TRƯỜNG ĐẠI HỌC HÀNG HẢI VIỆT NAM

KHOA CÔNG NGHỆ THÔNG TIN

-----*-----**

BÁO CÁO BÀI TẬP LỚN
MÔN AN TOÀN BẢO MẬT THÔNG TIN

Chương trình giấu tin trong ảnh

Nhóm 11: **Lê Nguyên Hiệu - 92552**

Phạm Thành Vinh - 92370

Nguyễn Trung Kiên - 90480

Phạm Đức Anh - 91961

Bùi Đức Hải - 93274

Lớp: **An toàn bảo mật thông tin N06 / 2022 – 2023**

Hải Phòng – 05/2023

MỤC LỤC

DANH MỤC HÌNH VẼ BẢNG BIỂU

Mở đầu

Trong cuộc sống hiện nay với sự hình thành và phát triển mãnh mẽ của ngành khoa học công nghệ thông tin đã tạo ra sự thay đổi được đánh giá là bước tiến lớn cho lịch sử phát triển của xã hội, cuộc sống của con người chuyển sang kỉ nguyên của công nghệ và phát triển nền kinh tế tri thức. Cuộc cách mạng công nghiệp 4.0 đã hoàn toàn thay đổi sâu sắc trong cuộc sống của loài người với sự ra đời của một các loại loạt máy móc và các thiết bị hiện đại hỗ trợ công việc của con người như máy tính cá nhân, máy ảnh kỹ thuật số, máy quét, máy in, hay trí tuệ nhân tạo AI, ... Bên cạnh những thiết bị công nghệ tiện ích là hành vi vi phạm bản quyền, ăn cắp thông tin, truy cập trái phép, … . Vậy nên một số kĩ thuật được ra đời để giải quyết hiện trạng trên ví dụ như mã hóa thông tin, chữ ký số, RSA, giấu tin trong các sản phẩm đa phương tiện hay đặc biệt là kĩ thuật ta tìm hiểu ở đây là giấu tin trong ảnh.

Giấu thông tin bí mật (Steganography) có lịch sử hình thành và phát triển từ rất lâu đời, nó bắt nguồn từ Hi Lạp và được sử dụng cho tới ngày nay, chủ yếu phục vụ cho mục đích liên lạc bí mật. Kỹ thuật giấu tin được biết đến bởi hai lĩnh vực chủ yếu là Steganography (giấu tin mật) và Watermarking (thủy vân). Steganography là kỹ thuật giấu tin mật vào các dữ liệu truyền thông (Ảnh, văn bản, nhạc, phim..) để chuyển tải đến người nhận mà thứ ba không thể biết đến sự tồn tại của thông tin mật trong quá trình truyền. Kỹ thuật Steganography cũng làm thay đổi tǫ̛ duy trong lĩnh vực bảo mật thông tin bởi tính khả thi của việc ẩn một lǫ̛ợng thông tin mật trong một dữ liệu thông thường mà khó bị phát hiện bằng giác quan của con ngǫ̛ời. Bên cạnh đó Watermarking được sử dụng chủ yếu trong lĩnh vực bảo vệ bản quyền sản phẩm số bằng cách đưa thông tin bản quyền như tên tác giả, logo.. vào sản phẩm. Với sự tồn tại của thông tin thủy vân nhà sản xuất có thể chứng minh được nguồn gốc của sản phẩm khi sản phẩm được phát tán không hợp pháp. Cả hai kỹ thuật được sử dụng với các mục đích khác nhau song chúng đều có đặc điểm chung là giấu thông tin vào sản phẩm số sao cho không bị phát hiện bởi người thứ ba trong quá trình trao đổi thông tin trên mạng.

Hiện nay kỹ thuật giấu thông tin mật đã được quan tâm, nghiên cứu và được

triển khai ứng dụng rộng rãi trong các cơ quan quân sự, ngoại giao, an ninh, giáo dục và cả các doanh nghiệp khi cần trao đổi các thông tin quan trọng.

CHƯƠNG 1: TỔNG QUAN VỀ KỸ THUẬT GIẤU TIN

Sơ lược về lịch sử giấu tin

Từ *Steganography* bắt nguồn từ thời Hi Lạp cổ và được sử dụng cho tới ngày nay, nó có nghĩa là tài liệu được phủ (covered writing). Các câu chuyện kể về kỹ thuật giấu thông tin được truyền qua nhiều thế hệ. Có lẽ những ghi chép sớm nhất về kỹ thuật giấu thông tin (thông tin được hiểu theo nghĩa nguyên thủy của nó) thuộc về sử gia Hi Lạp Herodotus. Khi bạo chúa Hi Lạp Histiaeus bị vua Darius bắt giữ ở Susa vào thế kỷ thứ năm trước Công Nguyên, ông ta đã gửi một thông báo bí mật cho con rể của mình là Aristagoras ở Miletus. Histiaeus đã cạo trọc đầu của một nô lệ tin cậy và xăm một thông báo trên da đầu của người nô lệ ấy. Khi tóc của ngɑời nô lệ này mọc đủ dài người nô lệ được gửi tới Miletus.

