Sơ bộ

Lĩnh vực mã hóa hình ảnh có thể được coi là cả một khoa học và nghệ thuật. Thành phần khoa học của lĩnh vực mật mã này bao gồm việc sử dụng các thành phần khác nhau để thực thi thuật toán mã hóa an toàn theo các cách khác nhau, chẳng hạn như trình tạo số ngẫu nhiên, sơ đồ hoán vị, sơ đồ thay thế tất cả được xây dựng trong chương này. Cùng với các công cụ này, các cơ chế khác như sử dụng các hệ thống hỗn loạn (ứng dụng lý thuyết hỗn loạn), chữ ký số (ứng dụng mã hóa bất đối xứng) hoặc thậm chí các ứng dụng toán học (như việc sử dụng các chữ số của số vô tỷ số pi pi hay chuỗi được tạo bởi một chuỗi Fibonacci) có thể được áp dụng cho một hệ thống mật mã. Mỗi cơ chế có những ưu điểm và khuyết điểm riêng; khoa học là để hiểu từng người trong số họ và áp dụng nó cho phù hợp với tình huống và ứng dụng trong tay. Tuy nhiên, nghệ thuật nằm ở cách áp dụng các công cụ và cơ chế khác nhau này. Ví dụ, kiến ​​trúc thay thế hoán vị (vẫn chưa được xây dựng) là một cơ chế đã được chứng minh, thực thi cả việc xáo trộn dữ liệu ở dạng pixel và chuyển đổi dữ liệu đó thành dạng không thể hiểu được

Như một ví dụ tầm thường, hãy xem xét một hình ảnh hoàn toàn trắng. Như mọi khi, mục tiêu cuối cùng của mã hóa hình ảnh là chuyển đổi một hình ảnh với dữ liệu trực quan có ý nghĩa thành một hình thức mà không có dữ liệu, chỉ dẫn hoặc suy luận nào có thể được ngoại suy từ đó.

Tóm lại, hành động mã hóa thông qua hoán vị được dự định để tranh giành bất kỳ ý nghĩa có thể có thể được suy ra từ một hình ảnh. Và hành động thay thế nhằm loại bỏ bất kỳ nguồn ý nghĩa logic thực sự nào trong hình ảnh bằng cách chuyển đổi dữ liệu hoặc pixel, từ dạng này sang dạng khác. Tuy nhiên, chúng ta hãy xem xét một cách sử dụng có thể của các kỹ thuật này riêng lẻ

Nếu chúng ta thực hiện hoán vị nghiêm ngặt mà không thay thế, hình ảnh sẽ vẫn như vậy, vì việc xáo trộn một tập hợp các pixel trắng sẽ dẫn đến cùng một tập hợp, vì bất kỳ hai pixel trắng nào cũng không thể phân biệt được với nhau. Tuy nhiên, nếu chúng tôi thực hiện thay thế nghiêm ngặt (giả sử thay thế là một hoạt động trong đó ánh xạ chuyển đổi một thành một giữa hai giá trị pixel độc lập được sử dụng để chuyển đổi một pixel thành một pixel khác), toàn bộ hình ảnh trắng sẽ được chuyển đổi thành một hình ảnh khác của một màu ngẫu nhiên (giả sử nó là màu vàng, vì lợi ích của cuộc thảo luận này). Điều này là do mỗi pixel trắng riêng lẻ sẽ được chuyển đổi thành pixel màu vàng đích. Từ quan điểm của nhà mật mã, trong khi điều này sẽ không tiết lộ màu sắc thật, nguyên bản của hình ảnh nhạy cảm (hoàn toàn đen), nó sẽ đưa ra một dấu hiệu cho thấy tất cả các pixel của ảnh gốc giống hệt nhau. Điều này đánh bại hiệu quả mục tiêu đã nói ở trên về mã hóa hình ảnh.

Để đạt được hiệu quả này, có thể sử dụng kết hợp các kỹ thuật ngoài hoán vị và thay thế (chẳng hạn như sử dụng chuỗi số ngẫu nhiên phù hợp) để chống lại các hạn chế trên. Một số phương pháp ví dụ được thảo luận trong các phần tiếp theo của chương này.

Tuy nhiên, trước tiên chúng ta phải hiểu ý nghĩa của hình ảnh thực sự là gì, thuộc tính của chúng là gì và làm thế nào điều này có thể có tác động khác nhau đối với bảo mật dữ liệu như một toàn bộ không chỉ từ góc độ nhị phân, mà còn từ góc độ hình ảnh.

