TỔNG QUAN VỀ KỸ THUẬT GIẤU TIN VÀ GIẤU TIN TRONG ẢNH SỐ
OVERVIEW ON DATA HIDING TECHNIC AND DATA HIDING IN DIGITAL IMAGES

ThS. NGUYỄN HẠNH PHÚC
Khoa Công nghệ Thông tin, Trường ĐHHH

Tóm tắt:

Bài viết này đưa ra cách nhìn tổng quan về kỹ thuật giấu tin nói chung cũng như kỹ thuật giấu tin trong ảnh số nói riêng. Đồng thời, tác giả cũng trình bày một số ứng dụng của kỹ thuật giấu tin trong ảnh số.

Abstract:

The article presents an overview on data hiding in general and data hiding in digital images. Besides, the author would like to introduce applications of data hiding in digital images.

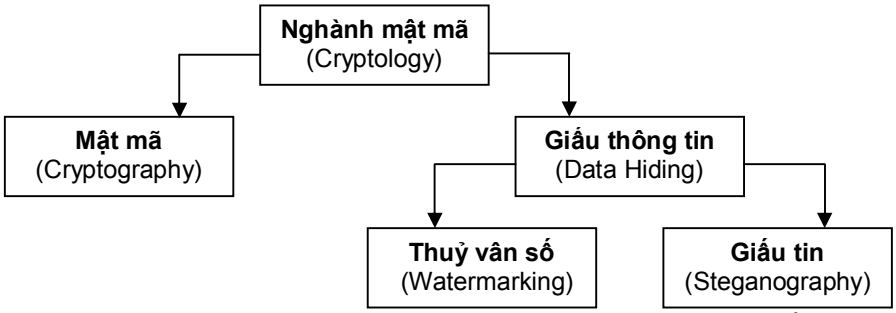
1. Định nghĩa

"Giấu thông tin là nghệ thuật nhúng mẩu tin mật vào một vật mang tin khác. Giấu tin trong ảnh số là giấu các mẩu tin cũng là dạng số trong máy tính vào các ảnh nhị phân sao cho không bị phát hiện."

Thuật ngữ giấu thông tin là **steganography** (bắt nguồn từ tiếng Hy Lạp - có nghĩa là covered writing).

2. Giấu tin và mật mã

Có thể coi nghệ thuật giấu tin là một nhánh của ngành mật mã với mục tiêu là nghiên cứu các phương pháp che giấu thông tin mật.



Steganography (Cover writing): Là nghệ thuật/khoa học/công việc truyền tin mà trong đó các thông ẩn được giấu trong thông tin chính.

Cryptography (Secret writing): Là nghiên cứu phương pháp gửi thông điệp dưới hình thức khác nhau sao cho chỉ người nhận mong đợi mới bỏ đi che giấu để đọc thông điệp.Thông điệp muốn gửi đi gọi là ***bản rõ***. Thông điệp bị che giấu gọi là ***bản mã hóa***. Sau khi người nhận loại bỏ che giấu để đọc thông tin thì thông điệp không còn được bảo vệ nữa.

Giấu tin và mật mã tuy cùng có mục đính là để đối phương không phát hiện ra tin cần giấu, tuy nhiên nó khác với mật mã ở chỗ:

+ Mật mã: Giấu đi ý nghĩa của bản thông tin.
+ Giấu tin: Giấu đi sự hiện diện của thông tin.

Watermarking (thuỷ ấn) là lĩnh vực nghiên cứu việc nhúng các thông tin phục vụ xác thực, ví dụ như xác nhận bản quyền. Nếu thông tin giấu là một định danh duy nhất, ví dụ định danh người dùng thì khi đó người ta gọi là **Fingerprinting** (nhận dạng vân tay, điểm chỉ).

Steganography (giấu tin, viết phủ) là lĩnh vực nghiên cứu việc nhúng các mẩu tin mật vào một môi trường phủ. Trong quá trình giấu tin để tăng bảo mật có thể người ta dùng một khoá viết mật khi đó người ta nói về **Intrinsic Steganography** (giấu tin có xử lý). Khi đó để giải mã người dùng cũng phải có khoá viết mật đó. Chú ý rằng khoá này không phải là khoá dùng để lập mật mã mẩu tin, ví dụ nó có thể là khoá để sinh ra hàm băm phục vụ rải tin vào môi trường phủ. Ngược

lại nếu không dùng khoá viết mật thì người ta chỉ giấu tin đơn thuần vào môi trường phủ thì khi đó người ta nói về **Pure Steganography** (giấu tin đơn thuần).

