BỘ GIÁO DỤC VÀ ĐÀO TẠO

TRƯỜNG ĐẠI HỌC DÂN LẬP HẢI PHÒNG

-------o0o-------

# LƯỢC ĐỒ GIẤU TIN DỰA TRÊN HÀM MODULUS

ĐỒ ÁN TỐT NGHIỆP ĐẠI HỌC HỆ CHÍNH QUY

Ngành: Công nghệ Thông tin

Sinh viên thực hiện: Nguyễn Văn Cường

Giáo viên hướng dẫn: TS. Hồ Thị Hương Thơm

Mã số sinh viên: 121303

HẢI PHÒNG 7 - 2012

# LỜI CẢM ƠN

Trước hết em xin bày tỏ lòng biết ơn sâu sắc nhất tới cô giáo hướng dẫn Tiến sỹ Hồ Thị Hương Thơm – giảng viên khoa CNTT trường ĐHDL Hải Phòng là người đã tận tình giúp đỡ em rất nhiều trong suốt quá trình tìm hiểu nghiên cứu và hoàn thành đồ án tốt nghiệp này. Em xin chân thành cảm ơn các thầy cô trong bộ môn công nghệ thông tin – trường DHDL Hải Phòng cũng như các thầy cô trong trường đã trang bị cho em những kiến thức cơ bản cần thiết để em có thể hoàn thành báo cáo. Xin gửi lời cảm ơn đến bạn bè những người luôn bên em đã động viên và tạo điều kiện thuận lợi cho em, tận tình giúp đỡ chỉ bảo em những gì em còn thiếu sót trong quá trình làm báo cáo tốt nghiệp.

Cuối cùng em xin bày tỏ lòng biết ơn sâu sắc tới những người thân trong gia đình đã dành cho em sự quan tâm đặc biệt và luôn động viên em. Vì thời gian có hạn, trình độ hiểu biết của bản thân còn nhiều hạn chế. Cho nên trong đồ án 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 đồ án của em được hoànthiện hơn.

Em xin chân thành cảm ơn!

Hải phòng, ngày  tháng năm 2012

Sinh viên thực hiện

Nguyễn Văn Cường.

# MỤC LỤC

# LỜI MỞ ĐẦU

Ngày nay, cùng với sự phát triển mạnh mẽ của ngành khoa học công nghệ thông tin, internet đã trở thành một nhu cầu, phương tiện không thể thiếu đối với mọi người, việc truyền tin qua mạng ngày càng lớn. Tuy nhiên, với lượng thông tin được truyền qua mạng nhiều hơn thì nguy cơ dữ liệu bị truy cập trái phép cũng tăng lên vì vậy vấn đề bảo đảm an toàn và bảo mật thông tin cho dữ liệu truyền trên mạng là rất cần thiết. Để đảm bảo an toàn và bí mật cho một thông điệp truyền đi người ta thường dùng phương pháp truyền thống là mã hóa thông điệp theo một qui tắc nào đó đã được thỏa thuận trước giữa người gửi và người nhận. Tuy nhiên, phương thức này thường gây sự chú ý của đối phương về tầm quan trọng của thông điệp. Thời gian gần đây đã xuất hiện một cách tiếp cận mới để truyền các thông điệp bí mật, đó là giấu các thông tin quan trọng trong những bức ảnh thông thường. Nhìn bề ngoài các bức ảnh có chứa thông tin cũng không có gì khác với các bức ảnh khác nên hạn chế được tầm kiểm soát của đối phương. Mặt khác, dù các bức ảnh đó bị phát hiện ra là có chứa thông tin trong đó thì với các khóa có độ bảo mật cao thì việc tìm được nội dung của thông tin đó cũng rất khó có thể thực hiện được. Xét theo khía cạnh tổng quát thì giấu thông tin cũng là một hệ mã mật nhằm bảo đảm tính an toàn thông tin, những phương pháp này ưu điểm là ở chỗ giảm được khả năng phát hiện được sự tồn tại của thông tin trong nguồn mang. Không giống như mã hóa thông tin là chống sự truy cập và sửa chữa một cách trái phép thông tin, mục tiêu của giấu thông tin là làm cho thông tin trộn lẫn với các điểm ảnh. Điều này sẽ đánh lừa được sự phát hiện của các tin tặc và do đó làm giảm khả năng bị giải mã. Kết hợp các kỹ thuật giấu tin với các kỹ thuật mã hóa ta có thể nâng cao độ an toàn cho việc truyền tin. Trong đồ án này em đã tìm hiểu một kỹ thuật giấu tin văn bản trong hình ảnh là kỹ thuật giấu tin dựa trên hàm modulus. Đồ án gồm ba chương, trong đó:

Chương 1. Tổng quan về kỹ thuật giấu tin trong ảnh: Định nghĩa giấu thông tin là gì, mục đích của giấu tin, tính chất, phân loại kỹ thuật giấu tin, cấu trúc ảnh Bitmap và phương pháp đánh giá ảnh trước và sau khi giấu tin.

Chương 2. Kỹ thuật giấu tin dựa trên hàm modulus: Giới thiệu và trình bày về kỹ thuật giấu tin, ví dụ minh họa.

Chương 3. Cài đặt và thử nghiệm: Một số giao diện của chương trình, đánh giá và nhận xét về thuật toán.

# *Chương 1.* TỔNG QUAN VỀ KỸ THUẬT GIẤU TIN TRONG ẢNH

## 1.1. Định nghĩa

Giấu thông tin là một kỹ thuật nhúng (giấu) một lượng thông tin số nào đó vào trong một đối tượng dữ liệu số khác (giấu thông tin chỉ mang tính quy ướckhông phải là một hành động cụ thể).

### *1.1.1. Mục đích giấu tin*

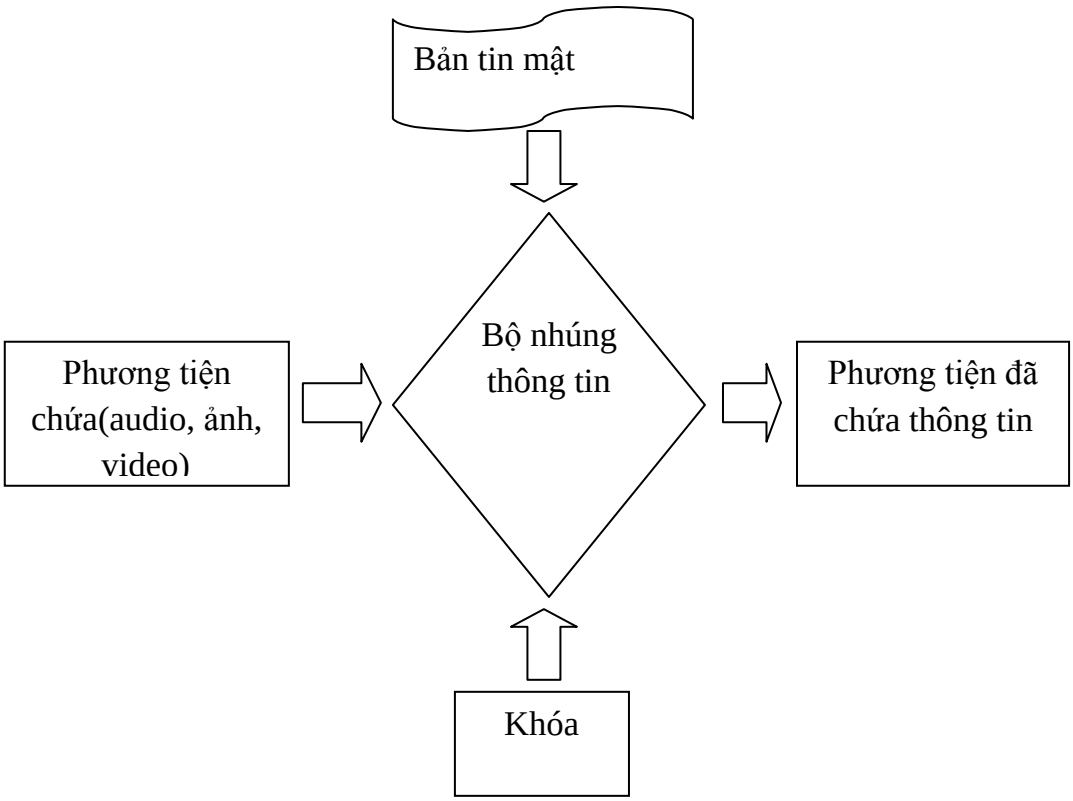
Có hai mục đích của giấu tin:

- Bảo mật cho những dữ liệu được giấu.
- Bảo đảm an toàn (bảo vệ bản quyền) cho chính các đối tượng chứa dữliệu giấu trong đó và phát hiện xuyên tạc thông tin.

### *1.1.2. Các thành phần chính của một hệ thống giấu tin trong ảnh*

Các thành phần chính của một hệ giấu tin trong ảnh số gồm:

- Bản tin mật (Secret Message): có thể là văn bản hoặc tệp ảnh hay bất kỳ một tệp nhịphân nào, vì quá trình xử lý chúng ta đều chuyển chúng thành chuỗi các bit.
- Ảnh phủ (hay ảnh gốc) (Cover Data): là ảnh được dùng để làm môi trường nhúng tin mật.
- Khoá bí mật K (Key): khoá mật tham gia vào quá trình giấu tin để tăng tính bảo mật
- Bộ nhúng thông tin (Embedding Algorithm): những chương trình, thuật toán nhúng tin.
- Ảnh mang (Stego Data): là ảnh sau khi đã chứa tin mật.
- Kiểm định (Control): kiểm tra thông tin sau khi được giải mã.




**Hinh 1. 1**: Lược đồ chung cho quá trình giấu tin.

*1.1.3. Các tính chất giấu tin trong ảnh*

Độ tin cậy: Giấu tin trong ảnh sẽ làm biến đổi ảnh mang. Tính vô hình thể hiện mức độ biến đổi ảnh mang. Một hương pháp tốt sẽ làm cho thông tin mật trở nên vô hình trên ảnh mang, người dùng không thể phát hiện trong đó có ẩn chứa thông tin.

Khả năng chống giả mạo: Vì mục đích của một phương pháp giấu tin là chuyển đi thông tin mật. Nếu không thể do thám tin mật thì kẻ địch cũng sẽ cố tìm cách làm sai lạc thông tin mật, làm giả mạo thông tin để gây bất lợi cho đối phương. Một phương pháp giấu tin tốt sẽ đảm bảo tin mật không bị tấn công một cách có chủ đích trên cơ sở những hiểu biết đầy đủ về thuật toán nhúng tin (nhưng không biết khoá) và có ảnh mang. Đối với lĩnh vực thuỷ vân số thì khả năng chống giả mạo là đặc tính vô cùng quan trọng. Vì có như vậy mới bảo vệ được bản quyền, chứng minh tính pháp lý của sản phẩm.

