**TRƯỜNG ĐẠI HỌC BÁCH KHOA - ĐẠI HỌC ĐÀ NẴNG**

**KHOA CÔNG NGHỆ THÔNG TIN**

**Logo

Description automatically generated**

PBL6: AN TOÀN THÔNG TIN

**Đề tài: Kỹ thuật giấu tin Steganography**

**GIẢNG VIÊN HƯỚNG DẪN: Ts. Lê Trần Đức**

**SINH VIÊN THỰC HIỆN:**

**Nguyễn Ngọc Hoài LỚP: 19TCLC\_DT3 NHÓM: 19.10B**

**Đà Nẵng 12/2022**

MỤC LỤC

[Hình ảnh 2](#_Toc122676375)

[LỜI MỞ ĐẦU 3](#_Toc122676376)

[1. TỔNG QUAN ĐỀ TÀI 4](#_Toc122676377)

[**1.1. Ý tưởng 4**](#_Toc122676378)

[**1.2. Mục tiêu 4**](#_Toc122676379)

[**1.3. Môi trường phát triển 4**](#_Toc122676380)

[2. Cơ sở lý thuyết 5](#_Toc122676381)

[**2.1. Kỹ thuật giấu tin Steganography 5**](#_Toc122676382)

[**2.2. Các kỹ thuật họ Steganography phổ biến 6**](#_Toc122676383)

[**2.3. Phương pháp Least Significant Bit (LSB ) 9**](#_Toc122676384)

[3. TRIỂN KHAI VÀ ĐÁNH GIÁ KẾT QUẢ 11](#_Toc122676385)

[**3.1. Quản lý dự án 11**](#_Toc122676386)

[**3.2. Thiết kế hệ thống 11**](#_Toc122676387)

[**3.3. Kết quả thực hiện 13**](#_Toc122676388)

[**3.3.1. Giao diện màn hình chính 13**](#_Toc122676389)

[**3.3.2. Giao diện Text Steganography 14**](#_Toc122676390)

[**3.3.3. Giao diện Image Steganography 16**](#_Toc122676391)

[**3.4. Đánh giá kết quả 18**](#_Toc122676392)

[4. Kết luận và hướng phát triển 19](#_Toc122676393)

[**4.1. Kết luận 19**](#_Toc122676394)

[**4.2. Hướng phát triển 19**](#_Toc122676395)

[TÀI LIỆU THAM KHẢO 20](#_Toc122676396)

# Hình ảnh

[**Hình 1: Kỹ thuật giấu tin Steganography 4**](#_Toc122674094)

[**Hình 2: Môi trường phát triển 4**](#_Toc122674095)

[**Hình 3: Ảnh trước và sau khi giấu tin 5**](#_Toc122674096)

[**Hình 4: Nhúng thông tin 5**](#_Toc122674097)

[**Hình 5: Trích rút thông tin 6**](#_Toc122674098)

[**Hình 6: Text Steganography 7**](#_Toc122674099)

[**Hình 7: Image Steganography 7**](#_Toc122674100)

[**Hình 8: Audio Steganography 8**](#_Toc122674101)

[**Hình 9: Giấu tin trong tệp HTML 9**](#_Toc122674102)

[**Hình 10: Least Significant Bit (LSB) 10**](#_Toc122674103)

[**Hình 11: Sử dụng GitHub để quản lý Source 11**](#_Toc122674104)

[**Hình 12: Sơ đồ Use Case 11**](#_Toc122674105)

[**Hình 13: Sơ đồ hoạt động 12**](#_Toc122674106)

[**Hình 14: Giao diện màn hình chính 13**](#_Toc122674107)

[**Hình 15: Giao diện Encode Text Steganography 14**](#_Toc122674108)

[**Hình 16: Kết quả Encode Text Steganography 14**](#_Toc122674109)

[**Hình 17: Giao diện và kết quả Decode Text Steganography 15**](#_Toc122674110)

[**Hình 18: Giao diện Encode Image Steganography 16**](#_Toc122674111)

[**Hình 19: Kết quả Encode Image Steganography 18**](#_Toc122674112)

[**Hình 20: Giao diện và kết quả Decode Image Steganography 19**](#_Toc122674113)

# LỜI MỞ ĐẦU

Ngày nay, cùng với sự phát triển mạnh mẽ của nghành khoa học công nghệ thông tin, internet đã trở thành một nhu cầu, phương tiện không thể thiếu đối với mọi người, nhu cầu trao đổi thông tin qua mạng ngày càng lớn. Và với lượng thông tin lớn như vậy được truyền qua mạng thì nguy cơ dữ liệu bị truy cập trái phép cũng tăng lên vì vậy vấn đề đảm bảo an toàn thông tin và bảo mật thông tin cho dữ liệu truyền lên mạng là rất cần thiết. Nhiều kỹ thuật đã được nghiên cứu nhằm giải quyết vấn đề này. Một trong nhứng kỹ thuật quan trọng nhất là mã hóa thông tin. Tuy nhiên một thông điệp bị mã hóa dễ gây ra sự chú ý và một khi các thông tin mã hóa bị phát hiện thì các tin tặc sẽ tìm mọi cách để giải mã.

Một công nghệ mới phần nào giải quyết được những khó khăn trên là giấu thông tin trong các nguồn đa phương tiện như các nguồn âm thanh, hình ảnh,… Xét theo khía cạnh tổng quát thì giấu thông tin cũng là một dạng mật mã nhằm đảm bảo tính an toàn thông tin, nhưng phương pháp này ưu điểm ở chỗ là giảm được khả năng phát hiện sư tồn tại của thông tin trong các nguồn mang.

Giấu thông tin là một kỹ thuật còn tương đối mới và đang phát triển rất nhanh, thu hút được cả sự quan tâm của giới khoa học và giới công nghiệp và cũng còn nhiều thách thức.Và một trong nhứng kỹ thuật giấu tin khá phổ biến chúng ta thường hay nghe nói đến là kỹ thuật giấu tin Steganography.

