(12) BẢN MÔ TẢ SÁNG CHẾ THUỘC BẰNG ĐỘC QUYỀN SÁNG CHẾ

(19) **Cộng hòa xã hội chủ nghĩa Việt Nam (VN)**
CỤC SỞ HỮU TRÍ TUỆ

(11) **1-0050517**

(51)[2020.01] **G06K 19/16**; G06K 7/14; G06K 19/06 (13) **B**

(21) 1-2022-01435
(22) 28/08/2020
(86) PCT/EP2020/074092 28/08/2020
(87) WO2021/038050 04/03/2021
(30) 19194679.7 30/08/2019 EP
(45) 25/08/2025 449
(43) 25/07/2022 412A
(73) AUTHENTIC VISION GMBH (AT)
Ludwig-Bieringer-Platz 1, 5071 Wals, Austria
(72) BERGMÜLLER, Thomas (AT); WEISS, Thomas (AT).
(74) Công ty Luật TNHH Phạm và Liên danh (PHAM & ASSOCIATES)

(54) DẤU CỦA ĐỐI TƯỢNG, PHƯƠNG PHÁP TẠO RA DẤU NÀY VÀ PHƯƠNG PHÁP XÁC THỰC

(21) 1-2022-01435

(57) Sáng chế liên quan đến dấu của đối tượng (9) có phần tử bảo mật thứ nhất (3) và ít nhất phần tử bảo mật thứ hai (4), trong đó mỗi phần tử bảo mật (3, 4) được liên kết với một tập hợp các đoạn dữ liệu (6, 7) và mỗi phần tử bảo mật (3, 4) hiển thị tùy thuộc vào điều kiện chụp ảnh, cụ thể là góc nhìn (10) và/hoặc hướng chiếu sáng, đoạn mã là một biểu diễn quang điện tử đọc được của một trong số các đoạn dữ liệu (5) của tập hợp được liên kết với phần tử bảo mật tương ứng (3, 4), trong đó các đoạn dữ liệu riêng biệt khác được biểu thị bằng các đoạn mã khác nhau (5) và tập hợp được liên kết với phần tử bảo mật thứ nhất (3) và tập hợp được liên kết với phần tử bảo mật thứ hai (4) khác nhau ở ít nhất một đoạn dữ liệu; phương pháp tạo ra dấu này và phương pháp xác thực.

Lĩnh vực kỹ thuật được đề cập

Sáng chế liên quan đến dấu của đối tượng có phần tử bảo mật thứ nhất và ít nhất là phần tử bảo mật thứ hai, trong đó mỗi phần tử bảo mật được liên kết với một tập hợp các đoạn dữ liệu và mỗi phần tử bảo mật hiển thị tùy thuộc vào điều kiện chụp ảnh, cụ thể là góc nhìn và/hoặc hướng chiếu sáng, đoạn mã là một biểu diễn quang điện tử đọc được của một trong số các đoạn dữ liệu của tập hợp được liên kết với phần tử bảo mật tương ứng. Hơn thế nữa, sáng chế liên quan đến một tập hợp các dấu của đối tượng.

Ngoài ra, sáng chế liên quan đến vật liệu cơ bản để tạo ra các dấu của đối tượng, có phần tử bảo mật thứ nhất và ít nhất phần tử bảo mật thứ hai, trong đó mỗi phần tử bảo mật được liên kết với một tập hợp các đoạn dữ liệu và mỗi phần tử bảo mật hiển thị tùy thuộc vào các điều kiện chụp ảnh, cụ thể là góc nhìn và/hoặc hướng chiếu sáng, một đoạn mã là một biểu diễn quang điện tử đọc được của một trong số các đoạn dữ liệu của tập hợp được liên kết với phần tử bảo mật tương ứng. Sáng chế cũng liên quan đến phương pháp xác thực dấu của đối tượng và phương pháp tạo ra dấu của đối tượng.

Tình trạng kỹ thuật của sáng chế

Một số loại dấu của đối tượng để xác thực hoặc xác minh và vật liệu cơ bản mà từ đó có thể tạo ra các dấu của đối tượng đó, cũng như các phương pháp xác thực hoặc xác minh các dấu của đối tượng đó đã được đề xuất trong các giải pháp kỹ thuật đã biết. Ví dụ, WO 2018/046746 A1 thể hiện một sản phẩm dạng tấm bao gồm các dấu và các dấu hiệu bảo mật. Các dấu là mã đọc được bằng máy. Các dấu hiệu bảo mật được thực hiện bởi các thiết bị bảo mật tách biệt với các dấu này. Chúng bao gồm hai thiết bị thay đổi quang (OVD) đặt cạnh nhau, ví dụ, các cách

tử nhiễu xạ khác nhau thể hiện, ví dụ, các thay đổi màu sắc khác nhau có thể nhận biết được từ máy ảnh hoặc mắt thường. Do đó, sự có mặt của dấu hiệu bảo mật có thể dễ dàng được nhận ra và xác minh với chức năng khử nhiễu lập trình được có một camera thông qua việc đảm bảo rằng hai OVD xuất hiện khác nhau. Tất cả các dấu hiệu bảo mật về cơ bản thể hiện rõ ràng cùng một ảnh có thể thay đổi quang học, tuy nhiên với các góc bắt đầu khác nhau. Sản phẩm dạng tấm có các dấu khác nhau, mỗi dấu có phần tử bảo mật được chọn ngẫu nhiên bên cạnh nó.

Hiệu ứng nhiễu xạ quang học, tức là ảnh mà một thiết bị thay đổi quang học "phát ra" hoặc có vẻ như thể hiện, phụ thuộc vào điều kiện chiếu sáng và góc nhìn. Trong cài đặt thông thường, nguồn sáng giống điểm được giả định và đặc tính của cách tử nhiễu xạ tạo ra dấu hiệu bảo mật được thiết kế cho tình huống chiếu sáng cụ thể này. Trong quá trình thiết kế, các cấu trúc vật lý được phát triển theo cách sao cho nó nhiễu xạ ánh sáng tới theo cách loại bỏ, tức là để hiển thị một ảnh nhất định ở một góc (phương vị) nhất định. Cụ thể hơn, nguồn sáng giống điểm ở một vị trí cụ thể được giả định và cách tử nhiễu xạ được thiết kế để thể hiện các ảnh cụ thể, ví dụ, màu sắc hoặc hình dạng cụ thể, ở các góc nhìn cụ thể khác nhau. Do đó, hành vi đã biết của phần tử bảo mật được giới hạn trong kịch bản chiếu sáng cụ thể này. Vì ảnh được hiển thị của một thiết bị bảo mật nhiễu xạ quang học vốn phụ thuộc vào điều kiện chiếu sáng cũng như góc nhìn, việc đọc nội dung thực tế của các dấu hiệu bảo mật trở thành một vấn đề vốn đã khó trong thực tế, khi các điều kiện môi trường xác định không thể được đảm bảo. Do đó, phần tử bảo mật phân tán quang học phản ứng - ít nhất là ở một mức độ nhất định - không thể đoán trước trong các điều kiện không được kiểm soát. Một cách tiếp cận thông thường để giải quyết vấn đề này là cung cấp một số loại thiết bị hoặc phương tiện khác (ví dụ, hướng dẫn người dùng, các chuyển động đặc biệt, đào tạo,...) để đảm bảo các điều kiện ít nhất là tương đồng với các điều kiện môi trường được sử dụng trong quá trình thiết kế. Nó là một đối tượng của sáng chế nhằm vượt qua giới hạn của một môi trường được kiểm soát để xác minh.

Sản phẩm dạng tấm nêu trong WO 2018/046746 A1 được tối ưu hóa một cách cụ thể để được xác minh bởi các thiết bị lập trình được có camera - với các dấu được sử dụng để xác định hành vi mong muốn của các dấu hiệu bảo mật xung quanh. Tuy nhiên, trong một cài đặt thực tế - không được kiểm soát -, hiếm khi xảy ra trường hợp tình huống chiếu sáng xác định có thể được lập bảng trong quá trình xác minh. Do đó, các thiết bị bảo mật sẽ phản ứng khác với dự đoán trong quá trình thiết kế. Do đó, người ta buộc phải trích xuất một tính năng bất biến của quốc gia - dân tộc từ một thiết bị bảo mật có thể thay đổi tùy ý tùy thuộc vào độ chiếu sáng. Không có gì đáng ngạc nhiên, đây là một vấn đề vốn đã khó giải quyết và luôn cần phải đánh đổi giữa tính nghiêm ngặt của việc xác minh / xác thực hoặc độ chính xác và mạnh để tính đến điều kiện ánh sáng không thể kiểm soát và ảnh hưởng của các yếu tố bên ngoài, không thể lường trước được. Điều này trở nên đặc biệt khó khăn, nếu có nhiều hơn một nguồn sáng giống điểm trong khi xác minh. Ngoài ra, ánh sáng khuếch tán có thể được hiểu là một số lượng không xác định của các nguồn sáng giống điểm (yếu). Trong điều kiện cài đặt các nguồn sáng như vậy, chắc chắn các chùm ánh sáng nhiễu xạ khác nhau sẽ chồng lên thiết bị lập trình được có máy ảnh cuối cùng tạo ra các ảnh chồng nhìn thấy ở một góc duy nhất do thiếu ánh sáng tới chuẩn trực. Không có cách nào đáng tin cậy để lọc và loại bỏ các phản xạ chồng và do đó việc xác minh ảnh phát ra phù hợp ở một góc cụ thể là một thách thức lớn.

Theo truyền thống, các thiết bị thay đổi quang học được thiết kế riêng nhằm mục đích tạo ra các hiệu ứng quang học làm hài lòng. Tính bảo mật của các thiết bị như vậy chủ yếu nằm trong việc sử dụng các kết cấu mà không ai khác có thể tạo ra, tức là làm cho việc tái tạo ra trở nên khó khăn. Để xác minh, cần có kiến thức chuyên môn và thông thường là các cấu trúc vi mô và nano được đánh giá trong điều kiện phòng thí nghiệm để xác minh cấu trúc vật lý chính xác của lưới. Khả năng xác minh tự động ở quy mô tế vi, ví dụ, dựa trên các ảnh được hiển thị, ví dụ, bằng phương tiện thị giác máy tính, thường không được xem xét ở tất cả. Ví dụ nổi bật về các thiết bị thay đổi quang học hiện đại là ảnh toàn ký cầu vồng

(cách tử nhiễu xạ bậc không/bậc một, thường có phản xạ đầy màu sắc) hoặc hoạt ảnh của các hình dạng hình học, ví dụ, đối tượng quay tròn hoặc chuyển động, hiệu ứng thu phóng (thường được tạo ra với cấu trúc Nano, vi gương hoặc cấu trúc tương tự), v.v.. Do mục đích chính của các OVD như vậy - cụ thể là làm hài lòng mắt về mặt quang học và có thể kiểm chứng trong điều kiện phòng thí nghiệm - nó thường được thử để tạo ra hoạt ảnh liền mạch và thay đổi màu sắc liên tục. Trong một được cho là lý tưởng, các thiết bị thay đổi quang học truyền thống được thiết kế với số lượng ảnh không giới hạn, được tạo ra dưới dạng một vùng màu duy nhất hòa vào nhau khi thay đổi góc nhìn, để tạo ra hiệu ứng thay đổi quang học mượt mà chuyên nghiệp. Đặc biệt là với ảnh toàn ký cầu vồng, điều này đạt được về mặt vật lý, vì ánh sáng trắng tới chỉ đơn giản là bị nhiễu xạ tại một cách tử. Vì chúng chỉ bao gồm một "pixel", hiển thị chuyển màu mượt mà, các OVD này không thể lưu trữ hoặc mã hóa bất kỳ dạng nào của các đoạn dữ liệu khác nhau hoặc riêng biệt.

Mặt khác, US 2012/0211567 A1 thể hiện các mã vạch động, cụ thể là một loạt mã vạch kế tiếp nhau, mã hóa một chuỗi thông tin. Một lớp quang học được tạo ra để ảnh hưởng đến việc hiển thị các mã vạch khác ở các góc nhìn khác nhau sao cho mỗi mã vạch được hiển thị ở một góc nhìn khác nhau. Mục đích của giải pháp này là tăng dung lượng dữ liệu được lưu trữ trong vùng của một mã vạch duy nhất. Để đạt được mục đích này, các điều kiện ánh sáng lý tưởng được mặc nhiên giả định và thực sự cần thiết. Tuy nhiên, như nêu trên, điều kiện ánh sáng như vậy trong khi có lẽ có thể chấp nhận được đối với các ứng dụng lưu trữ dữ liệu, nhưng lại không được chấp nhận đối với các ứng dụng đánh dấu bảo mật, nếu việc xác thực đáng tin cậy và thuận tiện là chìa khóa để người dùng chấp nhận và cuối cùng cần thiết để phát hiện ra sự gian lận và sự giả mạo.

Bản chất kỹ thuật của sáng chế

Mục đích của sáng chế là giải quyết vấn đề cố hữu về ảnh không thể đoán trước trong môi trường xác minh không được kiểm soát. Cụ thể là, sáng chế phải đề

xuất một thiết kế đặc biệt của các phần tử bảo mật thay đổi quang học của một dấu của đối tượng mà cho phép xác minh mạnh hơn bằng cách sử dụng thiết bị lập trình được có máy ảnh trong khi ít ảnh hưởng đến độ chuẩn xác và độ chính xác của quá trình xác minh.

Sáng chế đề xuất dấu của đối tượng như nêu trong phần đầu, trong đó các đoạn dữ liệu riêng biệt khác được biểu diễn bởi các đoạn mã khác và trong đó tập hợp này được liên kết với phần tử bảo mật thứ nhất và tập hợp này được liên kết với phần tử bảo mật thứ hai khác ít nhất một đoạn dữ liệu. Do đó, mỗi phần tử bảo mật hiển thị (tức là hiển thị, theo đặc tính phản xạ ánh sáng của nó) tùy thuộc vào điều kiện chụp ảnh ít nhất hai đoạn mã khác nhau. Các điều kiện chụp ảnh có thể có góc nhìn và/hoặc hướng chiếu sáng, trong đó cần có sự thay đổi của một trong hai hoặc cả hai để biểu lộ các đoạn mã khác nhau. Mỗi đoạn mã là một biểu diễn quang điện tử đọc được của một đoạn dữ liệu. Đoạn dữ liệu giống nhau có thể được biểu diễn bằng một hoặc nhiều đoạn mã. Mỗi đoạn mã đại diện cho chính xác một đoạn dữ liệu. Các đoạn dữ liệu được đại diện bởi các đoạn mã thuộc một tập hợp giới hạn các đoạn dữ liệu được liên kết với phần tử bảo mật tương ứng. Phần tử bảo mật thứ nhất được liên kết với tập hợp thứ nhất các đoạn dữ liệu. Phần tử bảo mật thứ hai được liên kết với tập hợp thứ hai các đoạn dữ liệu. Mỗi tập hợp có thể có ít nhất hai đoạn dữ liệu. Tập hợp thứ nhất các đoạn dữ liệu khác với tập hợp thứ hai các đoạn dữ liệu. Ví dụ, có thể có ít nhất một đoạn dữ liệu nằm trong tập hợp thứ nhất hoặc trong tập hợp thứ hai, nhưng không có trong cả hai tập hợp. Do đó, các đoạn mã được hiển thị bởi các phần tử bảo mật, và, cuối cùng, chính các phần tử bảo mật là khác nhau. Dấu của đối tượng có thể có nhiều hơn hai phần tử bảo mật khác nhau theo cùng một nghĩa; tức là nó có thể có ba hoặc nhiều phần tử bảo mật được liên kết với một số lượng tập hợp các đoạn dữ liệu tương ứng, trong đó mỗi cặp tập hợp là khác nhau theo định nghĩa nêu trên. Trong nhóm các phần tử bảo mật này, mỗi phần tử bảo mật có thể được tách biệt khỏi từng phần tử bảo mật khác. Tùy thuộc vào mức độ tương đồng giữa các tập hợp được xem xét (ví dụ, số lượng hoặc tỷ lệ của các đoạn dữ liệu trong nhiều tập

hợp), có thể phân biệt bất kỳ hai phần tử bảo mật nào trong một nhóm như vậy bằng cách đọc một hoặc nhiều đoạn mã của chúng trong một số điều kiện chụp ảnh tương ứng. Có thể có số lượng đoạn mã tối đa được xác định trước được hiển thị bởi mỗi phần tử bảo mật, sao cho ít nhất khi số lượng đoạn mã này được đọc từ hai phần tử bảo mật bất kỳ, có thể phân biệt được chúng.

