Nhóm 2 Bao Cao BTL Atbmtt 20221 IT6001001

Cơ bản công nghệ thông tin (Trường Đại học Công nghiệp Hà Nội)

TRƯỜNG ĐẠI HỌC CÔNG NGHIỆP HÀ NỘI
KHOA CÔNG NGHỆ THÔNG TIN

BÀI TẬP LỚN
MÔN: AN TOÀN VÀ BẢO MẬT THÔNG TIN

Đề tài: *Giấu tin trong ảnh sử dụng kết hợp mã hóa AES và kỹ thuật giấu tin trên sai phân*

Giảng viên hướng dẫn: **ThS. Trần Phương Nhung**

Nhóm 2: **Nguyễn Anh Đức – 2019600984**

Nguyễn Anh Đức - 2019602712

Lê Dũng - 2019601609

Nguyễn Tiến Dũng - 2019600428

Hà Nội, 2023

LỜI CẢM ƠN

Em xin chân thành cảm ơn các thầy, các cô khoa Công nghệ thông tin - trường Đại học Công Nghiệp Hà Nội đã tận tình dạy dỗ, truyền đạt cho chúng em nhiều kiến thức bổ ích và quý báu trong suốt những năm học đã qua.

Em xin tỏ lòng biết ơn sâu sắc đến cô Trần Phương Nhung, người đã trực tiếp hướng dẫn, giúp đỡ và truyền đạt cho em những kiến thức và kinh nghiệm để đề tài này có thể thực hiện được và hoàn thành.

Em xin cảm ơn gia đình và bạn bè đã động viên và giúp đỡ em trong suốt thời gian em làm đề tài này.

Vì thời gian có hạn, trình độ hiểu biết của bản thân còn nhiều hạn chế. Cho nên trong bài tập lớn không tránh khỏi những thiếu sót, em rất mong nhận được sự đóng góp ý kiến của tất cả các thầy cô giáo cũng như các bạn bè để bài tập lớn của em được hoàn thiện hơn.

Em xin chân thành cảm ơn!

MỤC LỤC

LỜI CẢM ƠN 2

MỞ ĐẦU 4

CHƯƠNG 1: TỔNG QUAN VỀ GIẤU TIN TRONG ẢNH VÀ MÃ HÓA THÔNG TIN 5

1.1 Định nghĩa giấu thông tin 5

1.2 Mô hình giấu thông tin cơ bản 6

1.3 Môi trường giấu tin 8

1.4 Một số ứng dụng của kỹ thuật giấu tin 11

1.5 Cấu trúc ảnh bitmap 12

1.6 Tổng quan về mã hóa thông tin 14

1.7 Phương pháp mã hóa AES 17

CHƯƠNG 2: KỸ THUẬT GIẤU TIN TRONG ẢNH SỬ DỤNG KẾT HỢP MÃ HÓA AES VÀ GIẤU TIN 20

2.1 Giới thiệu kỹ thuật giấu tin trên sai phân 20

2.2 Quá trình giấu tin trong ảnh sử dụng kết hợp mã hóa AES và kỹ thuật giấu 20

2.3 Quá trình tách tin 24

CHƯƠNG 3: CÀI ĐẶT THỬ NGHIỆM 27

3.1 Môi trường cài đặt 27

3.2 Giao diện chương trình 27

3.3 Phân công công việc 39

3.4 Kết luận 39

Tài liệu tham khảo 41

Phụ lục 42

MỞ ĐẦU

Sự phát triển vượt bậc của công nghệ mạng dẫn đến vấn đề an toàn thông tin là rất quan trọng. Có nhiều phương pháp để trao đổi thông tin mật, trong đó phương pháp mã hóa thông tin được coi là xuất hiện sớm nhất, tuy nhiên phương pháp này làm cho người ta dễ phát hiện. Do đó với một phương pháp khác giấu tin trong dữ liệu đa phương tiện được coi là "vô hình" đối với người dùng. Trong một số trường hợp để đảm bảo an toàn cho thông tin được đem giấu người ta đã kết hợp cả hai phương pháp này. Trong đề tài này sẽ sử dụng phương pháp mã hóa AES (Advanced Encryption Standard) để mã hóa thông tin mật trước khi giấu vào trong ảnh bằng phương pháp giấu trên sai phân. Nôi dung báo cáo gồm 3 chương chính sau:

- Chương 1. Tổng quan về giấu tin trong ảnh và mã hóa thông tin. Giới thiệu về một số định nghĩa giấu thông tin, môi trường giấu tin, sơ lược về mô hình giấu tin cơ bản, cấu trúc ảnh bitmap. Giới thiệu tổng quan về mã hóa thông tin, phương pháp mã hóa AES.
- Chương 2. Giới thiệu kỹ thuật giấu tin trên sai phân. Thuật toán, sơ đồ thuật toán, ví dụ minh họa của quá trình giấu tin sử dụng kết hợp mã hóa AES với kỹ thuật giấu tin trên sai phân.
- Chương 3. Cài đặt và thử nghiệm. Đưa ra môi trường cài đặt, giới thiệu chương trình và chạy thử nghiệm trên một số ảnh.

CHƯƠNG 1: TỔNG QUAN VỀ GIẤU TIN TRONG ẢNH VÀ MÃ HÓA THÔNG TIN

1.1 Định nghĩa giấu thông tin

1.1.1 Định nghĩa

Giấu thông tin là kỹ thuật giấu (hoặc nhúng) một lượng thông tin số nào đó vào trong một đối tượng dữ liệu số khác ("giấu tin" nhiều khi không cần phải chỉ hành động giấu cụ thể mà chỉ mang ý nghĩa quy ước).

Định nghĩa trên mang tính tổng quát về giấu tin. Xét riêng trong kỹ thuật giấu tin mật (Steganography), những định nghĩa sau đây cụ thể hơn và được chia theo các hệ giấu tin mật. Từ đó, các hệ thống giấu tin mật có thể chia thành ba loại như:

1.1.1.1 Giấu tin thuần tuý (Pure Steganography)

Một bộ 4 σ(C, M, D, E), trong đó C là tập các phương tiện chứa thông tin cần giấu, M là tập thông điệp cần giấu với |C|≥|M|, E: C×M → C là một hàm nhúng thông điệp M vào phương tiện chứa C và D: C → M là hàm giải tin sao cho D(E(c, m)) = m với mọi m ∈ M, c ∈ C được gọi là một hệ pure Steganography.

1.1.1.2 Giấu tin dùng khoá bí mật (Secret key Steganography)

Một bộ năm σ(C, M, K, Dk, Ek), trong đó C là tập các phương tiện chứa thông tin cần giấu, M là tập thông điệp cần giấu với |C|≥|M|, K là một tập khoá bí mật, Ek: C×M×K → C là một hàm nhúng thông điệp M vào phương tiện chứa C sử dụng khoá K và Dk: C × K→ M là hàm giải tin sao cho Dk(Ek(c, m, k), k) = m với mọi m ∈ M, c ∈ C và k ∈ K được gọi là một hệ Secret key Stegangraphy.

1.1.1.3 Giấu tin dùng khoá công khai (Public Key Steganography)

Giống như là hệ mã mật khoá công khai, hệ giấu tin mật khoá công khai không sử dụng việc truyền khoá bí mật mà sử dụng hai khoá là khoá bí mật và khoá công khai. Khoá công khai được lưu trong cơ sở dữ liệu công cộng. Được sử dụng trong quá trình giấu tin. Còn khoá bí mật được sử dụng trong quá trình giải tin.

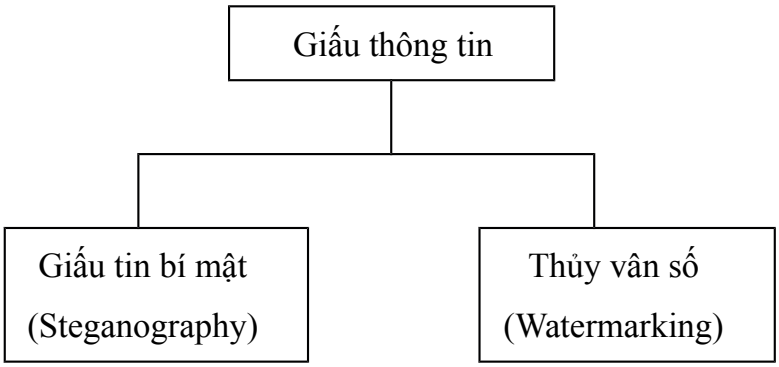
1.1.2 Mục đích của giấu tin

Giấu tin có hai mục đích:

- Bảo mật cho những dữ liệu được giấu.

- Bảo đảm an toàn (bảo vệ bản quyền) cho chính các đối tượng chứa dữ liệu giấu trong đó.

Có thể thấy hai mục đích này hoàn toàn trái ngược nhau và dần phát triển thành hai lĩnh vực với những yêu cầu và tính chất khác nhau.



Hình 1.1. Hai lĩnh vực chính của kỹ thuật giấu thông tin

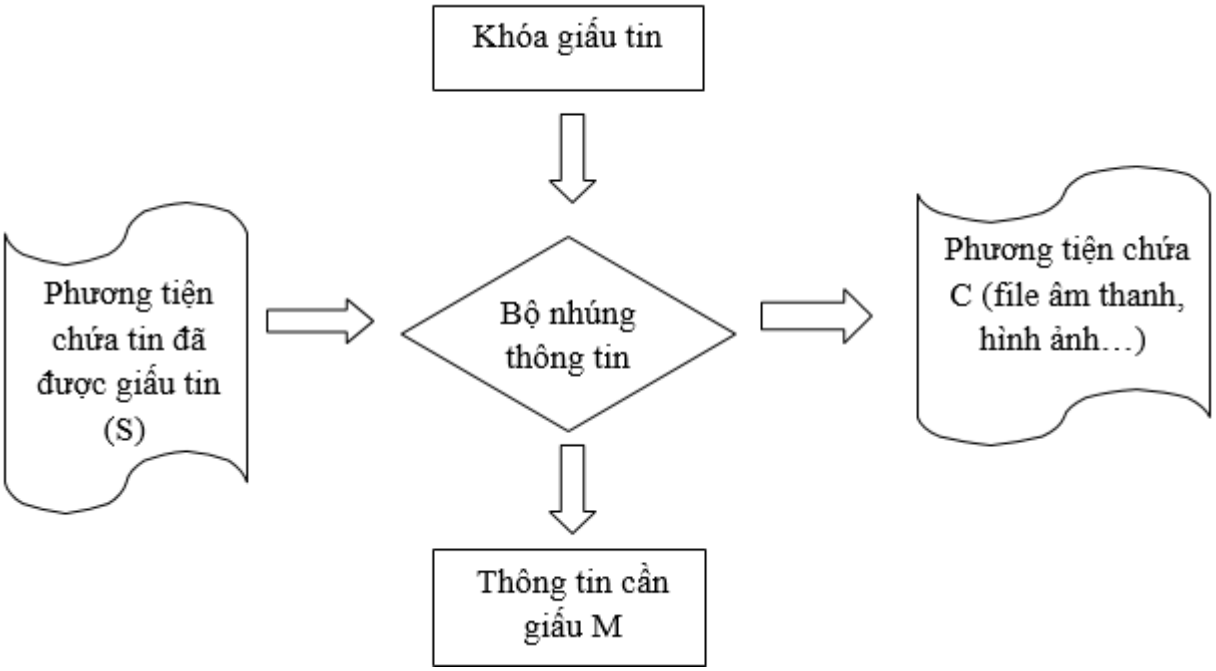
Kỹ thuật giấu thông tin bí mật (Steganography): với mục đích đảm bảo an toàn và bảo mật thông tin tập trung vào các kỹ thuật giấu tin để có thể giấu được nhiều thông tin nhất. Thông tin mật được giấu kỹ trong một đối tượng khác sao cho người khác không phát hiện được.

Kỹ thuật giấu thông tin theo kiểu đánh giấu (watermarking) để bảo vệ bản quyền của đối tượng chứa thông tin tập trung đảm bảo một số các yêu cầu như đảm bảo tính bền vững… đây là ứng dụng cơ bản nhất của kỹ thuật thủy vân số.

