**TRƯỜNG ĐẠI HỌC SƯ PHẠM TP. HỒ CHÍ MINH**Khoa Công nghệ thông tin

****

MÔN: BẢO MẬT AN NINH MẠNG

**Đề tài**

**STEGANOGRAPHY**

**TPHCM-NĂM 2019**

**TRƯỜNG ĐẠI HỌC SƯ PHẠM TP. HỒ CHÍ MINH**Khoa Công nghệ thông tin

**Đề tài**

**STEGANOGRAPHY**

**GVHD: ThS Lương Trần Hy Hiến**

Nhóm 8

Nguyễn Như Quỳnh - 42.01.104.129

Nguyễn Sơn Lâm **-** 42.01.104.076

Đỗ Thị Thanh Thi - 42.01.104.167

Nguyễn Văn Tuấn - 42.01.104.150

Trần Thị Yến Nhi - 42.01.104.099

Nguyễn Văn Hiền - 42.01.104.045

**TPHCM-NĂM 2019**

Mục lục

[1. Lời cám ơn 2](#_Toc6632026)

[2. Tổng quan 3](#_Toc6632027)

[3. Các trường hợp 7](#_Toc6632031)

[4. Ưu nhược điểm 7](#_Toc6632032)

[5. Khắc phục nhược điểm 7](#_Toc6632033)

[6. Mô hình demo 8](#_Toc6632034)

[7. Kết luận 12](#_Toc6632035)

[8. Tài liệu tham khảo. 13](#_Toc6632036)

# Lời cám ơn

Lời đầu tiên chúng em xin cám ơn Ban Giám Hiệu Nhà Trường DHSP TPHCM đã tạo điều kiện để sinh viên chúng em có một môi trường học tập thoải mái và cơ sở hạ tầng cũng như cơ sở vật chất.

Chúng em xin cám ơn khoa CNTT đã giúp chúng em mở mang kiến thức hơn về các vấn đề xưng quanh chiếc máy tính. Qua đó chúng em có thể nhận thức một cách đầy đủ và toán diện tầm quan trọng của ngành công nghệ thông tin trong công cuộc xây dựng và phát triển Đất nước.

Chúng em xin cám ơn thầy Lương Trần Hy Hiến đã hướng dẫn chúng em hoàn thành đồ án môn học này. Hi vọng thông qua nỗ lực tìm hiểu của mỗi thành viên, chúng em sẽ giúp các bạn hiểu rõ hơn các bước bảo vệ an ninh mạng,

# Tổng quan

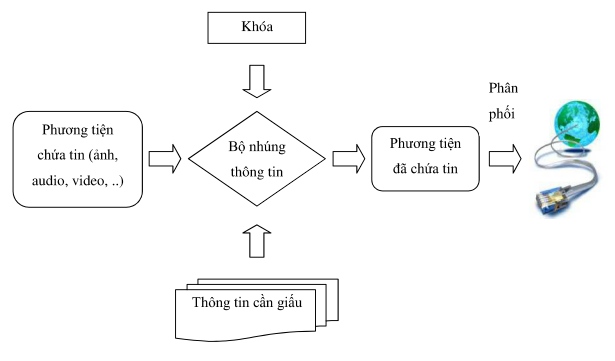
## Giới thiệu

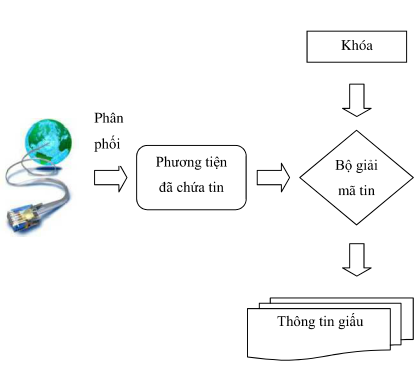
Giấu thông tin (steganography) là một kỹ thuật nhúng thông tin vào một nguồn đa phương tiện nào đó, ví dụ như file âm thanh, file ảnh, file text,.. Nguồn đa phương tiện này được gọi là môi trường chứa. Mục đích của việc giấu thông tin là làm cho đối phương không thể nhận biết được sự tồn tại của thông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

Mỗi kỹ thuật giấu tin gồm:

* Nhúng thông tin
* Trích rút thông tin

Thuật toán giấu tin được dùng để giấu thông tin vào một phương tiện chứa bằng cách sử dụng một khóa bí mật được dùng chung bởi người gửi và người nhận. Việc giải mã thông tin chỉ có thể thực hiện được khi có khoá. Sau khi giải mã, ta được thông tin mật.