Nguyên tắc cơ bản về hình ảnh

Một thuật toán mã hóa hình ảnh xử lý các pixel có ý nghĩa hình ảnh cũng như ý nghĩa nhị phân. Hình ảnh có các thuộc tính nội tại chung nhất định như mức độ dư thừa dữ liệu tương đối cao và phần lớn dữ liệu lớn hơn so với lượng dữ liệu logic được biểu thị. Khía cạnh đầu tiên có thể được giải thích bằng cách quan sát rằng trong hình ảnh trung bình của một đối tượng cụ thể (chẳng hạn như phong cảnh, người hoặc bất cứ thứ gì khác), có xác suất cao hơn rằng bất kỳ hai pixel nào liền kề nhau sẽ có điểm tương tự màu sắc, khi so sánh với một hình ảnh với các pixel hoàn toàn ngẫu nhiên. Khía cạnh thứ hai có thể được giải thích bằng cách quan sát rằng nếu một lượng thông tin cần được truyền từ thực thể này sang thực thể khác (chẳng hạn như mật khẩu hoặc tên của một người trong đám đông), thì dữ liệu đó được thể hiện tốt hơn nhiều ở dạng nhị phân so với trực quan dưới dạng tương tự, một hình ảnh của mật khẩu được viết trên bề mặt hoặc hình ảnh của một đám đông người trong một đối tượng) nếu mối quan tâm chính là để tiết kiệm băng thông truyền. Vì vậy, có thể nói rằng mật độ không gian logicto trong hình ảnh thấp hơn đáng kể so với các luồng dữ liệu nhị phân điển hình

Tất nhiên, đây chỉ là những khái quát và chỉ mô tả hình ảnh trung bình. Mặc dù chúng không nên được hiểu là các quy tắc khó và nhanh đối với tất cả các thuật toán mã hóa hình ảnh, chúng có thể được coi là hướng dẫn để hiểu ý nghĩa khác nhau của hình ảnh và cấu trúc pixel (Hình 33.1).

Cấu trúc hình ảnh

Nói chung, chúng tôi xem xét ba loại hình ảnh khác nhau, cụ thể là hình ảnh thang độ xám, hình ảnh RGB và hình ảnh RGBA.

Trực quan, sự khác biệt giữa các loại hình ảnh là đơn giản. Hình ảnh thang độ xám biểu thị các pixel dưới dạng độ đen và độ trắng và các pixel này được sắp xếp theo định dạng lưới để thể hiện trực quan dữ liệu. Hình ảnh RGB có ba lớp hoặc các kênh pixel được sắp xếp theo định dạng lưới được đặt chồng lên nhau để tạo hiệu ứng kết hợp màu sắc. Mỗi kênh sở hữu các mức độ khác nhau của màu đỏ, xanh lá cây và xanh lam, tương ứng (do đó có tên RGB). Hệ thống này hoạt động vì có một thực tế nổi tiếng là bất kỳ màu nào cũng có thể được tạo ra bằng cách trộn một lượng thích hợp của màu đỏ, xanh lá cây và xanh dương. Hình ảnh RGBA thêm một mức độ chi tiết bổ sung cho hình ảnh RGB tiêu chuẩn bằng cách bao gồm một kênh Alpha, kết hợp hình ảnh với nền để tạo ra hình ảnh trực quan của độ trong suốt một phần hoặc toàn bộ.

Trong hình 33.2, bpp là viết tắt của bit trên mỗi pixel.

Từ góc nhìn trực quan, tất cả các hình ảnh có bản chất hai chiều. Điều này là do, đối với mắt người, bất kỳ hình ảnh nào cũng có độ dài nhất định và chiều rộng nhất định. Nhận thức này độc lập với loại hình ảnh được quan sát, tức là, thang độ xám, RGB, RGBA hoặc bất kỳ đặc điểm kỹ thuật định dạng nào khác.

Đơn vị cơ bản của hình ảnh hai chiều nhận thức này được gọi là pixel.

Trong ảnh thang độ xám, một pixel được yêu cầu chỉ hiển thị mức độ trắng hoặc đen. Trong thực tế, pixel này có thể giả sử một giá trị nằm trong khoảng từ 0 đến 255 hoặc 0b00000000 đến 0b11111111 (trong biểu diễn nhị phân). Do đó, biểu diễn pixel này có kích thước 8 bit hoặc 8 bpp (bit trên mỗi pixel). Điều này đúng với bất kỳ đại diện một kênh nào của hình ảnh

Trong hình ảnh RGB, một pixel được yêu cầu để hiển thị ba mức độ đỏ, xanh lục và xanh lục riêng biệt (nhờ ba kênh màu riêng lẻ). Mỗi pixel phụ trong mỗi kênh lại được biểu thị bằng 8 bit. Do đó, pixel tổng thể trong hình ảnh RGB yêu cầu 3 × 8 = 24 bit cho biểu diễn của nó.

Một hình ảnh RGBA bao gồm 4 kênh độc lập. Do đó, bằng cách sử dụng logic tương tự, mỗi biểu diễn pixel yêu cầu 4 × 8 = 32 bit cho mỗi pixel.

Hình 33.1 Trực quan hóa các hình ảnh dựa trên màu xám, màu và alpha. (a) Một hình ảnh thang độ xám. Ở đây, nền của hình ảnh hoàn toàn là màu trắng và dấu tick được lấp đầy bằng một màu xám. (b) Một hình ảnh RGB. Ở đây, màu xanh lá cây có thể được quan sát làm đầy dấu tích trong hình ảnh. (c) Một hình ảnh RGBA. Nền rô có thể được quan sát đằng sau hình ảnh RGB, đây là hình ảnh tiêu chuẩn cho các hiệu ứng trong suốt.

Các dạng biểu diễn pixel khác nhau này cần được xem xét khi phát triển thuật toán mã hóa hình ảnh, vì các cấu trúc dữ liệu này cần được xử lý phù hợp và không được xem xét trong các thao tác bit đơn giản trong các thuật toán mã hóa tiêu chuẩn khác như AES, DES và các thuật toán khác.