Với điều kiện thời gian có hạn cùng lượng kiến thức chưa đủ nhiều nên sản phẩm không tránh khỏi xảy ra những sai sót. Em mong rằng sẽ nhận được ý kiến đóng góp của thầy cô để em có thể cải thiện sản phẩm cũng như nâng cao kinh nghiệm bản thân về việc xử lý, xây dựng các trang web có bảo mật sau này. Trong thời gian thực hiện đồ án, em đã nhận được sự quan tâm, chỉ bảo tận tình từ **TS. Lê Trần Đức** giúp em có đủ điều kiện để hoàn thành đề tài.

Em xin chân thành cảm ơn!

# 1. TỔNG QUAN ĐỀ TÀI

## **Ý tưởng**

Ý tưởng của đề tài “**Kỹ thuật giấu tin Steganography”** là ây dựng trang web thực hiện kỹ thuật giấu tin Steganography giúp người sử dụng giấu những thông tin cần ẩn giấu vào hình ảnh như giấu một đoạn thông tin, giấu một hình ảnh.



**Hình 1: Kỹ thuật giấu tin Steganography**

## **Mục tiêu**

* **Về giao diện:**
* Giao diện thân thiện, dễ dàng tiếp cận và sử dụng.
* **Về chức năng:**
* Giấu tin trong hình ảnh
* Giấu tin trong hình ảnh

## **Môi trường phát triển**

* **Các ngôn ngữ sử dụng:** Html, Css, JavaScript
* **Công cụ phát triển:** Visual Studio Code



**Hình 2: Môi trường phát triển**

# Cơ sở lý thuyết

## **Kỹ thuật giấu tin Steganography**

Giấu thông tin (steganography) là một kỹ thuật nhúng thông tin vào một nguồn đa phương tiện nào đó, ví dụ như file âm thanh, file ảnh, file text,... Nguồn đa phương tiện này được gọi là môi trường chứa. Mục đích của việc giấu thông tin là làm cho đối phương không thể nhận biết được sự tồn tại của thông tin đã được giấu.

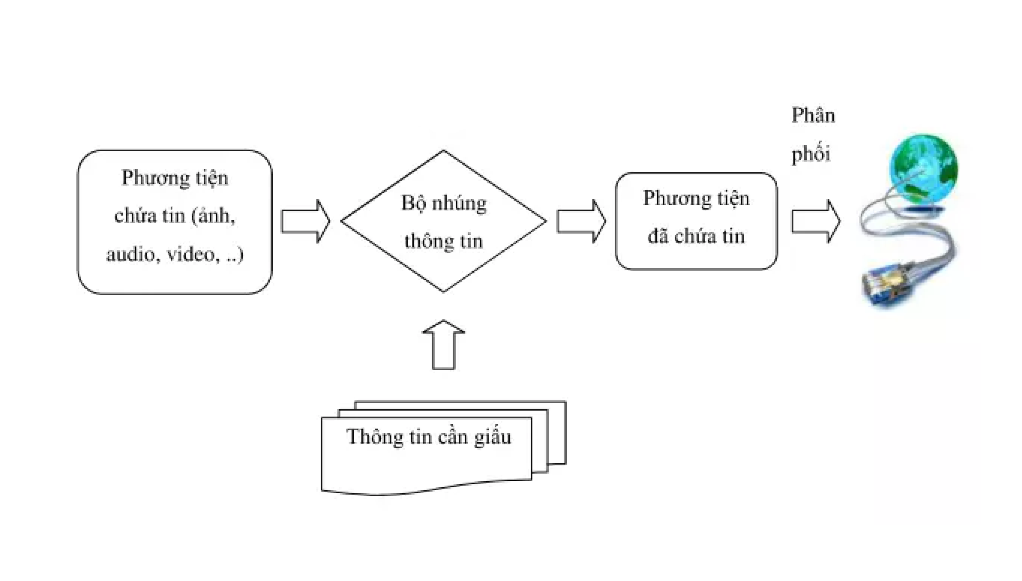
Ngày nay trên mạng có rất nhiều đoạn nhạc hay các bức hình tưởng chừng như bình thường nhưng nó lại chứa các thông tin hoàn toàn bí mật. Điều này càng làm cho Steganography càng trở nên phổ biến.



**Hình 3: Ảnh trước và sau khi giấu tin**

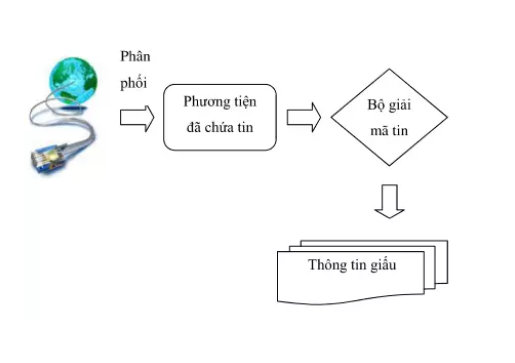
Mỗi kỹ thuật giấu tin gồm:

* Nhúng thông tin



**Hình 4: Nhúng thông tin**

* Trích rút thông tin



**Hình 5: Trích rút thông tin**

Qua trình nhúng và trích rút thông tin còn được gọi là quá trình mã hóa và giải mã của kỹ thuật giấu tin Steganography.

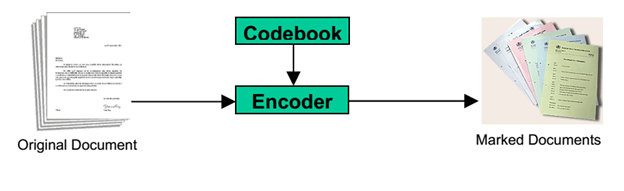
Thuật toán giấu tin được dùng để giấu thông tin vào một phương tiện chứa chỉ người gửi và người nhận biết được. Sau khi giải mã, ta được thông tin mật.