Trong những năm gần đây, chúng ta thường nghe nói nhiều đến thuật ngữ Steganography. Đây là một kỹ thuật mà theo nhiều chuyên gia trong lĩnh vực này - là một bộ môn nghệ thuật và khoa học nhằm che giấu sự tồn tại của thông tin. Khác với mật mã, mục tiêu của Steganogrpahy là che giấu các thông báo cần giữ bí mật trong các dữ liệu “vô hại” khác để đối phương không thể phát hiện được sự hiện diện của thông báo.

Các khái niệm thường được dùng trong giấu tin trong ảnh:

* Ảnh môi trường: Là ảnh gốc được dùng để nhúng thông tin.
* Thông tin nhúng: Là các thông tin mật cần gửi.
* Ảnh đã nhúng: Là ảnh gốc sau khi đã được nhúng thông tin mật.
* Khóa mật: Là khóa tham gia vào quá trình nhúng, được trao đổi giữa người gửi và người nhận.

Các yêu cầu trong giấu tin trong ảnh:

* Tính ẩn của giấu tin được chèn vào ảnh: Sự hiện diện của giấu tin trong ảnh không làm ảnh hưởng tới chất lượng của ảnh đã chèn tin.
* Tính bền vững: Thể hiện khả năng ít bị thay đổi (về nội dung, hình dạng) trước những tấn công từ bên ngoài. Hiện nay, chưa có kỹ thuật giấu tin nào đảm bảo được yêu cầu này một cách tuyệt đối.
* Khả năng không bị phát hiện: Thể hiện ở việc khó xác định được đối tượng có chứa thông tin mật hay không. Các kỹ thuật giấu tin hiện nay cố gắng đảm bảo yêu cầu này dựa vào hệ thống thị giác của con người.
* Khả năng lưu trữ: Thể hiện ở lượng thông tin được lưu trữ. Do còn phải đảm bảo “khả năng không bị phát hiện” nên với những thông tin mật lớn, ta thường chia nhỏ nó ra, nhúng nhiều lần và vào các đối tượng khác nhau.

Thực chất Steganography đã được con người biết tới từ rất lâu rồi. Năm 440 trước công nguyên, người Herodotus (Người Hy Lạp xa xưa) đã cạo trọc đầu các nô lệ tin cậy rồi xăm lên đó các thông điệp và chờ tóc mọc lại. Mục đích của việc này là nhằm gửi tin đi trong cuộc chiến tranh giữa người Herodotus và Persians (Người Ba Tư).

Trong cuộc cách mạng của Mỹ, mực không màu cũng được sử dụng để trao đổi thông điệp giữa người Mỹ và người Anh.

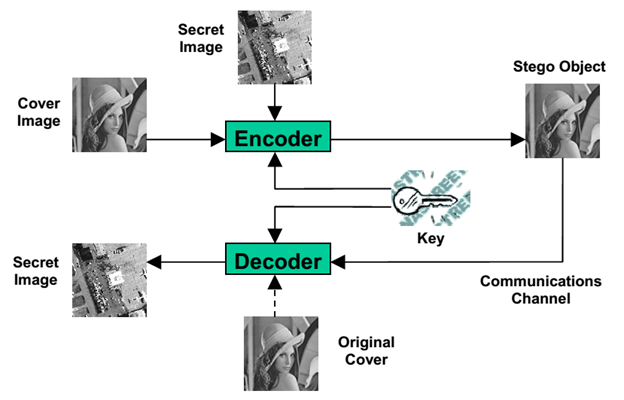
Trong các cuộc chiến tranh thế giới, Steganography cũng được sử dụng. Người Đức đã sử dụng mực không màu để viết các dấu chấm nhỏ lên phía trên và dưới các chữ cái bằng cách thay đổi chiều cao các chữ trong đoạn văn bản. Trong chiến tranh thế giới thứ nhất, các tù nhân cũng sử dụng mã Morse để gửi thư về nhà bằng cách viết các dấu chấm và gạch ngang lên các chữ cái i,j,t,f.