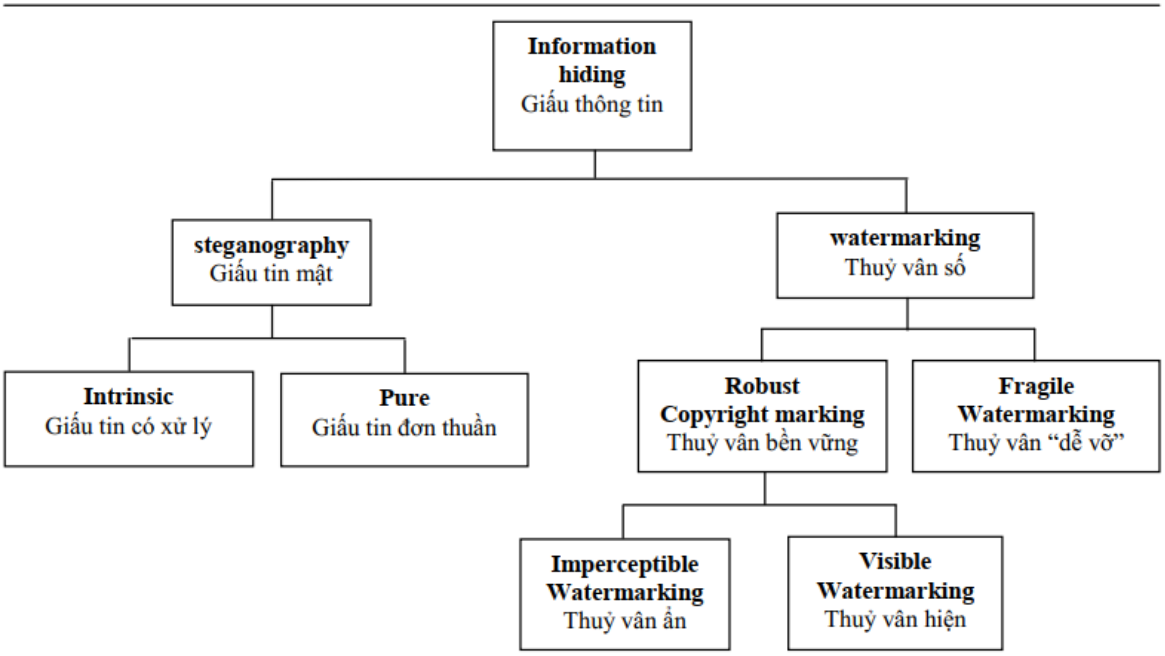
Câu chuyện khác về thời Hi Lạp cổ đại cũng do Herodotus ghi lại. Môi trường để ghi văn bản chính là các viên thuốc được bọc trong sáp ong. Demeratus, một người Hi Lạp, cần thông báo cho Sparta rằng Xerxes định xâm chiếm Hi Lạp. Để tránh bị phát hiện, anh ta đã bóc lớp sáp ra khỏi các viên thuốc rồi khắc thông báo lên bề mặt các viên thuốc này, sau đó bọc lại các viên thuốc bằng một lớp sáp mới. Những viên thuốc được chuyển công khai và lọt qua mọi sự kiểm soát một cách dễ dàng.

Như vậy, ý tưởng về che giấu thông tin đã có từ hàng nghìn năm về trước nhưng kĩ thuật này được dùng chủ yếu trong quân đội và trong các cơ quan tình báo. Mãi cho tới vài thập niên gần đây, giấu thông tin mới nhận được sự quan tâm của các nhà nghiên cứu và các viện công nghệ thông tin với rất nhiều công trình nghiên cứu. Cuộc cách mạng số hóa thông tin và sự phát triển nhanh chóng của mạng truyền thông là nguyên nhân chính dẫn đến sự thay đổi này. Những phiên bản sao chép hoàn hảo, các kĩ thuật thay thế, sửa đổi tinh vi cộng với sự lưu thông trên mạng của các dữ liệu đa phương tiện đã sinh ra rất nhiều những vấn đề nhức nhối về nạn ăn cắp bản quyền, phân phối bất hợp pháp, xuyên tạc trái phép… đây là lúc công nghệ giấu tin được chú ý và phát triển.

Khái niệm giấu tin

"Giấu tin" là một kỹ thuật nhúng (giấu) một lượng thông tin số nào đó vào trong một đối tượng dữ liệu số khác. Kỹ thuật giấu tin nhằm hai mục đích: một là bảo mật cho dữ liệu được đem giấu, hai là bảo vệ cho chính đối tượng mang tin giấu. Hai mục đích khác nhau này dẫn đến hai kỹ thuật chủ yếu của giấu tin. Đó là giấu tin mật (Steganography) và thủy vân số (Watermarking).