## **Các kỹ thuật họ Steganography phổ biến**

* **Kỹ thuật giấu tin trong trong văn bản (Text Steganography)**

Text Steganography đang ẩn thông tin bên trong các tệp văn bản. Nó liên quan đến những việc như thay đổi định dạng của văn bản hiện có, thay đổi từ trong văn bản, tạo chuỗi ký tự ngẫu nhiên hoặc sử dụng ngữ pháp phi ngữ cảnh để tạo văn bản có thể đọc được. Các kỹ thuật khác nhau được sử dụng để ẩn dữ liệu trong văn bản là:

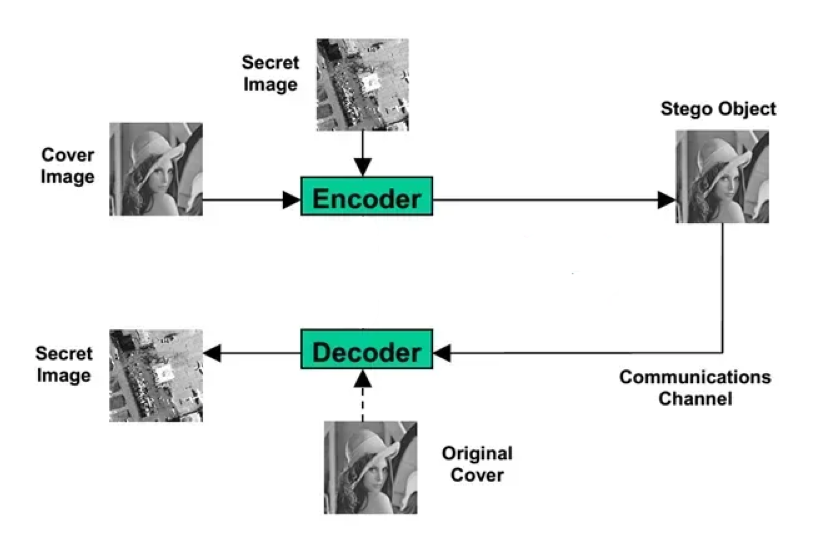
* Phương pháp dựa trên định dạng
* Tạo ngẫu nhiên và thống kê
* Phương pháp ngôn ngữ



**Hình 6: Text Steganography**

* **Kỹ thuật giấu tin trong ảnh (Image Steganography)**

Đây là một trong những kỹ thuật phồ biến nhất của họ Steganography khi dữ liệu được giấu sau một bức ảnh kỹ thuật số (digital image). Thậm chí còn có thể giấu một bức ảnh sau một bức ảnh khác. Để giúp các bạn hiểu rõ hơn về phương thức này thì mình có minh họa sau.



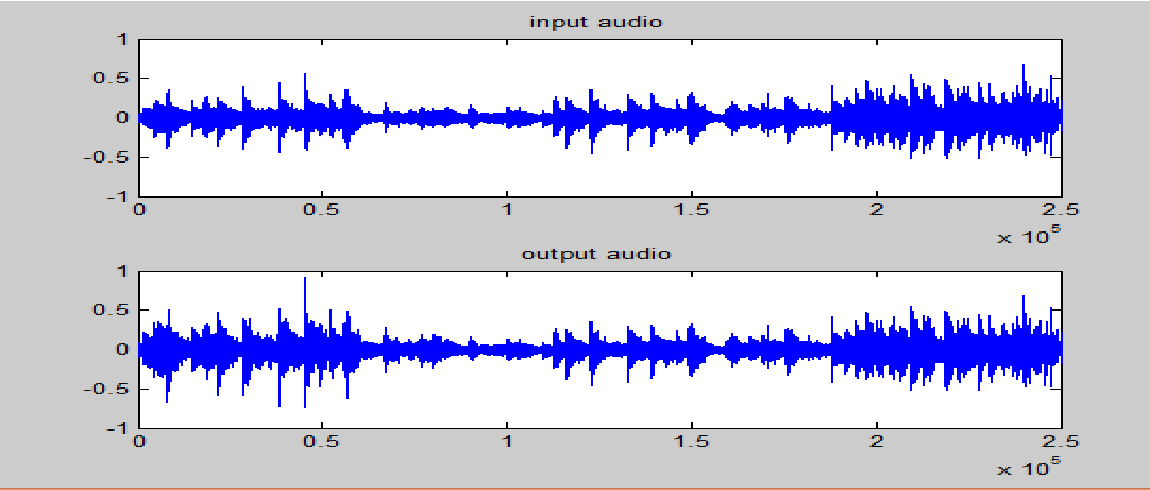
**Hình 7: Image Steganography**

Phía trên là bức ảnh biểu thị cách mà một bức ảnh được giấu vào một bức ảnh khác. Đầu tiên, sẽ có có 2 đối tượng là bức ảnh bao phủ hay bức ảnh nền (Cover Image) và bức ảnh được giấu (Secret Image). Cả hai bức ảnh sẽ đi qua một giai đoạn "Encoder" hay "Mã hóa". Song, sản phẩm của kỹ thuật giấu tin được gửi đến "đích" để tiến hành việc "Decoder" hay "Giải mã". Sử dụng giải mã sẽ tách hình ảnh ấy ra thành hai hình ảnh đơn lẽ như ban đầu. Tuy nhiên, qua các quá trình, chất lượng của các bức ảnh sẽ bị giảm đi nhưng không quá là đáng kể.

* **Kỹ thuật giấu tin trong tệp tin âm thanh (Audio Steganography)**

Trong kỹ thuật giấu tin trong tệp tin âm thanh , thông điệp bí mật được nhúng vào tín hiệu âm thanh làm thay đổi chuỗi nhị phân của tệp âm thanh tương ứng. Ẩn tin nhắn bí mật trong âm thanh kỹ thuật số là một quá trình khó khăn hơn nhiều so với những người khác, chẳng hạn như Image Steganography. Các phương pháp giấu tin trong tệp tin âm thanh khác nhau bao gồm:

* Mã hóa bit ít quan trọng nhất (Least Significant Bit Encoding)
* Mã hóa chẵn lẻ (Parity Encoding)
* Mã hóa pha ( Phase Coding)
* Trải phổ (Spread Spectrum)