Các phương pháp giấu tin:

* Phương pháp nhúng vào các bit có trọng số thấp.
* Phương pháp dựa vào kỹ thuật biến đổi ảnh.
* Phương pháp sử dụng mặt nạ giác quan.

## Quá trình mã hóa và giải mã của Stegranoraphy

Thông điệp và bức ảnh ban đầu sẽ được đưa vào trong bộ mã hóa (encoder). Trong bộ mã hóa, một bộ giao thức sẽ được thực thi để nhúng thông điệp vào trong bức ảnh. Kiểu của giao thức sẽ phụ thuộc vào kiểu của thông điệp và cách ta nhúng. Ví dụ hình dưới đây sẽ cho ta thấy giao thức để ẩn thông điệp trong các bức ảnh.

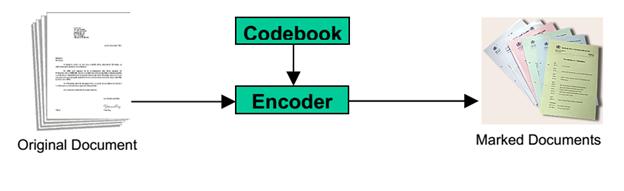


Khóa là cần thiết trong quá trình giấu thông tin. Người gửi có thể dùng khóa chính để mã hóa và người nhận có thể dùng khóa công khai để giải mã. Điều này có thể giảm thiểu khả năng bên thứ 3 biết được thông điệp và giải mã.

## Một số cơ chế trong Stegranography

#### c.1) Cơ chế ẩn thông diệp trong văn bản hoặc đoạn kí tự

Đối với các tài liệu giấy thì khi bạn copy, bạn có thể sẽ không vi phạm bản quyền vì chất lượng của các tài liệu này khác nhau. Tuy nhiên đối với các tài liệu trên máy tính thì các bản copy sẽ giống hệt các bản gốc nên bạn rất dễ vi phạm bản quyền. Sở dĩ có thể biết được là do trong các tài liệu này đã được chèn thêm vào một số đoạn text để đánh dấu. Những đoạn này là ẩn với người dùng và bằng mắt thường khó có thể nhận biết được. Chúng ta chỉ có thể giải mã nhờ máy tính thì mới có thể nhìn thấy được.



Dưới đây là một số cách để ẩn đoạn text trong văn bản.

c.1.1) Dịch chuyển vị trí dòng.

Chúng ta sẽ dịch chuyển vị trí của các dòng một khoảng nhỏ khoảng 1/300 inch. Điều này rất khó có thể phát hiện bằng mắt thường vì khoảng cách thay đổi khá nhỏ. Chúng ta chỉ có thể phát hiện nhờ máy tính bằng cách đo khoảng cách giữa các dòng. Trong các khoảng trống đó ta có thể chèn vào các bit 0 hoặc 1, do đó trong toàn bộ văn bản, ta có thể ẩn đi một lượng thông tin khá lớn.

c.1.2) Dịch chuyển vị trí từ.

Cơ chế này cũng giống như dịch chuyển vị trí dòng, nhưng ta sẽ dịch chuyển vị trí các từ. Sau đó tùy vào khoảng trống đó nằm bên trái hay bên phải từ mà ta quy định nó là bit 0 hay bit 1. Dịch trái sẽ là bit 0 còn dịch phải sẽ là bit 1.

c.1.3) Chèn vào khoảng trắng cuối mỗi dòng.