1.2 Mô hình giấu thông tin cơ bản

Giấu thông tin vào phương tiện chứa và tách lấy thông tin là hai quá trình trái ngược nhau và có thể mô tả qua sơ đồ khối của hệ thống như sau:

1.2.1 Sơ đồ giấu tin



Hình 1.2. Sơ đồ giấu tin

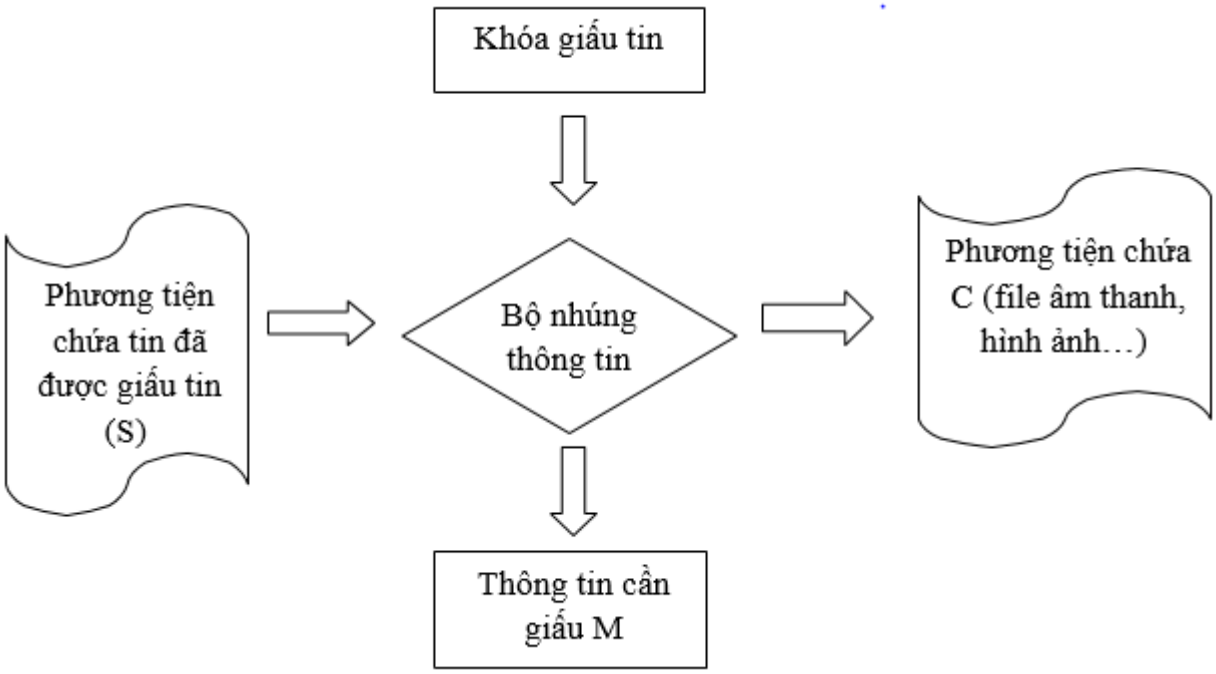
- Đầu vào:

- Thông tin cần giấu tùy theo mục đích của người sử dụng, nó có thể là thông điệp (với tin giấu bí mật) hay các logo, hình ảnh bản quyền.
- Phương tiện chứa: các file ảnh, text, audio… là môi trường để nhúng tin.
- Khóa là thành phần để góp phần làm tăng độ bảo mật.
- Bộ nhúng thông tin: là những chương trình thực hiện việc giấu thông tin.

- Đầu ra:

- Là các phương tiện chứa thông tin đã giấu trong đó.

1.2.2 Sơ đồ tách tin



Hình 1.3. Sơ đồ tách tin.

1.3 Môi trường giấu tin

1.3.1 Giấu tin trong ảnh

Giấu thông tin trong ảnh, hiện nay, là một bộ phận chiếm tỉ lệ lớn nhất trong các chương trình ứng dụng, các phần mềm, hệ thống giấu tin trong đa phương tiện bởi lượng thông tin được trao đổi bằng ảnh là rất lớn và hơn nữa giấu thông tin trong ảnh cũng đóng vai trò hết sức quan trọng trong hầu hết các ứng dụng bảo vệ an toàn thông tin như: nhận thực thông tin, xác định xuyên tạc thông tin, bảo vệ bản quyền tác giả, điều khiển truy cập, giấu thông tin mật... Chính vì thế mà vấn đề này đã nhận được sự quan tâm rất lớn của các nhà cá nhân, tổ chức, trường đại học, và viện nghiên cứu trên thế giới.

Thông tin sẽ được giấu cùng với dữ liệu ảnh nhưng chất lượng ảnh ít thay đổi và chẳng ai biết được đằng sau ảnh đó mang những thông tin có ý nghĩa. 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. Ví dụ như đối với các nước phát triển, chữ kí tay đã được số hoá và lưu trữ sử dụng như là hồ sơ cá nhân của các dịch vụ ngân hàng và tài chính, nó được dùng để xác thực

trong các thẻ tín dụng của người tiêu dùng. Phần mềm WinWord của MicroSoft cũng cho phép người dùng lưu trữ chữ kí trong ảnh nhị phân rồi gắn vào vị trí nào đó trong file văn bản để đảm bảo tính an toàn của thông tin. Tài liệu sau đó được truyền trực tiếp qua máy fax hoặc lưu truyền trên mạng. Theo đó, việc nhận thực chữ kí, xác thực thông tin đã trở thành một vấn đề cực kì quan trọng khi mà việc ăn cắp thông tin hay xuyên tạc thông tin bởi các tin tặc đang trở thành một vấn nạn đối với bất kì quốc gia nào, tổ chức nào. Thêm vào đó, lại có rất nhiều loại thông tin quan trọng cần được bảo mật như những thông tin về an ninh, thông tin về bảo hiểm hay các thông tin về tài chính, các thông tin này được số hoá và lưu trữ trong hệ thống máy tính hay trên mạng. Chúng rất dễ bị lấy cắp và bị thay đổi bởi các phần mềm chuyên dụng. Việc nhận thực cũng như phát hiện thông tin xuyên tạc đã trở nên vô cùng quan trọng, cấp thiết. Và 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 màu hay ảnh xám.

1.3.2 Giấu tin trong audio

Giấu thông tin trong audio mang những đặc điểm riêng khác với giấu thông tin trong các đối tượng đa phương tiện khác. Một trong những yêu cầu cơ bản của giấu tin là đảm bảo tính chất ẩn của thông tin được giấu đồng thời không làm ảnh hưởng đến chất lượng của dữ liệu gốc. Để đảm bảo yêu cầu này, kỹ thuật giấu thông tin trong ảnh phụ thuộc vào hệ thống thị giác của con người - HVS (Human Vision System) còn kỹ thuật giấu thông tin trong audio lại phụ thuộc vào hệ thống thính giác HAS (Human Auditory System). Và một vấn đề khó khăn ở đây là hệ thống thính giác của con người nghe được các tín hiệu ở các giải tần rộng và công suất lớn nên đã gây khó dễ đối với các phương pháp giấu tin trong audio. Nhưng thật may là HAS lại kém trong việc phát hiện sự khác biệt các dải tần và công suất điều này có nghĩa là các âm thanh to, cao tần có thể che giấu được các âm thanh nhỏ thấp một cách dễ dàng. Các mô hình phân tích tâm lí đã chỉ ra điểm yếu trên và thông tin này sẽ giúp ích cho việc chọn các audio thích hợp cho việc giấu tin. Vấn đề khó khăn thứ hai đối với giấu thông tin trong audio là kênh truyền tin. Kênh truyền hay băng thông chậm sẽ ảnh hưởng đến chất lượng thông tin sau khi giấu. Ví dụ để nhúng một

đoạn java applet vào một đoạn audio (16 bit, 44.100 Hz) có chiều dài bình thường thì các phương pháp nói chung cũng cần ít nhất là 20 bit/s. Giấu thông tin trong audio đòi hỏi yêu cầu rất cao về tính đồng bộ và tính an toàn của thông tin. Các phương pháp giấu thông tin trong audio đều lợi dụng điểm yếu trong hệ thống thính giác của con người.

1.3.3 Giấu thông tin trong video

Cũng giống như giấu thông tin trong ảnh hay trong audio, giấu tin trong video cũng được quan tâm và được phát triển mạnh mẽ cho nhiều ứng dụng như điều khiển truy cập thông tin, nhận thực thông tin và bảo vệ bản quyền tác giả. Ta có thể lấy một ví dụ là các hệ thống chương trình trả tiền xem theo đoạn với các video clip (pay per view application). Các kỹ thuật giấu tin trong video cũng được phát triển mạnh mẽ và cũng theo hai khuynh hướng là thủy vân số và data hiding. Nhưng phần giới thiệu này chỉ quan tâm tới các kỹ thuật giấu tin trong video. Một phương pháp giấu tin trong video được đưa ra bởi Cox là phương pháp phân bố đều. Ý tưởng cơ bản của phương pháp là phân phối thông tin giấu dàn trải theo tần số của dữ liệu chứa gốc. Nhiều nhà nghiên cứu đã dùng những hàm cosin riêng và các hệ số truyền sóng riêng để giấu tin. Trong các thuật toán khởi nguồn thì thường các kỹ thuật cho phép giấu các ảnh vào trong video nhưng thời gian gần đây các kỹ thuật cho phép giấu cả âm thanh và hình ảnh vào video. Như phương pháp của Swanson đã sử dụng phương pháp giấu theo khối, phương pháp này đã giấu được hai bit vào khối 8*8. Hay gần đây nhất là phương pháp của Mukherjee là kỹ thuật giấu audio vào video sử dụng cấu trúc lưới đa chiều...

1.3.4 Giấu thông tin trong văn bản dạng text

Giấu thông tin vào các văn bản dạng text khó thực hiện hơn do có ít các thông tin dư thừa, để làm được điều này người ta phải khéo léo khai thác các dư thừa tự nhiên của ngôn ngữ. Một cách khác là tận dụng các định dạng văn bản (mã hóa thông tin và khoảng cách giữa các từ khóa hay các dòng văn bản). Từ nội dung của thông điệp cần truyền đi, người ta cũng có thể sử dụng văn phạm phi ngữ cảnh để tạo nên các văn bản "phương tiện chứa" rồi truyền đi.

1.4 Một số ứng dụng của kỹ thuật giấu tin

Giấu tin trong ảnh số ngày càng được ứng dụng rộng rãi trong nhiều lĩnh vực. Các ứng dụng có sử dụng đến giấu tin trong ảnh số có thể là: ***Bảo vệ bản quyền tác giả*** (Copyright Protection), ***Điểm chỉ số*** (fingerprinting), ***Gán nhãn***(Labelling), ***Giấu thông tin mật*** (Steganography)…

Bảo vệ bản quyền: Là ứng dụng cơ bản nhất của kỹ thuật thủy vân số (watermarking) - một dạng của phương pháp giấu tin. Một thông tin nào đó mang ý nghĩa sở hữu quyền tác giả (người ta gọi nó là thủy vân - watermark) sẽ được nhúng vào trong các sản phẩm, thủy vân đó chỉ có một mình người chủ sở hữu hợp pháp các sản phẩm đó có và được dùng làm minh chứng cho bản quyền sản phẩm. Giả sử có một thành phẩm dữ liệu dạng đa phương tiện như ảnh, âm thanh, video cần được lưu thông trên mạng. Để bảo vệ các sản phẩm chống lại hành vi lấy cắp hoặc làm nhái cần phải có một kỹ thuật để "dán tem bản quyền" vào sản phẩm này. Việc dán tem hay chính là việc nhúng thủy vân cần phải đảm bảo không để lại một ảnh hưởng lớn nào đến việc cảm nhận sản phẩm. Yêu cầu kỹ thuật đối với ứng dụng này là thủy vân phải tồn tại bền vững cùng với sản phẩm, muốn bỏ thủy vân này mà không được phép của người chủ sở hữu thì chỉ còn cách là phá hủy sản phẩm.

Điểm chỉ số: Mục tiêu của điểm chỉ số là để chuyển thông tin về người nhận sản phẩm phương tiện số nhằm xác định đây là bản sao duy nhất của sản phẩm. Về mặt ý nghĩa điểm chỉ số tương tự như số xê ri của phần mềm.

Gán nhãn: Tiêu đề, chú giải và nhãn thời gian cũng như các minh họa khác có thể được nhúng vào ảnh, ví dụ đính tên người lên ảnh của họ hoặc đính tên vùng địa phương lên bảng đồ. Khi đó nếu sao chép ảnh thì cũng sẽ sao chép cả các dữ liệu nhúng trong nó. Và chỉ có chủ sở hữu của tác phẩm, người có được khoá mật (Stego-Key) mới có thể tách ra và xem các chú giải này. Trong một cơ sở dữ liệu ảnh, người ta có thể nhúng các từ khoá để các động cơ tìm kiếm có thể tìm nhanh một bức ảnh. Nếu ảnh là một khung ảnh cho cả một đoạn phim, người ta có thể gán cả thời điểm diễn ra sự kiện để đồng bộ hình ảnh với âm thanh. Người ta cũng có thể gán số lần ảnh được xem để tính tiền thanh toán theo số lần xem.

Giấu thông tin mật: Trong nhiều trường hợp sử dụng mật mã có thể gây ra sự chú ý ngoài mong muốn. Ngoài ra việc sử dụng công nghệ mã hoá có thể bị hạn chế một số kỹ thuật giấu tin trong ảnh mầu hoặc cấm sử dụng. Ngược lại việc giấu tin trong môi trường nào đó rồi gửi đi trên mạng ít gây sự chú ý. Có thể dùng nó để gửi đi một bí mật thương mại, một bản vẽ hoặc các thông tin nhạy cảm khác.

1.5 Cấu trúc ảnh bitmap

Bitmap Header (54 byte)
Color Palette
Bitmap Data

Bảng 1.1. Cấu trúc ảnh bitmap.

Mỗi file ảnh Bitmap gồm 3 phần theo bảng sau:

1.5.1 Bitmap header

Thành phần bitcount (Bảng 1.2) của cấu trúc Bitmap header cho biết số bit dành cho mỗi điểm ảnh và số lượng màu lớn nhất của ảnh.

Bảng 1.2. Thông tin về Bitmap header.