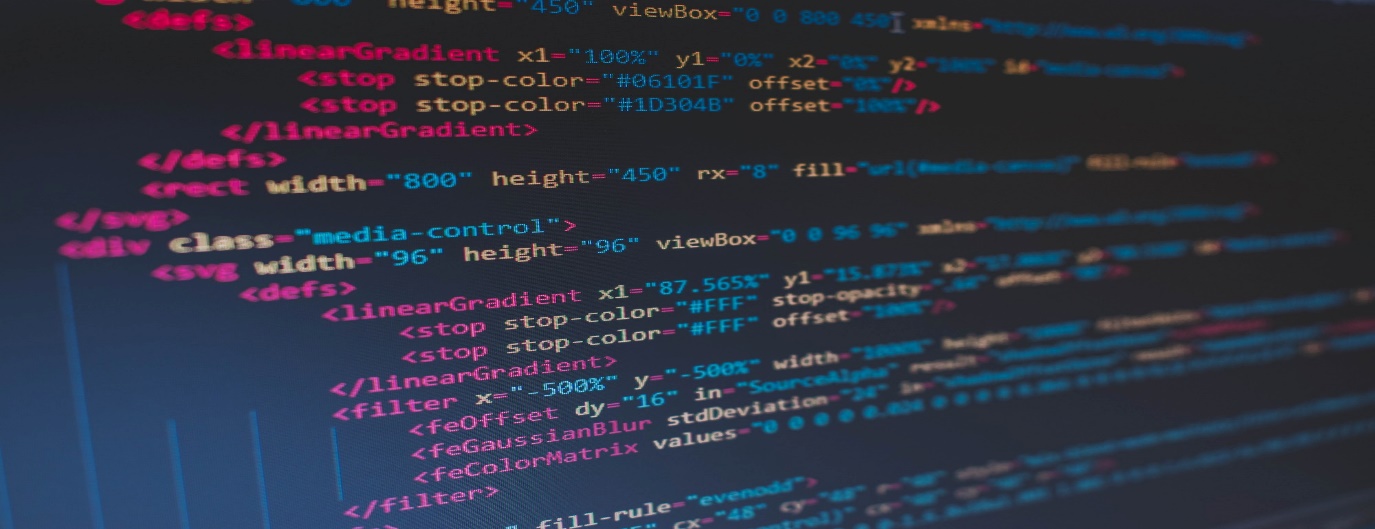


**Hình 8: Audio Steganography**

* **Kỹ thuật giấu tin trong tệp HTML**

Một trong những kỹ thuật khác của họ nhà Steganography đó là giấu thông tin trao đổi trong tệp HTML. Với sự bùng nổ của Internet trong những thập kỉ gần đây, việc số lượng lớn các tệp HTML tồn tại trên mạng ngày càng tăng lên bởi lẽ HTML hay Hyper Text Markup Language là một "ngôn ngữ đánh dấu" và cũng là khung xương cho toàn bộ các trang web hiện tại. Vậy nên có nhiều người sử dụng điều đó và trao đổi thông tin thông qua các tệp HTML. Một số kỹ thuật có thể kể đến như:

* Giấu thông tin vào cuối tệp HTML
* Giấu thông tin trong các comment của tệp HTML
* Steganography bằng cách tạo ra khoảng trắng trong các tag
* Thay đổi định dạng in hoa của các chữ
* Giấu thông tin trong thuộc tính id của các tag



**Hình 9: Giấu tin trong tệp HTML**

## **Phương pháp Least Significant Bit (LSB )**

Trong máy tính, các bit ít quan trọng nhất là bit đó là xa nhất về phía bên phải và giữ giá trị ít nhất là trong một số nhị phân đa-bit. Như số nhị phân được chủ yếu được sử dụng trong máy tính và các khu vực khác có liên quan, các bit ít quan trọng giữ tầm quan trọng, đặc biệt là khi nói đến truyền các số nhị phân.

Dữ liệu kỹ thuật số được tính trong định dạng nhị phân, và tương tự như ký hiệu số, các chữ số bên phải được coi là chữ số thấp nhất trong khi tận cùng bên trái được coi là chữ số cao nhất. Do các ký hiệu vị trí, các bit ít quan trọng còn được gọi là các bit ngoài cùng bên phải. Đây là đối diện của các bit quan trọng nhất, có thể mang theo những giá trị cao nhất trong một số nhị phân nhiều bit cũng như số lượng mà là xa nhất về phía bên phải. Trong một số nhị phân đa-bit, tầm quan trọng của một chút giảm khi nó tiếp cận bit ít quan trọng. Vì nó là nhị phân, bit quan trọng nhất có thể là 1 hoặc 0.

Có rất nhiều phương pháp để che giấu thông tin trong các hình ảnh số nhưng phương pháp dụng nhất là chèn bit có trọng số nhỏ nhất (LSB). Ví dụ ta có: 11110110 là một số nhị phân 8 bit. Bit tận cùng bên phải ( bit 0 ) được gọi là bit LSB vì sự thay đổi của nó có ảnh hưởng ít nhất đến giá trị của số. Dữ liệu nhị phân của thông báo mật sẽ bị chia nhỏ ra và thay thế các bit LSB của từng byte trong giá trị RGB của từng Pixel. Sỡ dĩ chúng ta chỉ thay thế các bit LSB là vì sau khi thay đổi các giá trị trong RBG chỉ dao động 1 đơn vị, dùng mắt thường sẽ khó phát hiện ra sự thay đổi của bức ảnh, giúp đạt được mục đích ẩn dấu.

