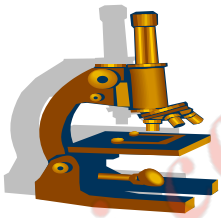
TRƯỜNG ĐẠI HỌC QUỐC GIA HÀ NỘI
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ
Khoa Công Nghệ
-------oOo-------



BÀI TẬP LỚN
ĐỒ HỌA MÁY TÍNH

Trình bày : Một số thuật toán giấu tin trong ảnh

Nhóm học viên thực hiện :
Bùi Gia Hiếu
Trần Thanh Lưu
Lớp : K10 – T2

Hà Nội – 10/2004

CHƯƠNG 1: TỔNG QUAN VỀ LĨNH VỰC GIẤU THÔNG TIN

Giới thiệu chung về giấu thông tin.

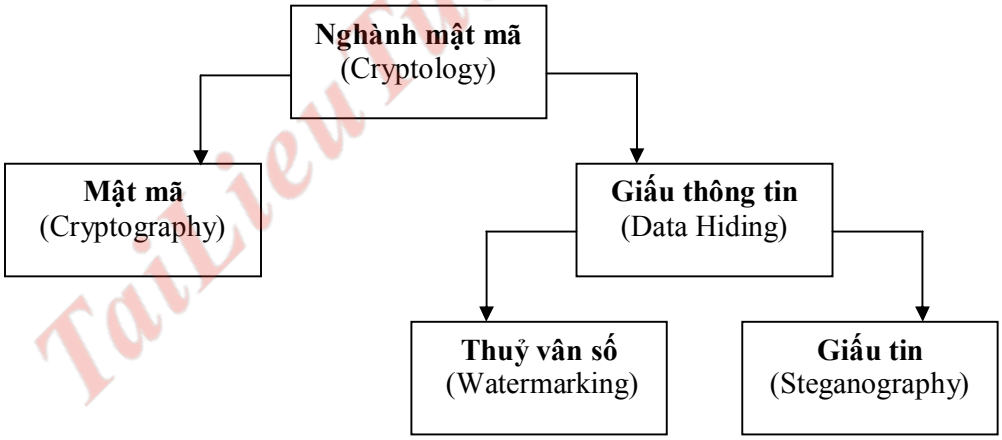
1. Định nghĩa :

"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)

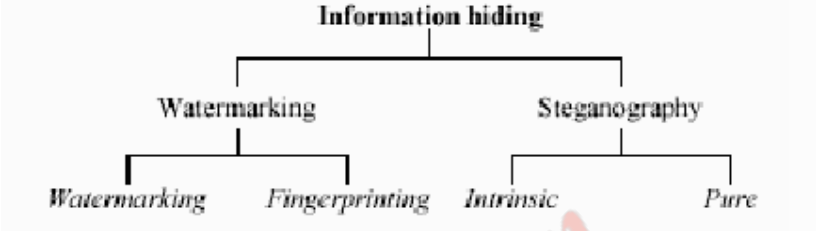
Là nghiên cứu phương pháp gửi thông điệp dưới hình thức khác nhau sao cho chỉ người nhận mong đợi mới bỏ đi che giấu để đọc thông điệp.Thông điệp muốn gửi đi gọi là ***bản rõ***. Thông điệp bị che giấu gọi là ***bản mã hóa***. Sau khi người nhận loại bỏ che giấu để đọc thông tin thì thông điệp không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

Steganography giấu thông điệp trong bản rõ thay cho mã hóa thông điệp. Nó được nhúng trong dữ liệu cần bảo vệ.

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.