Byte thứ	Ý nghĩa	Giá trị
1-2	Nhận dạng file	“BM” hay 19778
3-6	Kích thước file	Kiểu long trong Turbo C
7-10	Dự trữ	Thường mang giá trị 0
11-14	Byte bắt đầu vùng dữ liệu	Offset của byte bắt đầu vùng dữ liệu
15-18	Số byte cho vùng thông tin	4 byte
19-22	Chiều rộng ảnh BMP	Tính bằng pixel
23-26	Chiều cao ảnh BMP	Tính bằng pixel
27-28	Số Planes màu	Cố định là 1

29-30	Số bit cho 1 pixel (bitcount)	Có thể là 1, 4, 8, 16, 24 tùy theo loại ảnh
31-34	Kiểu nén dữ liệu	0: Không nén 1: Nén runlength 8bits/pixel 2: Nén runlength 4bits/pixel
35-38	Kích thước ảnh	Tính bằng byte
39-42	Độ phân giải ngang	Tính bằng pixel/metter
43-46	Độ phân giải dọc	Tính bằng pixel/metter
47-50	Số màu sử dụng trong ảnh	
51-54	Số màu được sử dụng khi hiện thị ảnh	

1.5.2 Palette màu

Bảng màu của ảnh, chỉ những ảnh nhỏ hơn hoặc bằng 8 bit mới có bảng màu.

Bảng 1.3. Bảng màu của ảnh Bitmap.

Địa chỉ (Offset)	**Tên**	**Ý nghĩa**
0	RgbBlue	Giá trị cho màu xanh Blue
1	RgbGreen	Giá trị cho màu xanh Green
2	RgbRed	Giá trị cho màu đỏ
3	RgbReserved	Dự trữ

1.5.3 Bitmap data

Phần này nằm ngay sau phần Palete màu của ảnh BMP. Đây là phần chứa giá trị màu của điểm ảnh trong ảnh BMP. Các dòng ảnh được lưu từ dưới lên trên, các điểm ảnh được lưu từ trái sang phải. Giá trị của mỗi điểm ảnh là một chỉ số trỏ tới phần tử màu tương ứng trong Palete màu.

1.6 Tổng quan về mã hóa thông tin

1.6.1 Các khái niệm

1.6.1.1 Mật mã học

Mật mã học là một ngành khoa học nghiên cứu về việc giấu thông tin. Cụ thể hơn, mật mã học là ngành học nghiên cứu về những cách chuyển đổi thông tin từ dạng "có thể hiểu được" thành dạng "không thể hiểu được" và ngược lại.

Một số khái niệm trong mật mã học gồm: Mã hóa (encrypt hay encipher), Giải mã (Decrypt hay decipher), Bản rõ (Plaintext), Cipher (hay cypher), Khóa (Key).

1.6.1.2 Hệ mật mã (Crypto System)

Một hệ mật mã là bộ 5 (P,C,K,E,D) thõa mãn các tính chất sau:

1. P là không gian bản rõ: là tập hữu hạn các bản rõ có thể có.

2. C là không gian bản mã: là tập hữu hạn các bản mã có thể có.

3. K là không gian khóa: là tập hữu hạn các khóa có thể có.

4. Đối với mỗi $k \in K$, có một quy tắc mã hóa $ek \in E$ và một quy tắc giải mã tương ứng $dk \in D$. Với mỗi ek: $P \rightarrow C$ và dk: $C \rightarrow P$ là những hàm mà $dk(ek(x))=x$ cho mọi bản rõ $x \in P$. Hàm giải mã dk chính là ánh xạ ngược của hàm mã hóa ek.

1.6.1.3 Nguyên tắc Kerckhoffs

Một hệ mật mã sẽ được an toàn ngay cả khi tất cả mọi thứ trên hệ thống đó là công khai ngoại trừ khóa (key).

"Thuật toán mã hóa được tạo ra không cần phải giữ bí mật, có thể được công bố công khai, rơi vào tay quân địch mà không có bất kỳ sự phiền phức nào cả".

1.6.2 Tính chất của mã hóa thông tin

Mã hóa thông tin phải đảm bảo các tính chất sau: Tính bí mật (Confidentiality), tính xác thực (Authentication), tính toàn vẹn (Integrity).

1.6.3 Độ an toàn của hệ mật mã

Độ an toàn của thuật toán phụ thuộc vào độ phức tạp của nó. Các yếu tố xem xét thuật toán an toàn là chi phí hay phí tổn, thời gian cần thiết để phá vỡ, lượng dữ liệu để phá vỡ.

1.6.4 Các phương pháp mã hóa

1.6.4.1 Mã hoá cổ điển (Classical cryptography)

Phương pháp này là tiền thân của các phương pháp mã hóa đối xứng ngày nay. Có hai phương pháp nổi bật đó là: Mã hoá thay thế (Substitution Cipher), Mã hoá hoán vị (Transposition Cipher).

1.6.4.2 Mã hoá đối xứng (Symetric cryptography)

Mã hoá đối xứng sử dụng cùng một khoá cho cả hai quá trình mã hoá và giải mã. Mã hoá đối xứng có thể tác động trên bản rõ theo từng nhóm bit hay theo từng bit một.

1.6.4.3 Mã hoá bất đối xứng (Asymetric cryptography)

Mã hóa bất đối xứng được thiết kế sao cho khoá sử dụng trong quá trình mã hoá khác biệt với khoá được sử dụng trong quá trình giải mã. Tất nhiên không thể suy luận khóa giải mã từ khóa mã và ngược lại. Khoá để mã hoá được gọi là khóa công khai (Public Key), khoá để giải mã được gọi là khóa bí mật (Private Key).

1.6.4.4 Hệ thống mã hoá khoá lai (Hybrid Cryptosystems)

Hệ thống mã hoá khoá lai ra đời là sự kết hợp giữa tốc độ và tính an toàn của hai hệ thống mã hoá ở trên.

1.6.5 Ứng dụng của mã hóa thông tin

Mã hóa thông tin được ứng dụng trong rất nhiều lĩnh vực cả về phần cứng và phần mềm.

1.6.6 Giới thiệu một số giải thuật mã hóa tiên tiến

1.6.6.1 Các hệ mã khối

Các hệ mã khối dựa trên cơ sở làm việc với các khối dữ liệu là các chuỗi bit có kích thước khau nhau (tối thiểu là 64bit), khóa của hệ mã hóa cũng là một xâu bit có độ dài cố định.

Một số giải thuật được sử dụng khá phổ biến là DES, Triple DES (3DES), AES.

● Mã hóa DES

DES (Data Encryption Standard) là thuật toán mã hóa với dữ liệu đầu vào và đầu ra là một khối 64 bit với độ dài khóa 64 bit (trong đó 8 bit được dùng để kiểm tra tính chẵn lẻ). Thuật toán thực hiện 16 vòng với 16 khóa (48bit) được sinh ra trong mỗi vòng.

Quá trình giải mã được diễn ra tương tự nhưng với các khóa con ứng dụng vào các vòng trong theo thứ tự ngược lại.

Thuật toán DES bộc lộ một số điểm yếu mà những kẻ lợi dụng nó để thám mã.

● Triple DES (3DES)

Triple DES thật chất là mã hóa theo DES ba lần với khóa K1, K2, K3 cho mỗi lần.

● Chuẩn mã hóa nâng cao AES

AES (Advanced Encryption Standard) là một chuẩn mã hóa cao cấp với khóa bí mật cho phép xử lý các khối dữ liệu đầu vào có kích thước 128 bit và sử dụng các khóa có độ dài 128, 192, 256 bit.

1.6.6.2 Các hệ mã hóa công khai

Mã hoá bằng khoá công khai là phương thức được thực hiện trên hai khóa, một được dùng để mã hóa (được gọi là khóa công khai – public key) và một khóa

được dùng trong quá trình giải mã (gọi là khóa bí mật – private key). Khóa giải mã không thể tính toán được từ khóa mã hóa.

1.6.6.3 Hàm băm

Hàm băm là hàm toán học chuyển đổi một thông điệp có độ dài bất kỳ thành một dãy bit có độ dài cố định. Mọi thay đổi dù là rất nhỏ trên thông điệp đầu vào đều làm thay đổi giá trị băm của nó.

1.7 Phương pháp mã hóa AES

1.7.1 Giới thiệu

Advanced Encryption Standard là thuật toán của hai nhà nghiên cứu Tiến sĩ Joan Daemon và Tiến sĩ Vincent Rijmen từ Bỉ.

Chuẩn mã hóa AES cho phép xử lý các khối dữ liệu đầu vào có kích thước 128 bit sử dụng các khóa có độ dài 128, 192 hoặc 256 bit. Thuật toán AES là một thuật toán khóa đối xứng có nghĩa là phím tương tự được sử dụng để mã hóa và giải mã tin nhắn. Ngoài ra, các thuật toán mã hóa văn bản được sản xuất bằng các thuật toán AES là như nhau kích thước như tin nhắn văn bản đơn giản. Hầu hết các hoạt động trong thuật toán AES xảy ra trên các byte dữ liệu hoặc trên từ dữ liệu dài 4 byte, được đại diện trong các trường GF (28), Được gọi là trường Galois. AES dựa trên một nguyên tắc thiết kế được biết đến như là một thay thế hoán vị mạng. AES hoạt động trên một ma trận 4 × 4 của byte, gọi là mảng trạng thái. Thuật toán mã hóa AES được quy định như một số lặp đi lặp lại vòng chuyển đổi đầu vào của bản rõ, thành quả cuối cùng sẽ là bản mã. Mỗi vòng bao gồm một số bước xử lý, trong đó có một phụ thuộc vào khóa mã hóa. Một tập hợp các vòng đảo ngược được áp dụng để biến đổi bản mã trở lại bản gốc bản rõ bằng cách sử dụng cùng một khóa mã hóa. AES thuật toán vòng lặp thông qua các phần nhất định Nr lần.

1.7.2 Qui trình mã hóa

Bắt đầu quá trình mã hóa, bản rõ được sao chép vào mảng trạng thái. Sau khi thực hiện thao tác cộng với khóa mã đầu tiên, mảng trạng thái sẽ được biến đổi qua Nr vòng trong đó lần cuối cùng được thực hiện khác với Nr-1 vòng trước đó. Nội dung của mảng trạng thái ở vòng cuối cùng sẽ là bản mã của quá trình mã hóa.

Trong quy trình mã hóa của AES, tất cả các vòng lặp đều sử dụng 4 hàm theo thứ tự: Subbytes(), ShiftRows(), MixColumns(), AddRoundKey(). Riêng vòng cuối cùng bỏ qua việc gọi hàm MixColumns().

Quá trình mã hóa AES có các bước sau đây:

1) KeyExpansion -Round (khóa vòng mở rộng) được tạo ra từ khóa mã hóa bằng cách sử dụng lược đồ khóa Rijndael.

2) Initial Round (vòng khởi tạo)

AddRoundKey - thực hiện bằng cách cộng một khóa vòng tại vòng đang xét với mảng trạng thái thông qua phép toán XOR đơn giản trên bit.

3) Rounds (vòng lặp)

a) SubBytes - làm biến mảng trạng thái hiện hành bằng cách sử dụng một bảng thay thế.

b) ShiftRows - làm biến đổi các byte trên ba hàng cuối cùng mảng trạng thái bằng cách dịch vòng.

c) MixColumns - là một phép biến đổi mã hóa được thực hiện bằng cách lấy tất cả các cột của mảng trạng thái trộn với dữ liệu của chúng một cách độc lập nhau để tạo ra các cột mới.

d) AddRoundKey - thực hiện bằng cách cộng một khóa vòng tại vòng đang xét với mảng trạng thái thông qua phép toán XOR đơn giản trên bit.

4) Final Round – vòng kết thúc (không có MixColumns)

Gọi lại các hàm SubBytes, ShiftRows, MixColumns ở bước 3 nhưng không gọi hàm AddRoundKey.

1.7.3 Qui trình giải mã

Quá trình giải mã được thực hiện theo chiều ngược lại với quy trình mã hóa, đồng thời các phép biến đổi trong quá trình này cũng được thực hiện đảo ngược. Ngoại trừ phép biến đổi AddRoundKey() không thay đổi vì chính bản thân nó là một phép biến đổi thuận ngịch do chỉ áp dụng một phép toán XOR.

- InvShiftRows() chính là phép biến đổi ngược của ShiftRows().
- Là phép biến đổi ngược của SubBytes() được thực hiện trên bảng thay thế S-Box là nghịch đảo của S-Box.
- InvMixColumns() là phép biến đổi ngược của MixColumns().

CHƯƠNG 2: KỸ THUẬT GIẤU TIN TRONG ẢNH SỬ DỤNG KẾT HỢP MÃ HÓA AES VÀ GIẤU TIN

2.1 Giới thiệu kỹ thuật giấu tin trên sai phân

Kỹ thuật giấu tin trên sai phân được đề xuất bởi Wu và Tsai [3] tháng 6 năm 2003. Kỹ thuật giấu tin trên sai phân là một phương pháp giấu tin mới và hiệu quả bằng cách nhúng các tin nhắn bí mật vào một ảnh màu xám. Trong quá trình nhúng một thông điệp bí mật, hình ảnh ban đầu được phân chia thành khối nhỏ không chồng chéo gồm hai điểm ảnh liên tiếp. Một giá trị chênh lệch được tính toán từ các giá trị của hai điểm ảnh trong mỗi khối. Tất cả các giá trị đó được phân loại vào một số phạm vi. Giá trị chênh lệch sau đó được thay thế bằng một giá trị mới khi nhúng các giá trị thông điệp bí mật. Sau đó tính các giá trị màu xám mới cho ảnh sau khi giấu tin ta được ảnh đã giấu tin. Kỹ thuật giấu tin trên sai phân cho chất lượng ảnh khá cao và khó để nhận biết bằng mắt thường. Thông điệp bí mật nhúng có thể được chiết xuất từ hình ảnh đã giấu thông tin mà không cần tham khảo hình ảnh ban đầu. Thống kê kép các cuộc tấn công cũng được thực hiện để thu thập dữ liệu liên quan đã cho thấy sự an toàn của phương pháp này.