Dung lượng giấu: Dung lượng giấu được tính bằng tỷ lệ của lượng tin giấu so với kích thước ảnh. Vì tin mật được gửi cùng với ảnh mang qua mạng nên đây cũng là một chỉ tiêu quan trọng. Các phương pháp đều cố làm sao giấu được nhiều tin trong khi vẫn giữ được bí mật. Tuy nhiên trong thực tế người ta luôn phải cân nhắc giữa dung lượng và các chỉ tiêu khác như tính vô hình, tính ổn định.

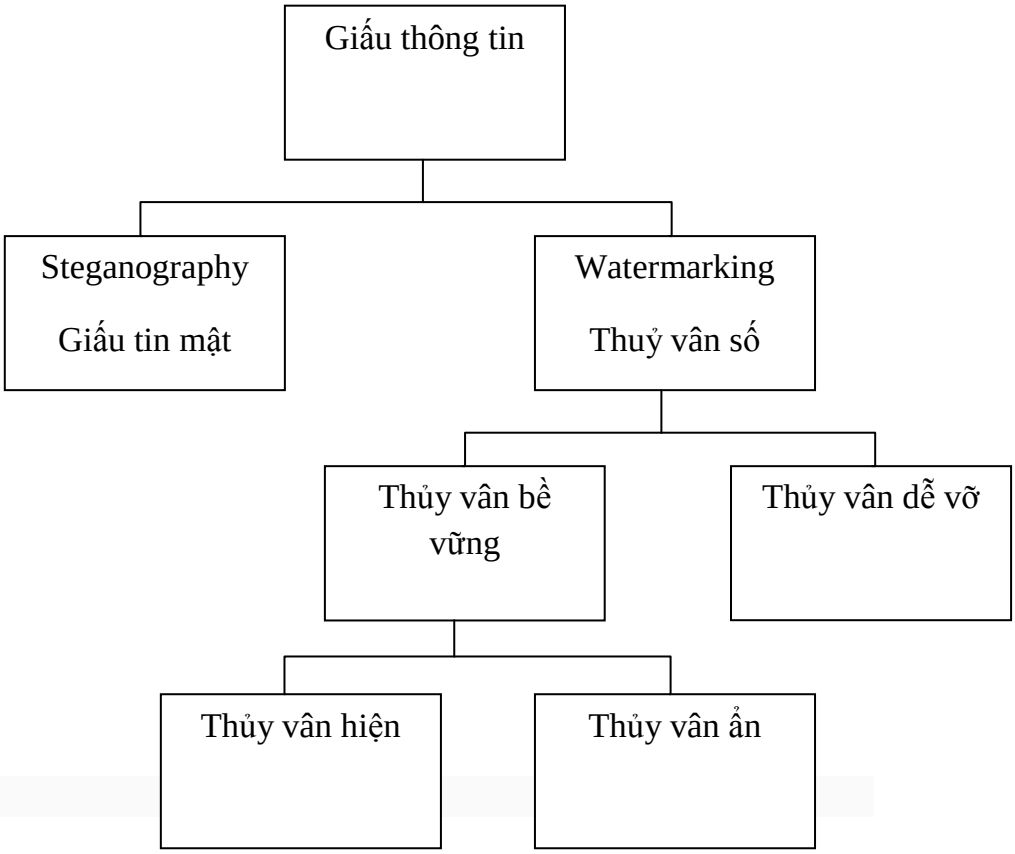
Tính bền vững: Sau khi giấu tin vào ảnh mang, bản thân ảnh mang có thể phải qua các khâu biến đổi khác nhau như lọc tuyến tính, lọc phi tuyến, thêm nhiễu, làm

sắc nét, mờ nhạt, quay, nén mất dữ liệu. Tính bền vững là thước đo sự nguyên vẹn của thông tin mật sau những biến đổi như vậy.

Độ phức tạp của thuật toán: Chỉ tiêu độ phức tạp trong mã hoá và giải mã cũng là một yếu tố quan trọng trong đánh giá các phương pháp giấu tin trong ảnh. Yêu cầu về độ phức tạp tính toán phụ thuộc vào từng ứng dụng. Ví dụ một ứng dụng tạo thuỷ ấnđể đánh dấu bản quyền cần phải có độ phức tạp tính toán cao thì mới đảm bảo chịu được sự tấn công của nhiều tin tặc nhằm phá huỷ thuỷ vân.

*1.1.4. Phân loại các kỹ thuật giấu tin*

- Có thể phân loại kỹ thuật giấu tin ra làm hai:
  + Giấu tin mật (Steganography)
  + Thuỷ vân số (Watermarking)




**Hình1. 2**: Sơ đồ phân loại kỹ thuật giấu tin

+ Giấu tin mật (Seganography) quan tâm tới việc giấu các tin sao cho thông tin giấu được càng nhiều càng tốt và quan trọng là người khác khó phát hiện được một đối tượng có bị giấu tin bên trong hay không bằng kỹ thuật thông thường.
+ Thủy vân số (Watermaking) đánh giấu vào đối tượng nhằm khẳng định bản quyền sở hữu hay phát hiện xuyên tạc thông tin. Thủy vân số được phân thành hai loại: thủy vân bền vững và thủy vân dễ vỡ.

- Thủy vân bền vững(Robust Watermarking): thường được ứng dụng trong các ứng dụng bảo vệ bản quyền. Thuỷ vân được nhúng trong sản phẩm như một hình thức dán tem bản quyền. Trong trường hợp này, thuỷ vân phải tồn tại bền vững cùng với sản phẩm nhằm chống việc tẩy xoá, làm giả hay biến đổi phá huỷ thuỷ vân. Thủy vân bền vững có hai loại:
  - ✓ Thủy vân ẩn (Visible Watermarking): cũng giống như giấu tin, bằng mắt thường không thể nhìn thấy thuỷ vân.
  - ✓ Thuỷ vân hiện(Imperceptible Watermarking): là loại thuỷ vân được hiện ngay trên sản phẩm và người dùng có thể nhìn thấy được.
- Thủy vân dễ vỡ (Fragile Watermarking): là kỹ thuật nhúng thuỷ vân vào trong ảnh sao cho khi phân bố sản phẩm trong môi trường mở nếu có bất cứ một phép biến đổi nào làm thay đổi đối tượng sản phẩm gốc thì thuỷ vân đã được giấu trong đối tượng sẽ không còn nguyên vẹn như trước khi dấu nữa (dễ vỡ).

### 1.1.5. 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.
- Điểm chỉ số.
- Gán nhãn.
- Giấu thông tin mật.

## 1.2. Cấu trúc ảnh Bitmap

Mỗi file ảnh Bitmap gồm 3 phần như bảng 1. 1:

**Bảng 1. 1.** Cấu trúc ảnh BitMap

| Bitmap Header (54 byte) |
|---|
| Color Palette |
| Bitmap Data |

### *1.2.1. Bitmap Header*

Thành phần bitcount (Bảng 1. 2 Thông tin về Bitmap Header) 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

| **Bytethứ** | **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 | Kiểu long trong Turbo C |
| 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<br>1: Nén runlength 8bits/pixel<br>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 hiển<br>thị ảnh (Color Used) | |

1.2.2. *Bitmap Data*

Phần này nằm ngay sau phần Palete màu của ảnh BMP. Đây là phần chứa giá trịmàu của điểm ảnh trong ảnh BMP. Các dòng ảnh được lưu từ dưới lên trên, các

điểmảnh được lưu trữ từ trái sang phải. Giá trị của mỗi điểm ảnh là một chỉ số trỏ tới phầntử màu tương ứng trong Palete màu.

### 1.3. Phương pháp đánh giá ảnh trước và sau giấu tin

PSNR dùng để tính tỉ lệ giữa giá trị năng lượng tối đa của một tín hiệu và năng lượng nhiễu ảnh hướng đến độ chính xác của thông tin. Bởi vì có rất nhiều tín hiệu có phạm vi biến đổi rộng, nên PSNR thường được biểu diễn bởi đơn vị logarit.

Ngoài ra, PSNR còn được sử dụng để đo chất lượng tín hiệu khôi phục của các thuật toán nén có mất mát dữ liệu (lossy compression) (ví dụ: dùng trong nén ảnh). Tín hiệu trong trường hợp này là dữ liệu gốc, và nhiễu là các lỗi xuất hiện khi nén. Khi so sánh các thuật toán nén thường dựa vào sự cảm nhận gần chính xác của con người đối với dữ liệu được khôi phục, chính vì thế trong một số trường hợp dữ liệu được khôi phục của thuật toán này dường như có chất lượng tốt hơn những cái khác, mặc dù nó có giá trị PSNR thấp hơn (thông thường PSNR càng cao thì chất lượng dữ liệu được khôi phục càng tốt).

Cách đơn giản nhất là định nghĩa thông quaMSE được dùng cho ảnh 2 chiều có kích thước m×n trong đó I và K là ảnh gốc và ảnhđược khôi phục tương ứng:

$$\text{MSE} = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}\lfloor I(i,j) - K(i,j)^2 \rfloor$$

Khi đó, PSNR được tính bởi:

$$\text{PSNR} = 10*\log_{10}\left(\frac{MAX_1^2}{MSE}\right) = 20*\log_{10}\left(\frac{MAX_1}{MSE}\right)$$

Ở đây, MAXI là giá trị tối đa của điểm ảnh trên ảnh. Khi các điểm ảnh được biểu diễn bởi 8 bits, thì giá trị của nó là 255. Trường hợp tổng quát, khi tín hiệu được biểu diễn bởi B bits cho một đơn vị lấy mẫu, thì MAXI là 2B−1. Trường hợp ảnh màu với 3 giá trị RGB trên một điểm ảnh, cách tính toán cho PSNR tương tự ngoại trừ việc tính MSE là tổng của 3 giá trị (tính trên 3 kênh màu) chia cho kích thước của ảnh và chia cho 3.

Giá trị thông thường của PSNR trong giấu ảnh và nén video nằm từ 30 đến 50 dB, giá trị càng cao thì càng tốt. Giá trị có thể chấp nhận được khi truyền tín hiệu không dây có tổn thất khoảng từ 20 dB đến 25 dB.

# *Chương 2*. KỸ THUẬT GIẤU TIN DỰA TRÊN HÀM MODULUS

## 2.1. Giới thiệu

Kỹ thuật giấu tin dựa trên hàm chia lấy dư được Chin-Feng Lee và Hsing-Ling Chen giới thiệu vào năm 2010.