Xét về tính chất, thuỷ ấn giống giấu tin ở chỗ tìm cách nhúng thông tin mật vào một môi trường. Tuy nhiên xét về bản chất thì thuỷ ấn có những nét khác ở một số điểm:

+ Mục tiêu của thuỷ ấn là nhúng thông tin không lớn thường là biểu tượng, chữ ký hay các đánh dấu khác vào môi trường phủ nhằm phục vụ việc xác nhận bản quyền

+ Khác với giấu tin ở chỗ, giấu tin sau đó cần tách lại tin còn thuỷ ấn tìm cách biến tin giấu thành một thuộc tính của vật mang

+ Chỉ tiêu quan trọng nhất của một thuỷ ấn là tính bền vững, của giấu tin là dung lượng bản tin được giấu

+ Điểm khác nữa giữa thuỷ ấn và giấu tin là thuỷ ấn có thể vô hình hoặc hữu hình trên ảnh mạng.

3. Giấu tin trong ảnh số

Giấu tin trong ảnh được thực hiện bằng cách thay thế một vài thông tin ít quan trọng nhất của ảnh gốc. Đối với ảnh màu: Sử dụng các bit thấp (least-significant bit -LSB) của mỗi pixel để giấu thông tin.*Thí dụ, ảnh Kodak Photo CD kích thước 2048x3072x24 bit màu RGB có thể giấu tới 2.36 Mb bit thông tin.* Ảnh 2 màu đen/trắng (ảnh nhị phân) (trang fax, mã vạch...) sẽ khó khăn hơn vì khi thay đổi 1 pixel ảnh thì mắt người dễ nhận biết. Ảnh JPEG hay MP3 của âm thanh: Phức tạp hơn. Phải tìm ra các "lỗ hổng" sao cho chất lượng ảnh ít bị ảnh hưởng khi thực hiện thuật toán nén và giải nén ảnh.

4. Kỹ thuật chung giấu thông tin trong ảnh

Chọn vị trí giấu thông tin:

- Vị trí ngẫu nhiên trong ảnh gốc
- Vùng tần số trung bình hay tần số cao (biên ảnh)

- Miền ảnh có tần số càng cao thì mắt người càng kém phân biệt sự thay đổi

Chọn miền giấu thông tin:

- Giấu thông tin trong miền quan sát: Thực hiện trực tiếp trên ma trận ảnh
- Giấu thông tin trong miền DFT, DCT hay DWT.
- Sau đó biến đổi ngược lại miền quan sát

Chọn kiểu chèn thông tin giấu :

- Cộng trực tiếp thông tin vào miền giá trị của ảnh.
- Thay đổi cách biểu diễn giá trị ảnh theo cách biểu diễn của thông tin ẩn

Chọn kiểu tách thông tin ẩn :

- Chọn kiểu tách thông tin ẩn
- Tách thông tin ẩn tương tự tách tín hiệu nhiễu.
- Các bước tách thông tin ẩn là các bước ngược lại của tiến trình chèn thông tin ẩn

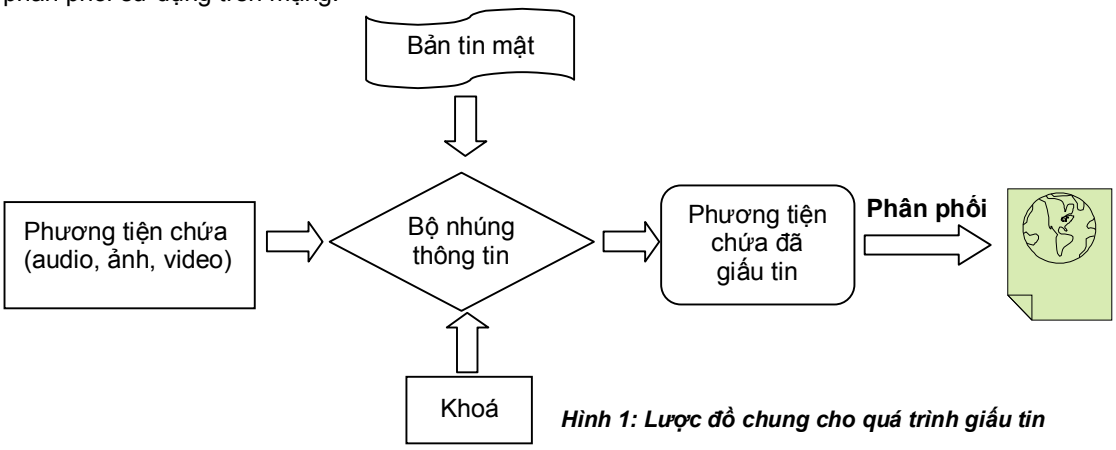
5. Các thành phần chính của một hệ giấu tin trong ảnh số