Kỹ thuật giấu tin



Hình 1. Các kỹ thuật giấu tin chính

- Kỹ thuật giấu tin mật (Steganography): Với mục đích đảm bảo an toàn và bảo mật thông tin được giấu. Các kỹ thuật giấu tin mật tập trung vào việc sao cho thông tin giấu được nhiều và người khác khó phát hiện ra thông tin có được giấu trong hay không.
- Kỹ thuật thủy vân số (Watermarking): Với mục đích bảo mật cho chính các đối tượng giấu tin. Đảm bảo một số các yêu cầu như: tính bền vững, khẳng định bản quyền sở hữu hay phát hiện xuyên tạc thông tin…

Nói chung giấu tin trong đa phương tiện là tận dụng "độ dư thừa" của phương tiện giấu để thực hiện việc giấu tin mà người ngoài cuộc "khó" cảm nhận được có thông tin giấu trong đó.

Steganography	Watermarking
- Tập trung vào việc giấu được càng nhiều thông tin càng tốt, ứng dụng trong truyền dữ liệu thông tin mật. - Cố gắng làm nhỏ nhất những ảnh hưởng đến chất lượng của đối tượng vỏ để không bị chú ý đến dữ liệu đã được giấu trong đó. - Thay đổi stego-object cũng làm cho dữ liệu giấu bị sai lệch (nhất là ứng dụng trong nhận thực thông tin)	- Không cần giấu nhiều thông tin, chỉ cần lượng thông tin nhỏ đặc trưng cho bản quyền của người sở hữu. - Trong trường hợp thuỷ vân nhìn thấy thì thuỷ vân sẽ hiện ra. - Thuỷ vân phải bền vững với mọi tấn công có chủ đích hoặc không có chủ đích vào sản phẩm.

Hình 2. Phân biệt kỹ thuật Steganography và Watermarking

Môi trường giấu tin

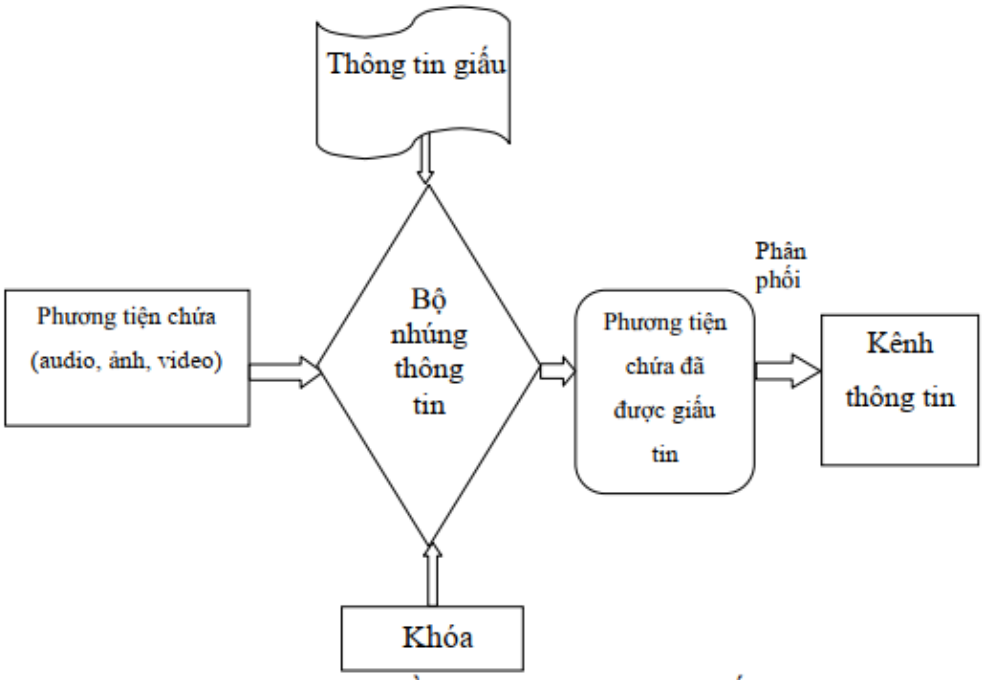
Bao gồm giấu tin trong ảnh, trong audio, trong video, trong văn bản dạng text… Hiện nay, giấu tin trong ảnh chiếm tỉ lệ lớn nhất hệ thống giấu tin trong đa phương tiện.