Ý tưởng của kỹ thuật giấu tin:

- Đầu tiên, ta sử dụng hai hàm Hr() và Hc() để tạo ra hai tập hợp Kr() và Kc() gồm các phần tử là hoán vị của 0, 1. Chuỗi bit thông điệp Ssẽ được chia thành các chuỗi nhỏ $s_k$để giấu vào từng điểm ảnh.
- Sau đó, mỗi điểm ảnh gốc được giấu tin sẽ tạo ra một nhóm G các điểm ảnh lân cận dựa trên hàm modulus. Ta dựa vào hai tập hợp Kr(), Kc() và các chuỗi nhỏ $s_k$ để xác định vị trí d trong nhóm G. Giá trị của điểm ảnh gốc được giấu tin sẽ được thay đổi bằng giá trị của điểm ảnh tại vị tri d trong nhóm G.

## 2.2. Kỹ thuật giấu tin Modulus

### *2.2.1 Một số khái niệm và hàm phụ trợ*

Hr($R_1$, $\alpha$) tạo ra Kr={$kr_i$ |i =1, 2,.., $2^{\alpha}$} với R1 $\in$ [1, $2^{\alpha}$!], Kr có $2^{\alpha}$! hoán vị.

**Bảng 2. 1**. Bảng hoán vị của Kr với $\alpha$=3

| **$R_1$** | **Hoán vị** |
|---|---|
| 1 | {001, 010, 000, 100, 011, 111, 110, 101} |
| 2 | {000, 111, 100, 011, 010, 101, 110, 001} |
| … | … |
| 40, 320 | {111, 100, 010, 011, 001, 110, 101, 000} |

Hc($R_2$, $\beta$) tạo ra Kc={$kc_j$ |j =1, 2,.., $2^{\beta}$} với R2 $\in$ [1, $2^{\beta}$!], Kc has $2^{\beta}$! hoán vị.

**Bảng 2. 2**. Bảng hoán vị của Kc với β=2

| $R_2$ | **Hoán vị** |
|---|---|
| 1 | {10, 00, 11, 01} |
| 2 | {00, 11, 10, 01} |
| … | … |
| 24 | {11, 01, 00, 10} |

$d = 2^{\beta} \times (i - 1) + j$.

Để nhúng các đoạn sk bí mật, một nhóm G điểm ảnh được tạo ra như sau:

$\{x_i - y, x_i - y + 1, .., x_i, x_i + n - y - 1\}$

Với $y = x_i \bmod n$

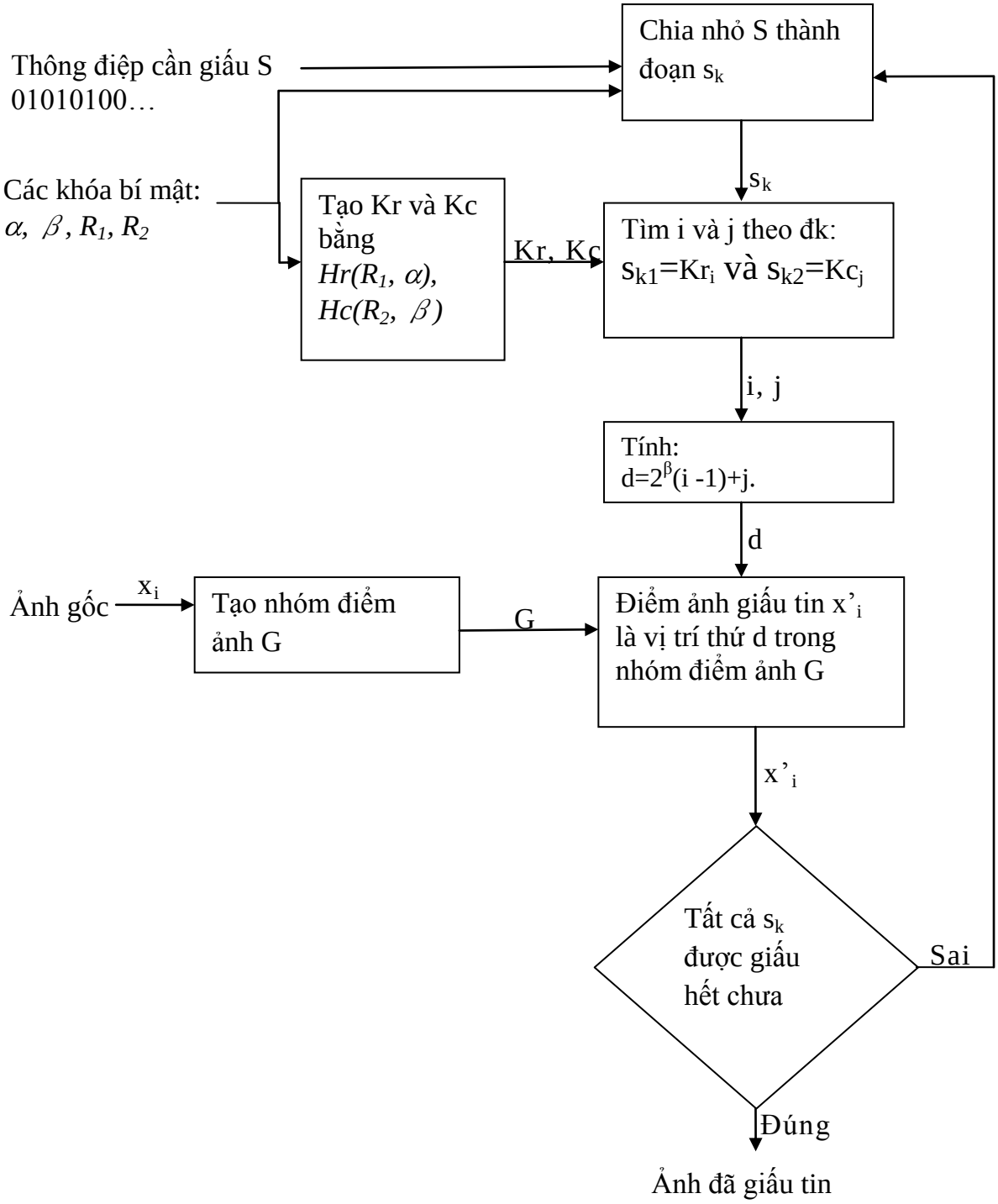
$(n = 2^{\alpha+\beta})$

### *2.2.2 Giấu tin*

Thuật toán:

- Đầu vào: Thông điệp cần giấu S, các khóa: α, β, $R_1$, $R_2$; một ảnh bất kỳ có kích cỡ (m×n).
- Đầu ra: Ảnh có chứa thông điệp S.
- Các bước thực hiện:
  - + Bước 1: Chia nhỏ S thành các sk có độ dài α + β.
  - + Bước 2: Tạo Kr và Kc từ Hr($R_1$, α) và Hc($R_2$, β).
  - + Bước 3: Tìm i và j theo điều kiện: $s_{ki} = Kr_i$ và $s_{kj} = Kc_j$
  - + Bước 4: Tính: $d = 2^{\beta} \times (i - 1) + j$.
  - + Bước 5: Tạo một nhóm điểm ảnh G từ ảnh đầu vào với công thức: $f(x_i) = x_i \bmod n$ (với $n = 2^{\alpha + \beta}$) và có được điểm ảnh giấu tin x'i là vị trí thứ d trong nhóm điểm ảnh G
  - + Bước 6: Lặp lại bước 3-5 cho đến khi tất cả các chuỗi thông điệp được giấu. Kết quả: Ta được ảnh đã giấu tin.

Sơ đồquá trình giấu tin:




**Hình 2. 1.** Sơ đồ giấu tin bằng thuật toán modulus

### *2.2.3 Tách tin*

Mô tả quá trình tách tin:

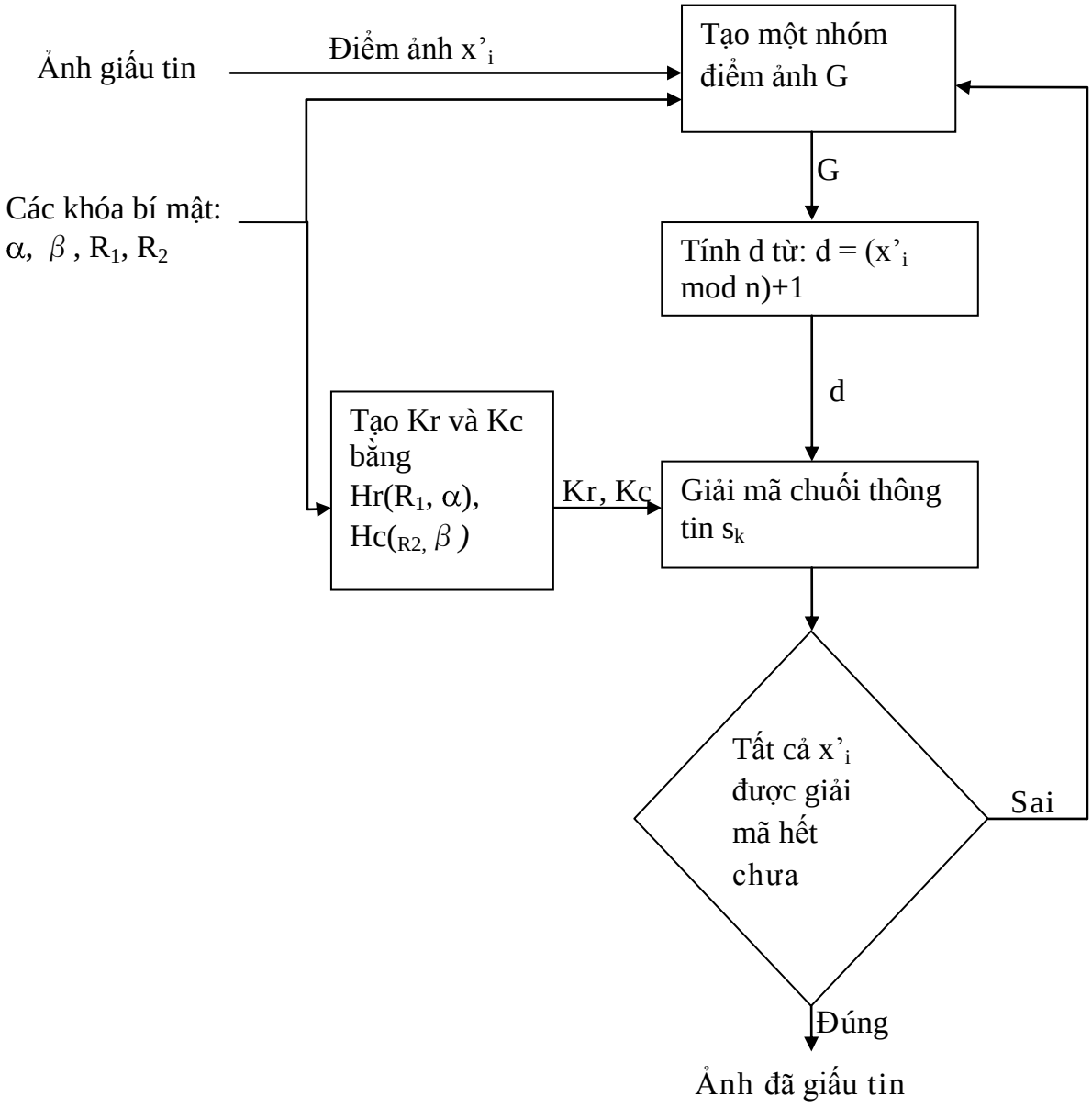
- Đầu tiên, hai tập hợp Kr và Kc được tạo ra bằng Hr(R1, $\alpha$) và Hc(R2, $\beta$). Điểm ảnh giấu tin $x'_i$ sẽ tạo ra nhóm điểm ảnh G và từ đó tính $d = (x'_i \bmod n)+1$ (với $n=2^{\alpha+\beta}$, $x'_i$ thuộc G).