3. Thủy vân số và giấu 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

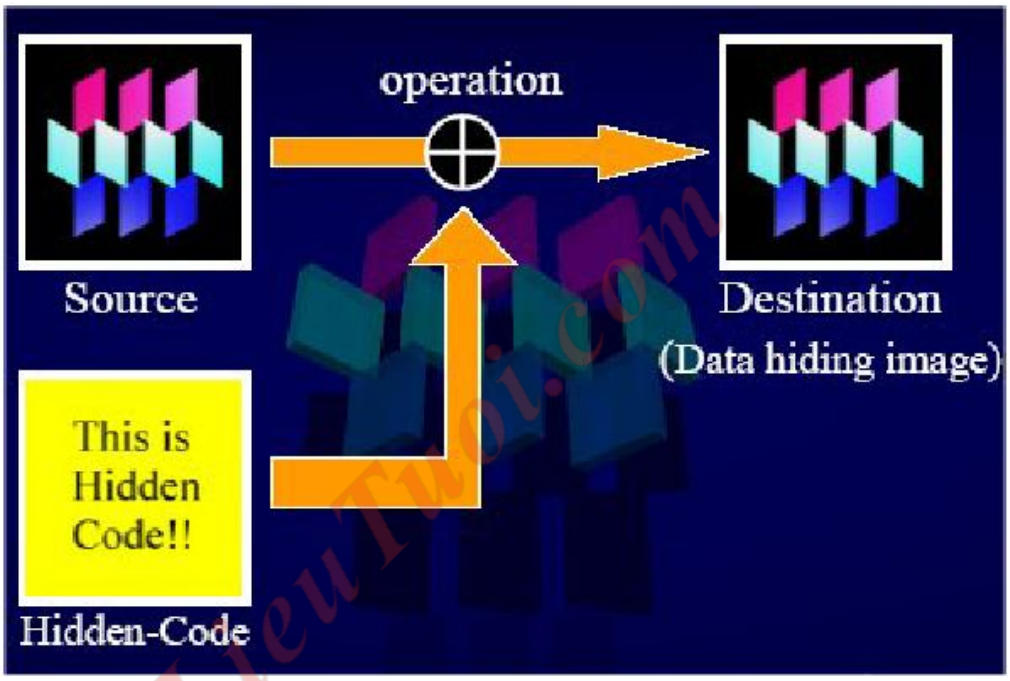
+ Khác với giấu tin ở chỗ, giấu tin sau đó cần tách lại tin còn thuỷ ấn tìm cách biến tin giấu thành một thuộc tính của vật mang

+ 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 trên ảnh mang.

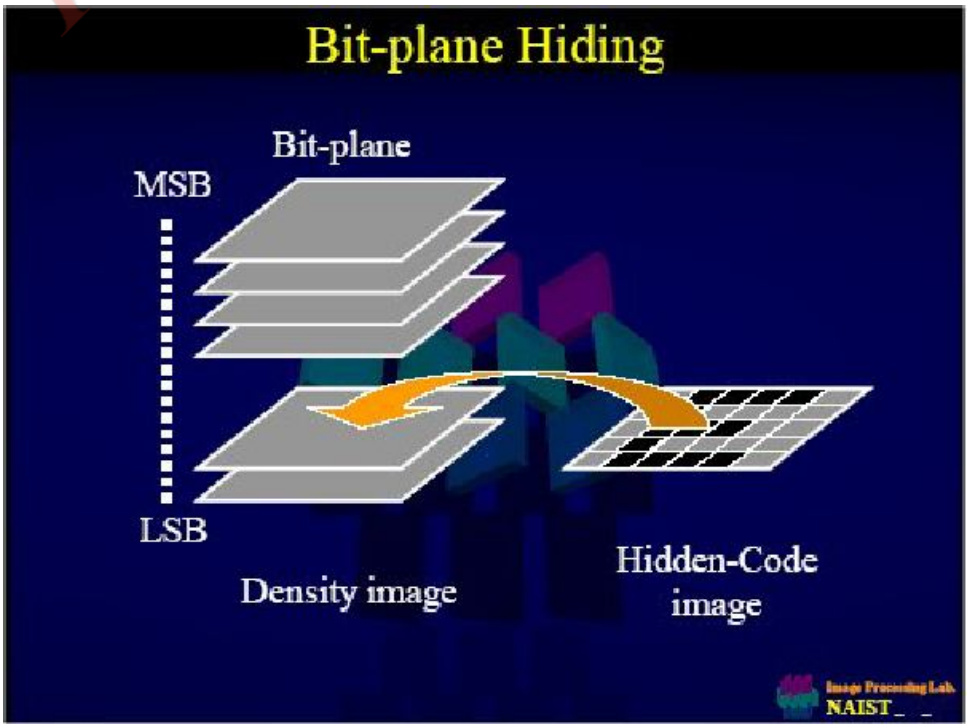
4. Giấu tin trong ảnh số:

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.

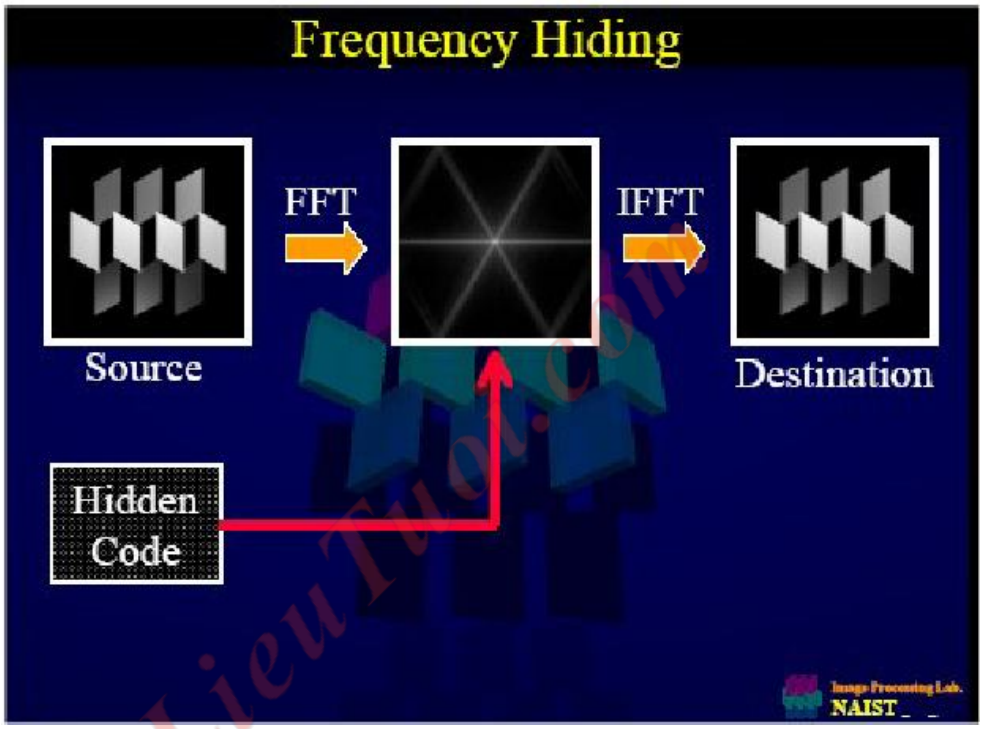


Giấu thông tin vào trong ảnh

Giải pháp giấu tin trong ảnh



Giấu tim trong miền quan sát



Giấu tin trong miền tần số

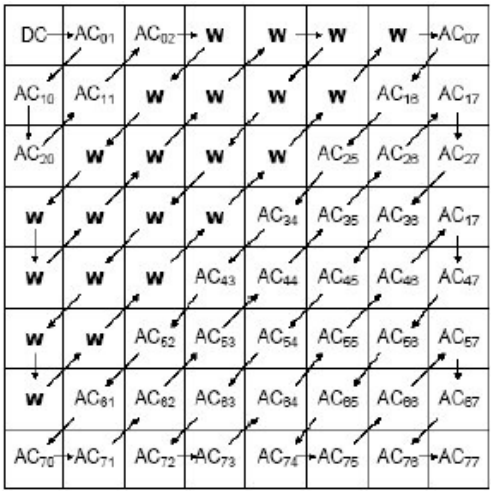
5. Kỹ thuật chung giấu thông tin trong ảnh :