Mô hình kỹ thuật giấu thông tin cơ bản

Để thực hiện giấu tin cần xây dựng được các thủ tục giấu tin. Các thủ tục này sẽ thực hiện nhúng thông tin cần giấu vào môi trường giấu tin. Các thủ tục giấu tin thường được thực hiện với một khóa giống như các hệ mật mã để tăng tính bảo mật Sau khi giấu tin ta thu được đối tượng chứa thông tin giấu và có thể phân phối đốitượng đó trên kênh thông tin.

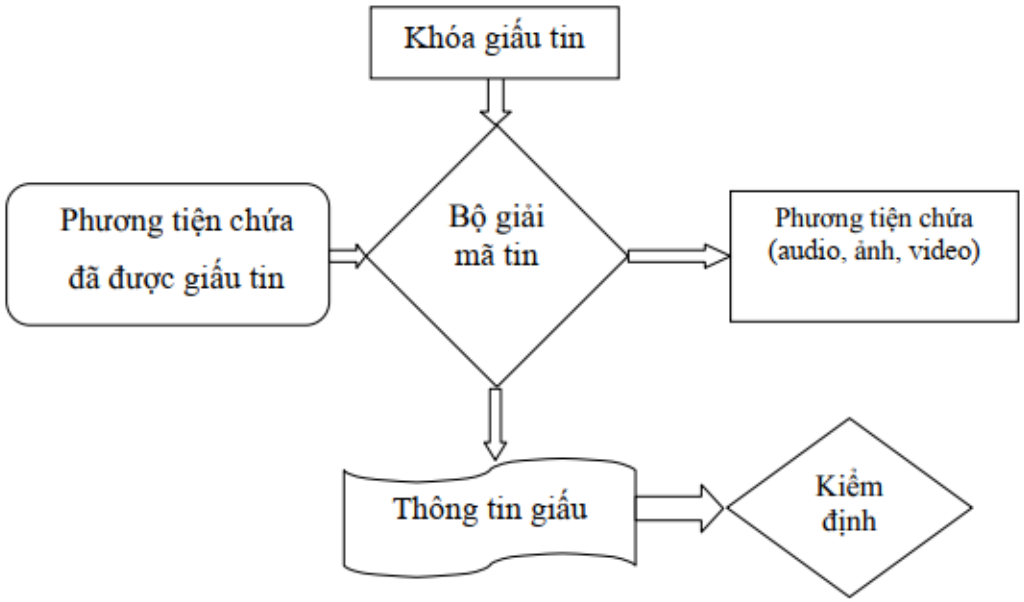
Giấu thông tin vào phương tiện chứa và tách lấy thông tin là hai quá trình trái ngược nhau và có thể mô tả qua sơ đồ khối của hệ thống trong đó:

- Thông tin cần giấu tuỳ theo mục đích của người sử dụng, nó có thể là thông điệp (với các tin bí mật) hay các logo, hình ảnh bản quyền.
- Phương tiện chứa: các file ảnh, text, audio… là môi trường để nhúng tin.
- Bộ nhúng thông tin: là những chương trình thực hiện việc giấu tin.
- Đầu ra: là các phương tiện chứa đã có tin giấu trong đó.



Hình 3. Lược đồ kỹ thuật giấu tin

Tách thông tin từ các phương tiện chứa diễn ra theo quy trình ngược lại với đầu ra là các thông tin đã được giấu vào phương tiện chứa. Phương tiện chứa sau khi tách lấy thông tin có thể được sử dụng, quản lý theo những yêu cầu khác nhau.



Hình 4. Lược đồ kỹ thuật giải mã

Sau khi nhận được đối tượng phương tiện chứa có giấu thông tin, quá trình giải mã được thực hiện thông qua một bộ giải mã tương ứng với bộ nhúng thông tin cùng với khoá của quá trình nhúng. Kết quả thu được gồm phương tiện chứa gốc và thông tin đã giấu. Bước tiếp theo thông tin đã giấu sẽ được xử lý kiểm định so sánh với thông tin ban đầu.

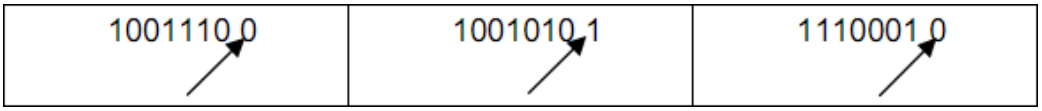
CHƯƠNG 2: KỸ THUẬT GIẤU TIN TRÊN K BIT LSB CỦA ẢNH

1. 1. Bit ít quan trọng LSB (Least Signification Bit)

Ý tưởng cơ bản của kỹ thuật này là tiến hành giấu tin vào vị trí các bit ít quan trọng LSB đối với mỗi phần tử trong bảng màu.