- Với Kr, Kc và d ta xác định được chuỗi bit thông điệp chính là thành phần vị trí thứ d trong tập hợp Kr × Kc.

Thuật toán:

- Đầu vào: Các khóa: $\alpha$, $\beta$, $R_1$, $R_2$; một ảnh giấu tin dựa trên hàm modulus.
- Đầu ra:Thông điệp giấu.
- Các bước thực hiện:
  - Bước 1: Tạo Kr và Kc từ Hr($R_1$, $\alpha$) và Hc($R_2$, $\beta$).
  - Bước 2: Tạo một nhóm điểm ảnh G từ ảnh đầu vào và tính $d = (x'_i \bmod n)+1$ (với $n=2^{\alpha+\beta}$, $x'_i$ thuộc G)
  - Bước 3: Lấy phần tử thứ d là đoạn thông điệp với ($\alpha+\beta$) bit từ Kr × Kc.
  - Bước 4: Lặp lại bước 2 và 3 cho đến khi tất cả các điểm ảnh có giấu tin được duyệt hết.
  - Bước 5: Ghép lại tất cả các mảnh thông điệp thành một thông điệp hoàn chỉnh. Kết thúc.

Sơ đồ quá trình tách tin:




**Hình 2. 2.** Sơ đồ tách tin

## 2.3. Ví dụ

### *2.3.1 Giấu tin*

Ta sử dùng bốn điểm ảnh gốc là: 25, 78, 0 và 255 để giấu 1 chuỗi bits: S = "0100010111011100". Giả sử $R_1 = 12$, $R_2 = 9$, $\alpha = 2$, $\beta = 2$.

Chuỗi S sẽ được chia thành các phần nhỏ sk, mỗi phần có độ dài 4 bits vì $\alpha + \beta = 4$: S="0100 0101 1101 1100".

Từ Hr(12, 2) => Kr = {11, 01, 00, 10 }và Hc(9, 2) => Kc = {00, 11, 10, 01}.

Với chuỗi bits đầu tiên $s_k$ = "0100" được giấu vào điểm ảnh $x_1 = 25$ ta xác định được i = 2 và j = 1, vì "01" là vị trí thứ 2 của Kr và "00" là vị trí đầu tiên của Kc. Từ đó, ta tính được $d=2^{\beta}\times(i -1) + j = 2^2\times(2 -1) + 1 = 5$.

Một nhóm điểm ảnh được tạo ra bằng công thức: $f(x_i) = x_i \mod n$ (với $n = 2^{\alpha + \beta}$). Với $x_1 = 25$ thì nhóm điểm ảnh $G_1$ sẽ nằm trong đoạn từ 16 đến 31. $g_{10} = 25$.

**Bảng 2. 3.** Nhóm điểm ảnh G1.

| **Giá trị** | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Vị trí** | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |

Điểm ảnh giấu tin sẽ là vị trí thứ d = 5 trong nhóm điểm G1 =>$x'_i = g_5 = 20$.

**Bảng 2. 4.** Nhóm điểm ảnh G1.

| **Giá trị** | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Vị trí** | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |

Tương tự, các điểm ảnh còn lại: 78, 0 và 255. Các chuỗi nhị phân còn lại được chia thành: “0101”, ” 1101” và “1100” và giá trị d có thể được tính tương ứng: 4×(2 - 1) + 4 = 8, 4×(1 - 1) + 4 = 4 và 4×(1 -1) + 1 = 1.

Từ $G_2$, $G_3$ và $G_4$ ta xác định được ba điểm ảnh giấu tin tương ứng với điểm ảnh gốc 78, 0 và 255 là: 71, 3 và 240.

$G_2$

| Giá trị | 64 | 65 | 66 | 67 | 68 | 69 | 70 | 71 | 72 | 73 | 74 | 75 | 76 | 77 | 78 | 79 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Vị trí | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |

$G_3$

| Giá trị | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Vị trí | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |

$G_4$

| Giá trị | 240 | 241 | 242 | 243 | 244 | 245 | 246 | 247 | 248 | 249 | 250 | 251 | 252 | 253 | 254 | 255 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Vị trí | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |

**Hình 2. 3.** Nhóm điểm ảnh $G_2$, $G_3$ và $G_4$

### *2.3.1 Tách tin*

Ta giải mã điểm ảnh giấu tin: $x'_i = 53$. Giả sử $R_1 = 12$, $R_2 = 9$, $\alpha = 2$, $\beta = 2$.

Từ Hr(12, 2) => Kr = {11, 01, 00, 10 } và Hc(9, 2) => Kc = {00, 11, 10, 01} => Kr × Kc = {1100, 1111, 1110, 1101, 0100, 0111, 0110, 0101, 0000, 0011, …, 1001}.

Một nhóm điểm ảnh được tạo ra bằng công thức: $f(x_i) = x_i \mod n$ (với $n = 2^{\alpha + \beta}$). Với $x'_i = 53$ thì nhóm điểm ảnh $G'_1$ sẽ nằm trong đoạn từ 48 đến 63.

**Bảng 2. 5**. Nhóm điểm ảnh $G'_1$.

| **Giá trị** | 48 | 49 | 50 | 51 | 52 | 53 | 54 | 55 | 56 | 57 | 58 | 59 | 60 | 61 | 62 | 63 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Vị trí** | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |

Tính được $d = (x'_i \mod n) + 1 = (53 \mod 16) + 1 = 6$.

Chuỗi bits thông điệp được tìm là: "0111" là vị trí thứ 6 của Kr x Kc.

# *Chương 3.* ***CÀI ĐẶT VÀ THỬ NGHIỆM.***

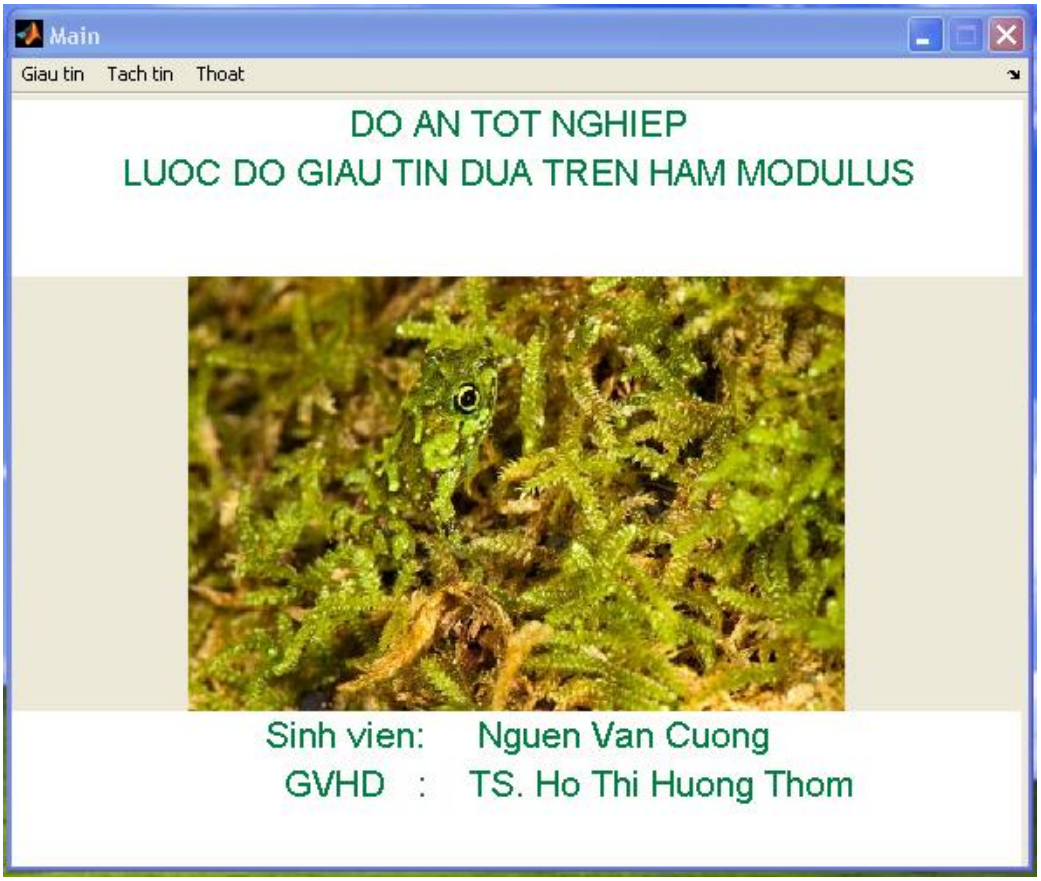
## 3.1. Môi trường cài đặt

Ngôn ngữ cài đặt: là ngôn ngữ lập trình Matlab 7. 0.

Môi trường soạn thảo: Matlab 7. 0.

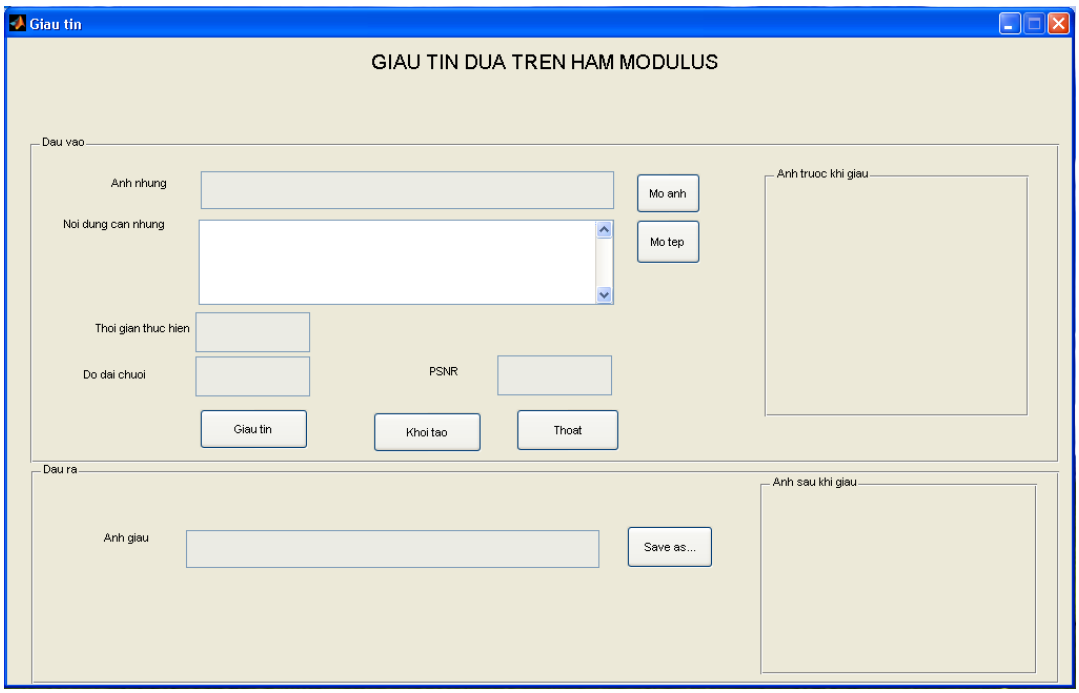
Môi trường chạy chương trình: môi trường giao diện Matlab 7. 0.