Chọn vị trí dấu 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
  - Chú ý: trong nén ảnh mất mát thông tin thường loại bỏ miền ảnh có tần số cao

Chọn miền giấu thông tin :

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



Chọn kiểu chèn thông tin giấu :

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

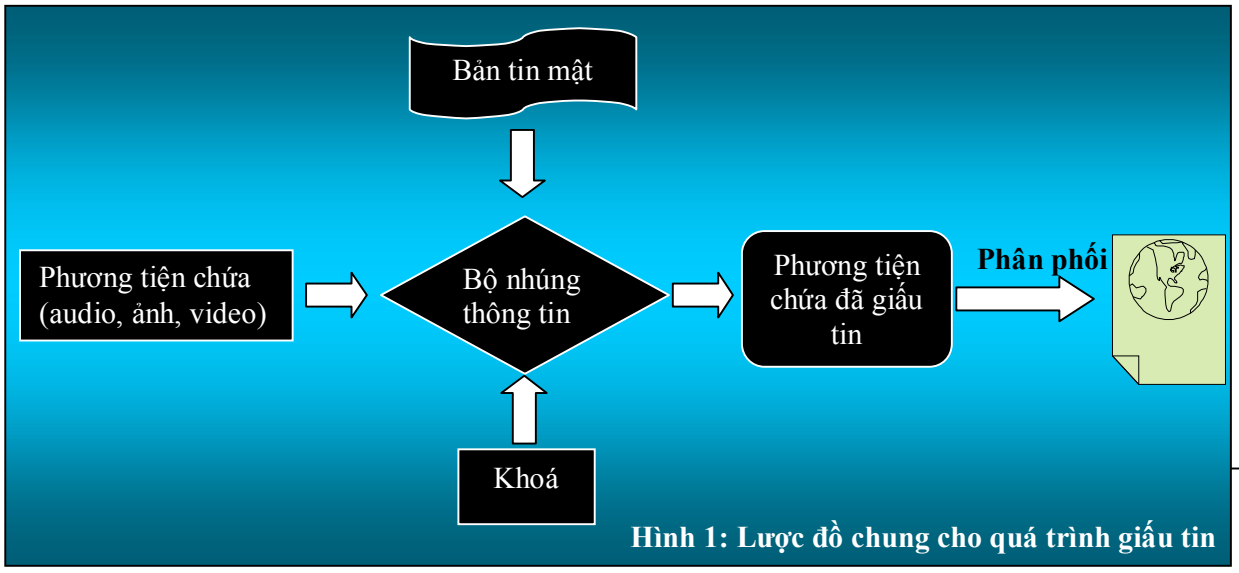
- Các bước tách thông tin ẩn là các bước ngược lại của tiến trình chèn thông tin ẩn

6. 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 :

