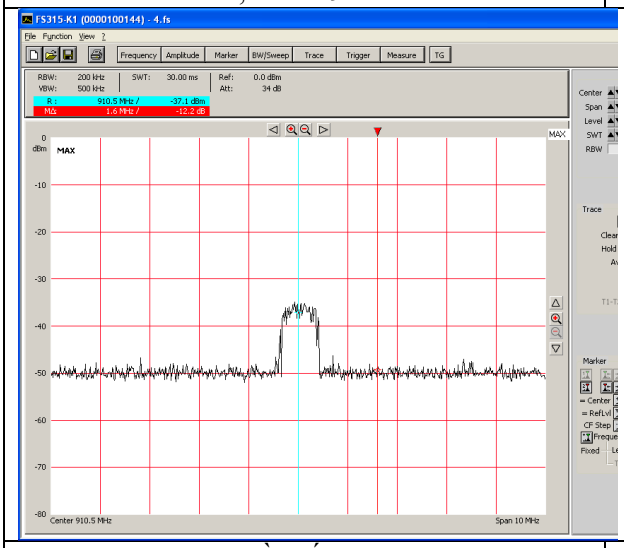
Kênh 3, tần số 911.4MHz



Kênh 2, tần số 911.1MHz



Kênh 1, tần số 910.8MHz



Kênh 0, tần số 910.5MHz

3. Đánh giá:

Chỉ tiêu yêu cầu	Kết quả kiểm tra, thử nghiệm		Đánh giá
- Dải tần số làm việc: 900MHz hoặc 2.4GHz	910MHz - 917.7MHz		Đạt
- Số kênh làm việc: <= 8 kênh	FHSS (nhảy tần 7 tần số)	25 kênh tần số đơn	Đạt
- Công suất máy phát: <=60mW	4mW		Đạt
- Phạm vi liên lạc có che khuất: 30 - 100m	20 - 70m		Đạt
- Nguồn cung cấp: 3 - 12VDC	9VDC, 1.1A		Đạt
- Dòng tiêu thụ khi phát: <50mA	75mA		Vượt 25mA
- Dòng tiêu thụ khi thu: <60mA	65mA		Vượt 5mA

- Nhận xét:
  - Các chỉ tiêu đã kiểm tra đạt yêu cầu cơ bản
  - Đề nghị tiếp tục hoàn thiện thiết bị

B. Kết quả thử nghiệm lần 2

Nội dung thử nghiệm: ***Thử nghiệm liên lạc của thiết bị cố định không che khuất***

1. Các chỉ tiêu đặt ra của đề tài cần thử nghiệm lần 2:

- Dải tần số làm việc: 900MHz
- Công suất máy phát: <=60mW
- Phạm vi liên lạc không có che khuất: 300 - 500m
- Mã hóa dữ liệu: 128bit AES
- Tốc độ dữ liệu RF: 9.6 - 34.8Kbps

2. Kết quả thử nghiệm:

2.1. Thiết bị sử dụng trong quá trình thử nghiệm:

- Máy phân tích phổ Rohde & Schwarz FS315 Spectrum Analyzer 9kHz … 3GHz

2.2. Điều kiện thử nghiệm

- Nguồn cung cấp cho mô-đun thu/phát: pin 9VDC (loại 6AM-6PI, Alkaline)
- Nguồn cung cấp cho mô-đun phát/thu: nguồn 9VDC, 1.1A
- Thử thu/phát một bản tin text dung lượng 5kb và bản tin hình ảnh dung lượng 28kb, 71kb, môi trường không có che khuất, tại đoạn đường Nguyễn Văn Huyên, trước cổng Tổng cục V, khoảng cách từ 100m đến 500m.
- Sử dụng bộ đàm trực tiếp liên lạc để kiểm tra nội dung bản tin thu/phát.
- Chế độ làm việc: làm việc ngay và hẹn giờ.