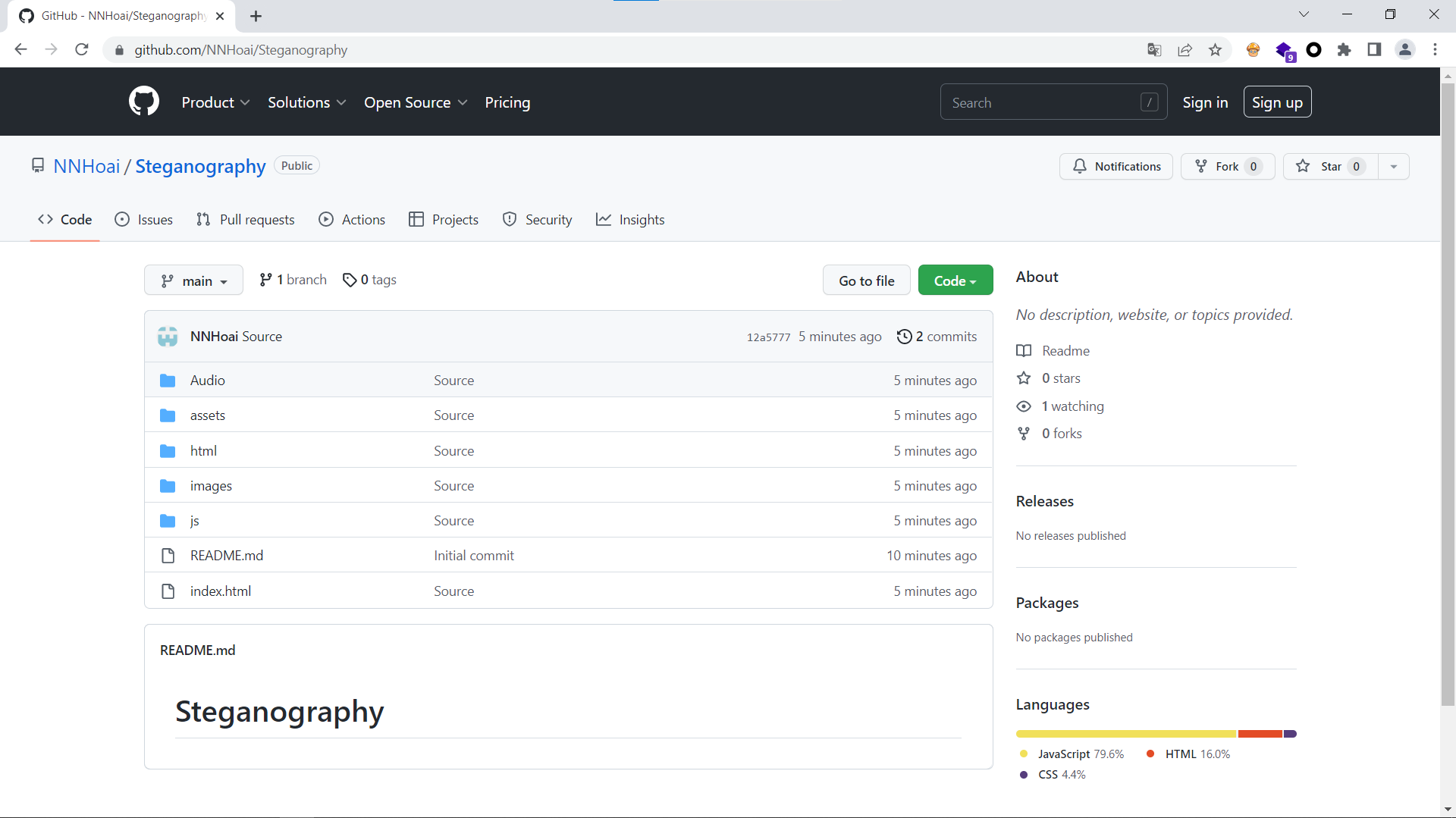


**Hình 10: Least Significant Bit (LSB)**

# TRIỂN KHAI VÀ ĐÁNH GIÁ KẾT QUẢ

## **Quản lý dự án**

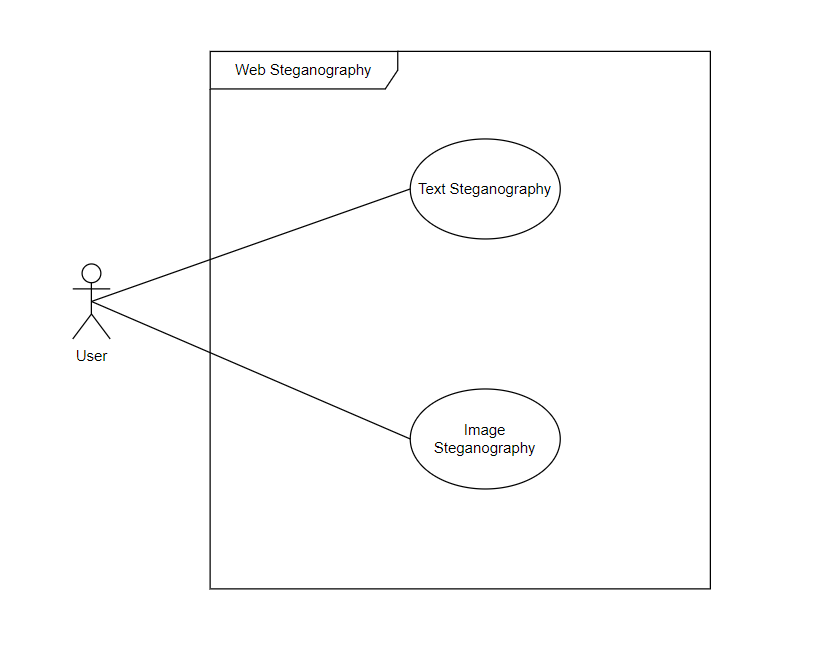
Dùng GitHub để quản lí code và để mọi người có thể theo dõi dự án.