2.2 Quá trình giấu tin trong ảnh sử dụng kết hợp mã hóa AES và kỹ thuật giấu tin trên sai phân

2.2.1 Thuật toán giấu tin

Đầu vào:

- Ảnh sử dụng để giấu tin.
- Thông điệp.

Đầu ra:

- Ảnh đã giấu tin.

Các bước thực hiện:

Bước 1: Sử dụng kỹ thuật mã hóa AES cho thông điệp cần giấu. Sau đó chuyển chuỗi thông điệp đã mã hóa sang nhị phân.

Bước 2: Từ ảnh cấp xám dùng để giấu tin ta có ma trận ảnh tương ứng. Tính giá trị di bằng cách trừ hai điểm ảnh liên tiếp cho nhau di = gi +1 - gi, với gi, gi +1 ∈ [0,. . . , 255], i=1:mxn (với m và n là kích cỡ ảnh).

Bước 3: Các giá trị tuyệt đối | di |, | di | ∈ [0,. . . , 255], được phân loại vào các phạm vi Ri (Ri gồm các miền giá trị sau [0 7], [8 15], [16 31], [32 63], [64 127] và [128 255]), với i = 1, 2,. . . n. Cận trên cận dưới và độ rộng của mỗi Ri được ký hiệu lần lượt là li, ui và wi. Giả sử | di | thuộc Rk với k ∈ [1,2. . . 6].

Bước 4: Ta xác định được số bit sẽ nhúng theo công thức (2.1)

$$n = \lfloor \log_2(w_k) \rfloor$$

Sau đó chọn n bit từ chuỗi bit cần giấu giấu vào mỗi giá di.

Bước 5: Tính lại d được d_i' theo công thức (2.2).

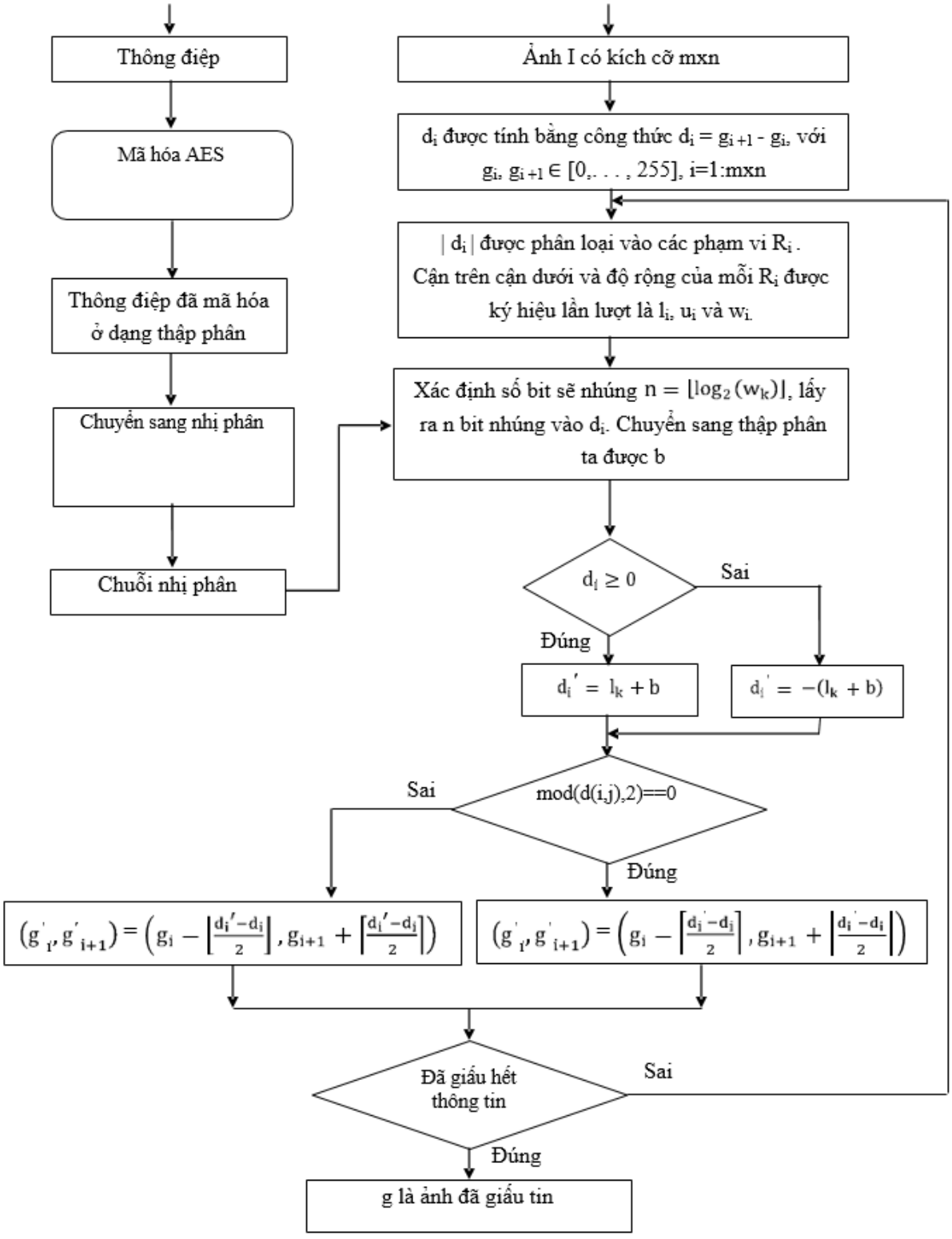
(2.2)
$$d_i' = \begin{cases} l_k + b & \text{for } d_i \geq 0 \\ -(l_k + b) & \text{for } d_i < 0 \end{cases}$$

Bước 6: Tính các giá trị màu xám mới (gi, gi +1) cho ảnh sau khi giấu tin theo công thức (2.3).

(2.3)
$$(g'_i, g'_{i+1}) = \begin{cases} \left(g_i - \left\lceil \frac{d_i' - d_i}{2} \right\rceil, g_{i+1} - \left\lfloor \frac{d_i' - d_i}{2} \right\rfloor\right) & \text{nếu } d_i \text{ là giá trị chẵn} \\ \left(g_i - \left\lfloor \frac{d_i' - d_i}{2} \right\rfloor - \left\lceil \frac{d_i' - d_i}{2} \right\rceil\right) & \text{nếu } d_i \text{ là giá trị lẻ} \end{cases}$$

Cuối cùng ta được ảnh đã giấu tin.

Sau đây là sơ đồ quá trình giấu tin hình 2.1.



Hình 2.1. Sơ đồ quá trình giấu tin.

2.2.2 Ví dụ minh họa quá trình giấu tin

Với chuỗi thông điệp cần giấu là “co”, chuyển chuỗi thông điệp cần giấu sang dạng thập phân ta được:

Plaintext = 99 111 32 32 32 32 32 32 32 32 32 32 32 32 32 32

Vì ta sử dụng mã hóa AES 16 bit nên nếu thông điệp nhập vào không đủ 16 bit các kí tự cách trống sẽ được tự động thêm vào phía sau chuỗi thông điệp cho đủ 16 bit.

Sử dụng kỹ thuật mã hóa AES cho thông điệp cần giấu ta được chuỗi thông điệp mã hóa ở dạng thập phân:

Ciphertext = 251 201 120 38 44 31 114 224 52 84 116 138 223 16 160 116

Chuỗi thông điệp đã mã hóa ở dạng văn bản là: “ûÉx&,rà4Ttß t”.

Sau đó ta chuyển chuỗi thông điệp đã mã hóa sang nhị phân ta được chuỗi bit thông điệp cần giấu:

str_bin=1111101111001001011110000010011000101100000111110111001011100000001101000101010001110100100010101101111100010000101000000111 0 100

Ảnh giấu tin là một khối ảnh được biểu diễn bởi ma trận 4x4: $\begin{bmatrix} 145 & 138 & 142 & 139 \\ 142 & 141 & 144 & 138 \\ 142 & 142 & 144 & 138 \\ 143 & 139 & 144 & 138 \end{bmatrix}$

Ta tính được di = $\begin{bmatrix} -7 & 3 \\ -1 & 6 \\ 0 & 6 \\ -4 & 6 \end{bmatrix}$

Sử dụng kỹ thuật giấu tin trên sai phân, áp dụng các công thức (2.1),(2.2) và (2.3) ta được ma trận ảnh sau khi giấu tin là: $\begin{bmatrix} 145 & 138 & 144 & 138 \\ 145 & 138 & 143 & 139 \\ 144 & 140 & 143 & 138 \\ 144 & 137 & 141 & 141 \end{bmatrix}$

2.3 Quá trình tách tin

2.3.1 Thuật toán tách tin

Đầu vào:

● Ảnh đã giấu tin.

Đầu ra:

● Thông điệp đã giấu.

Các bước thực hiện:

Bước 1: Từ ảnh đã giấu tin ta có ma trận ảnh tương ứng. Tính giá trị di bằng cách trừ hai điểm ảnh liên tiếp cho nhau di = gi +1 - gi, với gi, gi +1 ∈ [0,. . . , 255], i=1:mxn (với m và n là kích cỡ ảnh).

Bước 2: Xác định phạm vi Ri của mỗi giá trị tuyệt đối | di | được li, ui và wi. Từ đó tính được số bit thông tin đã giấu n = $\lfloor \log_2(w_k) \rfloor$.

Giá trị thập phân đã giấu vào di được tính bằng công thức (2.4).

$$b = |d_i| - l_i \qquad (2.4)$$

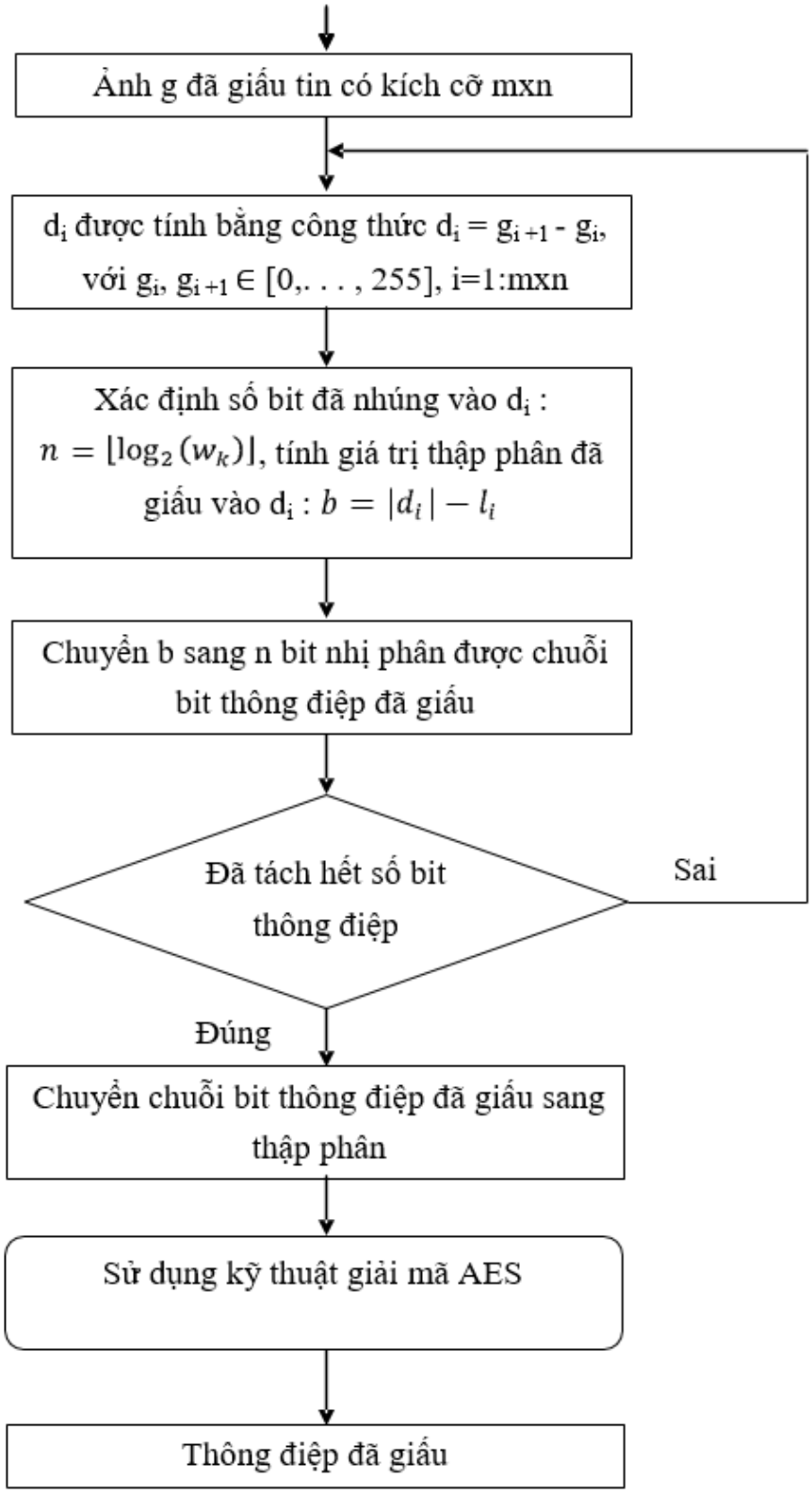
Chuyển b sang n bit nhị phân ta được chuỗi bit thông điệp đã giấu.