Đây là phương pháp giấu tin đơn giản nhất, thông điệp dưới dạng nhị phân sẽ được giấu (nhúng) vào các bit LSB – là bit có ảnh hưởng ít nhất tới việc quyết định tới màu sắc của mỗi điểm ảnh. Vì vậy khi ta thay đổi bit ít quan trọng của một điểm ảnh thì màu sắc của mỗi điểm ảnh mới sẽ tương đối gần với điểm ảnh cũ. Ví dụ đối với ảnh 16 bit thì 15 bit là biểu diễn 3 màu RGB của điểm ảnh còn bit cuối cùng không dùng đến thì ta sẽ tách bit này ra ở mỗi điểm ảnh để giấu tin…

Ví dụ: Tách bit cuối cùng trong 8 bit biểu diễn mỗi điểm ảnh của ảnh 256 màu.



Hình 2.1. Mỗi điểm ảnh bểu diễn bởi 8 bit bit cuối cùng được coi là bit ít quan trọng nhất tức là bit bên phải nhất

Trong phép tách này ta coi bit cuối cùng là bit ít quan trọng nhất, thay đổi giá trị của bit này thì sẽ thay đổi giá trị của điểm ảnh lên hoặc xuống đúng một đơn vị, với sự thay đổi nhỏ đó ta hi vọng là cấp độ màu của điểm ảnh sẽ không bị thay đổi nhiều.

Bảng 2.1. Ví dụ giấu chữ A (mã ASCII là 65 hay 01000001) vào trong 8 byte của file gốc

8 byte ban đầu	Byte cần giấu (A)	8 byte sau khi giấu

01001001	0	01001000
11010111	1	11010111
11001100	0	11001100
10110101	0	10110100
00100100	0	00100100

00100101	0	00100100
00100000	0	00100000
00001010	1	00001011

2. 2. Phương pháp giấu tin trên k-LSBs cổ điển

2. 2. 1. Mô tả phương pháp giấu tin trên k-LSBs đơn giản (cổ điển)

Với C là ảnh nguyên bản 8-bit màu xám, kích thước $M_c \times N_c$ điểm ảnh, có dạng:

$$C = \{x_{ij} | \ 0 \le i \le M_c, 0 \le j \le N_c , x_{ij} = \{0, 1, 2, \ldots, 255\}\}$$

và M là thông điệp dài n bit biểu diễn dưới dạng:

$$\mathbf{M = \{m_i \mid 0 \le i < n, m_i \in \{0,1\}\}}$$

Giả sử rằng n-bit thông điệp bí mật M được nhúng vào k bit LSB ngoài cùng bên phải của ảnh gốc C. Trước tiên, thông điệp bí mật M được sắp xếp lại để tạo thành một hình ảnh ảo k-bit, biểu diễn M dưới dạng:

$$\mathbf{M' = \{m_i' | 0 \le i < n', m_i' \in \{0, 1, \ldots, 2^k - 1\}\}}$$

Với $n' = M_c \times N_c$. Việc ánh xạ giữa các n-bit thông điệp bí mật $M = \{m_i\}$ và thông điệp nhúng $M' = \{m_i'\}$ có thể được định nghĩa như sau:

$$m_i' = \sum_{j=0}^{K-1} m_i \times k + j \times 2^{k-1-j}$$

Thứ hai, tập hợp con n' điểm ảnh $\{x_1, x_2, \ldots, x_n\}$ được chọn từ ảnh gốc C trong 1 chuỗi hành động liên tiếp nhau. Tiến trình nhúng hoàn tất bằng việc thay thế k-LSBs của x_i bởi m_i'. Theo toán học, một giá trị x_i của điểm ảnh được lựa chọn để lưu trữ k-bit thông điệp m_i' được thay đổi khớp với điểm ảnh đã giấu tin x'_i như sau:

$$X'_i = x_i - x_i \bmod 2^k + m'_i$$

Trong tiến trình tách, với ảnh đã giấu tin S, thông điệp nhúng có thể được tách

ra mà không đề cập đến ảnh gốc. Sử dụng cùng một trình tự như trong quá trình nhúng, tập hợp các điểm ảnh $\{x'_1, x'_2, \dots, x'_n, \}$ lưu trữ các bit thông điệp bí mật được lựa chọn từ ảnh đã giấu tin. K-LSBs của các điểm ảnh được tách ra và nối lại để tái tạo lại thông điệp bí mật. Trong toán học, việc nhúng thông điệp bit m_i có thể được khôi phục bằng:

$$m"_i = x"_i \bmod 2^k$$

2. 2. 2. Tiền xử lý thuật toán giấu và tách tin LSB cổ điển

- Để có thể thực hiện tốt chương trình, trước hết cần bổ sung một số hàm thành phần với mục đích cài đặt chương trình thuận lợi:
  - Hàm chuyển đổi từ chuỗi kí tự sang số nhị phân.
  - Hàm chuyển đổi từ chuỗi số nhị phân sang chuỗi kí tự.
- Tóm tắt thuật toán thay thế LSB đơn giản:

2. 2. 1. Thuật toán giấu

Đầu vào:

- Ảnh gốc cấp xám.
- Thông điệp bí mật.
- Số bit LSB cần mã hóa (2 hoặc 4 bit).