2.3. Kết quả: Thử nghiệm thiết bị trong phạm vi liên lạc không có che khuất

TT	Khoảng cách liên lạc	Số lần thử	Kết quả
1	100m	20	Tín hiệu thu/phát tốt, trích dấu watermark và trích tin đúng 100%
2	200m	20	Tín hiệu thu/phát tốt, trích dấu watermark và trích tin đúng 100%
3	300m	20	Tín hiệu thu/phát tốt, trích dấu watermark và trích tin đúng 100%
4	400m	50	Tín hiệu thu/phát lúc nhận được, lúc không nhận được, đạt tỷ lệ nhận tin 90-95%
5	500m	10	Không liên lạc được, tỷ lệ nhận tin 0%
6	600m	10	Không liên lạc được, tỷ lệ nhận tin 0%

3. Đánh giá:

Chỉ tiêu yêu cầu	Kết quả kiểm tra, thử nghiệm	Đánh giá
- Dải tần số làm việc: 900MHz hoặc 2.4GHz	910MHz - 917.7MHz	Đạt
- Công suất máy phát: <=60mW	4mW	Đạt
- Phạm vi liên lạc không có che khuất: 300 - 500m	100 - 400m	Đạt
- Nguồn cung cấp: 3 - 12VDC	9VDC, 1.1A	Đạt
- Mã hóa dữ liệu: 128bit AES	128bit AES	Đạt
- Tốc độ dữ liệu RF: 9,6 - 34,8Kbps	9600bps và 34800bps	Đạt

- Nhận xét:

- Các chỉ tiêu đã kiểm tra đạt yêu cầu
- Kiểm tra thử nghiệm lần 2 ở môi trường liên lạc không có che khuất đạt kết quả tốt

C. Kết quả thử nghiệm lần 3

Nội dung thử nghiệm: ***Thử nghiệm liên lạc của thiết bị trong khi di chuyển***

1. Các yêu cầu và điều kiện nguồn cung cấp đặt ra của đề tài cần thử nghiệm:

1.1. Yêu cầu liên lạc

- Liên lạc bản tin theo tầm nhìn thẳng - cự li làm việc 80m - 120m, khi cố định
- Liên lạc bản tin trong khi tốc độ di chuyển của xe ô tô là 20km/h; 30km/h; 35km/h; 40km/h; 2 xe ô tô di chuyển ngược chiều; 2 xe ô tô di chuyển cùng chiều; khoảng cách giữa 2 xe ô tô 20m - 50m

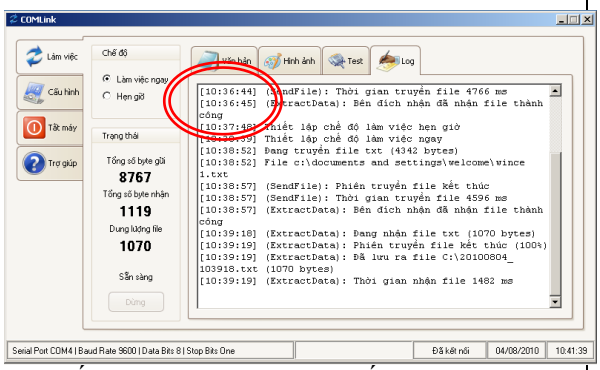
1.2. Điều kiện nguồn cung cấp trong khi thử nghiệm

- Nguồn cung cấp cho mô-đun thu/phát: pin 9VDC (loại 6AM-6PI, Alkaline)
- Nguồn cung cấp cho mô-đun phát/thu: nguồn 9VDC, 1.1A
- Liên lạc bằng bộ đàm cầm tay GP338 Motorola

2. Kết quả thử nghiệm:

2.1. Kết quả thử nghiệm thiết bị trong phạm vi liên lạc theo tầm nhìn thẳng, cố định

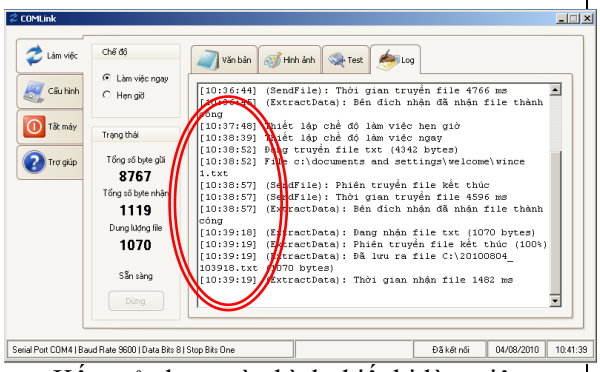
a. Khoảng cách liên lạc 80m: thiết bị liên lạc tốt