Bước 3: Lặp lại bước 2 cho đến khi tách được số bit đã giấu.

Bước 4: Chuyển chuỗi bit thông điệp đã giấu ở dạng nhị phân sang thập phân ta được chuỗi thông điệp mã hóa đã giấu ở dạng thập phân.

Bước 5: Sử dụng kỹ thuật giải mã AES cho chuỗi thông điệp mã hóa đã giấu ta được chuỗi thông điệp cần tách.

Sau đây là sơ đồ thuật toán tách tin.



Hình 2.2. Sơ đồ quá trình tách tin.

2.3.2 Ví dụ minh họa quá trình tách tin

Từ khối ảnh đã giấu tin ta có ma trận ảnh tương ứng: $\begin{bmatrix} 145 & & & 138 \\ 145 & 138 & 143 & 139 \\ 144 & 140 & 143 & 138 \\ 144 & & & 141 \end{bmatrix}$

Ta tính được di = $\begin{bmatrix} -7 & 6 \\ -7 & 4 \\ -4 & 5 \\ -7 & 0 \end{bmatrix}$

Sử dụng kỹ thuật tách trên sai phân, áp dụng bước 3 của thuật toán tách ta được chuỗi bit thông điệp đã giấu ở dạng nhị phân:

str_bin = 1111101111001001011110000010011000101100000111110111001011100000001101000101010001110100100010101101111100010000101000000111 0 100

Chuyển chuỗi bit thông điệp đã giấu ở dạng nhị phân sang thập phân ta được chuỗi thông thông điệp mã hóa đã giấu ở dạng thập phân:

str_dec = 251 201 120 38 44 31 114 224 52 84 116 138 223 16 160 116

Sử dụng kỹ thuật giải mã AES ta được chuỗi thông điệp đã giấu ở dạng thập phân:

Re_plaintext = 99 111 32 32 32 32 32 32 32 32 32 32 32 32 32 32

Chuyển chuỗi thông điệp đã được giải mã sang dạng văn bản text ta được chuỗi thông điệp đã giấu: “co”.

CHƯƠNG 3: CÀI ĐẶT THỬ NGHIỆM

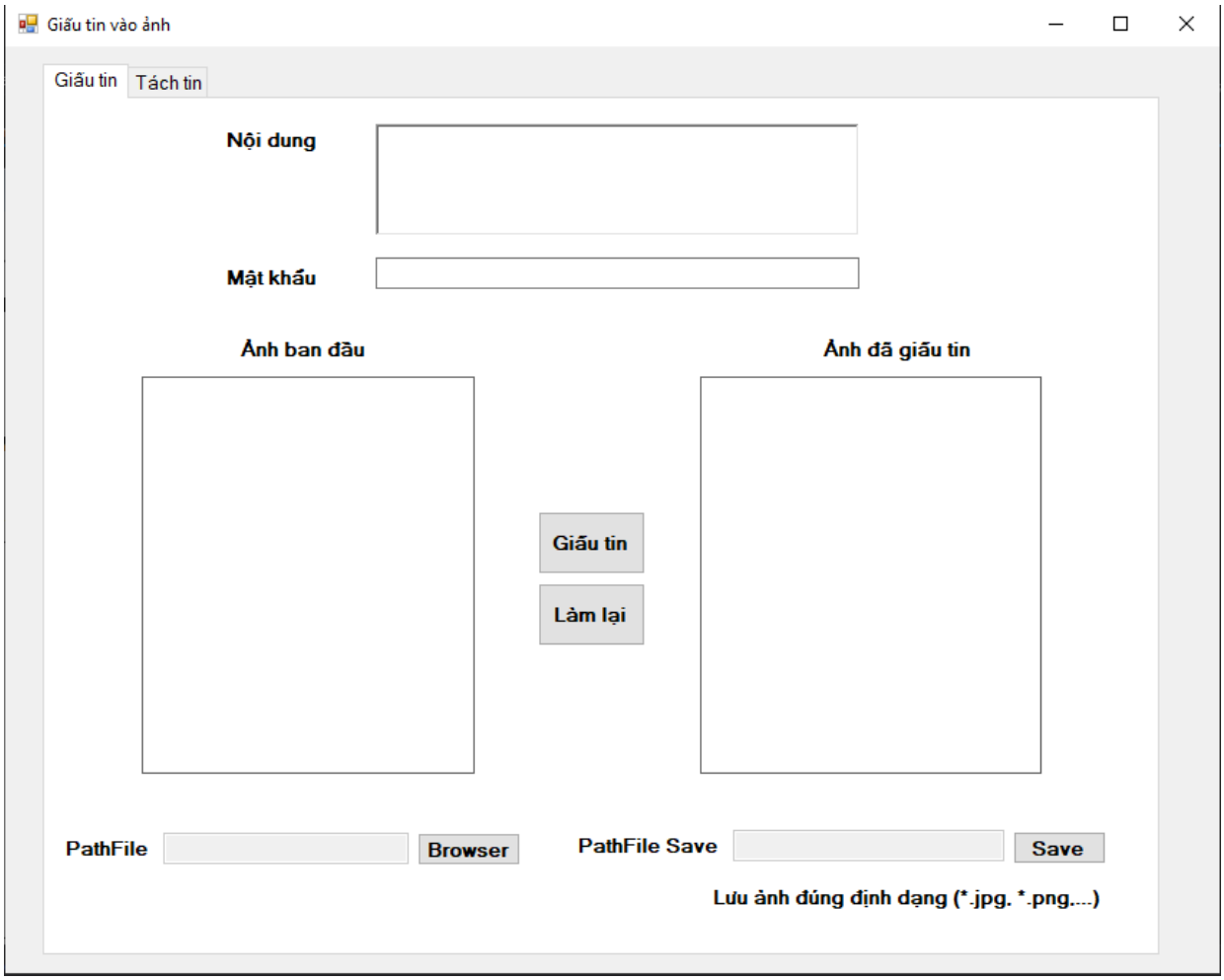
3.1 Môi trường cài đặt

Ngôn ngữ cài đặt, môi trường soạn thảo và chạy chương trình được thực hiện trên ngôn ngữ lập trình C#, Java.

Hệ điều hành Windows 10.

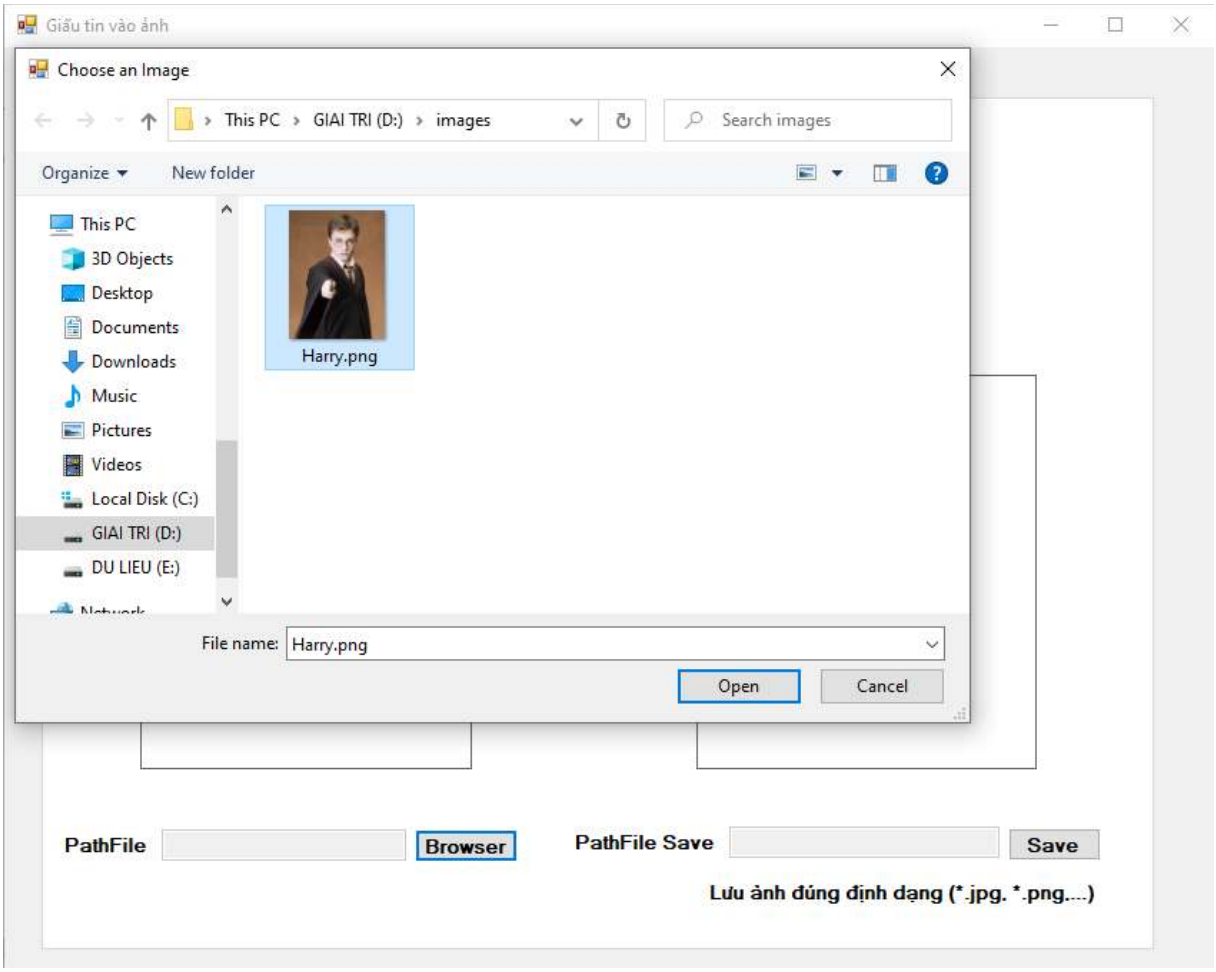
3.2 Giao diện chương trình

3.2.1 Chương trình demo với ngôn ngữ C#

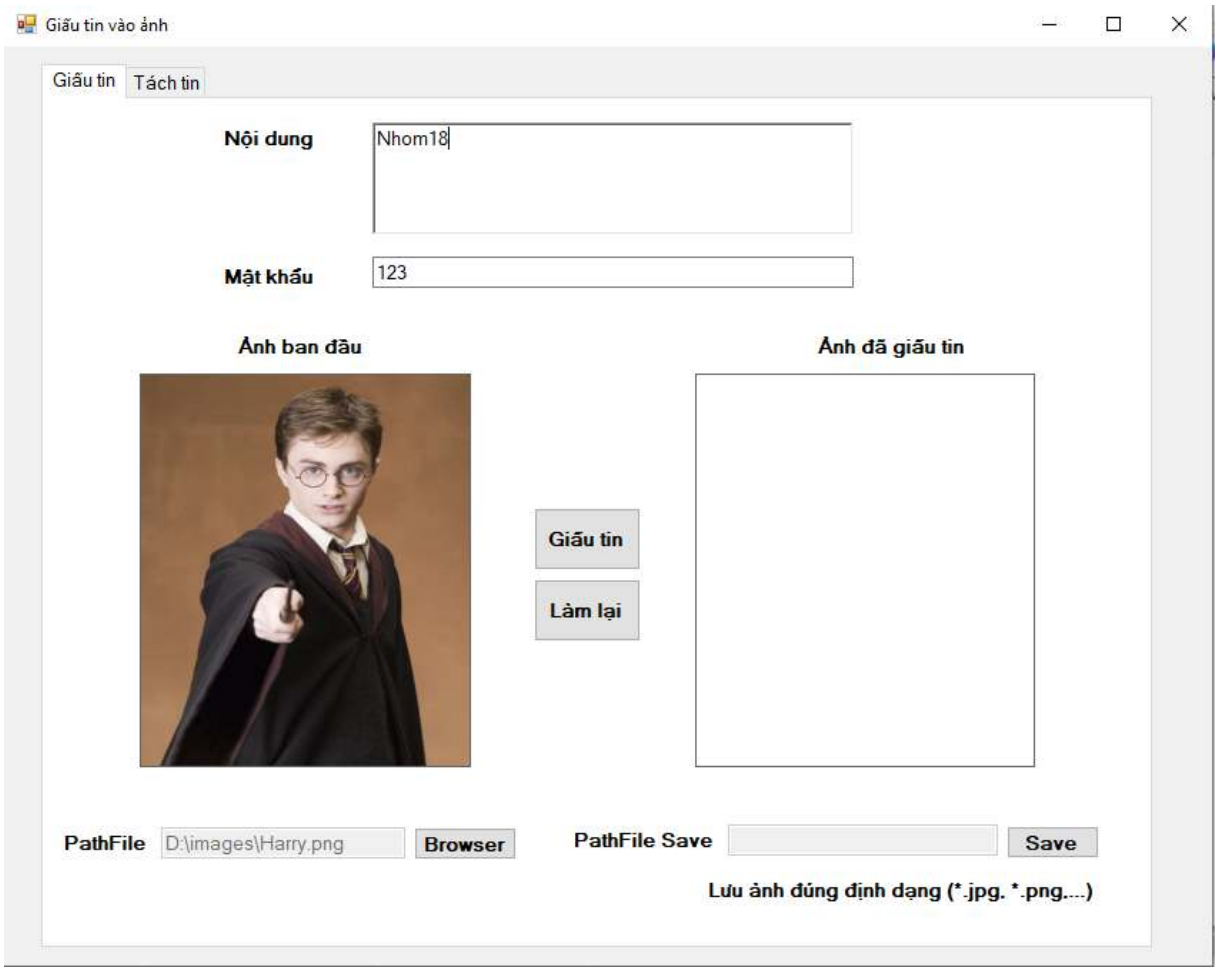


Đây là giao diện khi khởi động, từ đây ta sẽ gọi đến các giao diện khác thông qua menu.