Không giới hạn phạm vi của sáng chế, dấu của đối tượng có thể có các phần tử bảo mật tương tự, tức là hai hoặc nhiều phần tử bảo mật được liên kết với cùng một tập hợp các đoạn dữ liệu. Trong trường hợp có nhiều hơn một nhóm các phần tử bảo mật tương tự, các nhóm đó có thể là khác về kích thước của chúng (tức là số lượng các phần tử bảo mật của chúng) và/hoặc việc bố trí tương đối giữa các thành viên của chúng (ví dụ, khoảng cách giữa các phần tử bảo mật trong cùng một nhóm hoặc hướng của thành viên lân cận gần nhất trong cùng một nhóm). Các tính chất và biện pháp thích hợp này tạo ra các phần tử bảo mật khác biệt, nhưng tương tự có thể được phân biệt bằng các phần tử bảo mật khác nhau (hoặc liền kề), tương ứng của chúng. Nói cách khác, ngay cả các phần tử bảo mật tương tự cũng có thể - thường xuyên hơn không - được phân biệt với nhau, nếu đọc được phần tử bảo mật khác nhau lân cận (hoặc liền kề). Về bản chất, điều xảy ra là hai hoặc nhiều bộ tách dữ liệu được kết hợp dựa trên khoảng cách hình học của các phần tử bảo mật liên quan của chúng. Sau đó, tập hợp kết hợp thứ nhất và tập hợp kết hợp thứ hai khác ở ít nhất một đoạn dữ liệu. Để dễ hiểu hơn trong trường hợp đó, các tác giả sáng chế gọi là các "vùng lân cận" khác nhau của các phần tử bảo mật.

Việc phân biệt các phần tử bảo mật khác nhau hoặc các vùng lân cận khác nhau có thể được sử dụng để tăng tính đa dạng của các dấu của đối tượng có thể được tạo ra từ một vật liệu cơ bản nhất định. Tính đa dạng tăng có nghĩa là xác suất của bất kỳ dấu nào của hai đối tượng xác thực giống hệt nhau hoặc thậm chí giống nhau được giảm. Nỗ lực tạo ra một dấu của đối tượng tỷ lệ thuận với số lượng các trường hợp khác nhau mà có thể bị giả mạo, vì nguyên nhân sao chép cùng một

trường hợp thường đòi hỏi ít nỗ lực hơn một cách tương đối. Trong một cài đặt được ưu tiên, điều này có thể đạt được bằng cách quan sát tần suất tương đối của các dấu của đối tượng đã được xác minh với cùng một mẫu không thể phân biệt được - vì vậy về cơ bản là các bản sao xác thực về mặt vật lý. Quan sát này có thể được thực hiện bằng cách thu thập tất cả các xác minh từ một thiết bị xác minh duy nhất có máy ảnh hoặc từ một cơ sở dữ liệu, nơi dữ liệu xác minh của nhiều thiết bị lập trình được kết hợp với một máy ảnh được thu thập. Do xác suất của bản sao đích thực thấp, có thể có một ngưỡng thấp đối với thời gian tự do của bản sao và do đó, việc giả mạo có thể được phát hiện dễ dàng nếu nó được sử dụng để tạo ra một số lượng bản sao trên mức trung bình. Do đó, tính đa dạng cao hơn làm cho việc giả mạo mà không có nguy cơ bị phát hiện tầm thường trở nên tốn kém hơn và cuối cùng là kém hấp dẫn hơn.

Sáng chế đề xuất thêm một tập hợp các dấu của đối tượng, trong đó tập hợp này bao gồm một số dấu của đối tượng như được định nghĩa trên đây. Ví dụ, tập hợp bao gồm hai hoặc nhiều dấu của đối tượng thuộc loại được định nghĩa trên đây. Một bộ dấu của đối tượng , đặc biệt là khi nó có hơn 100, hơn 1000 hoặc hơn 10000 dấu của đối tượng, thể hiện các thuộc tính thống kê của một dấu của đối tượng. Đặc biệt, ví dụ, tốc độ lặp lại trung bình của các phần tử bảo mật với bất kỳ tập hợp đoạn dữ liệu cụ thể nào hoặc tốc độ lặp lại của bất kỳ vùng lân cận cụ thể hoặc tập hợp các đoạn dữ liệu kết hợp nào có thể được xác định từ một tập hợp các dấu của đối tượng hoặc kích thước tập hợp xác định một ranh giới trên cho tần số lặp lại như vậy. Nói cách khác, các thuộc tính thống kê của tập hợp là các biểu thức định lượng và có thể đo lường được của tính đa dạng được mô tả trên đây.

Hơn thế nữa, sáng chế đề xuất vật liệu cơ bản như nêu trên, trong đó các đoạn dữ liệu riêng biệt khác được đại diện bởi các đoạn mã khác và tập hợp này được liên kết với phần tử bảo mật thứ nhất và tập hợp này được liên kết với phần tử bảo mật thứ hai khác ở ít nhất một đoạn dữ liệu. Vật liệu cơ bản được cung cấp để tạo ra dấu của đối tượng. Tùy ý, vật liệu cơ bản có đủ số phần tử bảo mật để tạo ra ít

nhất hai dấu của đối tượng hoặc ít nhất ba dấu của đối tượng. Ví dụ, vật liệu cơ bản có thể có một mảng hai chiều các phần tử bảo mật với nhiều hơn đáng kể hai phần tử bảo mật, ví dụ, một mảng có ít nhất 5x5 phần tử bảo mật hoặc ít nhất 10x10 phần tử hoặc ít nhất 20x20 phần tử bảo mật. Không giới hạn phạm vi của sáng chế, vật liệu cơ bản này - như được giải thích cho một dấu của đối tượng nêu trên - ngoài ra có thể có các phần tử bảo mật tương tự, tức là hai hoặc nhiều phần tử bảo mật được liên kết với cùng một tập hợp các đoạn dữ liệu. Mọi thứ mà đã được giải thích cho một dấu của đối tượng nêu trên liên quan đến "vùng lân cận" có thể phân biệt được áp dụng như một khả năng tương tự đối với vật liệu cơ bản này. Hơn nữa, và một lần nữa không giới hạn phạm vi của sáng chế, vật liệu cơ bản có thể có trình tự lặp lại của các phần tử bảo mật, trong đó khoảng thời gian lặp lại, tức là khoảng cách giữa các lần lặp lại của các phần tử bảo mật, lớn hơn đáng kể so với kích thước của một dấu của đối tượng, ví dụ, lớn hơn ít nhất mười lần hoặc lớn hơn ít nhất trăm lần.

Hơn thế nữa, không giới hạn phạm vi sáng chế, sáng chế đề xuất phương pháp tạo ra các dấu của đối tượng bằng cách kết hợp ngẫu nhiên hoặc giả ngẫu nhiên ít nhất hai phần tử bảo mật khác nhau. Sự kết hợp ngẫu nhiên có thể đạt được bằng cách thay đổi cấu hình “vùng lân cận” của các thiết bị bảo mật có thể phân biệt được, tức là bố trí chúng theo cách khác nhau để có các dấu khác nhau của đối tượng. Để tạo ra các thiết bị bảo mật có ít nhất hai phần tử bảo mật khác nhau theo phương pháp này, một thiết bị được tạo cấu hình để chọn ngẫu nhiên hoặc giả ngẫu nhiên từ một tập hợp giới hạn các phần tử bảo mật có thể phân biệt được và đặt chúng một cách ngẫu nhiên hoặc giả ngẫu nhiên theo các bố trí hình học cụ thể có thể được dùng. Cụ thể hơn, các phần tử bảo mật có thể được tạo ra trước bằng bất kỳ phương tiện nào phù hợp để tạo ra các thiết bị thay đổi quang học . Hơn nữa, bất kỳ quy trình chuyển đã đăng ký nào phù hợp để chuyển các phần tử bảo mật đã được tạo ra trước sang vật liệu vận chuyển (tạo ra dấu của đối tượng) hoặc chính đối tượng có thể được sử dụng. Ví dụ, việc dập nóng hoặc dập nguội đã đăng ký, dập nguội kỹ thuật số, v.v. có thể được sử dụng để chuyển ít nhất hai

phần tử bảo mật giống OVD sang vật liệu hoặc đối tượng vận chuyển để tạo ra thiết bị bảo mật và dấu của đối tượng theo sáng chế.

Sáng chế cũng đề xuất một phương pháp tương ứng để xác thực dấu của đối tượng, dấu của đối tượng này có vùng được phân định rõ ràng bằng cách quang điện tử làm bằng vật liệu cơ bản (ví dụ, tạo dấu của đối tượng, tùy ý trên vật liệu vận chuyển hoặc trực tiếp trên đối tượng), trong đó vật liệu cơ bản là vật liệu cơ bản như được bộc lộ trên đây, trong đó vùng có phần tử bảo mật thứ nhất và ít nhất là phần tử bảo mật thứ hai, phương pháp này bao gồm các bước:

chụp ảnh thứ nhất dấu của đối tượng từ góc thứ nhất hoặc dưới hướng chiếu sáng thứ nhất;

xác định một đoạn mã thứ nhất được hiển thị bởi phần tử bảo mật thứ nhất trong ảnh thứ nhất;

giải mã đoạn mã thứ nhất để thu được đoạn dữ liệu thứ nhất;

chụp ảnh thứ hai dấu của đối tượng từ góc thứ hai và/hoặc dưới hướng chiếu sáng thứ hai;

xác định đoạn mã thứ hai được hiển thị bởi phần tử bảo mật thứ nhất trong ảnh thứ hai;

giải mã đoạn mã thứ hai để thu được đoạn dữ liệu thứ hai;

xác định từ một mô hình lưu trữ tập hợp các đoạn dữ liệu được liên kết với các phần tử bảo mật làm bằng vật liệu cơ bản này xem liệu có một tập hợp các đoạn dữ liệu chứa đoạn dữ liệu thứ nhất và đoạn dữ liệu thứ hai hay không.

Phương pháp nêu trên về cơ bản kiểm tra xem tổ hợp các đoạn dữ liệu có trong các phần tử bảo mật thứ nhất có tập hợp các đoạn dữ liệu tương ứng theo một mô hình được lưu trữ bao gồm các định nghĩa của tất cả các tập hợp đoạn dữ liệu hợp lệ hay không. Nếu không tìm thấy kết quả khớp nào, tức là không tìm thấy tập hợp tương ứng, thì phần tử bảo mật này có thể thuộc về một dấu của đối tượng giả mạo.

Đối nhằm mục đích xác thực của một phần tử bảo mật cụ thể, có thể chỉ quan sát một tập con có ít nhất hai đoạn mã của tất cả các đoạn mã có thể có đối với phần tử bảo mật cụ thể đó. Trong một cài đặt được ưu tiên, phương pháp xác thực này có thể được cài đặt để xác nhận tính xác thực khi N đoạn mã trong số M đoạn mã có thể có (đã biết từ mô hình này) đối với phần tử bảo mật cụ thể đó được quan sát từ các góc khác nhau hoặc trong các điều kiện chụp ảnh khác nhau (ví dụ, ánh sáng). Ví dụ về các tham số N và M là: N = 2 (N phải lớn hơn hoặc bằng 2), M = 5 (M phải lớn hơn hoặc bằng N, ví dụ M = N + 1, M = N + 2, M = N +3, M = N + 4). Vì tất cả các đoạn mã đều độc lập nên không quan trọng, N = 2 trong số M = 5 sẽ được giải mã. Bất kỳ sự kết hợp nào là đủ.

Nói chung, có thể đủ để quan sát hai hoặc nhiều đoạn mã khác nhau của một phần tử bảo mật cụ thể để thay đổi góc nhìn, trong khi hướng chiếu sáng (ví dụ, việc bố trí của nguồn sáng và phần tử bảo mật) vẫn không thay đổi.

Cuối cùng, sáng chế đề xuất phương pháp tạo ra dấu của đối tượng bao gồm các bước:

chọn ngẫu nhiên, giả ngẫu nhiên hoặc xác định một vùng làm bằng vật liệu cơ bản , trong đó vật liệu cơ bản là vật liệu cơ bản như được bộc lộ ở đây, vùng đã được chọn có phần tử bảo mật thứ nhất và ít nhất là phần tử bảo mật thứ hai, và

phân định rõ ràng bằng cách quang điện tử vùng đã được chọn từ phần không được chọn làm bằng vật liệu cơ bản.

Phương pháp chọn vùng làm bằng vật liệu cơ bản có thể góp phần vào sự thay đổi của các dấu của đối tượng thu được. Việc chọn ngẫu nhiên và cũng như giả ngẫu nhiên đảm bảo rằng không có sự lặp lại vô ý nào với tỷ lệ lặp lại tương đối cao hợp pháp được tạo ra. Do đó, các biện pháp này làm tăng thêm tính đa dạng. Hình dạng, kích thước của vùng chọn hoặc bất kỳ thuộc tính quang điện tử nào khác đọc được bằng cách quang điện tử có thể là khác nhau. Việc chọn có thể được thực hiện bằng cách cắt hoặc dập từ vật liệu cơ bản, kết hợp nhiều phần tử bảo

mật trực tiếp trên đối tượng hoặc in quá mức một phần vật liệu cơ bản và sử dụng mặt nạ chọn âm, để vật liệu cơ bản chỉ hiển thị trong vùng được che này.

Trong một cài đặt được ưu tiên khác, vì thông qua mô hình đã biết vị trí chọn từ bên trong vật liệu cơ bản, vật liệu cơ bản được đề xuất đặc biệt thích hợp để sử dụng nhằm tạo ra các thiết bị bảo mật như được đề xuất trong WO 2015/079014 A1 và/hoặc được sử dụng trong hệ thống bảo mật như nêu trong WO 2013/188897 A1. Trong một cài đặt cụ thể như vậy, điều kiện ngẫu nhiên được đưa vào thông qua quá trình chọn, ví dụ, do dung sai chế tạo, được kết hợp với thông tin hình học đã biết trước từ mô hình này, về cơ bản là ánh xạ vật liệu cơ bản.

Bằng cách cung cấp cho các phần tử bảo mật thể hiện các đoạn mã đại diện cho các đoạn dữ liệu bằng cách quang điện tử thay vì các phần tử bảo mật, ví dụ , với hiệu ứng cầu vồng, tức là thay đổi màu trơn tru, việc xác thực dấu của đối tượng mạnh hơn nhiều. Lý do giải thích điều này là nó có thể được xác định xem các đoạn mã có thực sự đại diện cho các đoạn dữ liệu hợp lệ hay không. Cơ hội mà các điều kiện chiếu sáng ngẫu nhiên hoặc khuếch tán sẽ dẫn đến phần tử bảo mật không hợp lệ vô tình hiển thị đoạn mã đại diện cho đoạn dữ liệu hợp lệ thấp hơn nhiều so với việc một ảnh chuyển màu không hợp lệ hoặc một hình dạng hình học đơn giản sẽ vô tình hiển thị một ảnh hợp lệ. Hơn thế nữa, bằng các phần tử bảo mật hiển thị các đoạn mã đại diện cho các đoạn dữ liệu, từ việc quét một đoạn mã, vị trí của đoạn mã đó trong vật liệu cơ bản ban đầu (hoặc một trong số ít các vị trí hợp lệ) có thể được xác định và tính hợp lệ của nó được xác minh thông qua một mô hình liên kết tập hợp các đoạn dữ liệu (hoặc vùng lân cận) với các vị trí. Nói cách khác, các phần tử bảo mật được sử dụng làm điểm mốc trong một mô hình (ví dụ, bản đồ hóa một vật liệu cơ bản, từ đó các dấu của đối tượng được tạo ra). Vì các phần tử bảo mật khác nhau trong ít nhất một đoạn dữ liệu, nên vị trí có thể được xác định bằng cách thay đổi các điều kiện chụp ảnh. Theo cách khác hoặc ngoài ra, tùy thuộc vào các tập hợp, vị trí cũng có thể được xác định bằng cách

chụp ảnh phần tử bảo mật thứ nhất và phần tử bảo mật thứ hai chỉ trong một điều kiện chụp ảnh duy nhất và tìm kiếm các tổ hợp tương ứng của các tập hợp lân cận (của các phần tử bảo mật lân cận hoặc liền kề). Trong trường hợp đó, "vùng lân cận" có thể đóng vai trò là điểm mốc trong mô hình này. Cần lưu ý rằng để xác minh trong cài đặt này cho ít nhất một phần tử bảo mật, ít nhất một đoạn mã thứ hai (và đoạn dữ liệu tương ứng) cần được quan sát từ ít nhất một môi trường thu khác thứ hai để đảm bảo rằng OVD thực sự có mặt (và không phải là một bản sao được in đại diện cho OVD từ trong một môi trường chụp ảnh duy nhất). Cần lưu ý thêm rằng dấu của đối tượng được bộc lộ ở đây, cụ thể là các phần tử bảo mật, không cho phép sử dụng mã vạch động để mã hóa nhiều thông tin hơn mã vạch thông thường. Thay vào đó, nó cho phép sử dụng mã vạch động để xác thực.