Một cách khác để ẩn đoạn text là sử dụng các khoảng trắng. Bằng cách vận dụng khéo léo các khoảng trắng, ta có thể lưu trữ được một lượng lớn các bit. Các khoảng trắng ở cuối mỗi dòng có thể bị bỏ qua và không hiện lên các bởi các ứng dụng đọc văn bản. Trong toàn bộ văn bản, ta có thể có đủ không gian để lưu trữ chuỗi bí mật.

c.1.4) Ẩn thông điệp trong nội dung của các đoạn văn bản khác

Một trong những cách khác để ẩn thông điệp là ta thay đổi cấu trúc của văn bản ban đầu sao cho nghĩa không bị thay đổi để mà ta có thể lưu trữ được thông điệp. TextHide là một chương trình sử dụng cơ chế này.

# Các trường hợp ứng dụng

Hiện nay, giấu tin trong ảnh chiếm tỉ lệ lớn trong các ứng dụng giấu tin trong dữ liệu đa phương tiện bởi vì lượng thông tin được trao đổi bằng hình ảnh là rất lớn. Giấu tin trong ảnh có nhiều ứng dụng trong thực tế, ví dụ như trong việc xác định bản quyền sở hữu, chống xuyên tạc thông tin hay truyền dữ liệu một cách an toàn,…

Giấu tin tại nhà đài phát thanh truyền đi.

# Thuật toán LSB

1. Thuật toán LSB cổ điển
2. Thuật toán giấu

Đầu vào:

Ảnh gốc cấp xám

Thông điệp bí mật

Đầu ra:

Ảnh mang tin

Các bước thực hiện

Bước 1: Biểu diễn ma trận điểm ảnh về dạng số thập phân với mxn phần tử, rồi chuyển ma trận về 1 chiều I với i phần tử, chuyển các điểm ảnh về dạng nhị phân

Bước 2: Biểu diễn thông điệp dưới dạng số nhị phân.

Bước 3: Cứ 8 bit ảnh tách bỏ số bit LSB ngoài cùng bên phải và ghép phần còn lại với 2 bit nhị phân đầu của thông điệp, kết quả thu được dưa về dạng thập phân rồi gán ngược lại vào I(i).

Bước 4: Thực hiện lại Bước 3 cho đến khi lấy hết các bit của mỗi chuỗi nhị phân thông điệp ghép với các bit ảnh. Chuyển đổi ảnh I từ mảng một chiều về mảng 2 chiều mxn phần từ. Được ảnh mới đã giấu tin

1. Thuật toán tách

Đầu vào:

Ảnh mang tin

Đầu ra:

Ảnh đã tách tin.

Thông điệp mật

Các bước thực hiện

Bước 1: Biểu diễn ma trận điểm ảnh về dạng số thập phân với mxn phân từ. Chuyển đổi ma trận ảnh mxn phần tử về mảng 1 chiều I với i phần tử.

Bước 2: Chuyển các bit ảnh về dạng nhị phân, cứ 8 bit ảnh tách lấy 2 bit ngoài cùng bên phải. Đem ghép các kết quả này lại với nhau.

Bước 3: Kết quả thu được sử dụng hàm chuyển đổi từ chuỗi số nhị phân về chuỗi ký tự. Sau khi lặp lại quá trình trên số lần bằng số lần duyệt ta thu được nội dung trên thông điệp.

1. Thuận toán LSB nâng cao

Giấu tin bằng phương pháp thay thế LSB sử dụng khóa hoán vị di truyền tối ưu.

1. Thuật toán giấu

Đầu vào:

Ảnh gốc

Thông điệp bí mật

Khóa

Đầu ra:

Ảnh mang tin

Khóa

Số bit thồn điệp cần mã hóa

Các bước thực hiện

Bước 1: Biễu diễn ma trận điểm ảnh về dạng số thập phân với mxn phần tử. Chuyển đổi ma trận ảnh mxn phần tử về dạng mảng một chiều I với i phần tử

Bước 2: Biễu diễn thông tin giấu dưới dạng chuỗi nhị phân

Bước 3: Sử dụng một khóa 8bit bất kỳ( khóa là ký tự, chuyển khóa về dạng mãng như với thông điệp) đem mã hóa với chuỗi thông điệp bí mật bằng phép XOR: cứ 8bit khóa đem XOR với 8 bit đầu của thông điệp. Thực hiện lai bước này cho đến khi thông điệp được mã hóa hết