## 3.2. Giao diện chương trình

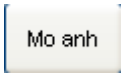


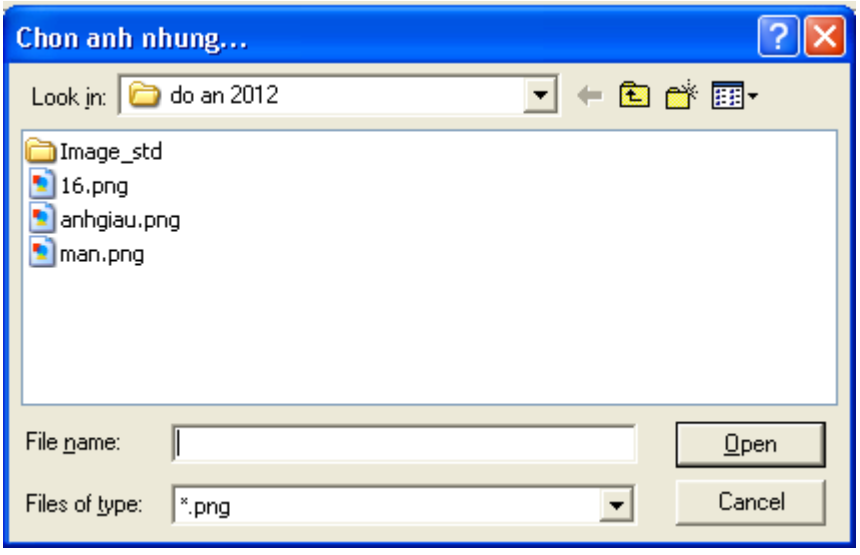

**Hình 3. 1.** Giao diện chính của chương trình.

*3. 2. 1. Một số giao diện giấu tin*



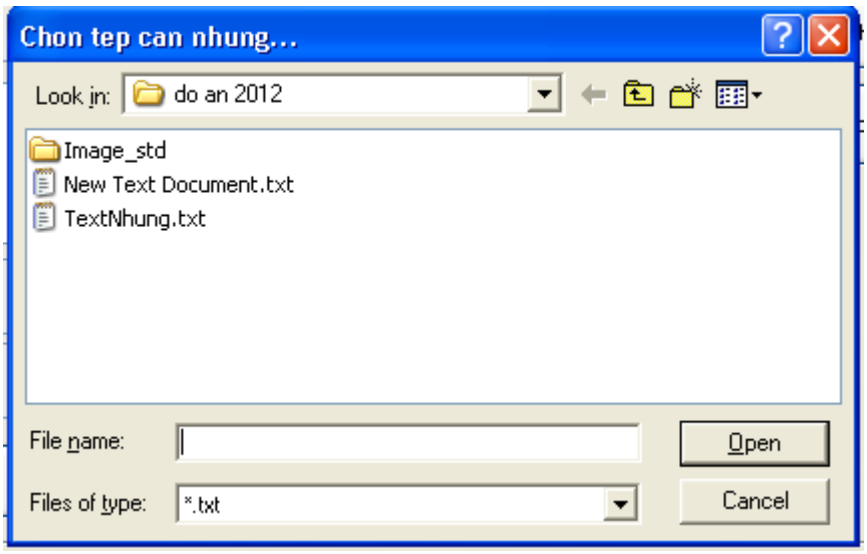

**Hình 3. 2.** Giao diện giấu 1 đoạn tin do người dùng nhập từ file text(trước khi nhập thông tin).

Từ giao diện giấu tin ta chọn vào  để tìm ảnh cần giấu.

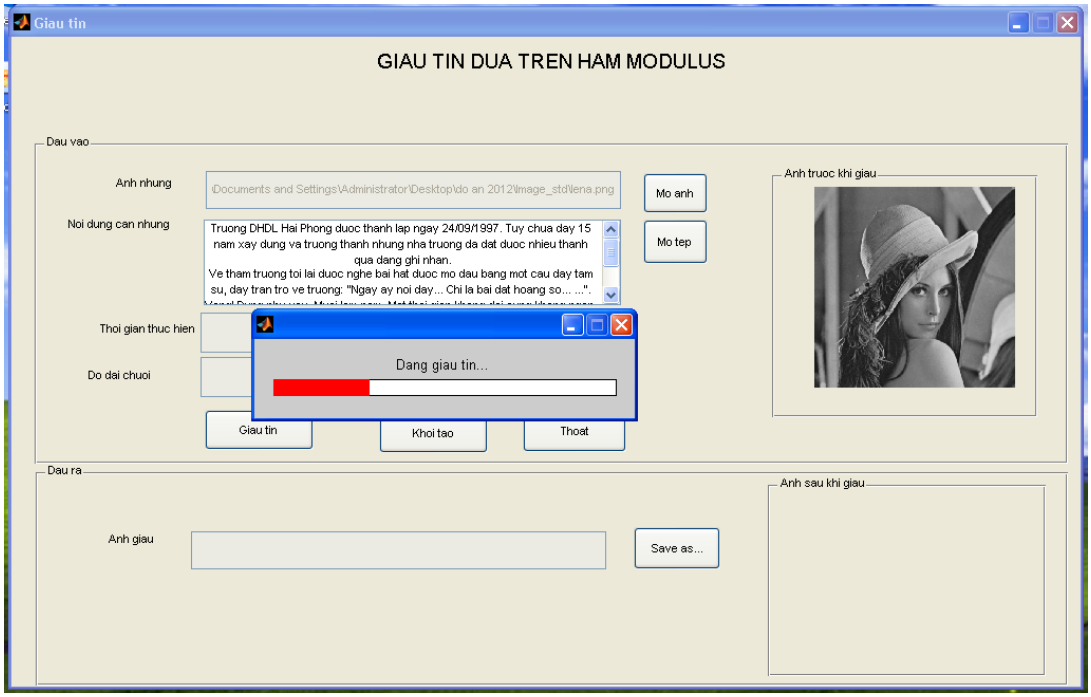

**Hình 3. 3.** Giao diện chọn ảnh gốc.

Sau đó, ta chọn vào  để tìm file text chứa nội dung cần giấu, hoặc nhập vào chuỗi thông điệp cần giấu vào ô.

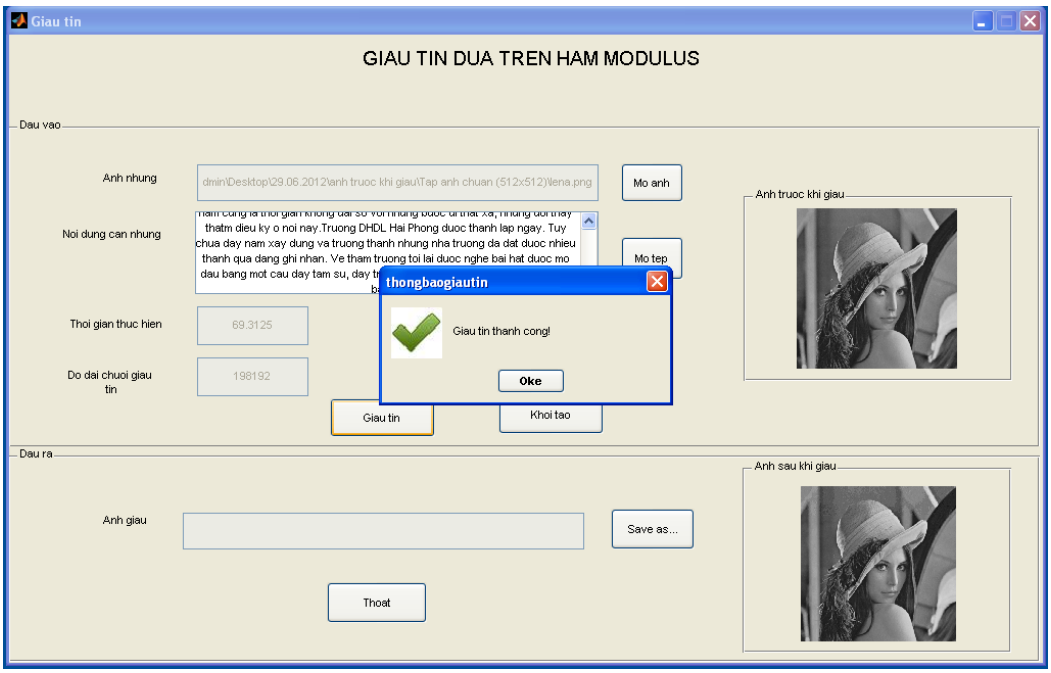



**Hình 3. 4** Giao diện chọn tệp văn bản cần nhúng.

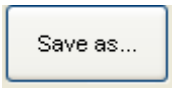
Click vào nút  để bắt đầu quá trình giấu tin.