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

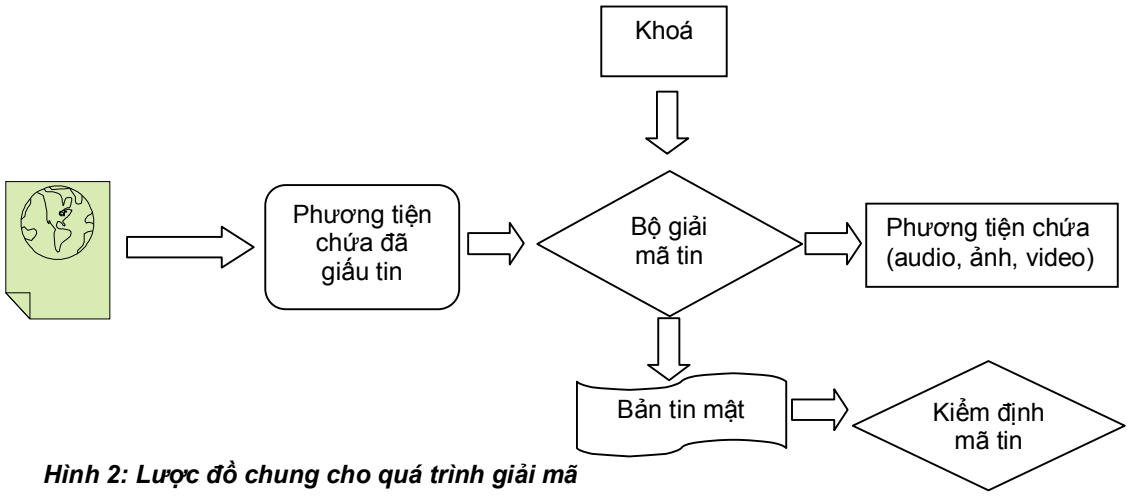
- **Bản tin mật** (Secret Message): Có thể là văn bản hoặc tệp ảnh hay bất kỳ một tệp nhị phân nào, vì quá trình xử lý chúng ta đều chuyển chúng thành chuỗi các bit.
- **Ảnh phủ** (hay ảnh gốc) (Cover Data): Là ảnh được dùng để làm môi trường nhúng tin mật.
- **Khoá bí mật K** (Key): Khoá viết mật tham 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 nhúng tin mật vào đó
- **Kiểm định** (Control) : Kiểm tra thông tin sau khi được giải mã.

Mô hình của kỹ thuật giấu tin cơ bản được mô tả theo hai hình vẽ dưới đây:

Hình 1 biểu diễn quá trình giấu tin cơ bản. Phương tiện chứa bao gồm các đối tượng được dùng làm môi trường giấu tin như: text, audio, video, ảnh, bản tin mật là một lượng thông tin mang một ý nghĩa nào đó như ảnh, logo, đoạn van bản… tuỳ thuộc vào mục đích của người sử dụng . Thông tin sẽ được giấu vào trong phương tiện chứa nhờ một bộ nhúng, bộ nhúng là những chương trình, triển khai các thuật toán để giấu tin và được thực hiện với một khoá bí mật giống như các hệ mật mã cổ điển. Sau khi giấu tin, ta thu được phương tiện chứa bản tin đã giấu và phân phối sử dụng trên mạng.



Hình 1: Lược đồ chung cho quá trình giấu tin



Hình 2: Lược đồ chung cho quá trình giải mã

Hình 2 chỉ ra các công việc giải mã thông tin đã giấu. Sau khi nhận được đối tượng phương tiện chứa có giấu thông tin, quá trình giải mã được thực hiện thông qua bộ nhúng thông tin cùng với khoá của quá trình nhúng. Kết quả thu được gồm phương tiện chứa gốc và bản tin mật đã được giấu. Bước tiếp theo bản tin mật thu được sẽ được xử lý kiểm định so sánh với thông tin giấu ban đầu.