**Hình 11: Sử dụng GitHub để quản lý Source**

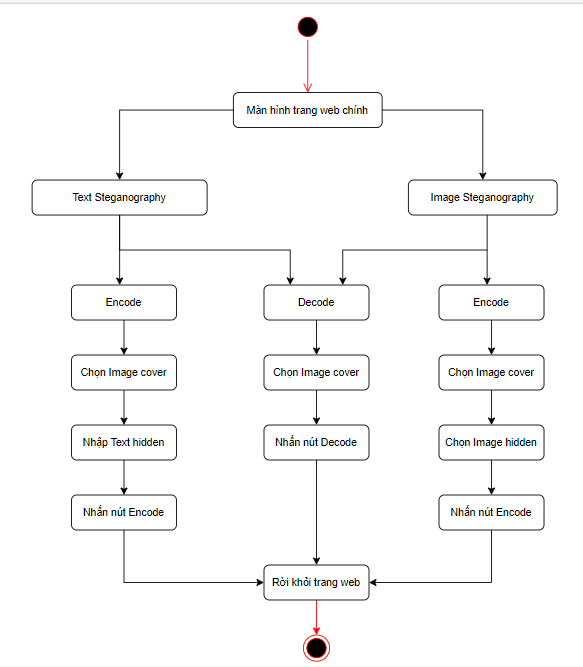
## **Thiết kế hệ thống**

* **Sơ đồ Use Case**



**Hình 12: Sơ đồ Use Case**

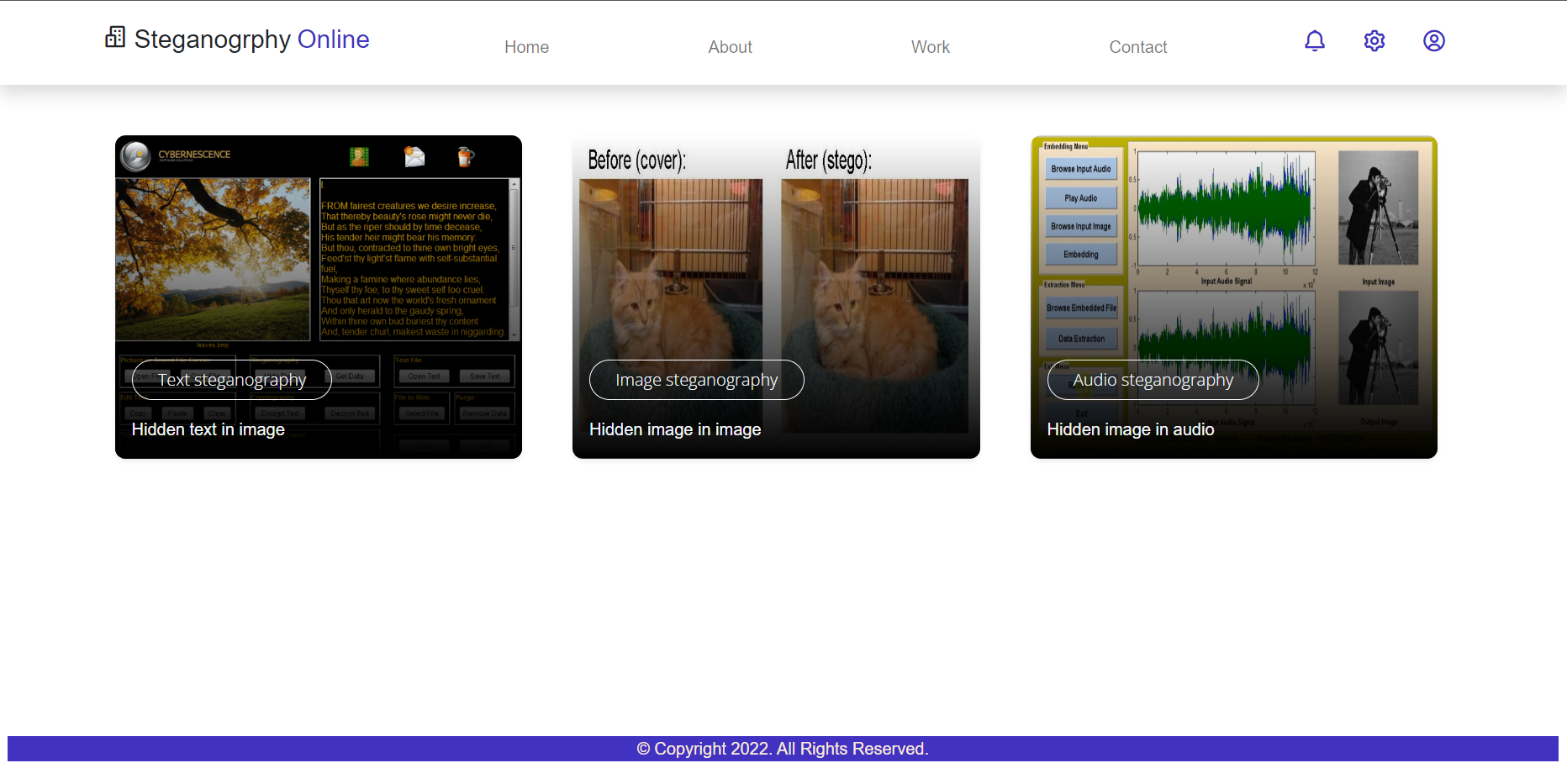
* **Sơ đồ hoạt động**

****

**Hình 13: Sơ đồ hoạt động**

## **Kết quả thực