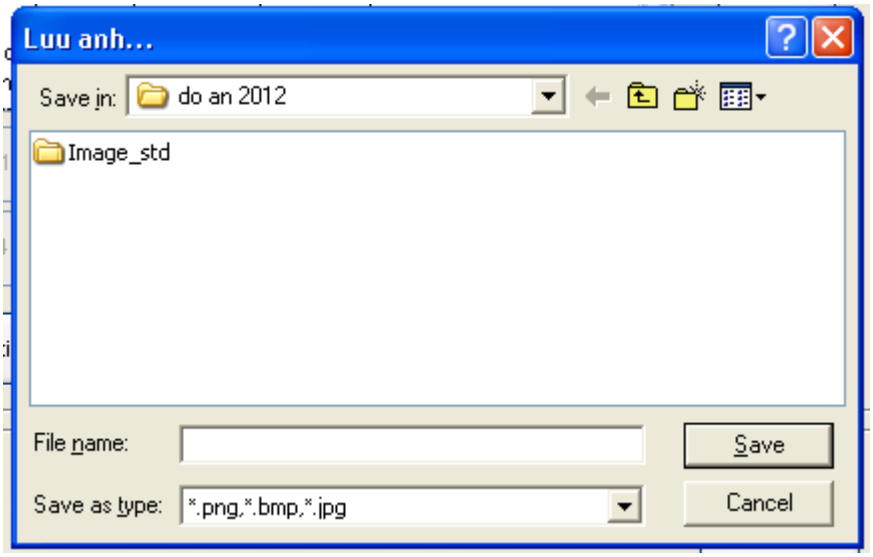

**Hình 3. 5.** Giao diện giấu 1 đoạn tin do người dùng nhập từ file text(sau khi nhập thông tin)




**Hình 3. 7.** Giao diện sau khi giấu tin thành công.

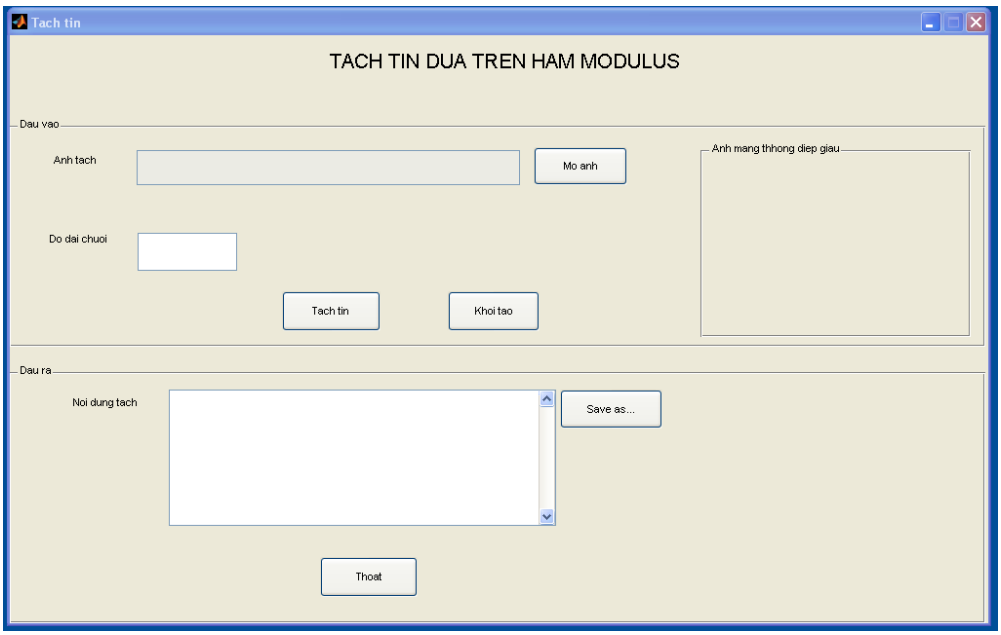
Sau khi giấu tin xong chon nút  để lưu ảnh đã giấu tin.






**Hình 3. 8.** Giao diện chọn nơi lưu ảnh đã mang thông tin giấu.

*3. 2. 2. Một số giao diện tách tin*



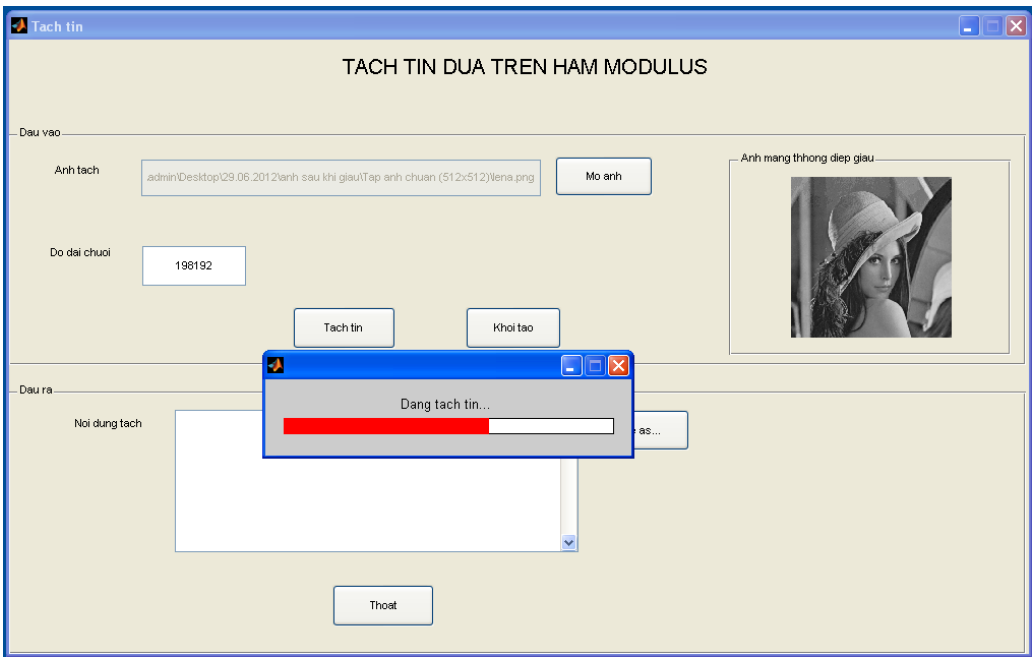

**Hình 3. 9.** Giao diện tách một ảnh giấu tin(trước khi nhập thông tin).

Từ giao diện giấu tin ta chọn vào  để tìm ảnh cần tách.

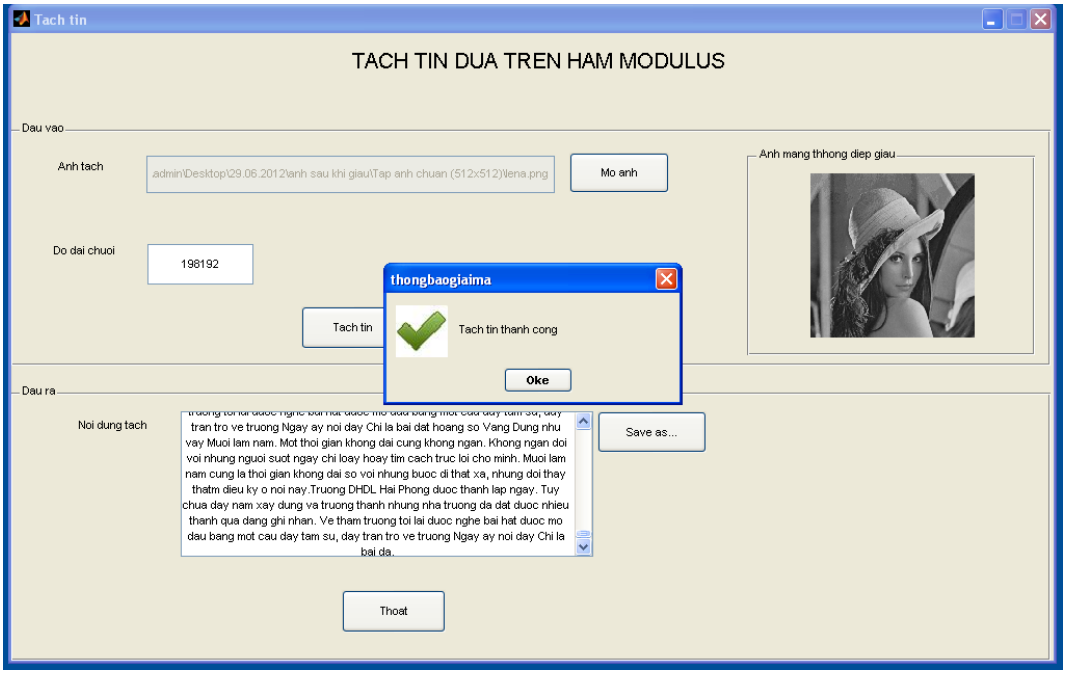


**Hình 3. 10.** Giao diện chọn ảnh tách tin.

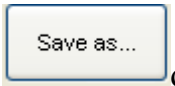
Click vào nút  để bắt đầu quá trình giải mã.




**Hình 3. 11.** Giao diện đang tách một ảnh chứa thông tin.




**Hình 3. 12.** Giao diện táchmột ảnh giấu tin(Sau khi thành công).

Sau khi giấu tin xong chọn nút 

để lưu thông điệp giải mã được ra file text.

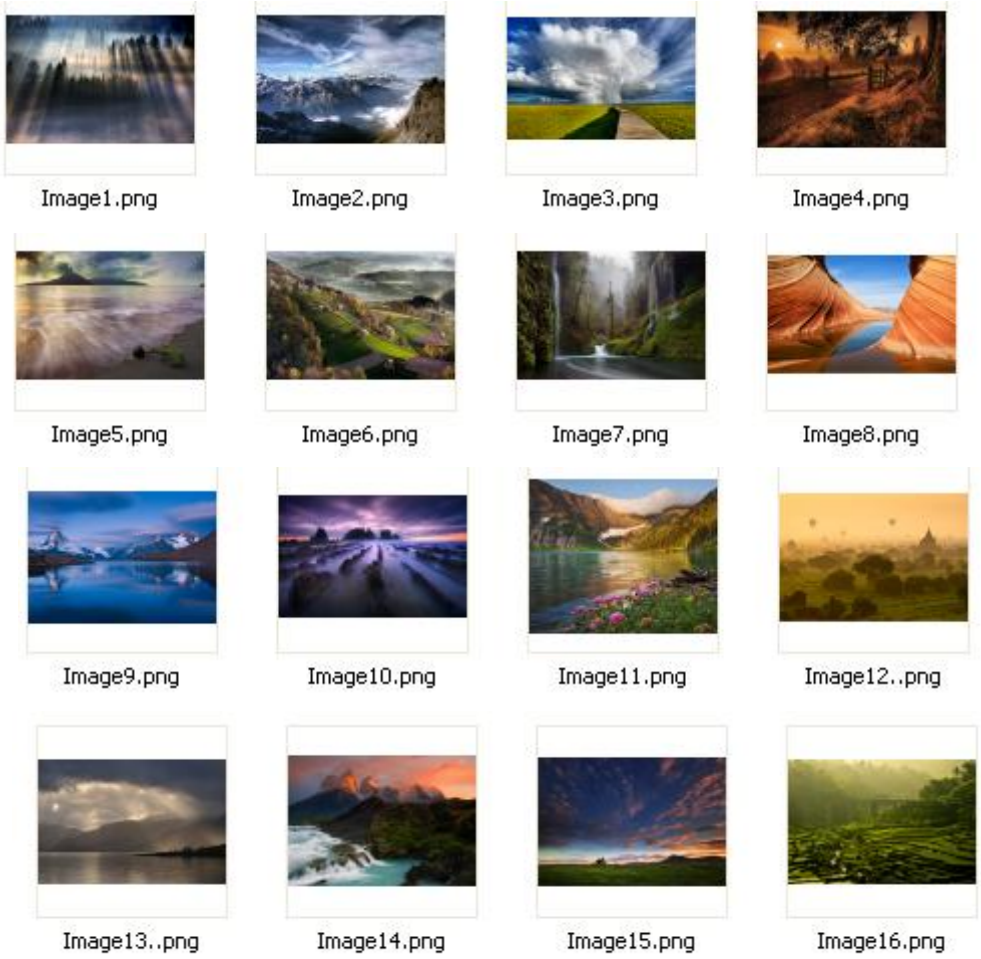
## 3.3 . Đánh giá kỹ thuật.