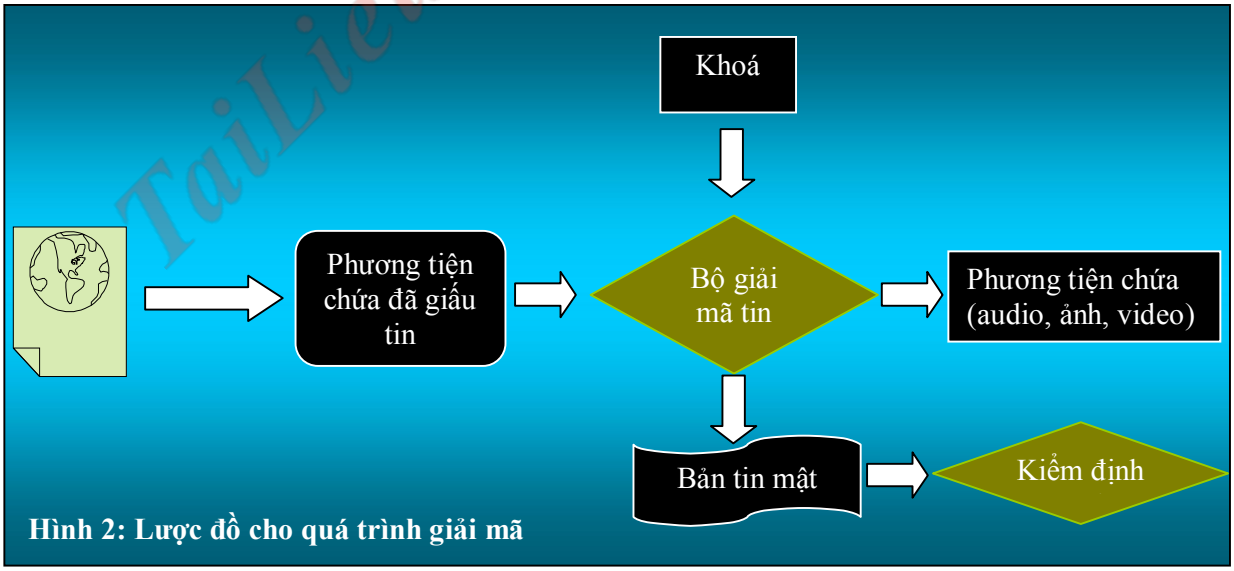
- **Bản tin mật** (Secret Message): có thể là văn bản hoặc tệp ảnh hay bất kỳ một tệp nhị phân nào, vì quá trình xử lý chúng ta đều chuyển chúng thành chuỗi các bit.
- **Ảnh phủ** (hay ảnh gốc) (Cover Data): là ảnh được dùng để làm môi trường nhúng tin mật.
- **Khoá bí mật K** (Key): khoá viết mật tham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



Hình 1: Lược đồ chung cho quá trình giấu tin

Hình vẽ trên 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.



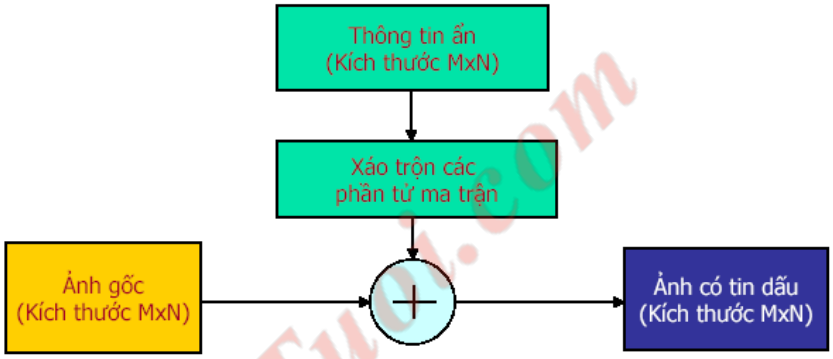
Hình 2: Lược đồ cho quá trình giải mã

Hình vẽ trên 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.

7. 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.



+ Chèn thông tin vào miền quan sát :
- Tạo dãy số nguyên S liên tục có thứ tự ngẫu nhiên theo luật sinh xác định trước.
- Cho trước a, bvà m, x_n là phần tử sinh, x_{n+1} là phần tử ngẫu nhiên tạo ra, theo Lehmer(1949) :