Trong việc hiển thị tùy thuộc vào các điều kiện chụp ảnh, một đoạn mã được hiểu rằng đoạn mã tương ứng được hiển thị vật lý ở ít nhất một dạng nào đó. Cụ thể, có ít nhất một điều kiện chụp ảnh cho mỗi đoạn mã, theo đó đoạn mã đó có thể được phân biệt với các đoạn mã khác của phần tử bảo mật đó và/hoặc có thể được xác định bằng cách quang điện tử từ các đoạn mã đại diện cho các đoạn dữ liệu của một tập hợp của phần tử bảo mật đó. Với góc nhìn có nghĩa là góc nhìn dấu của đối tượng, cụ thể hơn là của phần tử bảo mật tương ứng. Đối với các ứng dụng thực tế, điều quan trọng cần kể ra là - nói một cách chính xác - các góc nhìn và điều kiện chụp ảnh đã hơi khác đối với các phần tử bảo mật lân cận. Đây là một vấn đề khó giải quyết với các thiết bị thay đổi quang học truyền thống. Người ta có thể thiết kế các thiết bị thay đổi quang học với các đặc tính mạnh đến mức không thể bỏ qua độ lệch hình học. Theo cách khác, theo kinh nghiệm của các tác giả sáng chế là không thực tế, các điều kiện chụp ảnh có thể được ước tính từ ảnh hiển thị quan sát được từ đoạn mã thứ nhất và một mô hình toán học được sử dụng để kết luận về ảnh được hiển thị dự kiến của đoạn mã thứ hai lân cận.

Một ưu điểm có thể đạt được với sáng chế là việc xác thực về cơ bản là việc kiểm tra xem một đoạn dữ liệu cụ thể có thuộc tập hợp các đoạn dữ liệu của một phần

tử bảo mật cụ thể hay không. Phương pháp xác minh này rất mạnh và không còn yêu cầu tính đến sự thay đổi của các điều kiện chụp ảnh xảy ra trong một ảnh đã được chụp ảnh do sự biến dạng hình học trên thiết bị bảo mật hoặc cụ thể hơn là trên dấu của đối tượng.

Một đoạn mã của phần tử bảo mật thứ hai tốt hơn là ít nhất một phần, tốt hơn là hoàn toàn, không chồng lên một đoạn mã của phần tử bảo mật thứ nhất. Các đoạn mã đại diện cho các đoạn dữ liệu từ tập hợp được liên kết với phần tử bảo mật thứ nhất tốt nhất là ít nhất một phần, tốt hơn là hoàn toàn, không chồng lên các đoạn mã đại diện cho các đoạn dữ liệu từ tập hợp được liên kết với phần tử bảo mật thứ hai. Ngoài ra, chính các phần tử bảo mật, tức là phần tử bảo mật thứ nhất và phần tử bảo mật thứ hai, có thể ít nhất một phần không chồng lên hoặc (hoàn toàn) không chồng lên. Tức là, chúng có thể được bố trí mà không có sự chồng lên giữa phần tử bảo mật thứ nhất và phần tử bảo mật thứ hai. Chúng có thể được bố trí, ví dụ , liền kề, kề nhau hoặc cách xa nhau.

Tùy ý, tập hợp các đoạn dữ liệu được liên kết với mỗi phần tử bảo mật là tập hợp các đoạn dữ liệu đọc được bằng cách quang điện tử được thể hiện bằng tổng hợp các đoạn mã được hiển thị trong toàn bộ các điều kiện chụp ảnh. Tùy ý, đối với mỗi đoạn dữ liệu trong tập hợp các đoạn dữ liệu được liên kết với mỗi phần tử bảo mật, có ít nhất một đoạn mã đọc được bằng cách quang điện tử đại diện cho đoạn dữ liệu này trong ít nhất một điều kiện chụp ảnh xác định. Tức là, mỗi đoạn mã đọc được bằng cách quang điện tử đại diện cho một đoạn dữ liệu trong tập hợp các đoạn dữ liệu được liên kết với mỗi phần tử bảo mật được hiển thị bởi phần tử bảo mật này trong ít nhất một điều kiện chụp ảnh xác định.

Dấu của đối tượng này theo một phương án cụ thể, đối với một hướng chiếu sáng cố định, mỗi đoạn dữ liệu trong một tập hợp được liên kết với phần tử bảo mật (và, do đó, mỗi đoạn mã được hiển thị bởi phần tử bảo mật tương ứng) được liên kết với một chế độ nhìn riêng biệt vùng góc, trong đó độ tương phản của đoạn mã

đại diện cho đoạn dữ liệu tương ứng cao hơn độ tương phản của các đoạn mã đại diện cho tất cả các đoạn dữ liệu khác từ cùng một tập hợp. Nói cách khác, các đoạn mã được liên kết với phạm vi góc nhìn hoặc vùng mà chúng có thể được đọc ra. Ngược lại, mỗi góc nhìn chỉ được quy cho một đoạn mã cụ thể (và do đó, đoạn dữ liệu), nhưng mỗi đoạn mã có thể hiển thị từ các góc nhìn khác nhau. Phạm vi góc nhìn nói chung phụ thuộc vào độ chiếu sáng thực tế và có thể thực sự chồng lên trong trường hợp có các nguồn sáng phân tán. Cũng cần lưu ý rằng trong một ứng dụng thực tế, một đoạn dữ liệu cụ thể có thể được liên kết với các góc nhìn hoặc vùng góc nhìn riêng biệt, trong đó mỗi góc nhìn hoặc vùng góc nhìn có thể chỉ được quy cho chính xác một đoạn dữ liệu, tức là có thể có một phân phối độc quyền các góc nhìn hoặc vùng góc nhìn giữa các đoạn dữ liệu của một tập hợp cụ thể được liên kết với phần tử bảo mật.

Trong ngữ cảnh này, có thể tùy ý có ít nhất một vùng góc nhìn được liên kết với đoạn dữ liệu của tập hợp phần tử bảo mật thứ nhất, khác với từng vùng góc nhìn được liên kết với các đoạn dữ liệu của tập hợp phần tử bảo mật thứ hai. Do đó, có thể có ít nhất một góc nhìn mà ở đó phần tử bảo mật thứ nhất thay đổi đoạn mã được hiển thị trong khi phần tử bảo mật thứ hai không thay đổi đoạn mã được hiển thị. Nói một cách tổng quát hơn, các đặc tính chuyển có thể là khác nhau giữa các phần tử bảo mật thứ nhất và các phần tử bảo mật thứ hai. Ví dụ, các đặc tính chuyển có thể là khác nhau do các kích thước khác nhau của tập hợp đoạn dữ liệu thứ nhất và tập hợp đoạn dữ liệu thứ hai: ví dụ, tập hợp đoạn dữ liệu thứ nhất có thể có chín đoạn dữ liệu và tập hợp đoạn dữ liệu thứ hai có thể có 18 đoạn dữ liệu, trong đó phần tử bảo mật thứ nhất hiển thị một đoạn mã khác (tức là chuyển) cứ sau 20° giữa chế độ góc nhìn 0° và 180° và phần tử bảo mật thứ hai thể hiện một đoạn mã khác (tức là các lần chuyển) cứ 10° giữa góc nhìn 0° và 180 °.

Mỗi đoạn mã có thể là một ảnh có cấu trúc, cụ thể là cấu trúc giống mã vạch, tốt hơn là mã 2D, tốt hơn là mã mảng 2D. Các loại ảnh này tương đối dễ đọc bằng cách quang điện tử. Đặc biệt, ảnh có cấu trúc có thể tạo ra đủ độ tương phản để

phân biệt cấu trúc trong các điều kiện ánh sáng khác nhau.

Cụ thể hơn, mỗi đoạn mã có thể là mã mảng 2D, trong đó mỗi đoạn mã là một mảng ô và đoạn dữ liệu được đại diện bởi đoạn mã bởi mỗi ô của đoạn mã lấy ra một trong số ít nhất hai trạng thái có thể phân biệt bằng quang (ví dụ, tối hoặc sáng, đen hoặc trắng), trong đó các đoạn mã được hiển thị bởi phần tử bảo mật thứ nhất được bố trí liền kề với các đoạn mã được phần tử bảo mật thứ hai. Mã mảng 2D có thể thực hiện mà không có sự tách giữa các ô của các đoạn mã liền kề và/hoặc không tìm thấy các mẫu.

Theo một phương án của sáng chế, mọi đoạn mã có thể đại diện cho đoạn dữ liệu tương ứng ở dạng mã hóa được xác định trước, trong đó việc mã hóa được xác định trước có thông tin để phát hiện lỗi hoặc sửa lỗi.

Tùy ý, việc mã hóa được xác định trước có thể cho phép số lượng tối đa các đoạn dữ liệu riêng biệt có thể có và số lượng đoạn dữ liệu trong tập hợp các đoạn dữ liệu của mỗi phần tử bảo mật có thể nhỏ hơn 1/100, tốt hơn là nhỏ hơn 1/1000, tốt hơn tốt nữa là nhỏ hơn 1/10000, trong số tối đa các đoạn dữ liệu riêng biệt có thể có. Nói cách khác, chỉ một phần nhỏ các đoạn dữ liệu có thể có (và - do đó - các đoạn mã) có thể được sử dụng thực sự. Giả sử rằng lỗi đọc sẽ liên quan đến tất cả các phần của các đoạn mã gần như nhau, thì điều này có thể được sử dụng để phát hiện lỗi đọc, vì chúng có nhiều khả năng hơn là không dẫn đến đoạn dữ liệu đọc ra mà không được sử dụng. Về mặt này, các đoạn dữ liệu đã sử dụng có thể được chọn sao cho các đoạn mã đại diện cho chúng khác ở nhiều ô (trong trường hợp mã mảng 2D có ô), tốt nhất là nhiều hơn hai ô, sao cho một ô được lật sẽ dẫn đến một đoạn dữ liệu không được sử dụng và do đó là lỗi đọc có thể phát hiện được.

Vị trí của các phần tử bảo mật tương đối với nhau có thể được xác định trước. Ví dụ, các vị trí đó có thể được lưu trữ trong một mô hình và được sử dụng để xác định và phân biệt các vùng lân cận của các thiết bị bảo mật tương tự (ít nhất là

một phần), do đó cải thiện tính đa dạng của các dấu của đối tượng có thể phân biệt được.

Do đó, đối với vật liệu cơ bản, vị trí của các phần tử bảo mật trên vật liệu cơ bản có thể được xác định trước tương đối với nhau theo một mô hình và các đoạn dữ liệu của tập hợp liên kết với các phần tử bảo mật có thể được xác định trước theo mô hình này.

Do đó, khi dấu của đối tượng được tạo ra bằng cách đặt các phần tử bảo mật một cách ngẫu nhiên, giả ngẫu nhiên hoặc xác định theo một cách bố trí hình học, thì vị trí của các phần tử bảo mật này có thể được ghi lại trong một mô hình hoặc cơ sở dữ liệu. Thông tin này có thể được truy cập trong quá trình xác minh.

Tùy ý, mọi đoạn mã có thể đại diện cho đoạn dữ liệu tương ứng trong việc mã hóa được xác định trước, trong đó việc mã hóa được xác định trước tốt hơn là có thông tin để phát hiện lỗi hoặc sửa lỗi. Việc phát hiện lỗi đặc biệt hữu ích để kích hoạt việc đọc lại (tức là cố gắng đọc lặp lại) đoạn mã có liên quan, trong đó các lần đọc lại như vậy thường được thực hiện theo cách có lợi trong các điều kiện chiếu sáng khác nhau, làm tăng khả năng không lặp lại cùng một lỗi đọc.Việc sửa lỗi cung cấp khả năng đọc bằng cách quang điện tử mạnh hơn đối với các đoạn mã, trong đó các lỗi thường đọc của các phần nhỏ của đoạn mã có thể được chấp nhận. Cả hai, việc phát hiện lỗi và sửa lỗi, do đó góp phần vào sự mạnh của bản đọc. Điều này làm giảm khả năng dấu của đối tượng xác thực sẽ bị từ chối (từ chối sai). Điều đáng nói là, đặc biệt là sử dụng các bảng mã sửa lỗi nổi tiếng, ví dụ, Reed-Solomon, được biết là dễ bị giải mã sai khi được sử dụng trên một đoạn dữ liệu rất nhỏ, ví dụ, 16 bit, nhưng khả năng sửa lỗi cao.

Là một phần mở rộng cho những gì đã được bàn luận trên đây đối với các dấu đơn lẻ của đối tượng, việc mã hóa được xác định trước có thể cho phép số lượng tối đa các đoạn dữ liệu riêng biệt có thể có và số lượng các đoạn dữ liệu riêng biệt trong

tập hợp các đoạn dữ liệu của tất cả các phần tử bảo mật (tức là trên vật liệu cơ bản) có thể nhỏ hơn 1/100, tốt hơn là nhỏ hơn 1/1000, tốt hơn nữa là nhỏ hơn 1/10000 các đoạn dữ liệu riêng biệt tối đa có thể có. Việc sử dụng đoạn dữ liệu thưa thớt này có thể được khai thác để giảm đến mức tối thiểu hơn nữa số lượng từ chối sai đối với nhược điểm đã biết với các đoạn dữ liệu rất nhỏ trong mã sửa lỗi, như nêu trên.

Liên quan đến phương pháp xác thực dấu của đối tượng, phương pháp này có thể có thêm các bước:

xác định đoạn mã thứ ba được hiển thị bởi phần tử bảo mật thứ hai trong ảnh thứ nhất hoặc trong ảnh thứ hai;

giải mã đoạn mã thứ ba để thu được đoạn dữ liệu thứ ba;

xác định từ một mô hình lưu trữ các tập hợp các đoạn dữ liệu được liên kết với các phần tử bảo mật làm bằng vật liệu cơ bản và lưu trữ vị trí tương đối của các phần tử bảo mật làm bằng vật liệu cơ bản với nhau xem phần tử bảo mật thứ hai được định vị tương đối với phần tử bảo mật thứ nhất thu được liên kết với một tập hợp các đoạn dữ liệu chứa đoạn dữ liệu thứ ba. Trong trường hợp này, bản chất thay đổi quang của phần tử bảo mật thứ hai được xác minh và - ngoài ra - thông tin chứa trong đó được sử dụng để tăng tính đa dạng của các dấu của đối tượng.

Trong phương pháp này theo một phương án cụ thể để xác thực, các phần tử bảo mật làm bằng vật liệu cơ bản mà dấu của đối tượng có một phần, có thể được bố trí theo kiểu có ô và mỗi đoạn mã được hiển thị bởi các phần tử bảo mật là một mảng ô và các đoạn mã được hiển thị bởi một phần tử bảo mật được bố trí lan sang các đoạn mã được hiển thị bởi các phần tử bảo mật khác để tạo ra một mảng lớn hơn, trong đó phương pháp này còn bao gồm các bước:

a) xác định một ô của mẫu thứ nhất trong ảnh thứ nhất;

b) giải mã đoạn mã của mẫu thứ nhất trong ảnh thứ nhất đã được tạo ra bởi một mảng của mẫu thứ nhất có ô của mẫu thứ nhất nêu trên ở một vị trí được xác

định trước, để thu được đoạn dữ liệu của mẫu thứ nhất;

c) xác định từ một mô hình lưu trữ tập hợp các đoạn dữ liệu được liên kết với các phần tử bảo mật làm bằng vật liệu cơ bản này xem có ít nhất một tập hợp các đoạn dữ liệu kết hợp với đoạn dữ liệu của mẫu thứ nhất nêu trên hay không;

d) nếu không xác định được tập hợp nào như vậy ở bước c), lặp lại các bước từ a) đến c) với các ô khác của mẫu thứ nhất cho đến khi tìm thấy tập hợp đó ở bước c); và

l) xác định đoạn mã của mẫu thứ nhất hiện tại là đoạn mã thứ nhất.

Tùy ý, cụ thể hơn phương pháp này có thể có thêm các bước sau trước bước l):

e) xác định ô của mẫu thứ nhất trong ảnh thứ hai;

f) giải mã đoạn mã của mẫu thứ hai trong ảnh thứ hai đã được tạo ra bởi mảng ô của mẫu thứ nhất, để thu được đoạn dữ liệu của mẫu thứ hai;

g) xác định từ một mô hình lưu trữ tập hợp các đoạn dữ liệu được liên kết với các phần tử bảo mật của lớp cơ sở, xem liệu ít nhất một trong số ít nhất một tập hợp chứa đoạn dữ liệu của mẫu thứ nhất có chứa đoạn dữ liệu của mẫu thứ hai hay không;

h) nếu không xác định được tập hợp nào như vậy ở bước g), thì lặp lại các bước từ a) đến g) cho đến khi tìm thấy tập hợp đó ở bước g); và

m) xác định đoạn mã của mẫu thứ hai hiện tại là đoạn mã thứ hai.