Bước 4: thông điệp đã mã hóa đêm giấu vào ảnh tương tự như phương pháp cổ điển: là tách lấy 6 bit đầu của bit ảnh đem ghép với 2 bit đầu trong thông điệp rồi chuyển về dạng thập phân và gán ngược lại vào ảnh

Bước 5: Thực hiện Bước 4 cho đến khi lấy hết các bit của chuỗi nhị phân thông điệp để ghép với các bít ảnh. Chuyển đổi ảnh I từ mảng một chiều về mãng 2 chiều mxn phần tử, được ảnh mới đã giấu tin.

1. Thuật toán tách

Đầu vào:

Ảnh đã giấu

Khóa

Đầu ra:

Ảnh đã tách tin.

Thông điệp

Các bước thực hiện

Bước 1: Biễu diễn ma trận điểm ảnh về dạng số thập phân với mxn phần tử chuyển đỗi ma trận ảnh mxn về mảng một chiều I với i phần tử.

Bước 2: Chuyển các bit ảnh về dạng nhị phân, cứ 8 bit ảnh lấy 2 bit ngoài cùng bên phải. Đem ghép các kết quả này lại với nhau.

Bước 3: Kết quả thu được sử dụng hàm chuyển đỗi từ chuỗi số nhị phân về chuỗi ký tự. Sau khi lặp lại quá trình bằng số lần duyệt, ta thu được nội dung thông điệp đã mã hóa.

Bước 4: Sử dụng hàm giải mã thực hiện giải mã thông điệp bằng khóa 8 bit, ta thu được kết quả là nội dung của thông điệp.

# Ưu nhược điểm

Ưu điểm:

Giúp ta che giấu thông tin quan trọng, nhạy cảm mà không muốn công khai.

Là một công cụ mạnh mẽ nếu nó cho phép hai người được trao đổi với nhau bằng một đường dẫn truyền thông

Nhược điểm:

Ngay cả tin nhắn được ẩn, nếu ai đó biết được sự tồn tại của nó họ vẫn có thể đọc được.

Nếu người nào đó nghĩ bạn đang dùn Stego, họ có thể xóa bỏ thông điệp ẩn

# Khắc phục nhược điểm

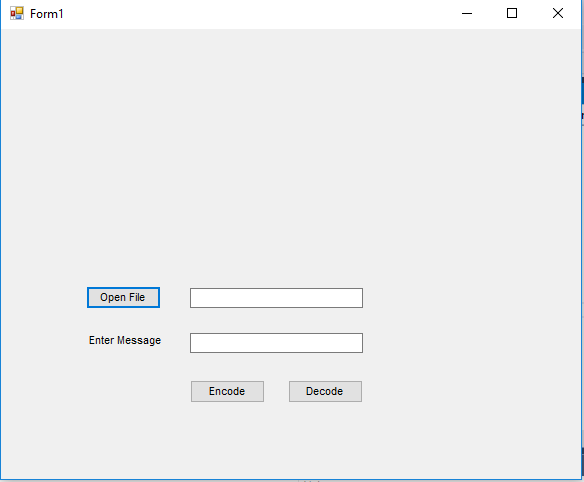
Để có một mức độ bảo mật cao, bạn phải triển khai nhiều cấp độ bảo mật.

Mã hóa trước khi ẩn dấu thông tin.

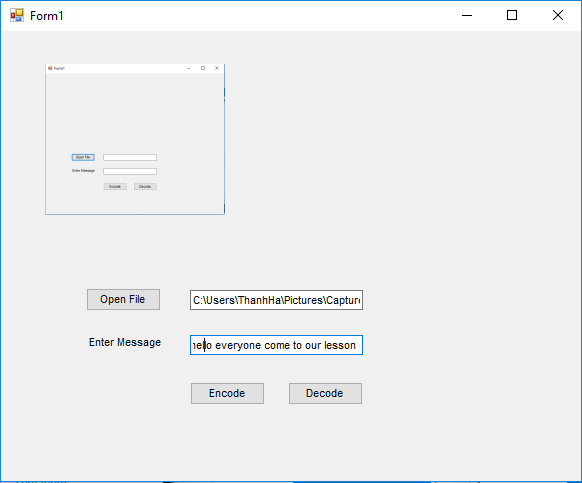
Chèn các tin nhắn vào các bit ít quan trọng nhất. Và tin nhắn có thể bị xóa bỏ bằng các chuyển đổi hình ảnh sang định dạng khác hay chuyển nó trở lại định dạng ban đầu

