

Báo cáo bài tập giữa kì môn Nhập môn An toàn thông tin

Danh sách thành viên nhóm

STT	Họ và tên	MSSV	Mã lớp
1	Đặng Duy Anh	20183471	124190
2	Phạm Duy Anh	20183481	124190
3	Từ Hoàng Giang	20183518	124190

Tên ý tưởng: Ứng dụng Visual cryptography và QR Code cho bài toán quản lý thuốc

1. Nội dung

Trong lĩnh vực chăm sóc sức khỏe, việc sai sót về thuốc có thể gây ra những hậu quả nghiêm trọng cho bệnh nhân. Vì vậy, các bệnh viện cần có một hệ thống quản lý thuốc an toàn để ngăn ngừa những sai sót đó. Các bệnh nhân cần có một hệ thống để họ có thể tự nhận thức và kiểm tra loại thuốc mà mình đang sử dụng.

Giải pháp do nhóm thực hiện có thể giảm xác suất mà một người bệnh có thể lấy sai thuốc, hoặc thiếu thuốc, và giúp đỡ những người không có khả năng đọc tên thuốc bằng tiếng anh. Đặc biệt, nó rất hữu dụng khi người bệnh không mua cả hộp thuốc mà họ chỉ mua một vài viên/ vi/ gói thuốc, do đó, họ không có bao bì gốc của thuốc và việc xác nhận thông tin cho họ trở nên khó khăn.

2. Triển khai

Khi một bệnh nhân đến khám bệnh và bác sĩ kê cho bệnh nhân một đơn thuốc chứa tổng cộng n loại thuốc. Thông tin cá nhân và một bức ảnh của bệnh nhân sẽ được chụp lại. Sau đó, bức ảnh của bệnh nhân sẽ được mã hóa thành n bản QR – code khác nhau. n bản mã QR này sẽ được dán hoặc in lên n túi thuốc của bệnh nhân. Khi bệnh nhân đến nhận thuốc, họ sẽ quét mã QR trên từng túi thuốc, nếu sau khi quét xong n túi thuốc, họ nhận được một hình ảnh chụp chính mình có nghĩa là họ đã lấy đúng và đủ số thuốc của mình, nếu có ít nhất một loại thuốc bị sai hoặc thiếu, họ sẽ không nhận được hình ảnh nào của mình cả.

3. Cách cài đặt

Đầu vào là 1 ảnh (màu, xám hoặc nhị phân), 1 dãy số định danh của khách hàng và tên các loại thuốc. Đầu ra là các bản mã QR mà khi ghép với nhau sẽ ra hình ảnh của khách hàng nếu đúng hoặc không gì cả nếu sai.

Hệ thống được triển khai dựa vào Visual cryptography và QR – code bao gồm hai pha:

Pha 1: Sử dụng phương pháp (n, n) – threshold visual cryptography để tạo ra n bản mờ từ bức ảnh gốc của bệnh nhân.

Bức ảnh gốc kích thước $p \times q$ ban đầu của bệnh nhân sẽ được giữ bí mật. Từ bức ảnh này, ta tạo ra n bản mờ mà khi xếp chồng chúng lên nhau, ta sẽ thu được hình ảnh gốc ban đầu. Nếu không có đủ n bản mờ, không có cách nào ta thu được bất cứ thông tin gì từ bức ảnh.

Pha 2: Mã hóa các bản mờ bằng QR – code.


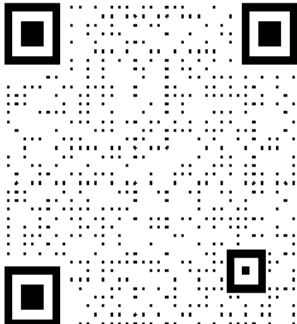
Khi 1 bản mờ ở bước trên được tạo ra, ta sẽ tạo ra một bản QR – code tương ứng với nó. Đầu tiên, sử dụng một thông tin của bệnh nhân như họ tên, căn cước công dân hoặc là thông tin loại thuốc của họ để mã hóa thành QR – code. Sau đó, mã QR này sẽ được điều chỉnh để có cùng kích thước với bản mờ tương ứng của nó. Tiếp đó, các pixel trên QR – code sẽ được rút gọn lại, ngoại trừ các hoa văn định vị và căn chỉnh. Cuối cùng, ta hợp nhất bản mờ và QR – code bằng cách xếp chồng QR – code lên bản mờ.

Như vậy, sau khi bệnh nhân được bác sĩ kê cho n đơn thuốc, n bản mã QR sẽ được tạo ra và lần lượt in trên n túi thuốc đưa cho bệnh nhân. Bệnh nhân có thể sử dụng điện thoại mà không cần kết nối internet để quét mã kiểm tra xem họ đã nhận đủ và đúng n đơn thuốc được bác sĩ kê hay chưa.

4. Thuật toán sử dụng

4.1 Thuật toán sinh QR code

Sinh ảnh QR-code từ một chuỗi ký tự nhờ sử dụng thư viện qrcode 7.1 của python. Sau đó, giữ nguyên các giá trị pixel mà tại vị trí đó là các ô vuông căn vị trí của bản mã qr. Còn lại các bit giá trị của qr code sẽ thu về chỉ còn 1 pixel để ảnh qr sẽ có nhiều khoảng trắng hơn để chèn ảnh sau này. Phóng to bản mã qr để vừa với bức ảnh đầu vào.

Ảnh QR được thư viện sinh ra	Ảnh QR sau khi được xử lý
	

4.2 Thuật toán mã hóa ảnh

Nhóm sử dụng hai thuật toán mã hóa hình ảnh.