Để nhập ảnh vào ta chọn nút "Browser" bên Ảnh ban đầu, một hộp thoại sẽ được mở ra để ta chọn ảnh đưa vào giấu tin.

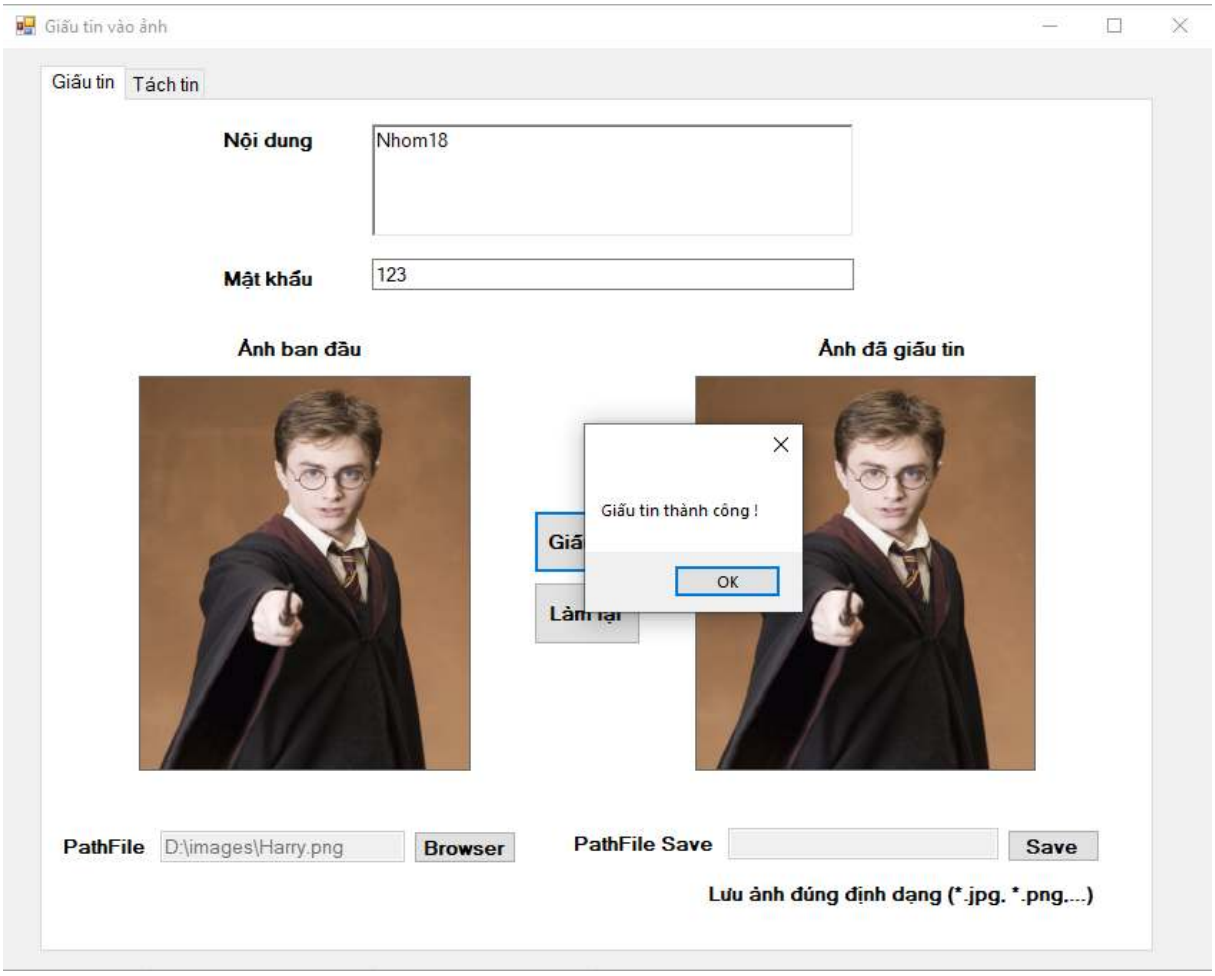


Tiếp theo, ta cần nhập dữ liệu cần giấu vào ảnh bằng cách nhập trực tiếp dữ liệu vào ô "Nội dung" và "Mật khẩu".

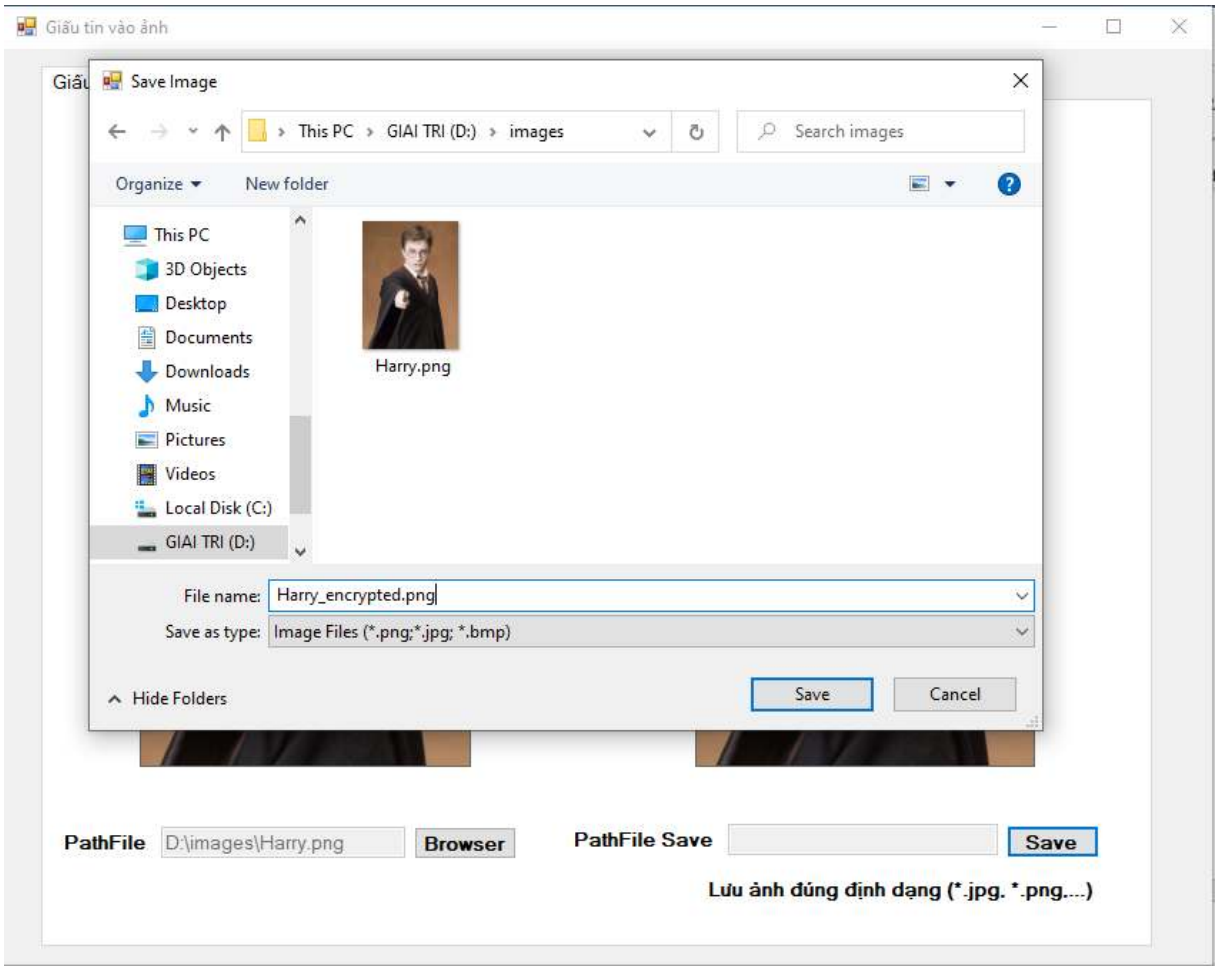


Và sau đó chọn nút "Giấu tin" để chương trình thực hiện giấu tin.

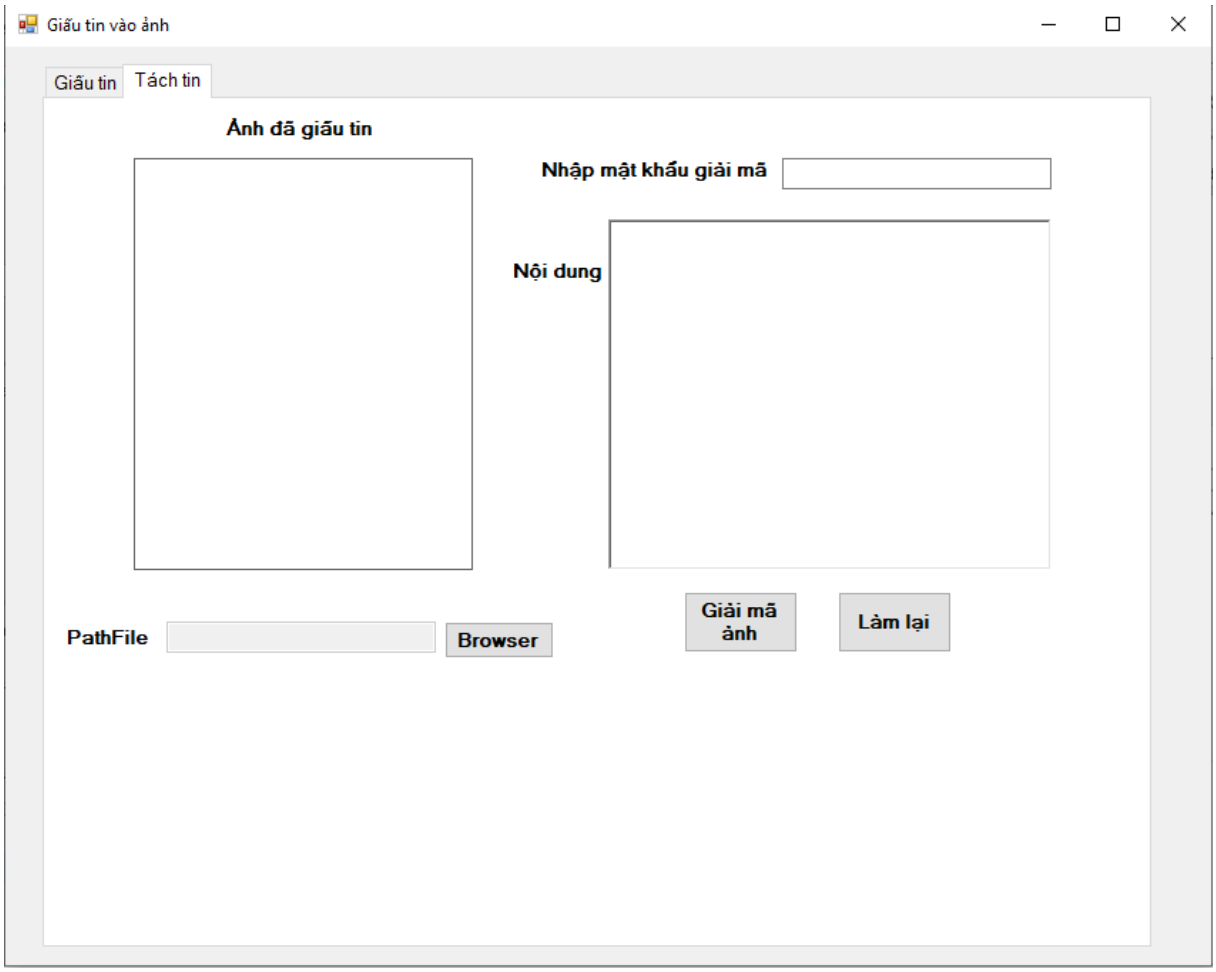
Sau khi giấu tin thành công ảnh đã giấu tin sẽ hiện lên tại mục “Ảnh đã giấu tin”.



Tiếp theo ta chọn nút “Save”, nhập tên và chọn nơi lưu ảnh kết quả.