Đầu ra:

- Ảnh mang tin.

Các bước thực hiện:

- Bước 1: Biểu diễn ma trận điểm ảnh về dạng số thập phân với m x n phần tử, rồi chuyển ma trận ảnh về mảng 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 đưa 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 chuỗi nhị phân thông điệp ghép với các bit ảnh. Chuyển đổi ảnh I từ mảng một chiều về mảng 2 chiều m x n phần tử. Được ảnh mới đã giấu tin.

2. 2. 2. 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 m x n phần tử. Chuyển đổi ma trận ảnh m x n 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 kí tự. Sau khi lặp lại quá trình trên số lần bằng số lần duyệt, ta thu được nội dung thông điệp.

❖ Với trường hợp giấu trên 4 bit thông điệp làm tương tự, nhưng tách lấy 4 bit nhị phân đầu của ảnh ghép với 4 bit nhị phân thông điệp.

2. 3. Phương pháp giấu tin trên k-LSBs nâng cao

- Tác giả: Marghny Mohamed, Fadwa Al-Afari và Mohamed Bamatraf.
- Tài liệu sử dụng: Data Hiding by LSB Substitution Using Genetic Optimal Key-Permutation (Giấu tin bằng phương pháp thay thế LSB sử dụng khóa hoán vị di truyền tối ưu), Tạp chí Quốc tế Ả Rập Điện tử - Công nghệ, Vol. 2, số 1, tháng 1 năm 2011.

2. 3. 1. Mô tả phương pháp giấu tin trên k-LSBs nâng cao (sử dụng khóa hoán vị)

Đây là phương pháp tối ưu khi k là rất lớn. Những hình ảnh C, và thông điệp bí mật M sẽ được sắp xếp lại hình thành các khối bit (blk) C" và M" tương ứng.

$$C'' = \{c''_i \mid 0 \le i \le 2^{blk}-1 \mid c_i'' \in \{0, 1, 2, \dots, 2^{blk}-1\}\}$$

$$M'' = \{m''_i \mid 0 \le i \le 2^{blk}-1 \mid m''_i \in \{0, 1, 2, \ldots, 2^{blk}-1\}\}$$

Theo toán học, quá trình mã khối sẽ được lấy bằng cách thực hiện trên bit XOR điều hành mỗi khối C"" và M"" như sau:

if ($cipher_i = c''_i$ xor m''_i, $1 \le i \le length(M)$ in blk (M_{blk}))

cipher = $\{cipher \mid 1 \le i \le length(M'')$ in blk | $cipher_i = \{0, 1, 2, \ldots, 2^{blk}-1\}\}$

$cipher_i = \{0, 1, 2, \ldots, 2^{blk}-1\}\}$

$i = c''_i$ xor m''_i

end

2. 3. 2. Tiền xử lý thuật toán giấu và tách tin LSB nâng cao

- Để có thể thực hiện tốt chương trình, trước hết cần bổ sung một số hàm thành phần với mục đích cài đặt chương trình thuận lợi:
  - Hàm mã hóa thông điệp.
  - Hàm giải mã thông điệp.
  - Với phương pháp giấu và tách tin nâng cao có quy đổi ta sử dụng bảng sau để quy đổi:

Bảng 2.2. Bảng quy đổi

STT	Kí tự	Mã quy đổi	STT	Kí tự	Mã quy đổi
1	A, a	000001	20	T, t	010100
2	B, b	000010	21	U, u	010101
3	C, c	000011	22	V, v	010110
4	D, d	000100	23	W, w	010111
5	E, e	000101	24	X, x	011000
6	F, f	000110	25	Y, y	011001
7	G, g	000111	26	Z, z	011010
8	H, h	001000	27	0	011011
9	I, i	001001	28	1	011100
10	J, j	001010	29	2	011101
11	K, k	001011	30	3	011110
12	L, l	001100	31	4	011111
13	M, m	001101	32	5	100000
14	N, n	001110	33	6	100001
15	O, o	001111	34	7	100010
16	P, p	010000	35	8	100011
17	Q, q	010001	36	9	100100
18	R, r	010010	37	„ „	100101
19	S, s	010011			

- Tóm tắt thuật toán thay thế k bit LSB nâng cao:

Trường hợp không quy đổi thông điệp:

2. 3. 2. 1. Thuật toán giấu

Đầu vào:

- Ảnh gốc cấp xám.
- Thông điệp bí mật.
- Khóa (8 bit).
- Số bit LSB cần mã hóa trên mỗi điểm ảnh (2 hoặc 4 bit).

Đầu ra:

- Ảnh mang tin.
- Khóa.
- Số bit thông điệp cần mã hóa.