Cuối cùng, để tùy ý tinh chỉnh thêm phương pháp xác thực, phương pháp này có thể có thêm các bước sau trước bước l) và - nếu có - trước bước m):

i) giải mã đoạn mã của mẫu thứ ba đã được tạo ra bởi mảng ô của mẫu thứ hai được định vị tương đối với mảng ô của mẫu thứ nhất, để thu được đoạn dữ liệu của mẫu thứ ba;

j) xác định từ một mô hình lưu trữ tập hợp các đoạn dữ liệu được liên kết với các phần tử bảo mật làm bằng vật liệu cơ bản và lưu trữ vị trí tương đối của các phần tử bảo mật làm bằng vật liệu cơ bản với nhau, xem liệu đoạn dữ liệu của mẫu thứ ba có nằm trong tập hợp các đoạn dữ liệu thuộc phần tử bảo mật được định vị tương đối với phần tử bảo mật mà tập hợp được xác định sơ bộ ở bước e) thuộc về;

k) nếu không xác định được tập hợp nào như vậy ở bước j), thì lặp lại các bước từ a) đến d) và các bước i) đến j) và tốt hơn là các bước từ e) đến h), cho đến khi tìm thấy tập hợp đó ở bước j);

n) xác định đoạn mã của mẫu thứ ba hiện tại là đoạn mã thứ ba.

Mô tả vắn tắt các hình vẽ

Bây giờ đề cập đến các hình vẽ, trong đó các hình vẽ này dùng để minh họa sáng chế và không nhằm mục đích mục đích giới hạn nó,

fig.1a thể hiện dưới dạng sơ đồ vật liệu cơ bản theo phương án thứ nhất để tạo ra các dấu của đối tượng theo sáng chế với sáu phần tử bảo mật hoàn chỉnh và bên dưới dấu của đối tượng biểu thị trực quan hai bộ đoạn dữ liệu được liên kết với hai trong số các phần tử bảo mật;

fig.1b thể hiện dưới dạng sơ đồ dấu của đối tượng và chỉ ra các đoạn mã được hiển thị ở ba góc nhìn khác nhau;

fig.2 thể hiện dưới dạng sơ đồ vật liệu cơ bản theo phương án thứ hai của sáng chế để tạo ra các dấu của đối tượng, với mười sáu thiết bị bảo mật thể hiện mã mảng 2D dưới dạng các đoạn mã, trong đó các đoạn mã ở các góc nhìn khác nhau được chỉ ra; và

fig.3a- fig.c minh họa dưới dạng sơ đồ phương pháp xác thực một dấu của đối tượng theo sáng chế.

Mô tả chi tiết sáng chế

Là khối xây dựng cơ bản làm bằng vật liệu cơ bản 1 và do đó dấu của đối tượng 8 theo sáng chế, các phần tử bảo mật 2 được tối ưu hóa để có thể được xác minh bằng thiết bị lập trình được có máy ảnh được đề xuất theo phương án thứ nhất. Mỗi phần tử bảo mật 2 làm bằng vật liệu cơ bản 1 chỉ có thể hiển thị một tập hợp ảnh có thể phân biệt được rất hạn chế, rời rạc. Điều này ngụ ý - do số lượng kết hợp không hạn định giữa cài đặt chiếu sáng và góc nhìn - mà mỗi ảnh của bộ giới hạn này sẽ có thể được nhìn thấy từ các góc nhìn. Trên thực tế, các thiết bị bảo mật 2 như vậy có thể được thiết kế bằng cách tạo ra các phần tử quang học, hiển

thị một ảnh nhất định cho một loạt góc (phương vị), tức là hiển thị cùng một ảnh cho +/- 5 độ. Điều này có thể được thực hiện với thấu kính dạng hai mặt lồi, cách tử nhiễu xạ, gương siêu nhỏ và thấu kính siêu nhỏ, cấu trúc nano, v.v..

Ảnh được hiển thị của các phần tử bảo mật có thể là ảnh theo nghĩa "truyền thống", ví dụ, hình dạng hình học, sự kết hợp của các hình dạng, màu sắc khác nhau, ảnh được pixel hóa, v.v.. Theo sáng chế, các ảnh đó còn được gọi là đoạn mã. Sau đó, các tác giả sáng chế sẽ minh họa các cấu trúc có thể có khác nhau làm bằng vật liệu cơ bản (thường là sản phẩm dạng tấm) và sáng chế theo các phương án khác nhau.

Để phác thảo chức năng chính của sáng chế, các tác giả sáng chế giả định trên FIG 1a nhằm mục đích minh họa là một cài đặt, trong đó tập hợp các ảnh có sẵn bao gồm các ảnh của các ký tự thường từ bảng chữ cái Latinh, tức là {a ... z}. Fig.1a còn thể hiện để làm ví dụ một phần làm bằng vật liệu cơ bản được đề xuất 1 có các phần tử bảo mật 2. Để dễ hiểu hơn, các tác giả sáng chế tập trung giải thích phần tử bảo mật thứ nhất 3 và phần tử bảo mật thứ hai 4. Phần tử bảo mật thứ nhất 3 được tạo cấu hình để hiển thị - tùy thuộc vào góc nhìn - một ảnh (hoặc, nói chung, là đoạn mã) 5 trong số tập hợp ảnh thứ nhất 6 (hoặc nói chung, các đoạn mã đại diện cho các đoạn dữ liệu từ tập hợp thứ nhất các đoạn dữ liệu). Phần tử bảo mật thứ hai 4 được tạo cấu hình để hiển thị - tùy thuộc vào góc nhìn - một ảnh (hoặc nói chung là đoạn mã) 5 trong số một bộ ảnh thứ hai 7 (hoặc nói chung, các đoạn mã đại diện cho các đoạn dữ liệu từ tập hợp các đoạn dữ liệu thứ hai). Số lượng ảnh trong hai tập hợp 6, 7 có thể là khác nhau cũng như tính liên kết góc, tức là các ảnh trong bộ thứ nhất 6 có thể có các đặc tính chuyển khác với các ảnh trong bộ 7. Ngoài ra, một số ảnh nhất định có thể xuất hiện trong nhiều bộ, ví dụ, trong tập hợp 6 và 7, miễn là chính các tập hợp này có thể phân biệt được, tức là không phải tất cả các phần tử đều là như nhau.

Như đã được phác thảo trên đây, các quy trình tạo ra dấu khác nhau có thể được

chọn để tạo ra một dấu của đối tượng 9 từ vật liệu cơ bản 1.

Fig.1b thể hiện để làm ví dụ, sau khi chọn từ vật liệu cơ bản 1, một dấu của đối tượng 9, chứa phần tử bảo mật thứ nhất 3 và phần tử bảo mật thứ hai 5. Fig.1b thể hiện thêm các ảnh được hiển thị (hoặc các đoạn mã) 5 của việc chọn nêu trên khi được nhìn từ các góc khác nhau 10. Khi được nhìn từ góc thứ nhất 10 α, phần tử bảo mật thứ nhất 3 hiển thị ảnh (hoặc mã) "a", là thành viên của bộ ảnh 6 tương ứng với phần tử bảo mật thứ nhất 3. Ở cùng một góc nhìn, phần tử bảo mật thứ hai 4 hiển thị ảnh (hoặc mã) "z", là thành viên của tập hợp các ảnh 7 tương ứng với phần tử bảo mật thứ hai 4.

Tương tự, ở góc 10 β, phần tử bảo mật thứ nhất 3 hiển thị "s", trong khi phần tử bảo mật thứ hai 4 thể hiện "v", cả hai thành phần của bộ ảnh tương ứng 6, 7. Các tác giả sáng chế muốn lưu ý rằng - do tập hợp rất hạn chế các ảnh có sẵn và số lượng vô hạn các tình huống chiếu sáng/phối cảnh có thể có, các kết hợp khác nhau hoặc tất cả các ảnh có thể trở nên khả thi. Ví dụ, dưới góc quan sát 10 γ, phần tử bảo mật thứ nhất 3 lại hiển thị ảnh "a" 5 (tương tự như ở góc 10 α), nhưng phần tử bảo mật thứ hai 4 hiển thị ảnh "b" 5. Tình huống này có thể xảy ra thêm nếu trong thiết kế làm bằng vật liệu cơ bản , 1 đặc tính chuyển khác nhau, tức là các phần tử và đặc tính quang học khác nhau, được sử dụng cho các phần tử bảo mật khác nhau 2. Phần tử bảo mật thứ nhất 3 có thể - ngoài việc có một bộ ảnh khác - cũng có các đặc tính chuyển khác nhau / các góc chuyển so với phần tử bảo mật thứ hai 4.

Như một lưu ý về ký hiệu, để dễ nhìn trên các hình vẽ tiếp theo, các tác giả sáng chế sẽ sử dụng chữ cái viết hoa A… P để biểu thị các phần tử bảo mật khác nhau 2. Các tác giả sáng chế sẽ biểu thị phần tử bảo mật thứ nhất 3 bằng chữ cái "A" và phần tử bảo mật thứ hai 4 bằng chữ cái "B", v.v. ảnh thứ nhất (hoặc đoạn mã) 5 trong tập hợp các ảnh 6 sau đó sẽ được ký hiệu là A_1, ảnh thứ hai là A_2, v.v. Tương tự, ảnh (hoặc đoạn mã) 5 đối với phần tử bảo mật thứ hai 4 trong số bộ ảnh

thứ hai tương ứng 7 sẽ được ký hiệu là B_1, bộ thứ hai là B_2, v.v. Trong trường hợp đơn giản nhất, mỗi đoạn mã có mối quan hệ 1: 1 với một đoạn dữ liệu tương ứng. Tuy nhiên, phạm vi của sáng chế mở rộng đến các tình huống trong đó nhiều đoạn mã (ví dụ, A_1.1, A_1.2, v.v.) có thể đại diện cho cùng một đoạn dữ liệu (ví dụ, A_1). Có liên quan đối với tập hợp này là đoạn dữ liệu. Để đơn giản, các tác giả sáng chế sẽ sử dụng, cùng với việc mô tả các hình vẽ tiếp theo, các cụm từ ảnh, đoạn mã và đoạn dữ liệu đồng nghĩa và có số chỉ dẫn là 5.

Trong các ứng dụng thực tế, khi sử dụng phương tiện thị giác máy tính trên các thiết bị lập trình được được có máy ảnh để xác minh hoặc đọc một số ảnh nhất định, thì tính chính xác của việc đọc/giải mã ảnh luôn là vấn đề được quan tâm. Mặc dù phần giới thiệu có nêu ví dụ về ảnh chuyển màu nghe có vẻ khá đơn giản, nhưng việc đọc và phân loại màu (tuyệt đối và thậm chí tương đối) vẫn là một vấn đề rất khó trong lĩnh vực thị giác máy tính. Do đó, việc chọn các màu khác nhau như các ảnh hiển thị khác nhau không được khuyến khích. Các hình dạng hình học hay nói chung, các ảnh có cấu trúc với độ tương phản tốt sẽ đáng tin cậy hơn để đọc và giải mã, nhưng vẫn - mà không cần thực hiện bất kỳ biện pháp bổ sung nào - thì không thể tránh khỏi hoàn toàn các lỗi giải mã. Vì vậy, trong một ứng dụng thực tế, việc sử dụng ảnh chung hoặc thậm chí ảnh của các chữ cái (như được sử dụng trên fig.1) đặt ra một vấn đề không nhỏ, khi thực tế cần phải đọc ít lỗi. Và điều đó thực sự được mong muốn nhằm mục đích này, vì các tác giả sáng chế cần một cách đáng tin cậy để xác định từ một ảnh đã được giải mã xem ảnh đại diện đoạn dữ liệu đó có phải là thành viên của tập hợp các đoạn dữ liệu đối với phần tử bảo mật cụ thể đó hay không. Và các tác giả sáng chế chắc chắn không muốn cản trở sự chấp nhận của người tiêu dùng bằng cách từ chối dấu của đối tượng xác thực do lỗi đọc.

Theo một phương án được ưu tiên, các ảnh 5 được thiết kế theo cách để có thể đọc dễ dàng và thực tế, không có lỗi theo cách tự động bởi thiết bị lập trình được có máy ảnh. Một biện pháp khả thi để đảm bảo khả năng đọc chính xác, đó là nhúng

các cấu trúc giống tổng kiểm tra/giống tính chẵn lẻ vào mỗi ảnh có thể. Khái niệm này được biết đến nhiều trong lĩnh vực viễn thông; ảnh này được tạo cấu trúc thành ít nhất hai phần có thể đọc/giải mã riêng biệt và có mối quan hệ giữa các phần đó. Trong không gian công nghệ thông tin, các phần này thường được gọi là "từ mã" lần lượt là "tải trọng"
và "tính chẵn lẻ". Các từ mã/phần được đọc và giải mã riêng biệt, và các kết quả được giải mã sau đó được đối sánh với nhau. Nếu chúng khớp nhau, việc đọc đúng được xác thực. Các phương pháp nổi bật trong lĩnh vực công nghệ thông tin là tổng kiểm tra, mã kiểm tra dự phòng theo chu kỳ (CRC) hoặc mã sửa lỗi (EC). Trong lĩnh vực mã vạch có thể giải mã trực quan, đặc biệt là Mã hóa Reed-Solomon - một ví dụ về mã EC - là phổ biến.

Do đó, các tác giả sáng chế đề xuất một phương án có thể có của sáng chế là sử dụng ảnh 5, được tối ưu hóa đối với khả năng đọc/giải mã mạnh bằng cách sử dụng các thiết bị lập trình được có máy ảnh. Một việc chọn trực quan là việc sử dụng các cấu trúc giống như mã vạch, ví dụ, Mã 2D hoặc cấu trúc theo pixel, đại diện cho từ mã đã được mã hóa bằng Mã EC, ví dụ, mã hóa Reed-Solomon.

Các mã hóa như vậy cung cấp khả năng mã hóa bất kỳ loại đoạn dữ liệu kỹ thuật số nào (ví dụ, số, số alpha-số, dữ liệu nhị phân, v.v.). Trong một cài đặt được ưu tiên, số nhận dạng số hoặc chữ và số có thể được mã hóa theo cấu trúc giống như 2D và tập hợp các ảnh có thể có tương ứng với tập hợp các số nhận dạng đã được mã hóa.

Mặc dù người ta có thể sử dụng cấu trúc Mã vạch tiêu chuẩn, như Mã vạch dữ liệu, Mã QR, v.v., các tác giả sáng chế đề xuất việc sử dụng cấu trúc tùy chỉnh và bố trí các từ mã bằng cách sử dụng mã sửa lỗi, ví dụ, Mã hóa Reed-Solomon. Điều này có hiệu quả hơn về không gian và dung lượng dữ liệu, tức là tăng số lượng ảnh có thể. Sở dĩ như vậy là do các cấu trúc mã vạch tiêu chuẩn này sử dụng các cấu trúc hoặc mẫu đặc biệt để mã hóa thông tin phiên bản, các mẫu

Finder để cục bộ hóa và xác định kích thước của mã trong ảnh, v.v.. Các tác giả sáng chế đề xuất một cách để cục bộ hóa và giải mã các cấu trúc đó mà không cần đến các mẫu Finder thường được sử dụng, v.v. sau này trong Bản mô tả này.

Việc sử dụng các lớp nhiễu xạ quang học để hiển thị - tùy thuộc vào góc nhìn - các cấu trúc mã vạch liên kết với nhau, chồng lên nhau về mặt không gian đã được biết đến từ ,ví dụ, US 2012/0211567 A1. US 2012/0211567 A1 đề xuất việc sử dụng một lớp quang học, hoạt động theo cách mà khi được nhìn từ các góc độ khác nhau, các mã vạch khác nhau sẽ được hiển thị. Họ còn đề xuất việc sử dụng một bảng mã để liên kết ít nhất hai mã phụ thuộc vào góc nhìn đó với nhau và xác định thứ tự của chúng. Mục đích chính của sáng chế này dường như là tăng dung lượng lưu trữ dữ liệu, do đó nỗ lực cài đặt các liên kết để tập hợp lại dữ liệu thành một đoạn dữ liệu khi đọc các mã khác nhau.

Các tác giả sáng chế muốn nhấn mạnh rằng trong Bản mô tả sáng chế này, các ảnh/đoạn mã/đoạn dữ liệu phụ thuộc vào góc nhìn là độc lập với nhau. Hơn nữa, sáng chế này - trái ngược với các ứng dụng lưu trữ dữ liệu - được thiết kế để chỉ một phần nhỏ các đoạn dữ liệu từ một tập hợp các đoạn dữ liệu cụ thể cần được giải mã. Thứ tự giải mã là không quan trọng, vì chỉ thành viên của một đoạn dữ liệu được giải mã với một tập hợp các đoạn dữ liệu cụ thể xác định một phần tử bảo mật cụ thể là quan trọng. Cuối cùng, mục đích của sáng chế là xác định vị trí của phần tử bảo mật trong vật liệu cơ bản, bằng cách xác định danh tính của phần tử bảo mật cụ thể thông qua việc giải mã ít nhất một đoạn dữ liệu từ ít nhất một góc nhìn và xác định vị trí bên trong vật liệu cơ bản - tốt hơn là khi giải mã các đoạn mã khác trong các điều kiện chụp ảnh khác nhau và xác định thành viên tập hợp tương ứng của chúng - bằng cách sử dụng kiến thức ưu tiên từ một mô hình, lưu trữ các tập hợp các đoạn dữ liệu xác định các phần tử bảo mật cũng như mối quan hệ hình học của chúng với nhau. Do đó - trái ngược hẳn với , ví dụ, US 2012/0211567 A1 - mối quan hệ giữa các đoạn dữ liệu /đoạn mã khác được xác định thông qua mô hình xác định trước thay vì (vật lý) liên kết mã hóa và thông

tin thứ tự trong chính các đoạn dữ liệu/đoạn mã.