# Mô hình demo

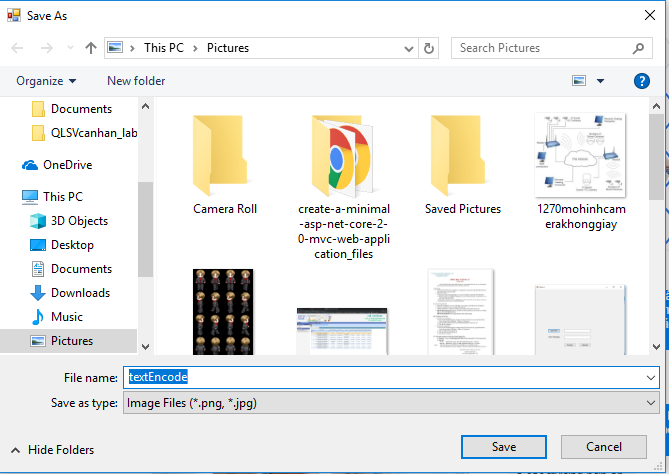
Màn hính chính của chương trình.



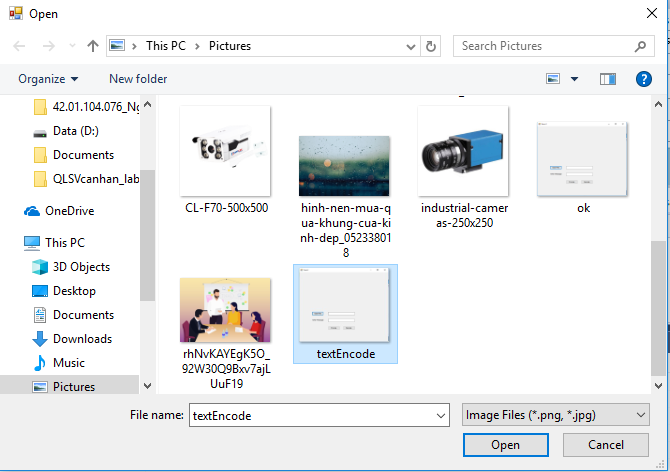
Xử lý chức năng Encode, ta nên chọn bức ảnh kích cỡ thấp, bởi vì khi chọn ảnh kích cỡ cao sẽ không decode được.

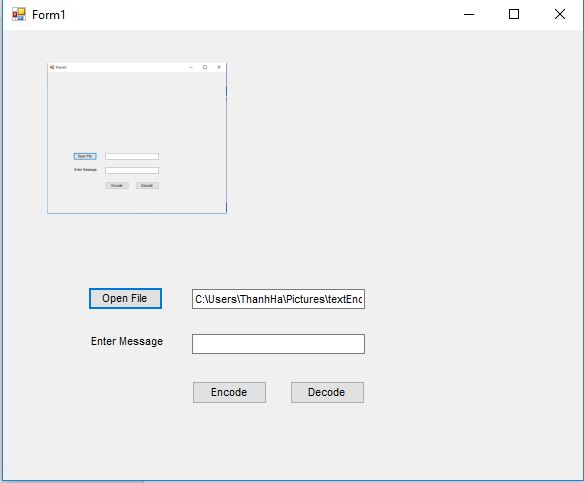


Sau đó, chúng ta sẽ encode và lưu ảnh mà chúng ta đã giấu đoạn mã ở trong đó.