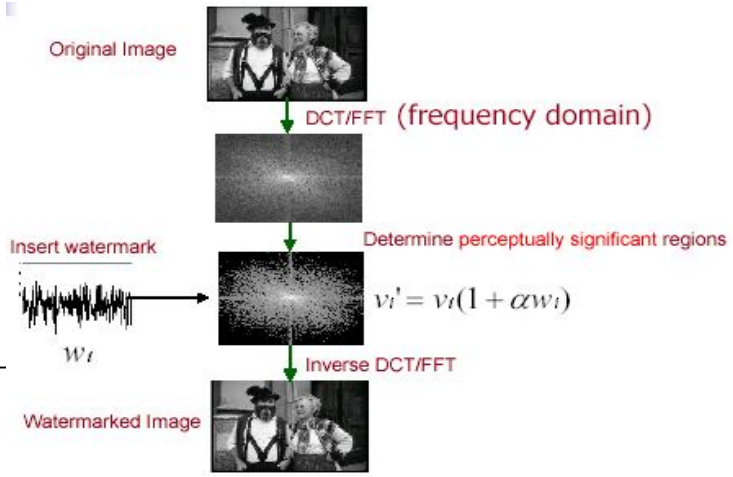
$$x_{n+1} = (a*x_n + b) \bmod m$$

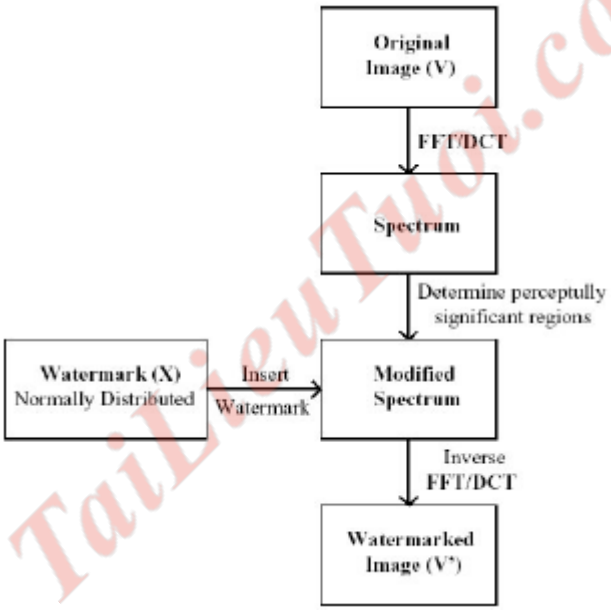
- Miền giá trị của dãy là {1..MxN}
- Chuyển đổi ma trận giấu tin 2 chiều thành dãy số W.
- Xáo trộn dãy W như sau : W[i] = W[S_i]
- Chuyển đổi ngược dãy W về ma trận MxN
- Cộng ma trận thông tin ẩn đã xáo trộn với ảnh gốc để có ảnh chứa thông tin ẩn.

+ Tách tin giấu trong miền quan sát :
- Gọi ảnh gốc là I và ảnh có thông tin ảnh là I'.Thực hiện phép trừ các phần tử tương ứng của I' cho I để có thông tin ẩn (ma trận W).
- Chuyển ma trận W thành dãy số W*
- Tạo dãy số nguyên S liên tục có thứ tự ngẫu nhiên theo luật sinh xác định ở bước chèn tin ẩn
- Sắp xếp lại dãy W*: W*[S_i] =W[i]
- Chuyển đổi dãy W* thành ma trận hai chiều để có thông tin ẩn.