Fig.2 minh họa một phương án được ưu tiên theo sáng chế. Phạm vi ảnh có thể được giới hạn bởi 6x6 pixel, có thể là màu đen hoặc trắng. Vật liệu cơ bản 1 có các phần tử bảo mật 2, được bố trí theo cách có ô. Ví dụ, phần tử bảo mật thứ nhất 3, được xác định là phần tử bảo mật A, được đặt liền kề (hoặc trực tiếp liền kề) với phần tử bảo mật thứ hai 4, được xác định là phần tử bảo mật B. Mỗi phần tử bảo mật 2 có một phần tử thay đổi quang, hiển thị một trong số N ảnh khác nhau khi nhìn từ các góc hoặc điều kiện chiếu sáng khác nhau. Vì vậy, phần tử bảo mật thứ nhất 3, được xác định là phần tử bảo mật A, có thể chuyển giữa N ảnh khác nhau A_1, A_2,… A_N (5) trong tập hợp có 6 ảnh có thể có đối với phần tử bảo mật cụ thể này trong các điều kiện chụp ảnh khác nhau α, β,… ω . Tập hợp thứ hai tương tự có 7 ảnh với các ảnh có sẵn B_1, B_2,… B_N được xác định đối với phần tử bảo mật thứ hai 4.

Điều quan trọng cần đề cập là trong cài đặt thực tế, cần phải cân bằng giữa độ nhạy chuyển, tức là "tốc độ" của hiệu ứng chuyển và độ mạnh cần được thực hiện. Đặc biệt, nếu có ánh sáng khuếch tán hoặc các nguồn sáng giống điểm có cường độ tương tự, có thể xảy ra hiện tượng chồng lên nhau giữa các ảnh, tức là hai hoặc nhiều hơn N ảnh trong tập hợp M ảnh có thể có có thể chồng lên nhau với các cường độ khác nhau. Trong trường hợp này, chức năng sửa lỗi trở nên đặc biệt hữu ích, vì nó cho phép lọc giữa các ảnh chồng lên nhau ở một mức độ nào đó hoặc ít nhất là xác định rằng trong điều kiện hiện tại, ảnh không thể đọc được một cách đáng tin cậy.

Trong một cài đặt thực tế trong quá trình đọc ra, thường có nhiều hơn một nguồn chiếu sáng (ánh sáng) hiện diện. Ví dụ, có thể có một nguồn sáng chuyên dụng được liên kết với thiết bị xác minh có máy ảnh. Khi hoạt động trong điều kiện thực tế, luôn có dư lượng ánh sáng xung quanh nhất định hoặc thậm chí có thể có các nguồn sáng giống điểm (đèn, mặt trời,…) gây nguy hiểm cho nguồn sáng

chuyên dụng. Trong một bối cảnh thực tế khác, có thể không có nguồn sáng chuyên dụng mà là vị trí siêu tập trung của các nguồn sáng "tự nhiên". Hơn nữa, có thể là có lợi nếu trang bị cho thiết bị xác minh có máy ảnh với các nguồn sáng chuyên dụng, có thể bật và tắt từng nguồn một hoặc trong một cài đặt được ưu tiên được bật cùng lúc tạo ra một hỗn hợp các nguồn sáng có hướng nhiều hay ít khác nhau.

Sự chồng lên nhau giữa các ảnh do các nguồn sáng hoặc ánh sáng khuếch tán gây ra có thể được tận dụng trong quá trình đọc ra. Dựa trên thông tin đã biết từ mô hình và sử dụng chức năng sửa lỗi, có thể tách các ảnh chồng lên nhau và giải mã các đoạn mã. Điều này cho phép trong một số trường hợp nhất định, phần tử bảo mật có thể được xác minh từ một ảnh đã được chụp ảnh duy nhất, nếu ảnh xếp chồng có thể được tách thành công thành ít nhất hai đoạn mã khác nhau thuộc tập hợp các đoạn mã có sẵn cho một phần tử bảo mật cụ thể. Một phương pháp rất đơn giản để tách là như sau:

- Từ ảnh xếp chồng, xác định cường độ của đoạn mã chiếm ưu thế trong ảnh xếp chồng (ví dụ, thông qua các trị số của thang độ xám và phân tích biểu đồ)
- Lọc tất cả các cường độ khác để cô lập đoạn mã nổi bật
- Giải mã đoạn mã nổi bật bị cô lập
- Xác định phần tử bảo mật tương ứng và do đó tập hợp các đoạn mã có sẵn đối với phần tử bảo mật cụ thể.
- Tiến hành tương tự với các cường độ có thể khác và cố gắng giải mã.
- Nếu có đoạn mã thứ hai, mà có thể được giải mã và khớp với tập hợp các đoạn mã có sẵn đối với phần tử bảo mật cụ thể, phần tử bảo mật này có thể được coi là hợp lệ và xác thực.

Trong một cài đặt được ưu tiên khác, người ta có thể không cố gắng tìm cường độ của đoạn mã chiếm ưu thế mà chỉ cần lặp lại trên tất cả các cường độ có thể có. Đối với mỗi cường độ, hãy tách riêng một đoạn mã "có thể có". Nếu nó có thể giải mã được, tức là sửa lỗi và phát hiện lỗi thành công, giả sử đây là một đoạn mã

hợp lệ và xác định phần tử bảo mật tương ứng. Sau đó, lặp lại các cường độ có thể còn lại, lọc từng cường độ và cố gắng giải mã các đoạn mã có thể có ở các cường độ đó. Nếu tồn tại ít nhất cường độ thứ hai, trong đó đoạn mã có thể được giải mã và đoạn mã là thành viên của tập hợp các đoạn mã có sẵn của các phần tử bảo mật tương ứng, thì phần tử bảo mật này có thể được coi là xác thực.

Trong mỗi trường hợp đó, tính xác thực của phần tử bảo mật (và do đó ít nhất là một phần của thiết bị bảo mật) có thể được xác minh từ một ảnh đã được chụp ảnh theo điều kiện tiên quyết, rằng môi trường chiếu sáng bao gồm sự chồng phù hợp của các nguồn sáng phù hợp với việc cô lập và lọc các đoạn mã khác nhau.

Trong ví dụ này về 6x6 pixel, số lượng ảnh có thể phân biệt được về mặt lý thuyết là 2 ^ 36. Trong bối cảnh đơn giản, điều này có nghĩa là các tác giả sáng chế có thể mã hóa 2 ^ 36 số nhận dạng khác nhau. Tuy nhiên, trong trường hợp này không có chỗ để sửa lỗi và không thể đảm bảo việc giải mã chính xác. Nếu mã sửa lỗi được sử dụng, các tác giả sáng chế có thể ,ví dụ, sử dụng 12 bit để sửa lỗi và 24 bit làm tải trọng - vì vậy số lượng ảnh có thể phân biệt được có thể giảm xuống còn 2 ^ 24.

Nếu các tác giả sáng chế chọn một số nhỏ, ví dụ, N = 5 ảnh, đối với mỗi tập hợp 6, 7 ảnh đối với phần tử bảo mật thứ nhất 3 và phần tử bảo mật thứ hai 4, điều này cho phép đã "mã hóa" một vùng khá lớn của sản phẩm dạng tấm bằng cách chỉ cần đặt các phần tử bảo mật trong một ô trên sản phẩm dạng tấm. Tuy nhiên, các ứng dụng thực tế đòi hỏi khả năng sửa lỗi thậm chí còn mạnh hơn, đặc biệt là khi điện thoại thông minh hoặc máy tính bảng có chất lượng chụp ảnh kém được sử dụng làm thiết bị lập trình xác minh có máy ảnh. Trong cài đặt có khả năng chịu đựng và dự phòng cao như vậy (ví dụ, tải trọng 16 bit, sửa lỗi 20 bit), một lượng khá lớn dữ liệu "bị phá hủy" (ví dụ, do chất lượng chụp ảnh kém, phân loại và phân loại sai, v.v.) có thể được sửa chữa. Điều này dẫn đến cái giá phải trả là việc đọc sai, tức là giải mã sai số nhận dạng, trở nên có khả năng xảy ra cao hơn

rất nhiều hoặc thậm chí có thể xảy ra.

Khi đó, trong cài đặt xác minh, người ta có thể hưởng lợi từ việc tạo ra mô hình của sản phẩm dạng tấm, tức là tập hợp các ảnh có thể có đối với từng phần tử bảo mật, có sẵn cho thiết bị lập trình xác minh có máy ảnh. Mô hình được biết đến là được ưu tiên, vì nó được coi là bản in màu xanh lam để thiết kế sản phẩm dạng tấm. Mặc dù một lần đọc sai có thể xảy ra trong cài đặt dự phòng cao như đã được mô tả trên đây - phải thừa nhận là đã có xác suất thấp hợp lý - thì rất khó xảy ra, rằng lần giải mã thứ hai dẫn đến lần đọc lại sai và đặc biệt là hai lần đọc sai đó tương ứng với hai ảnh của cùng một tập hợp N = 5 ảnh (trong số, ví dụ, 2 ^ 16 ảnh có sẵn). Vì vậy, việc đọc sai có thể được giảm đến mức tối thiểu hoặc loại bỏ thực tế hơn nữa bằng cách sử dụng hai ảnh từ các góc độ khác nhau của cùng một phần tử bảo mật và kiểm tra xem cả hai số nhận dạng có phải là một phần của tập hợp các ảnh xác định phần tử bảo mật cụ thể này hay không.

Theo cách khác - hoặc ngoài ra - người ta có thể sử dụng mối quan hệ không gian của các phần tử bảo mật khác nhau liên quan đến nhau. Vì vậy, nếu ví dụ, trong phần tử bảo mật thứ nhất (với tập hợp các ảnh có sẵn được mô hình hóa A_1… A_N (6)), một ảnh sai, ví dụ, P_2, được giải mã và trong phần tử bảo mật thứ hai lân cận (với bộ 7: B_1… B_N) - chính xác - B_2 được giải mã, rõ ràng từ mô hình rằng một trong hai phần tử phải là giải mã sai. Nếu vùng thứ nhất 3 ảnh giải mã thành 5 ảnh trong tập hợp 6: A_1… A_N và vùng thứ hai 4 ảnh giải mã thành 5 ảnh trong tập hợp 7: B1… B_N, điều này có thể được giả định là hai lần đọc đúng. Các tác giả sáng chế muốn nhấn mạnh rằng mối quan hệ hình học có trong mô hình này có thể là đặc biệt hữu ích để giảm đến mức tối thiểu khả năng giải mã sai khi sử dụng ảnh không có khả năng phát hiện lỗi/sửa lỗi.

Thông thường,ví dụ, đối với Định dạng mã 2D tiêu chuẩn, các mã nhỏ như 6x6 phần tử không tồn tại - đơn giản vì nguy cơ giải mã sai với tải trọng ngắn như vậy thường quá cao để phù hợp với các ứng dụng thực tế. Tuy nhiên và tương tự như

nêu trên, sáng chế cho phép sử dụng các mã nhỏ như vậy trong cài đặt đọc thực tế không có lỗi, bằng cách khai thác mối quan hệ góc và/hoặc không gian của ảnh. Điều này có thể được thực hiện bằng cách tăng độ chính xác giải mã bằng cách sử dụng kiến thức tiên nghiệm có sẵn từ mô hình xác định trước của sản phẩm dạng tấm trong thiết bị lập trình có máy ảnh. Lợi ích của việc sử dụng các mã nhỏ như vậy trên các kích thước mã phù hợp hơn (ví dụ, 10x10 và cao hơn) là các thiết bị bảo mật, cần chứa ít nhất một phần tử bảo mật, có thể trở nên nhỏ hơn và thực tế vẫn được giải mã không có lỗi.

Trong một cài đặt như vậy, cụ thể là sử dụng việc giải mã của ít nhất hai phần tử bảo mật và sử dụng mô hình làm bằng vật liệu cơ bản để xác thực giải mã chính xác, thực tế không thể xảy ra giải mã sai.

Có một cách thực tế không có lỗi để giải mã ảnh hoặc đúng hơn là xác định tập hợp ảnh thích hợp có thể cho phép hai cài đặt có lợi:
- Các phần tử bảo mật được đặc trưng bởi tập hợp các ảnh có thể có của chúng có thể hoạt động như các định danh (duy nhất hoặc gần như duy nhất) được quy cho một vị trí tuyệt đối trong vật liệu cơ bản. Điều quan trọng cần lưu ý là không phải tất cả N ảnh đều cần được giải mã để xác định một tập hợp các ảnh có thể có và xác định phần tử bảo mật tương ứng. Ví dụ, sẽ là đủ nếu hai ảnh từ các góc khác nhau được giải mã và một tập hợp chứa hai ảnh đó có thể được xác định từ mô hình có sẵn của sản phẩm dạng tấm. Vì các tập hợp được tạo cấu trúc theo cách sao cho không tập hợp nào có thể chứa cùng một cặp ảnh hơn bất kỳ tập hợp nào khác/để một cặp ảnh là duy nhất trên tất cả các tập hợp trong vật liệu cơ bản theo phương án giả định này.

- Mã hóa trong các phần tử bảo mật không cần cấu trúc thông thường Mã 2D như mẫu Finder, mẫu tần số hoặc bất kỳ biện pháp phân đoạn/cục bộ hóa nào khác. Các phần tử bảo mật có thể được đặt cạnh nhau theo cách có ô mà không có bất kỳ chỉ báo nào về nơi một phần tử bảo mật kết thúc và phần tiếp theo bắt đầu.

Tính đặc hiệu cao (khả năng đọc sai thấp) cho phép trượt từng pixel cửa sổ trên ảnh hiện đang được hiển thị. Mỗi vị trí có thể được giải mã. Nếu nó có thể được giải mã (tức là một số nhận dạng được trích xuất), thì tất cả các bộ có thể chứa ảnh/số nhận dạng cụ thể này đều được xác định trước từ mô hình. Ở bước thứ hai, một ảnh khác về mặt không gian hoặc góc sẽ được giải mã. Trong trường hợp có một ảnh khác một góc (tức là từ một ảnh đã được chụp ảnh thứ hai), tất cả các tập hợp xác định trước sẽ được tìm kiếm cho số nhận dạng đã được giải mã thứ hai. Tất cả các bộ không chứa ảnh thứ hai này, mã định danh này không còn là ứng viên. Bằng cách thực hiện lặp đi lặp lại việc này, sẽ chỉ còn lại một tập hợp - xác định phần tử bảo mật và đồng thời cho phép xác định ranh giới của phần tử bảo mật đó cho các lần đọc tiếp theo trong các ảnh đã được chụp ảnh khác. Trong trường hợp sử dụng ảnh khác về không gian, có thể sử dụng cùng một ảnh đã được chụp ảnh. Giả sử mã 6x6: Đối với mỗi vị trí ứng viên, nơi mã nhận dạng có thể được giải mã, thiết bị lập trình có máy ảnh cũng được tạo cấu hình để thử giải mã các vùng 6x6 liền kề. Nếu bất kỳ vùng nào trong số đó có thể giải mã được, thì tất cả các nhóm có thể có cho vùng này sẽ được xác định, để lại cho các tác giả sáng chế một tập hợp các phần tử bảo mật có thể nhận dạng được. Bằng cách sử dụng mối quan hệ không gian của hai phần tử bảo mật đã được quan sát với nhau và so khớp nó với mối quan hệ của các bộ định danh với mô hình được xác định trước, người ta có thể tìm thấy sự kết hợp phù hợp (ví dụ, một cặp bộ liền kề) và một lần nữa đã xác định được hai phần tử bảo mật liền kề cũng như ranh giới của các phần tử bảo mật này - vì chúng được bố trí theo cách có ô. Đương nhiên, nếu việc mã hóa cho phép, các bit không sử dụng có thể được đặt thành một mẫu bit cụ thể, có thể được sử dụng để thiết kế phỏng đoán và tăng tốc quá trình tìm kiếm các vùng có thể giải mã, tức là các vị trí và ranh giới của phần tử bảo mật.