Các bước thực hiện:

- Bước 1: Biểu diễn ma trận điểm ảnh về dạng số thập phân với m x n phần tử. Chuyển đổi ma trận ảnh m x n phần tử về mảng 1 chiều I với i phần tử.
- Bước 2: Biểu diễn thông tin giấu dưới dạng chuỗi nhị phân.
- Bước 3: Sử dụng một khóa 8 bit bất kỳ (khóa là kí tự, chuyển khóa về dạng mảng như với thông điệp) đem mã hóa với chuỗi thông điệp bí mật bằng phép XOR: cứ 8 bit khóa đem XOR với 8 bit đầu vào của thông điệp. Thực hiện lại bước này cho đến khi nội dung thông điệp được mã hóa hết.
- Bước 4: Thông điệp đã mã hóa đem giấu vào ảnh tương tự như phương pháp thay thế k bit LSB 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 bit ảnh. Chuyển đổi ảnh I từ mảng một chiều về mảng 2 chiều m x n phần tử, được ảnh mới đã giấu tin.

2. 3. 2. 2. Thuật toán tách

Đầu vào:

- Ảnh đã giấu tin.
- Khóa (8 bit).
- Số lần duyệt.
- Số bit thông điệp cần mã hóa.

Đầu ra:

- Ảnh đã tách tin.
- Thông điệp.

Các bước thực hiện:

- Bước 1: Biểu diễn ma trận điểm ảnh về dạng số thập phân với m x n phần tử. Chuyển đổi ma trận ảnh m x n 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 kí tự. Sau khi lặp lại quá trình trên số lần 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 gốc của thông điệp.

❖ Trường hợp chuyển đổi thông điệp về bảng mã đã được quy ước sẵn: Tương tự như trường hợp chuyển đổi kí tự về mã nhị phân của nó, nhưng ở đây khi giấu tin ta sử dụng bảng quy đổi các kí tự và chữ số theo một chuẩn do người lập trình tự định nghĩa. Đến bước tách ta lại quy đổi ngược lại về dạng kí tự và số ban đầu.

2. 4. Ví dụ minh họa

2. 4. 1. Trường hợp giấu và tách tin LSB cổ điển

2. 4. 1. 1. Giấu tin

Giả sử ta có 4 điểm ảnh đầu tiên như sau:

123 197 213 255

Chuyển các điểm ảnh về dạng nhị phân:

01111011 11000101 11010101 11111111

Thông điệp bí mật: chữ „a" có mã ASCII là 97, biểu diễn dưới dạng nhị phân như sau: **01100001**

Cứ 8 bit ảnh, ta lấy 6 bit đầu của điểm ảnh (từ vị trí I_0 đến I_5) ghép với 2 bit thông điệp (từ vị trí a_0 đến a_1) sẽ được:

01111001 11000110 11010100 11111101

2. 4. 1. 2. Tách tin

Lấy 2 bit ngoài cùng bên phải trong mỗi điểm ảnh mới:

011110-01 110001-10 110101-00 111111-01

Ghép lại với nhau được chuỗi nhị phân thông điệp, chính là chữ „a":

0110001

2. 4. 2. Trường hợp giấu và tách tin LSB nâng cao

2. 4. 2. 1. Giấu tin

Giả sử ta có 4 điểm ảnh đầu tiên như sau:

123 197 213 255

Chuyển các điểm ảnh về dạng nhị phân:

01111011 11000101 11010101 11111111

Thông điệp bí mật: chữ „a" có mã ASCII là 97, biểu diễn dưới dạng nhị phân:

01100001

Nhập khóa, cũng là 1 kí tự 8 bit, giả sử là chữ „b", có dạng nhị phân như sau:

01100010

Mã hóa thông điệp chính là dùng phép XOR(a, b) sẽ được:

00000011

Cứ 8 bit ảnh, ta lấy 6 bit đầu của điểm ảnh ghép với 2 bit thông điệp đã mã hóa sẽ được:

01111000 11000100 11010100 11111111

2. 4. 2. 2. Tách tin

Lấy 2 bit ngoài cùng bên phải trong mỗi điểm ảnh mới:

011110-00 110001-00 110101-00 111111-11

Ghép lại với nhau được chuỗi nhị phân thông điệp nhưng đã bị mã hóa:

00000011

Sử dụng hàm mã hóa để lấy lại thông điệp gốc M, bằng cách XOR(M, b) ta được nhị phân của chữ „a": **01100001**

- Trường hợp giấu và tách tin LSB nâng cao có quy đổi, tương tự như trên nhưng không chuyển chữ „a" về dạng nhị phân mà a =>**000001**.