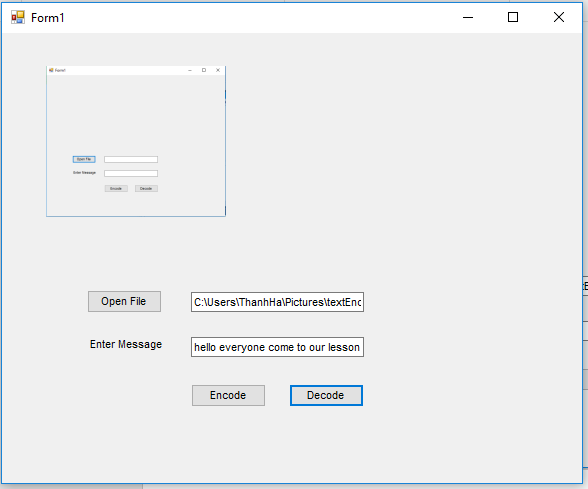


Bước tiếp theo, ta sẽ đi giải mã bức ảnh mà ta mới giấu đoạn mã.

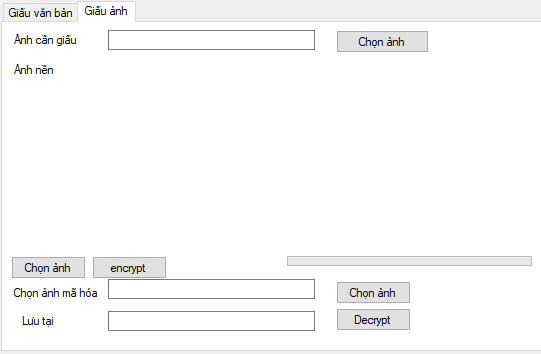




Bấm vào nút decode để giải mã.



Demo Giấu ảnh trong ảnh



Trường hợp 1: Ảnh giấu có kích thước ảnh nhỏ hơn ảnh nền.

ảnh được giấu

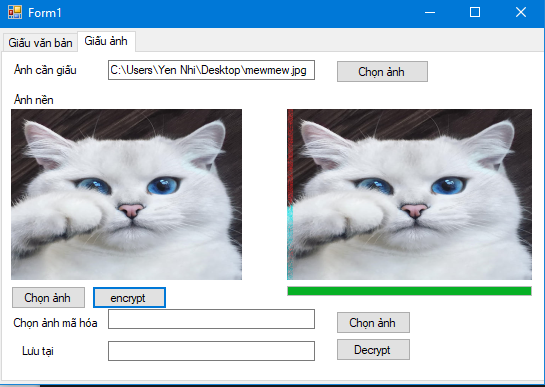
kịch thước: 9.60 kb



Ảnh nền

Kích thước: 48.1 kb





Ảnh sau khi giấu

Kích thước: 622 kb



Nhận xét: Ảnh sau khi bị giấu đã bị thay đổi hình ảnh, không giữ nguyên ảnh gốc ban đầu về mặt hình ảnh. Kích thước ảnh bị thay đổi gấp sấp sỉ 14 lần. Ảnh được giấu sau khi giải mã kích thước tăng lên 191 kb so với ban đầu, chất lượng hình ảnh bằng mắt thường nhìn thấy không thay đổi.

Trường hợp ảnh giấu lớn hơn ảnh nền:

Ảnh nền có kích thước về chiều dài và rộng không giấu được ảnh có kích thước dài rộng lớn hơn.

Với 2 hình cùng kích thước dài rộng nhưng không cùng kích thước kb, hình nền kb nhỏ hơn so với hình giấu ta có kq:

Hình giấu:

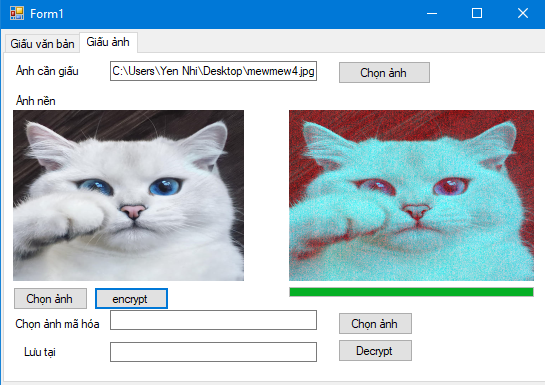
Kích thước: 622kb



Hình nền:

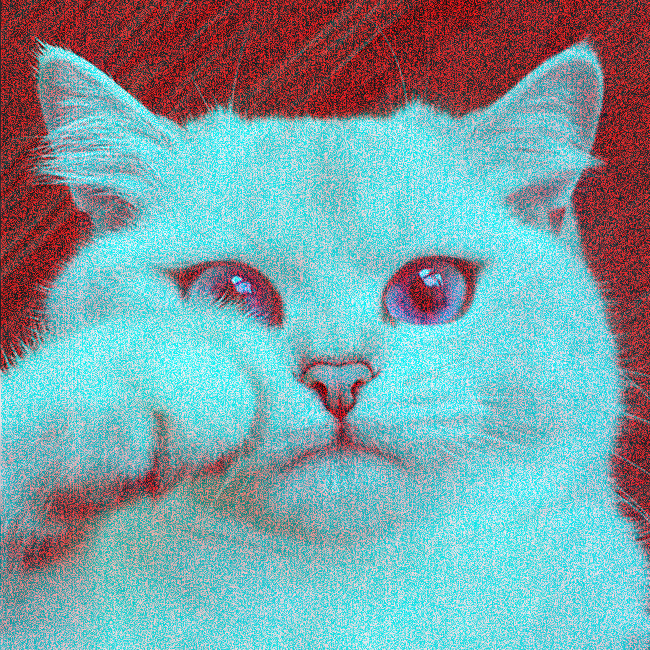
Kích thước: 48.1kb





Ảnh sau khi Giấu

Kích thước 1.07M



Nhận xét: Với ảnh giấu có kích thước ảnh (kb) lớn hơn ảnh nền sẽ làm biến dạng về kích thước(kb) lẫn về mặt hình ảnh.

# Kết luận

Kỹ thuật giấu thông tin trong ảnh số là một trong những hướng nghiên cứu chính của phương pháp giấu thông tin hiện nay và đã đạt được những kết quả khả quan. Đề tài nghiên cứu khoa học này đã tìm hiểu và trình bày lại một số kỹ thuật giấu tin điển hình trong ảnh số.

Do hạn chế về thời gian nên trong đề tài này mới chỉ nghiên cứu kỹ thuật giấu tin trong ảnh định dạng kích cỡ nhỏ, chưa nghiên cứu và thử nghiệm với các định dạng kích cỡ khác. Tuy nhiên báo cáo của nghiên cứu có thể coi làm tài liệu cho sinh viên chuyên ngành CNTT, vì đã tổng hợp và trình bày những khái niệm cơ bản nhất về giấu tin trong ảnh làm nền tảng mới cho các nghiên cứu sau này về an toàn thông tin trong dữ liệu đa phương tiện.

Hướng nghiên cứu tiếp theo của đề tài sẽ nghiên cứu phương pháp giấu tin bền vững trên thùy vân ảnh số,…

# Tài liệu tham khảo.

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

https://text.123doc.org/document/960318-bao-cao-an-ninh-mang-ky-thuat-steganography.htm

<https://securitydaily.net/gioi-thieu-ky-thuat-giau-tin-trong-anh-steganography-phan-2/>

Vladimír Hajduk, Martin Broda, Ondrej Ková, Dušan Levický, “Image Steganography with using QR code and cryptography”,

Faculty of Electrical Engineering and Informatics, Technical University of Košice, Letná 9, 042 00 Košice, Slovak Republic, April

2016

Akshara Gaikwad, KRSingh, “Information Hiding using Image Embedding in QR Codes for Color Images: A Review”,

Department of Computer Technology YCCE, Nagpur (India), International Journal of Computer Science and Information

Technologies, Vol. 6 (1), 2015

https://pdfs.semanticscholar.org/2329/0498a81d929c86653e93c7bf9ff983f9580f.pdf

https://duchm72.wordpress.com/2015/08/03/steganography-an-dau-thong-tin/