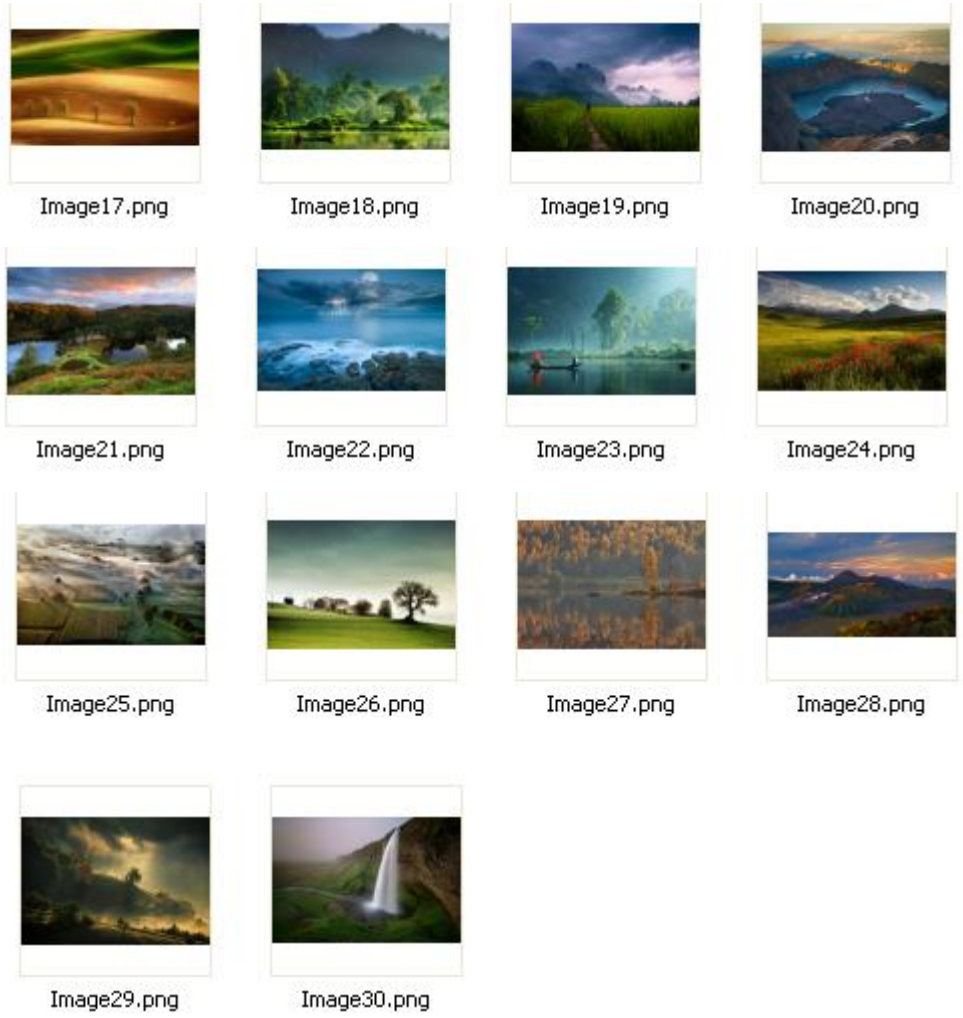
### *3.3.1. Kết quả thực nghiệm.*

Tập ảnh thử nghiệm D1 gồm 9 ảnh cấp xám chưa giấu tin kích cỡ 512 x 512. (hình 3. 13)


**Hình 3. 13.** Tập ảnh thử nghiệm D1.

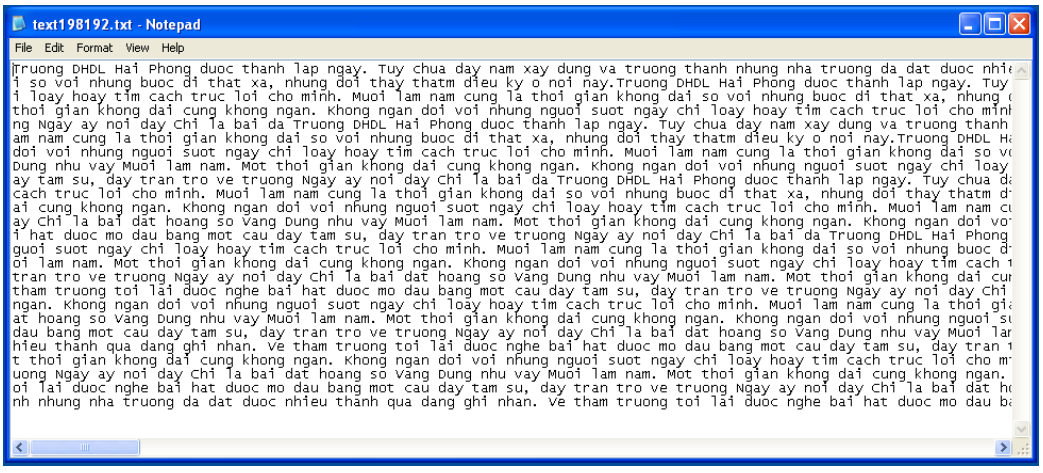
Tập ảnh thử nghiệm D2 gồm 30 ảnh màu ngẫu nhiên được tải về trên internet được đặt tên từ Image1.png đến Image30.png. (hình 3. 14)






**Hình 3. 14.** Tập ảnh thử nghiệm D2(30 ảnh màu bất kỳ).

Chuỗi thông điệp giấu có độ dài 192192 bit:




**Hình 3. 15.** Chuỗi thông điệp giấu.

### 3.3.2. *Độ đo đánh giá*

**Bảng 3. 1.** Độ đo PSNR của tập ảnh thử nghiệm D1.

| Tên ảnh | PSNR | Số bit nhúng | Thời gian nhúng (giây) |
|---|---|---|---|
| airplane. png | 40. 40 | 198192 | 139. 38 |
| baboon. png | 40. 38 | 198192 | 127. 52 |
| beer. png | 40. 22 | 198192 | 128. 13 |
| elaine. png | 40. 38 | 198192 | 127. 36 |
| house. png | 39. 46 | 198192 | 129. 73 |
| lena. png | 40. 30 | 198192 | 127. 44 |
| man. png | 52. 23 | 198192 | 127. 22 |
| peppers. png | 40. 45 | 198192 | 129. 30 |
| Sailboat. png | 40. 13 | 198192 | 128. 61 |
| **Trung bình** | **41. 55** | **198192** | **129. 41** |

**Bảng 3. 2.** Độ đo PSNR của tập ảnh thử nghiệm D2.

| Tên ảnh | PSNR | Số bit nhúng | Thời gian nhúng (giây) |
|---|---|---|---|
| Image1.png | 40. 40 | 198192 | 139. 38 |
| Image2.png | 40. 38 | 198192 | 127. 52 |
| Image3.png | 40. 22 | 198192 | 128. 13 |
| Image4.png | 40. 38 | 198192 | 127. 36 |
| Image5.png | 39. 46 | 198192 | 129. 73 |
| Image6.png | 40. 30 | 198192 | 127. 44 |
| Image7.png | 52. 23 | 198192 | 127. 22 |
| Image8.png | 40. 45 | 198192 | 129. 30 |
| Image9.png | 40. 13 | 198192 | 128. 61 |
| Image10.png | 40.24 | 198192 | 129. 30 |
| Image11.png | 40.56 | 198192 | 127.34 |
| Image12.png | 38.26 | 198192 | 128.63 |
| Image13.png | 38.96 | 198192 | 128. 30 |

| | | | |
|---|---|---|---|
| Image14.png | 38.22 | 198192 | 123. 30 |
| Image15.png | 38.79 | 198192 | 122. 30 |
| Image16.png | 39.79 | 198192 | 121. 30 |
| Image17.png | 39.02 | 198192 | 125.90 |
| Image18.png | 39.78 | 198192 | 129. 30 |
| Image19.png | 37.89 | 198192 | 128. 30 |
| Image20.png | 37.89 | 198192 | 129. 30 |
| Image21.png | 37.28 | 198192 | 125.36 |
| Image22.png | 39.45 | 198192 | 127.31 |
| Image23.png | 45.36 | 198192 | 128.34 |
| Image24.png | 48.67 | 198192 | 125.15 |
| Image25.png | 39.48 | 198192 | 127.26 |
| Image26.png | 39.78 | 198192 | 127.96 |
| Image27.png | 49.59 | 198192 | 125.24 |
| Image28.png | 38.49 | 198192 | 124.56 |
| Image29.png | 39.74 | 198192 | 128.45 |
| Image30.png | 40.26 | 198192 | 128.25 |
| **Trung bình** | **40.36** | **198192** | **126.90** |

*3.3.3. Nhận xét*

Khả năng giấu tin được điều chỉnh phụ thuộc vào chỉ số n = $2^{\alpha+\beta}$, nghĩa là khả năng giấu tin có thể được điều chỉnh tùy thuộc vào yêu cầu củaứng dụng có liên quan. Nếu n càng lớn thì khả năng giấu tin sẽ được nhiều hơn, vì sốlượng bit được giấu vào một điểm ảnh sẽ nhiều hơn. Sự khác biệt về giá trịgiữa điểm ảnh gốc và điểm ảnh giấu tin sẽ nằm trong khoảng giá tri$\{x-(x-\gamma),(x+n-\gamma-1)-x\}=\{\gamma,n-\gamma-1\}$; do đó, trường hợp tốt nhất khigiấu tin là không có điểm ảnh nào bị thay đổi, và trường hợp xấu nhất là số các điểm ảnh bị thay đổi là n – 1. Vì sự thay đổi giá trị của điểm ảnh gốc là nhỏ lên ảnh giấu tin nhận được sẽ khó nhận được bằng mắt thường.