Kết quả chụp màn hình thiết bị làm việc

Ảnh chụp ước lượng khoảng cách giữa 2 xe ô tô

b. Khoảng cách liên lạc 120m: thiết bị liên lạc tốt

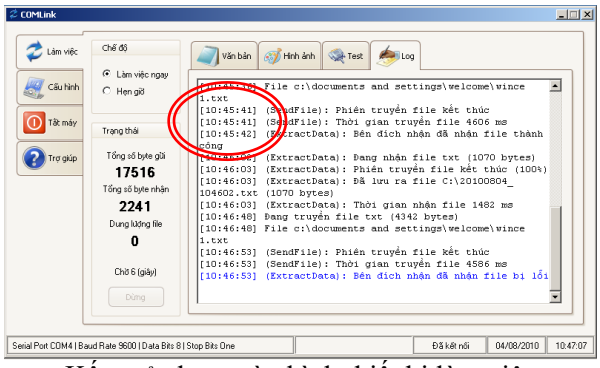


Kết quả chụp màn hình thiết bị làm việc

Ảnh chụp ước lượng khoảng cách giữa 2 xe ô tô

2.2. Kết quả thử nghiệm thiết bị liên lạc bản tin theo tốc độ và hướng di chuyển

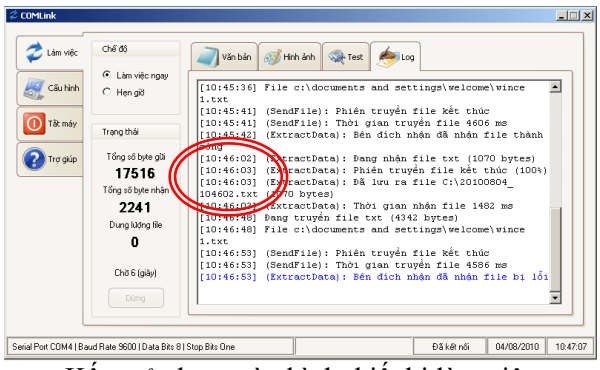
a. Tốc độ di chuyển của 2 xe ô tô 20km/h; 2 xe ô tô chạy cùng chiều: thiết bị liên lạc tốt



Kết quả chụp màn hình thiết bị làm việc

Ảnh chụp màn hình tốc độ xe ô tô

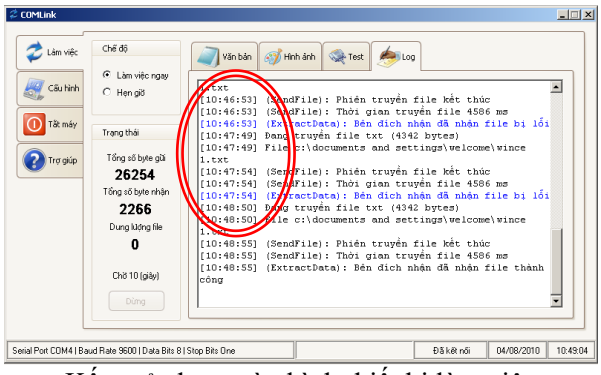
b. Tốc độ di chuyển của 2 xe ô tô 30km/h; 2 xe ô tô chạy cùng chiều: thiết bị liên lạc tốt



Kết quả chụp màn hình thiết bị làm việc

Ảnh chụp màn hình tốc độ xe ô tô

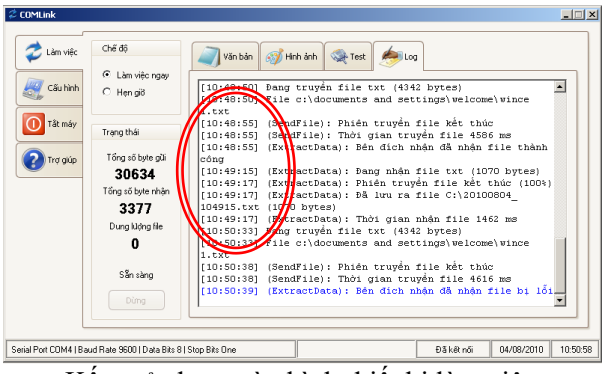
c. Tốc độ di chuyển của 2 xe ô tô 40km/h; 2 xe ô tô chạy cùng chiều: bản tin liên lạc bị lỗi nhiều lần