- Mã hóa bằng cách Xor pixel:

- + Sinh ảnh bí mật(n ảnh): Tạo ra $(n - 1)$ bức ảnh bí mật bằng cách sinh ngẫu nhiên $(n - 1)$ bức ảnh cùng kích thước, bức ảnh bí mật thứ n được tạo ra bằng cách xor $(n - 1)$ bức ảnh ngẫu nhiên với ảnh bí mật cần mã hóa ban đầu.

- + Giải mã ảnh: Sử dụng n ảnh bí mật xor đôi một lần lượt sẽ sinh ra được bức ảnh mã hóa ban đầu.

Đây là thuật toán visual cryptography(n, n), vì phải có đủ n bức ảnh bí mật thì mới có thể giải mã ra bức ảnh ban đầu. Nếu như chỉ 1 bức ảnh bị thiếu, thì sẽ phải thử $2^{m \times n}$ bit trong đó $(m \times n)$ là kích thước ảnh nên sẽ khó giải mã.

- Mã hóa bằng cách mở rộng pixel (chỉ sử dụng được cho ảnh nhị phân và ảnh xám):

- + Trong thuật toán này, mỗi pixel được chia thành các pixel con và hình ảnh gốc được chia thành n bản mã sau đó được chồng lên nhau để có được hình ảnh được giải mã cuối cùng. Mỗi bộ sưu tập của subpixel sẽ có số lượng subpixel trắng và đen bằng nhau. Màu sắc của các pixel phụ được chỉ định theo cách sao cho khi hai lượt chia sẽ chồng chéo lên nhau, pixel có màu đen trước đây sẽ vẫn có tất cả các pixel phụ của nó là màu đen và pixel màu trắng sẽ có một nửa số pixel phụ của nó là màu đen.


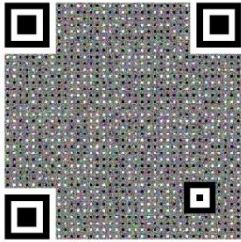
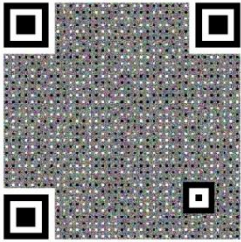
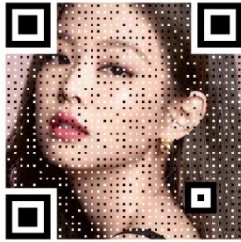

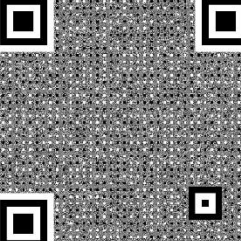
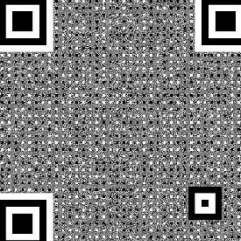
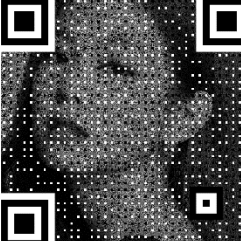
Cụ thể, ta lấy một pixel từ hình ảnh bí mật ban đầu. Sau đó chia nhỏ pixel đó thành n pixel phụ, tô màu trong các pixel phụ đó để khi phủ lên hình ảnh thì: nếu pixel ban đầu là màu đen, các pixel con được phủ sẽ có n pixel được tô màu, nếu pixel ban đầu là màu trắng, các pixel con được phủ sẽ có một nửa pixel được tô màu. Làm điều này với một mức độ ngẫu nhiên để các bản mã được an toàn, sau đó kết hợp các subpixel của mỗi bản mã và phân phối

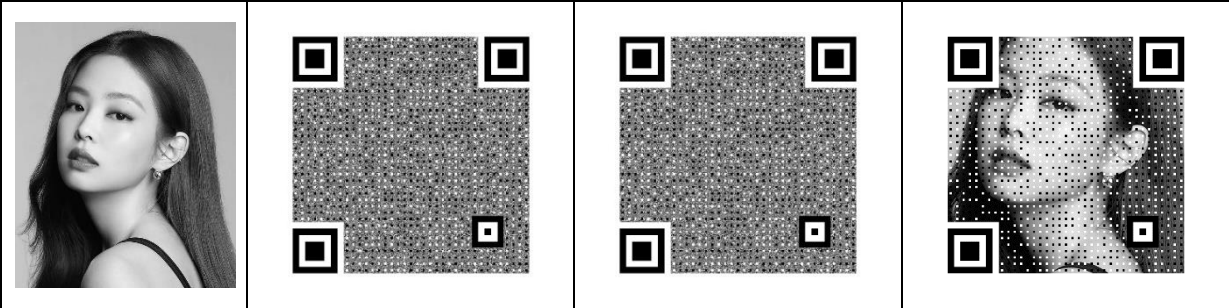
+ Giải mã ảnh:

Cách 1: Chồng các ảnh lên nhau.

Cách 2: Trích xuất (chỉ các pixel có tất cả các pixel phụ của nó là màu đen được gọi là màu đen, nếu không nó là màu trắng).

5. Kết quả

Ảnh đầu vào	Bản mã 1	Bản mã 2	Bản giải mã
5.1 Ảnh màu			
			
5.2 Ảnh xám			
<i>Giải mã bằng cách chồng ảnh</i>			
			
<i>Giải mã bằng cách trích xuất</i>			



5.2 Ảnh nhị phân

Giải mã bằng cách chồng ảnh

Giải mã bằng cách chích xuất