Sáng chế không giới hạn ở kích thước ảnh tương đối nhỏ, tức là 6x6 pixel. Các chiến lược nhận dạng nêu trên có thể là không cần thiết đối với ảnh lớn hơn, vì mã sửa lỗi đủ cụ thể để ngăn chặn việc đọc sai ngay từ đầu từ một kích thước nhất định, tức là số bit, trở đi. Trong trường hợp các mã lớn hơn với nhiều dung lượng

hơn, người ta có thể không cần các chiến lược bổ sung bằng cách sử dụng kiến thức tiên nghiệm từ mô hình được xác định trước để tránh giải mã sai. Trong cài đặt như vậy với các mã lớn hơn, có thể mã hóa sản phẩm dạng tấm theo cách để mỗi số nhận dạng xuất hiện chính xác một lần hoặc không xảy ra hai lần trong một vùng lân cận cục bộ nhất định - với điều kiện các cặp mã liền kề được sử dụng để xác định một vị trí trong vật liệu cơ bản. Vì vậy, do tính đặc hiệu cao/ việc giải mã thực tế ít lỗi được cung cấp bởi các mã có dung lượng/kích thước hợp lý lớn và thực tế là mỗi số nhận dạng có thể có ở mức tối đa. Một tập hợp các ảnh có thể có, một việc giải mã thành công là đủ để xác định ranh giới của các phần tử bảo mật cũng như xác định một phần tử bảo mật cụ thể (và do đó biết được vị trí tuyệt đối chính xác trong sản phẩm dạng tấm).

Một mục đích chính, tại sao các thiết bị lập trình được có máy ảnh được sử dụng với các thiết bị thay đổi quang là nhằm cung cấp một cách tự động để xác minh sự có mặt của chúng và do đó tính xác thực. Nếu không có bất kỳ thiết bị bổ sung nào ngoài máy ảnh, điều này thường đạt được nhờ phương tiện thị giác máy tính và một chương trình máy tính được tạo cấu hình để đánh giá các ảnh, tức là một dòng video, được chụp ảnh từ các góc độ và/hoặc điều kiện ánh sáng khác nhau. Theo cách khác, có thể xử lý các ảnh đã được chụp ảnh đồng thời từ nhiều máy ảnh. Giải pháp kỹ thuật đã biết ở đây là để đánh giá sự thay đổi màu sắc (thiết bị nhiễu xạ bậc không/bậc một) hoặc các hiệu ứng hoạt hình nhất định của ảnh hoặc hình dạng, độ tương phản chuyển, v.v.. Do môi trường không được kiểm soát, sự đánh đổi giữa tính bảo mật và độ mạnh / khả năng đọc là đáng kể, tức là chỉ có thể đạt được tính đặc hiệu vừa phải - do đó tính bảo mật - có thể đạt được. Thông thường, dòng đánh giá thứ hai với thiết bị pháp y hoặc thiết bị đọc chuyên dụng đánh giá cấu trúc vật lý của OVD thay vì các đặc tính phản xạ, được sử dụng trong quá trình xác thực, nếu lo ngại về tính bảo mật cao.

Đồng thời, các ứng dụng sử dụng thiết bị tiêu chuẩn như thiết bị lập trình được có máy ảnh thường nhắm mục đích để cho phép người dùng chưa được đào tạo xác

minh tính xác thực của thiết bị bảo mật, nếu người dùng mong đợi một quy trình xác thực thuận tiện (do đó mạnh). Do đó, OVD hoặc thậm chí sự có mặt của OVD tốt nhất là có thể được đánh giá một cách đại khái. Ví dụ, trong bối cảnh OVD thay đổi màu, điều này có nghĩa là việc chấp nhận thay đổi màu "bất kỳ" thường là cách để xác thực ít nhất sự có mặt của OVD. Việc xác thực sự có mặt của OVD thường là cần thiết để phân biệt giữa OVD 3 chiều tạo ra thiết bị bảo mật và bản sao hình ảnh/ảnh của nó. Thường xuyên hơn không, những thay đổi bất lợi trong ánh sáng hoặc chụp ảnh đồ giả tạo ra nhiều biến thể hơn về sự thay đổi màu sắc, độ mờ, v.v. đối với ảnh đã được chụp ảnh của một bản sao in của OVD ("bản sao ảnh") so với OVD gốc sẽ thể hiện trong các điều kiện chụp ảnh không thuận lợi thuộc một loại khác, ví dụ, ánh sáng khuếch tán. Do đó, các ngưỡng quyết định về việc phát hiện sự có mặt của OVD nhị phân (có / không) thường gần đến một điểm, nơi bản sao in được chấp nhận là OVD trong các điều kiện nhất định, trong khi OVD thực bị từ chối do thiếu phương sai đáng kể (ví dụ, chỉ có sự thay đổi nhỏ màu) trong các ảnh đã được chụp ảnh.

Một mục đích của sáng chế cũng là đề xuất cách xác thực rất đáng tin cậy sự có mặt của thiết bị thay đổi quang học. Bằng cách chụp ảnh ít nhất hai ảnh từ các góc độ/cài đặt chiếu sáng khác nhau và giải mã ít nhất hai ảnh cho cùng một phần tử bảo mật - tất nhiên cần phải có trong tập hợp các ảnh có thể có đối với phần tử bảo mật cụ thể đó - kết hợp với việc sửa lỗi gần như chắc chắn rằng có OVD, vì bản sao ảnh hoặc bản in không thể thể hiện hành vi chuyển ảnh này. Hơn nữa, việc chuyển mã được sửa lỗi thông qua việc mã hóa các dấu - có nghĩa là nếu quan sát thấy sự thay đổi trong ảnh, cơ hội xảy ra lỗi là không thể bỏ qua.

Fig. 3a-c liên quan đến phương pháp xác thực dấu của đối tượng được làm bằng vật liệu cơ bản 1 theo Fig.2. Trong ví dụ này, dấu của đối tượng có một phần làm bằng vật liệu cơ bản 1, trong đó phần được bao phủ một phần bởi một lớp che. Các phần tử bảo mật 2 làm bằng vật liệu cơ bản 1 được bố trí theo cách có ô. Mỗi đoạn mã được hiển thị bởi các phần tử bảo mật là một mảng (hình vuông, một

màu). Các đoạn mã được hiển thị bởi một phần tử bảo mật được bố trí lan sang các đoạn mã được hiển thị bởi các phần tử bảo mật khác, sao cho tổng thể một mảng lớn hơn có các ô (hình vuông, một màu) được tạo ra. Lớp che dành cho vùng được phân định rõ ràng bằng cách quang điện tử làm bằng vật liệu cơ bản 1. Vùng này có phần tử bảo mật thứ nhất 3 và phần tử bảo mật thứ hai 4.

Phương pháp xác thực dấu của đối tượng này bao gồm bước chụp ảnh thứ nhất 12 dấu của đối tượng từ góc thứ nhất hoặc dưới hướng chiếu sáng thứ nhất. Ảnh thứ nhất 12 được thể hiện trên Fig.3a mô tả hình dạng trực quan của vùng được phân định rõ ràng bằng cách quang điện tử trong các điều kiện chụp ảnh thứ nhất (ví dụ, góc nhìn thứ nhất). Phương pháp này bao gồm bước xác định đoạn mã 13 của mẫu thứ nhất được hiển thị bởi phần tử bảo mật thứ nhất giả định trong ảnh 12 thứ nhất (trong đó "mẫu" biểu thị rằng đây là ứng viên cho đoạn mã thứ nhất). Nhằm mục đích xác định đoạn mã thứ nhất thực tế, đoạn mã 13 của mẫu thứ nhất được giải mã để thu được đoạn dữ liệu 15 của mẫu thứ nhất. Chi tiết hơn, ô 11 của mẫu thứ nhất được xác định trong ảnh thứ nhất 12 ở bước a). Sau đó, đoạn mã 13 của mẫu thứ nhất trong ảnh thứ nhất 12 đã được tạo ra bởi một mảng của mẫu thứ nhất có ô 14 có ô 11 của mẫu thứ nhất ở một vị trí xác định trước được giải mã ở bước b) để thu được đoạn dữ liệu 15 của mẫu thứ nhất. Dựa trên đoạn dữ liệu 15 của mẫu thứ nhất này, xác định xem ở bước c) từ mô hình 16 lưu trữ các tập hợp các đoạn dữ liệu được liên kết với các phần tử bảo mật làm bằng vật liệu cơ bản 1, cho dù có ít nhất một tập hợp các đoạn dữ liệu 6 chứa đoạn dữ liệu 15 của mẫu thứ nhất nêu trên (tức là ứng viên của đoạn dữ liệu này) hay không. Nếu không xác định được tập hợp nào như vậy ở bước c), ứng viên của đoạn dữ liệu này sẽ bị từ chối và các bước từ a) đến c) được lặp lại với các ô khác của mẫu thứ nhất cho đến khi tìm thấy tập hợp như vậy ở bước c). Ví dụ, ô tiếp theo ở bên phải của ô 11 của mẫu thứ nhất có thể được xác định là "ô của mẫu thứ nhất" mới và các bước nêu trên được lặp lại. Điều này có thể được lặp lại cho đến khi một số bước tương ứng với chiều rộng được xác định trước (đã biết) của các phần tử bảo mật có các ô (ở đây chiều rộng là sáu ô) được bao phủ và khi đó ô ngay bên dưới ô

ban đầu 11 của mẫu thứ nhất có thể được xác định là "ô của mẫu thứ nhất" mới và các bước nêu trên được lặp lại, v.v.. Ngay khi có thể tìm thấy ít nhất một tập hợp đoạn dữ liệu 6 chứa đoạn dữ liệu 15 của mẫu thứ nhất (tức là ứng viên của đoạn dữ liệu), ví dụ, trên Fig.3a tập hợp A chứa A_1, đoạn mã của mẫu thứ nhất hiện tại 13 - được xác định sơ bộ - được xác định là đoạn mã thứ nhất.

Không theo trình tự hoặc thứ tự cụ thể nào, phương pháp này cũng bao gồm bước chụp ảnh thứ hai 17 dấu của đối tượng trong các điều kiện chụp ảnh khác nhau (ví dụ, từ góc thứ hai và/hoặc dưới hướng chiếu sáng thứ hai). Điều này được minh họa trên fig.3b. Đoạn mã thứ hai được hiển thị bởi phần tử bảo mật thứ nhất được xác định trong ảnh thứ hai 17. Nhằm mục đích xác định đoạn mã thứ hai, đoạn mã của mẫu thứ hai 18 đã được giải mã để thu được đoạn dữ liệu 19 của mẫu thứ hai. Đoạn mã này có thể hoạt động tương tự như đối với đoạn dữ liệu thứ nhất. Tức là, ở bước e) ô 11 của mẫu thứ nhất được xác định trong ảnh thứ hai 17 (nói chung là tùy ý, ví dụ, ô gần nhất với góc trên cùng bên trái của ảnh thứ hai 17); ở bước f) đoạn mã 18 của mẫu thứ hai trên ảnh thứ hai 17 đã được tạo ra bởi mảng của mẫu thứ nhất có các ô 14 được giải mã để thu được đoạn dữ liệu 19 của mẫu thứ hai; ở bước g) từ mô hình 16 xác định xem liệu ít nhất một trong số các tập hợp của mô hình 16 chứa đoạn dữ liệu 15 của mẫu thứ nhất cũng chứa đoạn dữ liệu 19 của mẫu thứ hai hay không; nếu không xác định được tập hợp nào như vậy ở bước g), thì bước h) chỉ ra một vòng lặp và các bước từ a) đến g) được lặp lại cho đến khi tìm thấy tập hợp 6 như vậy ở bước g). Điều đó có nghĩa là đoạn mã của mẫu thứ nhất bị từ chối nếu không thể xác định được đoạn mã của mẫu thứ hai phù hợp, như vậy cả hai đoạn mã của mẫu đều bị loại bỏ, quét các vị trí và ranh giới ô khác cho đến khi tìm thấy sự kết hợp hợp lệ của các đoạn mã của mẫu. Mặt khác, khi một tập hợp có cả hai đoạn dữ liệu của mẫu được tìm thấy, thì đoạn mã 18 của mẫu thứ hai hiện tại được xác định là đoạn mã thứ hai ở bước m). Tức là, phương pháp xác định từ mô hình 16 lưu trữ tập hợp các đoạn dữ liệu được liên kết với các phần tử bảo mật làm bằng vật liệu cơ bản 1 có tập hợp các đoạn dữ liệu chứa đoạn dữ liệu 15 của mẫu thứ nhất và đoạn dữ liệu 19 của mẫu

thứ hai. Chỉ khi khẳng định, tức là nếu tập hợp 6 đoạn dữ liệu như vậy là một phần của mô hình 16, thì dấu của đối tượng có thể được xác định là xác thực hay không.

Ngoài ra, như được minh họa trên Fig.3c, phương pháp này bao gồm bước xác định đoạn mã của mẫu thứ ba được hiển thị bởi phần tử bảo mật thứ hai giả định trong ảnh thứ nhất 12 (nhưng tương tự có thể sử dụng ảnh thứ hai 17 hoặc cả hai). Đoạn mã thứ ba đã xác định được giải mã để thu được đoạn dữ liệu của mẫu thứ ba. Dựa trên đoạn dữ liệu của mẫu thứ ba đã được giải mã, từ mô hình này xác định xem liệu có phần tử bảo mật thứ hai được định vị liên quan đến phần tử bảo mật thứ nhất (như được xác định bởi các đoạn dữ liệu của mẫu thứ nhất và thứ hai) mà được liên kết với tập hợp dữ liệu chứa đoạn dữ liệu của mẫu thứ ba hay không. Do đó, mô hình 16 không chỉ lưu trữ các tập hợp các đoạn dữ liệu được liên kết với các phần tử bảo mật làm bằng vật liệu cơ bản, mà còn cả vị trí tương đối của các phần tử bảo mật làm bằng vật liệu cơ bản với nhau. Do đó, trước khi xác nhận tính xác thực dấu của đối tượng, phương pháp này bao gồm các bước: giải mã đoạn mã của mẫu thứ ba 20 đã được tạo ra bởi một mảng của mẫu thứ hai của ô 21 được định vị tương đối với mảng của mẫu thứ nhất của ô 14 ở bước i), để thu được một đoạn dữ liệu thứ ba 22 của mẫu, xác định ở bước j) từ mô hình 16 có các tập hợp 6, 7 của các đoạn dữ liệu được liên kết với các phần tử bảo mật 2 làm bằng vật liệu cơ bản 1 và vị trí tương đối của các phần tử bảo mật 2 làm bằng vật liệu cơ bản 1 đến một đoạn khác 23 , xem liệu đoạn dữ liệu 22 của mẫu thứ ba có nằm trong tập hợp 7 đoạn dữ liệu, có thuộc về phần tử bảo mật 4 được định vị tương đối với phần tử bảo mật 3 hay không mà tập hợp được xác định sơ bộ bằng cách tìm kiếm một tập hợp với phần tử thứ nhất và thứ hai đoạn dữ liệu của mẫu thuộc về; nếu không xác định được tập hợp nào như vậy, quay lại bước k) và lặp lại các bước từ a) đến j), cho đến khi tìm được tập hợp đó; và khi tập hợp được tìm thấy, xác định các đoạn mã 13, 18, 20 của mẫu hiện tại là các đoạn mã hợp lệ ở bước n). Do đó, mô hình 16 chứa thông tin, tập hợp các đoạn dữ liệu nào được liên kết với các thiết bị bảo mật liền kề trên vật liệu cơ bản 1.

Tóm lại, phương pháp đã được mô tả trên đây về cơ bản quét (ít nhất) hai ảnh 12, 17 của các mảng ô bắt đầu từ một ô tùy ý và chọn một ô khác mỗi lượt cho đến khi các đoạn dữ liệu được đại diện bởi các đoạn mã lệch khỏi ô nhất định và việc bố trí tương ứng chúng tạo ra một kết quả phù hợp ở mô hình 16. Nếu không tìm thấy sự phù hợp nào như vậy, dấu của đối tượng sẽ bị từ chối (tức là không thể xác nhận tính xác thực).

YÊU CẦU BẢO HỘ

1. Dấu của đối tượng có một số lượng các phần tử bảo mật bao gồm phần tử bảo mật thứ nhất và ít nhất là phần tử bảo mật thứ hai, trong đó mỗi phần tử trong số một số lượng các phần tử bảo mật này được liên kết với một tập hợp các đoạn dữ liệu và mỗi phần tử trong số một số lượng các phần tử bảo mật này hiển thị tuỳ thuộc vào các điều kiện chụp ảnh bao gồm góc nhìn và/hoặc hướng chiếu sáng, đoạn mã mà là một biểu diễn quang điện tử của một trong số các đoạn dữ liệu của tập hợp được liên kết với phần tử bảo mật tương ứng,
đặc trưng ở chỗ,
các đoạn dữ liệu riêng biệt khác được đại diện bởi các đoạn mã khác và tập hợp được liên kết với phần tử bảo mật thứ nhất và tập hợp được liên kết với phần tử bảo mật thứ hai khác ở ít nhất một đoạn dữ liệu.