Kết quả chụp màn hình thiết bị làm việc

Ảnh chụp màn hình tốc độ xe ô tô

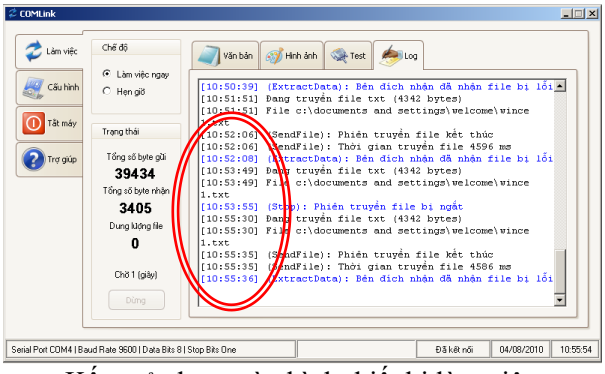
d. Tốc độ di chuyển của 2 xe ô tô 20km/h; 2 xe ô tô chạy ngược chiều: thiết bị liên lạc tốt



Kết quả chụp màn hình thiết bị làm việc

Ảnh chụp màn hình tốc độ xe ô tô

e. Tốc độ di chuyển của 2 xe ô tô 35km/h; 2 xe ô tô chạy ngược chiều: bản tin liên lạc bị lỗi nhiều lần



Kết quả chụp màn hình thiết bị làm việc

Ảnh chụp màn hình tốc độ xe ô tô

Ảnh chụp 2 xe chạy ngược chiều cách nhau 25m

Ảnh chụp 2 xe chạy ngược chiều cách nhau 150m

3. Đánh giá:

TT	Yêu cầu	Số lần thử	Kết quả kiểm tra, thử nghiệm	Đánh giá
1	Trạng thái hoạt động 2 thiết bị: - Khoảng cách: 80 m - Vị trí: cố định	20	Tín hiệu thu/phát tốt, trích dấu watermark và trích tin đúng 100%	Đạt
2	Trạng thái hoạt động: - Khoảng cách: 120 m - Vị trí: cố định	20	Tín hiệu thu/phát tốt, trích dấu watermark và trích tin đúng 100%	Đạt
3	Trạng thái hoạt động 2 thiết bị: - Khoảng cách: 20-30 m - Vị trí: di chuyển - Tốc độ: 20 km/h - Hướng di chuyển: cùng chiều	10	Tín hiệu thu/phát tốt, trích dấu watermark và trích tin đúng 100%	Đạt
4	Trạng thái hoạt động 2 thiết bị: - Khoảng cách: 30-40 m - Vị trí: di chuyển - Tốc độ: 30 km/h - Hướng di chuyển: cùng chiều	10	Tín hiệu thu/phát tốt, trích dấu watermark và trích tin đúng 100%	Đạt
5	Trạng thái hoạt động 2 thiết bị: - Khoảng cách: 40-50 m - Vị trí: di chuyển - Tốc độ: 50 km/h - Hướng di chuyển: cùng chiều	10	Tín hiệu thu/phát lúc nhận được, lúc không nhận được, đạt tỷ lệ nhận tin 90-95%	Không đạt
6	Trạng thái hoạt động 2 thiết bị: - Khoảng cách: 10-25 m - Vị trí: di chuyển - Tốc độ: 20 km/h - Hướng di chuyển: ngược chiều	10	Tín hiệu thu/phát tốt, trích dấu watermark và trích tin đúng 100%	Đạt
7	Trạng thái hoạt động 2 thiết bị: - Khoảng cách: 10-25 m - Vị trí: di chuyển - Tốc độ: 35 km/h - Hướng di chuyển: ngược chiều	10	Tín hiệu thu/phát lúc nhận được, lúc không nhận được, đạt tỷ lệ nhận tin 90-95%	Không đạt