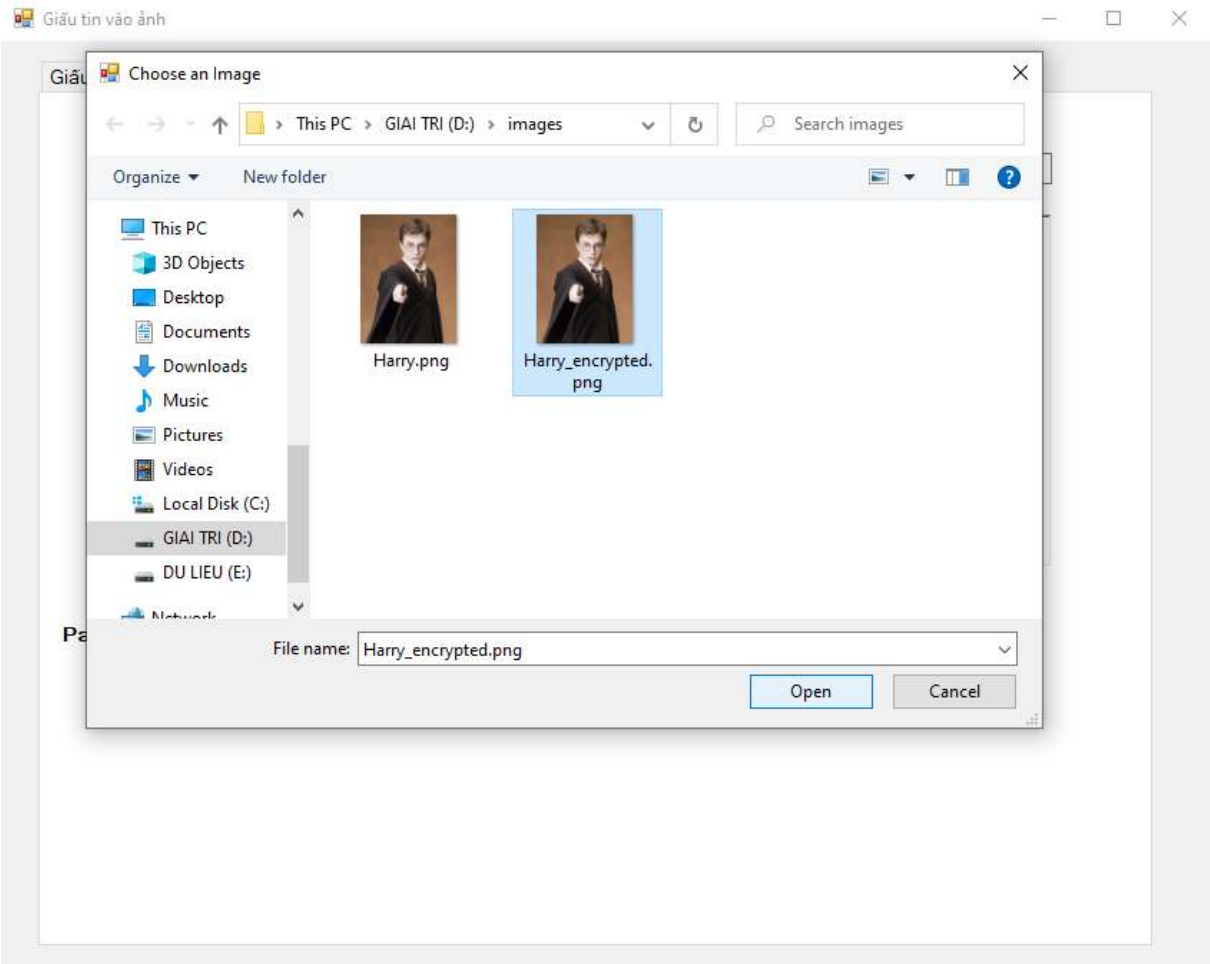


Từ menu “Tách tin” trên giao diện chính gọi ra giao diện tách tin.



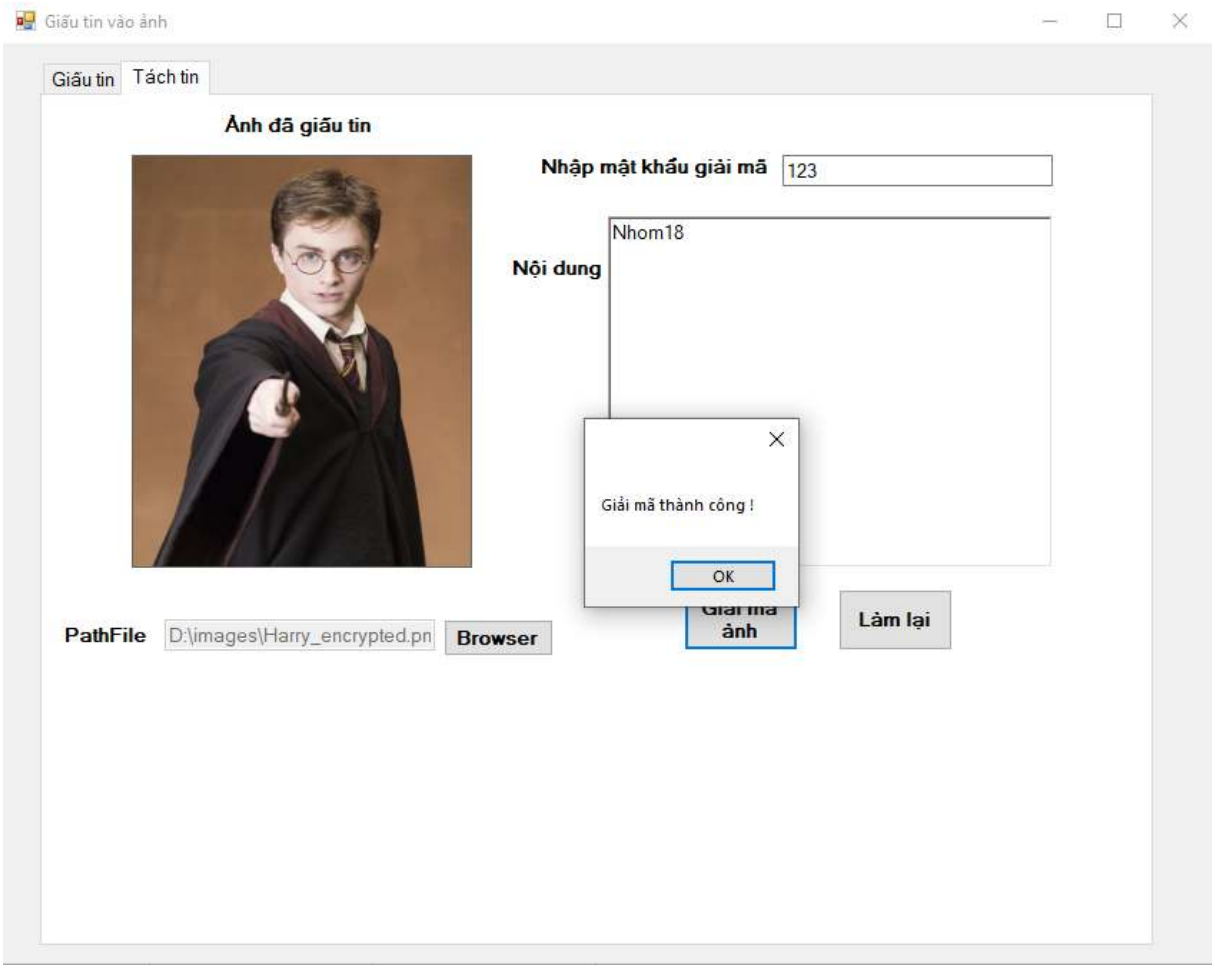
Đây là giao diện sẽ lấy ảnh đã giấu thông tin để xử lý tách tin lấy ra dữ liệu đã giấu trong ảnh.

Thực hiện mở ảnh có giấu tin để tách thông tin đã giấu.



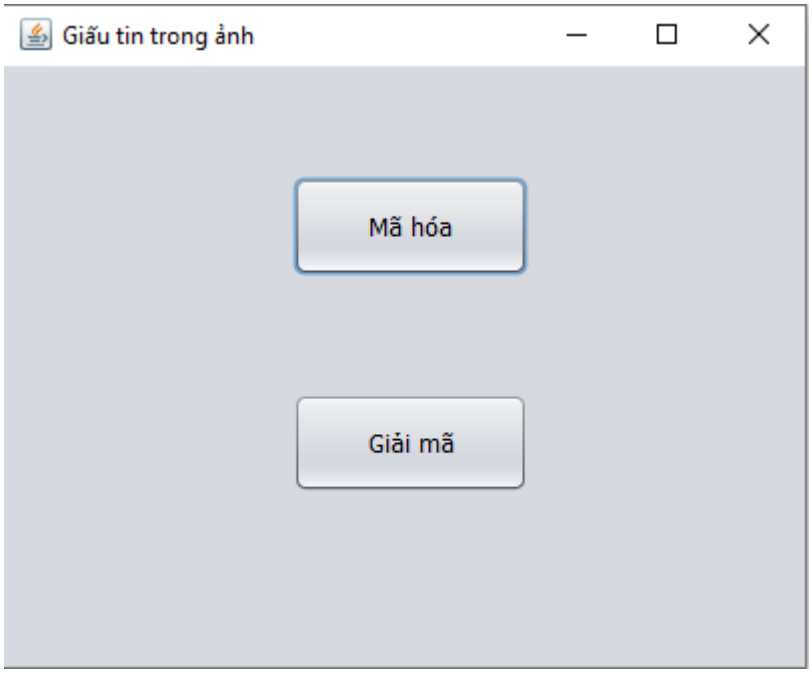
Sau đó nhập dữ liệu cho ô “Nhập mật khẩu giải mã” và chọn nút “Giải mã ảnh” để chương trình thực hiện giải mã.

Thực hiện xong quá trình tách tin ta nhận được dữ liệu được tách ra ở mục “Nội dung”.