Sơ đồ phân loại trên (hình 1,2) được Fabien A. P. Petitcolas đề xuất năm 1999.

6. Giải pháp giấu tin trong ảnh số

Giải pháp 1: *Giấu tin vào miền quan sát*

Phương pháp này đơn giản nhất vì không yêu cầu biến đổi sang miền tần số. Thông tin ẩn chèn trực tiếp vào pixel ảnh. Thông tin ẩn được trải đều trên toàn bộ mặt ảnh. Ma trận ảnh gốc và ma trận dấu ẩn phải có cùng kích thước.

Giải pháp 2: *Giấu tin trong miền tần số*

+ Chèn thông tin vào miền tần số
+ Tách thông tin trong miền tần số

7. Ứng dụng của giấu tin trong ảnh số

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

- **Bảo vệ bản quyền:** Là ứng dụng cơ bản nhất của kỹ thuật thuỷ vân số (watermarking) - một dạng của phương pháp giấu tin. Một thông tin nào đó mang ý nghĩa sở hữu quyền tác giả (người ta gọi nó là thuỷ vân - watermark) sẽ được nhúng vào trong các sản phẩm, thuỷ vân đó chỉ có một mình người chủ sở hữu hợp pháp các sản phẩm đó có và được dùng làm minh chứng cho bản quyền sản phẩm.
- **Điểm chỉ số:** Mục tiêu của điểm chỉ số là để chuyển thông tin về người nhận (chứ không phải chủ sở hữu) sản phẩm phương tiện số nhằm xác định đây là bản sao duy nhất của sản phẩm. Về mặt ý nghĩa điểm chỉ số tương tự như số xê ri của phần mềm
- **Gán nhãn:** Tiêu đề, chú giải và nhãn thời gian cũng như các minh hoạ khác có thể được nhúng vào ảnh, ví dụ đính tên người lên ảnh của họ hoặc đính tên vùng địa phương lên bảng đồ. Khi đó nếu sao chép ảnh thì cũng sẽ sao chép cả các dữ liệu nhúng trong nó. Và chỉ có chủ sở hữu của tác phẩm, người có được khoá mật (Stego-Key) mới có thể tách ra và xem các chú giải này. Trong một cơ sở dữ liệu ảnh, người ta có thể nhúng các từ khoá để các động cơ tìm kiếm có thể tìm nhanh một bức ảnh. Nếu ảnh là một khung ảnh cho cả một đoạn phim, người ta có thể gán cả thời điểm diễn ra sự kiện (timing) để đồng bộ hình ảnh với âm thanh. Người ta cũng có thể gán số lần ảnh được xem để tính tiền thanh toán theo số lần xem.
- **Giấu thông tin mật:** Trong nhiều trường hợp sử dụng mật mã có thể gây ra sự chú ý ngoài mong muốn. Ngoài ra việc sử dụng công nghệ mã hoá có thể bị hạn chế. Một số kỹ thuật giấu tin trong ảnh mầu hoặc cấm sử dụng. Ngược lại việc giấu tin trong môi trường nào đó rồi gửi đi trên mạng ít gây sự chú ý. Có thể dùng nó để gửi đi một bí mật thương mại, một bản vẽ hoặc các thông tin nhạy cảm khác.

8. Kết luận

Bài báo này mong muốn đưa đến cho độc giả những kiến thức cơ bản về giấu tin nói chung, cũng như giấu tin trong ảnh số nói riêng. Do khuôn khổ bài báo, tác giả chưa thể trình bày vấn đề một cách chi tiết, cũng như chưa thể trình bày một số thuật toán và phần cài đặt thử nghiệm liên quan. Mọi ý kiến đóng góp xin liên hệ với tác giả theo địa chỉ: phucvima@gmail.com.

TÀI LIỆU THAM KHẢO

[1] Đặng Văn Đức*, Kỹ thuật đồ hoạ máy tính - Viện Công Nghệ Thông Tin – Trung tâm khoa học và công nghệ quốc gia, 2003..*

[2] TS.Đặng Văn Đức,*Tài liệu bài giảng (file *.pdf): Kỹ thuật đồ hoạ máy tính – 2003*

[3] Lương Mạnh Bá, Nguyễn Thanh Thuỷ, *Nhập môn xử lý ảnh số- Nhà xuất bản Khoa học kỹ thuật, 1999*

[4] *Các Website có liên quan.(* www.ece.umd.edu, www.**data-hiding**.com,..)

Người phản biện: TS. Lê Quốc Định