Chúng ta sử dụng một hàm modulus đơn giản, nên quá trình giấu tin và tách tin mất ít không gian nhớ và độ phức tạp nhỏ. Ví dụ trong sơ đồ giấu tin ở hình 2. 1 ta có thể đánh giá được độ phức tạp như sau:

**Bảng 3. 3.**Độ phức tạp của thuật toán

| Các bước | Độ phức tạp |
|---|---|
| Tìm i và j | O(c) |
| Tính d | O(c) |
| Tạo nhóm điểm ảnh G | O(c) |
| Tìm điểm ảnh giấu tin x'i | O(c) |

Ta nhận thấy độ phức tạp chỉ bằng O(c) nên kỹ thuật giấu tin dựa trên hàm modulus rất hiệu quả. Ngoài ra, chúng ta chỉ sử dụng$C \times (\alpha \times 2^{\alpha} + \beta \times 2^{\beta})$ bit của bộ nhớ để lưu trữ Kr và Kc trong suốt quá trình giấu hoặc tách tin diễn ra; trong đó, C là số kênh trong ảnh gốc. Ví dụ: cho một ảnh cấp xám (C = 1), α = 1 và β = 3 thì chỉ sử dụng $1 \times (1 \times 2^1 + 3 \times 2^3) = 24$ bit của bộ nhớ để lưu trữ Krvà Kc.

Các khóa bí mật được sử dụng để bảo vệ sự an toàn trước những xâm hại. Người nhận phải có cùng một hàm thiết lập hàm Hr() và Hc() và phải biết được giá trị của các khóa: $R_1$, $R_2$, α, β. Ví dụ, trong khi tách tin (hình 2. 2) giá trị d được tính từ nhóm G sử dụng điểm ảnh giấu tin x'i. Chuỗi thông tin mật được tách ra chính là vị trí thứ d của Kr × Kc. Mà Kr và Kc lại có $2^{\alpha}!$ và $2^{\beta}!$ trường hợp, vậy Kr × Kc có $2^{\alpha}! \times 2^{\beta}!$ trường hợp. Vì vậy, người dùng khác muốn xâm hại và tách tin khi không có khóa bí mật là rất khó khắn. Nên giấu tin dựa trên hàm modulus rất an toàn và có tính bảo mật cao.

Các vấn đề về tràn trên hoặc tràn dưới không xảy ra với bất kỳ ảnh gốc nào. Giả sử rằng cường độ T của điểm ảnh gốc được xác định trong một miền màu xám 8 bit và một điểm ảnh gốc $x_i$, G ⊆ T có giá trị trong khoảng $\{x_i - y, x_i - y + 1,.., x_i, x_i + n - y - 1\}$. Với bất kỳ giá trị nào của điểm ảnh $x_i$ thì điểm ảnh giấu tin $x'_i$ luôn nằm trong nhóm điểm ảnh G. Vì G ⊆ T và giá trị của T luôn nằm trong đoạn [0, 255] nên mỗi giá trị của G cũng không nằm ngoài đoạn [0, 255]. Vì vậy, các điểm ảnh giấu tin sẽ không vượt quá 255 hoặc nhỏ hơn 0.

# KẾT LUẬN

Giấu tin trong dữ liệu đa phương tiện, đặc biệt là trong ảnhsố là một vấn đề đang được quan tâm hiện nay trong nhiều lĩnh vực. Để giấu thông tin vào một ảnh số nào đó đòi hỏi rất nhiều yếu tố và kỹthuật phức tạp.

Trong đồ án này đã đưa ra một cái nhìn tổng quan về giấu tin trong ảnh dựa trên hàm modulus.

Trong thời gian làm đồ án em đã nghiên cứu và phát hiện kỹ thuật giấu tin dựa trên hàm modulus có thể thỏa mãn bốn tiêu chuẩn thường được dùng để đánh giá hiệu xuất của lược đồ giấu tin, đó là:

- Khả năng giấu.
- Chất lượng hình ảnh sau khi giấu tin tốt.
- Giấu tin hoặc táchtin độ phức tạp nhỏ và đòi hỏi ít không gian bộ nhớ.
- Có khả năng bảo mật.
- Các vấn đề tràn trên hoặc tràn dưới không xảy ra với bất kỳ kiểu ảnh nào.

Trong quá trình làm đồ án, do hạn chế về thời gian nên việc nghiên cứu đề tàikhông thể tránh khỏi những thiếu sót. Rất mong nhận được sự đóng góp ý kiến củacác thầy, cô và toàn thể các bạn đồng môn để báo cáo của em được hoàn thiện hơn.

Em xin chân thành cảm ơn!

## TÀI LIỆU THAM KHẢO


[1]. Nguyễn Xuân Huy, Trần Quốc Dũng, "***Giáo trình giấu tin và thuỷ vân ảnh, Trung tâm thông tin tư liệu***", TTKHTN - CN 2003

[2]. Ingemar Cox, Jeffrey Bloom, Matthew Miller, Ton Kalker, "***Jessica Fridrich, Digital Watermarking and Steganography***", Morgan Kaufmann, 2008.

[3]. Chin – Feng Lee, Hsing – Ling Chen, *A novel data hiding scheme based on modulus function*, The Journal of Systems and Software 83 (2010), pp. 832 – 843.

*Một số đồ án tốt nghiệp ngành CNTT từ khóa 7 đến khóa 11 liên quan đến kỹ thuật giấu tin và phát hiện ảnh có giấu tin*:

[4]. Dương Uông Hiên - lớp CT701, "***Nghiên cứu kỹ thuật giấu tin mật trên vùng biến đổi DWT***", tiểuán tốt nghiệp ngành CNTT – 2008.

[5]. Ngô Minh Long – Lớp CT701, "***Phát hiện ảnh có giấu tin trên Bit ít ý nghĩa nhất LSB***", tiểu án tốt nghiệp ngành CNTT – 2008.

[6]. Đỗ Trọng Phú – CT702, "***Nghiên cứu kỹ thuật giấu tin trên miềm biến đổi DFT***", tiểu án tốt nghiệp ngành CNTT – 2008.

[7]. Hoàng Thị Huyền Trang – CT802, "***Nghiên cứu kỹ thuật phát hiện ảnh giấu tin trên miền biến đổi của ảnh***", đồ án tốt nghiệp ngành CNTT – 2008.

[8]. Nguyễn Thị Kim Cúc – CT801, "***Nghiên cứu một số phương pháp bảo mật thông tin trước khi giấu tin trong ảnh***", đồ án tốt nghiệp ngành CNTT – 2008.

[9]. Vũ Tuấn Hoàng – CT801, "***Nghiên cứu kỹ thuật phát hiện ảnh có giấu tin dựa trên LSB của ảnh cấp xám***", đồ án tốt nghiệp ngành CNTT – 2008.

[10]. Vũ Thị Hồng Phương – CT801, "***Nghiên cứu kỹ thuật giấu tin trong ảnh gif***", đồ án tốt nghiệpngành CNTT – 2008.

[11]. Đỗ Thị Nguyệt – CT901, "***Nghiên cứu một số kỹ thuật ước lượng độ dài thông điệp giấu trên bit có trọng số thấp***", đồ án tốt nghiệp ngành CNTT – 2009.

[12]. Mạc như Hiển – CT901, "***Nghiên cứu kỹ thuật giấu thông tin trong ảnh GIF***", đồ án tốt nghiệp ngành CNTT – 2009.

[13]. Phạm Thị Quỳnh – CT901, "***NGHIÊN CỨU KỸ THUẬT PHÁT HIỆN THÔNG TIN ẨN GIẤU TRONG ẢNH JPEG2000***", đồ án tốt nghiệp ngành CNTT – 2009.

[14]. Phạm Thị Thu Trang – CT901, "***Nghiên cứu kỹ thuật giấu thông tin trong ảnh JPEG2000***", đồ án tốt nghiệp ngành CNTT – 2009.

[15]. Trịnh Thị Thu Hà – CT901, "***Nghiên cứu kỹ thuật phát hiện thông tin ẩn giấu trong ảnh GIF***", đồ án tốt nghiệp ngành CNTT – 2009.

[16]. Vũ Trọng Hùng – CT801, "***Kỹ thuật giấu tin thuận nghịch dựa trên miền dữ liệu ảnh***", tiểu án tốt nghiệp ngành CNTT – 2009.

[17]. Đỗ Lâm Hoàng – CT1001, "***Nghiên cứu kỹ thuật giấu tin thuận nghịch trên miền dữ liệu ảnh cấp xám***", đồ án tốt nghiệp ngành CNTT – 2010.

[18]. Nguyễn Trường Huy- CT1001, "***Nghiên cứu kỹ thuật giấu tin trênảnh nhị phân***", đồ án tốt nghiệp ngành CNTT – 2010.

[19]. Vũ Văn Thành- CT1001, " ***Tìm hiểu giải pháp và công nghệ xác thực điện tử sử dụng thủy vân số***", đồ án tốt nghiệp ngành CNTT – 2010.

[20]. Vũ Văn Tập – CT1001, "***Nghiên cứu kỹ thuật phát hiện ảnh có giấu tin trên miền dữ liệu của ảnh***", đồ án tốt nghiệp ngành CNTT – 2010.

[21]. Vũ Khắc Quyết – CT1001, "***Nghiên cứu kỹ thuật giấu tin với dung lượng thông điệp lớn***", đồ án tốt nghiệp ngành CNTT – 2010.

[22]. Phạm Quang Tùng – CT1001, "***Tìm hiểu kỹ thuật phát hiện ảnh có giấu tin dựa trên phân tích tương quan giữa các bit LSB của ảnh***", đồ án tốt nghiệp ngành CNTT – 2010.

[23]. Vũ Thị Ngọc – CT1101, "***Nghiên cứu một giải pháp giấu văn bản trong ảnh***", đồ án tốt nghiệp ngành CNTT – 2011.

[24]. Cao Thị Nhung – CT1101, "***Tìm hiểu kỹ thuật thủy vân số thuận nghịch cho ảnh nhị phân***", đồ án tốt nghiệp ngành CNTT – 2011.

[25]. Hoàng Thị Thuy Dung – CT1101, "***Kỹ thuật giấu tin trong ảnh dựa trên MBNS (Multiple Base Notational System)***", đồ án tốt nghiệp ngành CNTT – 2011.

[26]. Vũ Thùy Dung – CT1101, "***Kỹ thuật giấu tin trong ảnh SES (Steganography Evading Statistical analyses)***", đồ án tốt nghiệp ngành CNTT – 2011.

[27]. Trịnh Văn Thành – CT1101, "***Phát hiện ảnh có giấu tin trên LSB bằng phương pháp phân tích cặp mẫu***", đồ án tốt nghiệp ngành CNTT – 2011

[28]. Phạm Văn Đại – CT1101, "***Kỹ thuật giấu tin dựa trên biến đổi Contourlet***", đồ án tốt nghiệp ngành CNTT – 2011

[29]. Nguyễn Mai Hương – CT1101, "***Kỹ thuật giấu tin PVD***", đồ án tốt nghiệp ngành CNTT – 2011

[30]. Phạm Văn Minh, "***Kỹ thuật phát hiện mù cho ảnh có giấu tin bằng LLRT (Logarithm likelihood Ratio Test)***", đồ án tốt nghiệp ngành CNTT – 2011.