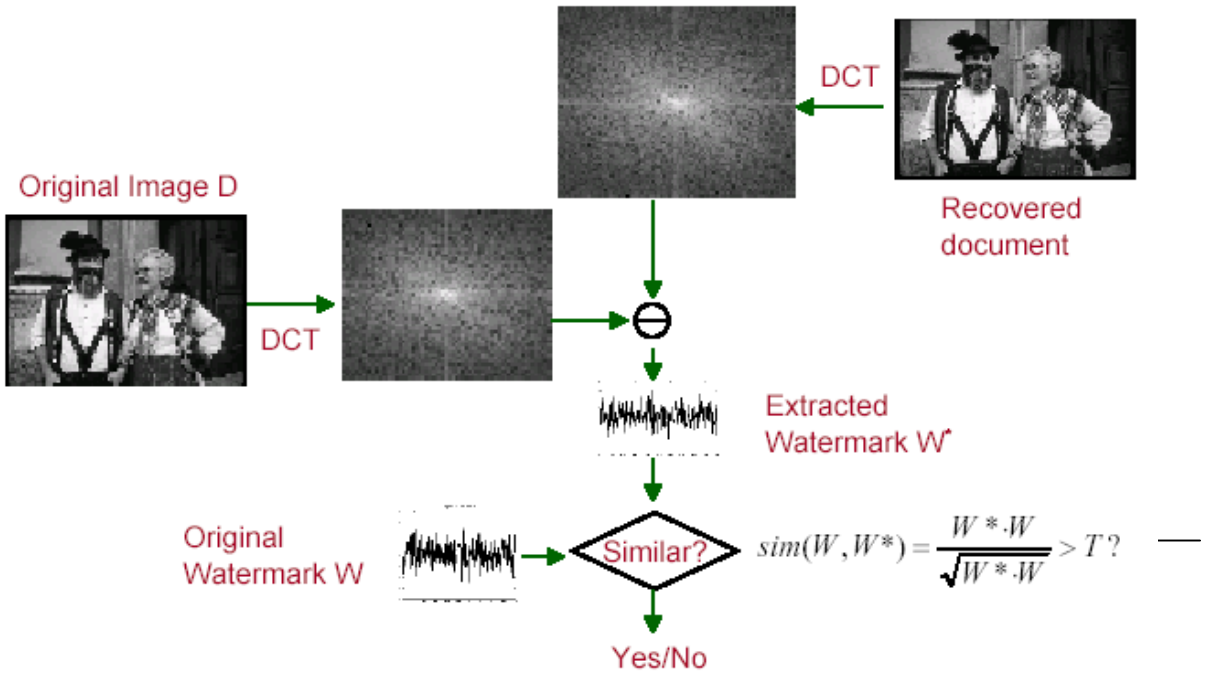
Giải pháp 2 :*Giấu tin trong miền tần số*

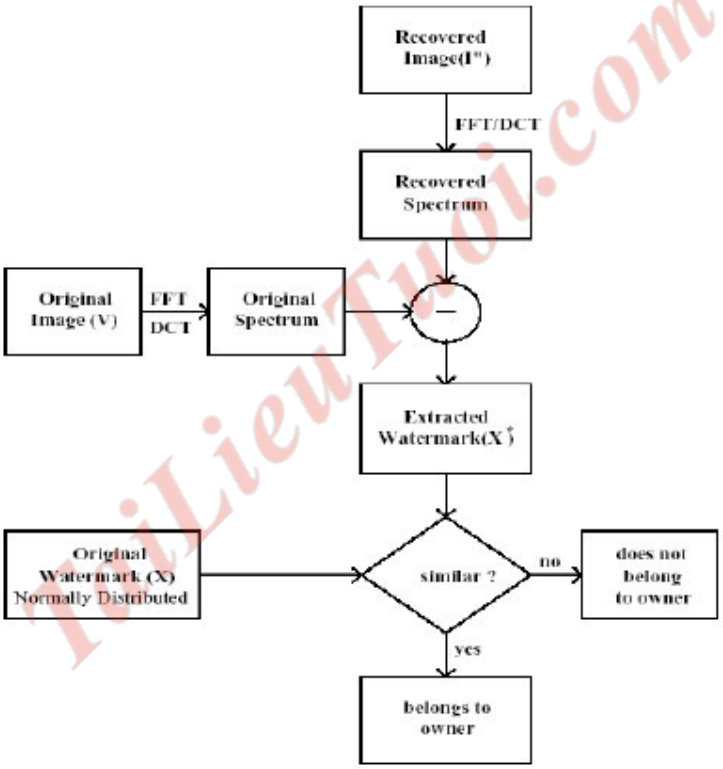
+ Chèn thông tin vào miền tần số :





+ Tách thông tin trong miền tần số:





8. Các tính chất giấu tin trong ảnh số:

a. Tính vô hình (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.

b. 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 ấn 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.

c. Dung lượng giấu :