hiện**

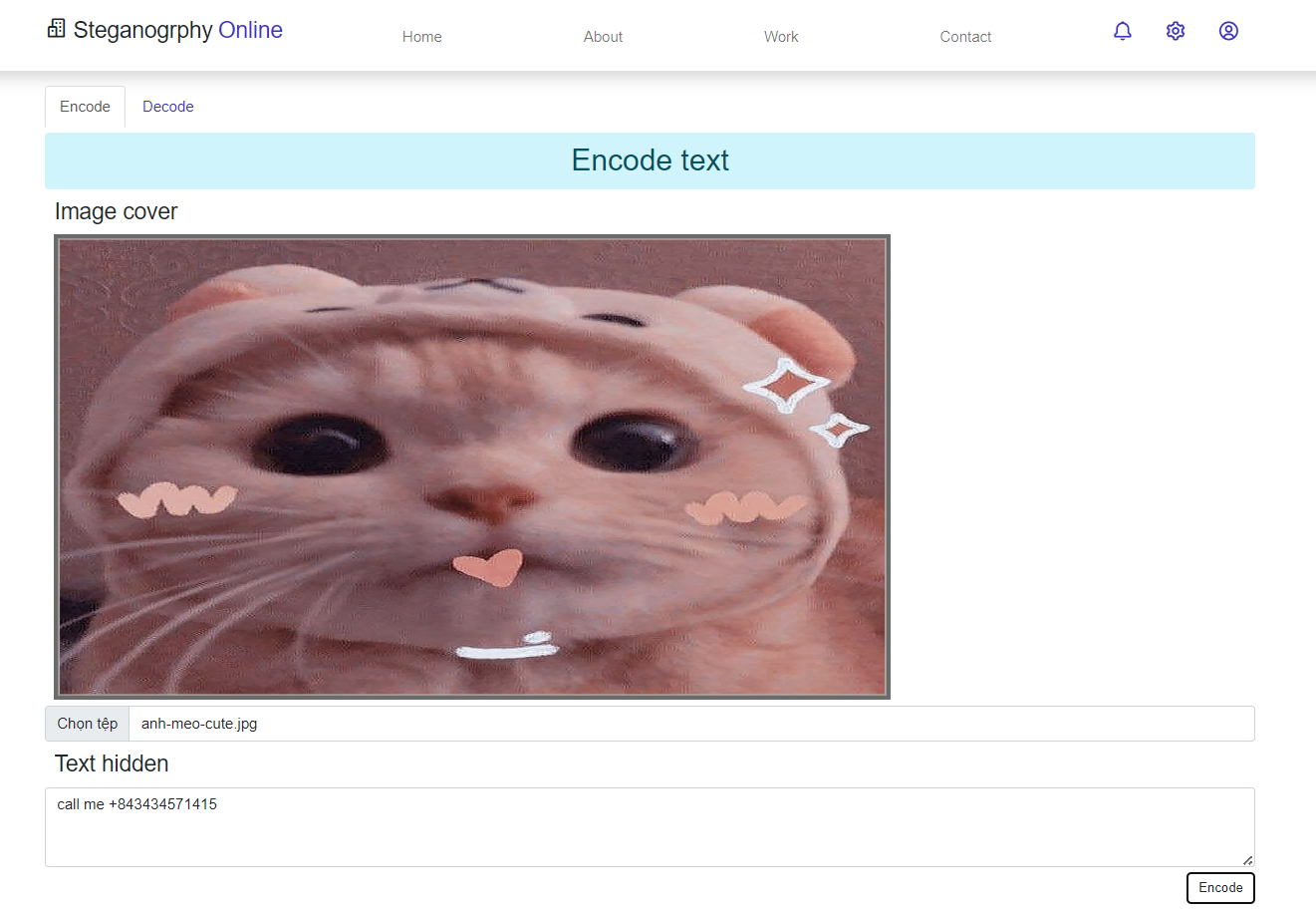
#### Giao diện màn hình chính



**Hình 14: Giao diện màn hình chính**

#### Giao diện Text Steganography

* **Giao diện Encode Text Steganography**



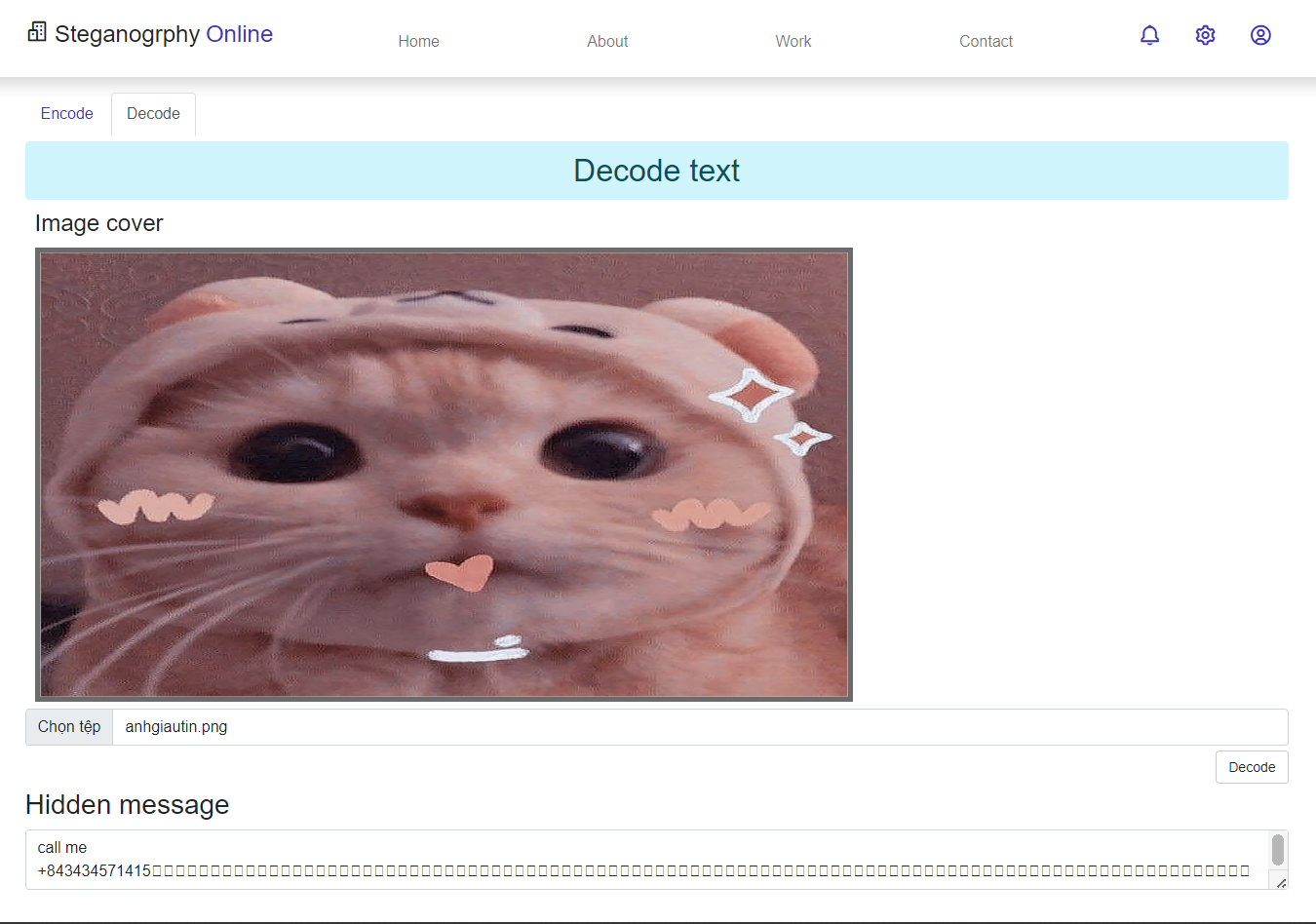
**Hình 15: Giao diện Encode Text Steganography**