2. Dấu của đối tượng theo điểm 1, đặc trưng ở chỗ, đối với một hướng chiếu sáng cố định, mỗi đoạn dữ liệu trong tập hợp được liên kết với phần tử bảo mật được liên kết với một vùng góc nhìn riêng biệt, trong đó độ tương phản của đoạn mã đại diện cho đoạn dữ liệu tương ứng cao hơn độ tương phản của các đoạn mã đại diện cho tất cả các đoạn dữ liệu khác từ cùng một tập hợp.

3. Dấu của đối tượng theo điểm 2, đặc trưng ở chỗ, có ít nhất một vùng góc nhìn được liên kết với mlột đoạn dữ liệu của tập hợp phần tử bảo mật thứ nhất, khác với từng vùng góc nhìn được liên kết với các đoạn dữ liệu của tập hợp phần tử bảo mật thứ hai.

4. Dấu của đối tượng theo điểm bất kỳ trong số các điểm từ 1 đến 3, đặc trưng ở chỗ mọi đoạn mã đại diện cho đoạn dữ liệu tương ứng trong việc mã hóa được xác định trước, trong đó việc mã hóa được xác định trước đưa ra số lượng tối đa các đoạn dữ liệu mà có thể xác định được bởi việc mã hóa và số lượng đoạn dữ liệu

trong tập hợp của mỗi phần tử trong số một số lượng các phần tử bảo mật này nhỏ hơn 1/100 số lương tối đa.

5. Tập hợp các dấu của đối tượng được đặc trưng bởi việc bao gồm số lượng dấu của đối tượng theo điểm bất kỳ trong số các điểm từ 1 đến 4.

6. Vật liệu cơ bản bao gồm một số lượng các phần tử bảo mật, mà từ đó dấu của đối tượng có thể được tạo bằng cách phân định một khu vực cụ thể sao cho khu vực cụ thể này có thể được đọc và phân biệt bằng quang điện tử với các khu vực khác của vật liệu cơ bản, khu vực cụ thể này bao gồm phần tử bảo mật thứ nhất và ít nhất là phần tử bảo mật thứ hai, trong đó mỗi phần tử trong số một số lượng các phần tử bảo mật này được liên kết với một tập hợp các đoạn dữ liệu và mỗi phần tử trong số một số lượng các phần tử bảo mật này hiển thị tuỳ thuộc vào các điều kiện chụp ảnh bao gồm góc nhìn và/hoặc hướng chiếu sáng, đoạn mã là là một biểu diễn quang điện tử đọc được của một đoạn dữ liệu trong số các đoạn dữ liệu của tập hợp được liên kết với mỗi phần tử trong số một số lượng các phần tử bảo mật này,
đặc trưng ở chỗ
các đoạn dữ liệu riêng biệt khác được đại diện bởi các đoạn mã khác và tập hợp được liên kết với phần tử bảo mật thứ nhất và tập hợp được liên kết với phần tử bảo mật thứ hai khác ở ít nhất một đoạn dữ liệu.

7. Vật liệu cơ bản theo điểm 6, đặc trưng ở chỗ vị trí của mỗi phần tử trong số một số lượng các phần tử bảo mật này trên vật liệu cơ bản được xác định trước tương đối với nhau theo một mô hình và các đoạn dữ liệu của các tập hợp được liên kết với mỗi phần tử trong số một số lượng các phần tử bảo mật này được xác định trước theo mô hình này.

8. Vật liệu cơ bản theo điểm 6 hoặc 7, đặc trưng ở chỗ mọi đoạn mã đại diện cho đoạn dữ liệu tương ứng trong việc mã hóa được xác định trước, trong đó việc mã hóa được xác định trước chứa thông tin để phát hiện lỗi hoặc sửa lỗi.

9. Vật liệu cơ bản theo điểm 8, đặc trưng ở chỗ việc mã hóa được xác định trước đưa ra số lượng tối đa các đoạn dữ liệu mà có thể xác định được bởi việc mã hóa và số lượng các đoạn dữ liệu riêng biệt trong tập hợp các đoạn dữ liệu của tất cả các phần tử bảo mật nhỏ hơn 1/100 số lương tối đa.

10. Phương pháp xác thực dấu của đối tượng có một khu vực cụ thể của vật liệu cơ bản, theo điểm bất kỳ trong số các điểm từ 6 đến 9, mà có thể phân biệt được với các vùng khác và đọc được bằng quang điện tử,
trong đó khu vực cụ thể này bao gồm phần tử bảo mật thứ nhất và ít nhất là phần tử bảo mật thứ hai trong số một số lượng các phần tử bảo mật, trong đó phương pháp này bao gồm các bước:
chụp ảnh thứ nhất dấu của đối tượng từ góc thứ nhất hoặc dưới hướng chiếu sáng thứ nhất;
xác định đoạn mã thứ nhất được hiển thị bởi phần tử bảo mật thứ nhất trong ảnh thứ nhất;
giải mã đoạn mã thứ nhất để thu được đoạn dữ liệu thứ nhất;
chụp ảnh thứ hai dấu của đối tượng từ góc thứ hai và/hoặc dưới hướng chiếu sáng thứ hai;
xác định đoạn mã thứ hai được hiển thị bởi phần tử bảo mật thứ nhất trong ảnh thứ hai;
giải mã đoạn mã thứ hai để thu được đoạn mã thứ hai;
xác định từ mô hình lưu trữ các tập hợp đoạn dữ liệu liên kết với mỗi phần tử trong số một số lượng các phần tử bảo mật của vật liệu cơ bản xem liệu có một tập hợp các đoạn dữ liệu chứa đoạn dữ liệu thứ nhất và đoạn mã thứ hai hay không.

11. Phương pháp theo điểm 10, đặc trưng ở chỗ, phương pháp này còn bao gồm các bước:
xác định đoạn mã thứ ba được hiển thị bởi phần tử bảo mật thứ hai trong ảnh thứ nhất hoặc trong ảnh thứ hai;
giải mã đoạn mã thứ ba để thu được đoạn dữ liệu thứ ba;
xác định từ mô hình lưu trữ các tập hợp đoạn dữ liệu liên kết với mỗi phần tử trong số một số lượng các phần tử bảo mật này của vật liệu cơ bản và lưu trữ vị trí tương đối của mỗi phần tử trong số một số lượng các phần tử bảo mật này của vật liệu cơ bản với nhau xem liệu phần tử bảo mật thứ hai được định vị tương đối với phần tử bảo mật thứ nhất được liên kết với một tập hợp các đoạn dữ liệu chứa đoạn dữ liệu thứ ba hay không.

12. Phương pháp theo điểm 10 hoặc 11, trong đó các phần tử bảo mật của vật liệu cơ bản được bố trí theo cách có ô và mỗi đoạn mã được hiển thị bởi một số lượng các phần tử bảo mật là một mảng ô và các đoạn mã được hiển thị bởi một phần tử bảo mật được bố trí lan sang các đoạn mã được hiển thị bởi các phần tử bảo mật khác, đặc trưng ở chỗ, phương pháp này còn bao gồm các bước:
a) xác định ô của mẫu thứ nhất trong ảnh thứ nhất;
b) giải mã đoạn mã của mẫu thứ nhất trong ảnh thứ nhất đã được tạo ra bởi một mảng ô của mẫu thứ nhất có ô của mẫu thứ nhất ở một vị trí được xác định trước, để thu được đoạn dữ liệu của mẫu thứ nhất;
c) xác định từ mô hình lưu trữ các tập hợp đoạn dữ liệu liên kết với một số lượng các phần tử bảo mật của vật liệu cơ bản xem liệu có ít nhất một tập hợp các đoạn dữ liệu chứa đoạn dữ liệu của mẫu thứ nhất nêu trên hay không;
d) nếu không xác định được tập hợp nào như vậy ở bước c), lặp lại các bước từ a) đến c) với các ô khác của mẫu thứ nhất cho đến khi tìm thấy tập hợp đó ở bước c); và
l) xác định đoạn mã của mẫu thứ nhất hiện tại là đoạn mã thứ nhất.

13. Phương pháp theo điểm 12, đặc trưng ở chỗ, phương pháp này còn bao gồm các bước sau trước bước l):

e) xác định ô của mẫu thứ nhất trong ảnh thứ hai;

f) giải mã đoạn mã của mẫu thứ hai trong ảnh thứ hai đã được tạo ra bởi mảng ô của mẫu thứ nhất, để thu được đoạn dữ liệu của mẫu thứ hai;

g) xác định từ mô hình lưu trữ các tập hợp đoạn dữ liệu liên kết với một số lượng các phần tử bảo mật của vật liệu cơ bản, xem liệu ít nhất một tập hợp trong số ít nhất một tập hợp chứa đoạn dữ liệu của mẫu thứ nhất có chứa đoạn dữ liệu của mẫu thứ hai hay không;

h) nếu không xác định được tập hợp nào như vậy ở bước g), lặp lại các bước từ a) đến g) cho đến khi tìm thấy tập hợp đó ở bước g); và

m) xác định đoạn mã của mẫu thứ hai hiện tại là đoạn mã thứ hai.

14. Phương pháp theo điểm 13, đặc trưng ở chỗ, phương pháp này còn bao gồm các bước sau trước bước l):

i) giải mã đoạn mã của mẫu thứ ba đã được tạo ra bởi mảng ô của mẫu thứ hai được định vị tương đối với mảng ô của mẫu thứ nhất, để thu được đoạn dữ liệu của mẫu thứ ba;

j) xác định từ mô hình lưu trữ các tập hợp đoạn dữ liệu liên kết với một số lượng các phần tử bảo mật của vật liệu cơ bản và lưu trữ vị trí tương đối của một số lượng các phần tử bảo mật của vật liệu cơ bản với nhau, xem liệu đoạn dữ liệu của mẫu thứ ba có nằm trong trong tập hợp các đoạn dữ liệu thuộc phần tử bảo mật được định vị tương đối với phần tử bảo mật mà tập hợp được xác định sơ bộ ở bước e) thuộc về hay không;

k) nếu không xác định được tập hợp nào như vậy ở bước j), lặp lại các bước từ a) đến d) và các bước từ e) đến j), cho đến khi tìm thấy tập hợp đó ở bước j);

n) xác định đoạn mã của mẫu thứ ba hiện tại là đoạn mã thứ ba.

15. Phương pháp tạo ra dấu của đối tượng, bao gồm các bước:

ngẫu nhiên, giả ngẫu nhiên hoặc chọn theo cách xác định một vùng làm bằng vật liệu cơ bản bao gồm một số lượng các phần tử bảo mật, vùng này có ít nhất hai phần tử bảo mật trong số một số lượng các phần tử bảo mật và

phân định vùng đã được chọn từ phần không được chọn của vật liệu cơ bản sao cho vùng đã được chọn có thể được đọc và phân biệt bằng quang điện tử với phần không được chọn của vật liệu cơ bản,

trong đó mỗi phần tử trong số một số lượng các phần tử bảo mật này được liên kết với một tập hợp các đoạn dữ liệu và mỗi phần tử trong số một số lượng các phần tử bảo mật này hiển thị tuỳ thuộc vào các điều kiện chụp ảnh bao gồm góc nhìn và/hoặc hướng chiếu sáng, đoạn mã là là một biểu diễn quang điện tử đọc được của một trong số các đoạn dữ liệu của tập hợp được liên kết với phần tử bảo mật tương ứng,

đặc trưng ở chỗ

các đoạn dữ liệu riêng biệt khác được đại diện bởi các đoạn mã khác và đối với mỗi cặp phần tử bảo mật được tạo ra từ ít nhất hai phần tử bảo mật trong số một số lượng các phần tử bảo mật, tập hợp được liên kết với một phần tử bảo mật của cặp này và tập hợp được liên kết với phần tử bảo mật kia của cặp này khác ở ít nhất một đoạn dữ liệu.