CHƯƠNG 3: CÀI ĐẶT CHƯƠNG TRÌNH ỨNG DỤNG

Để xây dựng chương trình,ta cần thiết kế các module như sau:

- Xây dựng 1 class có tên là CryptoHelper.cs chứa 2 phương thức
  1. `public static byte[] Encrypt(byte[] message,string password)`

     Phương thức này nhận vào 2 tham số gồm: thông điệp mà ta muốn mã hóa và mật khẩu để trao đổi tin giữa người gửi và người nhận. Phương thức này sẽ biến đổi mật khẩu thành 1 khóa có độ dài 128 byte thông qua lớp `PasswordDeriveBytes` của Microsoft.NET nhằm tăng tính bảo mật. Sau đó kết hợp trộn giữa thông điệp và khóa này bằng toán tử XOR để tạo ra mảng byte là cái ta thực sự đem giấu vào trong bức ảnh.

  2. `public static byte[] Decrypt(byte[] message, string password)`

     Phương thức này là quá trình giải mã ngược của phương thức trên,tham số thứ nhất là mảng byte sau khi đã trích ra được từ file ảnh cần giải mã,tham số thứ 2 là mật khẩu để lấy thông tin do người nhận nhập vào,với mật khẩu này,ta cũng dùng lớp `PasswordDeriveBytes` của Microsoft.NET để tạo ra 1 khóa 128byte (lưu ý rằng nếu người dùng nhập đúng mật khẩu,thì nó cũng sẽ sinh ra cùng 1 khóa như lúc ta mã hóa). Dùng phép XOR giữa mảng byte và khóa này ta sẽ nhận được thông điệp gốc ban đầu.

- Xây dựng 1 class có tên là LSBHelper.CS chứa 2 phương thức
  1. `public static void Encode(FileStream inStream,byte[] Message,FileStream outStream)`

     Phương thức này nhận vào 3 tham số: file ảnh đầu vào,mảng các byte cần đưa vào trong ảnh,và ảnh đầu ra.

  2. `public static byte[] Decode(FileStream inStream,int length)`

     Phương thức này nhận vào 1 file ảnh có chứa tin giấu, độ dài của thông điệp chứa trong đó. Kết quả trả về là 1 mảng các byte mà ta đã giấu trong thủ tục Encode ở trên.

KẾT LUẬN

Giấu tin trong ảnh vẫn là một chủ đề khá mới mẻ và đặc sắc trong lĩnh vực an toàn và bảo mật thông tin, mà cần nhiều hơn sự nghiên cứu và tìm hiểu để có thể hoàn thiện một cách trọn vẹn và đa chiều nhất về chủ đề này. Thông qua bài báo cáo này, chúng em đã nghiên cứu những vấn đề sau:

- Nghiên cứu tổng quan kỹ thuật giấu tin trong ảnh.
- Nghiên cứu cấu trúc ảnh Bitmap.
- Tìm hiểu kỹ thuật và cài đặt chương trình giấu tin trên k bit LSB của ảnh

Tuy nhiên chương trình vẫn còn nhiều hạn chế như mật độ giấu tin chưa cao,khi độ dài của thông điệp quá lớn so với dung lượng của bức ảnh thì sẽ không thực hiện được. Song đây cũng là cơ sở để tiếp tục phát triển chương trình cũng như triển khai thuật toán hiệu quả hơn. Chúng em rất mong nhận được sự góp ý quý báu của tất cả các thầy cô giáo để báo cáo của chúng em được hoàn thiện hơn.

Em xin chân thành cảm ơn!

Dưới đây là bảng phân công công việc của nhóm:

STT	Mã SV	Họ Tên	Công việc
1	92552	Lê Nguyên Hiệu	Làm PowerPoint, cài đặt chương trình
2	92370	Phạm Thành Vinh	Soạn và hoàn thiện báo cáo, hỗ trợ PP
3	90480	Nguyễn Trung Kiên	Tìm hiểu, cung cấp thông tin cho báo cáo
4	93274	Bùi Đức Hải	Tìm hiểu, thuyết trình bài tập lớn
5	91961	Phạm Đức Anh	Làm PowerPoint, cài đặt chương trình

TÀI LIỆU THAM KHẢO

1. **Giấu tin trong ảnh nhị phân và ứng dụng**, PGS.TS Phạm Văn Ất,ThS Nguyễn Hữu Cường, Khoa công nghệ thông tin, Trường ĐH giao thông vận tải.
2. **Một số thuật toán giấu tin và áp dụng giấu tin mật trong ảnh**. PGS.TS Nguyễn Văn Tảo, Đỗ Trung Tuấn, Bùi Thế Hồng báo cáo tại hội thảo RDA 8.

   Tiếng Anh:
3. **Fridrich, J.: A New Steganographic Method for Palette-Based Images**. Proc. of the IS&T PICS conference, April 1998, Savannah, Georgia (1998) 285–289.
4. **Digital Steganography:** *Hiding data within Data*. Donovan Artz
5. **Information Hiding:** Steganography & Digital Watermarking