* **Kết quả Encode Text Steganography**



**Hình 16: Kết quả Encode Text Steganography**

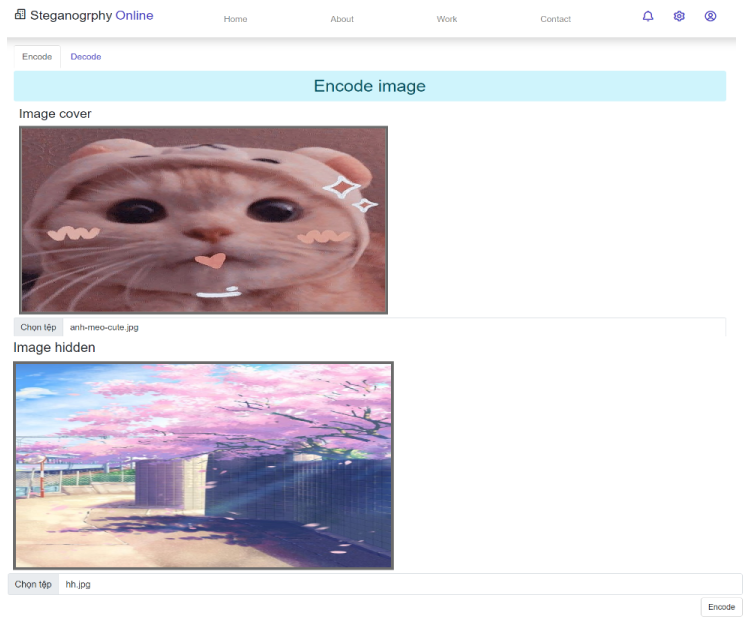
* **Giao diện Decode Text Steganography**



**Hình 17: Giao diện và kết quả Decode Text Steganography**

#### Giao diện Image Steganography

* **Giao diện Encode Image Steganography**

****

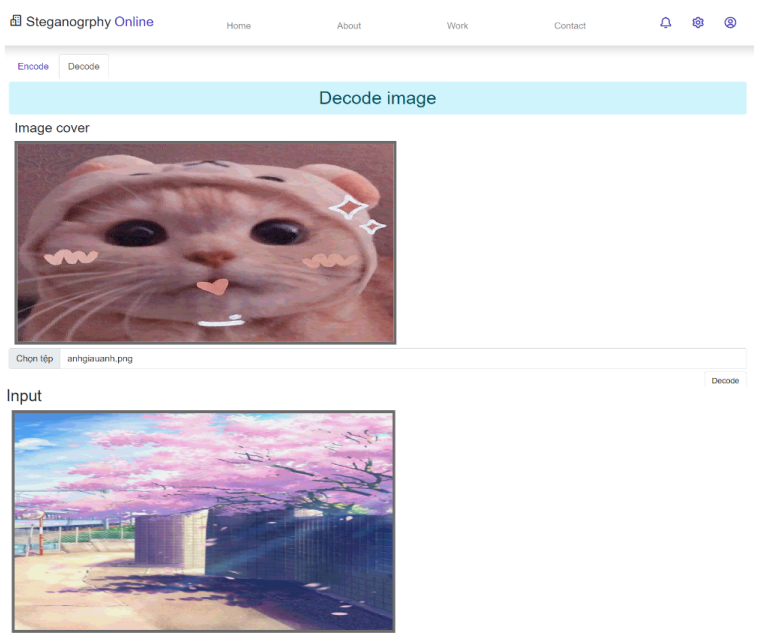
**Hình 18: Giao diện Encode Image Steganography**

* **Kết quả Encode Image Steganography**

****

**Hình 19: Kết quả Encode Image Steganography**

* **Giao diện Decode Image Steganography**



**Hình 20: Giao diện và kết quả Decode Image Steganography**

## **Đánh giá kết quả**

* Chương trình đã giải quyết được những mục tiêu mà đồ án đề ra, tạo ra được một trang web kỹ thuật giấu tin.
* Website hoạt động ổn định, phản hồi nhanh , đem lại niềm vui cho người trải nghiệm.
* Giấu tin trong hình ảnh và giấu hình ảnh trong hình ảnh hoạt động khá tốt.

# Kết luận và hướng phát triển

## **Kết luận**

* **Ưu điểm**
  + Ứng dụng có giao diện rõ ràng, dễ sử dụng. Ứng dụng đáp ứng đủ những mục tiêu mà đề tài đề ra.
  + Học tập được thêm kiến thức về An toàn thông tin. Cụ thể là kỹ thuật giấu tin Steganogrephy.
  + Biết quy trình và cách triển khai một dự án An toàn thông tin.
  + Biết dử dụng GitHub để quản lí code và triển khai dự án.
  + Tăng kinh nghiệm làm dự án, khả năng đọc tài liệu.
* **Nhược điểm**
  + Do thời gian có hạn và kiến thức tiếp thu chưa đầy đủ nên một số chức năng vẫn còn bất cập và chưa được hoàn thiện như mong muốn.
  + Ứng dụng chưa được thiết kế đẹp mắt.
  + Chức năng giấu tin còn ít, chưa giấu tin trên nhiều loại nguồn khác nhau chỉ hạn chế ở giấu tin trong hình ảnh.

## **Hướng phát triển**

* + Xây dựng thành một trang web có giao diện đẹp hơn, hoàn thiện hơn.
  + Xây dựng ứng dụng đa nền tảng trên điện thoại di động.
  + Tiếp tục nâng cấp, cập nhập thông tin cũng như các kỹ thuật giấu tin người dùng có nhu cầu.

# TÀI LIỆU THAM KHẢO

1. Giới thiệu về kỹ thuật giấu thông tin, thiên thần gãy cánh, 5/1/2011,

https://antoanthongtin.gov.vn/giai-phap-khac/gioi-thieu-ve-ky-thuat-giau-thong-tin-100319

1. Tìm hiểu về Text Steganography, Thao Hoang Thu, 20/4/2021,

https://viblo.asia/p/tim-hieu-ve-text-steganography-07LKXoVD5V4

1. Giới thiệu kỹ thuật giấu tin trong ảnh Steganography, Nguyễn Hồng Sơn, 29/10/2018,

https://securitydaily.net/gioi-thieu-ky-thuat-giau-tin-trong-anh-steganography/

1. Kỹ thuật che giấu thông tin bằng LSB - LSB steganography, MSE vlogs, 20/5/2020,

https://www.youtube.com/watch?v=Wkk3\_DqBEY0