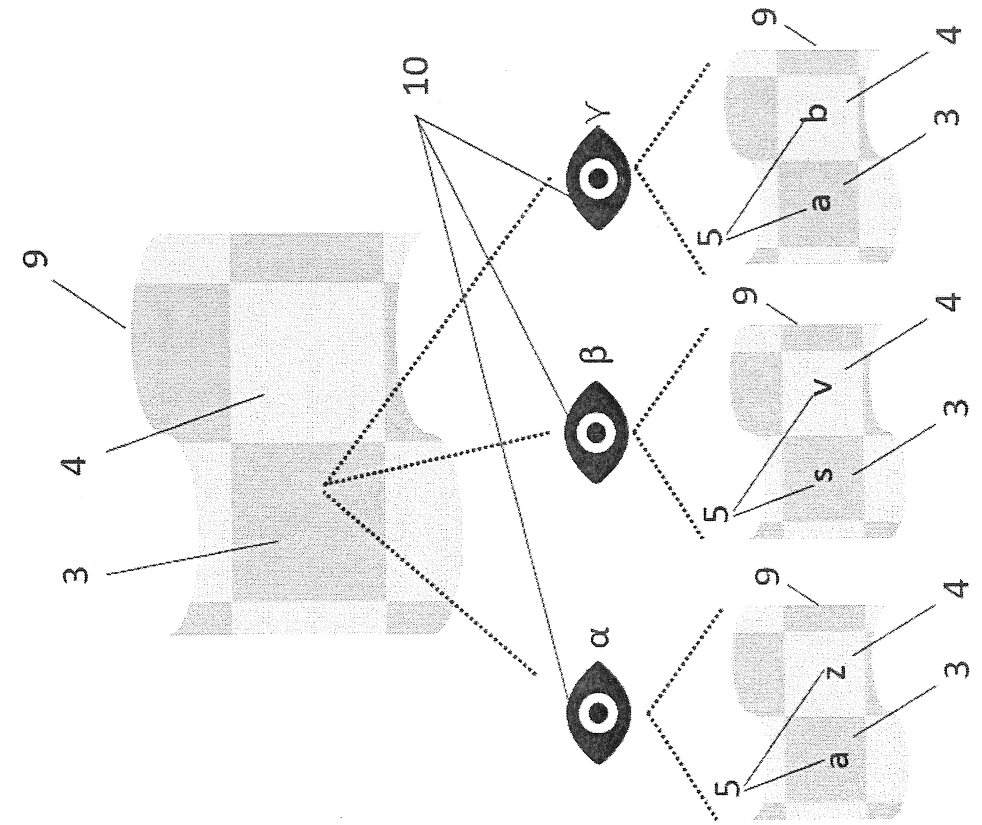


FIG 1b

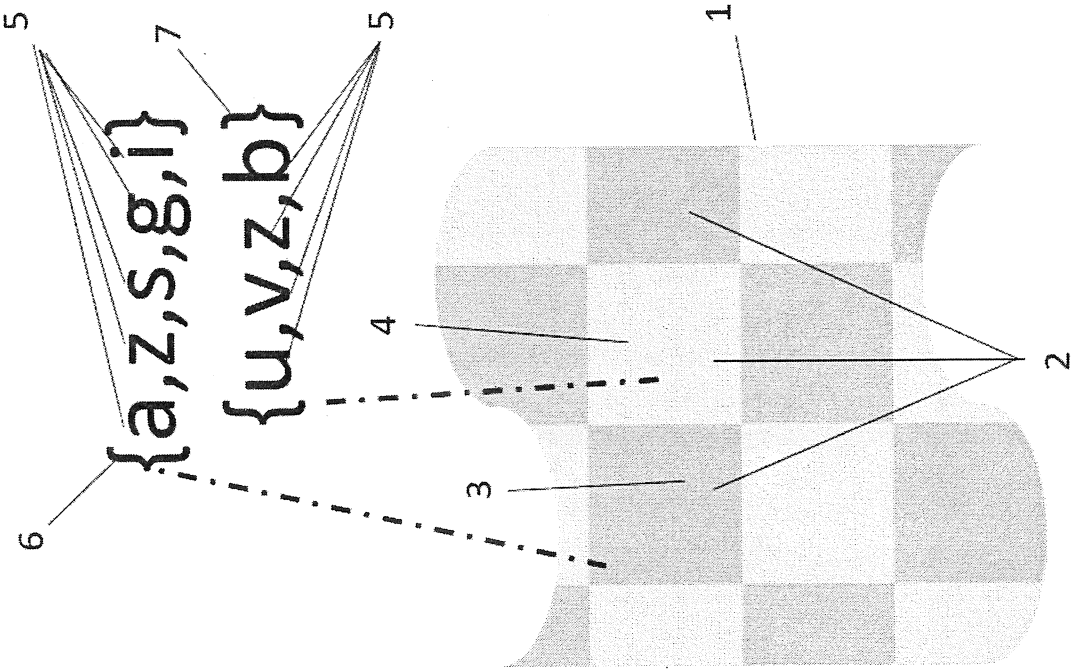
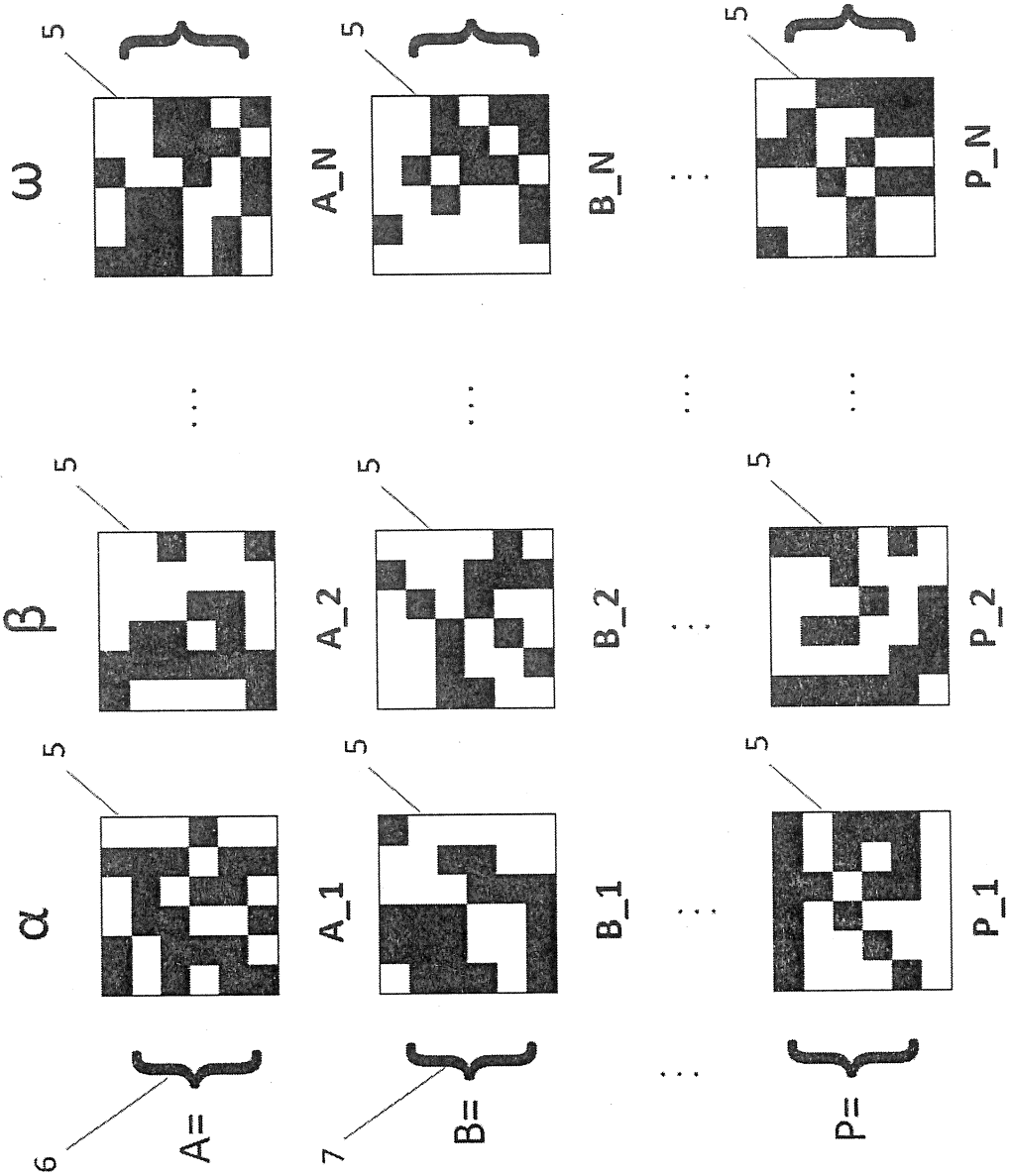


FIG 1a



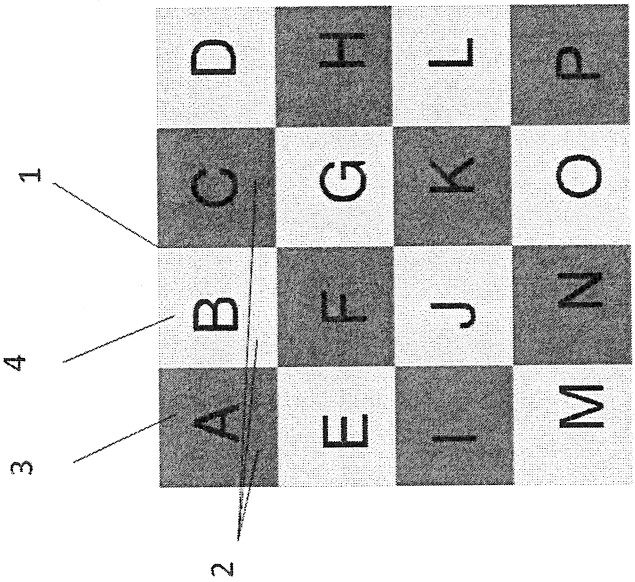


FIG 2

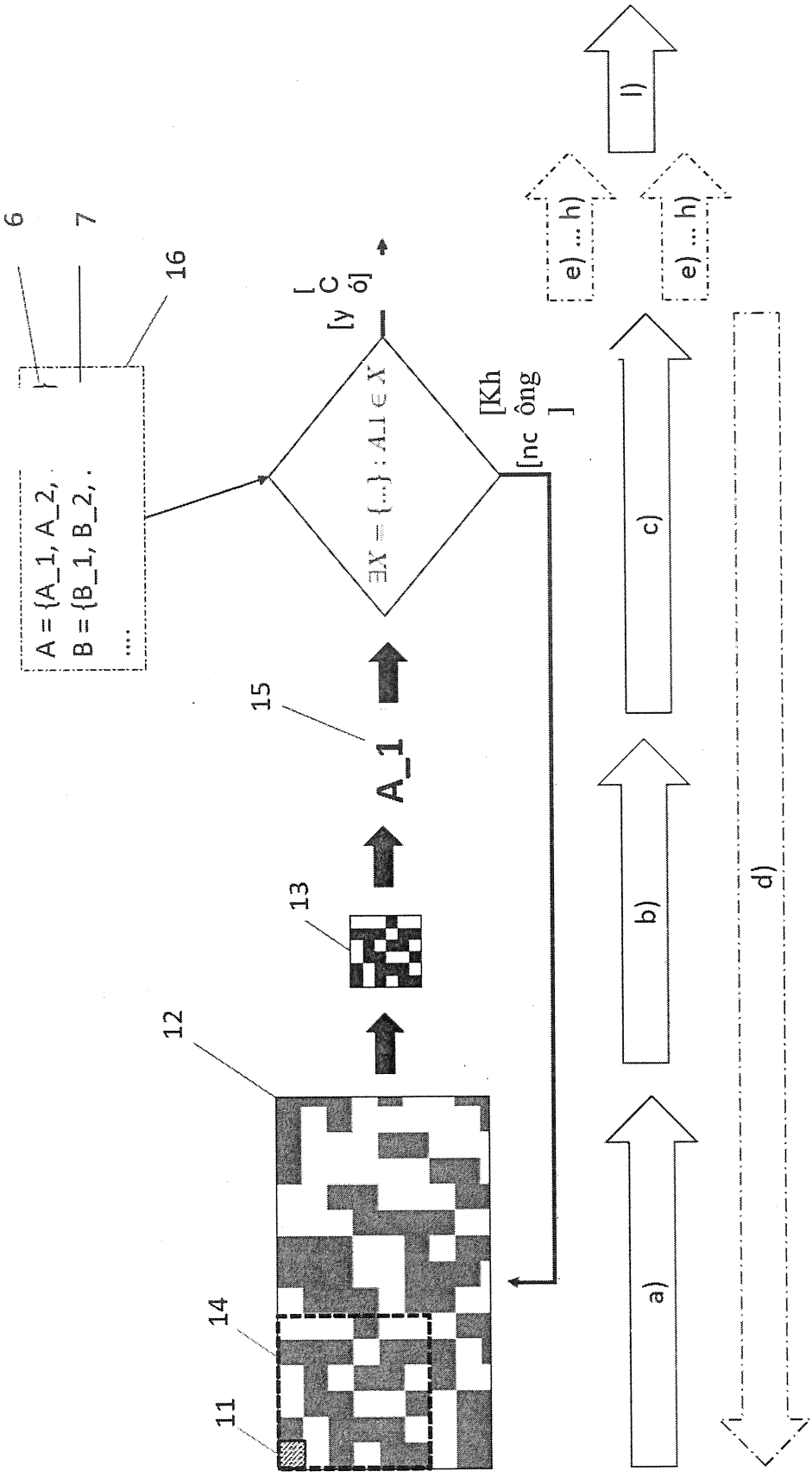


FIG 3a

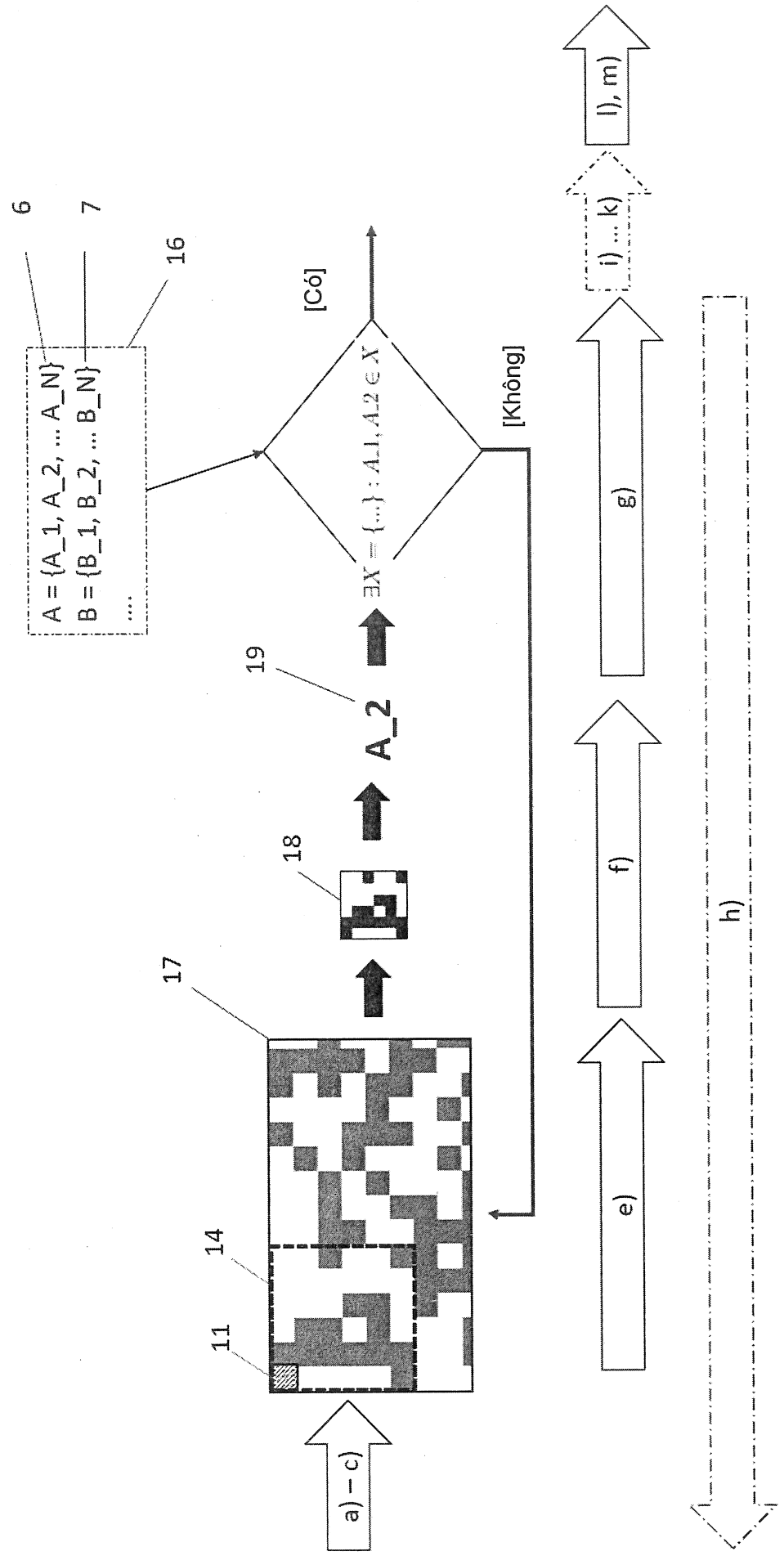

a) – c)
11
14
17
18
19
A_2
$\exists X = \{...\} : A\_1, A\_2 \in X$
[Có]
[Không]
A = {A_1, A_2, ... A_N}
B = {B_1, B_2, ... B_N}
....
6
7
16
e)
f)
g)
h)
i) ... k)
l), m)

FIG 3b

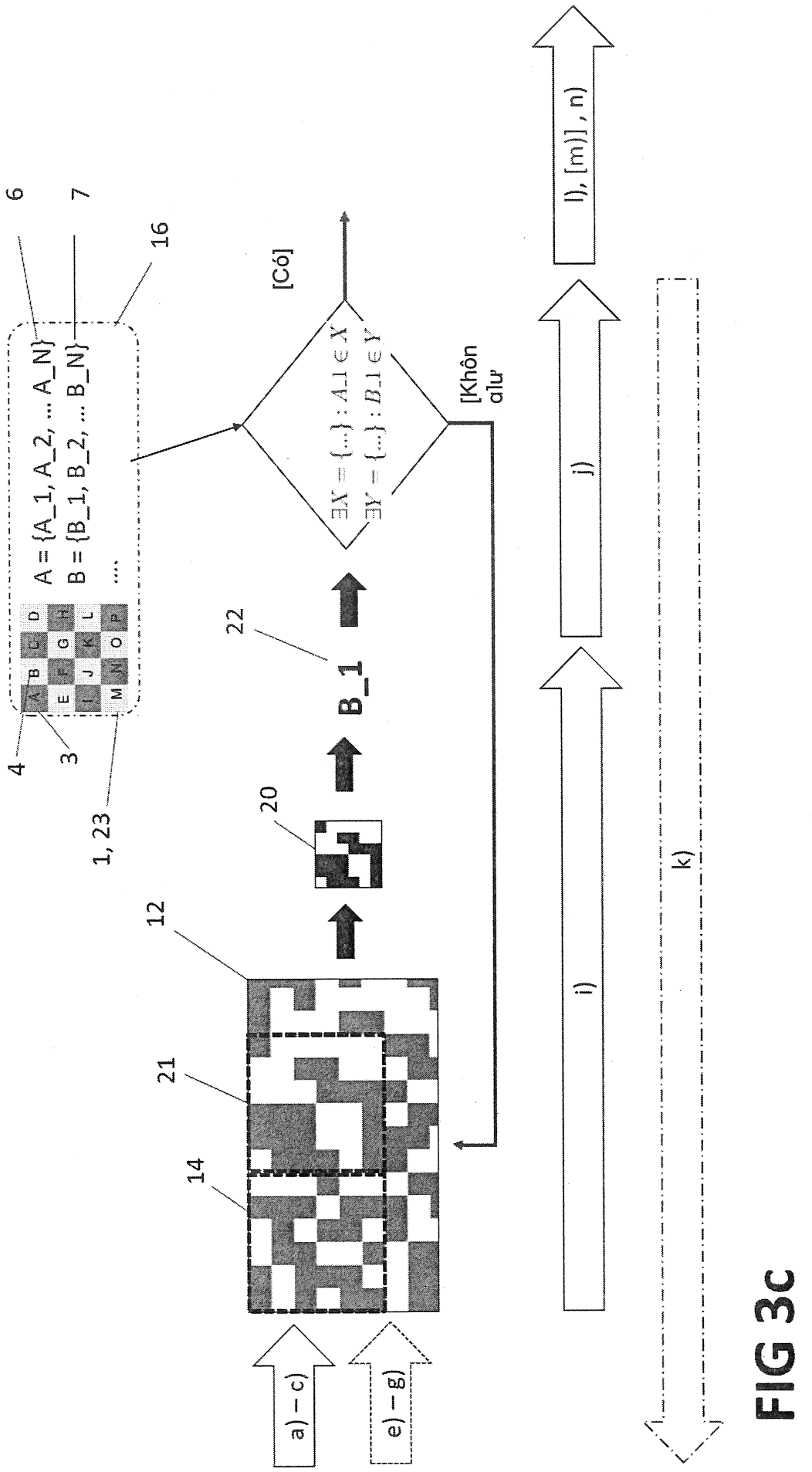

a) – c)
e) – g)
12
21
14
20
22
B_1
[Có]
[Khôn
g]
$\exists X = \{\ldots\} : A\_1 \in X$
$\exists Y = \{\ldots\} : B\_1 \in Y$
6
7
16
A = {A_1, A_2, ... A_N}
B = {B_1, B_2, ... B_N}
....
4
3
1, 23
i)
j)
k)
l), [m)] , n)

FIG 3c