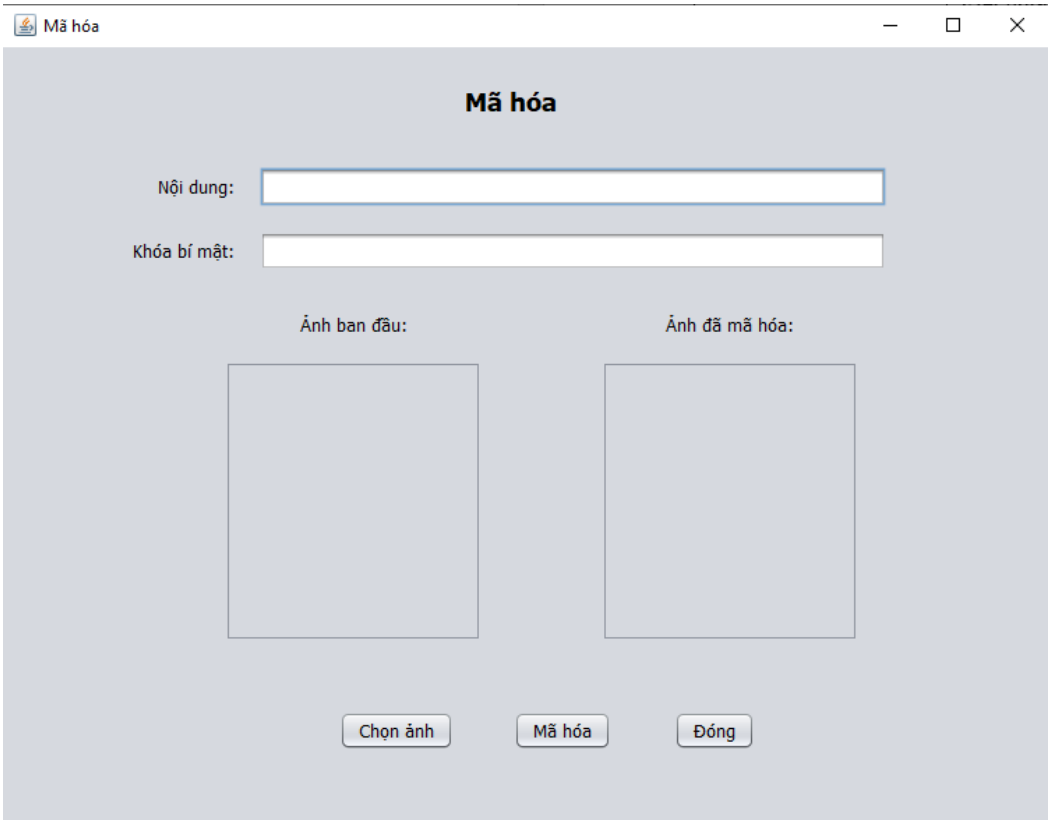


3.2.2 Chương trình demo với ngôn ngữ Java

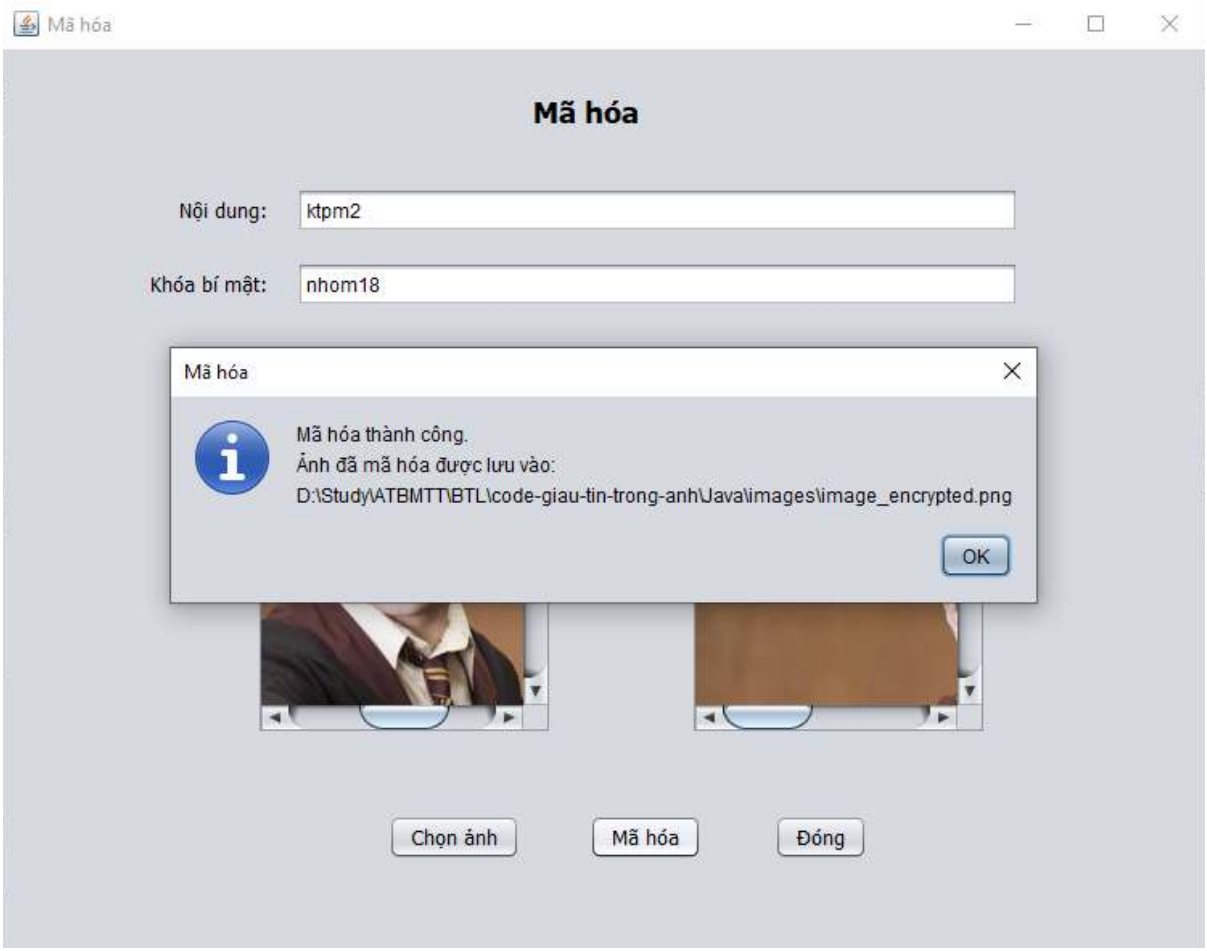
Đây là màn hình khởi động, sẽ có 2 phím chức năng là mã hóa và giải mã.



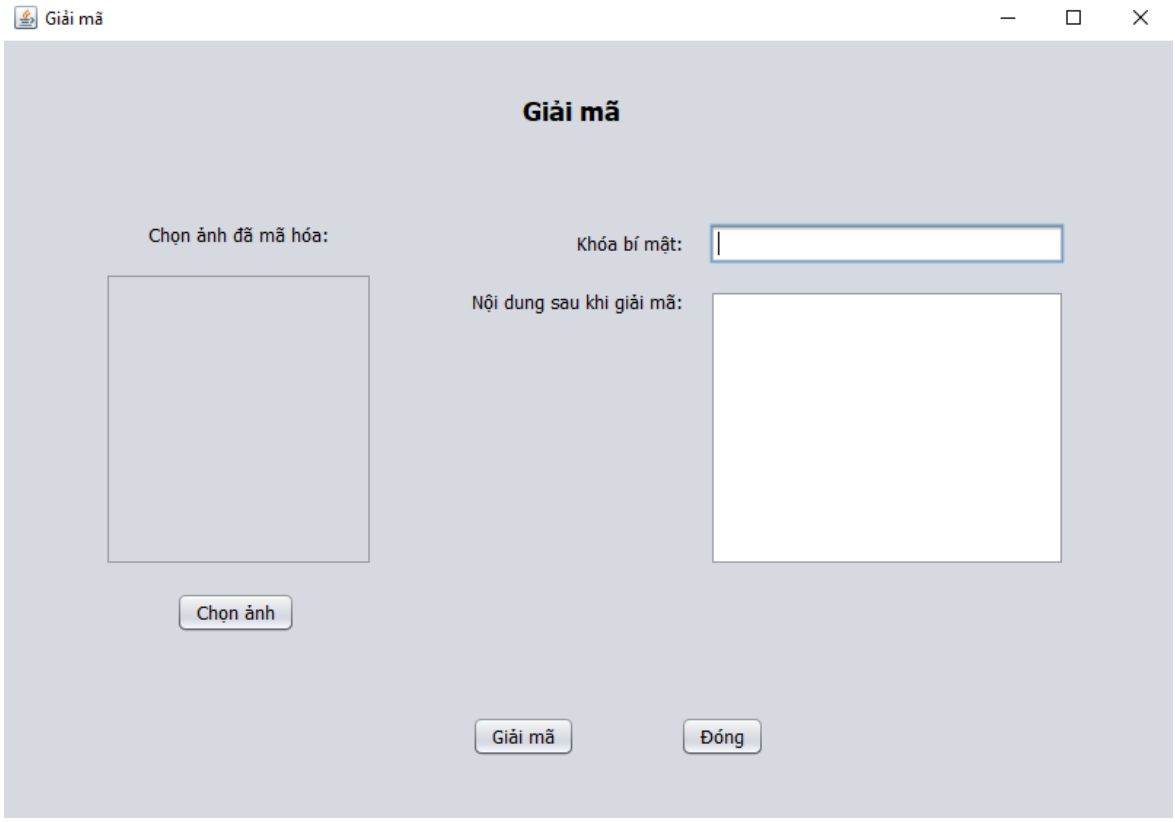
Để mã hóa chọn nút "Mã hóa". Màn hình mã hóa xuất hiện.



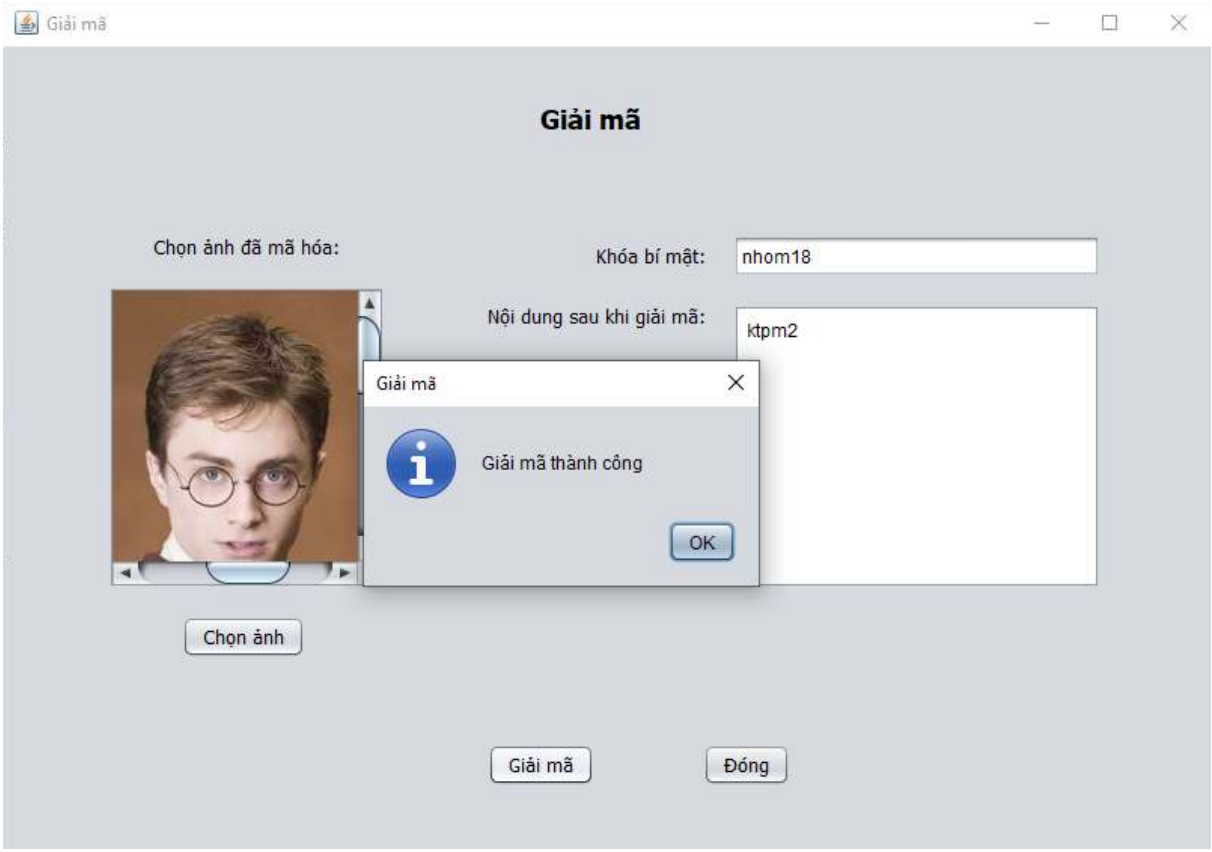
Nhập nội dung, khóa bí mật và chọn ảnh sau đó chọn nút “Mã hóa” để chương trình thực hiện mã hóa nội dung kết hợp giấu tin vào ảnh.



Chờ chương trình hoành thành rồi chọn nút “OK” để đóng thông báo thành công. Ảnh đã mã hóa được lưu vào thư mục “images” của project chương trình. Để thực hiện giải mã ta chọn nút “Đóng” để quay trở về màn hình chính rồi chọn “Giải mã”. Màn hình mã hóa xuất hiện.



Chọn ảnh cần giải mã rồi nhập khóa bị mật, chọn nút “Giải mã” để chương trình thực hiện giải mã.



Thực hiện xong quá trình giải mã ta nhận được dữ liệu được tách ra ở mục “Nội dung sau khi giải mã”.

3.3 Phân công công việc

Các nội dung:

- Tìm hiểu mật mã AES.
- Tìm hiểu về dấu tin trong ảnh và cấu trúc ảnh bitmap.
- Nghiên cứu kỹ thuật giấu tin trên sai phân.
- Tìm hiểu ngôn ngữ lập trình Matlab 7.7, Java, C#.
- Ứng dụng xây dựng chương trình giấu tin trong ảnh sử dụng kết hợp mã hóa AES và kỹ thuật giấu tin trên sai phân.

Tên sinh viên	Tên công việc
Nguyễn Anh Đức (984)	Tìm hiểu về: - Cấu trúc ảnh bitmap - Quá trình giấu tin và tách tin Viết chương trình demo với ngôn ngữ Python
Nguyễn Anh Đức (712)	Tìm hiểu về: - Mô hình giấu tin - Môi trường giấu tin Viết chương trình demo với ngôn ngữ C#
Lê Dũng	Tìm hiểu về: - Mã hóa thông tin - Phương pháp mã hóa AES Viết chương trình demo với ngôn ngữ Java
Nguyễn Tiến Dũng	Tìm hiểu về: - Ứng dụng của kỹ thuật giấu tin - Quá trình tách tin trên ảnh Viết chương trình demo với ngôn ngữ JavaScritp

3.4 Kết luận

Bài tập lớn của chúng em đã thực hiện những nhiệm vụ sau:

- Trình bày một số khái niệm cơ bản về: Giấu tin trong ảnh, môi trường giấu tin, sơ lược về mô hình giấu tin cơ bản, tổng quan về ảnh Bitmap, tổng quan về mã hóa thông tin, phương pháp mã hóa AES.
- Trình bày kỹ thuật giấu tin trên ảnh, kết hợp giữa mã hóa AES và phương pháp giấu tin trên ảnh.

Kỹ thuật giấu tin sử dụng kết hợp mã hóa AES và phương pháp giấu tin trên sai phân là một trong những phương pháp giấu tin bảo mật cao với hai tầng bảo mật dữ liệu và cho chất lượng ảnh tốt với khả năng nhúng cao. Với sự phát triển một cách bùng nổ của ngành công nghệ thông tin hiện nay, chúng ta cũng phải bắt kịp sự phát triển của thế giới để có thể tự bảo vệ quyền lợi của bản thân, của quốc gia.

Tuy nhiên do giấu tin mật là vấn đề phức tạp, cộng với khả năng và kinh nghiệm còn hạn chế nên đề tài này không tránh khỏi những thiếu sót, vì vậy em rất mong nhận được sự đóng góp ý kiến của các thầy cô cùng các bạn để báo cáo của chúng em được hoàn thiện hơn.

Em xin chân thành cảm ơn!

Tài liệu tham khảo

1. https://ourcodeworld.com/
2. https://www.hashbangcode.com/
3. https://www.dreamincode.net/
4. https://blog.hoangdoan.io/2014/01/steganography-ky-thuat-che-dau-thong.html
5. https://stackoverflow.com/
6. https://howtodoinjava.com/
7. https://csharphelper.com/
8. https://phpclasses.org/